06 (42) / 2023

CZASOPISMO RYNKU SECURITY

a&S POLSKA

www.aspolska.pl

20 zł
(w tym 8% VAT)

ISSN 2451-5175

RAPORT Security 50

Na podium bez zmian – liderzy utrzymali swoje pozycje! Sztuczna inteligencja i rozwiązania chmurowe nadal najpopularniejsze.

Co wpływa na polski handel?

Czynników zmian jest wiele. Branża security dostosowuje ofertę, aby spełnić rosnące wymagania menedżerów sektora handlowego.

Odporni na stres

Pracownik wyszkolony, to pracownik przygotowany. Warto szkolić z zarządzania w sytuacji kryzysowej, np. ataku terrorystycznego.

DC3.1 XL TEMPEST

Pierwsze produkowane w Polsce drzwi RC4 odporne na ulot elektromagnetyczny

Odporność na ulot elektromagnetyczny

Odporność na włamanie

Dowiedz się więcej:

DONIMET

Part of ASSA ABLOY

Szanowni Czytelnicy

Przeciętny Kowalski odwiedzający galerię handlową tuż przed świętami, z obłędem w oczach poszukujący prezentów, nie ma bladego pojęcia, ile osób pracowało na to, by wizyta w takim miejscu była nie tylko przyjemna, ale przede wszystkim bezpieczna. Nie zastanawia się też nad tym, ile w budynku działa synchronicznie różnych systemów, które mają sprawić, że wnętrze jest odpowiednio oświetlone, temperatura nie za wysoka i nie za niska, powietrze nie za suche, ale też nie za wilgotne, a świąteczne przeboje sączą się łagodnie do ucha. Z kolei Nowak za oczywistość przyjmuje fakt, że działają schody ruchome. Nie wie, bo i skąd miałby wiedzieć, że schody ruchome wyposażone są w stosowne czujniki prędkości i bezpieczeństwa, a wyjścia ewakuacyjne są pod stałym nadzorem kamer. Za naturalne uważa, że drzwi obrotowe wyposażone są w czujniki zapobiegające uwięźnięciu między skrzydłami. Tak to już bowiem jest, że każda osoba wchodząca do dużej galerii lub innego budynku użyteczności publicznej czyni to z ufnością, wierząc, że jest w jej wnętrzu bezpieczna.

Tylko Wy, Szanowni Czytelnicy, wiecie, ile pracy kosztuje to, by nie nadwyrężyć tego zaufania. Jak skomplikowane są systemy zabezpieczeń, co trzeba zrobić, by monitoring wizyjny nie rzucał się w oczy, ile trudu kosztowało takie zaprojektowanie wyjść ewakuacyjnych, by nie psuły wizji architekta. I tylko Wy wiecie, jaka odpowiedzialność spoczywa na waszych barkach. Olbrzymie rzesze ludzi każdego dnia odwiedzających polskie sklepy dzięki Wam może czynić to bezpiecznie.

O tym, jak ważne dla wszystkich jest poczucie bezpieczeństwa, może świadczyć kolejna edycja raportu *SECURITY 50* (str. 16) podsumowującego kondycję branży security w 2023 r. Z danych zawartych w raporcie jasno wynika, że wartość rynku urządzeń do dozoru wizyjnego w przyszłym roku wzrośnie o ok. 10%. Za ten wzrost odpowiadają zmieniające się potrzeby klientów, którzy chcą swoim organizacjom zapewnić bezpieczeństwo, zarówno fizyczne, jak i cyfrowe. Szczególnie ta ostatnia potrzeba zyskuje na znaczeniu. W artykule *Polski rodzinny handel ma znaczącą przewagę* (str. 50) piszemy m.in. o skali zagrożeń atakami hakerskimi wymierzonymi w sieci handlowe.

Jak zatem sobie radzić w tych turbulentnych czasach, gdy na świecie wybuchają kolejne konflikty zbrojne, a za naszą wschodnią granicą (a także i na niej) dochodzi do kolejnych niepokojących wydarzeń? Jacek Pałkiewicz, znany dziennikarz, podróżnik, propagator sztuk przetrwania, mówi wywiadzie (str. 66): *Odporność na stres można budować. Panujmy nad wyobraźnią i róbmy swoje.*

I tego właśnie Państwu życzymy w nadchodzącym nowym roku. Odporności na stres. Ale też wielu udanych inwestycji. Dla bezpieczeństwa nas wszystkich.

Redakcja

CZASOPISMO RYNKU SECURITY

a&s POLSKA

06 (42) / 2023

SPIS TREŚCI

REDAKCJA

ADRES REDAKCJI
a&s Polska
ul. M. Rodziewiczówny 1 lok. 801
04-187 Warszawa

info@aspolska.pl
www.aspolska.pl

PREZES ZARZĄDU
Mariusz Kucharski

REDAKTOR NACZELNA
Marta Dynakowska

Z-CA RED. NACZELNEGO
Jan T. Grusznic

REDAKCJA
Monika Żuber-Mamakis
Adela Prochyra

DZIAŁ REKLAMY
Iwona Krawiec

DZIAŁ PROJEKTÓW SPECJALNYCH
Jolanta A. Kucharska
Aleksandra Czapska

CENTRUM KOMPETENCJI
Jacek Grzechowiak

KOREKTA
Jolanta Kucharska

PROJEKT GRAFICZNY I SKŁAD
Bogusław Kalwala

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

www.sensgroup.pl

Redakcja zastrzega sobie prawo skracania i redagowania nadesłanych tekstów. Tytuły i śródtytuły pochodzą od Redakcji.

Opinie autorów nie muszą być tożsame z poglądami Redakcji.

Za treść reklam i artykułów partnerów Redakcja nie odpowiada.

Nie przegapimy tej chwili

Nowe modele
Kamer ANPR od BCS Line.
BCS-L-TIP74VSR3-ITC-Ai3
i BCS-L-TIP74VSR6-ITC-Ai3,
automatyzacja pracy przejazdu,
rozpoznanie przy dużej prędkości,
metadane o rozpozanym pojeździe.

» Więcej przeczytasz na stronie 10

POLSKA MARKA BCS

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

BCS®

CZASOPISMO RYNKU SECURITY

a&S POLSKA

06 (42) / 2023

SPIS TREŚCI

System kontroli dostępu RACS 5 w sektorze komercyjnym

roger
Intelligence for Building

- **Funkcjonalność**, dzięki której nie trzeba wybierać pomiędzy komfortem a bezpieczeństwem.
- **Design urządzeń** dobrze komponujących się z wnętrzami nowoczesnych przestrzeni biurowych.
- **Niezawodność** zapewniająca tysiącom użytkowników obiektu dostęp do ich miejsca pracy każdego dnia, przez wiele lat.
- **Efektywność** zarządzania przestrzenią, zasobami i użytkownikami dzięki integracji z aplikacjami biurowymi.
- **Redukcja** zużycia energii elektrycznej dzięki integracji z systemami windowymi oraz funkcjom automatyki budynkowej.

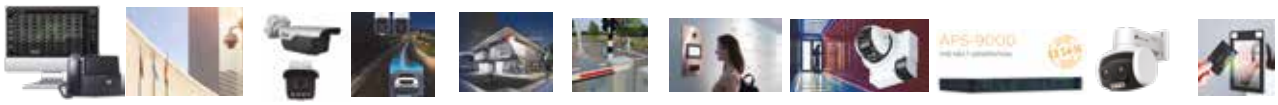
Wybrane realizacje






Prezentujemy najnowsze urządzenia z oferty firm

ASCS, Axis Communications, BCS (NSS), Hanwha Vision, Hikvision, Linc Polska, Nedap Security Management, Optex, Schrack Seconet Polska, TP-Link, ZKTeco



ASCS

System nagłośnieniowo-interkomowy V-Cast w chmurze

System nagłośnieniowo-interkomowy w chmurze to nowoczesne rozwiązanie, które zapewnia wiele korzyści. Jest niezwykle elastyczny, co pozwala na dostosowanie go do indywidualnych wymagań użytkownika, można go też łatwo rozbudowywać lub modernizować w zależności od zmieniających się potrzeb.

Dzięki dostępowi przez Internet użytkownicy mają kontrolę nad systemem z dowolnego miejsca na świecie, a zastosowanie otwartego protokołu SIP nie powoduje ograniczenia do jednego rodzaju urządzeń.

System V-Cast w chmurze oferuje nie tylko możliwość aktywacji nagłośnienia w monitorowanych obiektach, ale również możliwość połączenia zwrotnego przez interkom zamontowany w pomieszczeniu. Osoba potrzebująca pomocy może szybko zadzwonić do Centrum Ochrony i nawiązać kontakt, a następnie zostać przekierowana do odpowiednich służb.

Wykorzystując system V-Cast w funkcji centrali telefonicznej, otrzymujemy także dodatkowe korzyści. Automat może dzwoniącą osobę wstępnie zweryfikować po wpisanym kodzie, dzięki czemu operator wie, z kim rozmawia, i nie musi poświęcać czasu na jej weryfikację – może przejść od razu do działania.

System jest zintegrowany z najpopularniejszymi platformami oprogramowania dla stacji monitorowania.

Więcej na: ascs.pl

AXIS COMMUNICATIONS

Kamera panoramiczna AXIS P3827-PVE

Ta wieloprzetwornikowa kamera o rozdzielczości 7 Mpix oferuje jeden płynny i spójny strumień wideo z panoramicznym pokryciem 180° i rejestruje obrazy o wysokiej rozdzielczości i niewiarygodnej szczegółowości z prędkością strumienia do 30 kl./s.

Dzięki zabiegowi prostowania zakrzywienia horyzontu obrazy odpowiadają rzeczywistości. Kamera automatycznie optymalizuje balans bieli i czas ekspozycji. Co więcej, dzięki funkcji Forensic WDR oferuje doskonałą użyteczność dostarczania dowodów na potrzeby dochodzeń.

Kamera AXIS P3827-PVE z procesorem ARTPEC-8 jest wyposażona w moduł przetwarzania danych z funkcją głębokiego uczenia (DLPU). Pozwala to na lepsze przetwarzanie, gromadzenie, przechowywanie i analizowanie jeszcze większej ilości danych na brzegu sieci. Dostarcza cenne metadane ułatwiające szybkie, łatwe i wydajne wyszukiwanie na obrazie na żywo i na zarejestrowanym materiale wideo. Dzięki AXIS Object Analytics kamera potrafi wykrywać i klasyfikować osoby, pojazdy i typy pojazdów, a wszystkie te funkcje można dostosować do konkretnych potrzeb użytkownika. Co więcej, obsługa ACAP w wersji 4. podnosi wartość systemu dzięki wykorzystaniu wyspecjalizowanych aplikacji opartych na głębokim uczeniu.

Ta niedroga kamera zapewnia korzyści płynące z zastosowania jednego urządzenia zamiast czterech. Dostępne są różne opcje montażu i regulacji pozycji, a jej instalacja jest szybka, ekonomiczna i łatwa. Kamera AXIS P3827-PVE ma wbudowane funkcje cyberbezpieczeństwa.

Więcej na: www.axis.com/pl-pl

NOVUS MANAGEMENT SYSTEM

AC

POLSKI PRODUKT

INTEGRACJA • KONFIGURACJA • WIZUALIZACJA

SYSTEMÓW BEZPIECZEŃSTWA

JAK TO DZIAŁA?

NMSAC.AAT.PL

NOVUS MANAGEMENT SYSTEM AC to profesjonalne polskie oprogramowanie zarządzające systemami bezpieczeństwa w obiektach.

Do nabycia u najlepszych instalatorów!

AAT SYSTEMY BEZPIECZEŃSTWA

PRODUCENT I DOSTAWCA ELEKTRONICZNYCH SYSTEMÓW ZABEZPIECZENIA MIENIA

www.aat.pl

BCS

Kamery z funkcją rozpoznawania numerów tablic rejestracyjnych

Modele BCS-L-TIP74VSR3-ITC-AI3 oraz BCS-L-TIP74VSR6-ITC-AI3 to kolejna generacja kamer przeznaczonych do rozpoznawania numerów tablic rejestracyjnych pojazdów.

Stosując kamery o rozdzielczości 4 Mpix, można łatwo zautomatyzować wjazd na teren obiektu. Oba prezentowane modele są wyposażone w dwa wyjścia alarmowe, każde z nich po rozpoznaniu numerów rejestracyjnych może samo sterować szlabanem. Model BCS-L-TIP74VSR3-ITC-AI3 jest wyposażony w obiektyw motozoom o ogniskowej 2,7-12 mm, co pozwala na prawidłowe rozpoznanie numerów z odległości do 10 m, natomiast BCS-L-TIP74VSR6-ITC-AI3 ma obiektyw o ogniskowej 8-32 mm, umożliwiający rozpoznanie tablic z odległości nawet 30 m.

W kamerze można stworzyć tzw. białą listę pojazdów uprawnionych do wjazdu, która może zawierać maks. do 110 tys. wpisów. Prawidłowe rozpoznanie rejestracji jest możliwe nawet przy prędkości poruszającego się pojazdu do 80 km/h (BCS-L-TIP74VSR3-ITC-AI3) lub 120 km/h (BCS-L-TIP74VSR6-ITC-AI3).

W kamerach można wybrać jeden z trzech trybów wyzwolenia detekcji: przez analizę obrazu wideo, uruchamiając jedno z dwóch wejść alarmowych, bądź stosując tryb łączony, w którym oba wymienione warunki muszą

zostać spełnione. Wejście/wyjście audio umożliwia dwukierunkową komunikację operatora z kierowcą pojazdu oczekującego na wjazd.

Kamery można połączyć z rejestratorami IP BCS Line serii 4K i 4KE(2) lub aplikacją BCS Manager, zapewniając w ten sposób dodatkowe funkcjonalności.

Więcej na: www.bcs.pl

HANWHA VISION

Kamery PTZ PLUS ze sztuczną inteligencją

Hanwha Vision wprowadziła na rynek serię kamer PTZ PLUS wykorzystującą sztuczną inteligencję (AI) do jeszcze dokładniejszego wykrywania i klasyfikacji osób, obiektów oraz pojazdów. Ta wysoko wydajna seria jest przeznaczona do monitorowania dużych otwartych przestrzeni, takich jak lotniska, parkingi, stadiony, centra miast czy obszary przemysłowe.

Zaawansowana sztuczna inteligencja (AI) powoduje, że kamery ignorują nieistotne obiekty, takie jak ruszające się drzewa, przesuwające się chmury czy zwierzęta, które zazwyczaj są przyczyną fałszywych alarmów w przypadku standardowych technologii detekcji ruchu.

Protokół transmisji danych MQTT pozwala mu na bezproblemową współpracę kamery z innymi urządzeniami, w tym z czujnikami IoT. Informacje przekazywane poprzez MQTT powodują, że kamera będzie automatycznie nakierować się na wejścia/wyjścia, aby potwierdzić wizualnie, czy osoba ma autoryzowany dostęp do danego obszaru. Następnie prześle operatorowi e-mail z raportem. Możliwość komunikacji i wymiany danych z innymi urządzeniami poprzez MQTT sprawia, że kamera AI PTZ PLUS staje się urządzeniem zainstalowanym nie tylko na potrzeby bezpieczeństwa, ale również do analizy otrzymanych danych dla celów biznesowych.

Kamery AI PTZ Plus ważą o 65% mniej niż większość kamer PTZ, co przyczynia się do łatwiejszej instalacji. Podłączenie kabla staje się łatwe i szybkie dzięki pojedynczemu portowi RJ45. Ponadto elastyczna tuleja kablowa eliminuje potrzebę dodatkowych prac wodoszczelnych, skutecznie zapobiegając wnikaniu wody i zapewniając lepszą ochronę.

Więcej na: hanwhavision.eu/pl/

HIKVISION

Smart Hybrid Light – nowa seria kamer Hikvision

Nowe kamery z technologią Smart Hybrid Light, które dołączyły do serii Pro, cechują się innowacyjnym podejściem do rejestrowania obrazu w warunkach słabego oświetlenia.

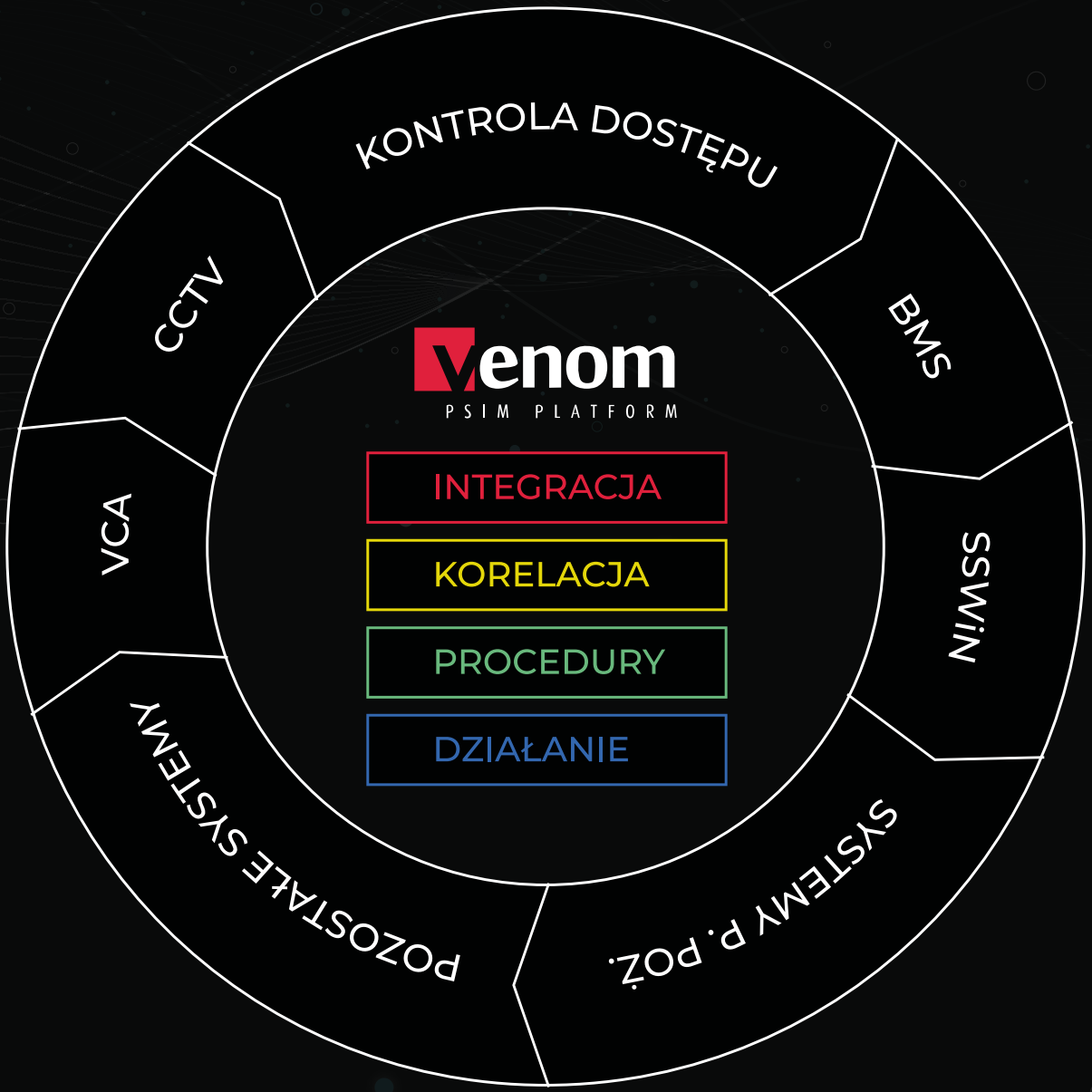
Rozwiązanie zapewniono dzięki zastosowaniu najwyższej jakości obiektywu z przysłoną F1.0, który gwarantuje jasny i wyraźny obraz niezależnie od pory dnia. Kamery z technologią Smart Hybrid Light oferują aż trzy tryby oświetlania sceny – klasyczna podczerwień, białe światło LED oraz tryb inteligentny, który wyzwoli oświetlacz światła białego dopiero wtedy, gdy intruz pojawi się na zdefiniowanym wcześniej obszarze.

Do skutecznego monitorowania otoczenia i zwiększenia poziomu bezpieczeństwa przyczynią się z pewnością zaawansowane funkcje inteligentnej analizy obrazu oraz odstraszania intruzów. Rozwiązanie to wyróżnia się na rynku m.in. dzięki zastosowaniu technologii AcuSense, która rozpoznaje ludzi oraz pojazdy spośród innych obiektów w otoczeniu i skupia się na prawdziwym zagrożeniu.

Dzięki odstraszaniu intruzów w czasie rzeczywistym i skuteczniejszemu rejestrowaniu kluczowych szczegółów kamery te znakomicie sprawdzają się w takich zastosowaniach, jak magazyny, sklepy detaliczne, ulice miast oraz rezydencje.

Więcej na: www.hikvision.com/pl

AVIGILON™ MOTOROLA SOLUTIONS Venom PSIM PLATFORM



MEGAVISION TECHNOLOGY Sp. z o. o., Heliotropów 1, 04-796 Warszawa, tel. **+48 22 292 3 292**, e-mail: **psim@psim.pl**

NEDAP SECURITY MANAGEMENT

Integracja AEOS z rozpoznawaniem twarzy SmartFace

Platforma kontroli dostępu AEOS wraz z systemem AEOS Locker Management firmy Nedap zostały zintegrowane z wiodącą w branży technologią rozpoznawania twarzy SmartFace firmy Innovatrics.

Dzięki współpracy obu firm użytkownicy mogą zdecydować, czy chcą używać standardowej karty RFID, czy postawią jednak na wygodę i skorzystają z rozpoznawania twarzy, aby wejść do budynku, a następnie uzyskać dostęp do konkretnej szafki.

Obu firmom zależy przede wszystkim na bezpieczeństwie oraz wygodzie użytkownika, ale nie zapomniano również o administratorach systemu. Do rejestracji użytkownika wykorzystywane jest już istniejące zdjęcie w profilu osobowym systemu kontroli dostępu AEOS, które następnie może być wykorzystane do stworzenia wzorca biometrycznego twarzy. Takie podejście eliminuje konieczność przeprowadzenia osobnego procesu wprowadzania wzorca biometrycznego od każdego z użytkowników, co znacząco skraca czas implementacji oraz upraszcza codzienną obsługę systemu.

Więcej na: www.nedapsecurity.com/pl/pl

SMART-I

CortexParking – kontrola dostępu z wykorzystaniem jednej kamery AVUTEC ANPR i szlabanu

Samochód wjeżdża na parking. Kamera AVUTEC ANPR odczytuje jego tablicę rejestracyjną, sprawdza ją na białej liście i po potwierdzeniu otwiera szlaban. To brzmi prosto... i takie też jest.

CortexParking opracowano z myślą o małych parkingach, które nie wymagają wszystkich funkcjonalności systemu kontroli dostępu, ale potrzebują dokładności i precyzji. Otwarcie szlabanu pojazdom znajdującym się na białej liście jest rozwiązaniem prostym i skutecznym.

Sekret prostoty CortexParking polega na tym, że AVUTEC ANPR to coś więcej niż tylko kamera. To kompletny system, który realizuje swoje zadania bez konieczności stosowania dodatkowej mocy obliczeniowej serwera lub innych urządzeń peryferyjnych. Urządzenie rozpoznaje tablice rejestracyjne i przechowuje je w pamięci. Może też nagrywać wideo. Odczytane tablice są sprawdzane na białej liście w bazie danych; po znalezieniu dopasowania kamera wykorzystuje swoje porty we/wy do otwarcia szlabanu.

Zarządzanie białą listą za pomocą aplikacji CortexParking

CortexParking jest wyposażona w oprogramowanie do zarządzania autoryzacją dostępu. Umożliwia też wyświetlanie obrazu z wejścia w czasie teraźniejszym i ręczne korygowanie otwarcia szlabanu po kontroli wzrokowej.

To przyjazna dla użytkownika aplikacja, która w prosty i szybki sposób kontroluje wjazdy pojazdów na parking i wyjazdy z niego. Można ją obsługiwać w recepcji, dodając lub usuwając tablice rejestracyjne z białej listy.

Więcej na: www.smart-i.pl

OPTEX

Precyzyjna detekcja LiDAR z REDSCAN mini-PRO

OPTEX ogłosił premierę najnowszej serii detektorów laserowych REDSCAN mini-Pro, wyposażonych w zintegrowaną kamerę z oświetlaczem. Seria REDSCAN LiDAR zapewnia dokładną i ultraszybką detekcję laserową krótkiego zasięgu oraz weryfikację wizualną w środowiskach wymagających wysokiego poziomu bezpieczeństwa, niezawodnie działając nawet w ekstremalnych warunkach atmosferycznych.

Nowy detektor z serii REDSCAN LiDAR tworzy niewidzialne ściany lub płaszczyzny detekcji o wymiarach 20 x 20 m i kącie 95⁰ oraz analizuje rozmiar, położenie i odległość poruszającego się obiektu. Zintegrowana z nim kamera dozorowa do weryfikacji alarmów i nagrywania zdarzeń obejmuje widokiem cały obszar detekcji. Jest wyposażona w oświetlacz IR z automatyczną regulacją, dzięki czemu wykrywany obiekt jest wyraźnie widoczny nawet w nocy lub w słabo oświetlonych miejscach. Sygnały alarmowe wraz z obrazem z kamery są zapisywane do pamięci wewnętrznej (maks. 500 zdarzeń).

Elastyczne opcje montażu zapewniają poziomy, pionowy lub nachylony pod kątem obszar detekcji, który można podzielić na 8 niezależnych stref alarmowania o dowolnym kształcie, położeniu i czułości.

Seria spełnia wymagania profilu S standardu ONVIF, co umożliwia wysyłanie standardowych sygnałów alarmowych do systemu dozoru wizyjnego zgodnego z ONVIF. Czujki są zgodne z protokołami sieciowymi (np. DNS, DHCP, NTP, Ws-Discovery). Wyjścia przekaźnikowe umożliwiają podłączenie urządzenia do tradycyjnej centrali alarmowej.

Więcej na: www.optex-europe.com/pl

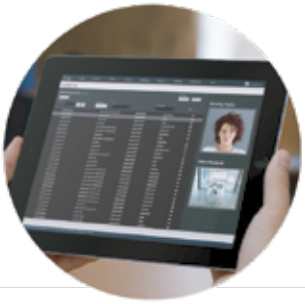
brivo

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

PARTNER:

smart-i

Ul. Marii Rodziewiczówny 1/810,
04-187 Warszawa

www.smart-i.pl

SCHRACK SECONET POLSKA

Nowa generacja głównego kontrolera systemu APS®-APROSYS – APS-9000

Schrack Seconet Polska wprowadza do oferty najnowszy produkt uznanej na świecie marki g+m elektronik ag – kontroler główny systemu APS®-APROSYS – APS-9000.

Następca uznanego poprzednika, modułu APS-990, został zaprojektowany zgodnie z wymaganiami normy EN-54-16, dzięki czemu może być stosowany przede wszystkim w Dźwiękowych Systemach Ostrzegawczych (DSO) i w komercyjnych systemach nagłośnienia typu *Public Address* (PA), może też pracować w trybie *stand alone*.

Kompaktowa budowa kontrolera (zaledwie 1 HU) z powodzeniem zastępuje funkcjonalność wielu modułów poprzedniej generacji, np. APS-990, APS-177.2-LAN, APS-16.3, APS-56.1-NL, APS-19.2, APS-59.2 LAN, APS-01, oraz wiele innych (w tym również te z wbudowanym DSP), które występują jako osobne karty systemowe instalowane w ramach systemowych MC-03.

Nawet w wersji podstawowej kontroler APS-9000 ma wbudowane 4 niezależne odtwarzacze audio (następcy APS-19.2) umożliwiające rozsyłanie czterech komunikatów w tym samym czasie. Z kolei wbudowana karta sieciowa zapewnia połączenie dowolnej liczby systemów w sieci LAN i transmisję sygnałów audio z wykorzystaniem standardu AES67. Dodatkowo wbudowany procesor DSP zapewnia swobodny routing źródeł dźwięku oraz jego cyfrową obróbkę z zachowaniem jakości, jak to ma miejsce w przypadku profesjonalnych systemów koncertowych.

Kontroler APS-9000 uzyskał certyfikat CPR na zgodność z normą EN-PN-54-16 oraz Świadectwo Dopuszczenia zgodnie z wymaganiami Dz.U. 2010 nr 85 poz. 553 – oba dokumenty zostały wydane przez CNBOP-PIB.

Więcej na: www.schrack-seconet.com/pl

TP-LINK

TP-Link VIGI C540V – kamera sieciowa do obserwacji terenów rozległych

TP-Link VIGI C540V to dwuobiektywowa, zmiennoogniskowa, obrotowa kamera sieciowa w szczelnej obudowie (IP66), co zapewnia odporność na trudne warunki atmosferyczne i stabilne działanie na zewnątrz budynku.

VIGI C540V wyposażono w obiektyw o rozdzielczości 4 Mpix, czuły przetwornik obrazu i 4 wbudowane diody LED światła punktowego. Może być zasilana przez PoE lub zasilacz DC 12 V.

Kamera ma opcje tworzenia tras patrolu. 3-krotny zoom umożliwia obserwowanie odległych obiektów na rozległych obszarach. Jest wyposażona w mikrofon i głośnik oraz alarm dźwiękowy i świetlny do odstraszania intruzów.

Po ustawieniu obszarów kamera wykrywa: wtargnięcie na wyznaczony teren, przekroczenie linii, wejście do strefy i jej opuszczenie, pozostawienie lub zabranie przedmiotu. Wykrywa osoby zachowujące się podejrzanie i zmianę sceny uniemożliwiającą nagrywanie obrazu. Nagrania z kamery mogą być rejestrowane na rejestratorze sieciowym NVR i lokalnie na kartach microSD (do 256 GB).

Kamera wykorzystuje kompresję H.265+, co zmniejsza obciążenie sieci i obniża koszty bez

utraty jakości obrazu. Jest zgodna ze standardem ONVIF, dzięki czemu współpracuje z kamerami i rejestratorami różnych producentów.

Dzięki aplikacji VIGI na urządzenia przenośne (iOS, Android), produktami z tej serii można zarządzać z poziomu urządzenia mobilnego. Systemem można sterować z poziomu dedykowanego oprogramowania komputerowego. Urządzenie jest objęte 3-letnią gwarancją.

Więcej na: www.tp-link.com/pl

ZKTECO

BioOnCard – bezpieczeństwo danych biometrycznych

Technologia BioOnCard firmy ZKTeco to rozwiązanie biometryczne nowej generacji do płynnego uwierzytelniania za pomocą rozpoznawania dłoni i twarzy w systemach kontroli dostępu wyposażonych w urządzenia SpeedFace-V5L RFID oraz ProFace X [P].

Technologia ta zapewnia podwójną weryfikację dzięki wykorzystaniu zaawansowanych algorytmów do poprawy bezpieczeństwa obiektów przy jednoczesnym spełnieniu wymogów RODO. Jej działanie pozawala na rozpoznanie twarzy i/lub dłoni w czasie krótszym niż 1 sekunda po przeniesieniu wzorca z karty do urządzenia. Prezentowane rozwiązanie można łatwo zintegrować z większością kołowrotów lub bramek przejścia firmy ZKTeco. Współpracuje z oprogramowaniem ZKBioAccess oraz ZKBioCVSecurity, jest też dostępne do integracji z rozwiązaniami innych firm wykorzystującymi protokół PUSH. Gwarantuje całkowite bezpieczeństwo danych biometrycznych, gdyż dane te po zaszyfrowaniu i kompresji są przechowywane wewnątrz karty, a nie na serwerze czy innym urządzeniu zewnętrznym.

Rozwiązanie to spełnia wymogi przepisów RODO. Zapewnia większą prywatność danych osobistych posiadacza karty BioOnCard (Mifare 8 kB) i możliwość uwierzytelnienia bez połączenia urządzenia z wewnętrzną bazą danych. Biometryczne obrazy dłoni lub twarzy nigdy też nie są przechowywane na urządzeniu. Wzorce biometryczne są własnością użytkownika (tak jak jego dowód osobisty), przy czym zgubienie lub kradzież karty nie umożliwi dostępu znalazcy czy złodziejowi.

Więcej na: https://zkteco.eu/

POLON-ALFA

dobrze zaprojektowane BEZPIECZEŃSTWO

KOMPLEKSOWE
SYSTEMY SYGNALIZACJI POŻAROWEJ

• PRODUKCJA • SERWIS • SZKOLENIA
• WSPARCIE TECHNICZNE I PROJEKTOWE

AUTOMATYKA POŻAROWA

POLON-ALFA S.A. | 85-861 Bydgoszcz, ul. Glinki 155 | www.polon-alfa.pl

RAPORT

Rok 2023 w branży security

SECURITY 50

Przetasowania w branży zabezpieczeń

W roku 2022 branża security działała w warunkach spowolnienia gospodarczego wynikającego z utrzymujących się konsekwencji pandemii i z powodu innych czynników, w tym inflacji i napięć geopolitycznych. Z ekonomicznego punktu widzenia wg Banku Światowego wzrost PKB na świecie w 2022 r. wyniósł średnio 4,1% w porównaniu do 5,5% w 2021 r. Gospodarka w wysoko rozwiniętych krajach, np. w Stanach Zjednoczonych, i strefa euro wzrosły w ubiegłym roku o 3,8% w porównaniu z 5% w 2021 r., podczas gdy rynki wschodzące odnotowały wzrost o 4,6%, w porównaniu z 6,3% w 2021 r.

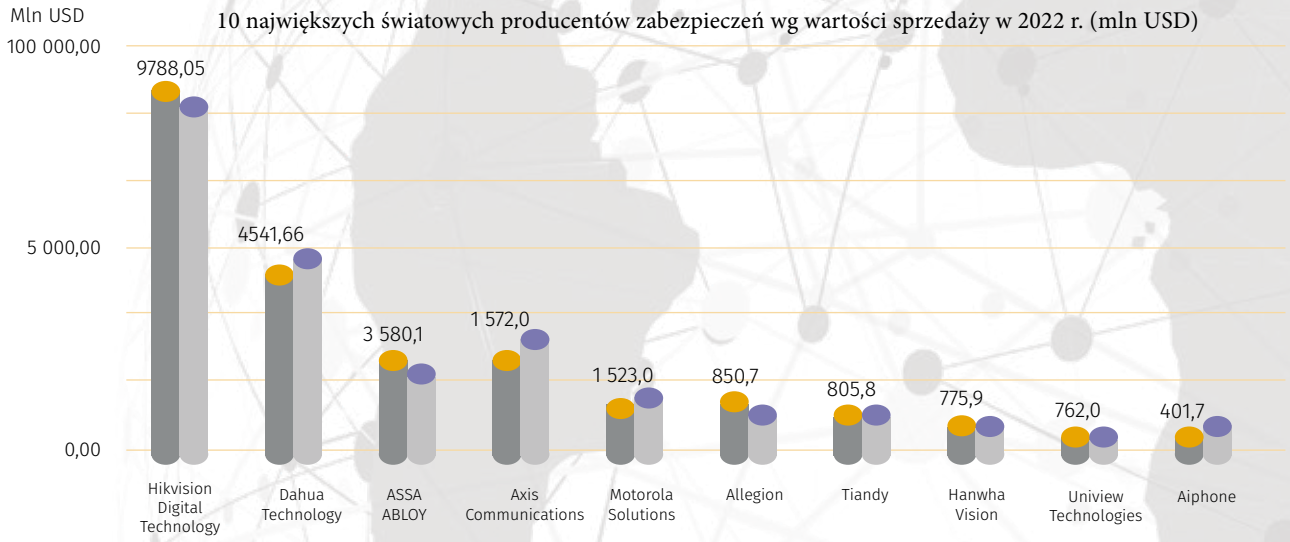
W Chinach w 2022 r. PKB wzrósł o 5,1% w porównaniu do 9% w 2021 r. Na słabszy wynik złożyły się m.in. blokady w różnych miastach, które władze wprowadziły ze względu na wzrost liczby przypadków COVID. Utrzymał się też kryzys na rynku nieruchomości. Wysiłki chińskiego rządu zmierzające do uregulowania limitów zadłużenia głównych chińskich deweloperów, takich jak Evergrande Group, spowodowały załamanie tego rynku. Pewną rolę odegrały również czynniki zewnętrzne. Napięcia geopolityczne między Stanami Zjednoczonymi a Chinami skłoniły USA do nałożenia na Państwo Środka poważnych ograniczeń i barier handlowych.

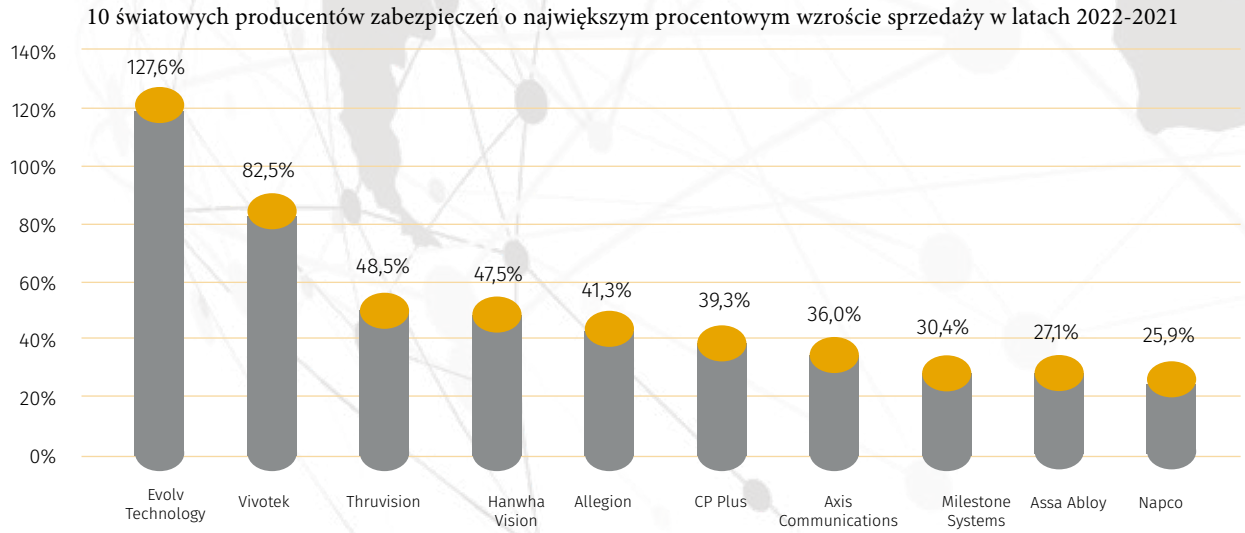
Wpływ na branżę zabezpieczeń

Jaki to miało wpływ na rynek security w ubiegłym roku? Na pierwszy rzut oka nie widać większych zmian w tegorocznym rankingu *Security 50*. Wśród 10 największych światowych producentów zabezpieczeń z sektora kontroli dostępu i monitoringu wizyjnego znalazły się Hikvision Digital Technology, Dahua Technology, ASSA ABLOY, Axis Communications, Motorola Solutions, Allegion, Tiandy, Hanwha Vision (dawniej Hanwha Techwin), Uniview Technologies i Aiphone.

Hikvision i Dahua pozostają największymi na świecie firmami z branży zabezpieczeń, a wartość ich sprzedaży w 2022 r. wyniosła odpowiednio: 9,8 mld USD i 4,5 mld USD (na podstawie średnich kursów wymiany walut IRS w 2022 r.). W zestawieniu pojawiły się dwie nowe firmy: chiński dostawca rozwiązań inteligentnego domu MEARI oraz koreański dostawca rozwiązań biometrycznych Union Community.

W tegorocznym zestawieniu *Security 50* znalazły się firmy, które odnotowały spadki. Spośród 17 przedsiębiorstw, które w latach 2021–22 odnotowały niższe przychody, aż 12 pochodzi z Chin. Wprawdzie można było oczekiwać spadku przychodów





firm chińskich, biorąc pod uwagę tamtejsze uwarunkowania, lecz liczba firm, których to dotyczy, oraz ich wielkość (ponad 40%) wywołują zaskoczenie.

Wewnętrzne i zewnętrzne wyzwania Chin – *lockdown*, kryzys na rynku nieruchomości i trudne stosunki z USA – odegrały swoją rolę.

– Chińskie wydatki rządowe zostały przekierowane z innych obszarów, m.in. na monitoring wideo, walkę z COVID-19 i wspieranie własnej gospodarki podczas lockdownu. Ograniczenia trwały znacznie dłużej, niż przewidywało wielu obserwatorów. Dopiero w grudniu 2022 r. chiński rząd ostatecznie złagodził swoją politykę zero COVID – powiedzieli Jon Cropley, główny analityk, i Josh Woodhouse, założyciel Novaira Insights, firmy analitycznej zajmującej się rynkiem IT.

Jednocześnie napięcia między Stanami Zjednoczonymi a Chinami, które doprowadziły do uchwalenia w 2019 r. przepisów (w ramach *National Defense Authorization Act* – NDAA) zakazujących firmom amerykańskim zakupu urządzeń do dozoru wizyjnego Hikvision i Dahua, spowodowały, że marki zachodnie i spoza Chin odnotowały proporcjonalny wzrost przychodów w 2022 r. Należą do nich Vivotec, (wzrost sprzedaży o 82,48%), Hanwha Vision (o 47,52%), Axis Communications (o 36,01%), Milestone Systems (o 30,43%) i IDIS (o 22,17%). Należy zauważyć, że wielu zachodnich sojuszników USA, np. Wielka Brytania, również uchwaliło przepisy podobne do NDAA.

– Odchodzenie od chińskich dostawców postępowało w szybkim tempie nie tylko w Stanach Zjednoczonych, ale także w całej Europie Północnej i krajach azjatyckich, w tym w Japonii i Korei Południowej. Po części wiele organizacji i integratorów systemów chce ustandaryzować urządzenia zgodnie z NDAA, aby zapewnić obecną i przyszłą działalność w USA. Również użytkownicy końcowi wyrażają obawy dotyczące spełniania przepisów w UE i Azji, słabych zabezpieczeń cyberbezpieczeństwa i potencjalnego uszczerbku na reputacji związanego z łamaniem praw człowieka przez niektórych zakazanych chińskich producentów – stwierdził Jamie Barnfield, dyrektor sprzedaży w IDIS Europe.

W tym roku można oczekiwać, że chińskie firmy poradzą sobie lepiej, nawet jeśli nie wyszły jeszcze na prostą.

– Przewiduje się, że rynek chiński nieco się ożywi w 2023 r., ale pozostanie zdecydowanie poniżej szczytowego poziomu z 2021 r. Wzrost popytu będzie znacznie niższy niż w latach poprzedzających pandemię. Jednocześnie słabnący kurs wymiany juana na dolara amerykańskiego również osłabi wzrost (mierzony w dolarach amerykańskich) – powiedzieli J. Cropley i J. Woodhouse.

Perspektywy i przewidywania

Ogólnie rzecz biorąc, w tym i przyszłym roku spodziewany jest wzrost na rynku zabezpieczeń, a Novaira Insights prognozuje, że wartość rynku urządzeń do dozoru wizyjnego wzrośnie odpowiednio o 11,8% i 10,2% w 2023 i 2024 r.

Eksperci branżowi zgadzają się z tym poglądem.

– W roku 2023 zaobserwowaliśmy pewien wzrost gospodarczy i ekspansję, chociaż był on nierównomiernie rozłożony w różnych regionach i sektorach rynku. Miało to różny wpływ na branżę zabezpieczeń – wyznał Choong Hoon Ha, dyrektor ds. sprzedaży i marketingu w Hanwha Vision. – *Pomimo to wymagania dotyczące bezpieczeństwa ze strony przedsiębiorstw i osób prywatnych*

» *Wśród 10 największych światowych producentów zabezpieczeń z sektora kontroli dostępu i monitoringu wizyjnego znalazły się Hikvision Digital Technology, Dahua Technology, ASSA ABLOY, Axis Communications, Motorola Solutions, Allegion, Tiandy, Hanwha Vision (dawniej Hanwha Techwin), Uniview Technologies i Aiphone.* «

wciąż rosną wraz ze wzrostem zapotrzebowaniem na zaawansowane systemy sieciowe, w tym inteligentne kamery dozorowe. Firmy są skłonne inwestować w rozwiązania zabezpieczeń, które chronią ich pracowników i aktywa, a nawet poprawiają wydajność i produktywność, zapewniając wgląd w działalność biznesową.

– Długoterminowy zrównoważony wzrost jest podstawą naszego planowania biznesowego. Zakładamy, że wyniesie on średnio 15%. I choć prognozuje się wzrost samego rynku, to Axis ponownie zamierza go wyprzedzić. Osiągniemy to poprzez dalsze poszerzanie naszego portfolio o nowe produkty, takie jak domofony, urządzenia kontroli dostępu, rozwiązania audio itp. – oznajmił Ray Mauritsson, prezes Axis Communications.

> *Sztuczna inteligencja będzie nadal zapewniać możliwość wprowadzania innowacji w całej branży. Zastosowanie AI do danych z fuzji czujników spowoduje przesunięcie rozwiązań zabezpieczeń w kierunku możliwości proaktywnych, które generują nową wartość. Sztuczna inteligencja jest wciąż w fazie transformacji, ale jej zastosowanie w branży jest duże i wyraźne.*

Trendy: sztuczna inteligencja, chmura i dostęp mobilny

Dominujące trendy w bezpieczeństwie to w dalszym ciągu sztuczna inteligencja i rozwiązania chmurowe.

– Sztuczna inteligencja będzie nadal zapewniać możliwość wprowadzania innowacji w całej branży. Zastosowanie AI do danych z fuzji czujników (łączenie i interpretowanie danych wejściowych z kamer i innych sensorów) spowoduje przesunięcie rozwiązań zabezpieczeń w kierunku możliwości proaktywnych, które generują nową wartość. Sztuczna inteligencja jest wciąż w fazie transformacji, ale jej zastosowanie w branży jest duże i wyraźne – powiedział Vince Wenos, wiceprezes i dyrektor ds. technicznych w Allegion.

– W tym roku byliśmy świadkami rosnącego zapotrzebowania klientów na maksymalizację możliwości, jakie dają kamery i czujniki, z naciskiem na funkcje analityczne. W branży nadal obserwuje się dominujący trend analityki brzegowej, a coraz większa liczba producentów kamer rozszerza swoje wsparcie dla tej technologii – oceniał William Hinton, Product Line Manager for Video w Genetec.

Według Hanwha klienci poszukują technologii, które pomogą im poprawić dokładność wykrywania zdarzeń oraz uczynić ich systemy monitoringu wizyjnego bardziej skalowalnymi i opłacalnymi. Chcą czerpać korzyści z zastosowania analizy wideo.

– Innymi słowy, szukają technologii bazującej na sztucznej inteligencji i chmurze – powiedział Choong Hoon Ha. – *Wielu klientów wciąż znajduje się na wczesnym etapie wdrażania rozwiązań do dozoru wizyjnego opartych na AI i chmurze. Oczekuje się jednak, że przyjęcie tych technologii przyspieszy w nadchodzących latach, ponieważ klienci dostrzegają korzyści, jakie mogą one zaoferować.*

Tymczasem wśród głównych trendów w 2023 r. pojawiły się również poświadczenia mobilne.

– Rosnąca popularność poświadczeń mobilnych i powiązanych z nimi czytników zapewnia dalszy wzrost branży security – podkreślił V. Wenos. – Mobilne dane uwierzytelniające nadal cieszą się zainteresowaniem klientów, ponieważ zapewniają większy komfort użytkownikom końcowym i dodatkową wartość operatorom systemów. Portfele cyfrowe, będące pochodną dostępu mobilnego, również zyskują na popularności.

– Obserwujemy duże zainteresowanie portfelami cyfrowymi w dużych, zaawansowanych technologicznie budynkach biurowych. Pierwszym europejskim wdrożeniem identyfikatora pracowniczego Apple Wallet był londyński 22 Bishopsgate, reklamowany jako najbardziej inteligentny budynek na świecie. 14 tys. użytkowników tego obiektu może teraz używać tylko swojego iPhone'a lub Apple Watcha, aby móc wejść do biura oraz korzystać ze wszystkich udogodnień

budynku – powiedział Prabhu Patel, dyrektor handlowy ds. rozwiązań kontroli dostępu w ASEAN i Indiach w HID.

Cyberbezpieczeństwo nadal jest ważnym tematem, ponieważ coraz więcej urządzeń działa online.

– *Od kilku lat obserwujemy rosnący nacisk na cyberbezpieczeństwo rozwiązań. Klienci są świadomi zwiększającego się ryzyka, wymagając solidnych procesów, czujności i przejrzystości. Gdy pojawiają się luki w zabezpieczeniach, przejrzystość dostawców jest niezbędna, gdyż umożliwia klientom szybką reakcję* – podkreślił R. Mauritsson.

Elastyczne płatności

W tym roku co najmniej dwie firmy oferują klientom elastyczne opcje płatności. Są to i-PRO, która wprowadziła FlexPay, oraz Eagle Eye Networks, która uruchomiła Eagle Eye Camera Direct Complete. Programy te mają na celu pomóc klientom osiągnąć większą elastyczność płatności, zmniejszyć początkowe inwestycje i ogólnie stać się bardziej konkurencyjnymi.

– *W niektórych organizacjach za coraz większą liczbę operacji związanych z bezpieczeństwem odpowiadają działy IT preferujące większy koszt operacyjny (OPEX), choć dla branży zabezpieczeń typowym wyborem są nakłady inwestycyjne (CAPEX)* – stwierdzili J. Cropley i J. Woodhouse. – *Ten rodzaj przejścia wskazuje na zmianę modelu biznesowego w chmurze. Jednak tylko sami dostawcy systemów monitoringu wizyjnego wiedzą, czy motyw ten jest związany wyłącznie z produktami konkretnych konkurentów.*

Konsolidacja kontra mniejsze start-upy

W branży zabezpieczeń nadal widać dwie ścierające się tendencje. Jedną z nich jest konsolidacja branży. Ostatnie przykłady obejmują transakcje przejęcia między ACRE i SISCO, Motorola Solutions i Rave Mobile Safety oraz IDIS i Costar. Jednocześnie obserwuje się również pojawienie się mniejszych firm koncentrujących się na rozwiązaniach w chmurze i sztucznej inteligencji. Nie wiadomo jeszcze, która strategia przeważy.

Jak twierdzą J. Cropley i J. Woodhouse, skala działania ma swoje zalety. – *Każdy scenariusz monitoringu wizyjnego jest inny, opracowywany pod konkretną inwestycję. Zmienne obejmują rozmiar instalacji, to, czy jest ona wewnątrz, czy na zewnątrz, a także warunki oświetleniowe i pogodowe. Jednocześnie kanał sprzedaży znacznie się różni w zależności od lokalizacji geograficznej, z których każda ma innych dystrybutorów, integratorów systemów i instalatorów obsługujących potrzeby klienta. Duzi dostawcy dysponują zarówno rozwiązaniami spełniającymi wszystkie scenariusze, jak i zasobami umożliwiającymi obsługę różnych kanałów w szerokim obszarze geograficznym* – podsumowali. •

SECURITY 50

Największe firmy branży security na świecie

asmag.com Security 50 to coroczny ranking 50 największych producentów systemów zabezpieczeń na świecie, oparty na przychodach i zyskach ze sprzedaży urządzeń i rozwiązań bezpieczeństwa. To jeden z najczęściej czytanych i długoletnich rankingów branżowych.

Analizując dane notowane w publicznych lub przesłanych raportach finansowych za rok 2022, wyróżniono zarówno światowych liderów, jak i nowe podmioty na rynku.

Ranking odzwierciedla dynamikę i rozwój branży, która porusza się w ciągle 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 zabezpieczenia ppoż. oraz inne powiązane.
- Podmioty, które przedstawiły sprawozdania finansowe za rok budżetowy 2022 i rok budżetowy 2021, 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 asmag.com pod kątem rozpoznawalności marki i udziałów w globalnym rynku.

Uwagi do danych finansowych:

Redakcja asamg.com nie ponosi odpowiedzialności za informacje finansowe dostarczone przez poszczególne firmy.

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

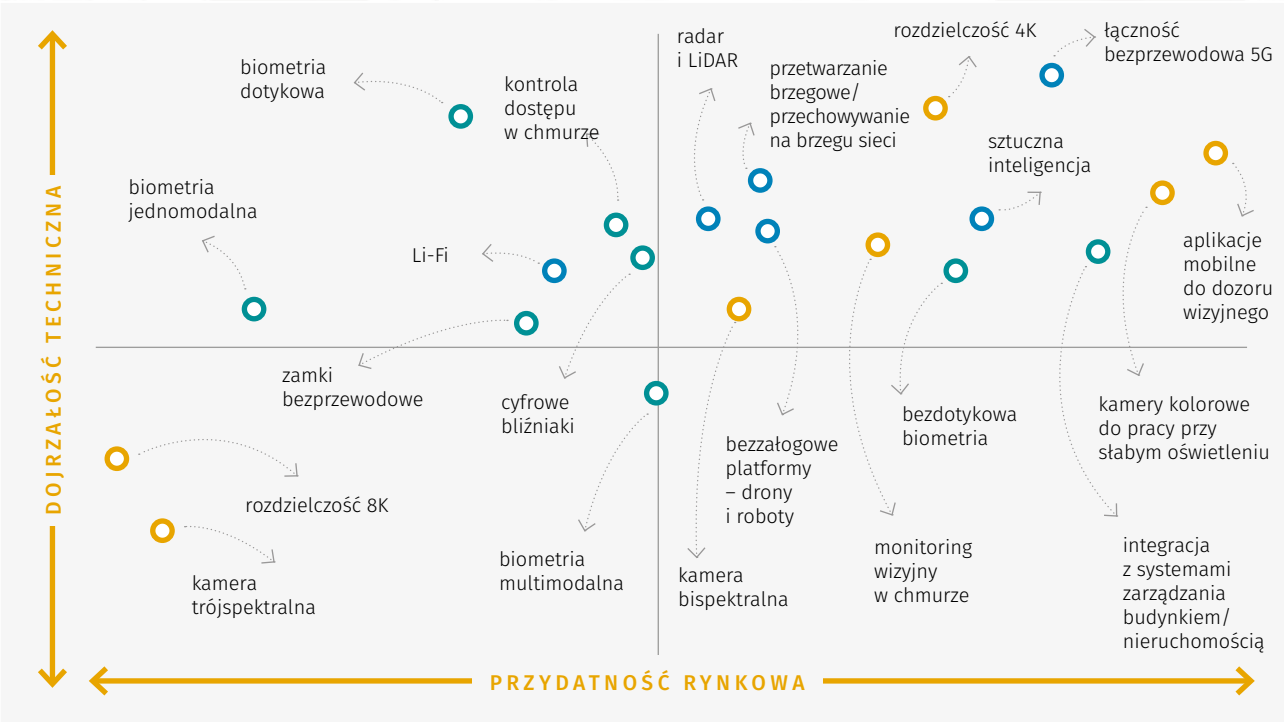
W rezultacie powstało jak najbardziej obiektywne zestawienie firm, które podzieliły się swoimi wynikami sprzedaży za lata 2021-22. ●

2023 S50	2022 S50	Nazwa firmy	Siedziba	Głowny obszar działania	PRZYCHODY W 2021 R. (MLN USD)	PRZYCHODY W 2022 R. (MLN USD)	WZROST PRZYCHODÓW (2022-2021)
1	1	HIKVISION DIGITAL TECHNOLOGY (telewizja dozorowa)	Chiny	różne	9 788,0	9 679,9	1,1%
2	2	DAHUA TECHNOLOGY	Chiny	różne	4 541,7	4 879,0	-6,9%
3	3	ASSA ABLOY (zamki elektromechaniczne i elektroniczne)	Szwecja	kontrola dostępu	3 580,1	2 815,9	27,1%
4	4	AXIS COMMUNICATIONS	Szwecja	różne	1 572,0	1 155,8	36,0%
5	5	MOTOROLA SOLUTIONS (telewizja dozorowa i analityka)	USA	różne	1 523,0	1 226,0	24,2%
6	8	ALLEGION (produkty elektroniczne i kontrola dostępu)	USA	kontrola dostępu	850,7	602,2	41,3%
7	7	TIANDY	Chiny	telewizja dozorowa	805,8	791,1	1,9%
8	9	HANWHA VISION	Korea	telewizja dozorowa	775,9	526,0	47,5%
9	6	UNIVIEW TECHNOLOGIES	Chiny	telewizja dozorowa	762,0	902,4	-15,6%
10	10	AIPHONE	Japonia	domofony	401,7	395,5	1,6%
11	13	INTELBRAS	Brazylia	różne	374,1	305,8	22,3%
12	17	VIVOTEK	Tajwan	telewizja dozorowa	333,7	182,9	82,5%
13	15	CP PLUS	Indie	telewizja dozorowa	292,1	209,7	39,3%
14	12	ZKTECO	Chiny	różne	285,1	290,5	-1,9%
15	11	DONGGUAN YUTONG OPTICAL TECHNOLOGY	Chiny	telewizja dozorowa (obiektywy)	274,3	306,4	-10,5%
16	18	MILESTONE SYSTEMS	Dania	telewizja dozorowa	210,3	161,2	30,4%
17	19	NEDAP	Holandia	różne	167,8	156,1	7,5%
18	21	IDIS	Korea	telewizja dozorowa	164,2	134,4	22,2%
19	14	INFINOVA	Chiny	telewizja dozorowa	153,7	235,5	-34,7%
20	20	TVT DIGITAL TECHNOLOGY	Chiny	telewizja dozorowa	144,2	149,1	-3,3%
21	26	NAPCO SECURITY TECHNOLOGIES	USA	różne	143,6	114,0	25,9%
22	24	OPTEX (systemy alarmowe)	Japonia	system alarmowy	122,2	103,9	17,7%
23	25	COMMAX	Korea	automatyka domowa	120,8	109,5	10,3%
24	23	RAYSHARP	Chiny	telewizja dozorowa	118,0	128,9	-8,5%
25	16	KEDACOM (telewizja dozorowa)	Chiny	telewizja dozorowa	115,5	193,2	-40,2%
26	30	IDENTIV	USA	kontrola dostępu	112,9	103,8	8,8%
27	27	GALLAGHER	Nowa Zelandia	kontrola dostępu	112,4	101,4	10,9%
28	32	SUPREMA	Korea	kontrola dostępu	94,3	80,1	17,8%
29	35	EVETAR	Chiny	telewizja dozorowa (obiektywy)	86,9	74,4	16,8%
30	33	TAMRON (telewizja dozorowa i obiektywy)	Japonia	telewizja dozorowa (obiektywy)	85,5	71,2	20,0%
31	N/A	MEARI	Chiny	automatyka domowa	82,2	82,5	-0,4%
32	34	KOCOM	Korea	automatyka domowa	73,8	71,7	2,8%
33	37	FOCTEK PHOTONICS	Chiny	telewizja dozorowa (obiektywy)	67,3	67,7	-0,6%
34	38	BLUESKY TECHNOLOGIES	Chiny	telewizja dozorowa	62,4	60,1	3,8%
35	36	MOBOTIX	Niemcy	telewizja dozorowa	58,9	65,6	-10,2%
36	39	DYNACOLOR	Tajwan	telewizja dozorowa	58,6	57,3	2,3%
37	40	COSTAR TECHNOLOGIES	USA	telewizja dozorowa	54,2	52,9	2,4%
38	48	EVOLV TECHNOLOGY	USA	systemy weryfikacji	49,6	21,8	127,6%
39	44	HI SHARP ELECTRONICS	Tajwan	telewizja dozorowa	35,9	31,3	15,0%
40	N/A	UNION COMMUNITY	Korea	kontrola dostępu	35,7	30,2	18,3%
41	43	SENSTAR TECHNOLOGIES	Izrael	różne	35,6	34,9	1,8%
42	41	C-PRO ELECTRONICS	Korea	telewizja dozorowa	34,1	40,4	-15,6%
43	45	SYNECTICS (dział systemów)	Wielka Brytania	telewizja dozorowa	29,8	25,5	17,1%
44	42	GEOVISION	Tajwan	telewizja dozorowa	29,2	47,7	-38,8%
45	46	ITX AI	Korea	telewizja dozorowa	20,6	24,3	-15,1%
46	52	ACTI	Tajwan	telewizja dozorowa	15,7	14,7	6,9%
47	N/A	THRUVISION	Wielka Brytania	weryfikacja osób	15,3	10,3	48,5%
48	49	AVA GROUP	Australia	różne	13,4	18,0	-25,7%
49	N/A	EVERFOCUS ELECTRONICS	Tajwan	telewizja dozorowa	10,9	12,6	-13,9%
50	47	HITRON SYSTEMS	Korea	telewizja dozorowa	8,3	21,3	-60,8%

SECURITY 50:

Badanie dojrzałości i przydatności trendów technologicznych – edycja 2023

W badaniu ankietowym 2023 *Tech Trends Maturity and Suitability Index Survey* wzięli udział przedstawiciele 633 firm, którzy odpowiedzieli na pytania dotyczące technologii mających znaczący wpływ na branżę telewizji dozorowej i kontroli dostępu. Tegoroczne wyniki badania obejmują analizę biometrii, przegląd trendów pojawiających się w branży oraz kompleksową analizę ankiety.



BIEŻĄCE I POJAWIAJĄCE SIĘ TRENDY

Dojrzałe i powszechnie obecne: radar i LiDAR (2), przetwarzanie brzegowe/przechowywanie na brzegu sieci (3), bezzałogowe platformy – drony i roboty (4), sztuczna inteligencja (5) i łączność bezprzewodowa 5G (6)

Dojrzałe, ale rzadko stosowane: Li-Fi (1)

Nie bez powodu 5G zajmuje wysokie miejsce w ankiecie. Technologia ta charakteryzuje się dużą szybkością oraz niskim opóźnieniem. Zyskuje popularność w monitoringu wizyjnym, ponieważ coraz więcej kamer obsługuje technologię 5G. Wysokie miejsca zajmują także przetwarzanie/przechowywanie na brzegu sieci, bezzałogowe platformy (roboty i drony) oraz radary/lidary, przy czym te ostatnie współpracują z systemami monitoringu wizyjnego przy wykrywaniu obiektów w niesprzyjających warunkach. Technologia Li-Fi, czyli następca Wi-Fi, powoli staje się dojrzała, m.in. za sprawą opublikowania przez IEEE standardu 802.11bb dla Li-Fi, ale nadal uważa się ją za nieodpowiednią do transmisji sygnałów z systemów zabezpieczeń.

KONTROLA DOSTĘPU

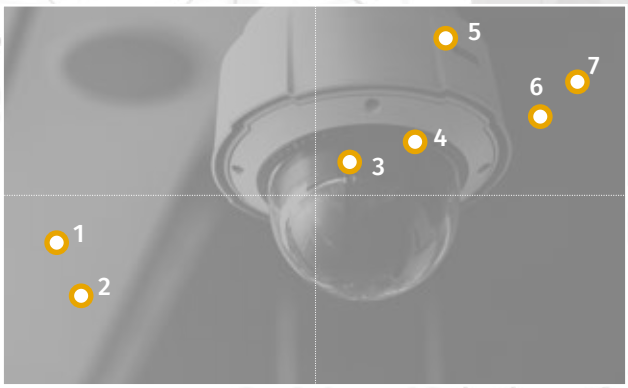
Dojrzałe i powszechnie obecne: bezdotykowa biometria (7) i integracja z systemami zarządzania budynkiem/nieruchomością (8)

Dojrzałe, ale rzadko stosowane: biometria jednomodalna (1), biometria dotykowa (2), zamki bezprzewodowe (3), kontrola dostępu w chmurze (4) i cyfrowe bliźniaki (5)

Niedojrzałe i bardzo rzadko stosowane: biometria multimodalna (6)

Bezdotykowe technologie biometryczne, takie jak rozpoznawanie twarzy czy dłoni, stają się coraz bardziej popularne, a integracja zarządzania budynkami dobrze wpisuje się w obecne trendy w zakresie ekologii i zrównoważonego rozwoju. Biometria jednomodalna i biometria dotykowa, choć zaawansowane technologicznie, mają niższą przydatność, ponieważ organizacje przykładają większą wagę do bezpieczeństwa, ochrony i zdrowia pracowników. Biometria multimodalna natomiast awansuje w rankingu przydatności ze względu na wyposażenie w dodatkową warstwę bezpieczeństwa.

MONITORING WIZYJNY



Dojrzałe i powszechne obecne: aplikacje mobilne do dozoru wizyjnego (7), kamery kolorowe do pracy przy słabym oświetleniu (6), rozdzielczość 4K (5), monitoring wizyjny w chmurze (4) i kamera bispektralna (3)

Niedojrzałe i bardzo rzadko stosowane: rozdzielczość 8K (1) i kamera trójspektralna (2)

Kamery kolorowe pracujące w warunkach słabego oświetlenia oferują coraz lepsze możliwości rejestrowania kolorów nawet przy minimalnym świetle i stale zyskują na popularności dzięki dostępnym bardziej zaawansowanym obiektywom i procesorom. Rozdzielczość 4K umożliwia użytkownikom powiększanie obrazu przy jednoczesnym zachowaniu wyraźnych szczegółów, co czyni ją przydatną do obserwacji dużych obszarów, np. w monitoringach miejskich. Kamery bispektralne, w których kamery światła widzialnego i kamery termowizyjne są połączone w jedno urządzenie, są idealne do zastosowań przemysłowych. Dla porównania kamery o rozdzielczości 8K i kamery trójspektralne (z kombinacją UV) na tym etapie rozwoju systemów telewizji dozorowej nie spełniają na razie wszystkich wymogów. ●

Wyniki ankiety tegorocznego badania w części dotyczącej technologii stosowanej w systemach telewizji dozorowej pokazują, że wysokie miejsca zajęły kamery dające kolorowy obraz nawet w warunkach bardzo słabego oświetlenia, rozdzielczość 4K i rozwiązania bispektralne.

SECURITY 50:

Trendy na rynku telewizji dozorowej. Dominacja sztucznej inteligencji trwa

Na popularności wyraźnie zyskuje sztuczna inteligencja jako narzędzie, które może być odpowiedzią na potrzeby użytkowników dotyczące bezpieczeństwa, a jednocześnie pomocne w działalności operacyjnej.

Sztuczna inteligencja

Sztuczna inteligencja, w szczególności analityka predykcyjna i wykrywanie anomalii, plasuje się bardzo wysoko w indeksie przydatności. To nie dziwi, ponieważ coraz więcej użytkowników wdraża sztuczną inteligencję, aby osiągnąć lepszą wydajność i wyższy poziom bezpieczeństwa.

– *W 2023 roku nastąpił wzrost zainteresowania sztuczną inteligencją w systemach monitoringu wizyjnego. W tej opartej na danych technologii zamiast operatorów oglądających materiał z wielu kamer to oprogramowanie „ogląda" wideo* – powiedział Rahul Yadav, dyrektor ds. technicznych w Milestone Systems. – *Oprogramowanie zbiera dane z urządzeń funkcjonujących na brzegu sieci, obserwuje, identyfikuje obiekty, rozpoznaje wzorce, trendy i korelacje oraz wykorzystuje je do tworzenia raportów i użytecznych informacji. Technologia wideo oparta na danych rewolucjonizuje zatem branżę zabezpieczeń, ale wcale nie oznacza, że ludzie staną się zbędni. Teraz będą potrzebni w centrum zarządzania.*

– *Na rynku monitoringu wizyjnego producenci koncentrują się na analityce opartej na sztucznej inteligencji. Funkcja wykrywania zmian scen i-PRO jest przykładem tego, jak analityka ewoluuje poza funkcje rozpoznawanie ludzi, pojazdów i ich atrybutów* – stwierdził Adam Lowenstein, dyrektor ds. zarządzania produktami w i-PRO Americas. – *Jednocześnie pojawiają się problemy i obawy związane z wykorzystaniem tych danych dotyczące prywatności, ponieważ coraz częściej nagranie jest emitowane w mediach. W rezultacie otrzymujemy mnóstwo zapytań o naszą funkcję SI Privacy Guard, która nakłada mozaikę na twarz lub całą sylwetkę osoby, animizując postać.*

Kamery kolorowe pracujące nawet przy słabym oświetleniu

Kamery dające kolorowy obraz nawet przy słabym oświetleniu zajmują wysokie miejsce pod względem zarówno przydatności, jak i dojrzałości. Dzięki lepszym obiektywom, przetwornikom i chipom przechwytywanie kolorowych obrazów nawet w warunkach ekstremalnie niskiego natężenia światła staje się coraz bardziej wykonalne. Ta cecha jest szczególnie przydatna użytkownikom, którzy przykładają dużą wagę do dozoru nocnego.

– *Ponieważ i-PRO od pewnego czasu wyprzedza konkurencję dzięki przetwornikom przetwarzającym obraz nawet przy słabym oświetleniu, zapewniającym doskonałe odwzorowanie kolorów, nie jest to coś, co określilibyśmy jako nowy trend. Ciężko pracowaliśmy, aby edukować rynek na temat korzyści płynących z kolorowego obrazu uzyskanego mimo słabego światła* – powiedział A. Lowenstein. – *Poza oczywistymi korzyściami wynikającymi z lepszej identyfikacji osoby lub pojazdu również rozpoznawanie obiektów oparte na sztucznej inteligencji działa znacznie lepiej, gdy ma ona do dyspozycji informacje o kolorze.*

UHD

Rozdzielczość 4K plasuje się najwyżej pod względem dojrzałości i w ścisłej czołówce pod względem przydatności. Dzięki wydajniejszym przetwornikom i lepszym kodekom kamery dozorowe 4K lub 8 Mpix mogą rejestrować obrazy UHD *(Ultra High Definition Television)* przy niskim zużyciu przepustowości i pamięci masowej. To sprawia, że 4K jest idealne do scenariuszy,

w których operator musi np. ustalić wzór ubrania osoby lub zidentyfikować numer rejestracyjny pojazdu. Ale czy to oznacza, że im wyższa rozdzielczość, tym lepiej? Niekoniecznie. Weźmy pod uwagę 8K, który plasuje się nisko pod względem zarówno przydatności, jak i dojrzałości. Co więcej, UHD mogą być droższe i mogą działać mniej efektywnie w warunkach słabego oświetlenia.

– Rynek kamer 4K wciąż rośnie w porównaniu z instalacjami full HD, mniej klientów wybiera rozdzielczość 8K. Wielu użytkowników odkryło, że połączenie kamery wieloprzetwornikowej, która obejmuje 360 stopni w rozdzielczości HD lub 4K, w połączeniu z kamerą PTZ z automatycznym śledzeniem i optycznym zoomem, jest bardziej praktyczne, elastyczne i korzystne cenowo. W porównaniu z kamerami 4K rozdzielczość 8K znacząco wpływa również na pamięć i przepustowość. Aby skorzystać z rozdzielczości 33 Mpix, w wypadku większości instalacji potrzebne są także wyjątkowo dobre warunki oświetleniowe – zauważył A. Lowenstein.

– Prawdą jest, że niższe rozdzielczości są bardziej opłacalnym rozwiązaniem. Co więcej, nadal są wystarczające w wielu zastosowaniach. W zakresie słabego oświetlenia niższe rozdzielczości są nawet lepsze, ponieważ przechwytują więcej światła. Dlatego też Mobotix oferuje również 4-megapikselowy przetwornik do słabego oświetlenia dla serii MOBOTIX 7 – powiedział Thomas Lausten, dyrektor generalny w Mobotix. *– Jesteśmy jednak przekonani, że im bardziej wymagająca ma być aplikacja, tym wyższe rozdzielczości będą potrzebne.*

Kamery bispektralne

Wysoko w rankingu znajdują się również kamery bispektralne, w których kamera światła widzialnego i termowizyjna są połączone w jednym urządzeniu. To idealne rozwiązanie do fabryk i zakładów przemysłowych, gdzie kluczowe znaczenie ma wykrywanie dymu, temperatury i ewentualnych punktów pożarowych. Obecnie dostępne są również kamery trójspektralne z dodanym trzecim komponentem – UV. Zajmują one jednak niższą pozycję w ankiecie.

– Na razie nie ma znaczenia czy obraz jest optyczny, IR czy UV. Decyzję o rodzaju kamery podejmuje się na podstawie celu monitoringu i warunków środowiskowych, w których będzie pracować. Nie bez znaczenia są też inteligentne funkcje, które wspierają system, np. oprogramowanie wykorzystujące algorytmy SI, które w połączeniu z kamerą prawidłowo wykrywa sytuacje poprzedzające niepożądane zdarzenia, aby im zapobiec, lecz także zoptymalizować procesy – wyjaśnił T. Lausten.

Inne elementy ankiety

Monitoring wizyjny z możliwością przechowywania danych w chmurze zajmuje wysoką pozycję, umożliwiając użytkownikom rezygnację z inwestowania w rejestratory NVR i serwery. SSD w pamięci masowej również zyskuje na znaczeniu, oferując szybsze i bardziej niezawodne rozwiązania. Rośnie też popularność monitoringu wizyjnego zasilanego energią słoneczną, zapewniając realne rozwiązanie w odległych obszarach, gdzie zasilanie nie jest łatwo dostępne.

» *Monitoring wizyjny z możliwością przechowywania danych w chmurze zajmuje wysoką pozycję, umożliwiając użytkownikom rezygnację z inwestowania w rejestratory NVR i serwery.* «

SECURITY 50:

Kontrola dostępu w 2023 r. Bezdotykowa multimodalna biometria zyskuje na popularności

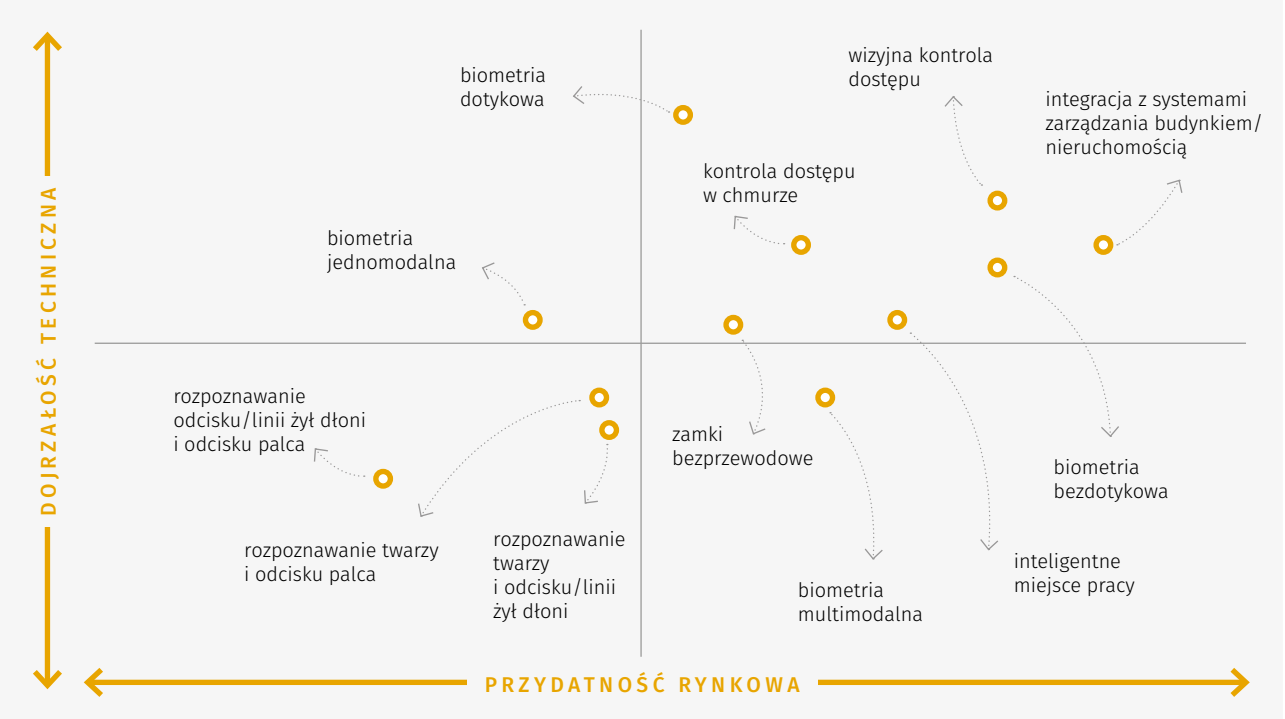
W tegorocznym badaniu najpopularniejszych technologii stosowanych w systemach kontroli dostępu integracja z systemami zarządzania budynkiem i biometria bezdotykowa zajęły wysokie miejsca ze względu na dojrzałość techniczną i przydatność rynkową.

Większym zainteresowaniem cieszy się też biometria multimodalna, dzięki której użytkownicy są uwierzytelniani za pomocą więcej niż jednej technologii biometrycznej.

Integracja z systemami budynkowymi

Zarządzanie budynkiem zintegrowane z kontrolą dostępu zajmuje najwyższe miejsce pod względem przydatności. Pod względem dojrzałości również zajęło wysoką pozycję. Coraz więcej firm decyduje się na integrację tych systemów ze względu na różne korzyści, w tym kompleksowe zarządzanie i oszczędność energii.

– *Nowoczesne budynki to złożona sieć wielu systemów, w tym klimatyzacji, zasilania energią, systemów zabezpieczeń i przeciwpożarowych oraz automatyki domowej lub biurowej. Zarządzanie każdym z tych systemów niezależnie może być trudnym zadaniem, często prowadzącym do nieefektywności i zwiększonego prawdopodobieństwa wystąpienia błędów. Coraz więcej właścicieli i zarządców budynków dostrzega wartość ujednoliconej platformy, która łączy zarządzanie wszystkimi tymi systemami* – powiedział Raymond So, szef marketingu w ZKTeco. – *W dobrze zintegrowanym systemie zarządzania budynkiem różne systemy i urządzenia są ze sobą w wysokim stopniu zintegrowane. Na przykład system kontroli dostępu może być połączony z systemami oświetlenia i HVAC, aby automatycznie dostosowywać parametry pomieszczenia do tego, czy ktoś w nim przebywa, czy też nie. Ten poziom interakcji zwiększa bezpieczeństwo budynku, efektywność energetyczną i poprawia ogólne wrażenia użytkownika, tworząc bardziej intuicyjne i responsywne środowisko.*



» W systemach kontroli dostępu biometria dotykowa jest stosowana od dziesięcioleci. (...) Jednak na popularności zyskuje biometria bezdotykowa ze względu na łatwość użytkowania i właśnie bezdotykowość. «

Biometria dotykowa i bezdotykowa

Badanie pokazuje, że biometria bezdotykowa, taka jak rozpoznawanie twarzy czy tęczówki oka, zajmuje wysokie miejsce pod względem zarówno przydatności, jak i dojrzałości. Tymczasem biometria dotykowa plasuje się najwyżej pod względem dojrzałości. Jest to zrozumiałe, ponieważ biometria dotykowa, głównie odcisk palca, jest stosowana od dawna. W czasie pandemii okazała się bardzo przydatna.

– *W systemach kontroli dostępu biometria dotykowa jest stosowana od dziesięcioleci. Zgadzamy się więc, że zdążyła już okrzepnąć* – powiedział Brian DeGonia, dyrektor ds. rozwiązań biometrycznych, Extended Access Technologies w HID. – *Jednak na popularności zyskuje biometria bezdotykowa ze względu na łatwość użytkowania i właśnie bezdotykowość, co jak pokazuje doświadczenie z okresu pandemii, ma duże znaczenie. Wydajność algorytmów ją obsługujących stale rośnie, więc czujniki bezdotykowe stają się coraz sprawniejsze.*

– *Rosnące znaczenie biometrii bezdotykowej jest przede wszystkim skutkiem wymagań dotyczących higieny, łatwości obsługi i szybkości działania. Mimo to biometria dotykowa nadal utrzymuje swoją pozycję ze względu na dojrzałość i popularność wśród użytkowników* – stwierdził R. So. – *W ZKTeco jesteśmy zaangażowani w rozwój zarówno dotykowych, jak i bezdotykowych technologii biometrycznych, aby zaspokoić potrzeby naszych globalnych klientów. Skupiamy się na dostarczaniu najnowocześniejszych, niezawodnych i przyjaznych dla użytkownika rozwiązań biometrycznych zgodnych z ewoluującymi potrzebami i trendami rynkowymi.*

Biometria multimodalna

Badanie wykazało ponadto, że biometria jednomodalna zajmuje wyższą pozycję pod względem dojrzałości, podczas gdy biometria multimodalna nie jest tak dojrzała, ale zyskuje na przydatności.

– *Biometria multimodalna może zmniejszyć poziom błędów i zwiększyć poziom zaufania do systemu poprzez łączenie mocnych stron różnych sposobów rozpoznawania i kompensowanie słabości każdego z nich. Dzięki niej uzyskuje się wyższy poziom bezpieczeństwa, ponieważ biometria multimodalna może zapobiegać atakom spoofingowym i zwiększać prywatność użytkowników, wymagając rozpoznania więcej niż jednej cechy biometrycznej w celu przyznania dostępu. Zwiększa też wygodę użytkownika, ponieważ może zaoferować większą elastyczność w wyborze najbardziej odpowiedniej i najwygodniejszej metody uwierzytelniania* – powiedział Hanchul Kim, CEO Suprema.

Jednak biometria multimodalna ma również pewne ograniczenia, które sprawiają, że jest mniej dojrzała niż biometria jednomodalna. Należą do nich wyższe koszty zakupu i złożoność instalacji, mniej stabilna infrastruktura.

– *Biometria multimodalna ma ogromny potencjał, aby przezwyciężyć swoje ograniczenia i stać się bardziej dojrzałą i szeroko stosowaną w przyszłości, ponieważ technologia ewoluuje, a zapotrzebowanie rynku zmienia się z czasem* – stwierdził H. Kim.

– *Coraz częściej do identyfikacji wykorzystuje się biometrię wielomodalną. W przypadku uwierzytelniania jednomodalność dobrze działa i jest bardzo dojrzała. Jednak w przypadku identyfikacji na dużą skalę lub w aplikacjach, które wymagają wyższego poziomu bezpieczeństwa, biometria multimodalna sprawdza się lepiej. Używając więcej niż jednego czynnika biometrycznego, zyskuje się większą pewność, że została zidentyfikowana właściwa osoba* – ocenił B. DeGonia.

Podwójna biometria

Obecnie multimodalne dane biometryczne są w większości dwuskładnikowe – wykorzystują dwa sposoby uwierzytelniania. Z badania wynika, że wyższą rangę pod względem zarówno przydatności, jak i dojrzałości mają metody jednoczesnego rozpoznawania palca i dłoni oraz twarzy i dłoni.

– *Jedną z najbardziej powszechnych i popularnych dwumodalnych technologii biometrycznych jest rozpoznawanie odcisku palca i dłoni. Twarz–dłoń jest stosunkowo nową metodą, która w ostatnich latach zyskała większe zainteresowanie. Łączy ona rozpoznawanie twarzy z rozpoznawaniem odcisku dłoni lub skanu układu naczyń krwionośnych dłoni, które są zarówno bezdotykowe, jak i niezawodne. Została zastosowana w niektórych sektorach, takich jak opieka zdrowotna, bankowość, edukacja. Ta forma uwierzytelniania oferuje wysoką wydajność, prywatność, higienę i elastyczność* – stwierdził H. Kim. – *Metoda palec–dłoń i metoda twarz–dłoń nadają się do zastosowań wymagających wysokiego poziomu bezpieczeństwa i wygody. Mogą zapewnić szybką i dokładną weryfikację lub identyfikację przy minimalnej interakcji i wysiłku użytkownika. Mogą również zapobiegać atakom spoofingowym i chronić prywatność użytkowników, ponieważ wymagają więcej niż jednej cechy biometrycznej do przyznania dostępu.*

Według H. Kima metoda rozpoznawania osób za pomocą odcisku palca i skanu dłoni jest mniej powszechną i mniej dojrzałą dwumodalną technologią biometryczną. – *Łączy dwie metody oparte na kontakcie, które wymagają różnych czujników i metod przechwytywania. Była wykorzystywana w niektórych niszowych zastosowaniach, takich jak badania kryminalistyczne czy identyfikacja przestępców* – powiedział. – *Metoda palec–dłoń jest mniej odpowiednia do zastosowań wymagających wysokiego poziomu bezpieczeństwa i wygody. Może zapewnić wysoką unikalność i różnorodność cech biometrycznych, ale wymaga również większej interakcji użytkownika i wysiłku w celu zarejestrowania obu rodzajów danych. Mogą na nią wpływać czynniki środowiskowe, takie jak brud, wilgoć i temperatura, które mogą pogorszyć jakość obrazów biometrycznych.* ●

ANALIZA RYNKU EUROPEJSKIEGO W 2023 R.

Zagrożenia, technologie i przepisy

Rynek zabezpieczeń technicznych w Europie w ostatnich latach doświadczył znaczących zmian i przekształceń. Nasiliły się obawy związane z bezpieczeństwem spowodowane różnymi czynnikami, od ataków terrorystycznych, przez pandemię, po konflikty zbrojne. Znaczenie solidnych i innowacyjnych rozwiązań w zakresie zabezpieczeń technicznych nigdy nie było większe.

Warunki rynkowe i wzrost

Europejski rynek zabezpieczeń technicznych wchodzi obecnie w okres dobrej koniunktury, a obiecujące wskaźniki wskazują na jego świetlaną przyszłość. W ostatnim roku rynek doświadczył atrakcyjnego wzrostu, który ma szansę się utrzymać, a nawet przyspieszyć w nadchodzących latach.

– *Z mojego punktu widzenia rynek jest obecnie w korzystnej sytuacji* – powiedziała Verena Rathjen, wiceprezes na region EMEA w Axis Communications. – *Niezależne badania rynku, takie jak przeprowadzone przez Omdia, wskazują, że możemy liczyć na średni wzrost rynku od 10 do 12% w ciągu najbliższych pięciu lat, co jest zgodne z naszymi przewidywaniami. Jest to więc obiecująca perspektywa dla naszej firmy.*

Wzrost wynika z kilku czynników odgrywających kluczową rolę w kształtowaniu trajektorii branży.

1. Zwiększone wydatki rządowe: W odpowiedzi na niepokoje geopolityczne, które ogarnęły różne części globu, nastąpił znaczny wzrost wydatków państwowych na środki bezpieczeństwa. Ten napływ funduszy działa jak katalizator ekspansji rynkowej.

2. Bezpieczeństwo i ochrona jako główne priorytety: Nacisk na bezpieczeństwo i ochronę nigdy nie był bardziej wyraźny, a kraje Europy umieściły je na szczycie swoich programów. Jest to szczególnie widoczne w Wielkiej Brytanii; podejście to stopniowo przenika do innych krajów, takich jak Francja.

3. Wykluczenie dostawców chińskich: Zauważalną zmianą było wykluczenie dostawców chińskich z rynku, przy czym niektóre firmy posunęły

się nawet do demontażu istniejących instalacji od tych producentów. Również to jest czynnikiem wzmacniającym firmy europejskie.
4. Transformacja cyfrowa i digitalizacja procesów: Rewolucja cyfrowa otworzyła wiele możliwości w dziedzinie bezpieczeństwa i optymalizacji biznesu. Integracja sztucznej inteligencji (AI) i procesów cyfrowych to nie tylko trend, ale także istotny czynnik, który zmienia branżę.

Wyzwania i strategie

Prężnie rozwijający się europejski rynek zabezpieczeń zmaga się z tymi samymi wyzwaniami co inne branże – wahania koniunktury gospodarczej, problemy z łańcuchem dostaw, zawirowania na scenie politycznej. Niestabilność geopolityczna i gospodarcza, np. wojna w Ukrainie czy konflikt w Izraelu, sporadyczne konflikty regionalne i recesja w Niemczech, ale też kolejne regulacje unijne mogą znacząco wpłynąć na wzrost i stabilność rynku. Firmy muszą zachować czujność i zdolność adaptacji, aby przynajmniej utrzymać swoje status quo.

– *Regulacje koncentrują się na sztucznej inteligencji, cyberbezpieczeństwie i zrównoważonym rozwoju, a nowe przepisy są już wprowadzane w życie* – stwierdziła V. Rathjen. – *Przyjmujemy proaktywne podejście w tych obszarach, aby móc szybko zareagować na zmiany. Jeśli chodzi o sztuczną inteligencję, dużo inwestujemy w etyczne jej użytkowanie i cyberbezpieczeństwo. Oprócz niedoboru zasobów kluczowym wyzwaniem, przed którym stoimy, jest nie tyle rekrutacja na nasze wolne stanowiska, ile zdolność produkcyjna. Moglibyśmy osiągnąć więcej, gdybyśmy dysponowali większą liczbą specjalistów. Ten problem dotyczy także naszych partnerów. Dlatego Axis nieustannie pracuje nad tym, aby jej produkty i rozwiązania były łatwiejsze w instalacji. Oferujemy także kompleksowe narzędzia ułatwiające naszym partnerom szybsze konfigurowanie i wdrażanie systemów.*

Branża rzeczywiście boryka się z niedoborem instalatorów. Aby rozwiązać ten problem, firmy modyfikują swoje produkty, chcąc ułatwić ich instalację, oraz opracowują narzędzia przyspieszające ich konfigurację. Jednocześnie sektor zabezpieczeń fizycznych jest liderem we wdrażaniu najnowocześniejszych technologii, takich jak sztuczna inteligencja, Internet rzeczy i uczenie maszynowe.

Nowe technologie

Nowe technologie zmieniają rynek security w Europie, wprowadzając branżę w nową erę innowacji i wydajności. Sztuczna inteligencja (AI), Internet rzeczy (IoT) i uczenie maszynowe to najważniejsze nowości wpływające na branżę. Nie są dodatkami do oferowanych rozwiązań, ale integralnymi komponentami nowoczesnych systemów zabezpieczeń, zwiększając ich możliwości i oferując organizacjom możliwość uporania się ze złożonymi wyzwaniami dotyczącymi bezpieczeństwa.

– *Większość kamer Axis najnowszej generacji jest wyposażona w funkcje analityczne bazujące na głębokim uczeniu, co sprawia, że zaczyna być to wręcz standard w kamerach IP* – powiedziała V. Rathjen. – *Rozwój sztucznej inteligencji poszerza horyzonty naszych klientów i otwiera nowe możliwości oparte na analityce. Pozwala na uzyskanie praktycznych informacji i potencjalnie automatycznych odpowiedzi na podstawie danych zebranych przez nasze kamery.*

Algorytmy sztucznej inteligencji i uczenie maszynowe zapewniają analizę ogromnych ilości danych z różnych źródeł, dostarczając praktycznych informacji, które można wykorzystać do ulepszenia zabezpieczeń, a nawet przewidywania potencjalnych zagrożeń, zanim się pojawią. Urządzenia IoT mogą być wykorzystywane do tworzenia systemów zabezpieczeń, które umożliwiają monitorowanie w czasie rzeczywistym i automatyczne reagowanie na naruszenia chronionych stref. Połączenie najnowszych technologii powoduje jednak, że firmy chcące je wykorzystywać muszą mieć pewność, że będzie się to dziać w sposób etyczny i odpowiedzialny. Muszą być także gotowe na prowadzenie badań, aby nadążyć za szybkim tempem postępu technologicznego i wyprzedzić potencjalne cyfrowe zagrożenia.

Możliwości rozwoju

Jednym z najważniejszych obszarów ekspansji jest optymalizacja bezpieczeństwa. Ponieważ cyfryzacja nadal przekształca branżę, duże platformy IT dążą do integracji kamer dozorowych ze swoją infrastrukturą. To otwiera nowe możliwości firmom mogącym dostarczać kompatybilnych rozwiązań.

– *Nie sądzę, aby istniał jeden segment, który by się wyróżniał* – wyjaśniła V. Rathjen. – *Spodziewany jest wzrost we wszystkich sektorach. Z punktu widzenia zastosowania nastąpi znaczny wzrost w obszarze optymalizacji biznesowej stymulowany transformacją cyfrową w wielu branżach. Co więcej, duzi gracze z branży IT i rozwiązań chmurowych badają możliwość integracji kamer dozoru wizyjnego ze swoimi platformami. Nasze podejście do otwartej platformy i interfejsy API powodują, że możemy integrować się z tymi platformami. W ten sposób oferujemy naszym klientom wartość dodaną.*

Otwarcie platformy i dostępność interfejsów API mają kluczowe znaczenie, ponieważ ułatwiają bezproblemową integrację z systemami IT innych firm.

Wymogi prawne

Dostosowanie się do różnorodnych systemów prawnych krajów europejskich i przepisów unijnych bywa wyzwaniem dla firm działających na rynku zabezpieczeń technicznych. Absolutna zgodność z przepisami to oczywista konieczność, która jednocześnie powoduje, że odbiorcy mają większe zaufanie do dostawców.

– *Firmy muszą stale monitorować otoczenie prawne. Wiele firm, w tym nasza, ma specjalne komitety lub grupy robocze, które śledzą to, co dzieje się w kwestii przepisów, oraz w cyberbezpieczeństwie, sztucznej inteligencji i zrównoważonym rozwoju* – podkreśliła V. Rathjen. – *Zmiany w przepisach mogą mieć znaczący wpływ, dlatego niezbędna jest proaktywna postawa w tym względzie.*

Niezależnie od zachowania zgodności z przepisami firmy muszą pamiętać o przejrzystości własnych działań, zachowaniu wysokich standardów etycznych i o ochronie prywatności. W miarę, jak postęp technologiczny przyspiesza, rośnie presja konsumentów oraz podmiotów regulacyjnych na społeczną odpowiedzialność biznesu. Firmy z branży security powinny mieć to na względzie, gdyż może się to przełożyć na utrzymanie korzystnej pozycji rynkowej.

Rynek zabezpieczeń technicznych w Europie znajduje się w kluczowym momencie, z wieloma możliwościami rozwoju i innowacji. Firmy muszą jednak radzić sobie ze złożonością sytuacji gospodarczej i rygorystycznymi regulacjami prawnymi. Przyjmując zmiany, traktując priorytetowo zgodność z przepisami i przestrzegając standardów etycznych, dostawcy europejscy mogą liczyć na czas prosperity. ●

ANALIZA RYNKU AMERYKI PÓŁNOCNEJ W 2023 R.

Zagrożenia, technologie i przepisy

Rynek security w Ameryce Północnej w 2023 r. szybko się zmienia, odzwierciedlając złożone i stale zmieniające się zagrożenia, z którymi borykają się organizacje. Systemy zabezpieczeń technicznych, w tym kamery dozorowe, systemy kontroli dostępu, personel ochrony i zabezpieczenia mechaniczne, nabierają szczególnej wagi, by skutecznie chronić zasoby, ludzi i informacje.

Rynek jest elastyczny i innowacyjny, a branżę kształtują postęp technologiczny i integracja systemów zabezpieczeń. Security powoli odchodzi od tradycyjnych metod na rzecz bardziej zaawansowanych i inteligentnych rozwiązań. To oznacza zmianę sposobu, w jaki organizacje zarządzają swoimi potrzebami w zakresie bezpieczeństwa. Przyglądamy się północnoamerykańskiemu rynkowi elektronicznych systemów zabezpieczeń w 2023 r., w tym jego kluczowym trendom i wyzwaniom. O wpływie tego sektora na bezpieczeństwo w Ameryce Północnej wypowiadają się eksperci branżowi.

Postęp technologiczny zmienia branżę

Postęp technologiczny powoduje szybką transformację rynku zabezpieczeń technicznych. Sztuczna inteligencja, uczenie maszynowe i Internet rzeczy (IoT) zwiększają skuteczność i wydajność systemów zabezpieczeń technicznych. Technologie nie tylko poprawiają możliwości systemów, ale także rewolucjonizują sposób, w jaki organizacje zarządzają swoimi potrzebami w zakresie bezpieczeństwa.

– *W roku 2023 rynek był dynamiczny i szybko ewoluujący, w dużej mierze zasilany przez innowacje technologiczne i integracje* – powiedział Steve Prodger, Chief Risk Officer w Arcules. – *Do najważniejszych trendów zaliczamy rosnącą popularność systemów monitoringu wizyjnego oferowanego jako usługa w chmurze i rosnące zaufanie do tej formy usługi. Systemy te oferują wyjątkową skalowalność i zalety zdalnego dostępu, które wpisują się w potrzeby klientów. Ponadto priorytet ma teraz cyberbezpieczeństwo. Wszystkie te czynniki nadal będą kształtować branżę w regionie przez następne pięć lat.*

Integracja urządzeń i systemów

Integracja urządzeń i systemów to kolejny istotny trend kształtujący rynek zabezpieczeń technicznych. Organizacje w coraz większym stopniu wykorzystują moc danych i analiz, aby uzyskać wgląd w potencjalne zagrożenia i luki w zabezpieczeniach. Kompleksowa integracja dostarcza specjalistom ds. bezpieczeństwa cennych informacji, które można wykorzystać do podejmowania świadomych decyzji i poprawy ogólnego stanu bezpieczeństwa organizacji.

Systemy monitoringu wizyjnego w chmurze

Wyraźnie zauważalna jest też rosnąca popularność systemów monitoringu wizyjnego w chmurze. Oferują one niezrównaną skalowalność i zaletę zdalnego dostępu, co czyni je atrakcyjną opcją dla organizacji każdej wielkości.

– *Rynek szybko ewoluuje z zauważalnym wzrostem wdrażania rozwiązań kontroli dostępu opartych na chmurze* – stwierdził John

Skowronski, prezes ACRE Security na Amerykę. – *Rosnące zapotrzebowanie na elastyczne, skalowalne i zdalnie zarządzane systemy zabezpieczeń jest impulsem do wdrażania technologii opartych na chmurze. Organizacje dążą do usprawnienia kontroli dostępu, zwiększenia zakresu integracji z innymi systemami zabezpieczeń i poszerzenia możliwości analizy danych.*

W ciągu najbliższych pięciu lat trend wdrażania sztucznej inteligencji i uczenia maszynowego będzie się umacniał, zwiększając skuteczność systemów zabezpieczeń. Doprowadzi to do łatwiejszego zarządzania, wygodniejszych poświadczeń i bezproblemowej integracji z urządzeniami IoT, co przełoży się na kompleksowe i wydajne podejście do bezpieczeństwa. Jednocześnie nacisk na prywatność danych i cyberbezpieczeństwo pozostanie najwyższym priorytetem przy ciągłych wysiłkach na rzecz wzmocnienia środków bezpieczeństwa w infrastrukturze chmury w celu ochrony informacji poufnych.

Znaczenie cyberbezpieczeństwa

Wraz z rozwojem technologii cyberbezpieczeństwo stało się kluczowe dla każdej organizacji. Firmy dostrzegają potrzebę ochrony przed zagrożeniami cyfrowymi, a połączenie bezpieczeństwa cybernetycznego i fizycznego stało się koniecznością. Bezpieczne sprawdzone wdrożenia systemów funkcjonujących w chmurze są coraz bardziej powszechne, a cyberbezpieczeństwo jest obecnie najważniejszym czynnikiem branym pod uwagę przy sprzedaży tych rozwiązań.

– Zapewnienie jednoczesnego bezpieczeństwa cyfrowego i fizycznego będzie priorytetem, zwłaszcza w przypadku operacji prowadzonych w centrach zarządzania. Najważniejsza jest ochrona przed cyberzagrożeniami – powiedział Ray May, Chief Technology Officer w Parker Group. – *Możliwości zdalnego monitorowania pomogą użytkownikom zidentyfikować problemy, zanim wpłyną one na działanie organizacji. Partnerstwa technologiczne i ekosystemy zwiększą możliwości centrów zarządzania, powodując, że pozostaną w czołówce innowacji w zakresie bezpieczeństwa w regionie.*

Nowoczesne centra zarządzania i zaawansowana wizualizacja danych

Nowoczesne centra zarządzania wyposażone w zaawansowane narzędzia do wizualizacji danych przodują w transformacji rynku zabezpieczeń technicznych. Centra zarządzania dają pracownikom ochrony kompleksowy obraz otoczenia, zwiększając świadomość sytuacyjną i umożliwiając szybkie podejmowanie decyzji. Integracja bezpieczeństwa cyfrowego i fizycznego zapewni ochronę przed zagrożeniami płynącymi zarówno ze świata fizycznego, jak i z cyberprzestrzeni.

– Postęp techniczny zmienia branżę elektronicznych systemów zabezpieczeń – stwierdził R. May. – *Centra zarządzania znajdują się na pierwszym miejscu transformacji, ponieważ organizacje dostrzegają potrzebę ich modernizacji w celu lepszego monitorowania, zarządzania i reagowania na zagrożenie bezpieczeństwa. Współczesne centra zarządzania to w istocie pomieszczenia wyposażone w zaawansowane systemy wizualizacji danych, które zapewniają pracownikom ochrony większą świadomość sytuacyjną, umożliwiającą podejmowanie odpowiednich decyzji.*

Inteligentne rozwiązania do zarządzania bezpieczeństwem

Pojawienie się inteligentnych rozwiązań do zarządzania bezpieczeństwem to kolejny kluczowy trend kształtujący branżę. Rozwiązania te wykorzystują analitykę opartą na algorytmach sztucznej inteligencji i skalowalne oprogramowanie, aby pomóc organizacjom w proaktywnym i szybkim zrozumieniu zdarzeń oraz reagowaniu na nie. Integracja technologii, takich jak rozpoznawanie wzorców, korelacja danych, modelowanie predykcyjne, automatyzacja i zaawansowana wizualizacja, dostarcza cennych informacji specjalistom ds. bezpieczeństwa.

– Rynek ewoluuje w kierunku tego, co nasz zespół nazywa erą inteligencji – ocenił Alan Stoddard, dyrektor generalny Intellicene. *– Era ta charakteryzuje się kompleksową integracją urządzeń i systemów, co generuje ogromne ilości danych. Owa integracja oznacza, że systemy potrafią rozpoznawać wzorce, dokonywać modelowania predykcyjnego i wizualizować zgromadzone dane, aby ułatwić menedżerom ds. bezpieczeństwa zrozumienie zgromadzonych informacji.*

To z kolei skłania dostawców do oferowania zintegrowanych inteligentnych platform, które umożliwiają organizacjom proaktywne reagowanie na zdarzenia. Wykorzystując analitykę AI i skalowalne oprogramowanie, rozwiązania te zwiększają bezpieczeństwo, pomagając organizacjom w przeciwdziałaniu zagrożeniom. Oczekuje się, że branża będzie w dalszym ciągu wykorzystywać inteligencję do zwiększania świadomości sytuacyjnej i bezpieczeństwa w przyszłości.

Prognozy na przyszłość

Rynek security w Ameryce Północnej jest gotowy do znacznego wzrostu i transformacji w nadchodzących latach.

– Obecnie rynek zabezpieczeń technicznych przechodzi znaczącą transformację w kierunku stosowania nowoczesnych technologii – powiedział Bob Wall, dyrektor ds. technologii w Edge360. *– To przejście pociąga odejście od konwencjonalnych, odizolowanych konfiguracji systemów zabezpieczeń na rzecz bardziej kompleksowych inteligentnych rozwiązań, które uwzględniają również protokoły cyberbezpieczeństwa, biorąc pod uwagę wrażliwe dane, które gromadzą te systemy.*

Coraz większy nacisk kładzie się na rozwiązania, które są skalowalne i mogą elastycznie reagować na zmieniające się wymagania przedsiębiorstw, eliminując konieczność gruntownych zmian w istniejącej infrastrukturze.

– Firmy skłaniają się ku inwestycjom w zaawansowane systemy analityczne i systemy wykorzystujące sztuczną inteligencję – stwierdził B. Wall. – *Zauważalny jest również wzrost popytu na platformy opracowane przez firmy IT, ponieważ są one wyposażone w silne funkcje szyfrowania i zabezpieczania danych. To podkreśla rosnące przenikanie się krajobrazów bezpieczeństwa fizycznego i cyfrowego. Jednocześnie przewiduje się spadek zależności od przestarzałych, skomplikowanych systemów, których utrzymanie jest nie tylko kosztowne, ale także mniej skuteczne w rozwiązywaniu bieżących problemów związanych z bezpieczeństwem.*

Rosnąca popularność systemów monitoringu wizyjnego w chmurze, znaczenie cyberbezpieczeństwa, nowoczesne centra zarządzania wyposażone w zaawansowane narzędzia do wizualizacji danych oraz inteligentne rozwiązania do zarządzania bezpieczeństwem to kluczowe trendy kształtujące przyszłość branży. Patrząc w przyszłość, rynek jest gotowy na znaczny wzrost i innowacje, ze zwiększonym naciskiem na skalowalne i elastyczne rozwiązania, integrację fizycznych i cyfrowych przestrzeni bezpieczeństwa oraz przyjęcie modeli *Software as a Service* (SaaS). ●

ANALIZA RYNKU AZJATYCKIEGO W 2023 R.

Dogłębne spojrzenie na rozwój rynku security

W latach 2022–23 azjatycki rynek zabezpieczeń technicznych doświadczył znacznego wzrostu i transformacji, które były skutkiem pojawienia się nowych rozwiązań, inicjatyw rządowych i zmieniających się wymagań. Zróżnicowany krajobraz tej części świata, w którym są kraje zarówno rozwinięte, jak i rozwijające się, powoduje, że branża security musiała się do tej różnorodności dostosować.

Niezależnie od tego, to właśnie firmy obecne na rynku azjatyckim są liderami we wdrażaniu najnowocześniejszych technologii: od systemów dozoru wizyjnego o wysokiej rozdzielczości po analitykę opartą na sztucznej inteligencji i rozpoznawanie twarzy.

Integracja sztucznej inteligencji i przetwarzania brzegowego

Niektóre z dużych firm przodują w implementacji algorytmów sztucznej inteligencji i przetwarzania brzegowego w swoich rozwiązaniach zabezpieczeń, tworząc tym samym inteligentniejsze i wydajniejsze systemy.

– *Na rynku security odnotowaliśmy dwucyfrowy wzrost sprzedaży, zwłaszcza w segmencie nowych technologii, tj. biometrycznego i opartego na sztucznej inteligencji uwierzytelniania i analityki rozpoznawania twarzy* – poinformował Hanchul Kim, dyrektor generalny Suprema. Z kolei Vivianna Wang, dyrektor generalny ds. marketingu i rozwoju kanałów w Hikvision, powiedziała, że w ciągu najbliższych pięciu lat można się spodziewać dominacji kilku trendów.

– *Zmiany zapoczątkują cyfryzacja i integracja innowacyjnych technologii, takich jak sztuczna inteligencja i IoT* – stwierdziłała V. Wang. – *Ponadto przewidujemy, że na znaczeniu zyskają rozwiązania w zakresie bezpieczeństwa, które będą zrównoważone i przyjazne dla środowiska, tym samym dostosowane do globalnych inicjatyw ekologicznych i niskoemisyjnych.*

Monitoring wizyjny wysokiej rozdzielczości

Rośnie zapotrzebowanie na systemy monitoringu wizyjnego wysokiej rozdzielczości. Zwiększenie rozdzielczości kamer IP do 5 Mpix staje się normą. Urządzenia te zapewniają wyraźniejsze i bardziej szczegółowe obrazy.

– *Obecnie na prowadzenie wysuwają się kamery o rozdzielczości 5 Mpix. Wcześniejszym standardem było zaledwie 2 Mpix* – wyjaśnił Alex Kuo, regionalny szef biznesu APAC w Vivotek. – *Specyfikacje techniczne różnych marek również stały się podobne, dlatego znaczenie zyskuje wartość dodana produktu. To ważny czynnik wpływający na stały rozwój Vivotek w regionie Azji i Pacyfiku. Na przykład dzięki naszej funkcji Smart Stream 3 nie tylko jakość i rozdzielczość obrazu są na wyższym poziomie, ale też większa jest przepustowość pasma. Ponadto analiza AI i możliwości VCA pozwalają na szybsze rozwiązywanie problemów klientów, zwiększając w ten sposób wydajność operacyjną systemu.*

Analityka oparta na sztucznej inteligencji

Analityka z wykorzystaniem sztucznej inteligencji i technologie rozpoznawania twarzy stają się coraz bardziej wyrafinowane i dokładne, rewolucjonizując sposób korzystania z systemów dozoru wizyjnego. Technologie te, działając w czasie rzeczywistym, ułatwiają operatorom podejmowanie decyzji dotyczących alertów i zwiększając ogólne możliwości systemów zabezpieczeń.

– *W krajach zaawansowanych technologicznie i tych, które inwestują w projekty na dużą skalę, już teraz obserwujemy szybkie wdrażanie funkcji analitycznych z wbudowanymi algorytmami sztucznej inteligencji* – zauważył Alex Lee, kierownik sprzedaży na region MEA i Azję w IDIS. – *Rewolucjonizuje to sposób korzystania z monitoringu wizyjnego, umożliwiając dokładniejsze i wydajniejsze monitorowanie środowiska, w takich obiektach jak węzły transportowe, szpitale, obiekty rządowe, centra handlowe i przestrzenie publiczne.*

W efekcie coraz wydajniejsze staje się rozpoznawanie twarzy czy wykrywanie obiektów, a coraz więcej firm jest w stanie uzasadnić ich wdrożenie. Wprowadzenie SI powoduje, że materiał wideo może być analizowany w czasie rzeczywistym, zapewniając operatorom większą świadomość sytuacyjną. Funkcje wyszukiwania metadanych przyspieszają również uzyskanie materiału na potrzeby dochodzeniowe w kilka godzin, a nawet minut.

– *To samo dotyczy analizy biznesowej, szczególnie w handlu detalicznym, gdzie obserwujemy duże zapotrzebowanie na analizy z zastosowaniem SI. Dotyczy ona np. liczenia osób odwiedzających dane miejsce, opracowania heat map (tzw. mapy ciepła to technika umożliwiająca graficzną prezentację najważniejszych informacji dotyczących zachowań użytkowników), monitorowania zajętości konkretnych przestrzeni i zarządzania kolejkami. Analiza tych informacji przekłada się na zwiększenie zysków, stąd duże zapotrzebowanie na kamery o wysokiej rozdzielczości i wysokiej wydajności, ponieważ wspomagają one strategie biznesowe służące maksymalizacji zysków i minimalizacji strat* – dodał A. Lee.

Rozwiązaniami chmurowe i poświadczenia mobilne

Rozwiązania chmurowe zyskują na popularności, zapewniając większą elastyczność i skalowalność systemów zabezpieczeń. Coraz powszechniejsze stają się również mobilne systemy uwierzytelniające, oferujące wygodne i bezdotykowe rozwiązanie kontroli dostępu.

Inicjatywy i inwestycje rządowe

W wielu krajach Azji są prowadzone duże inwestycje w infrastrukturę bezpieczeństwa, co powoduje znaczny wzrost wartości tamtejszego rynku security. Duże projekty infrastrukturalne, takie jak modernizacja sieci kolejowej w Indiach, są tego przykładami.

– *Rynek zabezpieczeń technicznych przeżywa rozkwit w Azji. W krajach rozwijających się w Azji Południowo-Wschodniej jest coraz więcej inwestycji typu greenfield (bezpośrednia inwestycja zagraniczna polegająca na tworzeniu nowego przedsiębiorstwa od podstaw) oraz inwestycji infrastrukturalnych* – powiedział David Thean, dyrektor generalny na Azję w Gallagher Security. – *Wraz z rozwojem tych krajów rośnie zapotrzebowanie na najwyższej klasy rozwiązania w zakresie bezpieczeństwa.*
Vivianna Wang również zwróciła uwagę na ogromne zróżnicowanie krajów tego rejonu. – *Obserwujemy znaczny wzrost na rynkach Azji Południowo-Wschodniej, wykazujących ogromny potencjał. Natomiast w krajach gospodarczo okrzepłych ten wzrost jest umiarkowany* – stwierdziła.

Inwestycje rządowe znacząco wpływają na wyniki branży security w krajach rozwijających się, w tym w Bangladeszu, Indiach, Tajlandii i Wietnamie. Gospodarka Indii rozwija się dzięki dużym projektom infrastrukturalnym. Jednym z przykładów jest modernizacja systemów zabezpieczeń i ochrony w największej w Azji sieci kolejowej.

– *Do tej pory dzięki produktom firmy IDIS India zmodernizowano blisko 3700 stacji kolejowych obsługiwanych przez RailTel Corporation of India Ltd.* – wyjaśnił A. Lee. – *Obiekty są bezproblemowo monitorowane, a system jest zarządzany za pomocą naszego rozwiązania IDIS Solution Suite VMS. RailTel wdrożył nasze moduły usługowe, w tym IDIS Critical Failover i IDIS Deep Learning Analytics, a także integrację z rozpoznawaniem twarzy innych firm.*

Przed Igrzyskami Olimpijskimi w Tokio IDIS odnotował znaczny wzrost popytu na modernizację systemów monitoringu wizyjnego. Firma podpisała w 2019 r. umowę partnerską z JVC w celu sprzedaży produktów marki IDIS w całej sieci dystrybucji. Ta strategia była dużym sukcesem, zwłaszcza że Japonia jest znana z przywiązania do krajowych rozwiązań, co nie dziwi po dziesięcioleciach popularności swoich marek elektronicznych.

– *Jesteśmy realistami, jeśli chodzi o region, dlatego spodziewamy się, że CAGR w ciągu najbliższych pięciu lat wyniesie nie więcej niż 10–15%* – powiedział A. Lee. – *Azja rozwija się dynamicznie, ale na gospodarkę każdego z krajów azjatyckich wpływają różne czynniki. Choć prawdą jest, że podobnie jak w wielu innych częściach świata w całym regionie obserwujemy stałe zapotrzebowanie na kompleksowe rozwiązania w sektorach handlu detalicznego, bankowości, opieki zdrowotnej, hotelarstwa, logistyki i produkcji.*

Wspólne dla wszystkich tych krajów jest jednak rosnące zapotrzebowanie na zwiększenie wydajności operacyjnej dzięki lepszym środkom bezpieczeństwa. Rosnąca przestępczość i akty terroryzmu powodują obawy o bezpieczeństwo publiczne, dlatego zarówno władze, jak i przedsiębiorstwa inwestują w systemy dozoru wizyjnego o wysokiej rozdzielczości, a także w analitykę danych. W efekcie następuje zwiększenie zapotrzebowania na systemy monitorujące w czasie rzeczywistym oraz na proaktywne środki bezpieczeństwa i ochrony.

Obawy i działania związane z cyberbezpieczeństwem

Wraz ze wzrostem znaczenia cyberbezpieczeństwa w produktach systemów zabezpieczeń firmy wdrażają różne techniki w celu ochrony prywatności i danych. Tendencja ta jest szczególnie widoczna w takich krajach jak Korea Południowa, w których społeczność ceni prywatność.

– *Znacząca staje się potrzeba zapewnienia wysokiego poziomu bezpieczeństwa i ochrony rozwijającej się infrastruktury i nowoczesnych budynków w regionie* – dodał D. Thean. – *Wymagania dotyczące cyberbezpieczeństwa rosną również w przypadku produktów systemów zabezpieczeń technicznych. Zauważamy też wzrost popularności coraz sprytniejszych systemuów kontroli dostępu, oferujących np. rozpoznawanie twarzy i skanowanie tęczówki oka oraz mobilnych rozwiązań uwierzytelniających. Rozwiązania chmurowe również zyskują na popularności.*

Bez wątpienia azjatycki rynek zabezpieczeń przeszedł znaczącą transformację, dostosowując się do zmieniających się wymagań regionu obejmującego wysoko rozwinięte kraje i te, które dopiero do takich aspirują. Integracja najnowocześniejszych technologii, takich jak sztuczna inteligencja, przetwarzanie brzegowe i dozór wizyjny w wysokiej rozdzielczości, zrewolucjonizowała branżę, zapewniając bardziej wyrafinowane i wydajne rozwiązania bezpieczeństwa. Rosnące znaczenie cyberbezpieczeństwa w produktach systemów zabezpieczeń technicznych, wraz z przyjęciem rozwiązań zbliżeniowych i biometrycznych, odzwierciedla zaangażowanie branży w podejmowanie współczesnych wyzwań związanych z bezpieczeństwem i ochroną.
Nie można jednak nie dostrzec faktu, że w tym regionie świata za sukcesem branży security w dużej mierze stoją inwestycje rządowe. ●

BADANIA RYNKU I KOMENTARZE

Memoori: Dominujące trendy na rynku zabezpieczeń technicznych w 2023 r.

Rynek zabezpieczeń technicznych przechodzi transformację, na którą wpływa wiele czynników, od postępu technologicznego po zmiany geopolityczne. Przedstawiamy najnowsze analizy przygotowane przez firmę badawczą Memoori dotyczące rynku telewizji dozorowej oraz kontroli dostępu.

Owen Kell

Niezależnie od tego, to właśnie firmy obecne na rynku azjatyckim są liderami we wdrażaniu najnowocześniejszych technologii: od systemów dozoru wizyjnego o wysokiej rozdzielczości po analitykę opartą na sztucznej inteligencji i rozpoznawanie twarzy.

Aktualna sytuacja na rynku monitoringu wizyjnego

Najnowszy raport Memoori *The Global Video Surveillance Business* bada perspektywy rynkowe dotyczące kamer dozorowych, pamięci masowej, oprogramowania i analityki w latach 2023–28. Szacunki oparte na kompleksowej analizie wyników łącznie 322 firm działających na globalnym rynku wskazują, że w 2022 r. wygenerowały przychody w wysokości 30,4 mld USD. Chociaż wydaje się, że era dwucyfrowego rocznego wzrostu w zakresie dozoru wizyjnego dobiegła końca, na rozwój rynku będą wpływać takie czynniki jak innowacje związane ze sztuczną inteligencją, rosnąca podaż i zapotrzebowanie na urządzenia i systemy oferujące wyrafinowane funkcje analityczne oraz przejście na urządzenia IP i zwiększenie rozdzielczości kamer. Eksperci Memoori uważają, że w latach 2023–28 rynek ten odnotuje skumulowaną roczną stopę wzrostu (CAGR) na poziomie 5,7%, a przychody do 2028 r. wyniosą 44,8 mld USD.

Wpływ sztucznej inteligencji

Integracja zaawansowanej sztucznej inteligencji (AI) i uczenia maszynowego z monitoringiem wizyjnym zaczyna osiągać dojrzałość. Do kluczowych czynników, które na to wpływają, należą:

- **Zastosowania praktyczne:** Dotychczasowe teoretyczne dyskusje na temat sztucznej inteligencji w systemach telewizji dozorowej zyskały praktyczny wymiar, a na pierwszy plan wysuwają się faktyczne zastosowania.
- **Zaawansowana analityka:** Możliwości analityczne stają się coraz bardziej wyrafinowane i niezawodne, zmniejszając liczbę fałszywych alarmów i umożliwiając uzyskanie bardziej szczegółowych informacji.
- **Malejący koszt SI**: Spadające koszty wdrożenia sztucznej inteligencji i uczenia maszynowego sprawiają, że technologie te stają się dostępne do szerszego zakresu zastosowań.
- **Rosnąca popularność analityki brzegowej:** Na coraz większą skalę wdrażana jest analityka brzegowa wykorzystująca m.in. urządzenia Internetu rzeczy, w których stosowane są specjalnie dla nich opracowane SoC *(System on Chip),* co umożliwia przetwarzanie danych bliżej źródła ich powstania, eliminując problemy z przepustowością sieci i pomagając użytkownikom końcowym zminimalizować ryzyko przesyłania lub przetwarzania danych związanych z prywatnością.

Memoori prognozuje, że do 2028 r. odsetek sieciowych kamer dozorowych z wbudowanymi funkcjami sztucznej inteligencji wzrośnie z obecnych 18% do ponad 50%. Wpłyną na to ich nowe funkcje, takie jak rozpoznawanie obiektów, analiza zachowania i inne formy inteligentnego monitorowania.

Wprowadzenie AI wiąże się jednak z wyzwaniami. Kwestie infrastrukturalne, takie jak ograniczenia przepustowości, opóźnienia i zabezpieczenia cybernetyczne, mogą utrudniać pełne wykorzystanie kamer wyposażonych w sztuczną inteligencję. Co więcej, brak ustandaryzowanych praktyk w zakresie danych i metodologii testowania dodatkowo komplikuje sytuację. Wyzwania te wymagają odpowiedzialnego i przejrzystego wdrażania technologii AI.

Wraz ze wzrostem ilości danych i zapotrzebowania na funkcje analityczne w latach 2022–28 rynek oprogramowania do zarządzania wideo (VMS) i analityki zwiększy się do poziomu 8,4% CAGR. Kontynuowane będzie przejście na analizę w chmurze, co ma wynikać z konieczności wykorzystania scentralizowanych zasobów obliczeniowych, niezbędnych do analizy olbrzymich zbiorów danych.

Zmiany geopolityczne wpływają na rynek telewizji dozorowej

W ostatnich pięciu latach napięcia geopolityczne i bariery handlowe stopniowo zmieniły globalny obraz rynku monitoringu wizyjnego. Ochłodzenie stosunków z Chinami spowodowało, że USA najpierw nałożyły stosunkowo niewielkie cła i ograniczyły producentom chińskim możliwość sprzedaży swoich produktów poszczególnym amerykańskim agencjom rządowym. Uchwalony w 2019 r. zakaz współpracy z firmami Hikvision i Dahua miał znaczny wpływ na rynek nie tylko w tym regionie. Wprawdzie wypchnięcie Hikvision i Dahua z USA znacząco zakłóciło łańcuchy dostaw, wymuszając rekalibrację dynamiki sił, to jednocześnie dało możliwość rozwoju firmom europejskim, koreańskim i japońskim. Axis, Hanwha Vision, IDIS, Secom i inni gracze opracowali nowe strategie i relacje w łańcuchu dostaw, by zapełnić lukę, jaka powstała, gdy z amerykańskiego rynku zniknęły Hikvision i Dahua.

Większość z tych firm skorzystała na tej sytuacji, np. Hanwha Vision, mając status zgodny z NDAA, w latach 2021–22 odnotowała 86-proc. wzrost sprzedaży w obu Amerykach. W tym samym czasie IDIS uzyskał wzrost przychodów zagranicznych z 50 mln USD do ponad 80 mln USD.

Producenci amerykańscy coraz częściej podkreślają pochodzenie produktów *Made in USA*, podczas gdy firmy europejskie, takie jak Axis Communications, wykorzystują swój status zgodny z NDAA, aby zwiększyć sprzedaż w Ameryce Północnej. Niektóre firmy zachwalają również rygorystyczne zasady i praktyki w zakresie bezpieczeństwa danych, aby jeszcze bardziej wzmocnić swoją pozycję wśród użytkowników końcowych, coraz bardziej świadomych kwestii związanych z cyberbezpieczeństwem i etyką.

Chińscy producenci systemów telewizji dozorowej, w tym Tiandy Technologies, Infinova, TVT Digital Technology i Raysharp, odnotowali spadki przychodów z 3% do 40% w 2022 r. w porównaniu z 2021 r. Znaczną część spadku można przypisać niekorzystnemu wpływowi blokad wywołanych przez COVID w Chinach oraz ogólnemu spowolnieniu chińskiej gospodarki w tym okresie, to niewątpliwie przyczyniły się do tego również ograniczenia handlowe. Chociaż wymienieni producenci chińscy nie zostali tak bezpośrednio dotknięci, jak Hikvision i Dahua, z pewnością będą nerwowo przyglądać się dalszemu negatywnemu wpływowi, jaki mogą mieć potencjalne ograniczenia ich działalność w USA.

Decyzja polityczna i związany z nim rozgłos medialny wywołany przez amerykańskie przepisy regulacyjne spowodowały skutki również poza USA. Przykładowo kilku głównych sprzedawców detalicznych w Wielkiej Brytanii postanowiło zrezygnować z kamer Hikvision i Dahua ze względu na obawy etyczne, a także trwające ruchy legislacyjne mające na celu ograniczenie korzystania z urządzeń obu firm w różnych organach sektora publicznego w niektórych krajach w Europie i poza nią.

Kontrola dostępu: urządzenia mobilne zyskują popularność

Prognozy Memoori dotyczące kontroli dostępu są nadal finalizowane, ale wstępne wskaźniki zapowiadają, że wzrost tego sektora wyprzedzi

→

wzrost rynku telewizji dozorowej w ciągu najbliższych 5 lat, odwracając dynamikę, która miała miejsce w branży zabezpieczeń technicznych od ponad dekady.

W tym sektorze dynamika łańcucha dostaw i systemów zabezpieczeń jest podobna, niepewność geopolityczna ma znacznie bardziej stonowany wpływ. Przyjęcie rozwiązań wykorzystujących biometrię zostało nieco zahamowane ze względu na zmiany zachowań i postaw wynikające z COVID. Motorem wzrostu stało się stopniowe przechodzenie na kontrolę dostępu opartą na urządzeniach mobilnych.

Z punktu widzenia użytkownika atrakcyjność mobilnej kontroli dostępu polega na jej wygodzie, ulepszonych funkcjach zabezpieczeń i elastyczności, jaką oferuje w zakresie administrowania systemem. Główni producenci tych rozwiązań, w tym HID Global, Brivo i WaveLynx, szybko dostrzegli tę zmianę, integrując się z Apple Wallet i Google Wallet, aby wykorzystać koniunkturę na rynku. Klienci również zwracają uwagę na te udogodnienia. Według wyników ankiety dotyczącej trendów w kontroli dostępu 42% respondentów na całym świecie planuje obecnie aktualizację do systemów mobilnych. Wstępne dane badania Memoori przewidują, że do końca 2023 r. systemy mobilne mogą generować ok. 20% wszystkich nowo wydanych poświadczeń kontroli dostępu do budynków niemieszkalnych.

Chociaż przejście na systemy mobilne jest coraz bardziej popularne, nie jest ono pozbawione wyzwań. Wśród wielu użytkowników końcowych kluczowymi obawami pozostają prywatność i cyberbezpieczeństwo, szczególnie w przypadkach, gdy urządzenia osobiste mają stanowić główne narzędzie do kontroli dostępu. Z tego powodu niektóre przedsiębiorstwa niechętne są tej zmianie, preferując korzystanie z fizycznych kart w celu ograniczenia ryzyka związanego z narażeniem utraty danych osobowych z urządzeń mobilnych.

Kolejną kwestią jest infrastruktura. Przejście na systemy mobilne często wymaga aktualizacji istniejących urządzeń, np. czytników Bluetooth lub NFC, dodając dodatkową warstwę złożoności i koszty modernizacji. Ponadto niektórzy niechętnie integrują swoje rozwiązania z portfelem Apple, twierdząc, że jest to proces uciążliwy. Należy również zauważyć, że Apple Wallet wiąże się z dodatkowymi opłatami za poświadczenia, co może zniechęcać firmy rozważające zmianę.

Mimo to wyraźny jest trend przechodzenia firm na mobilną kontrolę dostępu. Można się zatem spodziewać się, że ten segment będzie miał znaczący udział w rynku kontroli dostępu w nadchodzących latach.

Łączenie wszystkiego w całość

Wraz z ewolucją branży zabezpieczeń technicznych na pierwszy plan wysuwa się integracja. Zamiast utrzymywać osobne systemy zabezpieczeń (dozór wizyjny, kontrola dostępu czy system alarmowy), firmy poszukują wielofunkcyjnych możliwości zwiększenia wydajności i wartości dodanej w całym B-IoT *(Blockchain Driven Internet of Things)*. Zauważalny jest wzrost zapotrzebowania ze strony zarówno użytkowników, jak i sprzedawców na ujednolicone platformy, które nie tylko usprawniają przepływy pracy, ale także ułatwiają wgląd w dane poprzez zebranie informacji z różnych systemów. Pojawiają się głębsze formy interoperacyjności, które obejmują struktury danych, analitykę, zarządzanie tożsamością i możliwości automatyzacji, wspierane przez rozszerzone sieci partnerskie między domenami i poprawę funkcjonalności interfejsów API.

Jednym z kluczowych czynników umożliwiających tę transformację jest poprawa standaryzacji danych z systemów zabezpieczeń i ich metadanych. Dostarczanie bogatszych kontekstowo danych jest potrzebne do podejmowania inteligentnych decyzji. Dane zebrane ze wszystkich systemów zabezpieczeń i zarządzania budynkiem umożliwiają bardziej dopasowane i responsywne działania, takie jak selektywne blokowanie drzwi, regulacja oświetlenia w oparciu o zajętość lub planowanie ruchu wind w celu dopasowania do wzorców ruchu ludzi w budynku. W ten sposób oszczędza się energię i poprawia doświadczenia użytkowników budynku.

Chociaż integracja jest przekonująca, nie zawsze jest prosta. Odpowiednio wykwalifikowani integratorzy systemów, wyposażeni w wiedzę w zakresie technologii IT i OT, kontroli dostępu, systemów telewizji dozorowej, a nawet protokołów komunikacyjnych, takich jak BACnet *(Building Automation and Control Networks)*, będą niezbędni do wdrażania złożonych, ujednoliconych rozwiązań bezpieczeństwa i B-IoT.

Dopóki starsze systemy, zastrzeżone protokoły i brak ustandaryzowanych formatów danych nie zostaną wycofane, nadal będą stanowić przeszkody na drodze do integracji. W miarę, jak branża będzie zmierzać w kierunku ustandaryzowanych rozwiązań, bezproblemowe integracje staną się normą, a nie wyjątkiem.

Czekamy

Rynek zabezpieczeń technicznych zmienia się pod wpływem różnych czynników, w tym postępu technologicznego, zmian geopolitycznych oraz rosnącego nacisku na integrację i etykę. Firmy, które potrafią dostosować się do tych zmian, wprowadzać innowacje i oferować inteligentne, zintegrowane rozwiązania, będą się rozwijać. Jednak utrzymanie się na czele będzie wymagało ciągłych innowacji, rozważań etycznych i, co być może najważniejsze, zdolności dostosowywania się do stale zmieniających się warunków.

Wśród innych trendów wymienionych w raporcie Memoori na uwagę zasługują zmiany dotyczące systemów telewizji dozorowej i kontroli dostępu idące w kierunku wieloskładnikowego uwierzytelnianiem, zmagania z ciągłym niedoborem umiejętności (zwłaszcza w zastosowaniach międzysektorowych i sztucznej inteligencji), większy nacisk na zrównoważony rozwój środowiska oraz stale obecny wpływ ryzyka cyberzagrożeń na urządzenia, politykę i priorytety użytkowników końcowych.

Trwały sukces rynkowy będzie zależał od ciągłych innowacji i zwinnego podejścia do stale zmieniającego się otoczenia biznesowego. Firmy, które trzymają rękę na pulsie, dostosowują sytuację do wielu czynników i pozostają otwarte na nowe pomysły oraz pragmatyczne inwestycje, będą lepiej przygotowane do dominacji na tym ewoluującym rynku.

Owen Kell, współpracownik ds. badań nad IoT i bezpieczeństwem Memoori, jest specjalistą ds. analityki biznesowej z prawie dwudziestoletnim doświadczeniem w badaniach rynkowych nad nowymi technologiami wdrażanymi w firmach w celu zwiększenia wydajności, zrównoważonego rozwoju i inteligencji budynków oraz środowisk miejskich. Jest ekspertem rynku IoT, Big Data, AI, uczenia maszynowego oraz bezpieczeństwa fizycznego i cybernetycznego w sektorze inteligentnych budynków. Wspierał zarówno globalnych gigantów, jak i innowacyjne start-upy. Jest liderem w branży, autorem ponad 20 raportów rynkowych, które ukształtowały temat inteligentnych budynków. ●

Korekta na globalnym rynku telewizji dozorowej

Raport opracowany przez Novaira Insights wprowadza korektę do ubiegłorocznych prognoz dotyczących kondycji globalnego sektora telewizji dozorowej.

Wynika ona głównie z gwałtownego spadku wartości rynku chińskiego będącego następstwem blokad związanych z COVID-19. Korekta będzie prawdopodobnie przejściowa, ponieważ Chiny odzyskują siły.

Według raportu Novaira Insights spadek wartości globalnego rynku zabezpieczeń fizycznych w roku w 2022 r. wyniósł 3,4%. Było to jednak w dużej mierze spowodowane gwałtownym załamaniem się rynku chińskiego, który poniósł znacznie większe straty, ponieważ jego wartość spadła o 18,6% z powodu pandemicznych ograniczeń wprowadzonych przez władze Chin podczas kolejnej fali COVID-19 w 2022 r.

– *Wydatki chińskiego rządu zostały przekierowane z obszarów takich jak dozór wizyjny na walkę z COVID-19 i wspieranie gospodarki podczas lockdownów* – powiedział Josh Woodhouse, główny analityk i założyciel Novaira Insights. – *Szacuje się, że Chiny pozostaną największym na świecie regionalnym rynkiem urządzeń dozoru wizyjnego, ponieważ nawet w 2022 roku Chiny odpowiadały za 44% światowego rynku zabezpieczeń. Jest to jednak spadek, zważywszy na fakt, że rok wcześniej aż 52% rynku zabezpieczeń należało do firm chińskich. Dodał, że poza Chinami większość rynków nadal rośnie, a rynek na świecie z wyłączeniem Chin wzrósł o 13,2% w 2022 r.*

Jeśli chodzi o ten rok, wraz z ponownym otwarciem Chin i zniesieniem ograniczeń związanych z COVID w większości krajów widać, że inwestycje wracają na właściwe tory. Będzie to pozytywna zmiana dla globalnego rynku telewizji dozorowej, który według raportu Novaira Insights wzrośnie w tym roku o 11,8%, osiągając wartość ponad 27 mld USD.

Chińskie środki walki z COVID

Rok 2022 można opisać jako okres *lockdownu* w Chinach. Pierwsza fala ograniczeń zaczęła się w lutym 2022 r. w Szanghaju po gwałtownym wzroście liczby przypadków COVID. Była to największa blokada od czasu Wuhan w 2019 r., kiedy po raz pierwszy pojawił się wirus SARS-COV-2. Blokady w 2022 r. zarządzono również w innych chińskich miastach, w tym w Chengdu i Daqing. Miało to ogromny wpływ na gospodarkę chińską. Według Międzynarodowego Funduszu Walutowego PKB Chin wzrósł zaledwie o 3% w 2022 r. w porównaniu z 8,5% w 2021 r. To, a także zmęczenie społeczeństwa doprowadziło do protestów w całych Chinach, co ostatecznie zmusiło władze do wstrzymania polityki zero COVID i ponownego otwarcia kraju pod koniec 2022 r.

Wpływ na monitoring wizyjny

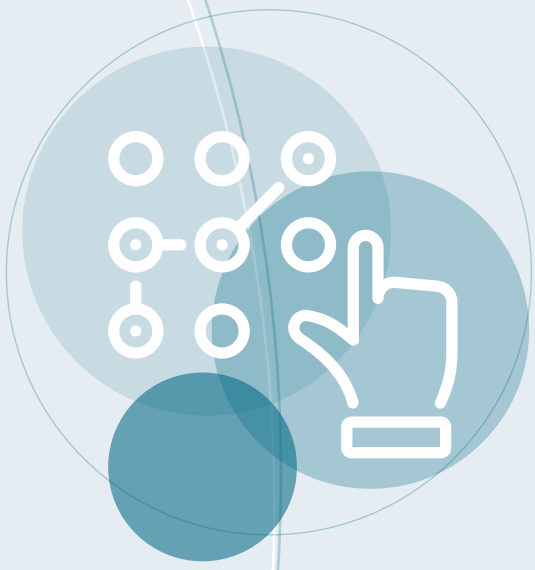
Podobnie jak inne branże, chiński rynek monitoringu wizyjnego odczuł skutki *lockdownów* i wynikającej z nich bezczynności biznesowej. Widać to wyraźnie w raporcie finansowym Hikvision za 2022 r., w którym odnotowano, że wartość sprzedaży urządzeń dozorowych wyniosła 65,9 mld juanów. To w porównaniu z rokiem poprzednim daje wzrost o zaledwie 1,12% (65,1 mld juanów). W latach 2020–21 wartość sprzedaży Hikvision wzrosła o 16,9%, natomiast przychody za pierwszy kwartał 2023 r. spadły o 1,94% rok do roku.

Powrót na ścieżkę wzrostu

Według Novaira Insights spadek wartości chińskiego rynku telewizji dozorowej jest tymczasowy. W najbliższym czasie spodziewany jest powrót do wzrostu z trzech powodów.

Po pierwsze rynek krajowy jest ogromny. Po drugie aktywny rozwój i udział Chin w niektórych gałęziach gospodarki, zwłaszcza inwestycje w inteligentne miastach i taki też transport, tworzy ogromne zapotrzebowanie na urządzenia dozoru wizyjnego. Po trzecie ciągłe zaangażowanie Chin w innowacje techniczne, szczególnie w dziedzinie obrazowania przy słabym oświetleniu i kamerach bispektralnych, zwiększy popyt na rynkach krajowym i zagranicznym. ●

Raport o handlu



Zmiany w postawach konsumentów, postępująca cyfryzacja, zrównoważony rozwój, wyzwania logistyki i rynku pracy. Co przesądzi w najbliższym czasie o modelu sprzedaży? W jaki sposób na zmiany w handlu reaguje rynek security? Oto nasz raport.

Adela Prochyra,
Jan Grusznic

Na początek trochę twardych danych. W roku 2021 działalność handlowa stanowiła 16% wartości dodanej brutto wytworzonej w całej gospodarce narodowej w Polsce. W roku 2022 udział handlu w łącznym PKB Polski wynosił 18% i – jak podaje portal wiadomoscihandlowe.pl – był jednym z najwyższych w Europie. Wówczas padł rekord eksportu polskich towarów – sprzedano produkty za sumę 343,8 mld euro, po raz pierwszy przekraczając granicę 300 mld euro.

Obroty towarowe handlu zagranicznego[1] od stycznia do czerwca 2023 r., jak podaje GUS w raporcie sygnalnym z sierpnia, wyniosły: 821,4 mld zł w eksporcie oraz 790,6 mld zł w imporcie. Saldo było dodatnie i wyniosło 30,8 mld zł, podczas gdy w analogicznym okresie 2022 r. miało wartość -42,4 mld zł. W ciągu roku eksport wzrósł o 6,1%, a import spadł o 3,2%.

W roku 2023 liczba sklepów internetowych przekroczyła 60 tys. Pod koniec 2022 r. było ich 57,9 tys. (wg danych Dun & Bradstreet). Tylko w pierwszym półroczu bieżącego roku otworzyło się 3,9 tys. nowych sklepów – to dwa razy więcej niż w latach ubiegłych. Jeżeli bieżący trend się utrzyma, wkrótce na polskim rynku będzie działać 65 tys. podmiotów e-commerce. Oznaczałoby to, że firm handlujących w sieci przybywa dwa razy szybciej, niż ubywa zamykających się placówek stacjonarnych.

Którędy idą trendy?

To, jak wygląda dany sektor gospodarki, zależy od wielu zmiennych. Handel jest o tyle specyficzny – w przeciwieństwie do np. transportu czy hotelarstwa – że dotyczy bezpośrednio nas wszystkich, chociażby poprzez kształtowanie cen podstawowego koszyka zakupów. Jednocześnie jest podatny na zachowania konsumenckie, co jest widoczne np. w czasie rosnącej inflacji. Wzrost cen zwykle skutkuje ograniczeniem konsumpcji, a to oznacza zmniejszenie wolumenu nabywanych dóbr i usług i zmusza sprzedawców np. do obniżania marż lub ograniczania zatrudnienia.

Tego typu czynników wpływających na stan tego sektora jest wiele. Razem tworzą splot, który nieustannie się zmienia. Liczby zacytowane powyżej są ich wypadkową. Oczywiście, trendów i zmiennych jest dużo, ale my ograniczymy się do czterech najważniejszych, które w największym stopniu wpływają na obecny kształt polskiego handlu.

Trend 1. COVID-19 i co z niego wynikło

Od tego, co się wydarzyło w 2020 r., nie ma ucieczki. Pandemia, choć przez ostatnie lata odmieniana przez wszystkie przypadki, odcisnęła głębokie piętno na społeczeństwach i gospodarkach poszczególnych krajów. Handel był jednym z tych sektorów, które pod wpływem gwałtownych wydarzeń w latach 2020–23 zmieniły się najbardziej.

Pandemia wprowadziła niepewność we wszystkich sektorach i jednocześnie zmieniła tradycyjne modele konsumpcji. *Lockdown* i różne poziomy restrykcji zmusiły wiele sklepów do czasowego zamknięcia lub ograniczenia działalności, promując tym samym wzrost e-commerce i usług dostawczych. Klienci, w obawie o swoje bezpieczeństwo, częściej wybierali zakupy online, co przyspieszyło lub wręcz wymusiło digitalizację wielu przedsiębiorstw handlowych, które adaptowały nowe technologie i strategię. Firmy, które wcześniej nie były obecne online, zainwestowały w rozwój własnych platform zakupowych oraz poprawę infrastruktury technologicznej. W tym okresie nastąpił dynamiczny wzrost zainteresowania e-handlem, który po zakończeniu pandemii nie wyhamował. Co więcej, rozwój technologii umożliwił wprowadzenie licznych nowości: sklepów bezobsługowych, przekształcenie tradycyjnych sklepów w po części samoobsługowe (instalacja kas samoobsługowych) czy automatyzację procesów magazynowych, co zmienia doświadczenie klienta.

Pierwsze udane uruchomienia autonomicznych punktów stały się impulsem do wykorzystania na większą skalę analizy obrazu wspartej algorytmami głębokiego uczenia do automatyzacji procesów zakupowych, logistycznych i merchandisingowych. Zwiększony popyt na kamery dozoru wizyjnego, stanowiących podstawę systemu jako źródła materiału do analizy, był konsekwencją tej zmiany. Decentralizacja oraz ogromne ilości danych wymusiły stosowanie dostępnych zasobów chmurowych zapewniających ich konsolidację i wydajniejsze zarządzanie informacją. Coraz popularniejsze wykorzystanie chmury publicznej przyczyniło się do rozpoczęcia migracji systemów zabezpieczeń technicznych w kierunku SaaS i potrzeby ich integracji.

UWAGA. Ze względu na zaokrąglenia danych, w niektórych przypadkach sumy składników mogą się nieznacznie różnić od podanych wielkości „ogółem".

[1] Zbiór danych o obrotach handlu zagranicznego ma charakter otwarty. Dane publikowane wcześniej są korygowane w miarę napływu zgłoszeń celnych oraz INTRASTAT. Dane za okres styczeń – czerwiec 2023 r. zostały uzupełnione o niezarejestrowane zgłoszenia celne za miesiące wcześniejsze br.

Inna zmiana, która zaszła pod wpływem pandemii COVID-19, wiąże się ze zwiększonym zapotrzebowaniem na produkty pierwszej potrzeby i stosowaniem wyższych standardów sanitarno-higienicznych. Zaspokojenie tych potrzeb stało się kluczowym wyzwaniem dla producentów i handlowców. Skala zapotrzebowania była ogromna, bo poza artykułami higienicznymi do indywidualnego użytku, takimi jak maseczki, rękawiczki jednorazowe itd., przemysł musiał dostarczać preparaty higieniczne na użytek publiczny. Sklepy i centra handlowe np. wprowadziły ścisłe procedury utrzymania czystości i higieny, aby zapewnić bezpieczeństwo klientom i pracownikom. Stosowano m.in. regularnie dezynfekcje i ozonowanie pomieszczeń, umieszczano dozowniki z płynami antybakteryjnymi w wielu miejscach i nakazywano korzystanie z nich przed wejściem.

Branża zabezpieczeń technicznych szybko odpowiedziała na potrzebę bezdotykowego mierzenia temperatury, dostarczając modyfikowane kamery termowizyjne. W większości wdrożeń rozwiązania te jednak nie spełniły pokładanych w nich oczekiwań, generując olbrzymią liczbę fałszywie dodatnich detekcji. Jednak popularyzacja tych rozwiązań wpłynęła pozytywnie na cenę kamer termowizyjnych, a znaczna liczba webinarów poszerzyła wiedzę na temat niechłodzonych kamer pracujących w paśmie LWIR.

Ten trend znacząco osłabł, ale pewne nawyki, jak regularne mycie rąk, zostaną z nami na dłużej. Autorzy raportu opublikowanego przez Grand View Research w kwietniu 2020 r. podają, że prognozowana wielkość globalnego rynku środków do dezynfekcji rąk (w 2019 r. wyceniona na 2,7 mld dolarów) wzrośnie ze złożoną roczną stopą wzrostu (CAGR) wynoszącą 22,6% w latach 2020–27. Jak wygląda to w Polsce? Rynek FMCG (dóbr szybko zbywalnych; *Fast Moving Consumer Goods)* według badania NielsenIQ w 2022 r. w porównaniu do 2021 r. osiągnął rekordowy wzrost wartości sprzedaży wynoszący 15,2%. Cały rynek FMGC był wart 246 bln zł, z czego kategorie kosmetyczno-chemiczne to aż 33,9 mld zł. Koszyk kosmetyczno-chemiczny odnotował wzrost w 2022 r. wynoszący 14,2%, jednak aż w 80% był on spowodowany wzrostem średniej ceny produktów. Wzrost wolumenowy był nieznaczny. Ta zmiana okazała się więc nietrwała i poza skokowym zainteresowaniem pewną kategorią produktów nie przełożyła się na trwałą zmianę nawyków.

W czasie pandemii przedsiębiorstwa, o czym nie można zapomnieć, borykały się również z problemami logistycznymi i dostawczymi z powodu globalnych zakłóceń w łańcuchach dostaw, co wymagało od nich większej elastyczności i poszukiwania alternatywnych rozwiązań. W rezultacie pandemia wywołała wiele trudności, ale również stymulowała innowacje i przyspieszyła zmiany w sektorze handlu w Polsce, takie jak rozbudowa lokalnych centrów magazynowych i logistycznych. To rynek dynamicznie się rozwijający, o czym pisaliśmy w numerze 1/2023 „A&S Polska".

Trend 2. Klient nasz pan, czyli zmiany w upodobaniach konsumenckich

Rewersem sytuacji opisanej powyżej była solidarność konsumentów z przedsiębiorcami. Części kupujących zależało na wspieraniu lokalnych przedsiębiorców i producentów, co zwiększyło popularność zakupów w mniejszych lokalnych sklepach i na bazarkach. Nie wszystkie jednak udało się ocalić i część zamknięto. Zdawać by się mogło, że to bezpośredni skutek pandemicznych lockdownów, przerw w dostawach i licznych restrykcji, które na zmianę wprowadzano i wycofywano.

Trend ten jednak jest już widoczny od dekady, w pandemii jedynie się uwypuklił. Portal money.pl w sierpniu 2021 r. pisał: „W dekadę w Polsce zamknięto ponad 100 tys. sklepów. O dziwo, najmniej w ostatnim roku". Zaznaczył jednak, że pandemiczne żniwo będziemy zbierać jeszcze długo. Które były najczęściej likwidowane? To m.in. sklepy z artykułami biurowymi i piśmienniczymi, jak również z artykułami używanymi, obuwiem i galanterią, a także tytoniem i wyrobami mięsnymi. Zamknięto także 164 apteki.

Kłopoty nie ominęły też branży elektronicznych systemów zabezpieczeń. W wyniku problemów z ciągłością dostaw wiele firm nie było w stanie zrealizować zakontraktowanych projektów i zostało zmuszone zamknąć działalność. Część przedsiębiorców, obserwując problemy producentów, zdecydowała się na przebranżowienie. Ale pojawiło się także kilku nowych graczy, którzy wcześniej nie stawiali na bezpieczeństwo fizyczne, i dzisiaj są zauważalnymi podmiotami w branży.

Likwidacje wskazują, czego jako konsumenci już dłużej nie potrzebowaliśmy. Jednocześnie zmiany widoczne w naszych koszykach informują, co teraz przyciąga uwagę kupujących. W ciągu ostatnich trzech lat upodobania zakupowe uległy znaczącej zmianie. Większy nacisk kładziono na produkty i usługi lokalne. Popularyzacja idei „kupuj lokalnie" przyczyniła się do wzrostu popytu na produkty regionalne, ekologiczne i ręcznie robione, podkreślając wartość autentyczności i jakości i często znosząc problem kosztownych oraz długotrwałych dostaw. Konsumenci częściej wybierali produkty lokalnych producentów i rzemieślników, wspierając tym samym lokalną ekonomię w czasie kryzysu, a także po nim, mając jeszcze w pamięci liczne kłopoty, które wygenerował.

Zauważalny był również wzrost świadomości zdrowotnej i ekologicznej wśród polskich konsumentów. Preferencje były skierowane ku zdrowszym wyborom żywieniowym, produktom wegańskim czy organicznym. Ponadto rosnąca odpowiedzialność ekologiczna przekładała się na zainteresowanie produktami przyjaznymi dla środowiska, takimi jak towary z recyklingu czy wyroby o mniejszym wpływie na środowisko naturalne.

Należy zauważyć, że konsumenci stali się bardziej oszczędni i rozważni w swoich decyzjach zakupowych. Promocje, wyprzedaże oraz różnorodne programy lojalnościowe stały się kluczowymi determinantami wyboru, gdzie cena i wartość oferowanego produktu czy usługi odgrywały istotną rolę. Wszystkie te czynniki: wzrost świadomości ekologicznej, kryzys finansowy, który wymusił oszczędniejsze sposoby gospodarowania budżetem domowym, i rozwój technologii złożyły się na dynamiczny wzrost popularności w ostatnich latach cyfrowych aplikacji oraz sklepów z odzieżą używaną i innymi artykułami vintage. Oprócz bardzo popularnego w Polsce Vinted warto wymienić też aplikację LESS_ autorstwa Mateusza Oleksiuka, OLX, Allegro lokalnie czy francuski Vestiaire Collective dla poszukujących towarów luksusowych.

Ostatnie trzy lata odznaczały się również zmianą w stylu życia i pracy. W skrócie: mniej w biurze, więcej w domu, co naturalnie przełożyło się na zmiany w upodobaniach zakupowych, jak chociażby wzrost zainteresowania produktami związanymi z pracą zdalną, wyposażeniem domowego biura, a także produktami z obszaru fitness i wellness w domu.

Budżety na bezpieczeństwo w handlu detalicznym względnie pozostają na niezmienionym poziomie lub są ograniczane. To sprawia, że przed zespołami ds. bezpieczeństwa stoi nie lada wyzwanie – mają zapewnić adekwatny jego poziom przy ograniczonych środkach. Tematem dyskusji liderów bezpieczeństwa w handlu detalicznym jest wykorzystanie na ten cel inwestycji technologicznych przeznaczonych na realizację innych zadań. Coraz bardziej popularne staje się stosowanie systemów wizyjnych do różnych celów – bezpieczeństwa, marketingu, zbierania informacji o doświadczeniu klienta. Sprzyja temu rozwój technologii analizy brzegowej (tj. bezpośrednio w kamerach lub dodatkowych niewielkich komputerach instalowanych w sklepie), która umożliwia wykorzystanie już istniejących urządzeń (np. kamer), ograniczając koszty inwestycji.

Trend 3. W kierunku zrównoważonego rozwoju

Zrównoważony rozwój stał się jednym z kluczowych czynników wpływających na kształtowanie strategii i praktyk handlowych na całym świecie, w tym również w Polsce. Wprowadzenie zasad zrównoważonego rozwoju do biznesu to nie tylko reakcja na globalne wyzwania, takie jak zmiany klimatyczne czy przekroczenie zasobów naturalnych, ale również odpowiedź na zmieniające się potrzeby i oczekiwania konsumentów, którzy coraz częściej poszukują produktów i usług przyjaznych dla środowiska i społeczności.

Przedsiębiorstwa handlowe, dążąc do zrównoważonego rozwoju, inwestują w innowacje i technologie, które mogą zmniejszyć ich ślad ekologiczny. Obejmuje to m.in. wprowadzanie opakowań wielokrotnego użytku, ograniczanie marnotrawstwa, promowanie recyklingu oraz wykorzystywanie energii ze źródeł odnawialnych. Coraz częściej pojawiają się produkty ekologiczne, lokalne czy też posiadające certyfikaty *fair trade*.

Ten trend jest ściśle powiązany z poprzednim. Co prawda zmiany w zakresie np. raportowania o źródłach pozyskiwania energii są wymuszane przez ustawodawcę, ale konsumenci odgrywają w tym procesie nie mniej istotną rolę, kierując się w swoich wyborach zakupowych świadomością ekologiczną i społeczną. Przy czym klienci nie muszą tu być rozumiani jako klienci indywidualni – to także firmy, które są inwestorami w nowych przedsięwzięciach. Preferencje te skłaniają przedsiębiorstwa do dostosowania oferty, umożliwiając klientom podejmowanie decyzji zgodnych z ich wartościami i przekonaniami, mając na uwadze nie tylko zysk finansowy, ale też środowisko naturalne. Transparentność stała się istotnym elementem zrównoważonego handlu. Klienci oczekują pełnej informacji na temat pochodzenia produktu, warunków jego produkcji oraz wpływu na środowisko. Inwestorzy również coraz częściej zwracają uwagę na długofalowe strategie zrównoważonego rozwoju w ocenie i wyborze przedsiębiorstw do inwestycji. Kluczowe znaczenie mają tu raporty niefinansowe, które uwydatniają zaangażowanie firm w aspekty środowiskowe, społeczne i zarządzanie korporacyjne. Te elementy stają się istotne dla wyceny firm, pozyskiwania finansowania i budowania relacji z inwestorami i klientami.

Firmy z branży handlowej i konsumenckiej angażują się w inicjatywy związane z ESG (środowiskowe, społeczne i ładu korporacyjnego). Koncentrują się na budowaniu marek, które odzwierciedlają wartości zrównoważonego rozwoju, odpowiadając tym samym na rosnące oczekiwania konsumentów w zakresie dbałości o środowisko i odpowiedzialności społecznej. Działania, takie jak redukcja emisji CO_2, oszczędzanie wody i kontrola źródeł surowców w łańcuchu dostaw, przyczyniają się do zwiększenia atrakcyjności oferty firmy i wpływają pozytywnie na wyniki sprzedaży oraz opłacalność przedsiębiorstwa. Wymogi prawne i regulacje, które promują zrównoważony rozwój, takie jak normy emisji CO_2 czy regulacje dotyczące odpadów, wpływają na działalność handlową, wymuszając na firmach dostosowanie swoich procesów i strategii.

Okiem security

Zrównoważony rozwój staje się także zauważalnie istotny przy wyborze producenta urządzeń do systemów zabezpieczeń i jego produktów. Choć nadal cena jest najistotniejszym kryterium wyboru systemu, coraz częściej do głosu dochodzą zrównoważony rozwój, wkład w ochronę środowiska, ład korporacyjny i społeczna odpowiedzialność. Nacisk na wydłużone wsparcie gwarancyjne i pogwarancyjne przekraczające 5 lat, wykorzystanie materiałów nadających się do powtórnego przetworzenia czy skład i wielkość opakowań to jaskółki zmian, które czekają branżę w najbliższych latach.

Trend 4. Otoczenie prawne

Krajowy sektor handlu jest kształtowany przez przepisy i regulacje prawne w nie mniejszym stopniu niż przez upodobania konsumentów czy rozwój technologii i e-commerce. W roku 2023 Polska wprowadziła istotne zmiany w przepisach i polityce dotyczące sektora handlowego, które miały na celu dostosowanie się do dynamicznie zmieniającego się globalnego środowiska biznesowego oraz podjęcie reakcji na lokalne i globalne wyzwania, takie jak zrównoważony rozwój czy cyfryzacja. Objęły one wszystkich uczestników rynku e-commerce, czyli zarówno sprzedających, jak i kupujących. O jakich zmianach mowa?

Wzmocniono przepisy dotyczące handlu elektronicznego, z naciskiem na bezpieczeństwo danych klientów i transakcji online. Zwiększono wymagania dotyczące przejrzystości i informowania klientów podczas zakupów online, co miało na celu zwiększenie zaufania konsumentów do e-handlu.

→

Wprowadzono zmiany, których celem jest wzmocnienie praw konsumentów, w tym poprawa dostępu do informacji o produktach i usługach, a także zasady dotyczące zwrotów i reklamacji. Chodzi o to, aby uczynić proces bardziej przyjaznym dla konsumentów. Firmy muszą teraz dostarczać bardziej czytelne i kompletne informacje na temat oferowanych produktów i usług, co pozwala konsumentom podejmować bardziej świadome decyzje zakupowe. Przykładem nowej regulacji jest wymóg informowania o najniższej cenie danego towaru w ciągu ostatnich 30 dni.

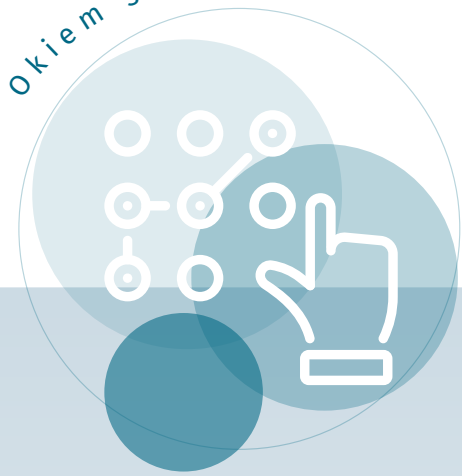
Procedury zwrotów i reklamacji również przeszły modernizację. Uproszczono i przyspieszono procesy, tak aby klienci mogli szybko i bez zbędnych trudności otrzymać odpowiedź lub rozwiązanie swojego problemu. Wprowadzenie tych zmian miało na celu zwiększenie satysfakcji konsumentów, budowanie długoterminowych relacji i lojalności, co jest kluczowe dla rozwoju i sukcesu przedsiębiorstw handlowych. Zaktualizowane przepisy mają spowodować, by rynek działał zgodnie ze standardami etycznymi i odpowiedzialnymi praktykami biznesowymi.

Wielkim wyzwaniem dla krajowych podmiotów e-handlu była konkurencja z Azji, oferująca nieraz dumpingowe ceny produktów. W celu wyrównania konkurencyjności pomiędzy różnorodnymi uczestnikami rynku e-handlu Unia Europejska wprowadziła pakiet e-commerce, który zaczął obowiązywać od 1 lipca 2021 r. W tym okresie Polska zaktualizowała swoje przepisy, implementując ustawę z 20 maja 2021 r. wprowadzającą zmiany w ustawie o podatku od towarów i usług oraz innych powiązanych ustawach. Nowe regulacje, zawarte w pakiecie VAT e-commerce, dotyczą opodatkowania VAT w handlu elektronicznym.

Unijne regulacje mają na celu wyeliminowanie przesyłek importowanych do krajów UE bez naliczonego VAT-u. Jednocześnie nowe przepisy ułatwiają procedury administracyjne związane z transakcjami e-handlowymi realizowanymi pomiędzy krajami członkowskimi UE, upraszczając tym samym proces handlu online na terenie Unii.

Jest jeszcze wiele zmiennych wpływających na kształt polskiego handlu, do których należą zagadnienia logistyczne, w tym drożejące paliwo i energia elektryczna, oraz dynamicznie zmieniający się rynek magazynowy; zmieniający się rynek pracy, także pod wpływem imigrantów i uchodźców, ale też cyfryzacji i coraz większej popularności pracy zdalnej; dynamicznie zmieniający się krajobraz geopolityczny, w którym zamykają się kolejne ścieżki połączeń handlowych (por. brexit, wojna w Ukrainie, wojna Izraela z Hamasem); zmiany polityczne, które wpłyną na regulacje podatkowe, np. Polski Ład; kryzys finansowy i inflacja.

Okiem security



Handel detaliczny to rynek wyjątkowy dla producentów, dostawców i integratorów elektronicznych systemów zabezpieczeń, gdzie różnią się sposoby wykrywania włamań, ochrony zasobów i zapobiegania stratom. Niezależnie od przyjętych rozwiązań widoczną potrzebą jest ich konsolidacja nie tylko w sklepach, ale także w centrach dystrybucyjnych. Korzyścią jest lepszy nadzór nad całym łańcuchem dostaw i sprostanie wyzwaniom związanym z istniejącą infrastrukturą teleinformatyczną. Dla producentów i integratorów zabezpieczeń stanowi to wyjątkową okazję do współpracy i wdrożenia rozwiązań, które mogą lepiej służyć sprzedawcom detalicznym oraz chronić pracowników, klientów i zasoby przed zagrożeniami – a co ważniejsze, chronić te marki.

Nowoczesne zasoby handlowe w Polsce

Zasoby GLA (powierzchnia wynajmowana)

13,10 mln m² GLA

Powierzchnia biurowa oddana do użytku w I poł. 2023

149 114 m² GLA

Powierzchnia w budowie

379 759 m² GLA

Wskaźnik nasycenia powierzchnią handlową

347 m² na 1000 mieszkańców

Wskaźnik nasycenia powierzchnią handlową dla miast z centrami handlowymi

678 m² na 1000 mieszkańców

Źródło: PRCH Retail Reserch Forum, I poł. 2023 r.

REKLAMA

Polski rodzinny handel to liczący się klient

Przyzwyczailiśmy się myśleć, że handel w Polsce został zdominowany przez obcy kapitał. Nic dziwnego, biorąc od uwagę liczbę sklepów sieci Lidl, Biedronki, Kauflandu czy Netto i dodając do nich np. rozwijającą się sieć Aldi czy drogeryjnego Rossmanna itp., doliczymy się ponad 7310 sklepów stanowiących własność zagranicznych koncernów handlowych.

Jacek Tyburek

Liczby imponujące i skala wręcz oszałamiająca z punktu widzenia możliwości wsparcia tych firm przez branżę security. Problem w tym, że z reguły mają one własne rozbudowane struktury bezpieczeństwa biznesu i ograniczania strat, działają zgodnie z wypracowanymi przez dziesięciolecia metodami *corporate security* oraz własnymi standardami.

Skala polskiego handlu

Wydawać by się mogło, że rodzime firmy handlowe ustępują liczbą i rozmachem korporacjom międzynarodowym. Ale jeśli przyjrzeć się bliżej, obraz zaczyna się zmieniać. Na liście 100 największych polskich firm, które jednocześnie spełniają kryteria definicji firm rodzinnych, znajdują się takie marki, jak Dino (2340 placówek), LPP (2141 sklepów), CCC (950 sklepów), Agata Meble (32 salony) czy Apart (200 sklepów). Właściciele sklepów Agata założyli sobie kiedyś, że na polskim rynku chcą być lepsi od IKEA. Obecnie Agata to 32 salony, IKEA 11. To łącznie ponad 6600 obiektów handlowych różnych branż. Do tego dochodzi wiele firm handlowych w przeważającej liczbie również tworzących konsorcja, np. pod szyldem Lewiatan działa ponad 3200 sklepów. Media Expert liczy 550 sklepów, 365 placówek wchodzi w skład sieci marketów budowlanych Mrówka. Widać zatem wyraźnie, że grupa rodzimych firm o charakterze rodzinnym to ponad 7000 sklepów, a przecież należy doliczyć także Polo Markety (250), sklepy pracujące w sieci Eurocash (500) czy wreszcie Żabki, które jako pojedyncze sklepy zazwyczaj stanowią niezwykle trudny do prowadzenia rodzinny biznes (dziesięciotysięczny sklep Żabka otworzyła w poznańskim Starym Browarze). Dołóżmy jeszcze lokalnie działające mniejsze sieci handlowe, a zobaczymy, że w szranki z kapitałem zagranicznym staje ponad 21 tysięcy (biorąc pod uwagę tylko te wcześniej wyliczone) jednostek handlowych.

Zważywszy na skalę tej części polskiej gospodarki, zadanie wypracowania polityki bezpieczeństwa i zapobiegania stratom jest dla każdej firmy z osobna wyzwaniem. To już nie są zadania dla pojedynczych Security Managerów bez względu na to, jak sprawnymi profesjonalistami by nie byli. Security Manager w tak dużych firmach musi być liderem zespołu złożonego z analityków, kontrolerów, planistów i regionalnych opiekunów biznesu. Niezależnie od tego, czy są to zasoby własne, czy matrycowa struktura, po to, aby na poważnie mówić o zapobieganiu stratom, świadomości ich skali i przyczyn, Security Manager musi mieć możliwość zbierania i analizowania danych.

Przy absolutnie minimalistycznym założeniu, że w średniej wielkości sklepie zainstalowano system składający się z 10 kamer CCTV, to w przypadku sieci handlowej liczącej takich sklepów np. 100 dział bezpieczeństwa, o ile istnieje, musi zapewnić sprawny nadzór nad pracą 1000 kamer. Na szczęście dla wielu rodzimych firm handlowych działy bezpieczeństwa są oczywistym elementem organizacji firm. W wielu, ale nie we wszystkich.

Coraz doskonalsze metody liczenia strat powodują, że w związku z tym pojawiają się większe oczekiwania w stosunku do działów bezpieczeństwa. Technologie security są bowiem tak zaawansowane, że umożliwiają m.in. wykorzystanie ich do wspomagania zarządzania gospodarką magazynową, nadzoru pracy osób obsługujących kasy, przestrzegania zasad BHP czy ogólnie jakości pracy zespołu. Do tego dochodzi sfera nadzoru nad łańcuchem dostaw (kontrola i terminowość oraz warunki dostaw w transporcie), która uzupełnia całą paletę czynników kontrolnych do maksymalizacji i efektywności biznesowej. Jakie jest rozwiązanie dla nowo powstających potrzeb?

W niektórych dużych firmach handlowych i oczywiście tych z branży TSL również powstają odrębne działy, których zadaniem jest sprawowanie maksymalnie ścisłej kontroli wszędzie tam, gdzie jest możliwe opomiarowanie procesu. Mowa o Control Tower.

Czym dokładnie jest Control Tower (wieża kontrolna)? Analogia do wieży kontrolnej nadzorującej ruch lotniczy jest nieprzypadkowa. Również w tym wypadku chodzi o to, by firmowa wieża kontrolna zapewniała pełen wgląd w procesy zachodzące w organizacji. Różnica jest taka, że biznesowa wieża kontrolna to zazwyczaj zestaw aplikacji dających ludziom z nich korzystającym nadzór nad konkretnymi procesami firmowymi. Jakie ma możliwości i do czego przede wszystkim jest wykorzystywana? W zasadzie można mówić o trzech głównych zadaniach:

- **Planowanie zamówień w czasie rzeczywistym**. Aby poprawić poziom obsługi klienta, wieża kontrolna powinna przechwytywać i wykorzystywać w czasie rzeczywistym dane dotyczące czasu dostawy, stanu zapasów i kosztów transportu. Dzięki temu zawsze można wybrać najlepszy i najbardziej opłacalny sposób dostawy.
- **Zarządzanie wyjątkami.** Wieża kontrolna powinna koncentrować się na konsekwentnym dostarczaniu zamówień poprzez

» Coraz doskonalsze metody liczenia strat powodują, że pojawiają się większe oczekiwania w stosunku do działów bezpieczeństwa. Technologie security są bowiem tak zaawansowane, że umożliwiają m.in. wykorzystanie ich do wspomagania zarządzania gospodarką magazynową, nadzoru pracy osób obsługujących kasy, przestrzegania zasad BHP czy ogólnie jakości pracy zespołu. «

> *» Integrowanie zasobów i technologii z zakresu SSP, KD, CCTV, SSWiN, DSO, systemów sterowania wentylacją i oddymianiem w jedno narzędzie zarządzające staje się rozwiązaniem najkorzystniejszym pod względem kosztów. «*

śledzenie łańcucha dostaw i wysyłanie alertów, gdy pojawią się problemy. Co ważniejsze, rozwiązanie powinno umożliwiać podejmowanie działań bezpośrednio w aplikacji.

- **Szczegółowy widok.** Oprócz śledzenia łańcucha dostaw wieża kontrolna może zapewniać wgląd w szczegóły każdego zamówienia, aby skutecznie zrealizować każdy wymagany element.

Stosowane w firmach systemy, które można nazwać wieżami kontrolnymi, dotyczą najczęściej dwóch obszarów, na których koncentruje się kadra zarządzająca. Są to:

- **Transport**, czyli pełen wgląd w przesyłki przychodzące i wychodzące, śledzenie trasy, wydatki z tym związane, czas dostaw itp. Ze względu na ich skoncentrowanie na transporcie są one zwykle dodatkiem do systemu zarządzania transportem i w związku z tym nie dają wglądu w inne elementy łańcucha dostaw.
- **Łańcuch dostaw,** systemy zbierają i analizują dane z całego łańcucha dostaw obejmującego często wiele przedsiębiorstw. Informacje dotyczą zamówień, sprzedaży, zakupów, poziomu zapasów własnych i od dostawców, produkcję oraz konserwację i naprawy. Oferując kompleksowy wgląd we wszystkie elementy łańcucha dostaw i kontrolę w aplikacji, zapewniają wszechstronną współpracę firmy z jej dostawcami i partnerami.

W przypadku handlu aplikacje funkcjonujące w ramach wieży kontrolnej powinny być wyposażone także w funkcje analizy obrazu. Niezwykle istotne jest stałe monitorowanie funkcji zarządzania obiektem tak, aby maksymalnie kontrolować koszty energii elektrycznej, ogrzewania, działania klimatyzacji oraz systemów ppoż. i innych kluczowych dla funkcjonowania obiektu. A praca na dużych

zbiorach danych *(big data)* powoduje konieczność dynamicznej analizy ryzyka w warunkach zbliżających biznes do stosowania AI. Z perspektywy realizacji polityki bezpieczeństwa i odporności handel jest wybitnie wrażliwym i trudnym biznesem. Wyzwaniem jest nie tylko zapobieganie kradzieżom. Duże skupiska ludzi, jakimi często są sklepy, to atrakcyjny cel ataku dla różnej maści przestępców i terrorystów.

Cyberprzestępcy atakują

Każdy sklep, niezależnie od swojej wielkości i rodzaju asortymentu, może stanowić łakomy kąsek dla przestępców ze względu na atrakcyjne towary na półkach czy gotówkę w kasie. Większość sklepów zbiera mnóstwo danych dotyczących płatności i osobowych klientów, sprzedawcy detaliczni będą w dalszym ciągu przyciągać uwagę wyrafinowanych atakujących. Cyberbezpieczeństwo musi zawsze być najwyższym priorytetem dla sprzedawców, jeśli chcą uniknąć cyberataku, zapobiec niezamierzonemu ujawnieniu i chronić ogromną ilość posiadanych danych klientów. Poniżej kilka przykładów ataków na obiekty handlowe w Stanach Zjednoczonych oraz ich konsekwencji:

- Cyberatak przeprowadzony w 2013 r. na sieć Target spowodował wyciek danych ok. 70 mln klientów i 41 mln kart płatniczych. Atak typu *spear phishing* skupiał się na zewnętrznym dostawcy i miał na celu kradzież danych uwierzytelniających użytkowników. Gdy zostały złamane zabezpieczenia sieci Target, w ciągu dwóch miesięcy złośliwe oprogramowanie przejęło dane klientów. W konsekwencji pracę stracił dyrektor Target, a firma zapłaciła grzywnę w łącznej wysokości 18,5 mln USD. Cały atak kosztował firmę ok. 290 mln USD.
- Korzystając z danych logowania zewnętrznego dostawcy, napastnicy uzyskali dostęp do sieci Home Depot, a następnie zainstalowali złośliwe oprogramowanie zaprojektowane w celu infekowania systemu POS, zbierając informacje o płatnościach klientów. W okresie od kwietnia do września 2014 r. przestępcy pozyskali dane 52 mln klientów. Home Depot zapłacił 17,5 mln USD w celu uregulowania roszczeń w całym kraju. To był jednak tylko ułamek całkowitych kosztów. Firma odnotowała wydatki przed opodatkowaniem w wysokości 198 mln USD związane z naruszeniem i późniejszymi postępowaniami sądowymi prowadzonymi przez klientów, wystawców kart płatniczych i instytucje finansowe przed ugodą.
- We wrześniu 2021 r. firma Neiman Marcus powiadomiła 4,6 mln klientów, że w maju 2020 r. haker włamał się na konta internetowe, uzyskując dostęp do danych osobowych, takich jak nazwy użytkowników i hasła, nazwy klientów, dane kontaktowe, numery kart kredytowych, a także daty ważności i numery kart wirtualnych.
- W 2021 r. audyt cyberbezpieczeństwa wykazał, że ogromna, błędnie skonfigurowana baza danych zawierająca ponad miliard rekordów, w tym adresy e-mail klientów, identyfikatory użytkowników i informacje o wyszukiwaniu klientów online zebrane w witrynach CVS Health i CVS.com, jest publicznie dostępna i niezabezpieczona.
- Nazwy użytkowników, adresy e-mail i zaszyfrowane hasła ok. 150 mln użytkowników MyFitnessPass firmy Under Armour zostały naruszone, gdy w lutym 2018 r. nieupoważniona osoba trzecia uzyskała dostęp do danych. Firma odkryła naruszenie dopiero miesiąc później.

SuperPower Control Tower – serwis na miarę potrzeb

Przedstawiony wcześniej obraz należy uzupełnić o sferę zarządzania funkcjami budynkowymi w celu spełnienia wymagań klimatycznych stawianych przez polityki państwowe i unijne. Efektywne i dostosowane do potrzeb zużycie energii i jej sterowanie poprzez używanie funkcji zbliżonych do BMS nie jest już wyborem z kategorii ciekawostki, ale koniecznością. Liczenie śladu węglowego wraz z precyzyjnym raportowaniem wyników wymaga dostępu do technologii, które mają zdolność integrowania różnych systemów automatyki budynkowej oraz technologii bezpieczeństwa. Integrowanie zasobów i technologii z zakresu SSP, KD, CCTV, SSWiN, DSO, systemów sterowania wentylacją i oddymianiem w jedno narzędzie zarządzające staje się rozwiązaniem najkorzystniejszym pod względem kosztów.

Tego typu rozwiązania oraz zbudowanie wokół nich dużego wielozadaniowego Centrum Zarządzania czy Control Tower jest i będzie ofertą dla ogromnego rynku usługobiorców, jakim jest polski rodzinny sektor handlu. Możliwości, jakie będzie dawało AI, wymusi pobieranie i dokładne analizowanie danych dotyczących bezpieczeństwa obiektów oraz wszelkich innych aspektów zarządzania obiektami.

Obecnie dostępne na rynku rozwiązania w okresie przejściowym pozwalają uniknąć nadmiernych inwestycji w *hardware* i skupić się na rozwiązaniach integracyjnych. Dodatkowym benefitem jest możliwość zlecenia monitorowania całego procesu zewnętrznym wyspecjalizowanym podmiotom, czego efektem będzie kupowanie wyłącznie danych niezbędnych do zarządzania bezpieczeństwem i funkcjami budynku. Przez okres przejściowy rozumie się tutaj moment, w którym de facto jesteśmy.

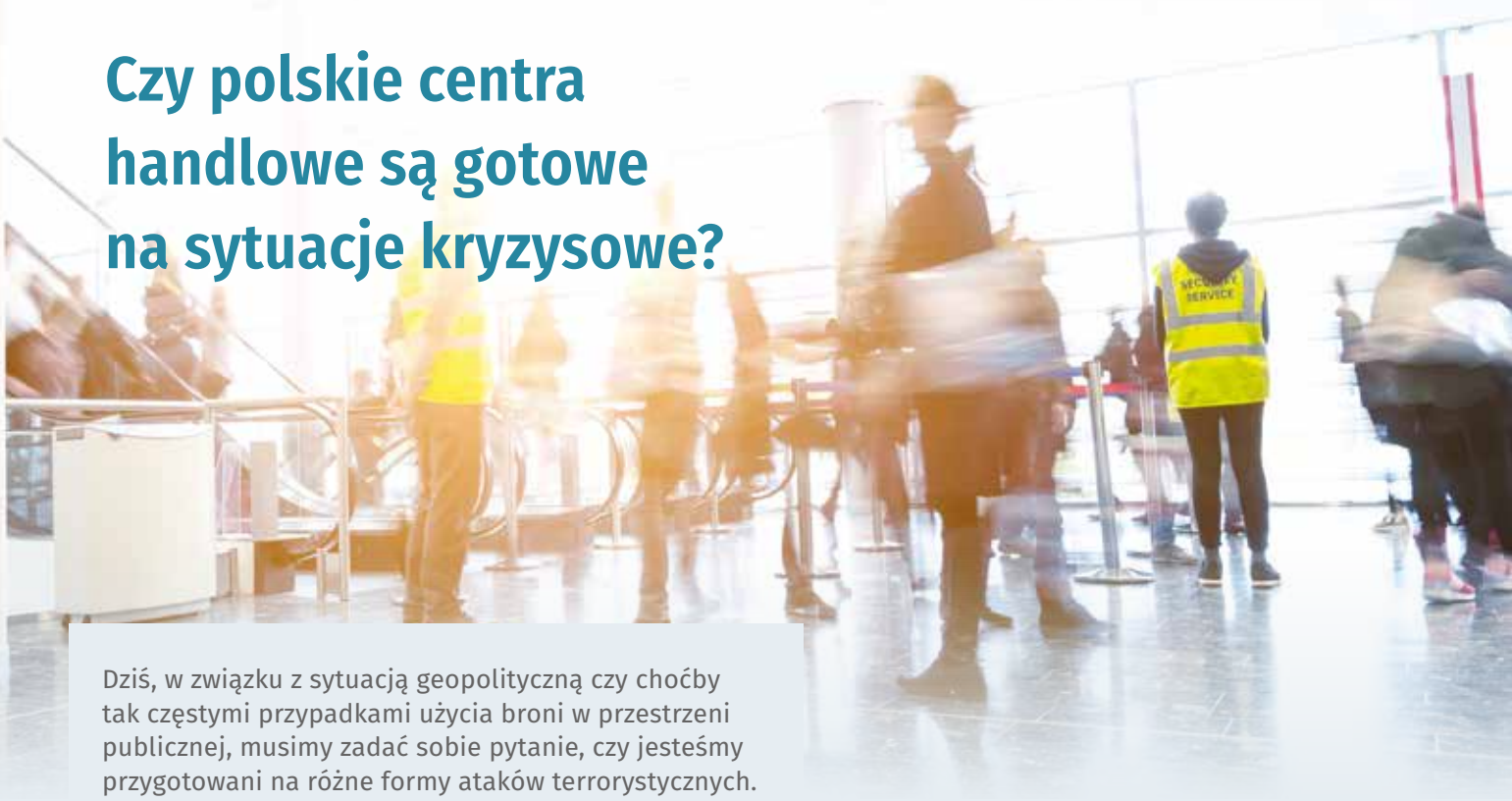
Dynamiczny rozwój AI, a także konieczność wdrożenia dodatkowych zabezpieczeń w zakresie cybersecurity spowoduje niebawem wejście na rynek nowych generacji systemów zarządzania budynkiem, w tym bezpieczeństwem. Wszystko w znacznie podwyższonych warunkach cyberbezpieczeństwa.

Polski sektor handlu to ogromny rynek dla dostawców rozwiązań, które w obecnej sytuacji stanowią faktyczny *game changer.* Oczywiście zagraniczne sieci handlowe są w podobnej sytuacji, również mają możliwość skorzystania z benefitów rewolucji technologicznej, ale to polski rodzinny biznes ma znaczącą przewagę ilościową i walor skali oraz dużych liczb. Oby te cechy stały się jednym ze źródeł sukcesu. Branża zabezpieczeń ma szansę odegrać znaczącą rolę w realizacji strategii wypracowania przewag konkurencyjnych w swoich obszarze, m.in. elastycznością i możliwością szybkiego podejmowania decyzji. Niemała jest tutaj rola osób zajmujących się w tych firmach bezpieczeństwem lub zarządzaniem nieruchomościami. ●

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.

Czy polskie centra handlowe są gotowe na sytuacje kryzysowe?



Dziś, w związku z sytuacją geopolityczną czy choćby tak częstymi przypadkami użycia broni w przestrzeni publicznej, musimy zadać sobie pytanie, czy jesteśmy przygotowani na różne formy ataków terrorystycznych.

Każda osoba związana z branżą security zna zasady i wytyczne ABW dotyczące takich ataków. Ale czy te zasady i wytyczne przekładają się na umiejętności praktyczne? Czy w ślad za wiedzą poszło dostosowanie procedur lub szkolenie struktur ochrony, a może przygotowanie scenariuszy i opracowanie dobrych praktyk? Z przykrością stwierdzam, że nadal panuje przekonanie, iż rzeczy przemilczane nie występują. Tymczasem zaangażowanie Polski w misje stabilizacyjne i pokojowe oraz jasna polityka zagraniczna powodują, że nasz kraj może znaleźć się na celowniku terrorystów. Nie możemy więc zakładać, że jesteśmy pod tym kątem bezpieczni.

Znane przypadki

W kraju już kilka razy doszło do ataków terrorystycznych, bo za takie należy uznać np. atak z użyciem noża lub maczety, wjazd do lokalu pojazdem czy wysadzenie budynku za pomocą butli z gazem. Działają jednak służby, które do tej pory skutecznie przeciwdziałały większym zdarzeniom o charakterze terrorystycznym. Mamy też infrastrukturę, która może być narażona na takie ataki, i nie chodzi tylko o metro, lecz także duże centra handlowe, które znów, po okresie pandemii, są pełne ludzi.

Należy pamiętać, że celem terrorystów jest wywołanie zniszczeń i wzbudzenie jak największego strachu, ale minimalnym kosztem. Idealnym tego przykładem jest np. atak „samotnego wilka". Większość bezpieczników zna zasady przekazywane przez ABW i docenia intensywną kampanię z 2021 r. promującą wiedzę dotyczącą tych zasad. Ale co z tym zrobiliśmy?

Niestety, w wielu przypadkach nadal jest stosowana procedura ewakuacji, która dotyczy wydarzeń związanych z uruchomieniem systemów przeciwpożarowych. W przypadku ataku terrorystycznego ta procedura wręcz zagraża bezpieczeństwu ludzi. Grupa terrorystyczna może przecież zaplanować atak na wyjścia ewakuacyjne, gdzie w przypadku paniki wywołanej pierwszymi strzałami pobiegną klienci galerii handlowej, wpadając wprost pod lufy terrorystów.

Jak przygotować się na atak terrorystyczny?

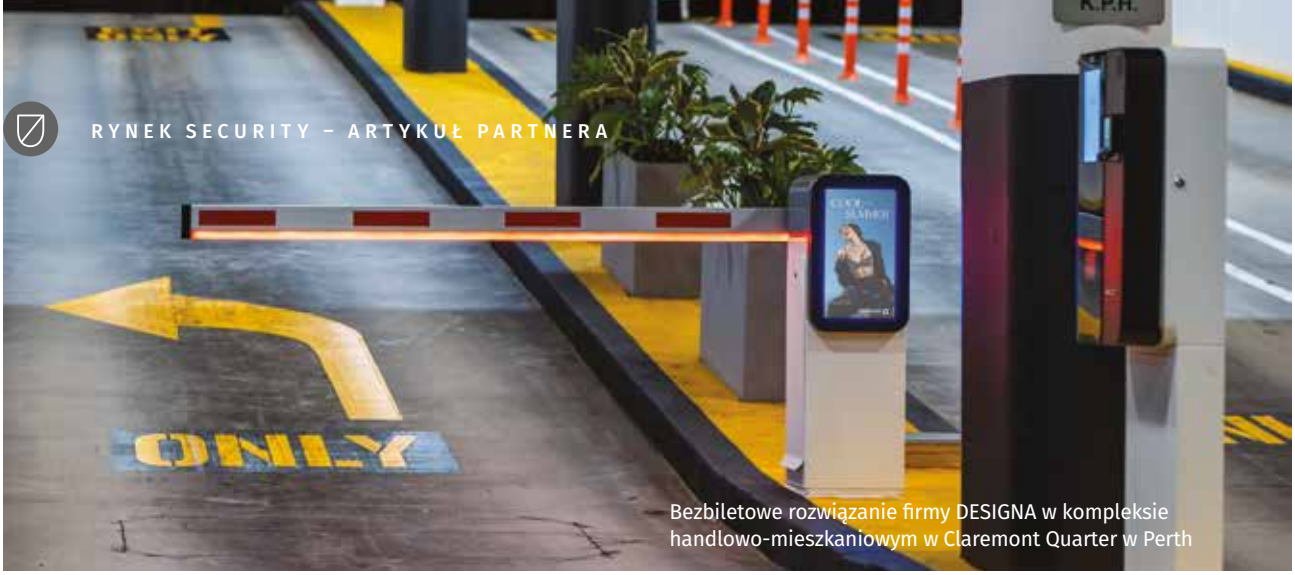
Tylko dobrze wyszkolone służby ochrony znające budynek i mające nawyki wyćwiczone podczas symulacji takich działań są w stanie ograniczyć liczbę ofiar, wykorzystując takie elementy jak grodzie ppoż., odpowiednie komunikaty głosowe czy bezpośrednie zarządzanie personelem ochrony i kierowanie ludzi do stref bezpiecznych. Wprawdzie mamy w strukturach państwa świetnie wyszkolone oddziały antyterrorystyczne, ale nie znają one każdego centrum handlowego. Ćwiczą w kilku największych i te znają, a tego typu budynków są setki.

Rekomendowanym rozwiązaniem omawianym w wielu organizacjach zajmujących się bezpieczeństwem jest wprowadzenie pakietów bezpieczeństwa umieszczonych na zewnątrz budynków w specjalnych skrytkach dostępnych dla służb specjalnych. Taki pakiet powinien zawierać aktualne plany budynku, środki łączności, hasła uwierzytelniające oraz – ze względu na fakt, że mamy nowe systemy IP – hasła dostępu do kamer. To może znacznie poprawić bezpieczeństwo i zminimalizować straty.

Nie ma regulacji prawnych, ale nic nie stoi na przeszkodzie, by wprowadzić taką praktykę, bo to, że coś dotychczas się nie wydarzyło, nie oznacza, że już nigdy się nie wydarzy. ●

Mirosław Lukowski

Ekspert w dziedzinie bezpieczeństwa handlu. Od 20 lat związany z branżą security. W latach 2017 -2019 krajowy koordynator w Dziale Ryzyka Prewencji i Ochrony Sieci Carrefour Polska. Dziś właściciel firmy Global Safe Development Technology.



Bezbiletowe rozwiązanie firmy DESIGNA w kompleksie handlowo-mieszkaniowym w Claremont Quarter w Perth

Rewolucja w zarządzaniu parkingami: bezbiletowa przyszłość

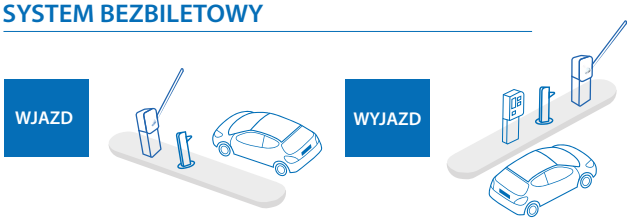
Elastyczność staje się słowem kluczowym kształtującym społeczeństwa, w tym branżę parkingową. Nowe technologie i indywidualne oczekiwania stawiają różnorodne wyzwania przed producentami systemów parkingowych.

Bycie liderem i kształtowanie trendów staje się coraz większym wyzwaniem. DESIGNA, działając od ponad 70 lat, wyznacza kierunki rozwoju systemów parkingowych. Firma zdefiniowała kluczowe trendy w zarządzaniu parkingami:

- elastyczność i zdolności adaptacyjne,
- przewidywanie oczekiwań; planując teraźniejszość, należy uwzględniać wymagania przyszłości,
- systemy bezbiletowe.

Dzięki systemowi bezbiletowemu przestaje być potrzebny bilet papierowy. Rozwiązanie to przynosi wiele korzyści zarówno dla zarządców parkingów, jak i dla odwiedzających. Utrata biletu parkingowego już nie jest problemem. Oszczędza się papier i nie generuje kosztów związanych z wydrukiem, a także skraca czas wjazdu na parking, ponieważ nie trzeba pobierać biletu. Dodatkowym atutem jest mniejsze zaangażowanie podzespołów mechanicznych. Celem DESIGNA jest bezstresowe korzystanie z obiektów parkingowych.

SYSTEM BEZBILETOWY



SYSTEM BEZBILETOWY
ZE SWOBODNYM WJAZDEM

Jak działa system bezbiletowy Ticketless?

Zintegrowany system rozpoznawania tablic rejestracyjnych (LPR) służy zarówno do rozpoznawania wjeżdżających i wyjeżdżających pojazdów, jak i do dokonywania płatności. To rozwiązanie eliminuje kłopoty z biletami papierowymi, zapewniając bezproblemowe, komfortowe korzystanie z parkingu.

Najnowsza instalacja bezbiletowego rozwiązania firmy DESIGNA została uruchomiona w kompleksie handlowo-mieszkaniowym w Claremont Quarter, w Perth w Australii. Monitorowana w okresach szczytu wydajność systemu wykazała, że czas od rozpoznania pojazdu do rozpoczęcia otwierania szlabanu został skrócony do 1100 milisekund. Koniec z korkami na wjeździe!

Rozwiązania przyszłości

Tylko niektóre parkingi są gotowe, by przejść na system całkowicie bezbiletowy. Jednak już dziś przyszłość należy do rozwiązań hybrydowych płynnie łączących nowoczesne technologie z tradycyjnymi.

W przypadku rozwiązań hybrydowych kierowcy mogą bez problemu wjeżdżać na parking, płacić i wyjeżdżać z parkingu z biletem lub bez. Tryb hybrydowy jest idealnym etapem ułatwiającym wdrożenie systemu całkowicie bezbiletowego. Ponieważ oba tryby są już zainstalowane, dezaktywacja opcji papierowego biletu nie stanowi problemu. Kiedy nadejdzie odpowiedni czas, płynne przejście na pełny system Ticketless będzie łatwiejsze, bez konieczności instalowania nowych urządzeń!

Najlepszym przykładem zastosowania tego rozwiązania jest duży kompleks handlowy Mammut Mall w Budapeszcie, którego zarząd, decydując się na aktualizację struktury parkingowej, wybrał płynne przejście na system bezbiletowy i zainstalował hybrydowy system dla 1000 miejsc parkingowych. Na 16 liniach wjazdowo-wyjazdowych i parkingu o łącznej powierzchni blisko 25 000 mkw. urządzenia i oprogramowanie dostarczone przez DESIGNA zaspokajają wszystkie potrzeby użytkowników: system biletowy, system bezbiletowy, awizacje dostaw, wszystkie rodzaje płatności: gotówka, karta, kupon z kodem QR. **DESIGNA ma rozwiązania dla wszystkich!** ●

DESIGNA AXESS POLSKA Sp. z o.o.
Plac Konesera 12, 03-736 Warszawa
https://designa.com/
e-mail: Konrad.Jaworski@designa.com

Pomagamy sprzedawcom detalicznym zwiększyć wydajność i rentowność

O najnowszych rozwiązaniach Checkpoint Systems oferujących najwyższą ochronę produktów w sklepach opowiada Mariano Tudela, wiceprezes ds. sprzedaży MAS Worldwide.

Identyfikacja towarów za pomocą RFID umożliwia firmom z sektora detalicznego lepszą obsługę klienta, zapewnia ochronę produktów i jednocześnie pozwala osiągnąć zrównoważony rozwój.

Checkpoint Systems jest światowym liderem w dostarczaniu rozwiązań w zakresie elektronicznego systemu antykradzieżowego EAS i technologii RFID dla wielu sektorów: od branży fashion, poprzez artykuły spożywcze, elektronikę czy kosmetyki, po branżę ogólnobudowlaną. Zabezpiecza też łańcuchy dostaw.

Dzięki ekosystemowi rozwiązań, na które składają się nowatorskie oprogramowanie, sprzęt, etykiety i znaczniki oraz łączące je rozwiązania oparte na chmurze, Checkpoint oferuje możliwość monitorowania produktów od momentu produkcji aż do ich ekspozycji na półkach sklepowych. Co więcej, te same rozwiązania zapewniają jednocześnie ochronę przeciwkradzieżową nie tylko w sklepie, ale także w całym łańcuchu dostaw.

Checkpoint Systems to firma wizjonerska, która chroni sklepy detaliczne niewidzialną tarczą. Nasze wyjątkowe rozwiązania zapewniają równowagę między ochroną a wizualnym merchandisingiem. Pozwalają w pełni zachować atrakcyjny wystrój sklepów bez ingerencji w jego zmianę i – co najważniejsze – bez uszczerbku dla poziomu bezpieczeństwa.

Doskonała ochrona bez wpływu na wystrój sklepu i wizualny merchandising

Dzięki ponad 50-letniemu doświadczeniu w technologii częstotliwości radiowych Checkpoint opracował wiele rozwiązań oferujących najwyższą ochronę produktów w sklepach bez wpływu na ich wizualny wystrój. Jednym z nich jest SFERO™ – w pełni konfigurowalny, modułowy system zapobiegania stratom, bazujący na technologii RFID. Testy Checkpoint wykazały, że system daje wysoki odsetek wykrycia prób kradzieży, który w wielu przypadkach przekracza 95%! Pozwala sprzedawcom detalicznym chronić produkty, tym samym zmniejszając straty i maksymalizując przychody.

Kluczową cechą rozwiązań SFERO™ jest możliwość ich pełnej adaptacji do każdego układu i projektu sklepu. Za pomocą inteligentnych anten stojących i podwieszanych (np. montowanych pod sufitem) sprzedawcy tworzą strefy ochrony, które można w pełni dostosować do specyficznych wymagań każdej placówki. System obejmuje pas 10 m wzdłuż wejścia do sklepu oraz do 3,5 m nad głowami klientów i jest niewidoczny. Kolejną zaletą SFERO i technologii RFID jest możliwość wykorzystania ich do monitorowania stanów magazynowych oraz zautomatyzowanej kontroli zapasów w placówkach.

Podobnie rozwiązanie – Checkpoint NEO™ – oferuje najbardziej zaawansowaną gamę anten elektronicznego systemu antykradzieżowego EAS, łącząc estetyczny wygląd ze zwiększoną wydajnością serii NEO™. Seria ta charakteryzuje się zintegrowaną łącznością bezprzewodową i mniejszą liczbą niezbędnych kabli, co upraszcza instalację. Dzięki zwiększonemu zasięgowi wykrywania do 2,7 m mogą być objęte ochroną szersze przejścia i wejścia. Z kolei innowacyjne

konstrukcje, takie jak wielokrotnie nagradzany system NS40, zapewniają lepszą ochronę na linii kas, ostrzegając personel o potencjalnych próbach kradzieży.

Ochrona, której potrzebują sklepy

Rozwiązania Checkpoint stały się synonimem najlepszych w swojej klasie rozwiązań RFID. Interesującym przykładem jest UNO™ – jedna z wiodących na rynku etykiet zabezpieczających, łącząca technologie RFID i RF dual. Stosowana przez największych europejskich detalistów UNO™ może być wykorzystywana do kontrolowania zapasów magazynowych, zwrotów produktów i prywatności danych.

W erze definiowanej przez szybki postęp technologiczny i zmieniające się oczekiwania klientów mające wszystkie funkcje RFID i RF rozwiązanie UNO™ służące do zapobiegania stratom jest przykładem innowacji i wydajności w branży detalicznej. To najlepsza propozycja dla sprzedawców, którzy już zainwestowali w sprzęt RF do zapobiegania stratom, chcącym stopniowo migrować do technologii RFID. UNO™ pozwala połączyć istniejące funkcje zapobiegania stratom i zarządzania zapasami w jednej aplikacji. Oszczędności pojawiają się bardzo szybko – sprzedawcy mogą wyeliminować tradycyjne zabezpieczenia wielokrotnego użytku oraz konieczność ich zakładania i usuwania przez personel sklepu.

Checkpoint oferuje również specjalistyczne przeźroczyste etykiety, takie jak Shield Tag, chroniące towary przed kradzieżą, bez wpływu na wygląd produktu. Mocny klej i specjalnie zaprojektowany wykrój uniemożliwiają usunięcie etykiety. Korzystając z Shield Tag, sprzedawcy detaliczni mogą zapobiegać kradzieżom i zwalczać zorganizowane grupy przestępczości detalicznej, ponieważ tego typu etykiety w znacznym stopniu utrudniają sprzedaż skradzionych przedmiotów.

Pełna kontrola jakości wszystkich elementów

Każdy sklep wdrażający system rozwiązań RFID potrzebuje trzech elementów: sprzętu, oprogramowania oraz tagów lub etykiet. Checkpoint dostarcza je, gwarantując ich najwyższą jakość.

Przyniosło to korzyści wielu prestiżowym klientom na całym świecie. Przykładem może być polska firma LPP mająca ponad 2000 sklepów, trzy centra dystrybucyjne i cztery magazyny e-commerce, która już w 2018 r. zainwestowała w rozwiązania RFID nowej generacji, a pierwszy sklep wyposażony w tę technologię uruchomiła rok później. W roku 2020 LPP wdrożyła rozwiązania RFID w całym łańcuchu dostaw. Szybko okazały się one kluczowe dla strategii zarządzania zmianą.

Firma LPP odkryła, że RFID jest kluczem do sprzedaży wielokanałowej, a technologia dostarczona przez Checkpoint pomaga monitorować zapasy i towary, poprawiając ich widoczność w sali sprzedaży i dokładność stanów magazynowych.

Cyfrowe etykiety nowej generacji

Checkpoint zdaje sobie sprawę z tego, że połączenie trudnych czynników ekonomicznych i coraz bardziej świadomych konsumentów zmusza marki do większego dbania o wizerunek. Kupujący chcą wiedzieć, gdzie, kiedy i jak produkt został wyprodukowany. Dla przykładu, w przypadku wina i napojów spirytusowych sprzęt i oprogramowanie oparte na technologii RFID przechwytują dane z etykiet umieszczonych na butelkach i skrzynkach, aby monitorować każdą jednostkę SKU i całą przesyłkę podczas łańcucha dostaw. Inteligentne etykiety Checkpoint, opracowane z myślą o rynkach wina, alkoholi i perfum, pokazują drogę produktu:

od miejsca pochodzenia (takiego jak winnica) po półki sklepowe, dostarczając wszystkie informacje potrzebne do celów kontroli jakości.

Innowacyjny i wydajny jak Checkpoint

Wymagania dotyczące tego, by firmy umieszczały etykiety RFID na swoich produktach już na etapie produkcji, pomagają producentom lepiej zrozumieć, że ich inwestycja w znakowanie u źródła przynosi korzyści sieciom sklepów. Checkpoint prowadzi już rozmowy z marką prowadzącą prawie 300 sklepów w całej Europie. Jej celem było uruchomienie nowego oprogramowania do zarządzania zapasami bazującego na RFID, czyli ItemOptix™, które jest łatwe do wdrożenia, użytkowania i adaptacji. Ta ulepszona wersja rozwiązania SaaS RFID dostarcza szczegółowych informacji o liczbie poszczególnych produktów w sklepach detalicznych, magazynach, centrach dystrybucji i sklepie online. Kompleksowa wiedza o zapasach może zwiększyć sprzedaż o 4%, dokładność inwentaryzacji o 99%, redukcję niedostępnych towarów o 90% i redukcję kosztów inwentaryzacji o 75%.

W erze zdefiniowanej przez szybki postęp technologiczny i zmieniające się oczekiwania klientów jesteśmy przykładem firmy innowacyjnej, zapewniającej wydajność branży detalicznej.

Checkpoint łączy najnowocześniejsze technologie i rozwiązania, wpływając na kształtowanie handlu detalicznego, co pozwala firmom rozwijać się w dynamicznie zmieniającej się sytuacji na rynku. ●

Checkpoint Systems
ul. L. Idzikowskiego 16, 00-710 Warszawa
checkpointsystems.com/pl/
biuro@checkpt.com

Przyszłość śledzenia przesyłek: inwestycja w nowoczesne rozwiązania

W zglobalizowanym świecie, gdzie tempo prowadzenia biznesu nieustannie rośnie, wyzwania logistyczne stają się coraz bardziej skomplikowane. Dyrektorzy centrów dystrybucyjnych muszą nie tylko zarządzać bieżącymi operacjami, ale także przewidywać potencjalne problemy i inwestować w technologie, które pozwolą im pozostać krok przed konkurencją. Jedną z takich technologii jest innowacyjne rozwiązanie śledzenia przesyłek Hikvision, które zmienia sposób, w jaki firmy zarządzają swoimi zasobami i logistyką.

Bartłomiej Skórski

Hikvision, lider w dziedzinie rozwiązań bezpieczeństwa i monitoringu, przedstawia nowe podejście do logistyki, oferując rozwiązanie do śledzenia przesyłek łączące istniejące systemy zarządzania magazynem z zaawansowanymi systemami wizyjnymi. To synergiczne połączenie umożliwia operatorom nie tylko śledzenie przesyłek w czasie rzeczywistym, ale także pozwala im na scentralizowany wgląd we wszystkie operacje logistyczne.

Gdy każda minuta jest bezcenna

Opóźnienia w dostawach, utrata przesyłki lub jej uszkodzenie, błędy w zarządzaniu zapasami – wszystkie te problemy przekładają się na zwiększone koszty operacyjne firmy i niezadowolenie klientów. Zintegrowane rozwiązanie Hikvision pozwala na szybkie identyfikowanie i rozwiązywanie tych kwestii, co znacząco skraca czas

potrzebny na zarządzanie incydentami i redukuje koszty związane z utratą lub uszkodzeniem towaru. Ponadto analiza w czasie rzeczywistym oferowana przez system pozwala na proaktywne zarządzanie operacjami, a to z kolei może przynieść w dłuższym okresie znaczące oszczędności.

Zadowolenie klienta jest priorytetem dla każdego dyrektora centrum dystrybucyjnego. Tradycyjne problemy, takie jak opóźnienia w dostawach czy błędy w zamówieniach, mogą obniżyć wiarygodność firmy. Rozwiązanie Hikvision pozwala firmom zminimalizować te problemy, oferując przejrzysty system śledzenia przesyłek. Klienci na bieżąco otrzymują informacje o statusie swoich zamówień, co z kolei znacząco poprawia ich doświadczenie i zadowolenie. W dłuższej perspektywie przejrzystość i niezawodność dostaw zwiększają lojalność klientów i przyczyniają się do lepszych opinii o firmie, co jest nieocenione w budowaniu trwałych relacji z klientami i utrzymaniu pozycji lidera na rynku.

Inwestycja w nowoczesne technologie śledzenia przesyłek to strategiczny krok w kierunku uzyskania trwałej przewagi konkurencyjnej. Hikvision oferuje platformę, która nie tylko ułatwia zarządzanie operacjami logistycznymi, ale także pozwala na przewidywanie potencjalnych wyzwań i podjęcie błyskawicznej reakcji, zanim staną się one rzeczywistym problemem. Dzięki zaawansowanej analizie danych i możliwościom monitorowania w czasie rzeczywistym dyrektorzy centrów dystrybucyjnych mogą podejmować świadome decyzje, które przyspieszają operacje, zmniejszają ryzyko i prowadzą do znaczących oszczędności operacyjnych.

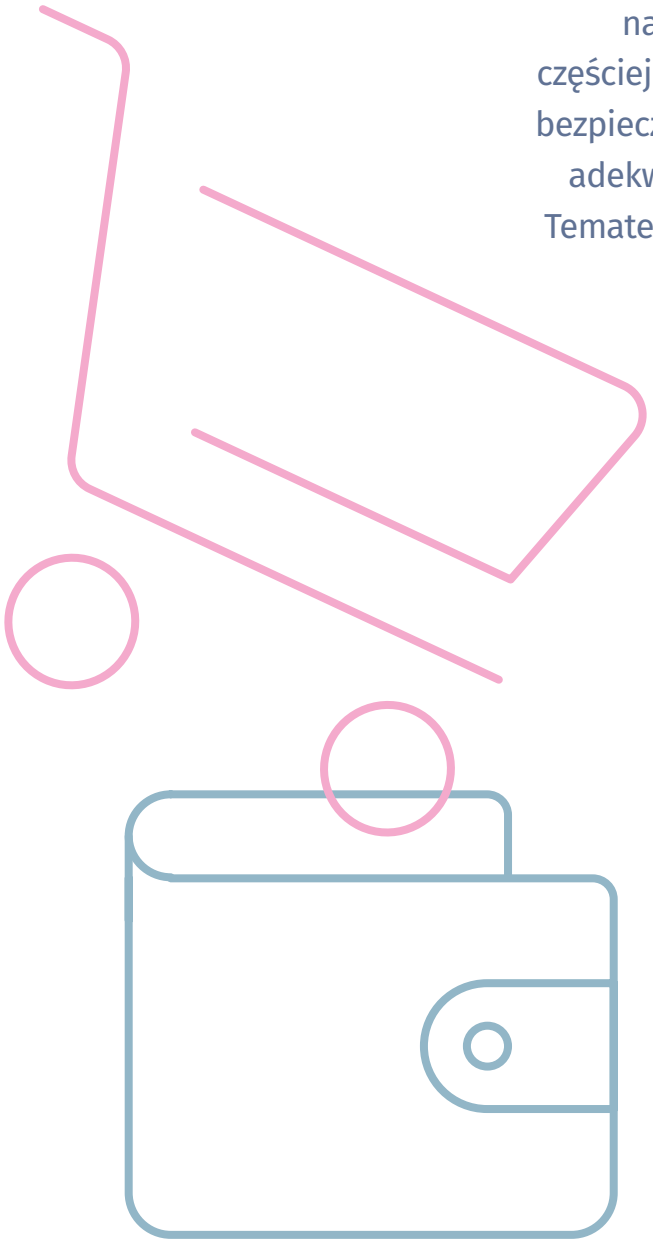
W świecie, gdzie czas to pieniądz, a zadowolenie klienta jest kluczem do sukcesu, inwestycja w zaawansowane rozwiązania śledzenia przesyłek oferowane przez Hikvision stanowi właściwy wybór dla firm, którym zależy na byciu liderem w dziedzinie logistyki. Przejrzystość, efektywność i innowacyjność to wartości, które każdy dyrektor logistyki powinien cenić. Hikvision dostarcza narzędzi, które przekształcają te wartości w realne rozwiązania, pomagając firmom osiągać cele biznesowe, jednocześnie przygotowując je do przyszłych wyzwań, które niesie ze sobą dynamicznie zmieniający się krajobraz branży logistycznej.

W erze cyfryzacji i rosnącej konkurencji wybór właściwych technologii może zdecydować o sukcesie lub porażce firmy, dlatego dyrektorzy centrów dystrybucyjnych, którzy patrzą w przyszłość, powinni rozważyć zainwestowanie w zaawansowane rozwiązania śledzenia przesyłek firmy Hikvision, aby pozostać na czele innowacji logistycznych i kontynuować dostarczanie wartości swoim klientom w coraz bardziej skomplikowanym świecie logistyki. ●

Hikvision Poland
ul. Żwirki i Wigury 16B, 02-092 Warszawa
Bartholomew.Skorski@hikvision.com
https://www.hikvision.com/europe/

głos branży

Ze względu na sytuację społeczno-ekonomiczną budżety na bezpieczeństwo w handlu detalicznym są coraz częściej ograniczane. To sprawia, że przed zespołami ds. bezpieczeństwa stoi nie lada wyzwanie – mają zapewnić adekwatny jego poziom przy ograniczonych środkach. Tematem dyskusji liderów jest wykorzystanie na ten cel inwestycji w najnowsze technologie.



Przemysław Borucki
TJX POLAND

Nieodzowna jest modernizacja technologiczna

W roku 1898 angielski polityk Joseph Chamberlain powiedział: „Zgodzicie się, że żyjemy w interesujących/ciekawych czasach (…)". Mimo że upłynęło 125 lat, sentencja wydaje się wciąż aktualna i, co więcej, oddaje ducha współczesnej rzeczywistości.

Lata dwudzieste XXI w. rozpoczęliśmy walką z pandemią COVID, wojną w Ukrainie oraz rosnącą inflacją. Wszystkie te czynniki mają ogromny wpływ na nastroje konsumenckie, ale też na widoczny wzrost przestępczości w handlu detalicznym (oficjalne statystyki policyjne wskazują na ponad 30-proc. wzrost). Podniesienie przez Sejm Rzeczypospolitej kwoty uznającej kradzież za przestępstwo do 800 zł zaczyna już się przekładać na zwiększoną aktywność przestępców w sklepach i w mojej opinii będzie skutkowało dalszym zwiększeniem poziomu strat.

Ta sytuacja stawia przed całą branżą security/Loss Prevention nowe wyzwania, aby nadążyć za aktualnymi potrzebami handlu. Działalność tego sektora w dużej mierze wciąż opiera się na pracy wykonywanej

przez ludzi. Wiążą się z tym dwa główne problemy – brak wyspecjalizowanej kadry na rynku pracy oraz narastające oczekiwania dotyczące wynagrodzenia (częściowo wynikające z podniesienia najniższej krajowej). Stoi to w dużej sprzeczności z oczekiwaniami firm, którym branża security świadczy usługi, ponieważ spadki po stronie sprzedaży, jak również zwiększone straty przekładają się na zmniejszenie budżetów na ochronę. Paradoks, który niestety jest rzeczywistością. Z drugiej strony oferta pracodawców z sektora ochrony często nie jest atrakcyjna dla pracowników, którzy znajdują ciekawsze możliwości (lepiej płatne) zatrudnienia w innych sektorach.

Szansą na poprawę sytuacji i zapewnienie kompromisu kosztowego jest modernizacja technologiczna obiektów chronionych. Inwestycje w systemy monitoringu wizyjnego, systemy przeciwkradzieżowe EAS oraz w rosnące możliwości w obszarze rozwiązań AI to absolutny *must have*. Oczywistym faktem jest, iż działania te wymagają odpowiednio wysokich nakładów inwestycyjnych, jednak w dalszej perspektywie to koszt, który się zwróci. Dużą rolą menedżerów do spraw bezpieczeństwa jest prowadzenie kampanii uświadamiającej i dostarczanie odpowiedniej wiedzy firmom z sektora handlowego.

Kierunek ten wydaje się nieuchronny i uzasadniony ze względu na rosnące koszty pracy, które stanowią znaczną część wynagrodzenia za usługi ochrony. Alternatywa w postaci korzystania z rozwiązań technologicznych staje się więc sposobem na powstrzymanie wzrostu kosztów i daje możliwość zabezpieczenia chronionych obiektów we właściwy sposób.

Łukasz Grzesik

BEZPIECZNYHANDEL.PL

Wzrasta problem kradzieży w sklepach

Negatywne skutki kradzieży są w sklepach coraz bardziej odczuwalne. Powstrzymanie tej tendencji jest jednym z największych wyzwań stojących dziś przed menedżerami bezpieczeństwa w handlu. Wiąże się to z realizacją szeregu powiązanych ze sobą działań. Jednym z nich jest wybór odpowiedniej strategii zapobiegania stratom. Kolejnym jest dobór narzędzi dopasowanych do tej realizacji.

Zakup odpowiedniej technologii nie stanowi dziś problemu. Większym wyzwaniem może okazać się jej obsługa ze względu na niedobór pracowników posiadających odpowiednie kompetencje cyfrowe. Nie bez znaczenia jest również wybór odpowiedniego partnera – firmy ochrony, która jest w stanie sprostać bieżącym wyzwaniom.

Idealnym kierunkiem jest posiadanie komplementarnego systemu ochrony, na który składają się m.in. elektroniczne systemy zabezpieczeń (takie jak monitoring wizyjny, system antykradzieżowy, system alarmowy) oraz ochrona fizyczna. Jednak tak rozbudowane rozwiązania nie zawsze kalkulują się detalistom. W takiej sytuacji warto wybrać te, które stosunkowo niewielkim kosztem mogą przynieść odpowiednie rezultaty.

Niemniej jednak należy zauważyć, że niezależnie od zastosowanych rozwiązań technicznych, a zwłaszcza gdy jest ich mało, ostatecznie na końcu pozostaje człowiek. Pracownik, niezależnie od tego, czy jest z firmy ochrony, czy jest pracownikiem sklepu, podejmuje decyzje i działania w odpowiedzi na zagrożenie.

Kluczowym wyzwaniem w tym momencie jest zapewnienie stosunkowo niskiej rotacji personelu, aby utrzymać wiedzę i praktykę na odpowiednim poziomie, a także działać konsekwentnie, by osiągnąć cel zapobiegania stratom.

Paweł Korzybski

POLSKI ZWIĄZEK PRACODAWCÓW OCHRONA

Ochrona fizyczna czy zabezpieczenia techniczne?

Trudno jednoznacznie wskazać, co odgrywa ważniejszą rolę w zabezpieczeniu sklepów przed kradzieżą – ochrona fizyczna czy technika. Z pełnym przekonaniem mogę natomiast stwierdzić, że jedno bez drugiego nie jest dziś w stanie osiągnąć pełnej skuteczności. Kluczem do sukcesu są rozwiązania hybrydowe, czyli mądre wykorzystanie wyszkolonego i dobrze opłaconego pracownika ochrony, który potrafi skutecznie używać technologii zastosowanej w obiekcie.

Znalezienie złotego środka jest kwestią indywidualną. Każdy klient musi odpowiedzieć sobie na pytania, na jakiej formie ochrony mu zależy i który model w jego przypadku sprawdzi się najlepiej (w wyborze odpowiedniego rozwiązania chętnie pomogą profesjonalne firmy z branży ochrony). Jednak nawet jeśli zdecyduje się on wykorzystać w większości zabezpieczenia techniczne (np. zaawansowany monitoring wraz z analityką obrazu, bramki antykradzieżowe), w naszej ocenie potrzebuje również pracownika ochrony, aby zapewnić pełne bezpieczeństwo klientów, obiektu i towaru. To właśnie ten pracownik, w sytuacji kradzieży, będzie w stanie schwytać złodzieja. Monitoring dostarczy oczywiście materiału dowodowego dla policji, lecz nie powstrzyma przestępcy przed wyniesieniem towaru ze sklepu.

Nowoczesne systemy zabezpieczeń znacząco zwiększają skuteczność ochrony, ale nie są w stanie zastąpić pracownika. Zauważamy, że w obiektach handlowych dochodzi do coraz większej liczby tzw. kradzieży zuchwałych, a przestępcy często testują skuteczność zabezpieczeń stosowanych w danej placówce. Jak pokazują statystyki, złodziej w pierwszej kolejności wynosi przedmioty o małej wartości, które w sytuacji zatrzymania narażą go jedynie na mandat karny. Jeśli kradzież się powiedzie, to w kolejnym kroku przestępca wróci po produkty znacznie droższe, kosztujące nawet kilkadziesiąt tysięcy złotych. Obecność pracownika ochrony w tej sytuacji nie tylko działa prewencyjnie, ale także pozwala wypełnić te luki, w których technologia niestety zawodzi.

Należy również pamiętać, że profesjonalny pracownik odpowiada za więcej czynności w obiekcie, niż na pierwszy rzut oka mogłoby się

→

wydawać. Pokażę to na przykładzie centrów handlowych. Pracownicy firm świadczących usługi ochrony zarówno powstrzymują złodziei czy agresorów, jak i wspierają działania ewakuacyjne, reagują odpowiednio na sygnały systemów ppoż., udzielają pierwszej pomocy przedmedycznej czy służą informacją klientom. Jeśli dochodzi do incydentu, np. na parkingu, pracownik ochrony asystuje uczestnikom zdarzenia – sporządza notatkę i zabezpiecza na wniosek stron materiał dowodowy w formie nagrań CCTV.

Czy kamera lub systemy zabezpieczeń wykonają te czynności lub będą ratować życie ludzkie w sytuacji zagrożenia? Być może w przyszłości – dziś jednak tak nie jest. W wielu przypadkach wiedza i doświadczenie pracowników ochrony zapobiegają eskalacji zdarzeń niepożądanych i niebezpiecznych.

Reasumując, proces ochrony ulega ciągłym zmianom głównie ze względu na szybki rozwój technologii. Z dużym prawdopodobieństwem mogę jednak stwierdzić, że jeszcze przez wiele lat skuteczna ochrona przed kradzieżą będzie opierać się na modelu hybrydowym – dobrze przeszkolonych i opłaconych pracownikach fizycznych i technice, która ich skutecznie wspiera.

Adam Kowalski
SECURITAS POLSKA

Przestępczość w centrach handlowych

W obiektach handlowych obserwujemy ostatnio nowy rodzaj przestępstw – udawanie przez złodziei manekinów na wystawach. Ten nietypowy sposób działania stanowi wyzwanie zarówno dla zarządców obiektów handlowych, jak i dla firm ochrony. Złodzieje doskonale dopasowują swój wygląd do aranżacji wystaw sklepowych, używają makijażu, dzięki czemu skutecznie wtapiają się w otoczenie.

Dodatkowym problemem dla pracowników ochrony jest uzasadniona obecności osoby na terenie sklepów. Przestępcy podszywają się pod obsługę sklepu, kurierów, pracowników serwisów technicznych. Mają wiedzę na temat standardowych zadań pracowników, zachowując się pewnie i wiarygodnie. Aby skutecznie przeciwdziałać tym nietypowym zagrożeniom, niezbędna jest prewencja obejmująca zwiększoną czujność ochrony, aktywną obserwację oraz raportowanie wszelkich podejrzanych zachowań.

Nowoczesne technologie stanowią istotne wsparcie w tych działaniach. Zaawansowane systemy monitoringu, oparte na kamerach o wysokiej rozdzielczości, wykorzystujące sztuczną inteligencję do analizy danych, są podstawowymi narzędziami prewencyjnymi. Ponadto systemy alarmowe i kontrola dostępu ograniczają możliwości złodziei, uniemożliwiając im dostęp do nieautoryzowanych obszarów. Regularne przeglądy procedur bezpieczeństwa oraz edukacja personelu sklepu również mają istotne znaczenie.

Przestępczość w centrach handlowych ewoluuje, a złodzieje opracowują różnorodne metody działania. Udawanie manekinów na wystawach sklepowych to tylko jedno z przykładów innowacyjnych technik. Współpraca między zarządcami centrów handlowych a firmami ochrony jest niezbędna, aby skutecznie przeciwdziałać temu zagrożeniu oraz zapewnić bezpieczeństwo klientom i pracownikom.

Bogumił Szymanek
AXIS COMMUNICATIONS

Priorytetem jest cyberbezpieczeństwo

Zasady cybersecurity w systemach telewizji dozorowej są kluczowe dla zapewnienia bezpieczeństwa i prywatności danych przesyłanych przez kamery, urządzenia sieciowe, serwery i oprogramowanie. W tym zakresie skupiamy się na przeciwdziałaniu. Dopuszczenie do złamania zabezpieczeń rodzi już poważne konsekwencje. W celu zminimalizowania ryzyka włamań, ataków i wycieku informacji przy wyborze komponentów systemu warto zapoznać się z podejściem dostawcy do zarządzania bezpieczeństwem w całym cyklu życia produktu.

Jakość jest dla nas priorytetem i zapewnienie bezpiecznych rozwiązań wynika z kultury organizacyjnej firmy. Biorąc odpowiedzialność za tworzony sprzęt i oprogramowanie, trzeba świadomie dobierać dostawców komponentów, przeprowadzać ciągłe testy i audyty oraz wdrażać najlepsze standardy, np. ISO 27001 czy IEC 62443.

Uważamy, że kwestie bezpieczeństwa powinny być uwzględniane od samego początku i przez cały proces rozwoju, nie tylko na końcu, czyli użytkowaniu. Aby stworzyć w pełni bezpieczny produkt i skutecznie zająć się cyberbezpieczeństwem, wdrożyliśmy metodologię działania na różnych etapach tworzenia oprogramowania. Celem jest zmniejszenie podatności na zagrożenia. Bardzo ważne jest również promowanie wiedzy na temat zasad cyberbezpieczeństwa i transparentność. Dlatego publikujemy przewodniki najlepszych praktyk dla wdrażanych systemów, informacje o wykrytych lukach zabezpieczeń i koniecznych aktualizacjach. Ponadto nasze urządzenia mają szereg funkcji sprzętowych i programowych zapobiegających cyberatakom. Spójność oprogramowania pozwala publikować tzw. SBOM i oferować jego utrzymanie przez wiele lat.

Artur Nowakowski
LINC POLSKA

Cyberbezpieczeństwo – dyrektywy i standardy

Podczas XXIV konferencji branży ochrony organizowanej przez Polską Izbę Ochrony miałem sposobność przeprowadzić wśród naszych partnerów krótką ankietę dotyczącą cyberbezpieczeństwa. Wyniki nie pozostawiają wątpliwości – prawie każdy z ankietowanych spotkał się z cyberatakiem, ale tylko 30% respondentów odpowiedziało, że ich zabezpieczenia są adekwatne do zagrożeń. Dlaczego? Powodów jest wiele, a niektóre z nich są banalne. Ludzie często nie zdają sobie sprawy ze źródeł zagrożenia, nie zastanawiają się nad codziennymi rutynowymi czynnościami, a teoretycznie każdy z nas może nieświadomie pomóc hakerowi dostać się do firmy lub domu. Nie tylko czynnik ludzki stanowi słabe ogniwo w tym łańcuchu, ale i systemy informatyczne nie są w pełni przygotowane, aby stawić czoła zagrożeniom. Kolejnymi słabymi punktami są urządzenia sieciowe – ich niska odporność na cyberzagrożenia sprawia, że stają się idealną „furtką" do naszej organizacji.

Celem jest zminimalizowanie ryzyka związanego z bezpieczeństwem informatycznym, ale jak to osiągnąć? Z pomocą przychodzą różne inicjatywy na szczeblu zarówno organizacyjnym, jak i ustawodawczym. Przykładem takiego właśnie rozwiązania jest Europejska Dyrektywa NIS 2, na której wdrożenie Polska ma już niecały rok. Dotyczy ona w szczególności firm i instytucji publicznych związanych z działalnością infrastruktury krytycznej. W tej grupie znajdują się przedsiębiorstwa energetyczne, z sektorów transportu i logistyki, producenci żywności oraz artykułów przemysłowych, firmy farmaceutyczne. W ramach tej dyrektywy podlegające jej firmy mają zadbać o bezpieczeństwo cybernetyczne swojej instytucji i dotyczy to również ich łańcucha dostaw. Innymi słowy firmy te będą oczekiwać gwarancji bezpieczeństwa od podmiotów, z którymi współpracują. Za niedopełnienie tych obowiązków będą grozić konkretne kary finansowe, podobne jak w przypadku RODO. Warto już dziś przyjrzeć się szczegółowym wytycznym i ocenić ich wpływ na naszą organizację.

W kwestiach cyberbezpieczeństwa mamy dostępne normy, narzędzia, wytyczne branżowe, które od wielu lat wspierają walkę z cyberprzestępczością. Do dyspozycji pozostają wytyczne branżowe, takie jak BSIMM, ISA/IEC 99/62443, ISO 27001 czy OWASP, które definiują zasady bezpieczeństwa zarówno organizacji, jak i wykorzystywanych komponentów.

Wybierając rozwiązania do systemu monitoringu wizyjnego, na pewno spotkamy się z wytycznymi NDAA z sekcji 889, która dotyczy pochodzenia produktu. Warto wiedzieć, że samo spełnienie tej wytycznej nie daje gwarancji cyberbezpieczeństwa. Jeżeli chcemy postawić bezpieczeństwo na wyższym poziomie, należy wymagać szyfrowania danych, prywatności połączenia itp. Standard PCI DSS związany z bezpieczeństwem kart płatniczych lub program bezpieczeństwa cybernetycznego UL CAP dają gwarancję, że urządzenie przeszło testy penetracyjne i spełnia szereg rygorystycznych norm.

Stosując się do tych zasad, możemy być pewni, że nasza organizacja będzie bezpieczniejsza, a spełnienie wytycznych dyrektywy NIS 2 na poziomie poszczególnych urządzeń i systemów nie będzie wyzwaniem, lecz standardem w naszej firmie.

Marcin Walczuk
BCS

Systemy zabezpieczeń pomagają zmniejszyć straty

Współczesny handel detaliczny nie może obejść się bez technologii cyfrowych, które umożliwiają sprawniejsze i wygodniejsze prowadzenie działalności. Jednak nawet one nie zapobiegną w 100% takim zagrożeniom, jak kradzież, fałszerstwo, manipulacja czy uszkodzenie towaru. Dlatego przedsiębiorcy i konsumenci muszą stosować odpowiednie systemy zabezpieczeń, które mogą zapewnić maksymalny poziom ochrony odpowiedni dla środowiska handlowego.

Jednym z najpopularniejszych elektronicznych systemów zabezpieczenia w branży retail jest system antykradzieżowy EAS *(Electronic Article Surveillance)*. Specjalne etykiety lub tagi przymocowane do produktów są wykrywane przez bramki antykradzieżowe umieszczone przy wejściach i wyjściach sklepu. Próba wyniesienia nieautoryzowanego produktu jest sygnalizowana sygnałem dźwiękowym lub świetlnym. EAS jest skutecznym sposobem na zmniejszenie strat i zwiększenie rentowności w placówkach sprzedażowych.

Równie ważnym systemem w obiektach handlowych jest dozór wizyjny. Kamery instaluje się w celu monitorowania podejrzanych zachowań, odstraszania potencjalnych złodziei lub wandali, rejestrowania dowodów przestępstw lub naruszeń, dostarczają też danych do analizowania wzorców ruchu i preferencji zakupowych klientów.

System monitoringu wizyjnego może być połączony z innym systemem, np. POS *(Point of Sale)*, który wykorzystuje terminale komputerowe lub urządzenia mobilne do przetwarzania transakcji sprzedaży i płatności w sklepie. POS ma na celu ułatwienie i przyspieszenie procesu sprzedaży i płatności poprzez automatyczne skanowanie kodów kreskowych lub QR, akceptowanie różnych form płatności, generowanie paragonów lub faktur, integrowanie się z innymi systemami księgowymi czy analitycznymi. Połączenie go z kamerami dozorowymi pozwala na nanoszenie informacji z transakcji kasowych na nagrania z kamer, co ułatwia wychwycenie bądź późniejsze odnalezienie nieprawidłowości sprzedażowych.

Podsumowując, elektroniczne systemy zabezpieczeń są nieodłączną częścią handlu, który musi dostosować się do zmieniających się warunków i wymagań rynku. Mogą pomóc przedsiębiorcom chronić towary, a klientom zapewnić komfort zakupów, jednak należy pamiętać, że nie są niezawodne. Wymagają stałej aktualizacji i dozoru człowieka, którego praca jest w tym sektorze niezastąpiona.

Bartłomiej Skórski
HIKVISION POLAND

Wyzwania w sektorze handlowym

Menedżerowie ds. bezpieczeństwa w sektorze handlowym w Polsce zmagają się z wieloma wyzwaniami. Brak danych specyficznych dla naszego kraju utrudnia uzyskanie pełnego obrazu, jednakże na podstawie globalnych i regionalnych trendów można zidentyfikować kilka kluczowych problemów.

Najczęstszymi są niewystarczające budżety na systemy zabezpieczeń, które mogą ograniczać dostęp do nowoczesnych rozwiązań technologicznych, co z kolei może prowadzić do niewystarczających szkoleń pracowników w zakresie bezpieczeństwa.

Nowoczesne technologie mogą znacząco przyczynić się do poprawy bezpieczeństwa w handlu detalicznym. Na przykład systemy oparte na kamerach i technologiach AIoT, oferujące zaawansowaną analizę obrazu, mogą pomóc w monitoringu w czasie rzeczywistym oraz analizie danych. Funkcje liczenia osób oraz mapy ciepła mogą dostarczyć cennych danych, które pomogą w lepszym zrozumieniu zachowań klientów oraz efektywniejszym zarządzaniu personelem i zasobami. Doskonałym przykładem są zintegrowane systemy dla sektora retail oferowane przez Hikvision. Wspierają bezpieczeństwo i jednocześnie dostarczają dane, dzięki którym sklepy stają się bardziej innowacyjne i efektywne operacyjnie.

Klienci często pytają o skuteczność różnych systemów zabezpieczeń, ich koszty i korzyści, jakie mogą przynieść dla ich operacji handlowych. Ponadto w świetle zmieniających się preferencji konsumentów klienci mogą być zainteresowani tym, jak nowe technologie pomogą im lepiej zrozumieć zachowania klientów i dzięki temu odpowiednio dostosować swoje operacje.

Rafał Kowal
SCHRACK SECONET POLSKA

Sprawna i bezpieczna ewakuacja

Bezpieczeństwo pożarowe w obiektach handlowych to nie tylko detekcja zagrożenia, ale też odpowiednie procedury, pozwalające na przeprowadzenie sprawnej ewakuacji. Ewakuacja może być wspierana sygnalizatorami akustycznymi lub optyczno-akustycznymi, a w przypadku większych obiektów także za pomocą dźwiękowych systemów ostrzegawczych (DSO). Istotny jest odpowiedni dobór rozwiązań w zakresie typów, mocy oraz lokalizacji głośników i podział na strefy nagłośnieniowe wykonany już na etapie projektu.

W niewielkich obiektach handlowych często stosowanymi rozwiązaniami są centrale sygnalizacji pożarowej w połączeniu z sygnalizatorami akustycznymi lub optyczno-akustycznymi. Takie rozwiązanie może się sprawdzić w przypadku niewielkich, jednopowierzchniowych przestrzeni, np. w supermarketach.

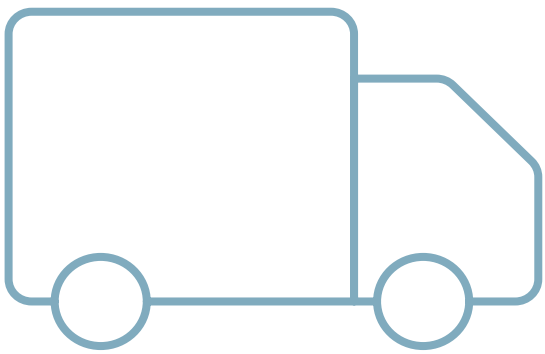
W dużych, wielokondygnacyjnych centrach handlowych z wieloma wyjściami pożarowymi, klatkami schodowymi czy wydzieleniami pożarowymi, np. w postaci bram przeciwpożarowych, jedynym słusznym rozwiązaniem wspomagającym proces ewakuacji jest instalacja DSO. Jego głównym zadaniem jest powiadamianie o powstałym zagrożeniu z wykorzystaniem funkcji rozgłaszania komunikatów głosowych (automatycznych lub tych nadawanych na żywo), zazwyczaj poprzedzanych sygnałem dźwiękowym typu syrena (najczęściej są to znormalizowane sygnały.).

O ile sygnalizatory akustyczne są w stanie wygenerować sygnał o wysokim poziomie ciśnienia akustycznego, który dodatkowo może być modulowany, celem zwiększenia uwagi osób przebywających w zagrożonej strefie, o tyle jest to nadal tylko sygnał. Nie jesteśmy w stanie stwierdzić, z jakiego typu zagrożeniem mamy do czynienia i jak należy się zachować w danej sytuacji.

Tymczasem zastosowanie DSO daje możliwość generowania krótkich sygnałów dźwiękowych, poprzedzających komunikat słowny, które mają zwrócić uwagę osób przebywających w danej strefie nagłośnieniowej, a następnie nadania komunikatu głosowego o konkretnej treści dostosowanej do typu, przeznaczenia obiektu oraz zagrożenia. Jest to podstawowa funkcja DSO i bezapelacyjnie niezbędna dla sprawnego i bezpiecznego przeprowadzenia ewakuacji ludzi z zagrożonej strefy. W zależności od treści komunikatów będą one miały różne przeznaczenie, np. komunikat ewakuacyjny – mobilizuje do natychmiastowej ewakuacji, ostrzegawczy (alarmowy) – przygotowuje do podjęcia ewakuacji lub odwołujący – informuje o zakończeniu zagrożenia.

W niektórych przypadkach może okazać się, że dojdzie do nakładania się na siebie różnych komunikatów, co poskutkuje ich niezrozumieniem i brakiem właściwej reakcji. Taka sytuacja może dotyczyć np. budynków z „otwartą" przestrzenią przechodzącą przez kilka kondygnacji lub gdy dojdzie do tzw. przesłuchów pomiędzy strefami choćby przez kanały wentylacyjne. W takim przypadku ewakuacja powinna odbywać się raczej w układzie naprzemiennym, co daje dodatkowo możliwość łatwiejszego porozumiewania się między sobą osób znajdujących się w zagrożonej strefie bez niepotrzebnego „przekrzykiwania się" z komunikatami nadawanymi przez DSO.

Chcąc zapewnić sprawną i bezpieczną ewakuację z zagrożonej strefy, należy pamiętać, że bardzo ważnym czynnikiem jest klarowność komunikatów dotyczących zaistniałych zdarzeń, co pozwoli na szybszą reakcję i podjęcie ewakuacji lub przygotowanie się do niej osób znajdujących się w zagrożonym obszarze. ●



Honeywell

35 SERIES
ZWIĘKSZ ŚWIADOMOŚĆ - NIE KOSZTY

Seria 35 korzysta z algorytmu sztucznej inteligencji – rozróżnia pojazdy i ludzi.

- Doskonała jakość obrazu do 8MP
- Elastyczny nadzór
- Wbudowana pamięć wideo
- Inteligentna detekcja ruchu i analityka
- Łatwy w instalacji i obsłudze

5 YEAR WARRANTY | SECURE BY DEFAULT | ONVIF | SGT

Premium security distributor:

Linc Polska Sp. z o.o.
ul. Czarnkowska 22, 60-415 Poznań
tel.: +48 61 839 19 00, www.linc.pl

Linc Polska Sp. z o.o.

Odporność na stres można budować

„Nigdy się nie poddawaj. Zawsze można zrobić coś jeszcze, by przetrwać. Musisz przeżyć” – mówi Jacek Pałkiewicz, dziennikarz, podróżnik, ojciec polskiego survivalu, w rozmowie z Jackiem Tyburkiem.

Pańskie dwa ostatnie poradniki to *Dżungla miasta* i *Wojna u progu. Poradnik przetrwania,* stąd moje pierwsze pytanie. Jak sobie radzić w tych turbulentnych czasach, po pandemii i z wojną tuż za granicą?
Przede wszystkim panujmy nad wyobraźnią i… róbmy swoje. Jeśli będziemy wstawać z łóżka z przekonaniem, że nic nie ma sensu, bo zaraz mogą spaść tu rakiety bądź wyparujemy w wyniku eksplozji bomby nuklearnej, już przegraliśmy. I nie chodzi o to, by udawać, że nic nam nie grozi, i wypierać myśl o zagrożeniach. Ale warto żyć z myślą o przyszłości: pracować, budować więzi, realizować marzenia i plany. Natomiast człowiek przezorny powinien zadać sobie pytanie, co zrobi, kiedy pojawi się kryzys wojenny. Gdy na przykład Putin w swoim skrajnym szaleństwie postanowi posłać swoje wojska na Zachód, czyli najpierw do nas? Albo ostrzelać nasze miasta w chwili, gdy będzie wiedział, że jego czas się kończy? Co zrobię, gdy dojdzie do kryzysu ekologicznego? Zabraknie energii, gospodarka się załamie, wybuchnie wojna domowa? A co zrobię, gdy w kolejnej pandemii pojawi się wirus bardziej śmiercionośny niż ostatni? Trzeba mieć gotowe odpowiedzi, być spać spokojnie. Strefa Gazy, Tajwan – to na mapie świata punkty zapalne, ale może być ich więcej. Dlatego zresztą, nie tylko ze względu na wojnę w Ukrainie, z Krzysztofem Petkiem, specjalistą od działań w sytuacjach ekstremalnych szkolącym i młodzież, i dorosłych, opracowaliśmy podręcznik *Wojna u progu.*

W *Dżumie* Alberta Camusa to szczury były sygnałem nadchodzącej katastrofy. Teraz, gdy miasta naszpikowane są czujnikami, systemami bezpieczeństwa, kamerami, narzędziami kontroli dostępu itp., nie potrzebujemy szczurów, by dostrzec zagrożenie. Jak pana zdaniem korzystać z danych zbieranych przez wszystkie miejskie systemy, by móc odpowiednio wcześniej zareagować?
Narzędzia tworzymy po to, by lepiej i łatwiej nam się żyło. Należy więc z nich korzystać optymalnie, zbierać dane, analizować i wyciągać wnioski. Jednak wielu analityków, szczególnie działających amatorsko, popełnia kardynalne błędy probabilistyczne. Obserwując różne zdarzenia losowe, choćby analizując zapis kamer umieszczonych w newralgicznych miejscach, możemy dokonywać nieprawidłowych uogólnień. Jeśli na to nałoży się mechanizm predykcyjny, czyli stawianie na to, co w naszym umyśle jest zapisane, znane, zrozumiałe, to w co drugiej osobie możemy widzieć potencjalnego terrorystę. Dlaczego o tym mówię? Bo morze danych, o których pan wspomina, zalewa nasze umysły, które nie ewoluują tak szybko jak świat techniki. Czujemy się bezradni w gęstwinie impulsów. Warto więc objąć swój świat refleksją i zadać sobie pytania, co tu i teraz stanowi czynnik decydujący, które z impulsów są najważniejsze. Piszemy o tym w *Wojnie u progu.* Jeśli media podsycają niepokój, służby mundurowe są stawiane w stan gotowości, wzmagają się kontrole… i tak dalej. Można się wspierać analizą statystyczną, ale wszystko przecież zależy od decyzji ludzi, dlatego nie zapominajmy, by przede wszystkim obserwować te osoby, które trzymają ster.

***Deep fake*, manipulacje medialne, sztuczna inteligencja, cyberataki, chiński system ratingu społecznego (podobny może kusić także rządy innych państw) – to już rzeczywistość, a nie tylko ponury scenariusz. Jak w takich czasach budować odporność indywidualną i organizacyjną? Jak skutecznie wykorzystać dostępne technologie, ale też wiedzę i umiejętności ludzi?**
Kiedyś rozpowszechnianiu niebezpiecznych informacji zapobiegano za pomocą takiego czy innego mechanizmu cenzury lub po prostu zakazu publikacji. Dziś to niemożliwe, a prawdziwe informacje toną w powodzi milionów sprzecznych danych, bzdur, teorii spiskowych i plotek. Tymczasem nie dzieje się tak, że im więcej przeczytamy wiadomości wylewających się z komputerów i smartfonów, tym bardziej jesteśmy mądrzejsi. Wpadamy wówczas w chaos informacyjny i emocjonalny. Dlatego trzeba korzystać z mediów, którym ufamy, wybierając przy tym kilka źródeł reprezentujących różne podejścia, poglądy, opcje, strategie. Jeśli zaś chodzi o budowanie odporności, jest ona funkcją naszej psychiki, nie zależy od jakości smartfonów i szybkości Internetu. Odporność na stres można budować samodzielnie, wystawiając się regularnie na mniejsze i większe próby, podejmując wyzwania, upadając i wstając, by pójść dalej. To jak trening bokserski. Nie uodpornię się na ciosy, jeśli nie wyjdę na ring. Inny poziom pracy nad odpornością, także zespołową, to przemyślane szkolenia integracyjne. Prowadzimy takie z Krzysztofem Petkiem w terenie, zarówno w Polsce, jak i w odległych regionach świata, wprowadzając uczestników w sytuacje dyskomfortu, deprywacji sensorycznej, narastającej niepewności. Oczywiście panujemy nad bezpieczeństwem, obserwując zachowania uczestników. Współpracujemy z psychologami, by w krótkim czasie przeszkolić ludzi, zaaplikować im niejako intelektualną i psychiczną szczepionkę na sytuacje kryzysowe.

> *» Narzędzia tworzymy po to, by lepiej i łatwiej nam się żyło. Należy więc z nich korzystać optymalnie, zbierać dane, analizować i wyciągać wnioski. «*

Ludzie pracujący w służbach mundurowych odchodzą z nich, choćby na emeryturę, będąc jeszcze w sile wieku. A przecież często dysponują unikatowym doświadczeniem, są znakomicie wyszkoleni i mają cechy charakteru, które powodują, że w trudnych czasach mogliby być liderami. Od lat prowadzi pan zajęcia z liderami biznesu. Ma więc pan porównanie różnego rodzaju liderów. Proszę zatem o wzorzec lidera idealnego na trudne czasy. Jakie cechy powinna mieć osoba, której powierzyłby pan przywództwo w czasie kryzysu lub wojny.

Kiedy prowadziłem unikatowe szkolenia z technik przetrwania na Saharze czy w brazylijskiej dżungli, uczestniczyli w nich oficerowie z oddziałów specjalnych z Austrii i Rosji, a z Polski ludzie rekrutujący się z np. policji, Straży Granicznej i formacji GROM. To wyselekcjonowani ludzie, silni nie tylko fizycznie, ale i odporni psychicznie. Szkolenie każdego z nich kosztuje grube miliony. Kiedy odchodzą ze służby, stanowią łakomy kąsek dla firm prywatnych. Tak działa rynek. Choć bywa, że skuszą się na „pracę" dla tych „po drugiej stronie", a to już tragedia. Jednak czy tak się stanie, zależy właśnie od ich lidera, od tego, jak ich „wychowa", czy nie pozwoli im zapomnieć, co stanowi ideę nadrzędną ich pracy. Lider musi wpoić ludziom, których wiedza i umiejętności przekraczają możliwości przeciętnego człowieka, że służba oznacza niesienie pomocy i ochranianie innych. Zatem w czasach kryzysu czy wojny biznes będzie potrzebować, poza specjalistami od finansów i psychologów budujących zespoły i uczących komunikacji, także typowych dowódców, którzy – korzystając również z wiedzy biznesowej i psychologicznej – potrafią uczynić swoich podwładnych twardymi, nieprzejednanymi, niezłomnymi, kiedy sytuacja tego wymaga.

Czy w takim razie uważa pan, że zarządy firm i np. samorządy powinny pomyśleć o tym, by w ich strukturach znalazło się miejsce dla byłych żołnierzy i funkcjonariuszy?
Naturalnie. To mogą być znakomici nauczyciele dla ludzi na kierowniczych stanowiskach w środowisku biznesowym, ale nie tylko. Byli żołnierze jednostek elitarnych mogą z powodzeniem pokazać, jak budować zespół i zarządzać nim, jak go motywować, jak radzić sobie ze stresem, jak rozbudować system bezpieczeństwa czy przeciwdziałać terroryzmowi.

Jacek Edward Pałkiewicz
polski dziennikarz i podróżnik, odkrywca źródła Amazonki; członek rzeczywisty Królewskiego Towarzystwa Geograficznego. Uczy elitarne jednostki specjalne strategii przetrwania w odmiennych strefach klimatycznych. W 1983 r. założył w Bassano del Grappa (Włochy) szkołę przetrwania. Autor wielu książek, m.in. *Sztuka podróżowania, Dżungla miasta,* oraz współautor poradnika przetrwania *Wojna u progu.*

> *» Warto szkolić pracowników ochrony z zarządzania w sytuacji wojny, ataku terrorystycznego czy katastrofy naturalnej. «*

Szkolenia, wypracowywanie odpowiednich odruchów, swoistej rutyny znacznie podnosi poziom przygotowania się do wyzwań. Jakie szkolenia dla firm dzisiaj są najbardziej zbliżone do współczesnych potrzeb?
Mechanizm szkolenia łatwo zrozumieć, spoglądając przez pryzmat zachowań mistrzów sztuk walki. Taka, a nie inna reakcja na konkretny typ ataku radykalnie zwiększa szansę na jego odparcie, jednocześnie obniżając poziom stres. To, co przetrenowane, przepracowane, znane, przestaje być potworem czającym się w mroku. Nadal z Krzysztofem Petkiem prowadzimy szkolenia, także w terenie, by nauczyć ludzi panować nad stresem spowodowanym niepewnością, dyskomfortem i obcym środowiskiem. Niezależnie bowiem od dynamicznych zmian technologicznych i rynkowych, jakie zaszły w ostatnich latach, mózg ludzki się nie zmienił. A my, prowadząc szkolenia, bazujemy na czynniku ludzkim, nie technicznym.

Gdy uważnie się rozejrzymy, zobaczymy wokół siebie wielu pracowników ochrony obecnych w różnych obiektach. Łącznie jest ich zapewne więcej niż żołnierzy i policjantów. To grupa zawodowa w czasie jakiekolwiek kryzysu mająca ogromny potencjał pomocowy. Mam rację?
Wszystko zależy od tego, jak zostali wyszkoleni – to podstawa – i co sobą reprezentują. Lata świetlne dzieli przecież dorabiającego „na bramce" emerytowanego kierowcę od kogoś, kto był wcześniej oficerem Biura Ochrony Rządu. Zakładając jednak, że mamy ludzi świadomych swojej odpowiedzialności i umiejętności, to mogą być np. tymi, którzy potrafią opanować panikę w tłumie i zarządzać sytuacją kryzysową. Nie mają problemu z rozróżnieniem, co jest ważne, a co ważniejsze. Dlatego uważam, że warto szkolić pracowników ochrony z zarządzania w sytuacji wojny, ataku terrorystycznego czy katastrofy naturalnej. Firmy powinny o tym pomyśleć dla dobra własnego i *pro publico bono.*

A może firmy powinny także pomyśleć o tym, że przydałoby się przygotować pracowników na różnego rodzaju sytuacje kryzysowe, pomagając im zorganizować coś, co na własny użytek nazwałem niezbędnikiem Pałkiewicza. Niezbędnik Pałkiewicza to lista zapasów i przedmiotów potrzebnych do przeżycia w sytuacji kryzysowej. Może firmy powinny same przygotowywać takie listy albo nawet pakiety ucieczkowe? Sami raczej ich nie robimy.
To prawda, większość ludzi nie ma takiego pakietu ucieczkowego. Jednym z głównych powodów tego stanu jest rodzaj pierwotnego,

Jacek Pałkiewicz wspólnie z brazylijskimi instruktorami prowadzi zajęcia survivalowe w Centrum Walki w Dżungli w Manaus

zabobonnego lęku przed „wywołaniem wilka z lasu". Opowiadają o tym uciekinierzy z Ukrainy – niektórzy aż do dnia, w którym spadły bomby, nie zrobili zapasów żywności, leków, wody. Chcieli żyć tak, jakby nic im nie groziło. To znany mechanizm wyparcia, co odradzam. Warto być świadomym zagrożeń. Postawić sobie pytanie, co się stanie, jeśli będę przygotowany, wyposażony, a bestia nie nadejdzie. I drugie: co wówczas, kiedy nie będę gotów, ani psychicznie, ani sprzętowo, a kataklizm zajrzy w moje okno. Kładziemy odpowiedzi na szalę i przyglądamy się, co przeważa. Jeśli zaś chodzi o zespołowe, firmowe przygotowanie do niebezpieczeństw, to pomysł niezły, który powinien iść w parze ze szkoleniem pracowników. Wymyślony na bieżąco zestaw przedmiotów, apteczek, racji żywnościowych, bez wiedzy, jak i kiedy z nich korzystać, może okazać się mało przydatny.

Nasz świat stał się cyfrowy, więc uzależniony od energii. Co zrobimy, gdy jej zabraknie?

To zależy, kto będzie sobie musiał z tym faktem poradzić. Krzysztof Petek zaprasza mnie na obozy survivalowe, które prowadzi dla młodzieży. Potwierdza się jego teza, że nowe pokolenia są wychowywane w skrajnej bezradności społecznej. Otacza je bańka cywilizacyjna oparta na komunikacji cyfrowej. Dla pokolenia lat 90. i młodszych ludzi deszcz to szum z głośników, ranę leczy się, znajdując apteczkę w cyfrowym korytarzu, a umiera się tylko na chwilę, by potem wrócić do gry. I tu zaczyna się dramat, gdyż komputerowi „komandosi" w prawdziwym deszczu, błocie, wreszcie wobec rzeczywistych życiowych problemów stają się bezradni. Bo na realny ból, zagubienie, głód nie ma skrótu klawiszowego. Dlatego niezbędne jest przyuczenie choć niewielkiego procenta obywateli do działania w sytuacji zderzenia z dziką przyrodą, brakiem komunikacji i koniecznością zdobywania wody czy żywności. W razie katastrofy globalnej to jedyny sposób, by nasz gatunek przeżył, przy mniejszych zagrożeniach to sposób minimalizowania zagrożenia i po prostu przetrwania jednostki. Nawet jeśli nie będziemy odwoływać się do wojny czy kataklizmu, wyobraźmy sobie, że nasz samochód psuje się nocą w styczniu na szosie wiodącej tatrzańską przełęczą. Zero zasięgu, ogrzewania, do cywilizacji kilometry, wokół zadymka śnieżna i minus dwadzieścia stopni. Lepiej być gotowym czy liczyć na cud?

W *Wojnie u progu* znajdziemy „10 zasad Pałkiewicza". Poproszę teraz o jedną, taką, którą uznaje pan za najważniejszą.

Nigdy się nie poddawaj. Zawsze można zrobić coś jeszcze, by przetrwać. Musisz przeżyć. ●

Landspítali – Krajowy Szpital Uniwersytecki w Rejkiawiku

ProtegeGX w służbie zdrowia

ProtegeGX to rozwiązanie klasy Enterprise z szeroką funkcjonalnością. Integruje m.in. kontrolę dostępu, system sygnalizacji włamania i napadu, CCTV, rejestrację gości, zarządzanie windami oraz rejestrację czasu pracy. Jest idealnym rozwiązaniem do instalacji rozproszonych wymagających zdalnego zarządzania w wielu lokalizacjach.

ProtegeGX umożliwia zaawansowane monitorowanie zdarzeń na wielu stacjach roboczych jednocześnie, za pomocą zaawansowanych interaktywnych map wizualizacji, widoków oraz aktywnych list zdarzeń na żywo z zaawansowanym filtrowaniem.

System jest przeznaczony do obiektów z różnych sektorów i branż, m.in. dla służby zdrowia, więziennictwa, obiektów handlowych i usługowych, biurowców i wielu innych. Znakomicie sprawdza się np. w Landspítali – Krajowym Szpitalu Uniwersyteckim w Rejkiawiku w Islandii. Landspítali z ponad 100 budynkami w 17 lokalizacjach jest obecnie w trakcie wieloletniej rozbudowy, która ma się zakończyć pod koniec 2030 r.

Audyt przed rozbudową wskazał na brak przeglądu systemu dla pracowników ochrony, nieefektywne zarządzanie użytkownikami i brak automatyzacji. Szpital Landspítali zmagał się z różnymi systemami alarmowymi, brakiem automatyzacji i ciągłymi kosztami ponownego dorabiania zamków i kluczy fizycznych. Przestarzała technologia nie pozwalała na pełny przegląd systemu, a trudności związane z zarządzaniem 10 tys. aktywnych użytkowników powodowały nieefektywność personelu zajmującego się bezpieczeństwem. Zarządzanie tak dużą liczbą stanowiło wyzwanie w przypadku zmian poziomów dostępu, dodawania nowych użytkowników lub anulowania dostępu byłym pracownikom, dlatego zaprojektowano i wdrożono ujednolicone rozwiązanie. Łącząc ProtegeGX z bazą danych HR za pomocą usługi SOAP Web Service firmy ICT, uproszczono procedury. W przypadku, gdy pracownik zostanie wprowadzony do jednego systemu, automatycznie aktualizuje się on w drugim, zapewniając spójne rozwiązanie do kontroli dostępu użytkowników. Jest to szczególnie przydatne, gdy pracownik nie zwróci swojej karty po zakończeniu zatrudnienia. Po usunięciu go z bazy danych HR karta nie umożliwi dostępu.

Zasadą szpitala jest środowisko pozbawione kluczy fizycznych. Teraz pracownicy zamiast posługiwać się wieloma kluczami, korzystają tylko z jednej karty dostępu. ICT jest w tym względzie idealną opcją. To pojedyncze uwierzytelnienie zapewnia dostęp do wszelkich autoryzowanych obszarów, w tym drzwi, wind, a nawet apteczek. Wszystko jest kontrolowane przez przypisane poziomy dostępu w ProtegeGX. Jedna karta umożliwia m.in. płacenie za posiłki w stołówce.

Bezpieczeństwo personelu i pacjentów zostało również zwiększone dzięki integracji wind szpitalnych. Pracownicy uzyskują dostęp wyłącznie do pięter, do których są uprawnieni. W przypadku części szpitala wymagających wyższego poziomu bezpieczeństwa, korzystając z wideodomofonów, można sprawdzić autoryzację i udzielić dostępu do tych obszarów na ekranach komputerów stacjonarnych przez wysyłanie sygnału do kontrolera ICT w celu otwarcia żądanych drzwi.

W rezultacie, dzięki spójnemu systemowi Landspítali uzyskał zwiększoną wydajność personelu, skrócony czas reakcji i znacznie lepszą obsługę pacjentów.

Ujednolicone rozwiązanie ProtegeGX firmy ICT zmodernizowało pracę szpitala i dzięki higienicznemu rozwiązaniu wymagającemu niewielkiego kontaktu zwiększyło poziom jego bezpieczeństwa. Tym samym położyło podwaliny pod przyszły rozwój szpitala. Przedstawiony przykład jest godny polecenia w obiektach polskiej służby zdrowia. ●

Miwi-Urmet
ul. Pojezierska 90A,91-341 Łódź
miwi@miwiurmet.pl
www.miwiurmet.pl

ICTProtegeGX®

Zintegrowany System Zarządzania Bezpieczeństwem

Przeznaczony do obiektów z różnych sektorów i branż

- Służba zdrowia
- Więziennictwo
- Handel i usługi
- Oświata
- Przemysł i produkcja
- Sport i rekreacja
- Administracja rządowa i lokalna
- Biurowce
- Budownictwo mieszkaniowe

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

urmet MIWI

Rickard Gudbrand, specjalista ds. produktów PTZ

Kent Fransson, menedżer produktów PTZ

Nowa generacja energooszczędnych kamer

Galopujące koszty energii i kryzys klimatyczny wymuszają inne podejście do zużycia energii. Nic więc dziwnego, że jej zużycie przez kamery stało się jednym z ważniejszych parametrów uwzględnianych przez kupujących.

O nowych produktach Axis z linii Q, w których wprowadzono funkcję oszczędzania energii, mówią Kent Fransson, globalny menedżer produktów PTZ, oraz Rickard Gudbrand, specjalista ds. produktów PTZ w Axis.

Nietypowy początek

Słysząc „mobilne urządzenie dozorowe", nie myśli się od razu – co zrozumiałe – „podatny grunt dla innowacji w zakresie oszczędzania energii". Jednak najlepsze pomysły rodzą się w najbardziej niespodziewanych okolicznościach. Tak też było i w tym przypadku. Do wprowadzenia innowacji zainspirował nas konkretny klient, który korzystał z wież mobilnych CCTV wyposażonych w duże akumulatory zapewniające ciągłość ich pracy. Niektóre z nich miały zamontowane nawet panele fotowoltaiczne, ale zarządzanie zużyciem energii jest trudniejsze, niż można przypuszczać. Wychodzimy jednak z założenia, że zawsze można próbować zmniejszyć zapotrzebowanie na energię, tym bardziej że klienci już wcześniej pytali nas o energooszczędne kamery, jednocześnie zaprojektowane pod kątem zastosowań w mobilnych i zdalnych obiektach oraz w związku z tym mogące pracować w warunkach dużych wahań temperatury.

Tymczasem kamery to urządzenia ciepłolubne. Temperatura ich wnętrza powinna wynosić ok. 20°C. Dlatego, podobnie jak inni producenci z branży, stosowaliśmy w nich niewielkie grzałki. Sęk w tym, że oznacza to zużycie dodatkowej energii. A jeśli kamery miałyby pracować w niskiej temperaturze, usunięcie modułu grzejnego nie wchodziło w grę.

Dlatego opracowaliśmy funkcję niskiego poboru mocy, której zadaniem jest wyłączanie większości grzałek w kamerze, gdy temperatura otoczenia jest wystarczająco wysoka, co zmniejsza zużycie energii. Już pierwsze statystyki dotyczące zużycia energii dowiodły, że pomysł był świetny. W niektórych zakresach temperatur odnotowaliśmy oszczędność energii na poziomie nawet 50%.

Kolejny krok był oczywisty: musieliśmy przetestować nową funkcję w innych warunkach temperaturowych i w nowych zastosowaniach.

Nie da się zoptymalizować tego, czego się nie mierzy

Zespół projektowy Axis opracował zatem model nowego trybu niskiego poboru mocy dostosowujący ogrzewanie do temperatury otoczenia. Wyniki ustaleń okazały się zachęcające, niezależnie od tego, czy testy

prowadzone były w Lund, Nowym Jorku, czy w tak ciepłych miastach jak Madryt lub Dallas. I niezależnie też od tego, czy kamery były instalowane na budynkach i latarniach ulicznych, obiektach przemysłowych i fabrykach bądź na jednostkach mobilnych korzystających z akumulatorów, we wszystkich przypadkach odnotowano znaczne oszczędności energii.

W każdej instalacji zamontowaliśmy miernik zużycia energii, aby kontrolować oszczędności energii w skali roku. Dzięki temu mogliśmy sprawdzić rzeczywistą efektywność nowego trybu niskiego poboru mocy w różnych sytuacjach. I jesteśmy zachwyceni wynikami. Dowiedliśmy skuteczności nowego podejścia do oszczędzania energii.

Zużycie energii znajduje się wysoko na liście ważnych kwestii w każdej firmie. W przetargach komercyjnych często pojawia się pytanie o wpływ instalacji na emisję dwutlenku węgla i zużycie energii. Liczby te mogą zdecydować o przyjęciu lub odrzuceniu przedstawionej oferty.

Dzięki naszym modelom i testom, a także wbudowaniu mierników zużycia energii klienci i instalatorzy mogą teraz dość dokładnie przewidzieć wpływ każdej instalacji na zużycie energii, a tym samym na emisję dwutlenku węgla. To informacje, których nabywcom nader często brakuje, a są niezbędne, by mogli podejmować decyzje i prowadzić biznes zgodnie z zasadami zrównoważonego rozwoju.

Nie tylko ogrzewanie

Wbudowanie miernika zużycia energii nie tylko pozwoliło nam udowodnić, że nowy tryb ma znaczny wpływ na zużycie energii, ale też zainspirowało nas do przetestowania innych pomysłów.

Nagle zaczęliśmy myśleć nie tylko o ogrzewaniu. Miernik umożliwia pomiar zużycia energii dla niemal każdego aspektu działania kamery – od prędkości, z jaką porusza się kamera, przez to, czy jest włączone oświetlenie podczerwone, po różną poklatkowość i inne parametry. Dysponując takimi informacjami i odpowiednimi narzędziami, użytkownicy mogą tak skonfigurować urządzenie, aby zoptymalizować zużycie energii, a jednocześnie dostosowywać je do własnych potrzeb.

Kiedyś, gdy klienci pytali, ile energii potrzebuje kamera przy określonych ustawieniach i warunkach otoczenia, odpowiedź była trudna. Wprowadzenie miernika umożliwia uzyskanie bardzo dokładnych wartości nie tylko w danym czasie, ale też w dłuższej perspektywie. Jest to bardzo ważne dla tych klientów, którzy używają kamer w instalacjach zasilanych za pomocą akumulatora, często mobilnych. Także w tych z akumulatorem jako zapasowym źródłem zasilania, ponieważ można bardzo dokładnie obliczyć, jak długo będzie działać urządzenie, zanim skończy się zewnętrzne zasilanie.

Nowa linia Q z trybem niskiego poboru mocy

Zależnie od okoliczności i temperatury otoczenia korzystanie z trybu niskiego poboru mocy może zmniejszyć zużycie energii nawet o 50% (w niektórych zakresach temperatur). Nic dziwnego, że przy tak zachęcających wynikach pomiarów nasza firma zdecydowała się już na stałe wprowadzić na rynek kamery z trybem niskiego poboru mocy. Nowe modele AXIS Q6318/15-LE, AXIS Q6215/25-LE i AXIS Q6135-LE są wyposażone także w miernik zużycia energii w czasie rzeczywistym. Podjęliśmy też zobowiązanie, że kolejne produkty z linii Q będą standardowo wyposażane w tryb niskiego poboru mocy i miernik zużycia energii.

Oczywiście, rzeczywiste obniżenie zużycia energii zależy od warunków panujących w otoczeniu kamery (takich jak temperatura), wersji oprogramowania sprzętowego, obciążenia kamery i oczywiście wybranego modelu kamery. Najbardziej cieszy fakt, że dzięki zaangażowaniu Axis w zrównoważony rozwój to oszczędność energii stała się kluczowym argumentem sprzedażowym naszych produktów. Ta nowość może mieć ogromny pozytywny wpływ zarówno na portfele naszych klientów, jak i na środowisko. ●

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

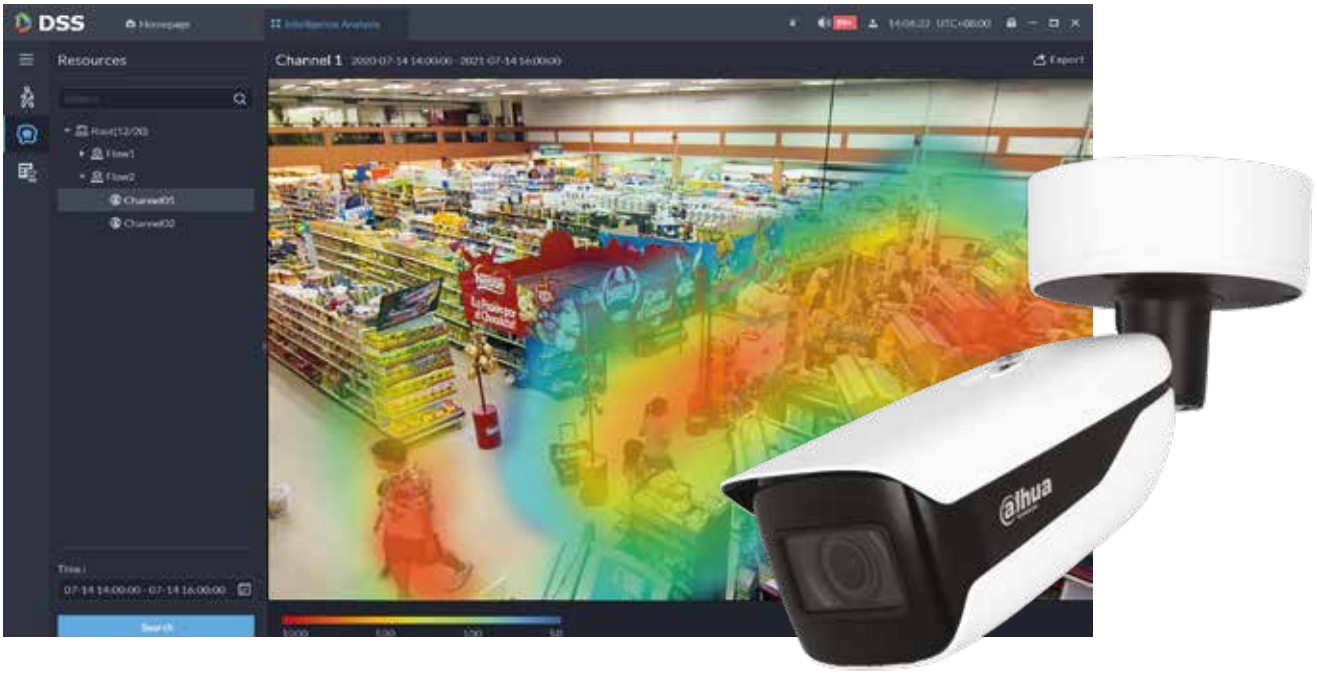
Nastawienie na zrównoważony rozwój

Przeprowadzona przez Axis analiza wykazała, że 60–80% całkowitego wpływu kamer sieciowych na środowisko jest związane z ich zużyciem energii.

Wyzwaniem jest jednak sprawienie, by mniejsze zużycie nie wpłynęło negatywnie na wydajność i niezawodność kamer. Opracowując rozwiązania z zakresu bezpieczeństwa, trzeba stawiać przede wszystkim na to, by urządzenia były niezawodne i w razie potrzeby dostarczyły wiarygodnego materiału dowodowego. Dlatego w Axis nie szczędzimy wysiłków, aby także stosowane przez nią zasilacze były jak najwydajniejsze. Już teraz zasilanie urządzeń odbywa się przy minimalnych stratach w postaci ciepła czy szumu elektrycznego. Dokładamy starań, aby wyznaczyć cele oparte na podstawach naukowych w zakresie emisji dwutlenku węgla. Chcemy jednak, by nasza praca stanowiła branżowy punkt odniesienia w zakresie postępowania zgodnego z zasadami zrównoważonego rozwoju. Koncentrujemy się na trzech strategicznych obszarach – przeciwdziałaniu zmianom klimatycznym, ochronie zasobów naturalnych i ochronie ekosystemów – w ten sposób w wprowadzamy zasady zrównoważonego rozwoju.

Kamera sieciowa AXIS Q6318-LE – jedna z dostępnych kamer z trybem niskiego poboru mocy.

Kamera IPC-HFW71242H-Z-X z rozbudowanym modułem analizy obrazu



Dahua Technology przedstawia zaawansowaną technologicznie kamerę sieciową IPC-HFW71242H-Z-X. Urządzenie wyposażono w najwyższej jakości komponenty optyczne i niezwykle wydajny procesor pozwalający na zaawansowaną analizę obrazu. To sprawia, że kamera sprawdza się w licznych zastosowaniach.

Kamera IPC-HFW71242H-Z-X generuje obraz o rozdzielczości 12 Mpix. Niezwykle czuły przetwornik 1/1,7" zapewnia wysoką jakość obrazu z wieloma detalami, niezależnie od warunków oświetlenia. Ponadto kamerę wyposażono w obiektyw typu motozoom (przysłona F1.6) z zakresem regulacji 2,7–12 mm.

Tym, co wyróżnia model IPC-HFW71242H-Z-X, jest rozbudowany moduł analizy obrazu. Dzięki wielordzeniowemu procesorowi, który ma do dyspozycji 8 GB ROM (pamięć służąca tylko do odczytu) oraz RAM 4 GB, kamera wspiera DHOP *(Dahua Hardware Open Platform),* czyli istnieje możliwość instalacji w pamięci kamery innych aplikacji firm trzecich.

Kamerę wyposażono w funkcje analizy obrazu oparte na algorytmach sztucznej inteligencji opracowane przez Dahua Technology. Są to m.in. detekcja twarzy, rozpoznawanie twarzy i identyfikacja osób na bazie danych zapisanych w pamięci kamery lub na urządzeniu zewnętrznym (NVR, DSS), zliczanie osób wchodzących do wyznaczonej strefy i wychodzących z niej, liczenie ludzi przebywających w strefie z jednoczesnym pomiarem czasu pobytu.

Powyższe funkcje doskonale sprawdzają się nie tylko w zapewnieniu wysokiego poziomu bezpieczeństwa. Informacje, jakich dostarczają algorytmy AI docenią również osoby odpowiedzialne za kreowanie kampanii sprzedażowych. Liczba klientów z podziałem na wiek, płeć, ich obecność w wyznaczonych miejscach – tego typu dane w sposób automatyczny są generowane za pomocą wbudowanych funkcji analitycznych i możliwe do przedstawienia w postaci graficznej lub liczbowej, co ułatwia analizę i dalsze ich przetwarzanie.

Kamery z serii 7 umożliwiają także analizę wizerunku postaci, co pozwala na wykrycie np. braku kasku czy kamizelki ochronnej, a nawet rękawic. To sprawia, że monitoring wizyjny z wykorzystaniem tych urządzeń daje możliwość dbania o bezpieczeństwo nie tylko obiektu, ale także ludzi w nim przebywających.

Obecnie dużą wagę przykłada się do ochrony danych osobowych. Również na tym polu z pomocą przychodzi nowoczesna technologia. Funkcja dynamicznej maski prywatności pozwala na anonimizację twarzy lub całej sylwetki widocznej w kadrze, dzięki czemu można dowolnie kreować politykę prywatności w odniesieniu do systemu dozoru wizyjnego.

Kamera IPC-HFW71242H-Z-X jest niewątpliwie najbardziej uniwersalnym i jednocześnie najbardziej zaawansowanym urządzeniem dostarczającym najwyższej jakości materiał wizyjny z zaawansowaną analizą obrazu. Więcej szczegółów jest dostępnych na stronie https://dahuasecurity.com oraz u Autoryzowanych Partnerów Sprzedaży. ●

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

System antydronowy

Poznańska firma Telbud SA opracowała wielosensorowy system wykrywania i neutralizacji dronów. Firma specjalizuje się w świadczeniu usług w zakresie projektowania, budowy i integracji systemów ochrony technicznej obiektów. Integrację realizuje przy wykorzystaniu autorskiej platformy zarządzania bezpieczeństwem ARGUS klasy PSIM.

Na rozszerzenie możliwości platformy ARGUS o system antydronowy Telbud zdecydował się w odpowiedzi na rosnące wymagania klientów związane z zapewnieniem bezpieczeństwa i ochroną przed inwigilacją.

Działanie systemów antydronowych

System antydronowy wykrywa, identyfikuje i neutralizuje bezzałogowe statki powietrzne (BSP), które zbliżają się do chronionego obszaru. Może składać się z radarów, detektorów RF, sensorów akustycznych, kamer i urządzeń neutralizujących.

W zależności od klasy oraz rodzaju obiektu i terenu, na którym działa system antydronowy, inżynierowie dobierają odpowiednie wyposażenie. W skład czujników i sensorów wchodzą radary o różnych zasięgach, z mechanizmami automatycznej klasyfikacji obiektów, detektory RF operujące na różnych częstotliwościach, sensory akustyczne (również AVS), a także zestawy kamer termowizyjnych i światła widzialnego, wyposażone w mechanizmy klasyfikacji i śledzenia obiektów. Dzięki integracji platforma ARGUS umożliwia współpracę systemów ustalających położenie obiektów BSP, klasyfikując je i określając ich rodzaj.

System inicjuje działania neutralizujące dron z wykorzystaniem jammerów. Bezpośrednio wpływa na zakłócenie czy zerwanie transmisji oraz danych lokalizacyjnych, co powoduje lądowanie lub lokalizację operatora.

Funkcje systemu antydronowego na platformie ARGUS

- System umożliwia operatorowi równoczesne korzystanie z tego samego systemu integrującego wszystkie pozostałe systemy zabezpieczeń działające na terenie obiektu, takie jak systemy dozoru wideo, system włamania i napadu z ochroną perymetryczną, kontrola dostępu czy system przeciwpożarowy.
- Oprogramowanie łączy wszystkie sygnały z poszczególnych elementów systemu, podejmuje decyzję, a następnie wizualizuje zagrożenie (również drona) na mapie.
- System działa w oparciu o podkład graficzny w postaci mapy wektorowej, na której mogą być rozmieszczone wszystkie elementy systemu zgodnie z szerokością i długością geograficzną.
- Do każdego bezzałogowego statku powietrznego przyporządkowywane są jego parametry: protokół komunikacyjny, długość i szerokość geograficzna, wysokość lotu, prędkość poruszania się.
- Na mapie jest również wyrysowywany tor jego lotu.
- Obiekty na mapie wizualizowane są zgodnie z ich kategoriami (pojazd, zwierzę, dron itd.), a na żądanie operatora każda kategoria może zostać wyłączona, aby zwiększyć czytelność dla operatora.
- System umożliwia stworzenie wielu stref ochrony: od najdalszej informującej, że statek powietrzny zbliża się do celu, do najbliższej, gdzie bezpieczeństwo obiektu jest zagrożone.
- W sytuacji zagrożenia system może zareagować automatycznie, włączając zagłuszanie fal radiowych, lub operator systemu może wyzwolić zagłuszanie ręcznie.
- System umożliwia włączanie i wyłączanie poszczególnych zakresów zagłuszania, a także śledzi obiekt latający za pomocą kamery dalekiego zasięgu.
- Jest wyposażony w kamerę światła widzialnego i kamerę termowizyjną w celu lepszego rozpoznania obiektu.
- Wszystkie zdarzenia są zapisywane w dzienniku zdarzeń systemu oraz w dostępnej pamięci i przechowywane przez określony czas; na żądanie zdarzenia mogą zostać odtworzone i wyeksportowane, łącznie z niezbędnymi metadanymi zawierającymi np. parametry i trasę lotu oraz materiał wideo. ●

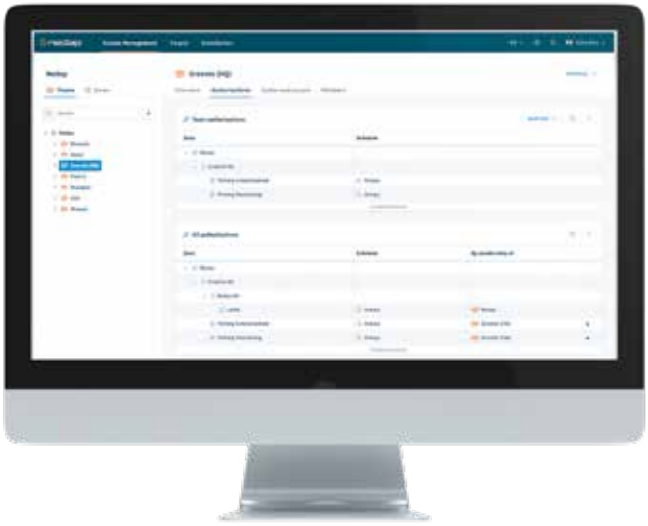
Telbud SA
ul. Krauthofera 23, 60-203 Poznań
telbud@telbud.pl
https://telbud.pl

Access AtWork® - usługa kontroli dostępu w chmurze

Trend przechodzenia na usługi chmurowe jest efektem rosnącego popytu klientów pożądających rozwiązań intuicyjnych i skalowalnych. Było oczywiste, że kwestią czasu było to, zanim wymyślimy własną kontrolę dostępu w chmurze, wymagającą minimalnego wysiłku ze strony użytkownika (i instalatora).

Wielu producentów tradycyjnych systemów kontroli dostępu nadal nie ma ofercie żadnych usług chmurowych. Tę niszę wykorzystują start-upy. Problem polega na tym, że chociaż ich rozwiązania funkcjonujące w chmurze i modelu SaaS mogą na pierwszy rzut oka wyglądać dobrze, to tym młodym firmom brak doświadczenia w zakresie zabezpieczeń. Wydaje się, że lepiej sobie radzą z zaspokajaniem potrzeb rynku konsumenckiego czy mieszkaniowego.

Powoduje to lukę na rynku, którą wykorzystał Nedap, oferując klientom Access AtWork®. Dlaczego? Ze względu na bardzo dobrą reputację w branży zabezpieczeń, bogate doświadczenie lidera rozwiązań chmurowych (w segmencie opieki zdrowotnej) i silną sieć partnerów. Ale być może przede wszystkim dlatego, że mamy 45 lat doświadczenia związanego z kontrolą dostępu!



Warto wyjaśnić, że najnowsze rozwiązanie Access AtWork® w żadnym wypadku nie zastępuje AEOS. Ze względu na rosnące zagrożenie dla infrastruktury krytycznej z jednej strony, z drugiej – chęć zdobycia przez nas dodatkowego udziału w rynku, widzimy miejsce dla dwóch rozwiązań kontroli dostępu, z których każde ma swój cel i idealny profil klienta (ICP).

- **AEOS:** lokalne rozwiązanie dla tych firm, które muszą kontrolować każdy szczegół swojego systemu i chcą samodzielnie zarządzać aktualizacjami oprogramowania. To najlepszy wybór do sektora infrastruktury krytycznej. AEOS zyskał wszystkie niezbędne certyfikaty, jest wyposażony w zaawansowane funkcje bezpieczeństwa i umożliwia integrację z innymi narzędziami, od aplikacji HR, przez urządzenia biometryczne, aż po Video Management Systems.
- **Access AtWork®:** system kontroli dostępu w chmurze oferowany w modelu SaaS dla tych organizacji, które chcą uzyskać pełen nadzór nad obiektem bez inwestowania w rozbudowę infrastruktury IT. Wprowadzenie tego modelu powoduje, że oprogramowanie jest zawsze aktualne, co uwalnia zespoły IT od konieczności czuwania nad tym zadaniem. Access AtWork® idealnie nadaje się do biur wielooddziałowych i zarządzania dynamicznym przepływem osób.

Klienci wybierają Access AtWork®

Jedną z głównych różnic w porównaniu z innymi tego typu systemami chmurowych jest to, że Access AtWork® został wyposażony w najbardziej zaawansowany i najpotężniejszy model autoryzacji. Podjęcie decyzji o tym, jakie osoby potrzebują dostępu do poszczególnych stref, powinno być proste. I teraz jest. Oczywiście dzięki Access AtWork®.

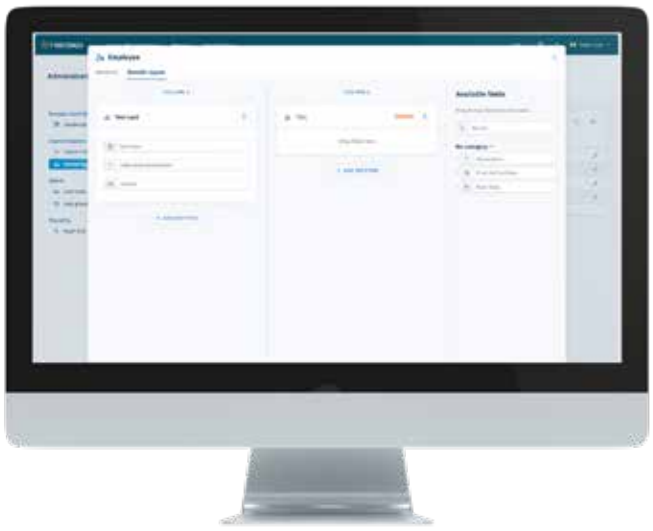
Zastosowanie zaawansowanego modelu autoryzacji powoduje, że administratorzy systemu mogą szybciej niż kiedykolwiek wcześniej konfigurować i modyfikować uprawnienia dostępu i zarządzać

nimi we wszystkich lokalizacjach i budynkach. Skalowanie profesjonalnego systemu KD w wielu lokalizacjach nigdy nie było tak proste.

Użytkownicy, oczywiście w zależności od uprawnień, błyskawicznie otrzymują informacje o tym, kto ma dostęp do jakich pomieszczeń lub stref, w jakich godzinach, a nawet jaki był powód zmiany. Osoba zajmująca się nadawaniem uprawnień może przełączać się na widoki zespołu, strefy lub konto indywidualnego użytkownika. I nie ma już kłopotów po zmianie organizacji stref budynku. Prawa dostępu są automatycznie aktualizowane. Inne opcje to m.in. możliwość tworzenia niestandardowych typów uprawnień, dodawanie pól oraz zakładanie „grup użytkowników". Inteligentne tabele pozwalają w dowolny sposób ukrywać, sortować i filtrować dane.

To oczywiście nie wszystko. Access AtWork® jest wybierany także z tego powodu, że stoi za nim niezawodność wbudowanych kontrolerów drzwi AEOS Blue. Oznacza to, że z wyjątkiem naszego kontrolera drzwi Access AtWork® jest niezależny od sprzętu. Nie trzeba wymieniać istniejących czytników i zamków. Niezależność od konkretnego producenta okazuje się sporą zaletą, gdy nadchodzi czas na modernizację.

Warto wiedzieć, że nasze solidne kontrolery drzwi działają nawet mimo utraty połączenia z siecią. Ponadto każdy ma własne połączenie z chmurą, co zapobiega sytuacji, w której awaria jednego kontrolera powoduje awarię całego systemu. W przypadku innych producentów zdarza się, że kierują wszystkie połączenia do pojedynczej bramy, co może sprawić, że cały system będzie podatny na ataki.



Wspólnie z partnerami osiągamy pożądany wynik

Współpraca z Access AtWork® oferuje szereg korzyści, w tym dostęp do nowych segmentów rynku, łatwość instalacji i konserwacji oraz poprawę rentowności. Rozszerzenie portfolio o nasz system kontroli dostępu w chmurze może przynieść korzyści ze względu na fakt, że rośnie liczba organizacji poszukujących łatwiejszych rozwiązań, elastyczności, jaką daje model SaaS, i braku konieczności inwestowania w zasoby IT. Ważną cechą Access AtWork® jest to, że umożliwia również szybszą i łatwiejszą konfigurację nowych lokalizacji klientów bez konieczności konfigurowania oprogramowania serwerowego. Ponadto Access AtWork® oferuje partnerom atrakcyjny model finansowy, w którym początkowemu zyskowi towarzyszy stały powtarzalny dochód.

Największe korzyści z zastosowania Access AtWork® naszym zdaniem odniosą organizacje rozproszone w wielu lokalizacjach i preferujące usługi typu Software-as-a-Service (SaaS), które odciążają ich zespoły IT.

Sprostanie zadaniu, jakim jest precyzyjna kontrola dostępu, jest niełatwe, a jednocześnie kosztowne w zarządzaniu za pomocą istniejących narzędzi. Dlatego klienci poszukują takich systemów, które pozwolą im nadążyć za rosnącymi wymaganiami, również w zakresie zgodności.

Sektory i branże, które najwięcej zyskają na wprowadzeniu Access AtWork® to organizacje zajmujące się oprogramowaniem i doradztwem IT, FinTechy, międzynarodowe koncerny z licznymi rozproszonymi biurami oraz firmy z branży nieruchomości komercyjnych.

Access AtWork® to produkt oferowany w modelu SaaS, co oznacza, że będzie on regularnie aktualizowany i wzbogacany o nowe funkcje. Jednocześnie Nedap śledzi uważnie wszystkie zagrożenia dla cyberbezpieczeństwa, błyskawicznie wprowadzając aktualizacje chroniące klientów przed zagrożeniem. ●

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

ZKBioCVSecurity – nowa platforma zarządzania bezpieczeństwem

W szybko rozwijającym się środowisku rozwiązań stosowanych w systemach zabezpieczeń niezawodność i integracja systemów mają ogromne znaczenie. ZKBioCVSecurity firmy ZKTeco to wszechstronna wielomodułowa platforma internetowa, która bezproblemowo spełnia wyśrubowane wymagania użytkowników w zakresie bezpieczeństwa.
Marek Piotrowski

Podstawowe zalety ZKBioCVSecurity

1. Kompleksowość rozwiązania: ZKBioCVSecurity to szereg modułów dopasowanych do potrzeb użytkownika, takich jak kontrola dostępu, obsługa parkingu, rejestracja czasu pracy, zarządzanie recepcją i przepływem gości, FaceKiosk, inteligentne zarządzanie wideo, wykrywanie masek, rejestracja wysokiej temperatury osób wchodzących, nadzór pracy patroli.
2. Integracja danych: platforma płynnie agreguje dane i prezentuje je na pulpicie nawigacyjnym, ułatwiając menedżerom szybkie i świadome podejmowanie decyzji.
3. Inteligentny nadzór wideo: wykorzystując technologię *computer vision* i aplikacje stosowane w inteligentnej analizie obrazu, system generuje zaawansowane ostrzeżenia, umożliwiając szybką reakcję na zdarzenia i ich dokładną weryfikację.

Ponadto ZKBioSecurity oferuje

DOSTĘP DO SYSTEMU PRZEZ INTERNET: użytkownicy mogą zdalnie zarządzać tysiącami terminali i kontrolerów za pośrednictwem platformy internetowej, do której mają zapewniony dostęp z dowolnego miejsca na świecie.

INTEGRACJĘ Z OPROGRAMOWANIEM HOTELOWYM ZKBIOHA: zapewnia synchronizację przesyłanych danych w czasie rzeczywistym oraz ochronę ciągłości działania obu systemów.

KONTROLĘ WIDEO PERSONELU: system wyświetla na ekranie w czasie rzeczywistym obraz wideo w celu identyfikacji pracowników i osób obcych.

MOŻLIWOŚĆ INTELIGENTNEJ ANALIZY SCEN: umożliwia wyszukiwanie celu, analizę trajektorii poruszającego się personelu, liczenie osób, kontrolę obecności czy ochronę perymetryczną.

BEZPIECZEŃSTWO DANYCH: wykorzystuje bezpieczne protokoły komunikacyjne stosowane w sieciach komputerowych, w tym HTTPS, TLS1.2, RSA2048 i AE256.

AUTOMATYCZNE POWIADOMIENIA: po skonfigurowaniu serwera poczty system może wysyłać automatyczne powiadomienia do wyznaczonych odbiorców za pomocą e-maili lub powiadomień przez WhatsApp, Line, Amazon SNS i SMS.

REJESTR OPERACJI: użytkownicy systemu mogą śledzić i przeglądać listę wykonanych operacji i alertów, w tym kto je wykonał oraz co, gdzie i kiedy zostało zrobione.

INTERFACE API: ZKTeco udostępnia API w pełni zgodne ze standardem REST do integracji z rozwiązaniami innych firm.

HYBRYDOWĄ WERYFIKACJĘ BIOMETRYCZNĄ: platforma obsługuje różne weryfikacje biometryczne, w tym linii papilarnych, rozpoznawanie linii i naczyń krwionośnych dłoni oraz rozpoznawanie twarzy.

ZKBioCVSecurity to rozwiązanie przeznaczone głównie do projektów średniej i dużej wielkości, ze szczególnym naciskiem na jego zastosowanie w sektorze bezpieczeństwa publicznego. Istotną cechą systemu jest integracja z urządzeniami zarówno firmy ZKTeco, jak i innych marek, w tym z systemami alarmowymi firm Bosch i Risco. Jeśli zajdzie potrzeba wdrożenia integracji z systemami innych producentów, może to nastąpić szybko i sprawnie. Ta elastyczność upraszcza proces wdrażania systemu przez integratorów i użytkowników końcowych. ●

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

ZKTeco

BĄDŹ PRO

Seria ProMA

ProMA

ProMA -QR

ProMA -RF

RFID QR PALEC DŁOŃ TWARZ

IP66 WATERPROOF

Wodoodporność **IP66**

IK07 VANDAL PROOF

Wandaloodporność **IK07**

Kompatybilne z platformą

ZKBio CVSecurity

Personel	Kontrola Dostępu	RCP	Windy	Goście	Parking	Wideo	Biuro
Alarm ppoż	Przejścia kontrolowane	FaceKiosk	Pomiar temperatury	Patrol Ochrony	Monitor danych	Automatyka budynkowa	Włamanie

www.zkteco.eu

Zasilacze UPS z serii PowerWalker

BlueWalker GmbH, ekspert w dziedzinie zasilaczy UPS, AVR i falowników, przedstawia VFI 5000 EVS – nową serię zasilaczy PowerWalker, profesjonalnych urządzeń łączących niezawodność i bezpieczeństwo z efektywnością energetyczną oraz doskonałym stosunkiem wydajności do ceny.

W nowej serii jednofazowych zasilaczy awaryjnych typu online zastosowano technologię podwójnej konwersji zapobiegającą zanikowi zasilania, co czyni je idealnym rozwiązaniem do urządzeń o znaczeniu krytycznym. Wszystkie zasilacze z serii VFI 5000 EVS są wyposażone w bardzo wydajną ładowarkę AC, która może pracować nie tylko z tradycyjnymi akumulatorami kwasowo-ołowiowymi, ale także z akumulatorami litowymi. Jest to szczególnie przydatne w rozwiązaniach wymagających długiego czasu podtrzymania zasilania.

Seria zasilaczy VFI 5000 EVS może współpracować z systemem akumulatorów PowerWalker LiFe, dzięki czemu zapewnia długi czas podtrzymania zasilania w bezpieczny, stabilny i kompaktowy sposób. Zasilacze umożliwiają pracę równoległą maksymalnie 9 urządzeń, a w przypadku połączenia równoległego mogą współdzielić baterie. Mogą też pracować w konfiguracji trójfazowej, do czego niezbędne jest zastosowanie trzech jednostek. Ponadto mogą współpracować z agregatami prądotwórczymi.

UPS online z system akumulatorów LiFe może długo podtrzymywać zasilanie z baterii litowo-żelazowo-fosforanowej (LFP). W porównaniu do akumulatorów kwasowo-ołowiowych i akumulatorów litowych LFP charakteryzują się dłuższą żywotnością, brakiem konieczności konserwacji i wyjątkowym bezpieczeństwem. Akumulatory są lżejsze i mają lepszą wydajność ładowania oraz rozładowania.

Połączenie zasilaczy z serii VFI 5000 EVS z system akumulatorów LiFe umożliwia łatwą budowę instalacji awaryjnego zasilania i świetny czas podtrzymania, a do tego szybkie ładowanie. Dodatkowymi atutami są wbudowany system zarządzania baterią i głębokość rozładowania 90%. Jest to najlepsze rozwiązanie do zastosowań wymagających nieprzerwanego zasilania, m.in. w przypadku transakcji płatności, ochrony przed utratą danych i ciągłej pracy systemów zabezpieczeń.

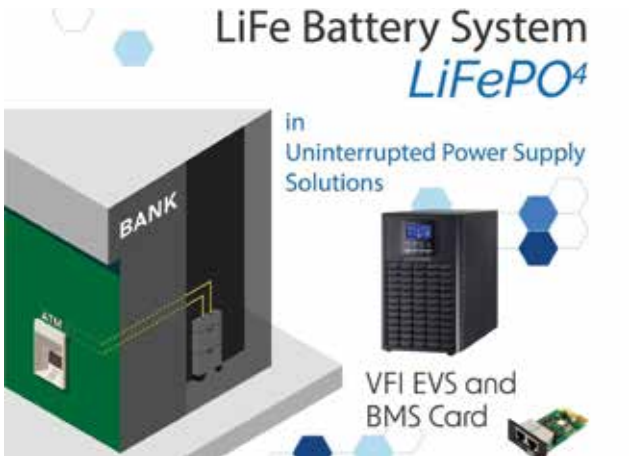
Najważniejsze zalety serii VFI 5000 EVS:

- inteligentne gniazdo na karty komunikacyjne,
- współczynnik mocy wyjściowej 1,0,
- bardzo wydajna ładowarka (do 60 A),
- zoptymalizowane zarządzanie baterią (OBM) – w celu wydłużenia żywotności baterii,
- współpraca z systemem LiFe PowerWalker i akumulatorami litowymi innych firm,
- możliwość pracy równoległej (do 9 jednostek),
- możliwość dzielenia baterii w przypadku połączenia równoległego,
- możliwość pracy w konfiguracji trójfazowej (wymagane >3 jednostki),
- obsługa generatorów.

Seria zasilaczy UPS online VFI 5000 EVS znakomicie sprawdzi się w obiektach handlowych, w firmach z różnych gałęzi gospodarki stosujących rozwiązania informatyczne i teleinformatyczne, w tym w przemyśle i obiektach infrastruktury krytycznej, w placówkach służby zdrowia do zasilania sprzętu medycznego i wszędzie tam, gdzie jest potrzebne ciągłe zasilanie urządzeń. Na urządzenia PowerWalker firma oferuje 24-miesięczną gwarancję.

Więcej informacji udziela przedstawiciel firmy Impakt, dystrybutor rozwiązań PowerWalker w Polsce. ●

IMPAKT SA
ul. Stanisława Lema 16, 62-050 Mosina
https://impakt.com.pl/
e-mail: bartlomiej.kolodziej@impakt.com.pl



BlueWalker GmbH

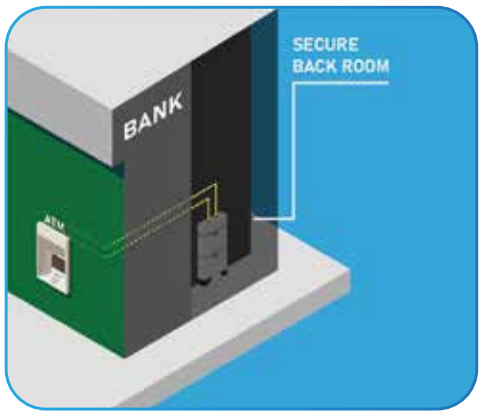
BlueWalker GmbH to producent zasilaczy UPS, AVR i falowników. Firma ma ponad 15-letnie doświadczenie i dysponuje rozległą siecią dystrybutorów działających w całej Europie, na Bliskim Wschodzie i w Afryce.

Dzięki portfolio obejmującemu ponad 400 modeli z 50 serii BlueWalker oferuje rozwiązanie dla większości wykorzystania UPS: od urządzeń przeznaczonych do zastosowań domowych po systemy o wysokiej wydajności i dużej mocy do profesjonalnych zastosowań komercyjnych.

VFI EVS

DOŚWIADCZ TURBODOŁADOWANEJ WYDAJNOŚCI

- Długie czasy podtrzymań
- Szybki i prosty montaż
- Możliwość instalacji w punktach w których brak miejsca na standardowe regały bateryjne i agregaty prądotwórcze
- Łatwe możliwości rozbudowy



VFI 5000 EVS

LIFE BATTERY SYSTEM 48-100

VFI 5000 EVS

- Współpracuje z zewnętrznymi bateriami litowymi
- Praca równoległa do 9 jednostek (od 5kVA do 45kVA)
- Możliwość pracy w konfiguracji trójfazowej
- Potężna ładowarka do 60A

LIFE BATTERY SYSTEM 48 100

- Żywotność baterii przewidziana na 12-15 lat
- Szybkie ładowanie (1 godzina do 90% naładowania)
- Możliwość pracy do 10 jednostek aby zwiększyć czas podtrzymania

Liczba Battery Packów	250 W	500 W	1000 W	1500 W	2000 W	2500 W
1	1080	540	270	180	135	108
2	2160	1080	540	360	270	216
3	3240	1620	810	540	405	324
4	4320	2160	1080	720	540	432

Szacunkowe czasy podtrzymań w minutach, w zależności od poboru mocy (W) podłączonych urządzeń

Jak w każdym wydaniu „A&S Polska", tak i w tym numerze prezentujemy mapę dużych inwestycji, które są obecnie w toku lub dopiero się rozpoczynają. Wybraliśmy te z przewidywanym terminem zakończenia nie wcześniejszym niż II kwartał 2024 r. Chcemy podkreślić, że nasz wybór nie ogranicza się do jednej branży przemysłowej. Szukamy przede wszystkim dużych inwestycji realizowanych przez uznane firmy, które mogą stwarzać możliwości współpracy dla firm z sektora bezpieczeństwa. Zachęcamy także do zapoznania się z informacjami zamieszczonymi w poprzednich wydaniach „A&S", gdzie omówiliśmy inne projekty długoterminowe.

Adela Prochyra, a&s Polska

Mapa inwestycji

ATREM SA

Co: BUDOWA STACJI 110/15 KV LESZNO ZACHÓD WRAZ Z LINIĄ ZASILAJĄCĄ, TRANSFORMATORAMI ORAZ BUDOWĄ WYPROWADZEŃ SN
Gdzie: Leszno
Kiedy: Brak informacji o terminie wykonania
1

Co: WYBUDOWANIE STACJI ELEKTROENERGETYCZNEJ 110KV RS SIEDLISKA, UMOŻLIWIAJĄCEJ POŁĄCZENIE SIECI INSTALACJI PODSTACJI TRAKCYJNEJ SIEDLISKA PKP ENERGETYKA SA
Gdzie: Białystok
Kiedy: 24 lipca 2024 r.
2

BUDIMEX

Co: BUDOWA TERMINALA INSTALACYJNEGO DLA MORSKICH FARM WIATROWYCH
Gdzie: Świnoujście
Kiedy: grudzień 2024 r.
3

Co: MODERNIZACJA STADIONU MIEJSKIEGO W ZĄBKOWICACH ŚLĄSKICH
Gdzie: Ząbkowice Śląskie
Kiedy: grudzień 2024 r.
4

Co: MODERNIZACJA ZABYTKOWEGO DWORCA KOLEJOWEGO PKP W GRUDZIĄDZU
Gdzie: Grudziądz
Kiedy: 20 miesięcy od dnia podpisania umowy (9.08.2023 r.)
5

ELEKTROTIM SA

Co: ROZBUDOWA SYSTEMU ALARMOWEGO W MAGAZYNACH ŚRODKÓW BOJOWYCH ORAZ NA OBWODNICY KOMPLEKSU WRAZ Z WYMIANĄ OŚWIETLENIA W KOMPLEKSIE WOJSKOWYM K-0596
Gdzie: Goławice
Kiedy: 540 dni od dnia podpisania umowy (3.10.2023 r.)
6

ENERGOAPARATURA

Co: WYKONANIE KOMPLETNYCH ROBÓT BUDOWLANYCH ELEKTRYCZNYCH I ENERGETYCZNYCH, W TYM OPRACOWANIE PROJEKTU WYKONAWCZEGO DLA LINII KABLOWYCH SN, W RAMACH BUDOWY „FARMY WIATROWEJ RUSIEC II" REALIZOWANEJ DLA VER LS-36 SP. Z O.O.
Gdzie: Rusiec, woj. łódzkie
Kiedy: 7 lipca 2024 r.
7

ERBUD

Co: EUROPEJSKIE CENTRUM FILMOWE CAMERIMAGE – WBUDOWANY KAMIEŃ WĘGIELNY
Gdzie: Toruń
Kiedy: 22 miesiące od października 2023 r.
8

MOSTOSTAL PŁOCK

Co: PREFABRYKACJA I MONTAŻ SZEŚCIU ZBIORNIKÓW STALOWYCH O POJEMNOŚCI 10 000 M^3 KAŻDY
Gdzie: Czechy
Kiedy: 1.04.2024–01.10.2025
9

MIRBUD S.A.

Co: HOTEL MARKI CAMPANILE W SĄSIEDZTWIE LOTNISKA IM. F. CHOPINA W WARSZAWIE
Gdzie: Warszawa
Kiedy: styczeń 2026 r.
10

Co: KRAKOWSKIE CENTRUM MUZYKI – WMUROWANY AKT EREKCYJNY
Gdzie: Kraków
Kiedy: III–IV kwartał 2025 r.
11

MOSTOSTAL WARSZAWA

Co: REKTORAT POLITECHNIKI POZNAŃSKIEJ
Gdzie: Poznań
Kiedy: do 36 miesięcy od dnia podpisania umowy (28.09.2023), w tym projektowanie, wybudowanie budynku wraz z uzyskaniem prawomocnego pozwolenia na użytkowanie powinny być wykonane w terminie do 24 miesięcy + testy akceptacyjne prowadzone przez 12 miesięcy
12

UNIBEP

Co: CENTRUM INNOWACJI I CYBERBEZPIECZEŃSTWA WAT
Gdzie: Warszawa
Kiedy: ok. 4 lata
13

Mniej fałszywych alarmów pożarowych

Wykorzystanie możliwości oprogramowania central oraz elementów instalacji sygnalizacji pożarowej pozwala znacząco ograniczyć liczbę fałszywych alarmów.

Mariusz Radoszewski

Zadaniem systemów sygnalizacji pożarowej jest wykrycie zagrożenia, wskazanie jego lokalizacji, a następnie powiadomienie o tym fakcie obsługę i użytkowników. Oczywiście im szybciej, tym lepiej, czemu służy automatyzacja procesu rozpoznania zagrożenia pożarowego. Aby wprowadzić taką automatyzację, należy najpierw skupić się na zrozumieniu zjawisk towarzyszących pożarowi, by potem móc je zidentyfikować. Najważniejsze zjawiska pojawiające się podczas pożaru to:

- utlenianie materiałów,
- wydzielanie energii cieplnej,
- unoszenie cząsteczek oderwanych podczas utleniania,
- degradacja spalanego medium,
- przy dużych energiach pożaru z występowaniem płomienia – wytwarzanie promieniowania elektromagnetycznego w zakresie podczerwieni i/lub ultrafioletu (niezależnie od światła widzialnego).

Aby móc wykryć pożar we wczesnym stadium za pomocą automatycznego procesu rozpoznawania zagrożenia pożarowego, należy określić, które z wymienionych zjawisk będą mierzone i analizowane.

Wykrywanie dymu

Wykrywanie dymu to najczęściej stosowany sposób pracy automatycznych ostrzegaczy pożarowych. Może być realizowane przez:

- rozproszenie wiązki światła w powietrzu (efekt Tyndalla),
- zmniejszenie przejrzystości powietrza (zmiana gęstości optycznej powietrza).

Dla obu powyższych metod sosowane są czujki dymu o zupełnie innej konstrukcji.

Detekcja dymu z wykorzystaniem efektu Tyndalla

Czujki dymu wykorzystujące zjawisko rozproszenia wiązki światła to najczęściej stosowane rozwiązanie. Zasada działania takiej czujki opiera się na zjawisku rozproszenia i odbicia światła od cząsteczek dymu *(rys. 1)*. Wiązka światła wysyłana jest ze specjalnie zbudowanego nadajnika. Po odbiciu od cząsteczek zawieszonych w powietrzu trafia do elementu odbiorczego. Proces ten przebiega wewnątrz specjalnej komory, zwanej też labiryntem, w której emitowane jest światło podczerwone lub ultrafioletowe.

Detekcji dymu za pomocą pomiaru przejrzystości powietrza

W tej metodzie również jest wykorzystywane źródło światła. W tym przypadku dokonuje się pomiaru, o jaką wartość jest mniejszy strumień światła trafiający do elementu odbiorczego *(rys. 2)*. Czujki tego typu są nazwane liniowymi czujkami dymu.

Analiza temperatury i detekcja płomienia

Kolejnym zjawiskiem najczęściej towarzyszącym pożarowi jest temperatura. Dla właściwej interpretacji zjawisk pożarowych temperatura może być analizowana w następujący sposób:

- przekroczenie określonej wartości, czyli praca statyczna,
- zmiana (przyrost lub spadek) o określony poziom w jednostce czasu, czyli praca różnicowa.

Uzupełnieniem klasycznych metod detekcji jest także detekcja płomienia. Czujki do tego stosowane mają szczególną konstrukcję. Ich sposób działania można porównać do kamer obserwujących określony obszar i reagujących na pojawienie się promieniowania elektromagnetycznego, odpowiadającego widmu światła w zakresie podczerwieni i/lub nadfioletu towarzyszącego płomieniowi *(rys. 3)*.

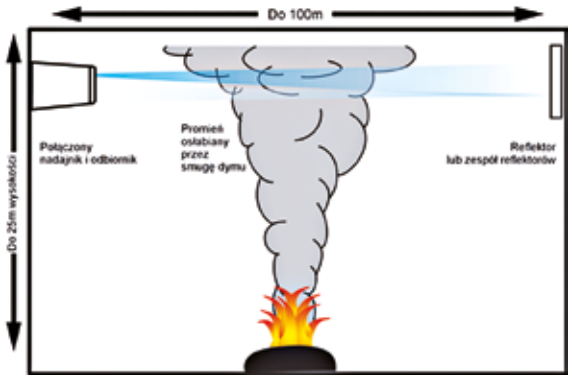
Czynniki zwodnicze – przyczyny fałszywych alarmów

Każde ze wspomnianych urządzeń może niestety spowodować uruchomienie fałszywego alarmu. W przypadku punktowych czujek dymu, czyli bazujących na rozproszeniu światła, do tzw. czynników zwodniczych należą m.in.:

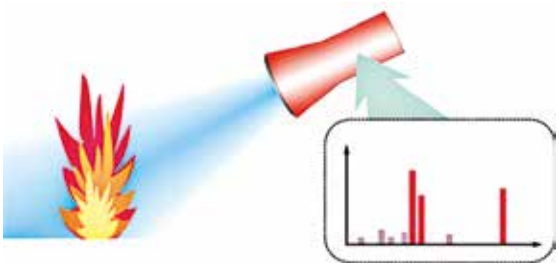
- pył różnego pochodzenia (będący np. skutkiem szlifowania ścian),
- duża ilość kurzu w powietrzu,
- para wodna kondensująca się wewnątrz komory czujki i odbijająca światło (np. w wyniku zmian temperatury),
- cząsteczki związków lotnych/aerozoli niewidocznych gołym okiem (np. ze źródeł),
- owady.

Nie do końca jest prawdą, że czujki dymu nie reagują na dym papierosowy. On także rozprasza światło, choć w niewielkiej ilości, i szybko ulega rozrzedzeniu. Działanie czujki może ulec zakłóceniu także w wyniku pojawienia się sztucznego dymu, specjalnie generowanego przez wytwornicę. Należy także pamiętać, że wiele lotnych związków chemicznych, niewidocznych gołym okiem, doskonale odbija światło w zakresie nadfioletu. Pojawienie się takich związków w obszarze dozorowanym przez czujkę dymu spowoduje uruchomienie fałszywego alarmu.

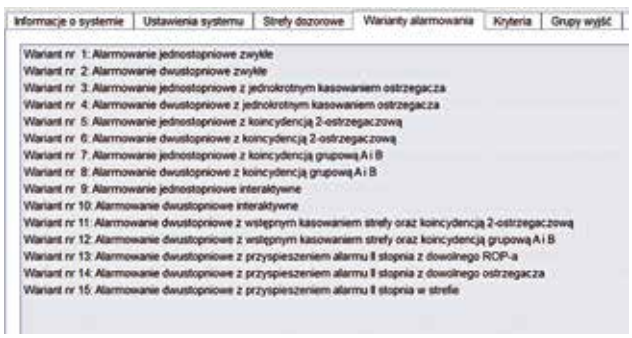
Rys. 1. Zasada działania czujek optycznych dymu



Rys. 2. Zasady działania liniowej czujki dymu



Rys. 3. Przykład pracy czujki płomienia



Rys. 4. Dostępne warianty alarmowania

W przypadku czynników zakłócających pracę czujek temperatury najczęściej mamy do czynienia z nagłą zmianą temperatury wokół sensora lub przekroczeniem progu temperatury, np. w wyniku awarii systemu klimatyzacji.

Natomiast czujki płomienia zazwyczaj są narażone na czynniki zwodnicze wykorzystujące „słabe punkty", wynikające z budowy czujek i sposobu ich pracy. Są to bezpośrednio padające lub odbite promienie słoneczne (zakres ultrafiolet i/lub podczerwień), prace spawalnicze (zakres ultrafiolet), lampy dezynfekcji i/lub oświetlenie korzystające z lamp wyładowczych (zakres ultrafiolet), elementy grzejne – promienniki ciepła (zakres podczerwień).

Eliminowanie fałszywych alarmów

Czujki pożarowe mają za zadanie wykrywać właściwe dla swojego typu medium pożarowe, jakim jest dym, temperatura lub płomień.

Gdy weźmiemy pod uwagę czynniki zwodnicze, a także pożary, które nie przewidują typowych zjawisk spodziewanych w wyniku pożaru, dochodzimy do wniosku, że skupienie się na pojedynczym zjawisku fizycznym towarzyszącym pierwszej fazie pożaru nie zawsze jest właściwe i może spowodować nadwrażliwość na czynniki zwodnicze bądź całkowitą niewrażliwość na pewną grupę zjawisk pożarowych.

Dlatego należy tak dobierać czujki, aby funkcjonowały we właściwym zakresie wykrywanych mediów w celu uruchomienia szybkiego alarmu. Osiągnięcie tego jest możliwe dzięki:

- doborowi czujek pożarowych do warunków, w jakich mają pracować,
- ustawieniu właściwych parametrów pracy urządzeń za pomocą dobrania odpowiedniego rodzaju sensorów, określeniu zależności między nimi i ustawieniu poziomu czułości, z jaką mają pracować.

Warianty alarmowania

Alarmowanie, czyli zgłoszenie zagrożenia pożarowego, jest realizowane przez centralę sygnalizacji pożarowej wraz ze wskazaniem lokalizacji.

Ta strefa dozorowa jest jednostką określającą miejsce powstania pożaru. Znajdujące się w tym obszarze czujki lub ręczne ostrzegacze pożarowe wspólnie wskazują odpowiedni komunikat.

W przypadku systemów POLON-ALFA, czyli POLON 6000, POLON 3000 i POLON 4000, strefy dozorowe pracują w ramach ustawień (konfiguracji) dostępnych wariantów alarmowania. Domyślny wariant to alarmowanie dwustopniowe zwykłe. Ręczne ostrzegacze pożarowe standardowo działają w ramach alarmowania jednostopniowego zwykłego, niezależnie od wariantu alarmowania przypisanego do strefy. Dostępne warianty alarmowania pokazano na *rys. 4.*

Biorąc pod uwagę właściwości elementów detekcyjnych i oprogramowania central sygnalizacji pożarowej, można założyć, że odpowiedni wybór trybu pracy czujek i wariantu alarmowania pozwoli na działanie systemu w taki sposób, aby maksymalnie ograniczyć fałszywe alarmy. ●

POLON-ALFA S.A.
ul. Glinki 155
85-861 Bydgoszcz
www.polon-alfa.pl

Jubileuszowa edycja Ogólnopolskich Dni Zintegrowanych Systemów Bezpieczeństwa Pożarowego Schrack Seconet i Partnerzy

4–5 października 2023 r. w hotelu Windsor w Jachrance odbyła się kolejna 10. edycja Ogólnopolskich Dni Zintegrowanych Systemów Bezpieczeństwa Pożarowego – Schrack Seconet i Partnerzy. Odnotowano kolejny rekord. W tegorocznym szkoleniu wzięło udział ponad 600 osób!

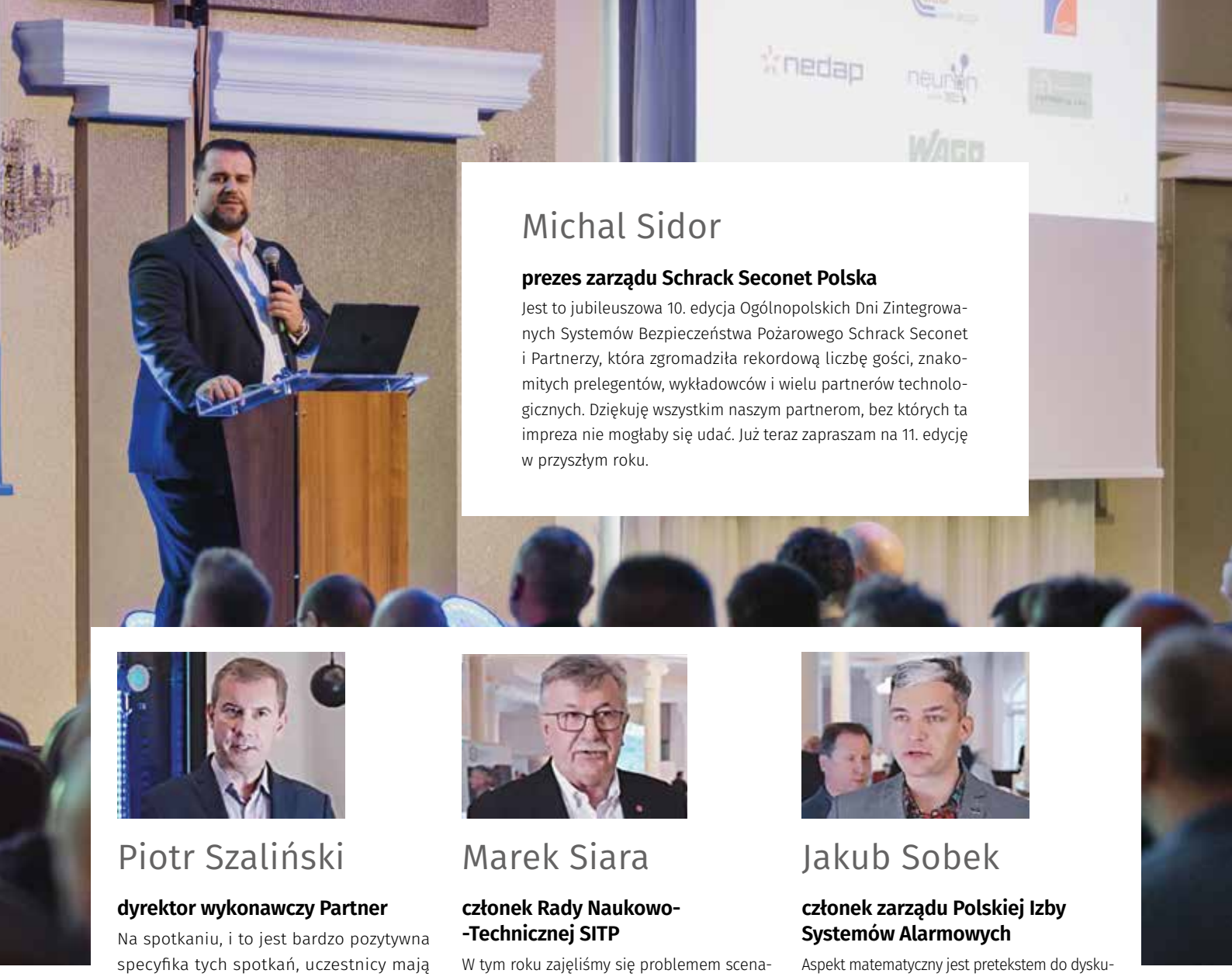
Partnerami Technologicznymi tegorocznej edycji szkolenia były firmy: Atest Gaz, BELIMO Siłowniki, C-AIM, GRAS, InGas, Nedap Security Management, PARTNER, WAGO.

Wsparcie merytoryczne 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 oraz eksperci reprezentujący Centrum Naukowo-Badawcze Ochrony Przeciwpożarowej – Państwowy Instytut Badawczy.

Krzysztof Kunecki

dyrektor ds. technicznych Schrack Seconet Polska

Pokazaliśmy uczestnikom zintegrowany system bezpieczeństwa pożarowego, w którego skład wchodzi system sygnalizacji pożarowej i sterowania urządzeniami przeciwpożarowymi, system integrujący urządzenia przeciwpożarowe SIS-FIRE oraz dźwiękowy system ostrzegawczy APS-APROSYS i centralę sterująco-zasilającą urządzenia przeciwpożarowe SIS-POWER. Zaprezentowaliśmy też innowacyjne rozwiązanie dotyczące monitorowania skuteczności realizacji sterowań wynikających ze scenariusza pożarowego. To kluczowa kwestia związana z zarządzaniem w przypadku alarmu pożarowego, żeby wykrywać wszelkie anomalie związane z tym, co nie zostało uruchomione w odniesieniu do zaplanowanego scenariusza realizacji sterowań.



Michal Sidor

prezes zarządu Schrack Seconet Polska

Jest to jubileuszowa 10. edycja Ogólnopolskich Dni Zintegrowanych Systemów Bezpieczeństwa Pożarowego Schrack Seconet i Partnerzy, która zgromadziła rekordową liczbę gości, znakomitych prelegentów, wykładowców i wielu partnerów technologicznych. Dziękuję wszystkim naszym partnerom, bez których ta impreza nie mogłaby się udać. Już teraz zapraszam na 11. edycję w przyszłym roku.

Piotr Szaliński

dyrektor wykonawczy Partner

Na spotkaniu, i to jest bardzo pozytywna specyfika tych spotkań, uczestnicy mają możliwość w małych grupach w sesjach warsztatowych pogłębić wiedzę o najnowszych technologiach. Prezentowaliśmy studium przypadku w trudnych akustycznie pomieszczeniach.

Marek Siara

członek Rady Naukowo-Technicznej SITP

W tym roku zajęliśmy się problemem scenariuszy pożarowych, bo całe szkolenie dotyczyło przede wszystkim organizacji działania urządzeń przeciwpożarowych w obiekcie tak, aby był bezpieczny. A ta sprawa organizacji to jest nic innego, jak realizacja scenariuszy pożarowych.

Jakub Sobek

członek zarządu Polskiej Izby Systemów Alarmowych

Aspekt matematyczny jest pretekstem do dyskusji, bo tak naprawdę nie ma wzoru, który pozwoli nam przemnożyć dwie rzeczy przez siebie i dać odpowiedź, czy już powinniśmy inwestować, czy też nie. Ja akurat tłumaczyłem, jak za pomocą dość prostych narzędzi matematycznych można ryzyko opisać po to, aby te rozwiązania były łatwiejsze i można było dać odpowiedź, co tak naprawdę jest nam potrzebne, aby obiekt prawidłowo zabezpieczyć.

Michał Krawczykowski

key account manager Gras

Na spotkaniu prezentowaliśmy innowacyjny system do ochrony miejsc postojowych pojazdów elektrycznych. System, który polega na wczesnej detekcji i automatycznym gaszeniu pożarów, zapewnia ochronę mienia znajdującego się po bokach tego pojazdu.

Wojciech Leciński

manager rynku budownictwa WAGO

Na spotkaniu poruszamy się na dwóch warstwach. Jedna to ta czysto merytoryczna i bardzo mi się podoba to, że na sesji plenarnej możemy przeprowadzić żywy scenariusz. I druga warstwa integracyjno-biznesowa, która się odbywa równolegle.

Wojciech Erhard

prezes zarządu Belimo Siłowniki

Prezentowaliśmy integrację naszych elementów wykonawczych, czyli siłowników do klap wentylacji pożarowej, klap odcinających z systemem Schrack w budynkach inteligentnych.

Monika Kołodziejczyk

prezes zarządu C-aim

W tym roku na warsztatach zdecydowaliśmy się pokazać dwie rzeczy: jedna to mobilne wykorzystanie rozwiązań w telewizji dozorowej, czyli mobilne kamery. I drugie ciekawe rozwiązanie to bezprzewodowe i bezbateryjne zamki, które mogą być również uzupełnieniem systemów zabezpieczeń.

Paweł Gancarczyk

kierownik Jednostki Certyfikującej CNBOP-PIB

Bardzo cenna inicjatywa, która daje środowisku, a więc projektantom, instalatorom i konserwatorom zabezpieczeń przeciwpożarowych możliwość zapoznania się z nowymi rozwiązaniami technologicznymi i wykorzystanie tej wiedzy w codziennej pracy.

Kamil Sągol

specjalista ds. techniczno-handlowych INGAS

Coraz więcej naszych klientów jest zainteresowanych integracją wszystkich systemów, które posiadają, w tym gaszenia gazem, z naszej oferty. Taka integracja pozwala z jednego miejsca zarządzać wszystkimi systemami nawet na obiektach, które znajdują się w różnych miejscach kraju. To duże ułatwienie, ale też możliwość nadzorowania tego, co klient posiada.

Błażej Ożga

regional consultant manager CEE Nedap Security Management

Zależało nam, żeby pokazać wspólne działanie wszystkich urządzeń. Systemy powinny oferować otwartość, swobodę integracji i używanie protokołów, które umożliwiają łączenie się z innymi systemami współistniejącymi w budynku.

Krzysztof Kawecki

inżynier bezpieczeństwa pożarowego Protect

Prowadziłem dziś prezentację dotycząca koincydencji. Innego ujęcia z perspektywy projektanta instalacji bezpieczeństwa pożarowego, systemów sygnalizacji pożarowej i z perspektywy inżyniera rzeczoznawcy ds. pożarowych. Chciałem wskazać te dwa różne podejścia do tego samego tematu i punkt styku. Temat jest ważny, bo uważam, że te dwa środowiska rozmawiają ze sobą, czasem nie rozumiejąc się nawzajem. Myślę, że prezentacja pomaga lepiej się porozumieć automatykom pożarnictwa ze środowiskiem inżynierów rzeczoznawców ds. ppoż. Myślę, że jest to krok w dobrym kierunku i możliwość wymiany poglądów.

Wiesław Sochacki

przedstawiciel ds. sprzedaży technicznej Atest Gaz

Tutaj w bardzo dużym skrócie pokazaliśmy możliwości naszych urządzeń. Generalnie praca związana z doborem systemu detekcji gazu jest rozłożona w czasie. Polega najpierw na sprawdzeniu warunków, w jakich ten system będzie funkcjonował na obiekcie. Później musimy się zastanowić, jakie wymagania ma spełniać. Następnie musimy przygotować dokumentację projektową, która będzie zgodna z wytycznymi inwestora, i dopiero na końcu możemy przystąpić do przygotowania systemu do zamontowania na danym obiekcie.

Janusz Sawicki

prezes zarządu IBP NODEX

Konferencji tego rodzaju nie jest w Polsce wiele. Cieszę się, że widzę dużo młodych ludzi. Najważniejszą korzyścią ze spotkań jest wykorzystanie najnowszych zdobyczy nauki, fizyki po to, aby w jak najwcześniejszej fazie wykryć zagrożenia pożarowe. ●

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

ALNET SYSTEMS

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

www.alnetsystems.com

Jesienny BootCamp

Za nami 6. edycja szkolenia strategiczno-terenowego, które odbyło się na początku października br. W przepięknych okolicznościach przyrody hotelu Manor House w Chlewiskach spotkali się security managerowie, aby w praktyce poznać najnowsze rozwiązania firm partnerskich i wymienić się doświadczeniami w gronie najlepszych w kraju specjalistów ds. bezpieczeństwa.

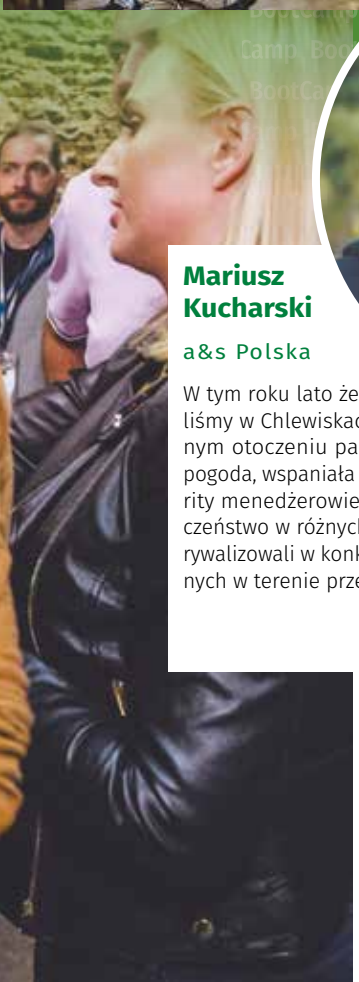
Partnerami jesiennej edycji były firmy: Axis Communications, Genetec, Linc Polska, Securitas i STid.

Drugiego dnia uczestnicy wzięli udział w szkoleniu warsztatowym w formule gry decyzyjnej z autorskim scenariuszem Jana T. Grusznica.

Artur Nowakowski

Linc Polska

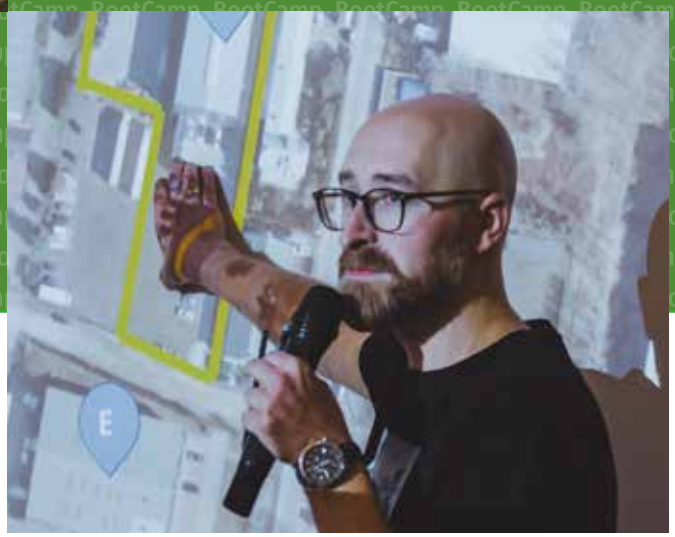
Zabraliśmy naszych uczestników w ciekawą podróż przez fakty i mity dotyczące systemów zabezpieczeń. Omówiliśmy tematy termowizji, systemów radarowych i kontroli dostępu oraz inne poboczne zagadnienia dotyczące szeroko rozumianych systemów zabezpieczeń. Widzimy, że jest potrzeba zdobywania nowych doświadczeń i wdrażania nowych rozwiązań, bo wielu klientów ma problemy z różnymi zagadnieniami. A są na nie rozwiązania.



Mariusz Kucharski

a&s Polska

W tym roku lato żegnaliśmy w Chlewiskach w pięknym otoczeniu parkowo-pałacowym. Była wspaniała pogoda, wspaniała atmosfera i świetni uczestnicy. Security menedżerowie i osoby odpowiedzialne za bezpieczeństwo w różnych firmach i instytucjach całego kraju rywalizowali w konkurencjach technicznych przygotowanych w terenie przez naszych partnerów.



Jan Grusznic

a&s Polska

W grze strategicznej mówiliśmy o kilku rzeczach, ale najistotniejszy był element audytu. Trzeba pamiętać, aby zidentyfikować odpowiednie strefy, myśleć perspektywicznie i holistycznie o bezpieczeństwie nie tylko fizycznym, ale też cyber i połączyć obie te rzeczy. Myślę, że pomimo dość trudnego charakteru dzisiejszej gry, bo omawialiśmy ewidentnie bardzo techniczny problem, uczestnicy świetnie sobie poradzili i doskonale współpracowali ze sobą po to, aby dojść do pozytywnego wyniku.

Piotr Karpiński

STID

W naszej ofercie mamy rozwiązania typu Proximity Check do sprawdzania prędkości odpowiedzi karty kontroli dostępu i przede wszystkim do sprawdzania, czy ta karta znajduje się bezpośrednio przed czytnikiem. Jeżeli nie, taka karta zostanie zignorowana. To jest to, co pokazywaliśmy, ale też bardzo dużo rozmawialiśmy na temat nowej dyrektywy. NIS 2 wprowadza kary: 10 mln euro lub 2% globalnego obrotu. Dotyczy to nie tylko świata cyfrowego, czyli nie tylko infrastruktury IT, ale także wszystkich urządzeń, które zabezpieczają te obiekty. W związku z czym kontrola dostępu, karty – one też muszą być bezpieczne.

Bogumił Szymanek

Axis Communications

Na tym Security BootCamp najciekawsze były dyskusje związane z całkowitym kosztem posiadania systemu, ponieważ wielu naszych klientów na początku skupia się na kryterium ceny zakupu konkretnego urządzenia, np. kamery. Nie ukrywajmy, że nasze rozwiązania nie należą do najtańszych, ale charakteryzują się najwyższym poziomem jakości. Wielu naszych gości potwierdziło, że koszty wdrożenia i eksploatacji, czyli utrzymania i konserwacji takiego systemu, są dużo niższe od tego, jakby zastosowali urządzenia niskiej jakości i znacznie tańsze.

Marek Skowronek

Securitas Polska

Głównym założeniem systemu mgły ochronnej, którą prezentowaliśmy, jest neutralizacja intruza w początkowej fazie wtargnięcia na obiekt. Mgła, która może być rozpylana automatycznie lub zdalnie, wpływa na zmysł wzroku oraz percepcję przestrzenną. W ćwiczeniach skupiliśmy się na zmyśle węchu i było zaskakujące, jak ludzie odbierają i jak reagują, gdy znajdują się w centrum mgły.

Tomasz Nawrat

Genetec

Omawiając pracę jednej z naszych kamer z rozwiązaniem do rozpoznawania numerów tablic rejestracyjnych, użyłem określenia Deep Learning. I tu muszę stwierdzić, że termin AI, czyli sztuczna inteligencja, jest dzisiaj nadużywany. Myślę, że dużo osób jeszcze nie rozumie, co to pojęcie znaczy. Zeszliśmy na offlinowe tematy, żeby kontynuować tę ciekawą dyskusję. Myślę, że to jest coś, co dzisiaj przykuło uwagę uczestników.

Magdalena Jamrozik

Brembo

Najbardziej podobała mi się prezentacja dotycząca nowoczesnego monitoringu wizyjnego oraz możliwości zastosowania kamer i wyboru ich parametrów do codziennej pracy i użytkowaniu w zastosowaniach security.

Adam Sawicki

DSV

Przede wszystkim cenię sobie nawiązane tu kontakty. Spotkałem ludzi, z którymi już się umówiłem, wymieniliśmy opinie na tematy związane z cybesecurity i ochroną fizyczną. To było to, czego oczekiwałem.

Patryk Klinert

Fiege North

Przedstawiono nam różne produkty. Można było np. poznać, jakie są możliwości kart kontroli dostępu, ale też z drugiej strony, jak można złamać ich zabezpieczenia.

Paulina Celeban

Wielton

Przyjechali eksperci, którzy przedstawiali swoje produkty. Na stoiskach można było bliżej poznać ich rozwiązania. Bardzo dużo dowiedziałam się o branży i poznałam ciekawych ludzi.

DAHUA TECHNOLOGY POLAND

Innowacyjne rozwiązania Dahua dla integratorów

Blisko 100 osób uczestniczyło w najnowszym wydarzeniu przeznaczonym dla integratorów systemów, które pod koniec października Dahua Technology Poland zorganizowała w Toruniu.

To już drugie w tym roku wydarzenie poświęcone innowacyjnym rozwiązaniom AI oferowanym przez Dahua, tym razem dla partnerów z północnej i centralnej Polski.

– *Cieszę się, że mogłem powitać naszych gości dokładnie w siódmą rocznicę powstania oddziału Dahua w Polsce. Od tego czasu firma poszerzyła znacznie portfolio produktów, powiększył się też nasz zespół sprzedażowo-projektowy. Podczas spotkania nasi eksperci przybliżyli uczestnikom wiedzę o najnowszych rozwiązaniach Dahua, w tym o systemach trafficowych, parkingowych oraz termowizyjnych. Działanie tych urządzeń można było przetestować na specjalnie przygotowanych stoiskach* – powiedział Artur Prusinowski, Country Manager Poland.

Spotkanie było okazją do zapoznania się z najnowszymi produktami, które przedstawił Maciej Pietrzak, Technical Manager. Jak podkreślił: „Dahua inwestuje w rozwój swoich rozwiązań nie tylko sprzętowych, ale i programowych. Tylko taka strategia przynosi konkretne efekty, które pozwalają zaspokoić rosnące potrzeby naszych klientów."

Z możliwościami oprogramowania DSS Pro zapoznał uczestników Marcin Kulik, menedżer produktu.

– *Szczególne zainteresowanie wzbudził parkingowy moduł DSS. Dużo pytań dotyczyło możliwości odczytu tablic rejestracyjnych i innych funkcji analitycznych dostarczających dane pomocne w wyszukiwaniu konkretnych zdarzeń* – skomentował.

Z kolei rozwiązania termowizyjne przybliżył uczestnikom Marian Maroszek, inżynier wsparcia technicznego.

– *Kamery termowizyjne znakomicie sprawdzają się nie tylko w ochronie perymetrycznej obiektów. Mogą też sygnalizować zmiany temperatury, np. na liniach produkcyjnych, mogące zapobiec przegrzaniu newralgicznych elementów maszyn, a także wykryć zagrożenie pożarowe już na bardzo wczesnym etapie rozwoju* – dodał.

Nie zabrakło ciekawych dyskusji i możliwości nawiązania wartościowych relacji biznesowych.

– *To było świetne przedstawienie najnowszych rozwiązań Dahua. Jestem bardzo zadowolony ze spotkania, dowiedziałem się bardzo dużo, uzupełniłem wiedzę, a dzięki temu będę mógł zapewnić bezpieczeństwo i komfort moim klientom* – powiedział Michał Syska z firmy Inskam.

Organizatorzy już teraz zapraszają na kolejne spotkania w przyszłym roku. ●

Motorola Solutions świętuje 30-lecie działalności w Polsce

Motorola Solutions, globalny lider w dziedzinie bezpieczeństwa publicznego i ochrony przedsiębiorstw, świętuje 30-lecie istnienia w Polsce. Firma założyła swoje pierwsze biuro w Warszawie w 1993 r. i od tego czasu zwiększyła liczbę pracowników z 30 do 2600.

W tym roku przypada również 25. rocznica działalności Motorola Solutions w Krakowie, jednym z największych na świecie ośrodków firmy opracowujących innowacyjne rozwiązania w zakresie bezpiecznej komunikacji radiowej, systemów monitoringu wizyjnego, analityki, cyberbezpieczeństwa i rozwiązań do centrów zarządzania dla klientów na całym świecie.

Mark F. Brzezinski, ambasador USA w Polsce, z zadowoleniem obserwuje inwestycje Motorola Solutions w kraju i docenia jej wkład w rozwój sektora technologicznego. – *Partnerstwo między Polską a Stanami Zjednoczonymi jest nadal bardzo bliskie, szczególnie w takich obszarach, jak energetyka, obronność, cyberbezpieczeństwo i komunikacja* – powiedział M. Brzeziński dodając: – *Jestem zaszczycony, że mogę uczestniczyć w obchodach 30-lecia Motorola Solutions w Polsce, firmie, która nieustannie wprowadza innowacje na globalny rynek, jednocześnie przynosząc korzyści społecznościom, w których działa.*

– *Nasza działalność w Polsce rozwija się dzięki wysoko wykwalifikowanej kadrze inżynierskiej i programistycznej* – powiedział Jacek Drabik, Country Manager w Motorola Solutions Polska. – *Dzięki ponad 1600 pracownikom działu badań i rozwoju i ponad 160 przyznanym patentom nasz zespół odgrywa ważną rolę w opracowywaniu innowacyjnych urządzeń i oprogramowania, które pozwalają organizacjom – od agencji bezpieczeństwa publicznego po szkoły, szpitale i infrastrukturę krytyczną – pracować bezpieczniej i pewniej. Nasza kultura opiera się na tworzeniu pomysłów i wynalazków, które są napędzane różnorodnością naszych pracowników, reprezentujących ponad 40 narodowości, z doświadczeniem w zakresie badań i rozwoju, łańcucha dostaw, usług wspólnych i obsługi klienta* – podkreślił Jacek Drabik. ●

Bezp. inf. prasowa

„Potencjał i rola sektora prywatnego w systemie bezpieczeństwa narodowego". 24. Konferencja Branży Ochrony już za nami

Technologie służące narodowemu bezpieczeństwu, współpraca z mieszkańcami i partycypacja społeczna w tworzeniu bezpiecznych przestrzeni, bezpieczeństwo społeczności, organizacja cyberbezpieczeństwa, praca zdalna w branży ochrony oraz potencjał i rola sektora prywatnego w systemie bezpieczeństwa narodowego w obecnej sytuacji geopolitycznej to tylko kilka wybranych tematów, które poruszono podczas 24. Konferencji Branży Ochrony, która odbyła się 28-29 września 2023 r. w Jachrance.

Organizatorem konferencji była Polska Izba Ochrony Osób i Mienia we współpracy m.in. z Akademią WSB z Dąbrowy Górniczej, firmą Securex, Stowarzyszeniem Polskich Specjalistów Bombowych, Centrum Prewencji Antyterrorystycznej ABW.

Konferencję otworzyli Marcin Pyclik, prezes Zarządu Polskiej Izby Ochrony, i prof. dr. hab. Bernard Wiśniewski, AWSB.

W trakcie konferencji uczestnicy mogli wysłuchać ciekawej dyskusji w panelu dyskusyjnym nt. udziału prywatnego sektora ochrony w systemie bezpieczeństwa państwa, w których wzięli udział m.in. dr Jarosław Cymerski, płk SOP, Paweł Płużyczka, koordynator ds. bezpieczeństwa Igrzysk Europejskich w Krakowie w 2023 r., Piotr Gąstal, pułkownik rezerwy SZ RP, były dowódca Jednostki Wojskowej GROM.

Dyskusja stanowiła wprowadzenie do merytorycznych wykładów, w których uczestnicy spotkania mogli poznać najnowsze rozwiązania użyteczne dla narodowego bezpieczeństwa. ●

Bezp. inf. prasowa

SICUREZZA 2023

Zakończyły się jedne z najważniejszych w Europie targi bezpieczeństwa – SICUREZZA 2023. Od 15 do 17 listopada Mediolan gościł 347 firm branży security z 31 krajów, w tym kilka z Polski. Targi były częścią pierwszej edycji MIBA-Milan International Building Alliance, która łącznie zgromadziła 1350 firm i ponad 80 tysięcy odwiedzających.

Adela Prochyra

Można zaryzykować tezę, że branża security odgrywa wręcz kluczową rolę w dzisiejszym świecie. Jej projekty są fundamentem do ochrony osób, mienia, a także danych osobowych. W dobie rosnącej cyfryzacji i globalnej łączności zagrożenia cyberatakami, kradzieżą danych i naruszeniami prywatności są coraz powszechniejsze. Produkty oferowane przez tę branżę nie tylko chronią przed atakami, ale też wspierają zgodność z regulacjami prawnymi i standardami ochrony danych, takimi jak GDPR, co jest kluczowe dla budowania zaufania i reputacji firm. Ponadto branża security inwestuje w zaawansowane technologie, takie jak sztuczna inteligencja i uczenie maszynowe, aby skuteczniej przewidywać i zapobiegać zagrożeniom. Wreszcie rozwój tej branży ma znaczący wpływ na kształtowanie polityk bezpieczeństwa na poziomach krajowym i międzynarodowym, co ma zasadnicze znaczenie dla globalnej stabilności i bezpieczeństwa.

Te założenia odzwierciedlała zawartość stoisk poszczególnych wystawców. Już pobieżny przegląd dawał obraz branży bardzo nowoczesnej, gotowej na wyzwania ery cyfrowej, śmiało wychodzącej z nowymi propozycjami, odpowiadającymi niemal na każde zapotrzebowanie. Na żywo można było obejrzeć m.in. wysoko zaawansowane systemy monitoringu wizyjnego oraz powiązane z nimi systemy zasilania, systemy przeciwpożarowe, alarmowe, oświetlenia i wiele rozwiązań z obszaru *smart home*.
Wśród wystawców znajdowali się giganci branży, tacy jak Hikvision, którego stanowisko było jednym z największych, Geutebrick, Motorola czy rodzimy Satel, który również zaprezentował się z rozmachem. Z okazji przedstawienia swoich rozwiązań na międzynarodowym forum skorzystało także wielu mniejszych producentów, wśród których wymieńmy chociażby dwie polskie firmy – Tedee i Ferguson, które przyjechały do Włoch z bardzo interesującymi ofertami,

o czym później. Swoje możliwości zaprezentowały także lokalne służby – Polizia di Stato, Guardia di Finanza, Polizia Penitenziaria. Zdecydowana większość wystawców to były firmy włoskie, podobnie jak gros odwiedzających. Wielu gości przybyło także z innych regionów, m.in. z Bliskiego Wschodu, Stanów Zjednoczonych i Azji. Agnieszka Pitrus z Satel podkreśliła, że Włochy to bardzo duży, ale też nasycony rynek. Działa na nim wiele lokalnych firm, nierzadko z długą historią, a firmom bez doświadczenia na Półwyspie Apenińskim lub bezpośrednich kontaktów z tamtejszymi przedsiębiorcami jest się trudno przebić.

Nasi w Mediolanie

Konkurencja, to było widać, jest ogromna, ale oferta polskich wystawców na SICUREZZA 2023 była atrakcyjna. Z oryginalnym pomysłem przyjechał producent inteligentnych zamków Tedee. Zaprezentował swoje dwa podstawowe produkty, czyli zamek Tedee GO do samodzielnej instalacji (bez konieczności wymiany wkładki), oraz zamek Tedee PRO (z gamą własnych wkładek). CTO firmy, Andrzej Kaszycki, podkreślił, że części do zamków produkowane są w Polsce, a produkty Tedee można znaleźć na wielu zagranicznych rynkach, m.in. w Brazylii.

Pulsar – producent urządzeń i akcesoriów do systemów alarmowych, kontroli dostępu i telewizji przemysłowe, obudów zasilaczy oraz samych zasilaczy buforowych 27,6 VDC, certyfikowanych normą EN54-4, EN12101-10. Także ten wytwórca sprzedaje swoje produkty na europejskich i pozaeuropejskich rynkach.

Firma Ferguson, która zaczynała działalność jako producent dekoderów telewizji naziemnej, a w międzyczasie poszerzyła ofertę o wiele produktów *smart home,* zaprezentowała z kolei zintegrowany system automatyki domowej. W jego skład – oprócz inteligentnej centrali sterującej – wchodzą: czujki dymu, czadu, gazu, zalania i ruchu oraz akcesoria do sterowania oświetleniem i temperaturą – oczywiście za pomocą aplikacji mobilnej.

Największe i najbardziej efektowne z polskich stoisk należało bez wątpienia do gdańskiego Satela, który przygotował dla swoich gości niespodziankę. Pierwszego dnia miała miejsce huczna prapremiera ich najnowszego produktu, czyli systemu alarmowego Be Wave do samodzielnego montażu. Oprócz tego prezentowane były flagowe produkty firmy wchodzące w skład systemu Integra i nowość w ofercie, multikontroler Integra 2.

Jak chronić cyfrowy świat

SICUREZZA to nie tylko stoiska. Tradycją targów jest łączenie środowisk producentów, sprzedawców oraz specjalistów w celu stworzenia forum wymiany doświadczeń. Dlatego wydarzeniu towarzyszył szereg wykładów i paneli dyskusyjnych na tematy związane z bezpieczeństwem, ale też przyszłością miast, innowacji budowlanych, zrównoważonego rozwoju. Jednym z głównych tematów było cyberbezpieczeństwo.

Szczególnie interesujący był wykład *Essential Toolkit for Cyber Security Risk Management,* zorganizowany przez Sicurezza i Smart Building Expo. Profesor Greta Nasi z Universita Bocconi w Mediolanie omówiła aktualne wyzwania cyberbezpieczeństwa. Koszt cyberataków w 2020 r. osiągnął wartość 5,5 mld euro. W zestawieniu z faktem, że na specjalistów cyberbezpieczeństwa czeka w Europie aż 350 tys. wakatów, można mówić o pilnej potrzebie zwiększenia wysiłków na rzecz ochrony obywateli i instytucji.

Sektory zdrowia, transportu i finansów to główne obszary, które padają ofiarą ataków. Profesor G. Nasi zasugerowała, że cyberprzestrzeń może być uznawana za piąty żywioł, obok ziemi, wody, powietrza i ognia, biorąc pod uwagę jej definicje i wpływ na współczesny świat. ●

VI Międzynarodowy Kongres Naukowo-Techniczny SAFE PLACE 2023

Tegoroczna edycja VI Międzynarodowego Kongresu Naukowo-Technicznego SAFE PLACE 2023 odbyła się pod hasłem: *Odporność budynków użyteczności publicznej infrastruktury krytycznej wobec zagrożeń wojennych, hybrydowych i terrorystycznych.*

Wśród gości Kongresu, który odbył się 20-22 listopada 2023 r. w Klubie Wojskowej Akademii Technicznej w Warszawie, znaleźli się m.in. dr Jacek Siewiera, sekretarz stanu – szef Biura Bezpieczeństwa Narodowego; gen. bryg. prof. dr hab. inż. Przemysław Wachulak – rektor Wojskowej Akademii Technicznej w Warszawie; prof. Piotr Gawliczek – dyrektor NATO DEEP eAcademy; Beata Janowczyk – zastępca dyrektora Rządowego Centrum Bezpieczeństwa; dr hab. Juliusz Piwowarski – rektor i założyciel WSBPI „Apeiron"; płk. Dmytro Bobrov z Uniwersytetu Obrony Narodowej Ukrainy.

Trzy dni Kongresu były wypełnione przez merytoryczne prezentacje i dyskusje ekspertów dotyczące m.in. dobrych praktyk i rekomendacji w obszarze przygotowania obiektów do wojny, obowiązków osób zarządzających bezpieczeństwem obiektów infrastruktury krytycznej i planów jej ochrony, a także wyzwań związanych z wprowadzaniem nowych rozwiązań legislacyjnych czy specyfiki zagrożeń w cyberprzestrzeni. Przedstawione i analizowane studia przypadków dotyczyły ataków na różne instytucje, wykorzystanie cyberataków w działaniach wojennych i hybrydowych oraz możliwości przeciwdziałania zagrożeniom.

Podczas pierwszego dnia odbyła się uroczysta inauguracja polskiej wersji językowej certyfikowanego kursu e-learningowego NATO *e-Counterterrorism Reference Curriculum* (e-CTRC), opracowanego na podstawie wzorcowego programu nauczania NATO DEEP CTRC.

Równolegle z prezentacjami i panelami dyskusyjnymi odbyły się warsztaty z reagowania na zamachy. Uczestnicy mieli możliwość wzięcia udziału w praktycznych zajęciach z następujących tematów:

- udzielanie pierwszej pomocy,
- praktyczny wymiar zabezpieczeń technicznych,
- reagowanie na zagrożenia wojenne i terrorystyczne.

Nie zabrakło pokazów sprzętów i wyposażenia specjalistycznego sił policyjnych oraz wojskowych, w tym sił specjalnych. Zorganizowano również zawody strzeleckie.

Na specjalnie wydzielonych stoiskach przygotowanych przez firmy z branży security uczestnicy mieli możliwość zapoznania się z najnowszymi rozwiązaniami zabezpieczeń firm partnerskich Kongresu SAFE PLACE 2023. ●

AAT SYSTEMY BEZPIECZEŃSTWA

Aktywne odstraszanie

Kamery IP NVIP-4VE-4231/WLAD oraz NVIP-4H-4231/WLAD marki NOVUS z oświetlaczem światła białego i IR zostały wyposażone w funkcję aktywnego odstraszania.

Funkcja aktywnego odstraszania powoduje, że po wykryciu obecności intruzów w obszarze monitorowanym przez kamerę urządzenie może uruchomić reakcję alarmową w postaci uruchomienia oświetlenia światłem ciągłym lub migającym, włączenia dźwięków ostrzegawczych (liczba i dobór funkcji odstraszania może różnić się w zależności od modelu kamery). Funkcja ta ma na celu ochronę miejsca, które jest monitorowane, zniechęcenie intruza do dalszych działań i odstraszenie go bez potrzeby interwencji ochrony.

Dzięki zastosowaniu Starlight Pro Duo kamery wykorzystują dwa rodzaje oświetlaczy: złożony z białych diod LED oraz z diod podczerwonych IR LED. Niezwykle wysoka czułość kamery w połączeniu z dużej mocy światłem białych diod LED umożliwia obserwację w kolorze niezależnie od pory dnia (24/7) i warunków atmosferycznych. Diody IR LED umożliwiają pracę w nocy w sposób „tradycyjny", w trybie czarno-białym, co może być przydatne w sytuacjach, w których pożądana jest dyskrecja obserwacji. ●

AXIS COMMUNICATIONS

Nowy dekoder 4K AXIS D1110

Axis Communications wprowadza na rynek dekoder wideo 4K wyposażony w intuicyjny interfejs Axis, który może być używany z monitorami obsługującymi wyjścia HDMI™, aby wyświetlać obrazy na żywo.

Dekoder 4K AXIS D1110 można stosować do wyświetlania materiału wizyjnego na żywo w widoku sekwencyjnym oraz do 8 strumieni w trybie wieloekranowym. Jest to ekonomiczne rozwiązanie do monitoringu, w którym obrazy mogą być wyświetlane na żywo bez użycia komputera. Natomiast dzięki zastosowaniu portów wyjściowych sygnału audio możliwe jest podłączenie do dekodera głośników zewnętrznych.

To elastyczne urządzenie może być używane niezależnie lub stanowić część kompleksowego systemu firmy Axis. Nie wymaga do funkcjonowania podłączenia do systemu zarządzania wideo (VMS), co nie zmienia faktu, że jeśli wystąpi taka potrzeba, dekoder w każdej chwili może stać się częścią VMS. Przyjazny interfejs Axis powoduje, że obsługa urządzenia jest łatwa i nie wymaga szkolenia.

Dekoder może być zasilany przez Power over Ethernet (PoE) lub prądem stałym (DC). Samo uruchomienie urządzenia za sprawą technologii plug and play jest przy tym bardzo proste. Obudowa została wyposażona w mocowanie VESA, dzięki czemu dekoder można łatwo umieścić z tyłu monitora. Axis Edge Vault, sprzętowa platforma cyberbezpieczeństwa, zapewnia integralność urządzenia oraz chroni wrażliwe dane przed nieautoryzowanym dostępem. ●

LINC POLSKA

Honeywell | Secured by Default – cyberbezpieczeństwo w archiwizacji

Wraz z nowymi kamerami serii 35 Honeywell wprowadził na rynek rejestratory sieciowe spełniające najwyższe normy związane z cyberbezpieczeństwem, obejmujące m.in. bezpieczną transmisję szyfrowaną w TLS1.2. Dostępne urządzenia oferują od 4 do 16 kanałów IP.

Ponadto wersja z wbudowanym switchem PoE minimalizuje liczbę pobocznych elementów w systemie.

Obsługa kamer 8 Mpix z kompresją H.265, HDMI w 4K to już standard w tego typu urządzeniach. Dzięki zwiększonym wymogom bezpieczeństwa rejestratory są zgodne z NDAA, doskonale wpisują się też w najnowsze wymagania związane z certyfikatami PCI DSS. Wybierając serię 35 Honeywell, wchodzimy na wyższy poziom cyberbezpieczeństwa.

Urządzenia są dostępne w ofercie Linc Polska. ●

ROGER

Zamek ADL-2 – autonomiczna kontrola dostępu do budynku

Zamek ADL-2 składa się z dwóch metalowych szyldów drzwiowych zintegrowanych z klamkami. W szyldzie zewnętrznym wbudowany jest czytnik elektroniczny z klawiaturą, który umożliwia elektroniczną kontrolę wejścia do pomieszczenia.

Wejście wymaga podania kodu PIN lub użycia karty zbliżeniowej. Może odbywać się także z poziomu aplikacji mobilnej. Kody PIN mogą być zapisane w pamięci zamka lub generowane zdalnie.

ADL-2 pracuje autonomicznie bez konieczności komunikacji z nadrzędnym urządzeniem zewnętrznym. Zamek jest zasilany z wewnętrznych baterii i nie wymaga zewnętrznego okablowania, a jego montaż następuje bezpośrednio na skrzydle drzwi. Do konfiguracji zamka oraz jego obsługi służy bezpłatna aplikacja mobilna RogerMDM (iOS, Android).

Zamek ADL-2 można zainstalować na większości drzwiach z zachowaniem istniejącego wewnętrznego zamka wpuszczanego (o rozstawie 72 mm między wkładką a klamką) oraz wkładki bębenkowej, która może być wykorzystana do mechanicznego blokowania drzwi oraz ich awaryjnego otwarcia.

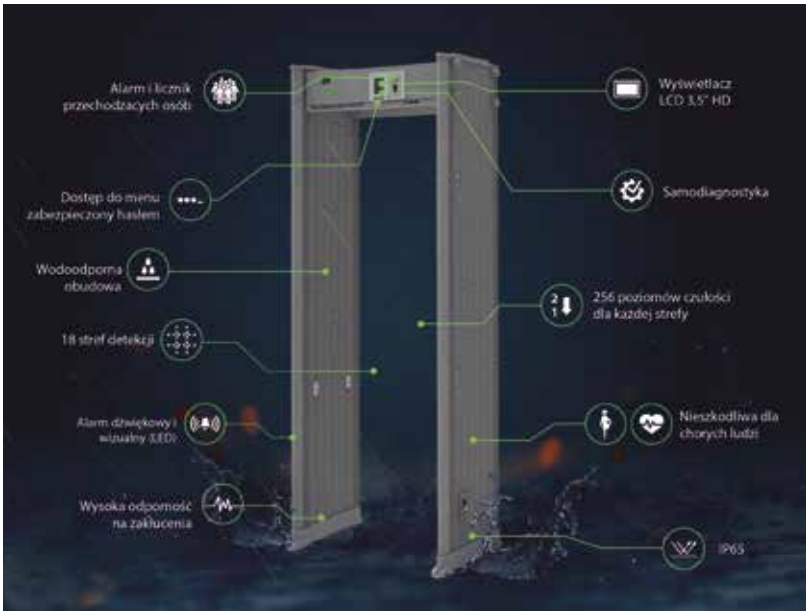
Zamek umożliwia autonomiczną kontrolę dostępu w biurach, urzędach, przychodniach, szkołach i innych miejscach, gdzie zachodzi potrzeba kontroli ruchu osób bez instalacji systemu kontroli dostępu.

Ze względu na możliwość zdalnego generowania kodów dostępu zamek nadaje się również do wykorzystania w apartamentach przeznaczonych na wynajem krótkoterminowy. ●

ZKTECO

Wodoodporny wykrywacz metali AMD1800 Pro

Firma ZKTeco wciąż rozszerza swoją ofertę produktową o kolejne bramki do wykrywania metali. Tym razem jest to bramka pyło- i wodoszczelna (P65), którą z powodzeniem można stosować na zewnątrz, również w miejscach narażonych na deszcz. Urządzenie ma 18 stref detekcji z regulowanym poziomem czułości (256 poziomów).



Bramki wyposażono w wyświetlacz LCD 3,5", licznik przechodzących osób oraz alarm dźwiękowy i wizualny (LED). Są zasilane napięciem stałym 12 V.

Do komunikacji z komputerem i Internetem służy wbudowany port komunikacyjny TCP/IP. Dostęp do menu ekranowego jest chroniony hasłem. Bramką można też sterować zdalnie za pomocą oprogramowania WTMD lub aplikacji mobilnej WTMD. Aby zapewnić bezawaryjność pracy, urządzenie wyposażono w system samodiagnostyki.

Bramkę charakteryzuje wysoka odporność na zakłócenia elektromagnetyczne, a jej praca jest nieszkodliwa dla organizmu ludzkiego. Jest kompatybilna z innymi bramkami i urządzeniami firmy ZKTeco. Instalacja, a także późniejsza obsługa bramki jest bardzo prosta.

Urządzenie doskonale sprawdzi się w bankach, instytucjach rządowych i finansowych, w sądach, wojsku, więziennictwie oraz fabrykach o znaczeniu strategicznym i innych obiektach, w których obowiązuje podwyższony stopień ochrony. Może też być bardzo przydatne w biurach, hotelach, szkołach, centrach handlowych i rekreacyjnych oraz obiektach wystawienniczych. Ze względu na swoją wodoodporność nadaje się do obsługi masowych imprez plenerowych, w tym stadionowych. ●

MEGAVISION TECHNOLOGY

AVIGILON · MOTOROLA SOLUTIONS · Venom PSIM PLATFORM

O NAS

Megavision Technology to wiodący, polski dostawca systemów bezpieczeństwa wysokich technologii. W ofercie firmy znajdują się wyłącznie kluczowe rozwiązania, spełniające wszelkie wymagane certyfikaty i dopuszczenia, gwarantując użytkownikom systemów pełne bezpieczeństwo i najwyższą jakość.

MISJA

Jesteśmy grupą ekspertów systemów klasy PSIM oraz CCT/KD budujących unikalną wartość dla klientów od ponad dekady. Posiadamy rozległą wiedzę i doświadczenie z wielu realizacji zakończonych sukcesem.

WIZJA

Tworzymy zespół kompetentnych, twórczych i profesjonalnych specjalistów. Budujemy długofalowe relacje z klientami, którym oferujemy skuteczne, dedykowane i innowacyjne rozwiązania zapewniające osiągnięcie założonych celów.

VENOM PSIM

Physical Security Information Management, Otwarta platforma, Unikalny na rynku całkowicie polski system PSIM najwyższej klasy.

AVIGILON

Wspólnie z Motorola Solutions dostarczamy zintegrowane rozwiązania bezpieczeństwa najwyższej klasy światowej. Wszystkie nasze technologie wytwarzane są w krajach NATO.

MEGAVISION TECHNOLOGY Sp. z o. o., Heliotropów 1, 04-796 Warszawa, tel. +48 22 292 3 292, e-mail: psim@psim.pl

Firma HIOB

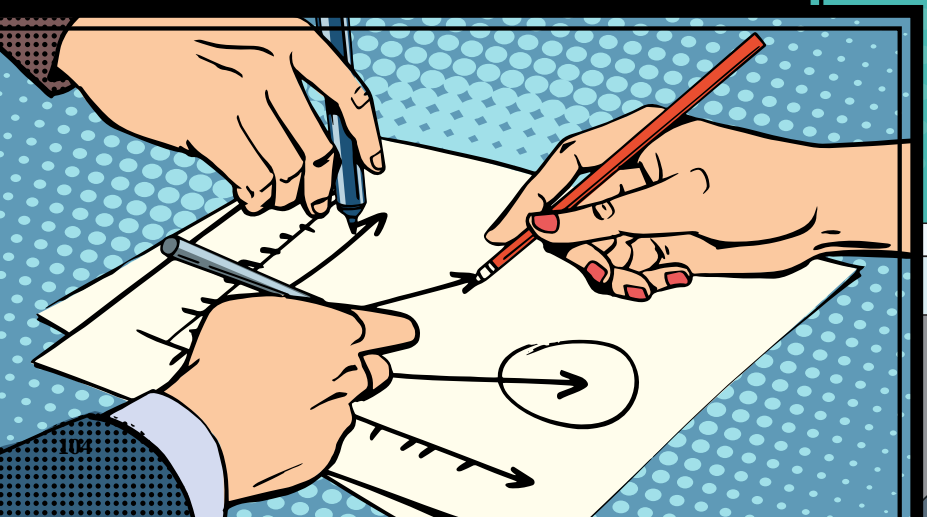
Dwa razy do roku znany magazyn zajmujący się tematyką security organizował edukacyjne warsztaty branżowe. *Crème de la crème* na krajowej mapie szkoleń. Ale wszyscy dobrze wiedzieli, że nie samymi szkoleniami security manager żyje.

Wieczory integracyjne cieszyły się więc równie wielką popularnością jak najbardziej merytoryczne prezentacje. Albo nawet większą, ale o tym ciii...

Tego dnia hotelowy pub był pełen uczestników bootcampu. Z ogólnego gwaru co chwilę dało się wyłowić dziwne słowa: peryferyjna, infiltracja, perymetryczna, lidar itp.

Damian Maliszewski wszedł do sali i się rozejrzał. W jego stronę machała Katarzyna Trzmiel, specjalistka do spraw bezpieczeństwa fizycznego, którą poznał na poprzednich warsztatach i tak jakoś dobrze im się rozmawiało.

– Uff, no w końcu można odsapnąć. Dali mi w kość. – Damian Maliszewski ciężko opadł na krzesło.



Wszyscy zgromadzeni przy stoliku pokiwali głowami ze zrozumieniem. Maliszewski był w branży nowy. Na security dopiero się poznawał. O jego nowej profesji zdecydował przypadek. Jako główny technolog w pewnej firmie produkcyjnej miał za sobą mały detektywistyczny sukces, w związku z czym wysyłano go teraz na kolejne szkolenia. Okazało się, że dobrze jest, gdy w zakładzie jest więcej czujnych oczu. A Maliszewski nie miał nic przeciwko tego typu kursom, szczególnie od czasu, gdy na jedno ze spotkań „przyfrunęła" Katarzyna Trzmiel.

– Nareszcie jesteś. – Grzegorz Jackowiak podniósł się, by przywitać się z nowo przybyłym. Nie krył zadowolenia, że przy stoliku zasiedli już jego wszyscy ulubieni branżowi znajomi, zwłaszcza że miał niebywałą opowieść.

– Damianie, siadaj tutaj, zarezerwowałam ci miejsce. – Trzmiel, zazwyczaj kąśliwa jak szerszeń, poklepała miejsce obok siebie. I zarządziła:

– Posuń się, Bzyku, bo nam się tu ciasno zrobiło.

Bzyk bez dyskusji wypełnił jej polecenie.

Przy jednym stoliku siedziała już spora grupa osób, za dnia uczestników warsztatów i kiedyś zupełnie sobie obcych, a teraz dobrych znajomych. Przed Damianem na miejsce zdążyli już dotrzeć wścibska Marianna, na co dzień pracująca w wydziale ochrony środowiska w małej hucie, oraz jej kolega z pracy zajmujący się zaopatrzeniem Robert Mucha, zwany Bzykiem. To właśnie Bzyka przegoniła stanowczo Trzmiel, by zrobić miejsce dla Damiana Maliszewskiego. Obok siedział też Kacper Kacperski, spec od cyberbezpieczeństwa w dużej sieci handlowej. Tylko Jackowiak był doświadczonym bezpiecznikiem. Reszta dopiero startowała w branży.

Gdy Maliszewski usiadł, Trzmiel wróciła do opowieści. Jak zwykle opowiadała barwnie, emocjonalnie gestykulując.

– Coś mnie ominęło? – Maliszewski wziął łyk grzańca i rozejrzał się po zgromadzonych.

– Eeee, nic takiego. – Trzmiel machnęła ręką. – Już ci wspominałam o tym urzędniczym „przemycie". Pamiętasz sprawę w wydziale inwestycji? Gdy okazało się, że nikt nie zabezpieczył wyjścia na klatkę ewakuacyjną i złodzieje weszli jak do siebie. Ześlili mnie, bo nie wierzą, że ten, kto projektował system zabezpieczeń, tak mógł to spartolić. A najbardziej nie dowierza on! – Trzmiel oskarżycielsko wskazała palcem na Kacperskiego. – Co on wie o security?! Tylko się gapi w te swoje serwery!

Kacper Kacperski takiej zniewagi nie zamierzał puścić płazem.

– Tylko nie serwery, nie serwery! Od serwerów są sysadmini, ja się zajmuję walką z hakerami. Owszem – dodał już bardziej pokojowo – wierzyć mi się nie chce, że ktoś mógł nie przewidzieć, że złodzieje wejdą tylnymi drzwiami. Przecież to… – przez chwilę szukał słowa – głupota i zaniedbanie. Ja zawsze sprawdzam backdoory.

– Ja w to wierzę – wtrąciła się Marianna. – U nas, w hucie, też miało miejsce dziwne zdarzenie…

Nim skończyła, Kacperski ryknął śmiechem:

– Surówkę wam ukradli? Z buraczków?!

No wiesz! – Marianna się zaperzyła. – Wcale nie surówkę, tylko surowiec. I nie będę się tu przechwalać, ale to ja wpadłam na to, że nas okradają. Mam wzrok jak słoń i zauważyłam to i owo. Bzyk świadkiem.

Bzyk pokiwał głową.

Teraz śmiechem parsknęła Trzmiel:

– Chyba jak jastrząb?

– Jaki jastrząb?

– Mówi się wzrok jak jastrząb, a pamięć jak słoń – wyjaśniła Trzmiel.

– Mniejsza o to, jakie zwierzę. Ważne, że nakryłam oszustów i złodziei.

– Marianna siorbnęła grzańca bezalkoholowego (w myślach poniewierając się za taki wybór, bo trunek smakował jak woda po płukaniu beczki).

Do akcji postanowił wkroczyć Grzegorz Jackowiak.

– Młodzieży… – Grzegorz potoczył po zebranych wzrokiem dystyngowanego starszego pana, choć wszyscy, poza młodziutką Marianną, byli mniej więcej w tym samym wczesnym wieku średnim. – Otóż chcę wam powiedzieć, że nie ma takiej rzeczy, jakiej oszust i złodziej by nie wymyślił. – Wszyscy zastrzygli uszami, a Grzegorz, ujęty ich zainteresowaniem ciągnął: – Ostatnio byłem w firmie, którą permanentnie okradano. Trafił się szantażyk, a do tego wyciekły dane i do sprawy włączył się KNF. Wiele już widziałem, ale ten przypadek nawet mnie zaskoczył. Tylko nie wiem, czy mogę wam opowiedzieć… – Jackowiak znacząco zawiesił głos.

– Grzesiek – jęknął Kacperski – bądź człowiek, nie możesz tak nas trzymać.

– Powiem, ile mogę, bo tajemnica klienta rzecz święta. Ale przyda się wam taka wiedza na przyszłość. – Jackowiak lubił dzielić się wiedzą, a zainteresowanie towarzystwa przyjemnie połechtało jego ego. Następnie podniósł kufel złocistego rarytasu, łyknął trunku, by zwilżyć gardło, i zaczął opowieść: – Nie tak dawno temu i nie za górami ani za lasami, tylko w sąsiedniej gminie grasował siedmiogłowy smok, czyli szajka, której herszt upatrzył sobie całkiem sporą firmę i zaczął ją łupić. I ty, Marianka, słuchaj, bo w hucie też może się tak zdarzyć… Prawie pół godziny trwała opowieść, *ad hoc* uzupełniana planami sytuacyjnymi rysowanymi na serwetkach. Gdy Jackowiak skończył, wszyscy siedzieli jak skamieniali.

– I to wszystko w jednej firmie? – Kacperski nie mógł wyjść ze zdumienia.

– Otóż właśnie – Grzegorz rozejrzał się po zamarłym z wrażenia towarzystwie – kradzież, szantaż, wyciek danych. Taka, powiedziałbym, firma Hiob.

Opracowała Monika Mamakis na bazie scenariusza Jacka Grzechowiaka

- **Czy możliwe, by na jedną firmę spadło aż tyle nieszczęść, czy też Grzegorz Jackowiak koloryzował, by zaimponować zebranym?**

Odpowiedzi na te pytania poznali uczestnicy strategicznych warsztatów Security Forum przeprowadzonych 30 stycznia przez Jacka Grzechowiaka, dyrektora Centrum Kompetencji a&s Polska.

Centrum Kompetencji a&s Polska organizuje szkolenia i warsztaty dla osób odpowiedzialnych za bezpieczeństwo fizyczne, cyfrowe i zabezpieczenia techniczne. Przekonaj się, co o warsztatach sądzą osoby, które wzięły w nich udział.

Łukasz Leśniewski, Euro RTV AGD

Bardzo dziękuję za zaproszenie, szkolenie bardzo mi się podobało. Szczególnie forma jego prowadzenia, bo aktywny udział biorą wszyscy uczestnicy. To trochę jak burza mózgów, gdzie patrzy się na bezpieczeństwo w firmach z różnych perspektyw. Każdy może podzielić się swoim doświadczeniem, a to daje nam wiedzę, jak można zapobiec lukom w bezpieczeństwie.

Katarzyna Sikora, Neonet

To było bardzo ciekawe forum wymiany informacji. Takie spotkania są bardzo potrzebne, szczególnie osobom, które nie mają dużego doświadczenia w sektorze handlowym. Możliwość poznania różnych przypadków i wynikających z nich zagrożeń pozwala uniknąć takich sytuacji w naszej pracy. Wymiana doświadczeń jest bardzo cenna, a rady doświadczonych kolegów na pewno się przydadzą.

Tomasz Wypych, Rossmann

Szkolenie było znakomite. Rozstrzał case'ów był bardzo przydatny szczególnie dla takiej organizacji, jak nasza, gdzie mamy wiele segmentów: od logistyki, przez sprzedaż, po biura i dział R&D. To pozwala spojrzeć całościowo na różne aspekty bezpieczeństwa. To szkolenie pokazało, w jaki sposób adresować problemy bezpieczeństwa, z którymi mierzymy się na co dzień. To bardzo potrzebna wiedza.


check. create. manage.
Checly
Zakład produkcyjny
wszystkie lokalizacje
Zadania do wykonania
dla mnie
wszystkie
2 gru
Kontrola ochrony fizycznej
Krzysztof Pacel
3 gru
Inspekcja obiektu Południe
Zbigniew Kaczwara
4 gru
Kontrola bramy głównej
Łukasz Bleniek
5 gru
Sprawdzenie czujek na wejściu
Jarosław Reguła
6 gru
Kontrola pracownika w recepcji
Franciszek Gola
Checly
the best startup 2023
checly.app

MERRY
Christmas
& HAPPY NEW YEAR

DZIĘKUJEMY ZA KOLEJNY WSPÓLNY ROK.

PRAGNIEMY ŻYCZYĆ PAŃSTWU
ZDROWYCH, SPOKOJNYCH I CIEPŁYCH
ŚWIĄT BOŻEGO NARODZENIA
ORAZ SZCZĘŚLIWEGO NOWEGO ROKU
PEŁNEGO SUKCESÓW, WYZWAŃ I SATYSFAKCJI.

ZESPÓŁ BCS

POLSKA MARKA BCS

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