06 (48) / 2024

CZASOPISMO RYNKU SECURITY

a&S POLSKA

## RANKING SECURITY 50

Jak co roku publikujemy zestawienie największych globalnych firm z branży security. Przedstawiamy także ogólny stan rynku i prognozy na przyszłe lata. Eksperci są nastawieni optymistycznie.

## RAPORT: HANDEL SIĘ LICZY

Skoro handel, to pieniądze. Czy dzisiejszy konsument liczy każdą złotówkę przed wydaniem? Jaka jest kondycja handlu detalicznego w Polsce i jaki to ma wpływ na branżę security?

## CYBERBEZPIECZEŃSTWO

Wiele firm popełnia błędy zwiększające ich podatność na cyberzagrożenia. Kluczem do ich unikania jest świadomość problemu, przeprowadzenie audytu oraz wdrożenie właściwych zabezpieczeń.

www.aspolska.pl

20 zł
(w tym 8% VAT)

ISSN 2451-5175

blue**Evo**

# Ewolucja inspirowana tradycją

blueEvo

Zarządzaj dostępem do każdego pomieszczenia, drzwi i bramy za pomocą **jednego klucza.**

Pełna kontrola, prostota i bezpieczeństwo w nowoczesnym wydaniu.

**Kontakt:**
Winkhaus Polska Beteiligungs
ul. Przemysłowa 1
64-130 Rydzyna

tel: 538 818 723
e-mail: masterkey@winkhaus.pl
www.blueEvo.com

WINKHAUS

# *Obywatelu, broń się sam?*

Motto polskiej policji brzmi „Pomagamy i chronimy". Rzecz jednak w tym, że sukcesywnie maleje liczba stróżów prawa, dla których ma to być najważniejszą służbową regułą. Dzieje się tak z prozaicznego powodu – brak chętnych do pracy w polskiej policji. W roku 2023 z formacji odeszło blisko 10 tys. funkcjonariuszy, a w tym roku można się spodziewać, że będzie ich o 5 tys. mniej. Dane opublikowane przez Komendę Główną Policji we wrześniu tego roku wskazują na niepokojący wzrost liczby wakatów. Obecnie nieobsadzonych jest prawie 15 tys. stanowisk. Nie bardzo ma więc kto pomagać i chronić. Braki kadrowe stają się boleśnie odczuwalne. Jak pisze tygodnik „Polityka" w artykule *Zmęczony jak pies* (48/2024, str. 17), wydłuża się czas reakcji na wezwania (do drobnych kradzieży sklepowych w Warszawie patrol czasem już nie dojeżdża), dochodzeniowcy zawalają terminy procesowe [...]. A cytowany przez „Politykę" mł. inspektor Sławomir Koniuszy, wiceszef NSZZ Policjantów, zwraca uwagę na pewną znaczącą zmianę, jaka dokonała się w ostatnich latach: *Zagrożeń przybywa. Jeszcze kilka lat temu sabotaż wydawał się opowieścią z innego świata, a teraz w Poznaniu zamykamy z tego powodu konsulat rosyjski.*

Czyżby obywatel musiał bronić się sam? Nie ma takiej potrzeby, natura bowiem nie znosi próżni. W sytuacji, gdy policja nie jest w stanie zapewnić odpowiedniego poziomu bezpieczeństwa, wiele osób i firm zaczyna szukać rozwiązań alternatywnych. Firmy zajmujące się ochroną i bezpieczeństwem stają się naturalnym wyborem dla tych, którzy pragną zadbać o swoje mienie i bezpieczeństwo osobiste.

Wzrost zainteresowania usługami security można zaobserwować nie tylko w sektorze prywatnym, ale także wśród instytucji publicznych i przedsiębiorstw. Zatem, co dla jednych stanowi problem, dla innych jest szansą. Branża security potrafi tę szansę wykorzystać, czego dowodem nasz raport *Kto sobie radzi najlepiej? Raport Security 50 – wzrosty, nowi gracze i geopolityczne wyzwania* (str. 12), będący podsumowaniem kondycji całego globalnego rynku systemów i usług security. Jak wynika z raportu, wartość tego rynku rośnie. Po pierwsze, dlatego że nie tylko Polska boryka się z problemami kadrowymi w policji, choć nasz kraj znajduje się poniżej średniej UE pod względem liczby funkcjonariuszy przypadających na 100 tys. mieszkańców. Z niedoborem policjantów mierzą się m.in. Francja, Wlk. Brytania, Niemcy i Estonia. Po drugie, kiedy bezpieczeństwo biznesu zależy nie tylko od finansów, ale także od faktycznie jego fizycznej ochrony, każde przedsiębiorstwo sięga po rozwiązanie sprawdzone i niezawodne, czyli współpracę z dostawcą dobrych rozwiązań security. Pracownicy tych firm są często lepiej przeszkoleni w zakresie reagowania na konkretne sytuacje kryzysowe i mogą szybko dostosować swoje działania do zmieniających się warunków. Co więcej, dzięki nowoczesnym technologiom zabezpieczeń firmy te są w stanie zapewnić wysoki poziom ochrony. To zaś ma znaczące przełożenie na wartość rynku security.

Redakcja

CZASOPISMO RYNKU SECURITY

a&S POLSKA

06 (48) / 2024

# SPIS TREŚCI

## HANDEL SIĘ LICZY



## 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

BCS ULTRA


**BCS-U-NVR6408R-A-4K(2X12TB)** **BCS-U-NVR3208R-A-4KR(8TB)**

Nowe rozwiazania BCS Ultra to zwiększony poziom bezpieczeństwa każdego projektu.
Rejestratory od małych 4 kanałowych modeli po rozwiazania serwerowe na 256 kamer
zapewnią ochronę zarówno transmisji wideo, jak również
danym zapisanym na dyskach twardych.

>> Więcej przeczytasz na stronie 8

POLSKA MARKA BCS

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

CZASOPISMO RYNKU SECURITY

a&S POLSKA

06 (48) / 2024

# SPIS TREŚCI



Honeywell

# 35 NOWA SERIA KAMER

# 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
- Łatwa w instalacji i obsłudze

5 YEAR WARRANTY | SECURE BY DEFAULT | ONVIF | SGT | NDAA COMPLIANT | NIS2 DIRECTIVE COMPLIANT

**OFICJALNY DYSTRYBUTOR:**

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

**www.linc.pl**

**WIĘCEJ O NAS:**

Linc Polska Sp. z o.o.

# Prezentujemy najnowsze urządzenia z oferty firm

## Axis Communications, BCS, Hikvision Polska, Linc Polska, TP-Link

AXIS COMMUNICATIONS

## AXIS Camera Station Pro

**AXIS Camera Station Pro to potężny i oferujący wiele funkcji VMS ułatwiający przeglądanie materiału wizyjnego na żywo, wyszukiwanie i eksportowanie nagrań, a także zarządzanie kontrolą dostępu. Dzięki temu, że obsługuje wszystkie urządzenia i narzędzia analityczne Axis, umożliwia stworzenie odpowiedniego rozwiązania sieci prywatnej i korzystanie z opcjonalnej łączności w chmurze.**

AXIS Camera Station Pro oferuje elastyczność i kontrolę niezbędną do wdrożenia niezawodnego systemu opartego na serwerze w sieci prywatnej spełniającego potrzeby biznesowe klienta. Nie ma znaczenia, czy chodzi o jedną lokalizację z małą liczbą kanałów i kilkoma kamerami, kilka lokalizacji, czy też wiele lokalizacji z setkami kamer i innych urządzeń IP.

AXIS Camera Station Pro współpracuje ze wszystkimi produktami z oferty Axis, dzięki czemu można w pełni wykorzystać kamery, interkomy, produkty audio, narzędzia analityczne, kamery nasobne Axis i nie tylko. Obsługuje również produkty innych firm.

Zarządzanie odwiedzającymi i weryfikowanie dostępu umożliwia zakładka AXIS Camera Station Secure Entry. Ujednolicone oprogramowanie kontroli dostępu oraz możliwości VMS pozwalają zarządzać dostępem do budynku, wizualnie weryfikować osoby wchodzące, ostrzegać w przypadku incydentów, a także weryfikować zdarzenia podczas badania incydentów. Skalowalne rozwiązanie zaprojektowane do współpracy z kontrolerami drzwi i czytnikami kart firmy Axis może obsługiwać do 192 drzwi na serwer i do 10 tys. kart z obsługą wielu poświadczeń, takich jak karty, kody PIN, kody QR i tablice rejestracyjne.

Więcej na: www.axis.com/pl-pl

BCS

## Nowa linia produktowa BCS Ultra

**Urządzenia z nowej linii produktowej BCS Ultra doskonale sprawdzają się zarówno w małych domowych instalacjach dzięki zastosowaniu rejestratorów 4-kanałowych BCS-U-NVR0402-A-4K-4P, jak i dużych systemach z rejestratorami 256-kanałowymi BCS-U-SVR25608R-4KR.**

Urządzenia charakteryzują się przede wszystkim zgodnością z wymogami dyrektywy NDAA. Dzięki specjalnym protokołom komunikacji spełnią najbardziej restrykcyjne wymagania związane z cyberbezpieczeństwem infrastruktury teleinformatycznej, zwiększając bezpieczeństwo dostępu do systemu.

Rejestratory wyposażono w wydzieloną sieć dla kamer. Za pomocą specjalnie zaprojektowanego bazodanowego systemu plików – IBANK przechowują nagrania przed niepowołanym dostępem oraz zwiększają odporność na uszkodzenie nośnika danych. Ponadto, stosując funkcję łańcuchowego odcisku palca, można oznaczać edytowane nagranie jako niepoprawne.

Dzięki szerokiemu zastosowaniu funkcji stawiających ochronę systemu na bardzo wysokim poziomie uzyskuje się możliwość stworzenia infrastruktury zgodnej z najnowszymi regułami NIS2.

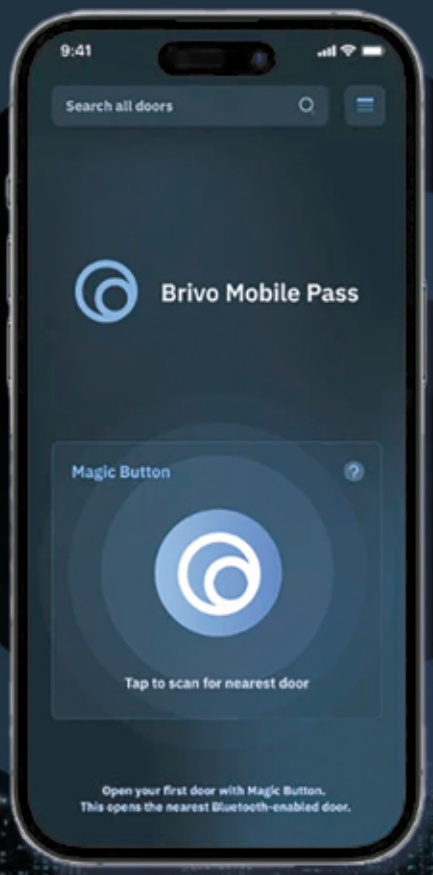
Więcej na: www.bcs.pl

brivo

smart-i

# DOSTĘP JEST PRZYSZŁOŚCIĄ INTELIGENTNYCH BIUR

## ZOPTYMALIZUJ SWOJE NIERUCHOMOŚCI DZIĘKI KONTROLI DOSTĘPU BRIVO




Technologia zabezpieczeń klasy korporacyjnej dla każdego rodzaju obiektu

**60+**

KRAJÓW NA CAŁYM ŚWIECIE

Kontrola dostępu i dane wideo, dzięki którym Twoje budynki staną się bardziej inteligentne

**90+**

TYSIĄCE WDROŻEŃ

Możliwości integracji, aby połączyć istniejące inwestycje technologiczne

**450Mkw**

NIERUCHOMOŚCI W ZARZĄDZANIU

brivo

866.692.7486 | brivo.com

Brivo oferuje kompleksowy zestaw narzędzi dostosowanych do Twoich potrzeb w zakresie kontroli dostępu. Dowiedz się więcej na

www.brivo.com/solutions/commercial-real-estate/

PARTNER:

smart-i | Ul. Marii Rodziewiczówny 1/810, 04-187 Warszawa | www.smart-i.pl

HIKVISION POLSKA

# Zestaw wideodomofonowy 2-wire HD z klawiaturą

**Hikvision wprowadza do oferty zestaw wideodomofonowy z klawiaturą, oparty na technologii 2-wire HD. Technologia 2-wire HD pozwala na jednoczesne przesyłanie dwiema żyłami sygnału sterowania, audio i wideo w rozdzielczości HD. Dzięki tylko dwóm żyłom o średnicy nawet od 0,2 mm każda można wykorzystać już istniejące okablowanie, co znacznie upraszcza i obniża koszty modernizacji systemu domofonów wideo.**

Technologia 2-wire HD pozwala utrzymać duże odległości pomiędzy elementami systemu. Uproszczony proces konfiguracji poszczególnych elementów: kamery, klawiatury, monitora, jest realizowany poprzez wbudowane przełączniki. Dodatkowo stacja bramowa umożliwia aktywację trybu AP *(Access Point)*, który pozwala na programowanie zestawu z poziomu telefonu, bez konieczności instalacji dodatkowych aplikacji. Z poziomu trybu AP można m.in. dodać użytkownika i skonfigurować kod PIN.

Monitor DS-KH7300EY-WTE2/White ma moduł Wi-Fi i po dodaniu do konta Hik-Connect pozwala na zdalne odebranie połączenia. W zestawie znajdują się maskownice pozwalające na personalizację liczby dostępnych przycisków stacji bramowej (brak, jeden lub dwa przyciski). Solidna metalowa obudowa stacji bramowej pozwala na pracę nawet w trudnych zewnętrznych warunkach.

Zestaw zawiera: monitor (DS-KH-7300EY-WTE2/White), stację bramową z kamerą (DS-KD7003EY-IME2/Aluminum), klawiaturę (DS-KD-KP), dystrybutor (DS-KAD7040EY), kartę TF 32GB, zasilacz (36W DIN RAIL PSU) i pakiet akcesoriów. W ofercie dostępne są zestawy z obudową stacji bramowej do montażu natynkowego i podtynkowego.

Więcej na: www.hikvision.com/pl

SMART-I

# Najnowszy trend – kontrola dostępu w chmurze!

**Współczesne organizacje inwestują w hybrydowe miejsca pracy. W efekcie firmy oczekują, że systemy KD będą dostarczać informacji biznesowych, pozwalać na zrozumienie zachowań użytkowników, dokumentować trendy. Te informacje pomogą organizacjom w podejmowaniu lepszych decyzji biznesowych w takich obszarach, jak podróże służbowe, negocjacje najmu czy inwestycje kapitałowe w technologię.**

Wraz z postępującą transformacją cyfrową, która unowocześnia wszystkie aspekty działalności biznesowej, korzyści płynące z KD opartej na chmurze stają się coraz bardziej widoczne, w szczególności niższy całkowity koszt posiadania.

Rozwiązania mobilne umożliwiają użytkownikom otwieranie drzwi, bram i innych systemów wejściowych za pomocą smartfonu. Pandemia przyspieszyła rozwój aplikacji mobilnych z powodu zapotrzebowania na bezdotykowy sposób rejestrowania nowych osób.

Ponadto, w przeciwieństwie do fizycznych kart czy breloków, smartfony są bezpieczniejsze, łatwiejsze w zarządzaniu i bardziej opłacalne.

Kontrola dostępu oparta na chmurze ułatwia integrację z innymi aplikacjami działającymi w chmurze. Oznacza to, że rozwiązania mogą działać szybciej już od pierwszego dnia.

Pakiet bezpieczeństwa Brivo zbudowany na solidnej, opartej na chmurze platformie kontroli dostępu umożliwia i optymalizuje hybrydowe modele pracy, modernizuje operacje i dostarcza dane, które zamieniają praktyczne wnioski w decyzje oparte na danych w całym ekosystemie przedsiębiorstwa.

Więcej na: https://smart-i.pl

&

TP-LINK

# Most bezprzewodowy TP-Link Omada EAP215-Bridge

**TP-Link EAP215-Bridge KIT to zestaw dwóch urządzeń mostu bezprzewodowego pozwalający na przesyłanie sygnału Wi-Fi na duże odległości. To idealne rozwiązanie np. dla rozległych posiadłości z wieloma budynkami czy do obsługi systemów monitoringu na dużym obszarze.**

Urządzenia EAP215-Bridge pracują w paśmie 5 GHz w standardzie 802.11ac i pozwalają na przesyłanie danych z prędkością do 867 Mb/s na odległość nawet 5 km. Każda z jednostek zestawu jest również wyposażona w 3 gigabitowe porty Ethernet umożliwiające stworzenie wydajnej sieci komputerowej, np. do obsługi kamer monitoringu.

Kierunkowe anteny o wysokim zysku 11 dBi pozwalają na bezproblemową transmisję Wi-Fi nawet w najbardziej wymagających warunkach środowiskowych. Dodatkowo możliwość zasilania poprzez pasywne PoE (adapter znajduje się w zestawie z urządzeniem) umożliwia montaż w miejscach, gdzie nie ma dostępu do gniazdka elektrycznego. Niezawodną pracę urządzenia w nawet najtrudniejszych warunkach środowiskowych gwarantuje odporna na warunki atmosferyczne obudowa z certyfikatem IP65 oraz ochroną odgromową 6 kV.

Wsparcie zaawansowanych funkcji, takich jak Omada Mesh, MU-MIMO, Beamforming oraz Airtime Fairness, zapewnia nie tylko doskonałą wydajność, ale także optymalizację działania sieci.

Dzięki scentralizowanemu zarządzaniu w chmurze poprzez platformę Omada SDN oraz automatycznemu parowaniu instalacja i zarządzanie mostem EAP215-Bridge jest niezwykle proste i efektywne, co pozwala na skoncentrowanie się na kluczowych aspektach prowadzonej działalności biznesowej.

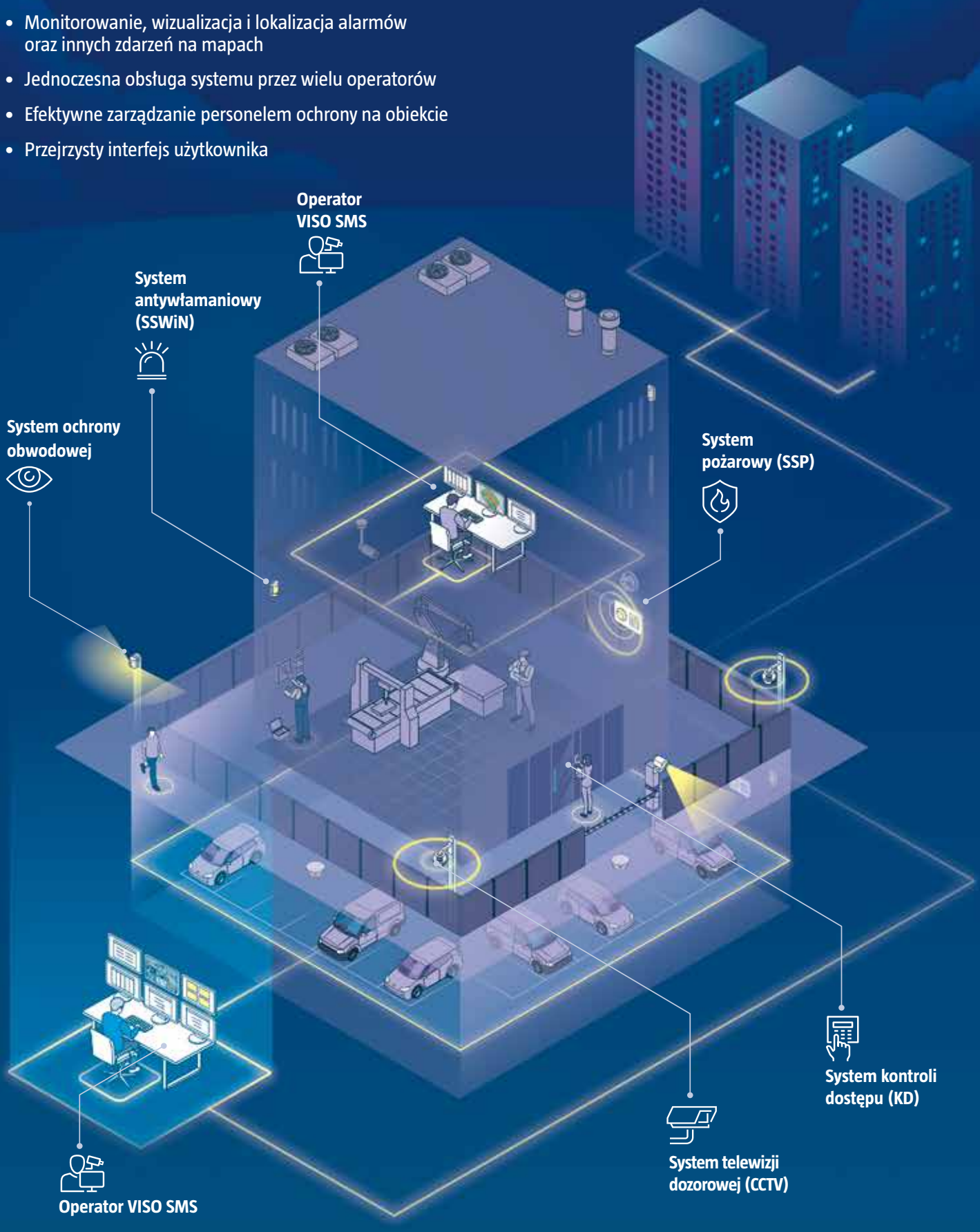
Więcej na: www.tp-link.com/pl

# VISO SMS

# Monitorowanie i wizualizacja systemów bezpieczeństwa

roger
Intelligence for Building

- Integracja z systemami Bosch, Dahua, Hikvision, Honeywell, Milestone, SATEL, Siemens i innymi w ramach jednej platformy
- Monitorowanie, wizualizacja i lokalizacja alarmów oraz innych zdarzeń na mapach
- Jednoczesna obsługa systemu przez wielu operatorów
- Efektywne zarządzanie personelem ochrony na obiekcie
- Przejrzysty interfejs użytkownika




50
2024
SECURITY

# Kto sobie radzi najlepiej?

# SECURITY 50

## wzrosty, nowi gracze i geopolityczne wyzwania


*» Według Banku Światowego średni wzrost produktu krajowego brutto (PKB) w 2023 r. wyniósł 2,6% rok do roku. Nic dziwnego, że także firmy branży security odnotowały zadowalające wzrosty własnych przychodów. «*

Jak co roku publikujemy zestawienie Security 50 zawierające 50 największych pod względem przychodów firm sektora security. Dziesięć z nich, czyli Hikvision Digital Technology, Dahua Technology, ASSA ABLOY, Motorola Solutions, Axis Communications, Allegion, Tiandy, Hanwha Vision, TKH (Smart Vision Systems) i Aiphone, odnotowało wzrost przychodów rok do roku od kilku do kilkunastu procent. Hikvision i Dahua pozostają firmami z największymi przychodami ze sprzedaży produktów security na świecie, osiągając w 2023 r. odpowiednio: 9,31 mld dol. i 4,32 mld dol.

W tegorocznym zestawieniu pojawił się nowy uczestnik: GWELLTIMES, producent inteligentnych kamer, dzwonków do drzwi i reflektorów ze Shenzhen. Na listę wróciły również firmy TKH (Smart Vision Systems), DNAKE, JOVISION i Sparsh CCTV.

## Jest lepiej niż gorzej

Ze wszystkich przedstawianych firm aż 36 firm zanotowało w roku obrachunkowym 2022–2023 wzrost przychodów. Pozostałe nie tylko nie zarobiły, ale wręcz odnotowały straty. Najlepiej powiodło się Sparsh CCTV, GWELLTIMES, Synectics, Kedacom, Evolv, MEARI, CP Plus, Allegion, NAPCO i ASSA ABLOY. Warto zauważyć, że obecne w rankingu firmy z Państwa Środka, poza dwoma, ponownie odnotowały wzrost sprzedaży. W jakiejś mierze jest to skutek ogólnie dobrej kondycji gospodarki chińskiej, co wynika m.in. z szybkiego ożywienia gospodarczego po COVID-19, stymulacji rządowej wspierającej popyt w różnych sektorach oraz większego eksportu.

## Pierwsze półrocze bardzo obiecujące

Dane dotyczące przychodów za pierwsze półrocze 2024 r. napawają optymizmem. Wiele wskazuje na to, że firmy branży security ten rok również zakończą wzrostem przychodów. Większość z nich odnotowała wzrost rok do roku. Można uznać, że branża security w końcu wraca do „normalności" po pandemii COVID-19.

Lepsze przychody są zapewne efektem wystąpienia kilku czynników, w tym większego zainteresowania klientów integracją systemów, większym popytem na rozwiązania dotyczące cyberbezpieczeństwa, a także chmurowe.

Ponadto rośnie popyt na rozwiązania oparte na sztucznej inteligencji (AI) i inteligentnej automatyzacji (IA), chociaż prawda jest taka, że dużemu zainteresowaniu tymi narzędziami wcale nie towarzyszą, przynajmniej na razie, wymierne wyniki finansowe.

Coraz bardziej popularna staje się analiza z zastosowaniem AI, ale wykorzystywana w urządzeniach działających na brzegu sieci. Przyczyną tego stanu rzeczy jest to, że prowadzenie analizy na chmurowych maszynach ma dwa uboczne, nieprzyjemne skutki związane z koniecznością transferu plików wideo na serwery chmurowe. Pierwszym są często nieakceptowalne opóźnienia. Drugim koszt transferu plików. Analiza dokonywana bezpośrednio przez urządzenia funkcjonujące na brzegu sieci jest zatem rozsądną alternatywą, tym bardziej że jeśli jest ona dokonywana na nieskompresowanych obrazach, to siłą rzeczy jest bardziej precyzyjna. Wówczas na serwer chmurowy trafia jedynie „lekka" metadana opisująca zdarzenia i atrybuty, co może się przydać do dalszej analizy.

## Fuzje i przejęcia

Nie ma sensu wróżyć z fusów, zastanawiając się, jak będzie wyglądało podsumowanie tegorocznych wyników finansowych. Warto jednak wiedzieć, że w 2024 r. doszło do kilku znaczących fuzji i przejęć, które na te wyniki mogą mieć wpływ. Jednym z nich jest przejęcie działu bezpieczeństwa Identiv przez Grupę Vitaprotech za 145 mln dol., przejęcie działu bezpieczeństwa Carrier przez Honeywell za 4,95 mld dol. oraz połączenie Milestone z BriefCam i Arcules – w tym przypadku firmy wykorzystały fakt, że każda z nich ma inną mocną stronę. Dzięki tej fuzji będą mogły oferować kompletne rozwiązania łączące oprogramowanie do zarządzania materiałem wizyjnym, analitykę wideo i VSaaS.

Można się spodziewać, że wiodące w branży firmy security w dalszym ciągu będą dążyć do współpracy z organizacjami zajmującymi się analityką bazującą na AI, zwiększając swoje zdolności w zakresie dozoru predykcyjnego i automatycznego wykrywania zagrożeń. Ten trend jest wyjątkowo mocny.

## Zawsze coś

Dobre zeszłoroczne wyniki i nie najgorsze tegoroczne prognozy nie zmieniają faktu, że przed branżą stoją pewne wyzwania. Jednym z nich jest utrzymująca się liczba cyberataków. Urządzenia wykorzystywane w branży zabezpieczeń, coraz częściej funkcjonujące w ramach IoT są atakowane równie chętnie jak „poważne" laptopy i komputery stacjonarne. Zagrożenie cyberatakami nie zmalało w 2024 r., a liczba głośnych naruszeń bezpieczeństwa i dużych wycieków danych wciąż rośnie. Pojawia się także więcej ostrzeżeń o potencjalnych atakach sponsorowanych przez wrogie państwa. Z tego względu cyberbezpieczeństwo pozostaje jednym z największych wyzwań, przed jakimi stoi sektor bezpieczeństwa. Nie można też nie zauważyć, że surowe regulacje dotyczące prywatności danych także nie ułatwiają życia firmom z branży. Mowa zwłaszcza o tych firmach, które oferują urządzenia wyposażone np. w funkcje rozpoznawania twarzy albo stosujące inne metody biometryczne. Dla nich zgodność z przepisami może być naprawdę sporym wyzwaniem.

Eksperci wskazują też na zestaw innych problemów, z którymi boryka się branża security: brak rąk do pracy lub niedostatek kompetencji, nieefektywność łańcucha dostaw, ograniczenia budżetowe sygnalizowane przez klientów oraz rosnące obawy o bezpieczeństwo infrastruktury krytycznej. Pod tym względem w roku 2025 wiele się zapewne nie zmieni, a to znaczy, że aby się uporać z niektórymi z wymienionych wyzwań, liderzy w firmach security powinni pomyśleć przynajmniej o szkoleniach dla pracowników, wprowadzaniu innowacyjnych programów bezpieczeństwa oraz wzmocnieniu relacji z partnerami z własnej branży.

Na branżę mają też wpływ konflikty zbrojne – szczególnie wojny w Ukrainie i na Bliskim Wschodzie. Trochę za ich sprawą wzrosło zapotrzebowanie na systemy dozoru, zwłaszcza w obszarach wrażliwych, takich jak infrastruktura krytyczna. Konflikty te zwiększyły potrzebę szybkich rozwiązań dozoru obsługiwanych przez AI do wykrywania zagrożeń w czasie rzeczywistym. Na rozwój rynku wpłynęły także wyższe wydatki rządowe na obronę i bezpieczeństwo.

Skutki trwających konfliktów zbrojnych są jednak trudne do przewidzenia. Można spodziewać się rosnącej niestabilności w regionie, zakłóceń w globalnym transporcie, większej wymuszonej migracji, ale też wzrostu napięć międzynarodowych prowadzących do nałożenia ceł, po rozwój nowych broni i metod prowadzenia wojen.

## Co dalej?

Branża security znajduje się na ścieżce wzrostu. Według niedawnego wspólnego raportu SIA, ASIS i Omdia średnioroczny wzrost wartości rynku urządzeń security w latach 2022–2026 ma wynieść 8,2%, a dla rynku usług ochrony: 6,9%. Kluczowymi czynnikami mającymi na to wpływ będą rosnąca popularność kontroli dostępu świadczonej jako usługi (*Access Control as a Service* – ACaaS) oraz monitoringu wideo jako usługi (*Video Surveillance as a Service* – VSaaS). Te technologie pozostaną kluczowe dla ewolucji branży, ponieważ organizacje szukają skalowalnych, elastycznych i wydajnych rozwiązań zabezpieczających.

Zapotrzebowanie na zaawansowane rozwiązania zabezpieczające będzie zapewne rosnąć. Sprzyja temu trwająca urbanizacja, rozwój inteligentnych miast oraz dalsza niestabilność geopolityczna. Kluczowe czynniki wzrostu obejmują rosnące zastosowanie AI i oprogramowania analitycznego, zwłaszcza analityki behawioralnej, rozwój platform opartych na chmurze oraz większy nacisk na cyberbezpieczeństwo i systemy zgodne z NDAA. W niedalekiej przyszłości na rynek wpłyną również rosnące znaczenie zrównoważonego rozwoju i rozwiązań energooszczędnych.

Niektórzy eksperci przewidują, że rok 2025 przyniesie nowe innowacje, zwłaszcza w dziedzinach kryptografii kwantowej i autonomicznego nadzoru dronów. Szyfrowanie kwantowe, z jego potencjałem zabezpieczania komunikacji przed najbardziej zaawansowanymi zagrożeniami cybernetycznymi, może zdefiniować przyszłość cyberbezpieczeństwa. Autonomiczne drony wyposażone w AI mogą odegrać większą rolę w monitorowaniu rozległych obszarów przy minimalnej interwencji ludzkiej. Na horyzoncie pojawia się również nowa generacja biometrii, pozwalająca na rozpoznawanie chodu i identyfikację głosu, która może stać się powszechna. Te innowacje pomogą rozwiązać nieustannie zmieniające się wyzwania, przed którymi stają profesjonaliści w dziedzinie bezpieczeństwa, zapewniając, że branża pozostanie w czołówce pod względem zagrożeń zarówno fizycznych, jak i cybernetycznych. ●

# Największe firmy branży security na świecie

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

Analizując dane notowane w publicznych lub przesłanych przez firmy raportach finansowych za rok 2023, 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 2023 i rok budżetowy 2022, 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 2022-23. ●

| 2024 S50 | 2023 S50 | NAZWA FIRMY | GŁÓWNY OBSZAR DZIAŁANIA | SIEDZIBA | PRZYCHÓD W 2023 R. (MLN USD) | PRZYCHÓD W 2022 R. (MLN USD) | WZROST PRZYCHODU (2023-2022) |
|---|---|---|---|---|---|---|---|
| 1 | 1 | HIKVISION DIGITAL TECHNOLOGY (telewizja dozorowa) | różne | Chiny | 9721,52 | 9 310,8 | 4,4% |
| 2 | 2 | DAHUA TECHNOLOGY | różne | Chiny | 4553,83 | 4 320,2 | 5,4% |
| 3 | 3 | ASSA ABLOY (zamki mechaniczne i elektromechaniczne) | kontrola dostępu | Szwecja | 3977,65 | 3 414,5 | 16,5% |
| 4 | 5 | MOTOROLA SOLUTIONS (telewizja dozorowa i analityka) | różne | USA | 1726,00 | 1 523,0 | 13,3% |
| 5 | 4 | AXIS COMMUNICATIONS | różne | Szwecja | 1639,13 | 1 499,2 | 9,3% |
| 6 | 6 | ALLEGION (kontrola dostępu i urządzenia elektroniczne) | kontrola dostępu | USA | 1022,22 | 850,7 | 20,2% |
| 7 | 7 | TIANDY | telewizja dozorowa | Chiny | 858,54 | 766,6 | 12,0% |
| 8 | 8 | HANWHA VISION | telewizja dozorowa | Korea Płd. | 801,02 | 767,0 | 4,4% |
| 9 | N/A | TKH (Smart Vision) | różne | Holandia | 539,86 | 530,83 | 1,7% |
| 10 | 10 | AIPHONE | interkomy | Japonia | 436,51 | 375,8 | 16,1% |
| 11 | 11 | INTELBRAS | różne | Brazylia | 434,44 | 386,9 | 12,3% |
| 12 | 13 | CP PLUS | telewizja dozorowa | Indie | 338,60 | 278,3 | 21,7% |
| 13 | 15 | DONGGUAN YUTONG OPTICAL TECHNOLOGY | telewizja dozorowa (obiektywy) | Chiny | 303,18 | 260,9 | 16,2% |
| 14 | 12 | VIVOTEK | telewizja dozorowa | Tajwan | 294,04 | 319,3 | -7,9% |
| 15 | 14 | ZKTECO | różne | Chiny | 278,47 | 271,2 | 2,7% |
| 16 | 16 | MILESTONE SYSTEMS | telewizja dozorowa | Dania | 244,97 | 216,0 | 13,4% |
| 17 | 17 | NEDAP | różne | Holandia | 192,96 | 171,8 | 12,3% |
| 18 | 21 | NAPCO SECURITY TECHNOLOGIES | różne | USA | 170,00 | 143,6 | 18,4% |
| 19 | 20 | TVT DIGITAL TECHNOLOGY | telewizja dozorowa | Chiny | 153,42 | 137,2 | 11,8% |
| 20 | 18 | IDIS | telewizja dozorowa | Korea Płd. | 153,37 | 162,3 | -5,5% |
| 21 | 25 | KEDACOM (telewizja dozorowa) | telewizja dozorowa | Chiny | 144,05 | 109,9 | 31,1% |
| 22 | 22 | OPTEX (systemy alarmowe) | systemy alarmowe | Japonia | 125,43 | 114,3 | 9,7% |
| 23 | 19 | INFINOVA | telewizja dozorowa | Chiny | 121,58 | 150,8 | -19,4% |
| 24 | 26 | IDENTIV | kontrola dostępu | USA | 116,38 | 112,9 | 3,1% |
| 25 | 27 | GALLAGHER | kontrola dostępu | Nowa Zelandia | 114,92 | 108,8 | 5,6% |
| 26 | N/A | DNAKE | interkomy | Chiny | 111,31 | 108,4 | 2,7% |
| 27 | 23 | COMMAX | systemy alarmowe i automatyka | Korea Płd. | 104,85 | 119,4 | -12,2% |
| 28 | 24 | RAYSHARP | telewizja dozorowa | Chiny | 96,95 | 112,2 | -13,6% |
| 29 | 31 | MEARI | systemy alarmowe i automatyka | Chiny | 95,11 | 77,5 | 22,7% |
| 30 | 32 | KOCOM | systemy alarmowe i automatyka | Korea Płd. | 76,90 | 72,9 | 5,5% |
| 31 | N/A | JOVISION | telewizja dozorowa | Chiny | 76,22 | 76,2 | 0,1% |
| 32 | N/A | GWELLTIMES | systemy alarmowe i automatyka | Chiny | 72,96 | 50,8 | 43,8% |
| 33 | 28 | SUPREMA | kontrola dostępu | Korea Płd. | 72,42 | 68,4 | 5,9% |
| 34 | 30 | TAMRON (telewizja dozorowa i obiektywy) | telewizja dozorowa (obiektywy) | Japonia | 69,65 | 80,0 | -12,9% |
| 35 | 35 | MOBOTIX | telewizja dozorowa | Niemcy | 68,36 | 60,6 | 12,7% |
| 36 | 33 | FOCTEK PHOTONICS | telewizja dozorowa (obiektywy) | Chiny | 65,95 | 64,0 | 3,0% |
| 37 | 38 | EVOLV TECHNOLOGY | systemy weryfikujące | USA | 64,28 | 50,9 | 26,4% |
| 38 | 36 | DYNACOLOR | telewizja dozorowa | Tajwan | 49,13 | 56,0 | -12,3% |
| 39 | 39 | GEOVISION | telewizja dozorowa | Tajwan | 40,57 | 42,3 | -4,1% |
| 40 | 44 | SYNECTICS (dział systemów) | telewizja dozorowa | Wlk. Brytania | 39,82 | 30,1 | 32,3% |
| 41 | 41 | UNION COMMUNITY | kontrola dostępu | Korea | 39,21 | 35,3 | 11,0% |
| 42 | N/A | Sparsh CCTV | telewizja dozorowa | Indie | 32,90 | 20,8 | 58,1% |
| 43 | 42 | SENSTAR TECHNOLOGIES | różne | Izrael | 32,79 | 35,6 | -7,8% |
| 44 | 40 | HI SHARP ELECTRONICS | telewizja dozorowa | Tajwan | 31,27 | 34,4 | -9,1% |
| 45 | 43 | C-PRO ELECTRONICS | telewizja dozorowa | Korea Płd. | 26,03 | 33,8 | -22,9% |
| 46 | 46 | ACTI | telewizja dozorowa | Tajwan | 15,67 | 15,0 | 4,5% |
| 47 | 48 | AVA GROUP | różne | Australia | 14,90 | 12,8 | 16,1% |
| 48 | 49 | EVERFOCUS ELECTRONICS | telewizja dozorowa | Tajwan | 11,72 | 10,4 | 12,5% |
| 49 | 45 | ITX AI | telewizja dozorowa | Korea Płd. | 10,25 | 19,8 | -48,2% |
| 50 | 47 | THRUVISION | weryfikacja osób | Wlk. Brytania | 9,72 | 15,4 | -37,1% |

# Głos światowych ekspertów

Każdego roku publikujemy raport Security 50, w którym przedstawiamy najlepsze firmy w branży zabezpieczeń i analizujemy trendy. Jak wypadła branża zabezpieczeń w tym roku? Czy w najbliższym czasie oczekiwany jest jej wzrost? Czy firmy dostosowały się do rosnących potrzeb klientów? Odpowiedzi na te pytania podjęli się eksperci z największych firm.

### Jaka jest ogólna kondycja branży zabezpieczeń w 2024 r.? Jakie były główne czynniki wzrostu w tym roku i czy przewiduje się dalszy rozwój w 2025 r.?

**Allen Tang:** *W roku 2024 zauważyliśmy stabilny wzrost w branży zabezpieczeń, ponieważ bezpieczeństwo pozostaje podstawową potrzebą społeczną. Oprócz segmentu wideo nastąpił rozwój w takich sektorach, jak kontrola dostępu, systemy alarmowe oraz systemy wyświetlania. Wzrosła też liczba aplikacji branżowych w transporcie, produkcji, edukacji, handlu detalicznym i logistyce. W 2025 roku oczekujemy dalszego wzrostu.*

**Fu Liquan:** *Globalne ożywienie gospodarcze wciąż nie nabiera tempa, pojawiają się lokalne trudności, a sytuacja geopolityczna jest niepewna. Mimo to obserwujemy szybki rozwój takich technologii jak sztuczna inteligencja, Internet rzeczy (IoT) i cyfrowe bliźniaki. To one wzmacniają tempo wdrażania nowych produktów i aplikacji. Przyszłym możliwościom towarzyszyć będą zapewne wyzwania, szczególnie związane z transformacją cyfrową i rosnącym zapotrzebowaniem na inteligentne, oparte na danych rozwiązania bezpieczeństwa.*

**Ray Mauritsson:** *Na całym świecie rośnie zapotrzebowanie na urządzenia i usługi security, co pozytywnie wpływa na rozwój rynku. W roku 2025 zapewne nic się w tym względzie nie zmieni. Postęp technologiczny napędza wzrost, a innowacje oferują nowe i lepsze sposoby zaspokajania potrzeb klientów w zakresie bezpieczeństwa.*

**Chuck Jeon:** *Branża zabezpieczeń w 2024 r. nie może narzekać na brak innowacji i zapotrzebowanie na jej urządzenia i usługi. Jest to szczególnie widoczne w krajach, które przechodzą gwałtowną urbanizację i rozwijają swoją infrastrukturę. Jeśli chodzi o urządzenia, to z pewnością na znaczeniu zyskały te, które wyposażono w algorytm AI, zwłaszcza kamery funkcjonujące na brzegu sieci. Dzięki nim możliwe jest lokalne przetwarzanie danych, co zmniejsza opóźnienia i zużycie przepustowości, oferując jednocześnie analizy w czasie rzeczywistym i ulepszone funkcje bezpieczeństwa.*

### Jakie trendy rynkowe lub technologiczne są obecnie szczególnie istotne w branży zabezpieczeń i jak wpływają na strategie firm?

**Allen Tang:** *Wierzymy, że kluczem do sukcesu są innowacje. Inwestujemy zatem w badania i rozwój, aby tworzyć produkty spełniające potrzeby rynku oraz poprawiające bezpieczeństwo i efektywność operacyjną klientów.*

**Fu Liquan:** *Konsekwentnie inwestujemy ponad 10% przychodów w badania i rozwój, co umożliwia nam wprowadzanie konkurencyjnych produktów. Skupiamy się na badaniach nad percepcją wielowymiarową, modelach AI, inteligentnym przetwarzaniu danych i robotach mobilnych.*

**Ray Mauritsson:** *Nadal rozwijamy wysokiej jakości produkty i rozwiązania, rozszerzając naszą ofertę o systemy interkomowe, audio i kontrolę dostępu, koncentrując się przy tym na cyberbezpieczeństwie, jakości, usługach i zrównoważonym rozwoju.*

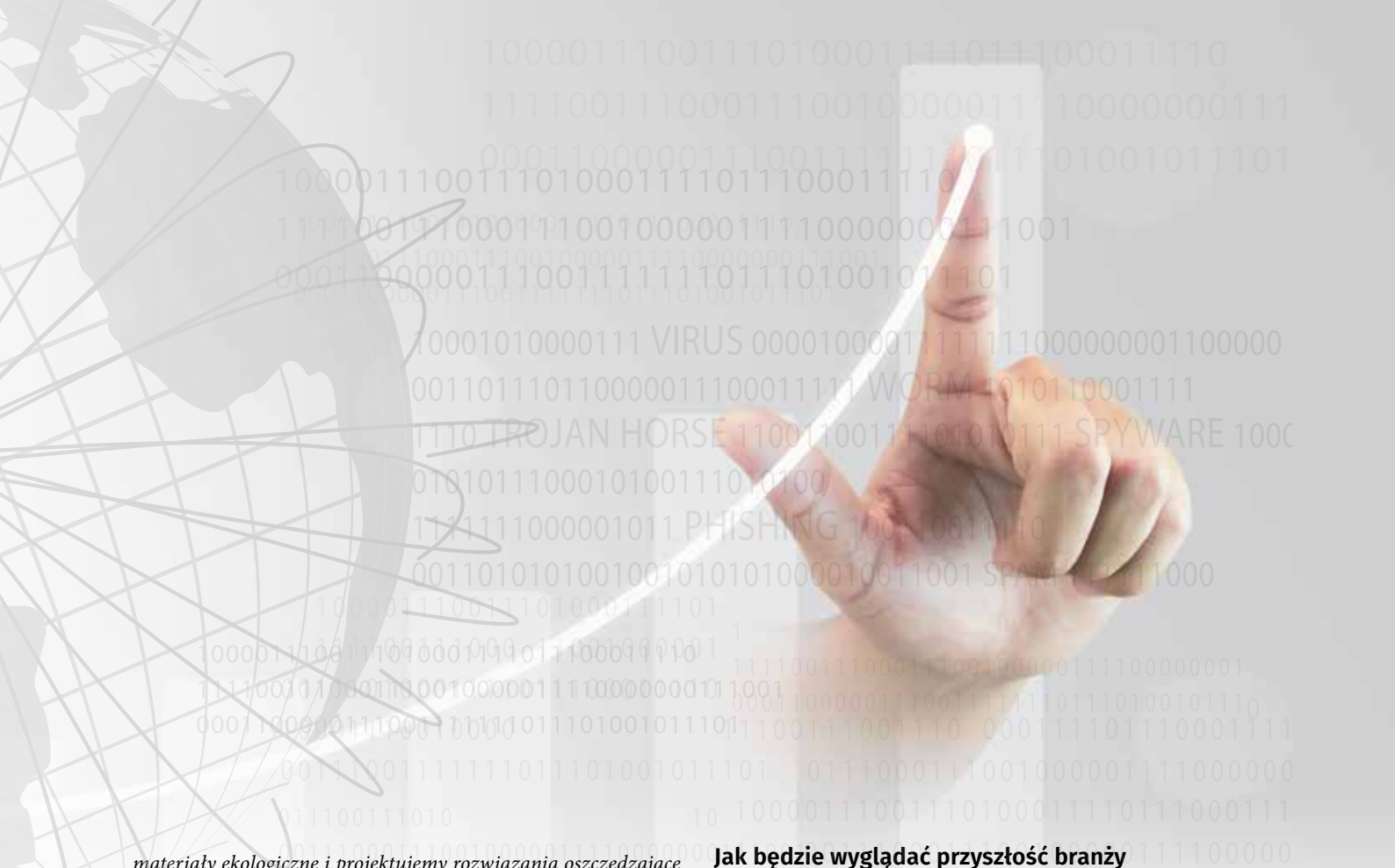
**Chuck Jeon:** *Nasza strategia obejmuje innowacje oraz tworzenie partnerstw technologicznych, które zapewniają klientom optymalizację efektywności i dostosowanie do potrzeb.*

### Jakie dodatkowe działania wspierają strategię zrównoważonego rozwoju w firmach?

**Allen Tang:** *W Hikvision koncentrujemy się na opracowywaniu i wdrażaniu technologii przyjaznych dla środowiska. Wykorzystujemy*

**Allen Tang**
wiceprezes Hikvision
International Business Center

**Fu Liquan**
przewodniczący i prezes
Dahua Technology



*materiały ekologiczne i projektujemy rozwiązania oszczędzające energię, co wpływa na zmniejszenie emisji dwutlenku węgla. Wspieramy inicjatywy dotyczące ochrony środowiska, zarządzania ruchem oraz inteligentnych budynków. Ponadto łączymy rozwój technologii zrównoważonych z transformacją cyfrową, co umożliwia bardziej wydajne zarządzanie miastami i przedsiębiorstwami.*

**Fu Liquan:** *Zrównoważony rozwój jest kluczowym elementem naszej strategii. W ramach strategii Dahua Think#2.0 integrujemy inteligencję z myśleniem ekologicznym, starając się wspierać różne sektory, od ochrony przyrody po zarządzanie zasobami energetycznymi. Poprzez innowacje cyfrowe pomagamy przedsiębiorstwom w ich transformacji ku bardziej zrównoważonym i ekologicznym procesom, co jest również odpowiedzią na potrzeby w zakresie ochrony różnorodności biologicznej.*

**Ray Mauritsson:** *W Axis zrównoważony rozwój jest fundamentem naszego podejścia biznesowego. Zwracamy uwagę na wybór materiałów i optymalizację energetyczną naszych produktów, dążąc do zmniejszenia śladu węglowego. Ponadto nasze praktyki operacyjne są zgodne z rygorystycznymi standardami środowiskowymi, by mieć pewność, że nasze działania biznesowe są odpowiedzialne i wspierają globalne cele zrównoważonego rozwoju.*

**Chuck Jeon:** *W Hanwha Vision dbamy o to, by nasze działania były zgodne z międzynarodowymi standardami zrównoważonego rozwoju, co potwierdza uzyskany przez naszą firmę certyfikat ISO 37301. Inwestujemy w projekty, które wspierają ekologiczne zarządzanie zasobami oraz wprowadzamy energooszczędne technologie do naszych produktów, aby minimalizować ich wpływ na środowisko.*

## Jak będzie wyglądać przyszłość branży zabezpieczeń w perspektywie długoterminowej?

**Allen Tang:** *Przyszłość branży zabezpieczeń jest związana z dalszym rozwojem AIoT oraz automatyzacją operacyjną. Technologie te będą napędzać wzrost w sektorach, które potrzebują nie tylko bezpieczeństwa, ale także efektywności operacyjnej. Wierzymy, że nastąpi zwiększenie zapotrzebowania na inteligentne systemy, które integrują różne technologie, by zapewniać bezpieczne, efektywne i ekologiczne rozwiązania.*

**Fu Liquan:** *W perspektywie długoterminowej inteligentne cyfrowe zabezpieczenia zintegrowane z urządzeniami IoT przyczynią się do tworzenia bardziej złożonych systemów, funkcjonujących w cyfrowych miastach. Spodziewamy się, że przyszłe rozwiązania będą ściśle związane z zarządzaniem danymi i nowoczesnymi technologiami, umożliwiając skuteczniejszą analizę i przewidywanie zagrożeń.*

**Ray Mauritsson:** *Przyszłość branży security będzie związana z integracją z AI, algorytmami głębokiego uczenia i zaawansowaną analizą danych. Kluczowym elementem będzie również zgodność z regulacjami dotyczącymi bezpieczeństwa, co stanie się standardem w związku z zaawansowanymi rozwiązaniami analitycznymi.*

**Chuck Jeon:** *W miarę rozwoju technologii Edge AI i dalszego rozwoju IoT będziemy obserwować wzrost zainteresowania rozwiązaniami cyberbezpieczeństwa i zarządzania danymi. Technologie te zapewnią większą dokładność analiz, a to sprawi, że nadchodzące rozwiązania będą bardziej zaawansowane, efektywne i zrównoważone.* ●

**Ray Mauritsson**
prezes Axis Communications

**Chuck Jeon**
wiceprezes i szef Działu Sprzedaży APAC Hanwha Vision

# Dojrzałość i przydatność trendów technologicznych w 2024 r.

Przedstawiamy wyniki ankiety przeprowadzonej przez asmag.com, dotyczącej trendów, które zdominowały branżę security w roku 2024.

Przedstawiciele ankietowanych organizacji oceniali nie tylko przydatność i dojrzałość technologii zabezpieczeń, ale także zainteresowanie klientów tymi technologiami oraz ich potencjał wzrostu w najbliższym czasie. W badaniu, którego partnerem była firma ZKTeco, wzięło udział 250 firm. Mamy nadzieję, że wyniki ankiety pomogą czytelnikom lepiej zrozumieć trendy technologiczne, które zdominowały naszą branżę, a tym samym lepiej przystosować się do przyszłych oczekiwań klientów.

## Architektura chmurowa i hybrydowa

Monitoring wizyjny jako usługa (VSaaS) oraz kontrola dostępu jako usługa (ACaaS), które coraz częściej są wdrażane przez podmioty z branży bezpieczeństwa, nie wydają się szczególnie różne od rozwiązań, jakie oferowano już w roku 2023. Ich popularność rośnie, ale same technologie nie wykazują znaczącej zmiany w zakresie przydatności i dojrzałości. Niezależnie od tego ACaaS zajmuje pierwsze miejsce w rankingu technologii kontroli dostępu o wysokim potencjale wzrostu.

Warto podkreślić, że architektura hybrydowa uzyskała wyższe oceny: 4,03 w zakresie przydatności i 3,7 w zakresie dojrzałości. W odniesieniu do zapytań klientów i potencjału wzrostu architektura hybrydowa zajmuje odpowiednio 4. i 3. miejsce. Wyniki pokazują, że rozwiązania chmurowe nie tracą na popularności, szczególnie w przypadku chmury hybrydowej, która rozdziela przetwarzanie i przechowywanie danych pomiędzy infrastrukturą lokalną a chmurą.

Według ekspertów architektura hybrydowa zyskuje na popularności, ponieważ łączy najlepsze cechy systemów lokalnych i chmurowych. Pozwala organizacjom zachować kontrolę nad najbardziej wrażliwymi danymi, jednocześnie umożliwia im korzystanie z wydajności serwerów chmurowych oraz wygodę zarządzania nimi. To rozwiązanie jest szczególnie przydatne firmom mającym systemy starszego typu, które nie mogą zostać przeniesione do chmury.

W przypadku chmury hybrydowej wszystkie systemy działające na serwerach lokalnych lub połączonych z chmurą, niezależnie od ich liczby, mogą być centralnie zarządzane z jednej platformy. Podejście hybrydowe upraszcza też przejście na systemy chmurowe w kontrolowanym tempie, umożliwiając przystosowanie urządzeń brzegowych do pracy z chmurą, dodanie usług chmurowych do istniejącej infrastruktury oraz stworzenie długoterminowej strategii, która maksymalizuje zwrot z inwestycji, jednocześnie unikając kosztownych modernizacji.

## Generatywna sztuczna inteligencja

Generatywna sztuczna inteligencja (*Generative AI*) to rodzaj sztucznej inteligencji, która potrafi tworzyć nowe treści na podstawie przekazanych jej zbiorów danych. Narzędzie to może przynieść branży zabezpieczeń swoisty przełom, dlatego uzyskało ocenę przydatności 4,16 i zajmuje pierwsze miejsce pod względem zarówno zainteresowania klientów, jak i przewidywanego potencjału wzrostu w ciągu najbliższych pięciu lat.

Generatywna SI przyciąga wiele uwagi w kontekście bezpieczeństwa ze względu na możliwość poprawy dokładności i szybkości wykrywania zagrożeń oraz zmniejszenia liczby fałszywych alarmów. Ucząc się z ogromnych zbiorów danych, generatywna SI potrafi identyfikować wzorce, które ludzie mogą przeoczyć. I choć jest jeszcze w fazie rozwoju, to postępuje on tak szybko, że dla branży security jej adaptacja powinna być priorytetem. Należy się zatem spodziewać coraz bardziej innowacyjnych aplikacji, które zrewolucjonizują podejście do bezpieczeństwa fizycznego i cyfrowego.

Niektórzy eksperci dostrzegają jednak, że generatywna SI może być źródłem zagrożeń, takich jak rosnąca liczba *deepfake'ów* i podatności na błędy w modelach bazowych, które są szkolone na ogromnych ilościach publicznie dostępnych danych z Internetu. Modele te coraz częściej stają się celem ataków, np. poprzez próby wprowadzania złośliwych danych do zbiorów treningowych. Branża security musi szczególnie uważać na identyfikację i neutralizację tych zagrożeń, aby zapewnić integralność i bezpieczeństwo swoich systemów. Jeśli jednak SI zostanie wprowadzona z zachowaniem restrykcyjnych zasad bezpieczeństwa, to może prowadzić do szybszych reakcji i bardziej efektywnych dochodzeń, co ostatecznie poprawi efektywność operacyjną.

## Przetwarzanie na brzegu sieci

Przetwarzanie na brzegu sieci uzyskało ocenę przydatności 4,3 i dojrzałości 3,86. W kategorii zapytań klientów zajmuje 3. miejsce. Tak wysoka ocena przydatności dowodzi, że użytkownicy cenią korzyści wynikające z przetwarzania danych na brzegu, kiedy jedynie metadane są przesyłane do systemu głównego w celu dalszej analizy. Takie podejście umożliwia lepsze wykorzystanie przepustowości oraz szybszą reakcję na incydenty. Do rozwoju tego trendu przyczynia się również coraz większa dostępność kamer wyposażonych w sztuczną inteligencję.

## Cyberbezpieczeństwo

Cyberbezpieczeństwo otrzymało ocenę przydatności 4,39 i dojrzałości 3,91. Zajmuje też drugie miejsce pod względem zapytań klientów i potencjału wzrostu. Wyniki te odzwierciedlają rosnące znaczenie cyberbezpieczeństwa w obliczu wysokiej liczby ataków. Według danych Broadcom kamery podłączone do Internetu stanowiły cel 15% wszystkich ataków na IoT. Ankieta *US News and World Report* pokazuje, że 13% respondentów doświadczyło włamań do oprogramowania tych urządzeń, a 49% pytanych obawia się, że ich urządzenia staną się ofiarą takiego ataku. To skłoniło producentów do projektowania rozwiązań z uwzględnieniem zasad cyberbezpieczeństwa.

Producenci urządzeń monitoringu wizyjnego coraz częściej podkreślają zgodność z ustawą NDAA, która zabrania używania kluczowych komponentów pochodzących z Chin.

## Bezzałogowe drony i roboty

Jeśli chodzi o drony i roboty, technologia ta uzyskała umiarkowane oceny przydatności i dojrzałości na poziomie odpowiednio: 3,7 i 3,34, zajmując czwarte miejsce pod względem potencjału wzrostu w najbliższej przyszłości. Temat bezpieczeństwa bezzałogowego był szeroko omawiany kilka lat temu, ale zainteresowanie użytkowników i entuzjazm w tej kwestii nieco osłabły. Niemniej jednak drony nadal znajdują zastosowanie, zwłaszcza w krytycznych misjach, w których monitoring za pomocą kamer stacjonarnych okazuje się niewystarczający. Drony wyposażone w kamery wizyjne i termowizyjne mogą wykrywać np. małe źródła ognia, mogące się przekształcić w większe pożary.

Ranking technologii bezpieczeństwa wg zapytań klientów

| MIEJSCE | TECHNOLOGIA |
|---|---|
| 1 | Sztuczna inteligencja (generatywna SI) |
| 2 | Cyberbezpieczeństwo / rozwiązania cyberochrony |
| 3 | Przetwarzanie / magazynowanie na brzegu sieci |
| 4 | Architektura chmurowa hybrydowa |
| 5 | Platformy bezzałogowe |
| 6 | 5G |
| 7 | Radar i lidar |

Ranking technologii bezpieczeństwa wg potencjału wzrostu

| MIEJSCE | TECHNOLOGIA |
|---|---|
| 1 | Sztuczna inteligencja (generatywna SI) |
| 2 | Cyberbezpieczeństwo / rozwiązania cyberochrony |
| 3 | Architektura chmurowa hybrydowa |
| 4 | Platformy bezzałogowe |
| 5 | 5G |
| 6 | Przetwarzanie / magazynowanie na brzegu sieci |
| 7 | Radar i lidar |

# Monitoring wizyjny:
## 4K i kamery do zastosowań specjalnych wyznaczają trendy

W tegorocznym badaniu dotyczącym technologii w monitoringu wizyjnym pod względem przydatności i dojrzałości wysoko zostały ocenione kamery 4K, kamery do pracy w słabym oświetleniu oraz kamery wieloprzetwornikowe. Coraz większą popularność zdobywają także przemysłowe karty microSD, które charakteryzują się wyższą trwałością i niezawodnością niż ich konsumenckie odpowiedniki.

William Pao

### Monitoring wizyjny jako usługa (VSaaS)

Jeśli chodzi o monitoring wizyjny w formie usługi (VSaaS), technologia ta osiągnęła w 2024 r. ocenę przydatności na poziomie 3,75 oraz dojrzałości: 3,63. To nieznaczny spadek w porównaniu z wynikami z 2023 r., wynoszącymi odpowiednio: 4,04 i 3,82. W rankingu technologii, które wzbudzają największe zainteresowanie klientów, VSaaS zajmuje 8. miejsce, a w rankingu technologii z największym potencjałem wzrostu plasuje się na 4. pozycji. Choć wyniki są umiarkowane, nadal widoczny jest potencjał w odniesieniu do rozwoju VSaaS, który w najbliższym czasie nie zniknie.

Zainteresowanie monitoringiem wizyjnym wykorzystującym serwery chmurowe pozostaje wysokie ze względu na jego elastyczność, łatwość wdrożenia i niższe koszty początkowe. Wiele firm sukcesywnie odchodzi od tradycyjnych systemów utrzymywanych na serwerach lokalnych, więc potencjał wzrostu pozostaje znaczący. Ponadto integracja analizy wideo, sztucznej inteligencji i przetwarzania na krawędzi przesuwa VSaaS na wyższy poziom efektywności, co przyczyni się do jego dalszego rozwoju w nadchodzących latach. VSaaS umożliwia organizacjom zdalne zarządzanie systemami monitoringu, oferując automatyczne aktualizacje, elastyczne opcje przechowywania oraz wzmocnione zabezpieczenia.

## Kamery coraz doskonalsze

Przeprowadziliśmy ankietę wśród czytelników na temat różnych innowacyjnych technik pojawiających się w kamerach dozoru wizyjnego. Szczególnie dobrze wypadły kamery z obsługą słabego oświetlenia oraz kamery wieloprzetwornikowe, które uzyskały wysokie oceny przydatności i dojrzałości – odpowiednio: 4,34 i 4,25 oraz 3,94 i 3,82. Oba typy tych urządzeń zajmują wysokie miejsca w rankingu zapytań klientów (kamery z obsługą słabego oświetlenia na pierwszym miejscu, a kamery wieloprzetwornikowe na drugim). Oferują one bowiem przydatne funkcje w dozorze wizyjnym – kamery z obsługą słabego oświetlenia dobrze rejestrują kolory w warunkach ograniczonego światła, a kamery wieloprzetwornikowe umożliwiają objęcie dużych obszarów przy mniejszej liczbie urządzeń i licencji. W badaniu uwzględniliśmy też kamery bispektralne, łączące moduł wizyjny i termowizyjny w jednym urządzeniu. Jeśli chodzi przydatność i dojrzałość, otrzymały umiarkowane oceny (odpowiednio: 3,75 oraz 3,62). Mimo to trzeba pamiętać, że są nad wyraz przydatne w przypadku ochrony obwodowej, zwłaszcza obiektów przemysłowych i infrastruktury krytycznej, dlatego oczekujemy dalszego zainteresowania tą technologią.

## Przemysłowe karty microSD i dyski SSD

Przeanalizowaliśmy również opinie użytkowników na temat przechowywania materiału wizyjnego w urządzeniach brzegowych, które zdobywają popularność w systemach monitoringu wizyjnego. Mowa o przemysłowych kartach microSD oraz dyskach SSD. Karty microSD uzyskały wysokie oceny przydatności i dojrzałości – odpowiednio: 4,08 i 4,01 – podczas gdy dyski SSD osiągnęły wartości: 3,86 i 3,75. Przemysłowe karty microSD charakteryzują się lepszym niż w przypadku kart konsumenckich wskaźnikiem żywotności, na który składają się m.in. wskaźnik liczby zapisanych terabajtów *(Total Bytes Written*, TBW – parametr, który oznacza całkowitą liczbę zapisanych [tera]bajtów w całym okresie eksploatacji) i średni czas między awariami (*Mean Time Between Failures*, MTBF). To po prostu nośniki trwalsze i bardziej niezawodne niż ich „prywatne" odpowiedniki, które nie są przeznaczone do zapisu prowadzonego w trybie 24/7. Przemysłowe microSD stają się bardziej opłacalnym rozwiązaniem w urządzeniach brzegowych niż rejestratory NVR (*Network Video Recorder*), ponieważ są tańsze, fizycznie mniejsze i łatwiej je w razie potrzeby wymienić. Inna rzecz, że w przypadku zastosowania NVR to dyski Solid State stają się preferowanym rozwiązaniem, jeśli chodzi o przechowywanie danych w NVR. Są bardziej niezawodne niż tradycyjne HDD, które zawierają ruchome części mechaniczne. Kompaktowy rozmiar, konstrukcja niepotrzebująca wentylatora i możliwość pracy w szerokim zakresie temperatur sprawiają, że w przypadku NVR-ów SSD są idealnym nośnikiem pamięci, który można zamontować wewnątrz rejestratora lub do niego podpiąć. Te cechy SSD sprawiają, że ich popularność rośnie.

## Rozdzielczość 4K

Podobnie jak w zeszłym roku, technologia 4K uzyskała wysokie oceny przydatności (4,21) i dojrzałości (4,18), co stanowi wzrost w porównaniu do 4,09 i 4,06 w roku 2023. W rankingu zapytań klientów 4K zajmuje 3. miejsce. Rozdzielczość 4K, czyli 3840 x 2160 pikseli, pozostaje popularna, zwłaszcza w urządzeniach stosowanych w miastach inteligentnych. A postęp w tej dziedzinie i rosnąca konkurencja spowodowały, że kamery 4K znacząco staniały. Różne modele są oferowane w szerokim przedziale cenowym, tym samym są dostosowane do potrzeb użytkowników o różnym budżecie. W związku z tym przewidujemy dalszy wzrost zapotrzebowania na rozwiązania monitoringu 4K.

## Kamery zasilane energią słoneczną

Kamery zasilane energią słoneczną mają ocenę przydatności na poziomie 3,67 i dojrzałości 3,62, co w porównaniu z wynikami z 2023 r. (odpowiednio: 3,72 i 3,47) pokazuje niewielki wzrost dojrzałości. W rankingu potencjału wzrostu zajmują wysokie 3. miejsce. Kamery te są szczególnie użyteczne do monitoringu obszarów rozległych, gdzie dostęp do źródeł zasilania jest ograniczony. Przemysł systemów monitoringu wizyjnego jest obecnie zorientowany na zrównoważony rozwój, a kamery zasilane energią słoneczną doskonale wpisują się w ten trend.

### Ranking technologii monitoringu wizyjnego wg zapytań klientów

| MIEJSCE | TECHNOLOGIA |
|---|---|
| 1. | Kamery z obsługą słabego oświetlenia |
| 2. | Kamery wieloprzetwornikowe |
| 3. | Rozdzielczość 4K |
| 4. | Kamery zasilane energią słoneczną |
| 5. | Kamery 4G/5G |
| 6. | SSD do przechowywania danych |
| 7. | Przechowywanie w urządzeniach na brzegu sieci z przemysłowymi kartami microSD |
| 8. | VSaaS |
| 9. | Kamery bispektralne |

### Ranking technologii monitoringu wizyjnego wg potencjału wzrostu

| MIEJSCE | TECHNOLOGIA |
|---|---|
| 1. | Kamery 4G/5G |
| 2. | Kamery wieloprzetwornikowe |
| 3. | Kamery zasilane energią słoneczną |
| 4. | VSaaS |
| 5. | Rozdzielczość 4K |
| 6. | SSD do przechowywania danych |
| 7. | Kamery z obsługą słabego oświetlenia |
| 8. | Kamery bispektralne |
| 9. | Przechowywanie w urządzeniach na brzegu sieci z przemysłowymi kartami microSD |

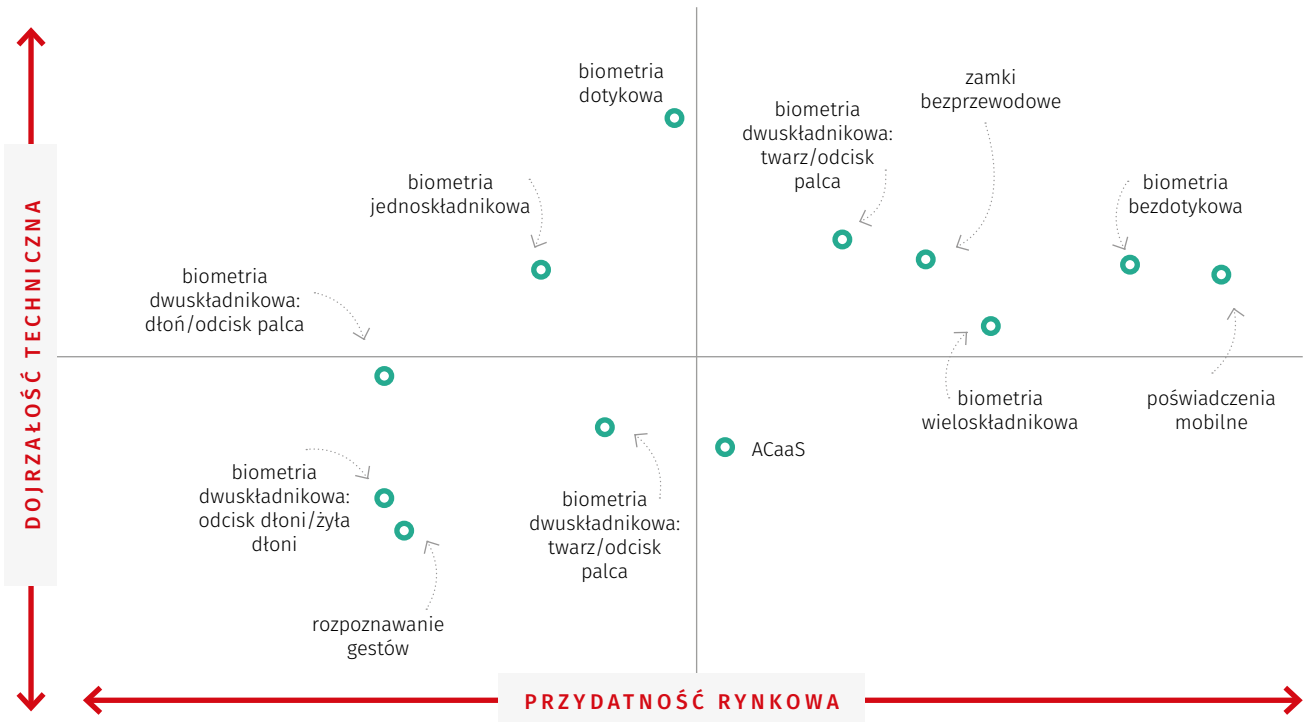
# Kontrola dostępu:
## na popularności zyskują ACaaS i mobilne poświadczenia

W tegorocznym badaniu wyraźnie widoczna jest rosnąca popularność kontroli dostępu świadczonej jako usługa (ACaaS) oraz mobilnych poświadczeń, umożliwiających dostęp za pomocą urządzeń przenośnych. Równocześnie zyskuje na znaczeniu biometria bezdotykowa.

### Kontrola dostępu jako usługa (ACaaS)

W przypadku kontroli dostępu świadczonej jako usługa (*Access Control as a Service,* ACaaS) ocena przydatności i dojrzałości wynosi odpowiednio: 3,61 i 3,37, co oznacza niewielki spadek w porównaniu z oceną o rok wcześniejszą (3,86 i 3,8). ACaaS zajmuje czwarte miejsce w rankingu technologii kontroli dostępu najczęściej poszukiwanych przez klientów, ale pierwsze miejsce pod względem potencjału wzrostu.

ACaaS zyskuje na znaczeniu. W nadchodzących latach przewiduje się jej dynamiczny rozwój. Obecna umiarkowana ocena dojrzałości tej technologii wynika głównie z faktu, że jest to stosunkowo nowe rozwiązanie, jednak wraz z rosnącą popularnością chmury, szczególnie wśród firm poszukujących skalowalnych i efektywnych kosztowo rozwiązań, rośnie także popularność ACaaS. Możliwość zdalnego zarządzania dostępem, łatwe aktualizowanie organizacyjnej polityki bezpieczeństwa oraz integracji



z innymi platformami chmurowymi sprawiają, że ACaaS doskonale odpowiada na współczesne wymagania dotyczące bezpieczeństwa, szczególnie w sektorach, gdzie ważne są elastyczność i kontrola rozproszonych lokalizacji.

## Metoda uwierzytelniania – mobilne poświadczenia

W kategoriach przydatności oraz potencjału wzrostu biometria dotykowa i rozpoznawanie gestów uzyskały umiarkowane oceny. Tymczasem mobilne poświadczenia zajęły pierwsze i drugie miejsce w obu rankingach. Rozwiązania mobilne oferują dwie ważne korzyści. Po pierwsze, są wygodne, gdyż użytkownicy zawsze mają przy sobie swoje urządzenia. Po drugie, są bezpieczne, ponieważ użytkownik jest już uwierzytelniony na urządzeniu, a komunikacja między nim a czytnikiem jest szyfrowana.

| Technologia | Przydatność | Dojrzałość |
|---|---|---|
| **Biometria dotykowa** | 3,55 | 4,22 |
| **Rozpoznawanie gestów** | 3,22 | 3,14 |
| **Poświadczenia mobilne** | 4,21 | 3,78 |

Biometria dotykowa (mowa głównie o odcisku palca) ma jednak pewne ograniczenia, takie jak trudność odczytania odcisku zabrudzonego palca (np. pracowników budowlanych), brak uniwersalności (odciski niektórych osób są trudne do rozpoznania) oraz obawy higieniczne, szczególnie w erze postpandemicznej. Natomiast rozpoznawanie gestów, które uwierzytelnia na podstawie wykonanych ruchów, wciąż jest traktowane jako nowinka. Z tych względów mobilne poświadczenia są liderem wśród technologii uwierzytelniania.

## Biometria dotykowa vs. bezdotykowa

Według opinii czytelników biorących udział w badaniu rozwiązania bezdotykowe zajmują drugie miejsce. Generalnie widać, że biometria dotykowa jest uznawana za bardziej dojrzałą, podczas gdy biometria bezdotykowa – za bardziej odpowiednią.

| | Biometria dotykowa | | Biometria bezdotykowa | |
|---|---|---|---|---|
| **Rok** | Przydatność | Dojrzałość | Przydatność | Dojrzałość |
| **2024** | 3,55 | 4,22 | 4,11 | 3,84 |
| **2023** | 3,74 | 4,05 | 4,11 | 3,74 |

Technologie bezdotykowe, takie jak rozpoznawanie twarzy, tęczówki czy układu żył dłoni, stają się coraz powszechniejsze. Przede wszystkim są higieniczne. Nie trzeba niczego dotykać, by uzyskać dostęp, a to duża zaleta. Rozwiązania bezdotykowe zapewniają szybsze uwierzytelnianie, co czyni je odpowiednimi do zastosowań o dużym natężeniu ruchu, np. w przedsiębiorstwach i na lotniskach. Nie bez znaczenia jest też to, że nie trzeba pamiętać żadnego kodu czy hasła.

## Biometria jedno- kontra wieloskładnikowa

W przypadku biometrii jedno- i wieloskładnikowej wyniki ankiety przedstawiają się następująco:

| | Biometria dotykowa | | Biometria bezdotykowa | |
|---|---|---|---|---|
| **Rok** | Przydatność | Dojrzałość | Przydatność | Dojrzałość |
| **2024** | 3,39 | 3,83 | 3,93 | 3,68 |
| **2023** | 3,56 | 3,64 | 3,89 | 3,49 |

Biometria, w której uzyskanie dostępu wymaga wykorzystania więcej niż jednej cechy, czyli wieloskładnikowa, wyraźnie przeważa nad tą, w której do używana jest tylko jedna cecha. To zrozumiały trend. Każda dodatkowo sprawdzana cecha to kolejna warstwa zabezpieczenia i mniejsze ryzyko nieautoryzowanego dostępu.

## Opcje biometrii wieloskładnikowej

Wyniki badania dotyczące przydatności i dojrzałości metod rozpoznawania opartych na kombinacji cech biometrycznych:

| Technologia | Przydatność | Dojrzałość |
|---|---|---|
| **Odcisk dłoni/żyła dłoni** | 3,2 | 3,24 |
| **Twarz/dłoń** | 3,47 | 3,43 |
| **Dłoń/palec** | 3,2 | 3,53 |
| **Twarz/palec** | 3,75 | 3,92 |

Rozpoznawanie za pomocą dwóch cech, a dokładnie wizerunku twarzy i odcisku linii papilarnych, cieszyło się największym zainteresowaniem czytelników biorących udział w badaniu, stając się wyraźnym zwycięzcą wśród metod biometrycznych łączących kilka cech.

### Ranking technologii kontroli dostępu wg ankietowanych

| MIEJSCE | TECHNOLOGIA |
|---|---|
| **1.** | ACaaS (kontrola dostępu jako usługa) |
| **2.** | Mobilne poświadczenia |
| **3.** | Biometria bezdotykowa |
| **4.** | Biometria wieloskładnikowa |
| **5.** | Rozpoznawanie gestów |
| **6.** | Biometria dwuskładnikowa: twarz/dłoń |
| **7.** | Zamki bezprzewodowe |
| **8.** | Biometria dotykowa |
| **9.** | Biometria dwuskładnikowa: twarz/odcisk palca |
| **10.** | Biometria dwuskładnikowa: odcisk dłoni/żyła dłoni |
| **11.** | Biometria dwuskładnikowa: dłoń/odcisk palca |
| **12.** | Biometria jednoskładnikowa |

# Globalny obraz rynku security

Na całym świecie firmy stają przed wyzwaniem, któremu łatwiej sprostać, jeśli zastosuje się strategię opisaną w *Sztuce wojny* Sun Tzu. Zgodnie z nią przewidywaniom ruchów przeciwnika powinno towarzyszyć sięgnięcie po wszystkie dostępne zasoby i technologie.
Te organizacje, które stosują taką strategię, inwestują w nowoczesne systemy monitoringu wizyjnego i kontroli dostępu, wychodząc z całkiem słusznego założenia, że lepiej dmuchać na zimne. Inwestycje w innowacyjne technologie zabezpieczeń są nie tylko odpowiedzią na zagrożenia, ale także sposobem na umocnienie relacji z pracownikami i klientami poprzez zapewnienie im poczucia bezpieczeństwa. Sun Tzu radził, aby znać siebie i swojego przeciwnika. Współczesne firmy również muszą zrozumieć zarówno zagrożenia, jak i możliwości, jakie niesie ze sobą nowoczesna technologia.

## Europa

**Europejskie firmy coraz bardziej skupiają się na wzmacnianiu swoich systemów zabezpieczeń technicznych, takich jak monitoring wizyjny czy kontrola dostępu. W obliczu wzrostu zagrożeń fizycznych i nowych wymogów prawnych przedsiębiorstwa inwestują w nowoczesne technologie, by skuteczniej chronić swoje obiekty i pracowników. Rozwój tych systemów to dziś nie tylko kwestia bezpieczeństwa, ale również kluczowy element budowania zaufania i odpowiedzialności w biznesie.**

### Kontrola dostępu: innowacja, integracja i zgodność z przepisami

Rozwiązania z zakresu kontroli dostępu stały się jednymi z najważniejszych elementów strategii bezpieczeństwa firm europejskich. W tym sektorze odnotowano wzrost innowacji napędzany rozwojem technologii biometrycznych, rozwiązań chmurowych oraz koniecznością integracji z innymi systemami bezpieczeństwa. Jednak te postępy są regulowane przez ścisłe przepisy, takie jak RODO, które wymagają solidnych środków ochrony prywatności danych.

### Innowacje powodują wzrost

Europejski rynek kontroli dostępu rozwija się dzięki zastosowaniu nowoczesnych technologii z zakresu biometrii, uwierzytelniania dwuskładnikowego i technologii mobilnych. Rosnące zapotrzebowanie na rozwiązania bezdotykowe przyczyniło się do rozpowszechniania biometrii, w tym rozpoznawania twarzy i linii papilarnych. Ten sposób dostępu nie tylko gwarantuje lepszy nad nim nadzór, ale też przy okazji jest dla użytkowników wygodniejszy.

Zapotrzebowanie na urządzenia bezdotykowe (oraz mobilne) jest szczególnie widoczne w sektorze opieki zdrowotnej i edukacji, ponieważ we wszelkiego rodzaju placówkach, takich jak przychodnie czy szkoły, zarówno wygoda, jak i zachowanie higieny jest w cenie. Aplikacja na smartfon, zastępująca fizyczną kartę, to przykład rozwiązania, które do niezbędnego minimum ogranicza liczbę punktów dotykowych.

### Rośnie znaczenie interoperacyjności i integracji

Interoperacyjność, czyli zdolność systemu lub produktu do pełnej współpracy z innymi systemami lub produktami, powoli staje się immanentną cechą nowoczesnych systemów kontroli dostępu, zwłaszcza że europejskie

firmy cenią wartość, jaką zapewniają zintegrowane systemy bezpieczeństwa. Połączenie kontroli dostępu, monitoringu wizyjnego oraz sygnalizacji włamania i napadu w jeden system pozwala organizacjom na szybszą reakcję na incydenty i poprawę ogólnego bezpieczeństwa.

## Wpływ RODO na systemy kontroli dostępu

Wprowadzenie RODO miało duży wpływ na systemy kontroli dostępu w Europie. Przepisy wymagają, aby producenci tych systemów stosowali bardziej rygorystyczne zabezpieczenia prywatności danych. Użytkownik musi wyrazić zgodę na zbieranie danych, a producent wyraźnie określić, jakie informacje są zbierane, jak są przechowywane i do jakich celów są używane. Przepisy te zatem wymuszają na producentach, by kwestię ochrony prywatności uwzględnili już na etapie projektowym.

James Clark, dyrektor sprzedaży w EMEA i APAC w AMAG Technology, podkreśla, że wprowadzenie RODO spowodowało innowacyjne podejście do takich rozwiązań jak mobilne identyfikatory i technologie biometryczne, ponieważ wówczas konieczne jest minimalizowanie ilości zbieranych danych. W praktyce RODO wymusiło wprowadzenie nowych zabezpieczeń, takich jak szyfrowanie *end-to-end* oraz anonimizacja danych osobowych. Zapewnienie zgodności z przepisami RODO daje przewagę konkurencyjną, użytkownicy końcowi są coraz bardziej świadomi kwestii prywatności danych i oczekują, że producenci będą te obawy traktować poważnie.

## Elastyczność dzięki chmurze i aplikacjom mobilnym

Rynek europejski notuje także wzrost popularności systemów kontroli dostępu i zarządzania wizytami wykorzystującymi przechowywanie danych w chmurze. Rozwiązania chmurowe umożliwiają zdalne zarządzanie kontrolą dostępu, oferując większą elastyczność i zmniejszając konieczność posiadania infrastruktury na miejscu.

James Clark zauważył, że wzrasta zainteresowanie chmurowymi systemami zarządzania wizytami, które są ściśle zintegrowane z systemem kontroli dostępu. Rozwiązania chmurowe umożliwiają również organizacjom uproszczenie operacji poprzez zarządzanie danymi dostępu i wizyt w jednej platformie. Mobilna kontrola dostępu zyskuje na popularności niezależnie od miejsca stosowania: od biur po uniwersyteckie kampusy. Dzięki mobilnym identyfikatorom pracownicy i goście mogą wejść, korzystając z aplikacji na smartfonie, bez konieczności wydawania im fizycznych kart i identyfikatorów. Jest to szczególnie przydatne w miejscach o dużej rotacji, takich jak kampusy uniwersyteckie, gdzie dostęp musi być często przyznawany i odbierany. Przejście na rozwiązania mobilne i chmurowe odzwierciedla szerszy trend transformacji cyfrowej w zakresie kontroli dostępu. Organizacje coraz częściej poszukują systemów, którymi można zarządzać zdalnie i które oferują skalowalność.

## Wyzwania dla integratorów

Pomimo licznych zalet zaawansowanych systemów kontroli dostępu integratorzy napotykają wyzwania związane z kosztami, skalowalnością i zgodnością z przepisami. Radzą sobie z tym wyzwaniem, bo jak wyjaśnia James Clark: *Zaawansowane systemy kontroli dostępu są droższe, ale integratorzy pokonują te bariery, edukując klientów końcowych, m.in. pokazując, że takie systemy obniżają koszty operacyjne.*

Rozsądnym podejściem jest wdrażanie etapami, ponieważ pozwala to organizacjom na rozpoczęcie od mniejszej skali i stopniowe rozbudowywanie systemu. Ponadto niektórzy producenci oferują leasing, co czyni zaawansowane systemy bardziej przystępnymi dla organizacji o ograniczonym budżecie.

Zgodność z RODO i innymi regulacjami stanowi kolejne wyzwanie. Integratorzy muszą wdrażać systemy kontroli dostępu z wbudowanymi narzędziami raportowania, aby wykazać zgodność podczas audytów.

Integratorzy często współpracują z producentami oferującymi jednocześnie kilka różnych rozwiązań, takich jak kontrolowany dostęp, zarządzanie wizytami i zarządzanie tożsamością. Integracja jest bowiem kluczowa dla uzyskania zaawansowanego systemu kontroli dostępu, dlatego ważne jest, aby oferowali oni rozwiązania otwarte.

## Monitoring wizyjny – jak pogodzić AI, chmurę i przepisy

Technologia monitoringu wizyjnego rozwija się, a wraz nim rynek europejski się zmienia. Tę zmianę charakteryzuje wprowadzenie analityki wideo opartej na sztucznej inteligencji, wzrost popularności rozwiązań chmurowych oraz rosnące znaczenie ochrony danych i zgodności z regulacjami.

Według Josa Beerninka, wiceprezesa Milestone Systems na region EMEA, te zmiany przekształcają krajobraz rynku, oferując nowe możliwości zwiększenia bezpieczeństwa i efektywności operacyjnej w różnych sektorach.

## AI podnosi możliwości monitoringu

Analiza materiału wizyjnego dokonywana przez AI stała się znaczącym elementem europejskiego rynku monitoringu. Wynika to z rosnącego zapotrzebowania na przydatne informacje i oczekiwania wydajniejszego niż dotychczasowe sposobu analizowania obrazu AI, który pozwala identyfikować konkretne obiekty, działania czy anomalie, umożliwiając użytkownikom przeszukiwanie ogromnej liczby nagrań i skupienie się wyłącznie na najważniejszych zdarzeniach.

Jos Beernink podkreślił wydajność tego podejścia: *Zwiększona efektywność operacyjna zapewnia możliwości przeszukiwania wideo wg konkretnych obiektów, działań lub anomalii – co oznacza, że tylko najważniejsze wydarzenia, wymagające interwencji operatora, będą uruchamiać alarm.*

To znacznie więcej niż tradycyjne wykorzystanie wideo, a predykcyjna analiza nagrań staje się narzędziem do przewidywania zdarzeń. Dzięki zdolnościom predykcyjnym organizacje mogą proaktywnie reagować na potencjalne zagrożenia bezpieczeństwa, co ostatecznie poprawia bezpieczeństwo i efektywność wykorzystania zasobów.

## Innowacje w rozwiązaniach monitoringu wizyjnego wykorzystujących chmurę

Chmura zyskuje na znaczeniu, a firmy europejskie nie są pod tym względem wyjątkiem. Rozwiązania VSaaS są skalowalne, a co za tym idzie, kosztowo optymalne dla firm poszukujących centralnego zarządzania monitoringiem wizyjnym.

– *Oczekujemy znacznego wzrostu popularności rozwiązań VSaaS, takich jak Milestone Kite, które oferują proste, bezpieczne i skalowalne oprogramowanie do zarządzania wideo (VMS), pozwalające klientom i instalatorom korzystać z chmury na potrzeby bezpieczeństwa* – powiedział Jos Beernink.

VSaaS doskonale sprawdza się w firmach dysponujących wieloma różnymi lokalizacjami, takimi jak duże sieci handlu detalicznego. Rozwiązania te są bezpieczne ze względu na automatycznie przeprowadzane aktualizacje i łatwo skalowalne.

Monitoring wizyjny bazujący na przechowywaniu i analizowaniu danych w chmurze zmienia podejście organizacji do bezpieczeństwa, umożliwiając im zarządzanie wieloma lokalizacjami za pomocą jednego

→

interfejsu. Centralizacja zarządzania VSaaS nie tylko upraszcza operacje, ale także zapewnia większe bezpieczeństwo danych dzięki infrastrukturze chmurowej, którą utrzymują wyspecjalizowani dostawcy.

### Integracja monitoringu wizyjnego z innymi systemami bezpieczeństwa

Integracja monitoringu wizyjnego z innymi systemami zabezpieczeń, takimi jak kontrola dostępu, zyskuje na popularności w Europie. Obserwuje się dalsze zainteresowanie analizą systemową, gdzie kamery wideo są wykorzystywane jako czujniki do redukcji fałszywych alarmów, lepszego przewidywania, zarządzania i reagowania na ryzyko oraz uzyskiwania informacji operacyjnych, które dostarczają wartości wykraczającej poza samo bezpieczeństwo.

Konsolidacja wielu funkcji bezpieczeństwa na jednej platformie umożliwia organizacjom poprawę świadomości sytuacyjnej i usprawnienie zarządzania bezpieczeństwem. Na przykład system zarządzania materiałem wizyjnym (VMS) może działać jako centralny hub monitoringu, umożliwiając operatorom dostęp do obrazów wideo, kontrolę punktów dostępu i reagowanie na alarmy w czasie rzeczywistym.

Integracja systemów nie tylko zwiększa poziom bezpieczeństwa, ale również dostarcza informacji wspomagających działalność operacyjną firmy. Przykładowo, analiza wideo może być wykorzystywana do monitorowania zachowań klientów sklepów, ułatwiając optymalizację rozłożenia towarów i poprawiając obsługę klienta.

### Jak poruszać się w gąszczu przepisów?

Regulacje dotyczące ochrony danych, takie jak RODO, a także nowe przepisy, jak unijna ustawa o sztucznej inteligencji (AI Act), mają znaczący wpływ na wdrażanie systemów monitoringu wideo w Europie. Oprócz RODO rynek kształtują takie regulacje, jak NIS2, dyrektywa o odporności krytycznych podmiotów (CER) oraz ustawa o cyberodporności (CRA), nakładając rygorystyczne wytyczne dotyczące zarządzania danymi i bezpieczeństwa.

Firmy stają się bardziej wymagające, dokonując wyboru partnera, preferując tych, którzy wykazują zaangażowanie w przestrzeganie przepisów. Zgodność z przepisami regulacyjnymi jest więc niezbędna, by być zaufanym dostawcą systemów bezpieczeństwa.

### Mocniejszy łańcuch dostaw dzięki otwartym platformom

Zakłócenia w łańcuchu dostaw i niedobory komponentów stanowią wyzwanie dla każdego przedsiębiorstwa. W przypadku firm zajmujących się bezpieczeństwem wpływają na dostępność kluczowych urządzeń. Jednak wprowadzenie rozwiązań opartych na otwartych platformach pomaga złagodzić te problemy.

– *Otwarta platforma VMS, taka jak XProtect firmy Milestone, pozwala integratorom na złagodzenie zakłóceń w łańcuchu dostaw, ponieważ mogą współpracować z najszerszym możliwym zakresem producentów kamer i urządzeń IP, zamiast być ograniczonym do jednego dostawcy* – powiedział Jos Beernink.

Ekosystem kompatybilnych urządzeń i otwarte platformy pozwalają organizacjom dostosować się do zmieniających się warunków rynkowych przy jednoczesnym zapewnieniu ciągłości projektów.

### Patrząc w przyszłość

Połączenie funkcjonalności sztucznej inteligencji, przetwarzania w chmurze i zintegrowanych systemów bezpieczeństwa prawdopodobnie będzie powodować dalszy wzrost wartości europejskiego rynku urządzeń i usług security. Przyjmując innowacyjne technologie i przestrzegając rygorystycznych standardów zgodności, firmy z branży security będą mogły sprostać różnorodnym potrzebom przedsiębiorców europejskich.

## Azja

**Ten region, wyróżniający się szybkim postępem cyfrowym i innowacyjnym podejściem do technicznych nowinek, notuje dynamiczny wzrost popytu na bezpieczne i wygodne rozwiązania kontroli dostępu. Technologie oparte na sztucznej inteligencji, takie jak rozpoznawanie twarzy czy bezdotykowe odciski palców, zdobywają coraz większą popularność, wpisując się w potrzeby rynku. Natomiast coraz większa presja na zachowanie prywatności i bezpieczeństwa danych kształtuje sposób rozwoju i zgodność tych technologii z regulacjami prawnymi, tworząc dynamiczne otoczenie dla dostawców systemów kontroli dostępu. Przyjrzyjmy się kluczowym trendom na azjatyckim rynku kontroli dostępu.**

### Rozwój biometrycznych systemów kontroli dostępu

Biometryczne systemy kontroli dostępu już od lat są obecne w wielu krajach azjatyckich. Technologie bazujące na sztucznej inteligencji, rozpoznawanie twarzy i bezdotykowe odciski palców są wdrażane w różnych sektorach, od bankowości po inteligentne miasta.

– *Rozpoznawanie twarzy oparte na sztucznej inteligencji jest szczególnie popularne w Azji, gdzie jest szeroko stosowane w sektorze zarówno publicznym, jak i prywatnym do celów kontroli dostępu i bezpieczeństwa* – mówi Hanchul Kim, prezes firmy Suprema. – *W wielu krajach azjatyckich akceptacja tej technologii jest większa niż w innych regionach świata.*

Rozwój inteligentnych miast oraz rosnące zapotrzebowanie na narzędzia służące bezpieczeństwu publicznemu powodują, że rośnie tempo wdrażania systemów rozpoznawania twarzy, zwłaszcza w takich projektach, jak kontrola graniczna czy inicjatywy związane z bezpieczeństwem publicznym. Rządy m.in. Chin, Japonii i Korei Południowej aktywnie wspierają rozwój tych technologii.

Steve Bell, prezes Gallagher Security, zauważa, że w Azji technologie te zyskują popularność, ponieważ sektor bankowy, administracja publiczna i rozwijające się inteligentne miasta stawiają na wysokie standardy bezpieczeństwa, co jest możliwe dzięki szybkiej transformacji cyfrowej i koncentracji na ochronie publicznej.

### Sztuczna inteligencja

Sztuczna inteligencja (AI) odgrywa znaczącą rolę w zwiększaniu skuteczności systemów biometrycznych, poprawiając ich precyzję i komfort użytkowania. W systemach kontroli dostępu AI wspiera analizę predykcyjną, umożliwiając organizacjom prognozowanie potencjalnych zagrożeń i szybsze reagowanie na incydenty. Azjatyckie firmy coraz częściej wykorzystują AI w swoich systemach, aby zwiększyć zarówno poziom bezpieczeństwa, jak i komfort użytkowników. Rozwój technologii bezdotykowych odcisków palców ma szczególne znaczenie w kontekście higieny i usprawnienia obsługi, co stało się priorytetem po globalnej pandemii.

### Przepisy dotyczące prywatności a technologie kontroli dostępu

Postępujący rozwój technologiczny systemów kontroli dostępu jest równoważony rosnącą presją na ochronę prywatności danych. Region stopniowo dostosowuje się do światowych standardów ochrony danych,

chociaż ogólnie pozostaje w tyle za Europą pod względem opracowania i wdrożenia kompleksowych przepisów dotyczących prywatności.

Nowe regulacje dotyczące prywatności wymuszają na dostawcach priorytetowe traktowanie szyfrowania danych, zgody użytkownika oraz bezpiecznego przechowywania danych. Przepisy te obligują producentów do zachowania pełnej zgodności ich rozwiązań biometrycznych i mobilnych, spełniają lokalne wymogi prawne i jednocześnie odpowiadają na potrzeby związane z bezpieczeństwem.

## Perspektywy: rosnący rynek i innowacje

W miarę zaostrzania przepisów o ochronie danych firmy, także azjatyckie, będą musiały zrównoważyć innowacje z wymaganiami dotyczącymi bezpieczeństwa informacji. Przykładem są mobilne systemy uwierzytelniania umożliwiające użytkownikom dostęp za pomocą smartfonów. Rozwiązania te, obok wygody, muszą spełniać wymogi ochrony danych, gwarantując, że dane użytkowników pozostaną zabezpieczone. Rosnące zapotrzebowanie na bezpieczne systemy w takich sektorach, jak opieka zdrowotna, edukacja i infrastruktura krytyczna stanowi dodatkowy impuls dla innowacji w obszarze kontroli dostępu.

Rynek kontroli dostępu w Azji w 2024 r. dynamicznie się zmienia, a technologie, takie jak rozpoznawanie twarzy oparte na AI i bezdotykowa biometria, przeplatają się z rosnącymi wymaganiami regulacyjnymi dotyczącymi ochrony prywatności. W miarę kontynuacji cyfrowej transformacji systemy kontroli dostępu będą musiały nadążać za nowymi standardami technologicznymi i prawnymi. Producenci, którzy priorytetowo traktują zasady bezpieczeństwa oraz ochronę danych, wyróżnią się jako zaufani partnerzy w regionie, który coraz bardziej skupia się na bezpieczeństwie i prywatności.

## Ewolucja rynku monitoringu wizyjnego

Rynek monitoringu wizyjnego w Azji dynamicznie rośnie, a sektory, takie jak handel detaliczny, infrastruktura miejska i logistyka w coraz większym stopniu wdrażają zaawansowane technologie w celu poprawy bezpieczeństwa i efektywności operacyjnej.

W roku 2024 rozwój rynku napędzają innowacje w obszarach analityki materiału wizyjnego opartej na sztucznej inteligencji, technologii chmurowych, a także inwestycje w inteligentne miasta. Jednak wzrost zainteresowania tymi technologiami wiąże się z narastającymi obawami o prywatność danych i cyberbezpieczeństwo, co wymaga dostosowania rozwiązań do rosnących wymogów w zakresie bezpieczeństwa i zgodności.

## Niezależnie od branży bezpieczeństwo jest w cenie

Zapotrzebowanie na zaawansowany, zintegrowany system monitoringu wizyjnego wzrasta zwłaszcza w takich sektorach, jak handel detaliczny, opieka zdrowotna, produkcja i transport. Projekty inteligentnych miast rozszerzają rolę monitoringu wizyjnego poza tradycyjne zastosowania bezpieczeństwa, podnosząc efektywność operacyjną i bezpieczeństwo publiczne. Technologie, takie jak chmura hybrydowa, 5G oraz sztuczna inteligencja umożliwiają analizę danych w czasie rzeczywistym, wspierając podejmowanie szybkich i trafnych decyzji w różnorodnych branżach.

Marie-Helene Mansard, dyrektor ds. rozwoju w Axis Communications na region Azji i Pacyfiku, zauważa: – *Ewolucja monitoringu przekształciła podstawowe wykrywanie ruchu w zaawansowaną analitykę brzegową, dostarczając cennych informacji, które podnoszą poziom bezpieczeństwa i efektywności operacyjnej, szczególnie w branżach takich jak produkcja i logistyka.*

## Analiza AI: wyższa efektywność i precyzja

Jednym z kluczowych trendów na rynku monitoringu wizyjnego jest rosnące wykorzystanie sztucznej inteligencji do analizy wideo. Technologie oparte na sztucznej inteligencji zwiększają precyzję i redukują liczbę fałszywych alarmów, umożliwiając szybkie reagowanie na krytyczne zdarzenia.

Allen Hsieh, dyrektor globalnego działu marketingu i rzecznik prasowy Vivotek, podkreśla: – *Sztuczna inteligencja znacząco zwiększa efektywność identyfikacji kluczowych zdarzeń i rozwiązywania rzeczywistych problemów z zakresu bezpieczeństwa, szczególnie w środowiskach o dużym natężeniu ruchu, jak inteligentne miasta.*

## Inteligentne miasta pod nadzorem

W całej Azji inicjatywy związane z inteligentnymi miastami nabierają tempa, a monitoring wizyjny odgrywa istotną rolę w poprawie bezpieczeństwa publicznego oraz zarządzania miastami. Integracja sztucznej inteligencji i analityki wideo umożliwia monitorowanie zdarzeń →

i reagowanie na nie w czasie rzeczywistym, co wspiera m.in. zarządzanie ruchem i reagowanie kryzysowe.

### Przejście na monitoring wizyjny w chmurze

W związku z rozwojem technologii chmurowych rynek monitoringu wizyjnego zmierza ku rozwiązaniom hybrydowym, które łączą zalety systemów brzegowych, chmurowych oraz lokalnych. Model chmury hybrydowej pozwala na przechowywanie i analizowanie danych wizyjnych bezpośrednio w urządzeniach brzegowych, z możliwością tworzenia kopii zapasowych w chmurze. Takie rozwiązanie optymalizuje przepustowość oraz pamięć, co jest kluczowe dla dużych systemów monitoringu.

### Prywatność danych i cyberbezpieczeństwo

Wraz ze wzrostem popularności monitoringu wizyjnego opartego na chmurze rosną także obawy o prywatność danych i cyberbezpieczeństwo. Firmy wprowadzają zaawansowane zabezpieczenia, aby zapewnić zgodność z regionalnymi przepisami.

Przykładem jest platforma VORTEX firmy Vivotek, która wykorzystuje zaawansowane szyfrowanie i standardowe środki zgodności w celu ochrony danych w sieci i w chmurze. Axis Communications przyjmuje podejście *privacy by design,* oferując m.in. funkcję tarczy prywatności, która maskuje wrażliwe obszary na nagraniach.

Azjatycki rynek monitoringu wizyjnego jest gotowy na dalszy wzrost, lecz staje przed wyzwaniami w zakresie prywatności danych, cyberbezpieczeństwa i zgodności z przepisami. Wzrost liczby regulacji w regionie wymaga, aby firmy kontynuowały innowacje i adaptację do nowych wymogów.

Rynek monitoringu wizyjnego w Azji w 2024 r. wchodzi w czas intensywnego wzrostu, będącego skutkiem synergii rozwiązań takich jak analiza materiału wizyjnego z wykorzystaniem AI, obliczeń chmurowych oraz rozwojem inteligentnych miast, który zwiększa popyt na inteligentne i połączone systemy monitoringu. Wyzwania związane z prywatnością danych, cyberbezpieczeństwem i regulacjami wymuszają na firmach ciągłe innowacje. Liderzy rynku koncentrują się na dostarczaniu elastycznych, skalowalnych rozwiązań, które spełniają rosnące wymagania w zakresie bezpieczeństwa i prywatności, wspierając budowę bezpieczniejszych, bardziej połączonych miast.

## Ameryka Północna

**W roku 2024 rynek systemów kontroli dostępu w Ameryce Północnej ulega głębokim zmianom, będących skutkiem popularyzacji mobilnego dostępu, centralizacji zarządzania oraz zwiększenia zapotrzebowania na rozwiązania zintegrowane. Przemiany te są widoczne szczególnie w branżach związanych z budownictwem wielorodzinnym, opieką zdrowotną i szkolnictwem wyższym.**

### Nowy standard – mobilna kontrola dostępu

Mobilny dostęp stopniowo staje się podstawowym elementem systemów zabezpieczeń w Ameryce Północnej, przechodząc z fazy testowej do powszechnego wdrożenia w wielu branżach. Smartfony i inne urządzenia, które stale nosimy ze sobą, umożliwiające bezpieczny i wygodny dostęp do budynków, stały się niezastąpionym narzędziem, szczególnie dla organizacji poszukujących nowoczesnych rozwiązań kontroli dostępu. Integracja z takimi aplikacjami, jak Apple Wallet i Google Wallet podnosi wygodę użytkowania, upraszczając autoryzację w czasie rzeczywistym.

### Deweloperzy budowlani – liderzy mobilnej kontroli dostępu

W budownictwie wielorodzinnym mobilna kontrola dostępu zyskuje na znaczeniu jako kluczowe udogodnienie. Coraz więcej osób preferuje mobilne rozwiązania, a 82% respondentów jest skłonne zapłacić więcej za możliwość zdalnego nadzorowania nieruchomościami. Ten dynamiczny trend otwiera szanse integratorom systemów, oferując deweloperom, ale też posiadaczom nieruchomości narzędzia niezbędne do przejścia z tradycyjnych zamków mechanicznych na nowoczesne elektroniczne systemy kontroli dostępu, dostosowane do potrzeb użytkowników.

### Integracja to przyszłość kontroli dostępu

Na rynku kontroli dostępu rośnie znaczenie rozwiązań zintegrowanych, które można łatwo dostosować do przyszłych innowacji. Inwestycja w otwarte systemy zabezpieczeń pozwala na ich późniejszą bezproblemową integrację z nowymi narzędziami i urządzeniami. Prace nad standardami wspólnymi dla mobilnych systemów dostępowych korelują z tworzeniem uniwersalnych rozwiązań, minimalizując tym samym problemy ze zgodnością i przyspieszając wdrożenie nowoczesnych rozwiązań mobilnych w różnych branżach.

### Wyzwania i możliwości dla integratorów

Wraz z rosnącym zapotrzebowaniem na mobilne i scentralizowane systemy kontroli dostępu integratorzy mają szansę stać się kluczowymi partnerami organizacji modernizujących swoje systemy zabezpieczeń. Oferowanie specjalistycznej wiedzy i wsparcia na każdym etapie wdrażania systemów kontroli dostępu stanowi istotną przewagę na konkurencyjnym rynku, szczególnie w sektorze budownictwa wielorodzinnego, które w ostatnich latach coraz intensywniej wykorzystuje różnego rodzaju cyfrowe rozwiązania kontroli dostępu. W najbliższych latach rynek kontroli dostępu w Ameryce Północnej będzie kształtowany przez rosnące oczekiwania dotyczące zarówno bezpieczeństwa, jak i wygody użytkowania.

Rok 2024 to czas dalszego dynamicznego rozwoju rynku kontroli dostępu na tym kontynencie, na który wpływają trendy mobilności, centralizacji i integracji. Integratorzy, którzy potrafią przewidzieć postęp technologiczny i oferować elastyczne, przyszłościowe rozwiązania, mogą stać się nieocenionymi partnerami dla organizacji modernizujących swoje systemy zabezpieczeń.

### Monitoring wizyjny

Wraz ze wzrostem zapotrzebowania na zaawansowane technologie monitoringu wizyjnego w Ameryce Północnej kluczowe sektory, takie jak handel detaliczny, opieka zdrowotna, transport i bankowość stały się liderami w zakresie adaptacji najnowszych rozwiązań. Dzięki dynamicznemu rozwojowi sztucznej inteligencji (AI), technologii chmurowych oraz coraz bardziej zintegrowanych narzędzi cyberbezpieczeństwa branża dozoru wizyjnego przechodzi intensywną transformację.

Rozwiązania te nie tylko wzmacniają tradycyjne zabezpieczenia, ale także poprawiają wydajność operacyjną i otwierają nowe możliwości zastosowań w różnych branżach.

### AI i chmura fundamentem monitoringu wizyjnego

Integracja sztucznej inteligencji z systemami monitoringu wizyjnego zasadniczo zmieniła sektor bezpieczeństwa w ostatnich latach, a rok 2024 to czas, w którym technologie te stają się standardem w zarządzaniu

bezpieczeństwem i analizach operacyjnych. AI umożliwia automatyczne wykrywanie zagrożeń, rozpoznawanie obiektów oraz przewidywanie incydentów, co znacznie podnosi skuteczność systemów monitoringu.

Rozwiązania chmurowe odegrały kluczową rolę, oferując wyższą skalowalność, bezpieczeństwo i elastyczność. Dzięki chmurze firmy mogą usprawnić instalację systemów oraz zarządzanie nimi, jednocześnie redukując koszty. Połączenie AI i chmury przekształca monitoring wizyjny nie tylko jako narzędzie bezpieczeństwa, ale też sposób na optymalizację operacyjną i zwiększenie zaangażowania klientów, zwłaszcza w handlu detalicznym.

## Handel detaliczny liczy na optymalizację

W handlu detalicznym monitoring wizyjny to od dawna sprawdzone narzędzie zapobiegające np. kradzieżom sklepowym czy wandalizmowi. Teraz jednak zyskuje nowe, strategiczne znaczenie. Przedsiębiorstwa detaliczne coraz częściej wykorzystują analitykę wideo do śledzenia zachowań klientów, optymalizacji ulokowania towarów w sklepach oraz doskonalenia strategii marketingowych. Monitoring wizyjny pozwala także na kontrolę przestrzegania standardów i produktywności pracowników, podnosząc efektywność operacyjną i konkurencyjność wobec handlu online.

## Opieka zdrowotna: delikatny balans między ochroną a prywatnością

W instytucjach świadczących opiekę zdrowotną głównym zadaniem monitoringu jest przede wszystkim ochrona pacjentów, a następnie personelu z zachowaniem rygorystycznych wymagań dotyczących prywatności. Skomplikowane przepisy wymuszają stosowanie rozwiązań, które z jednej strony pozwolą na prowadzenie monitoringu w czasie rzeczywistym, z drugiej – będą skutecznie chronić prywatność pacjentów.

## Transport efektywny i bezpieczny

W transporcie monitoring wizyjny odgrywa istotną rolę na lotniskach, autostradach, w metrze i systemach tranzytowych, wspierając bezpieczeństwo publiczne i zarządzanie przepływem ruchu. Rozwiązania te umożliwiają zarządzanie incydentami, reagowanie na zagrożenia oraz optymalizację przepływu pasażerów, co zwiększa bezpieczeństwo i wydajność transportu publicznego.

## Instytucje finansowe odporne na oszustwa

W sektorze finansowym, a ściśle rzecz biorąc bankowym, zaawansowane technologie monitoringu wizyjnego odpowiadają na coraz bardziej złożone zagrożenia bezpieczeństwa, takie jak *skimming*. Rozwiązania do monitoringu prowadzonego w czasie rzeczywistym umożliwiają instytucjom finansowym natychmiastowe wykrywanie podejrzanych działań.

## Nowe wyzwania: manipulacje wideo

Wraz z rozwojem AI i technologii monitoringu pojawiają się nowe zagrożenia, takie jak *deep fake*, które powodują, że łatwo zmanipulować nagrania wideo, co może uczynić je mało wiarygodnymi. Wzrost liczby manipulacji cyfrowych sprawia, że technologia, która umożliwia autentyfikację nagrań wizyjnych, staje się koniecznością dla instytucji i firm.

## Przyszłość monitoringu wizyjnego w Ameryce Północnej

Przyszłość monitoringu wizyjnego zapowiada dalszy rozwój i innowacje. AI oraz chmura przyczynią się do poszerzenia zastosowań, od wydajności operacyjnej po poprawę doświadczeń klientów. Jednocześnie konieczne będą inwestycje w technologie weryfikacji danych wideo i cyberbezpieczeństwo, aby sprostać dynamicznie zmieniającym się wyzwaniom. Dzięki strategicznym decyzjom i odpowiednim technologiom przyszłość monitoringu wizyjnego w Ameryce Północnej jest obiecująca, otwierając nowe możliwości w zakresie bezpieczeństwa i efektywności operacyjnej dla firm i instytucji. ●

# Eksperci patrzą z optymizmem

Wzrost wartości rynku monitoringu wizyjnego w ostatnim roku, mimo globalnych wyzwań, wskazuje na dynamiczny rozwój branży, ze szczególnym uwzględnieniem monitoringu wizyjnego jako usługi (VSaaS). O tym, jak miewa się branża, mówią eksperci firm badawczych specjalizujących się w rynku security: Novaira Insights oraz Security Industry Association (SIA), ASIS International i Omdia.

Choć chiński rynek, będący największym graczem w tej dziedzinie, odnotował spadki, to inne regiony świata, takie jak Indie i Ameryka Łacińska, wykazują znaczący wzrost. Eksperci przewidują dalszy rozwój rynku, który osiąganie wartość ponad 27 mld dol. w 2024 roku, co jest wynikiem rosnącego zapotrzebowania na innowacyjne rozwiązania technologiczne oraz chmurowe.

## Wartość rynku monitoringu wizyjnego

Według najnowszego raportu przygotowanego przez Novaira Insights w ubiegłym roku wzrosła wartość globalnego rynku monitoringu wizyjnego. Był to jednak wzrost niewielki, spowodowany faktem, że w Chinach, kraju będącym w tej branży znaczącym graczem, zarejestrowano spadek, który „skonsumował" wzrost w pozostałych częściach świata.

O jakich wielkościach mowa? Otóż ze wspomnianego raportu wynika, że w ubiegłym roku wartość globalnego rynku systemów i oprogramowania monitoringu wizyjnego faktycznie zwiększyła się o zaledwie 3,4%. Dlaczego tak mało? Dlatego, że w Chinach nastąpił spadek jego wartości do 2,7%, co wpłynęło na cały rynek, mimo że w pozostałych regionach mowa o wzroście o 8,2%. Państwo Środka jest bowiem największym regionalnym rynkiem systemów monitoringu wizyjnego na świecie, w 2023 r. stanowiącym 41% globalnego rynku. Jednakże zauważono, że jest to spadek w porównaniu do dwóch lat wcześniej, kiedy to wskaźnik ten wynosił 52%.

### Słabość rynku chińskiego

Spowolnienie na chińskim rynku security rozpoczęło się w 2022 r., kiedy wzrost PKB Chin wyniósł jedynie 5,1% w porównaniu do 9% w 2021 r. Na ten wynik wpłynęły m.in. lockdown związany z COVID-19, załamanie rynku nieruchomości oraz napięcia geopolityczne. Ówczesny ranking Security 50 wyraźnie pokazał, że na 17 firm, które odnotowały spadki przychodów w latach 2021–2022, aż 12 pochodziło z Chin. Gospodarka Państwa Środka w zeszłym roku odzyskała jednak wigor. Różne sektory gospodarki odnotowały zwiększony popyt, ale chiński rynek monitoringu wizyjnego nadal zmagał się z wyzwaniami, takimi jak zmniejszenie wydatków rządowych, wolne tempo realizacji niektórych projektów oraz spowolnienie na rynku nieruchomości. W rzeczywistości, wraz z zakończeniem dużych projektów miejskich, takich jak Projekt Xueliang, inwestycje rządu w bezpieczeństwo publiczne zmalały. Co nie zmienia faktu, że chińscy dostawcy rozwiązań nieustannie doskonalą swoje produkty i rozbudowują ofertę. Na przykład Hikvision i Dahua wprowadziły zaawansowane rozwiązania, takie jak kamery bispektralne, wieloprzetwornikowe czy kamery do pracy w słabym oświetleniu. Mniejsi dostawcy znajdują swoje nisze, chińskie firmy nadal oferują innowacyjne rozwiązania użytkownikom w specyficznych zastosowaniach, takich jak inteligentny transport i inteligentne fabryki. To pozytywny znak dla rynku chińskiego, który według ekspertów ponownie wejdzie na ścieżkę wzrostu.

### Wzrost rynku VSaaS

Inna rzecz, że zauważalny jest znaczny wzrost wartości usług VSaaS (monitoring wizyjny jako usługa). Na tym polu przodują Stany Zjednoczone. Jak czytamy w raporcie, w 2023 r. w USA liczba kamer połączonych z chmurą wzrosła o ponad milion w porównaniu do 2022 r., choć ogólny odsetek kamer z aktywnym połączeniem nadal pozostaje niewielki.

Dane te częściowo potwierdzają wyniki ankiety *Edge Storage in Cloud-Based Video Security Applications,* przeprowadzonej przez asmag.com we współpracy z Micron. Na pytanie, czy respondenci obecnie oferują rozwiązania monitoringu wizyjnego wykorzystujące

rozwiązania w chmurze 62% respondentów odpowiedziało twierdząco. Spośród 38% firm, które jeszcze tego nie robią, prawie połowa (47%) planuje wprowadzenie takiej usługi w ciągu najbliższych 12 miesięcy.

### Rynek monitoringu wizyjnego – oczekiwany wzrost

Mimo mało spektakularnych tegorocznych wyników eksperci Novaira Insights z optymizmem patrzą w przyszłość rynku monitoringu wizyjnego. Przewidują, że rynek chiński będzie rósł, mimo że wolniej niż wcześniej. W innych regionach wzrost wartości tego rynku powinien przyspieszyć, głównie za sprawą dynamicznego rozwoju rynkach wschodzących, takich jak Indie, Ameryka Łacińska i Bliski Wschód. Na pewno też należy się liczyć z rosnącym popytem na rozwiązania chmurowe na ugruntowanych rynkach, takich jak Ameryka Północna i Europa Zachodnia. W rezultacie globalny rynek systemów do monitoringu wizyjnego ma wzrosnąć o 8,4% w 2024 r., osiągając wartość ponad 27 mld dol.

# Rynek zabezpieczeń technicznych i usług bezpieczeństwa ma się dobrze

Najnowszy raport opracowany przez Security Industry Association (SIA), ASIS International i Omdia *Złożoność globalnego rynku bezpieczeństwa: 2024-2026* wskazuje, że wartość branży security będzie w najbliższym czasie nadal rosnąć.

Z pewnością spory wpływ na to ma fakt wykorzystania najnowszych narzędzi, takich jak AI i chmura. Nie można też zapomnieć, że firmy sektora zabezpieczeń technicznych i usług bezpieczeństwa są ważnym graczem na rynku pracy.

Zgodnie z ustaleniami autorów raportu wartość rynku systemów zabezpieczeń technicznych w 2024 r. osiągnie 60,1 mld dol. (w 2023 r. było to 56 mld, a rok wcześniej 51 mld dol.). Szacuje się, że w roku 2026 będzie to już 70 mld dol. Liczby te pokazują, że roczna stopa wzrostu w latach 2022–2026 wyniesie 8,2%.

Autorzy raportu podzielili rynek na pięć kategorii: monitoring wizyjny, kontrola dostępu, alarmy przeciwwłamaniowe, sygnalizacja pożaru oraz inne urządzenia zabezpieczeń. Monitoring wizyjny stanowi około połowy globalnego rynku urządzeń zabezpieczeń, a największym pod względem przychodów rynkiem krajowym są w tej kategorii Chiny. Kontrola dostępu jest drugą co do wielkości kategorią, przy czym Ameryka Północna jest największym rynkiem regionalnym, natomiast Ameryka Łacińska oraz Bliski Wschód i Afryka są w tej kategorii najszybciej rosnącymi regionami. Systemy sygnalizacji pożarowej są trzecią co do wielkości kategorią i to z Ameryką Północną jako największym rynkiem regionalnym. Nieco inaczej wygląda sytuacja dotycząca alarmów antywłamaniowych. Prognozy dla tej kategorii są takie, że wartość tego rynku będzie rosnąć wolniej niż wartość rynku sygnalizacji pożaru.

### Usługi ochrony fizycznej

W roku 2022 wartość rynku usług ochrony fizycznej szacowano na 298 mld dol. Rok później było to już 319 mld, a wiele wskazuje na to, według autorów raportu, że w roku 2026 będzie to już 389 mld dol., co w latach 2022–2026 daje roczną stopę wzrostu na poziomie 6,9%.

Raport dzieli rynek ochrony fizycznej na usługi bezpieczeństwa, usługi wykrywania pożaru, monitoring alarmów oraz ochronę fizyczną. Usługi bezpieczeństwa obejmują usługi świadczone przez integratorów i instalatorów systemów bezpieczeństwa i podlegają kilku trendom, w tym rosnącemu zapotrzebowaniu na oprogramowanie wykorzystujące funkcje predykcyjne oraz systemy zarządzania budynkami (BMS).

Jeśli chodzi o usługi wykrywania pożarów, eksperci zwracają uwagę, że w wielu regionach zarówno systemy przeciwpożarowe, jak i firmy zajmujące się nimi podlegają wielu regulacjom, co czasami hamuje tempo rozwoju tej kategorii.

Znaczący wkład w rynek usług ma zdalne monitorowanie alarmów przeciwwłamaniowych oraz innych urządzeń zabezpieczeń. Jest to duży segment rynku, za którego wielkość odpowiada przede wszystkim zapotrzebowanie na ochronę lokalizacji użytkowników końcowych, a nawet, w niektórych przypadkach, zastosowanie monitoringu jest warunkiem niezbędnym do zawarcia umowy ubezpieczenia. W tej kategorii najwięcej takich usług świadczonych jest w Ameryce Północnej.

### Trendy technologiczne

Pod względem trendów technologicznych, według raportu, sztuczna inteligencja (AI) i chmura nadal dominują w branży security.

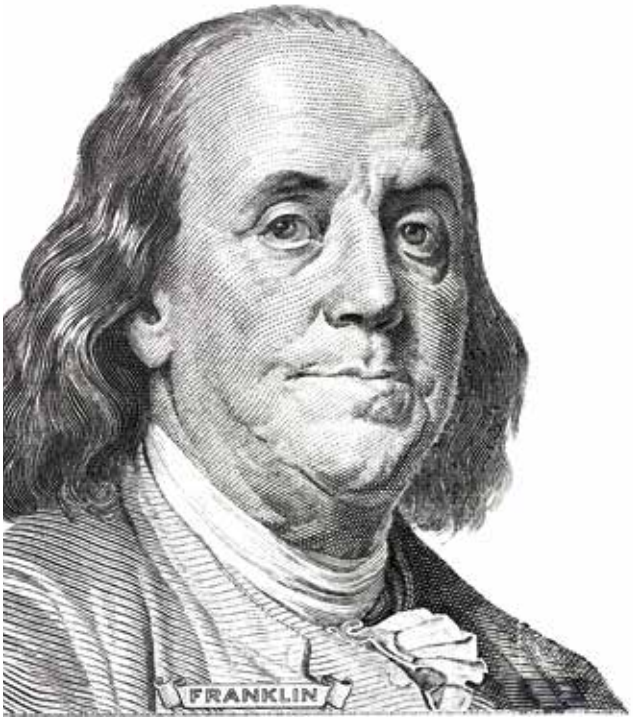
AI jest coraz bardziej obecna na rynku monitoringu wizyjnego. Stosowanie rozproszonej architektury w połączeniu z algorytmami AI w oprogramowaniu do obsługi urządzeń końcowych umożliwia przetwarzanie danych w urządzeniach funkcjonujących na brzegu sieci. Innym podejściem jest powierzenie obliczeń serwerom chmurowym, czemu sprzyja rozwój sieci 5G. Coś jest na rzeczy. Takie podejście obserwujemy również na rynku polskim.

Oferta systemu monitoringu wizyjnego proponowana jako usługa (VSaaS) staje się coraz ważniejszym modelem biznesowym. Wielu użytkowników końcowych szuka rozwiązania hybrydowego, oferują one bowiem elastyczność, pozwalając organizacjom na przechowywanie krytycznych danych na miejscu, jednocześnie wykorzystując skalowalność i dostępność chmury do przechowywania danych mniej wrażliwych.

Wyraźny staje się także trend stosowania m.in. kamer monitoringu wizyjnego do gromadzenia danych przydatnych do wprowadzania zrównoważonych rozwiązań w inteligentnych miastach. ●

**FIRMY BRANŻY SECURITY LICZĄCYM SIĘ PRACODAWCĄ**

Omdia szacuje, że na całym świecie ponad 30 mln osób jest zatrudnionych (w wymiarze pełnego etatu) bezpośrednio w usługach związanych z bezpieczeństwem fizycznym i wykrywaniem pożarów. Oczywiście najwięcej jest pracowników ochrony, tych działających, można by rzec, na froncie – mowa bowiem o ponad 28 mln.




# HANDEL SIĘ LICZY

Handel w Polsce odbywa się jak kraj długi i szeroki: w sklepach, punktach gastronomicznych, na stacjach paliw, ale także na bazarach, w eleganckich butikach i demokratycznym Internecie. Z pozoru to nic nowego, ale nawyki konsumentów się zmieniają, a co za tym idzie – samo zjawisko także. Co obecnie wywiera na nie największy wpływ? Istotnych czynników jest kilka. Zapraszamy do naszego raportu!

Tekst: **Adela Prochyra**
Komentarz eksperta: **Jan T. Grusznic**

Przed rokiem w *Raporcie o handlu* („a&s Polska" 6/2023) pisaliśmy o czterech głównych trendach, które w największym stopniu kształtują polski handel: konsekwencjach pandemii COVID-19, zmieniających się upodobaniach klientów, wymogach zrównoważonego rozwoju i zmianach w prawie. Rzecz z trendami – w każdej dziedzinie gospodarki, nie tylko w handlu – ma się tak, że oddziałują one długofalowo i rzadko wysycają się w ciągu kilku(nastu) miesięcy, aby być zastąpione kolejnym nurtem. Można to łatwo zaobserwować na przykładzie skutków pandemicznego „trzęsienia ziemi". Dopiero teraz, pięć lat od jej wybuchu, możemy mówić, że sytuacja się ustabilizowała i gwałtowne zmiany, jakie zachodziły w światowej gospodarce w latach 2020–22, można uznać za zakończone. Trzy pozostałe trendy wymienione w zeszłorocznym raporcie nadal mają się dobrze i ich oddziaływanie pozostaje w mocy. W przypadku tak złożonego zjawiska, jakim jest handel piątego pod względem wielkości państwa w Unii Europejskiej i jego dużej gospodarki, liczba czynników mających na niego wpływ jest jednak bardzo duża. W tym roku zamierzamy przyjrzeć się im z większą szczegółowością, rozważyć mniej namacalne wpływy, które w ostatecznym rozrachunku mogą okazać się wyjątkowo istotne.

## Handel w liczbach

Skoro handel, to pieniądze. Tradycyjnie zacznijmy więc od oglądu sytuacji finansowej. Pierwsza niezła wiadomość jest taka, że po bardzo niespokojnym 2023 r. inflacja hamuje. W roku 2024 poziom inflacji w Polsce, mierzony wskaźnikiem CPI (wskaźnik cen towarów i usług konsumpcyjnych) przedstawiał się następująco. W styczniu wyniosła ona 3,7%, w lutym spadła do 2,8%. W marcu i kwietniu utrzymał się trend spadkowy, osiągając odpowiednio: 2,0% i 2,4%. Następnie w maju i czerwcu inflacja wzrosła nieznacznie – do 2,5% i 2,6%. W lipcu nastąpił pierwszy w tym roku znaczny skok – do 4,2%, a w sierpniu do 4,3%, co wskazuje na przyspieszenie inflacji po wcześniejszym okresie spadków. Wrzesień i październik przyniosły dalszy wzrost, osiągając poziomy 4,9% i 5%.

Badania makroekonomiczne nad związkiem między inflacją a wzrostem gospodarczym pokazują, że do pewnego poziomu inflacja może stymulować wzrost gospodarczy państw. Zdaje się, że jesteśmy właśnie w tym punkcie. Konkretna liczba zależy od zastosowanego modelu badawczego oraz od tego, czy mowa o kraju rozwijającym się, czy rozwiniętym. Wysoka inflacja zazwyczaj hamuje rozwój gospodarczy, a progowy poziom najczęściej jest określany w okolicach 10% dla krajów rozwiniętych i 15% dla krajów rozwijających się. Należy jednak pamiętać, że zmiany inflacji wyjaśniają tylko część zmian dynamiki PKB. PKB Polski w bieżącym roku wzrósł o 2,1% w pierwszym kwartale 2024 i 3,2% w drugim kwartale w stosunku do danych zeszłorocznych.

Jak podaje GUS w raporcie sygnalnym, sektor eksportowy odnotował w pierwszych ośmiu miesiącach 2024 r. niewielkie spowolnienie, osiągając łączną wartość 229,6 mld euro. (Dla porównania: w zeszłym roku od stycznia do czerwca eksport wyniósł 821,4 mld zł, w tym – 752,0 mld zł; import 790,06 mld zł w 2023 roku i 732,0 mld zł w 2024 roku). To spadek o 2,2% w porównaniu z analogicznym okresem poprzedniego roku. Eksport do Niemiec, które pozostają głównym partnerem handlowym Polski, był do końca sierpnia 2024 r. o 6,5%

## Security w handlu

**Komentarz eksperta**

Jak wynika z danych Komendy Głównej Policji (KGP), w trzech pierwszych kwartałach 2024 r. stwierdzono 22 948 przestępstw kradzieży w sklepach, co stanowi spadek o 30,5% w porównaniu do analogicznego okresu 2023 r., kiedy to odnotowano 32 997 takich przypadków. Eksperci uważają, że branża handlowa najgorszy okres ma już za sobą, a trend spadkowy liczby przestępstw kradzieży utrzymuje się od początku roku. Jednakże, patrząc z perspektywy długoterminowej, poziom kradzieży wciąż pozostaje wysoki i zbliżony do tego z 2022 r.

Jednym z czynników wpływających na te dane była zmiana progu między wykroczeniem a przestępstwem. Zgodnie z art. 119 § 1 kodeksu wykroczeń, kto kradnie rzecz o wartości do 800 zł, podlega karze aresztu, ograniczenia wolności albo grzywny. Jeżeli wartość skradzionej rzeczy przekroczy kwotę 800 zł, to popełnione zostaje przestępstwo. Kwota ta została zmieniona 1 października 2023 r. Dane policyjne za rok 2023 wskazują, że najwięcej przestępstw kradzieży i wykroczeń popełniały osoby w wieku 30–49 lat, a w przypadku przestępstw drugą co do wielkości grupą były osoby w wieku 25–29 lat. Natomiast najwięcej wykroczeń popełniały osoby w wieku co najmniej 50 lat. Złodzieje często wybierają sklepy wielkopowierzchniowe, gdzie łatwiej można się ukryć w tłumie, natomiast w mniejszych sklepach są z reguły szybciej zauważani.

Z danych KGP wynika również, że w pierwszych trzech kwartałach 2024 r. stwierdzono 200,2 tys. wykroczeń kradzieży w sklepach, co stanowi spadek o 3,9% w porównaniu do analogicznego okresu ubiegłego roku. Duże sklepy są najczęściej okradane, a na tego typu placówki przypadło ponad 81% wykroczeń kradzieży. Wynika to głównie z kas samoobsługowych, które mimo inwestycji w nowe systemy zabezpieczeń nadal pozostawiają luki wykorzystywane przez nieuczciwych klientów.

Eksperci przewidują, że sytuacja w IV kwartale 2024 r. oraz w I kwartale 2025 r. może się zmienić. Rosnąca inflacja, wyższe ceny w sklepach oraz zwiększone potrzeby konsumpcyjne w sezonie świątecznym mogą spowodować wzrost liczby kradzieży, dlatego konieczne jest dalsze monitorowanie sytuacji oraz wprowadzanie skuteczniejszych środków zapobiegawczych.

niższy niż przed rokiem. Do pozostałych krajów strefy euro był on w tym samym okresie o 2,3% niższy. Jeśli chodzi o kraje spoza strefy euro, spadek eksportu do nich wyniósł 1,9%. Lepiej sprawa ma się w przypadku eksportu do wysoko rozwiniętych krajów spoza Unii, takich jak Wielka Brytania (+6,4%) czy Stany Zjednoczone (+7,7%). Zwiększył się także eksport do krajów Europy Środkowo-Wschodniej (łącznie o 3,7%), zwłaszcza Ukrainy (+14,7%).

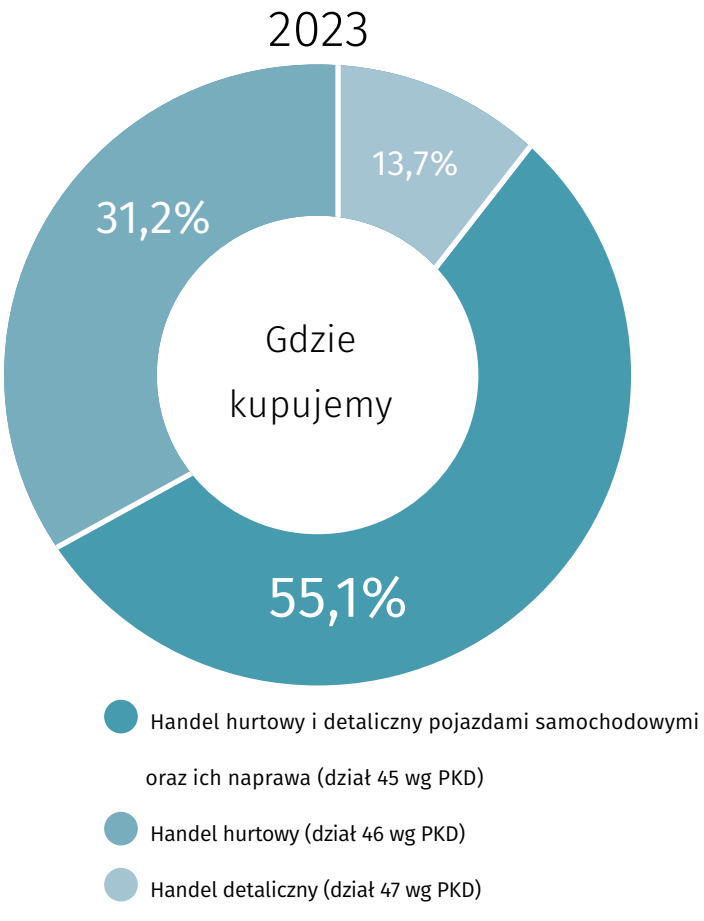
W pierwszych ośmiu miesiącach 2024 r. także import do Polski nieco spadł – o 0,1% w porównaniu z analogicznym okresem 2023 roku i wyniósł 227,1 mld euro. Obserwowano zróżnicowane trendy w zależności od regionu pochodzenia towarów: spadek importu z Niemiec wyniósł 1,9%, z pozostałych krajów strefy euro przyjechało do Polski o 1,2% mniej towarów niż w analogicznym okresie zeszłego roku. Nie zmieniła się wartość importu z krajów UE poza strefą euro, natomiast, podobnie jak w przypadku eksportu, odnotowano wzrost, jeśli chodzi o kraje wysokorozwinięte spoza Unii (4,4%), głównie Stany Zjednoczone (17,2%). Miał miejsce duży spadek importu z krajów Europy Środkowo-Wschodniej (10,5%) i niewielki spadek z krajów rozwijających się (1,0%), głównie ze względu na intensywną wymianę z Chinami, naszym drugim partnerem w imporcie (+1,9%). Warto mieć jednak na względzie, że w przypadku importu z Chin kwota 31,6 mld euro jest zawyżona, ponieważ część tych towarów przechodzi przez inne kraje, zanim trafi do Polski.

## Z bazaru do dyskontu

W przypadku handlu pierwszą kategorią, której należy się przyjrzeć, są artykuły spożywcze. Popyt na żywność charakteryzuje się większą sztywnością niż popyt na dobra, które nie są artykułami pierwszej potrzeby. Oznacza to, że nawet w obliczu podwyżek cen konsumenci są skłonni utrzymywać względnie stały poziom konsumpcji żywności. Z powodu efektu inflacyjnego można było zaobserwować zwiększony udział wydatków gospodarstw domowych na żywność w latach 2022–23, choć nie przekładało się to ani na wolumen zakupów, ani na zwiększenie zysków sprzedawców. Do roku 2025 rynek nie oczekuje istotnego odbicia.

Handel tradycyjny jest systematycznie wypierany przez handel w innych postaciach. „Rzeczpospolita", powołując się na przygotowane specjalnie dla niej dane zebrane przez firmę analityczną Dun & Bradstreet, podaje, że w pierwszym półroczu 2024 r. z polskich

Struktura przychodów netto ze sprzedaży produktów, towarów i materiałów w przesiębiorstwach handlowych (ceny bieżące)




źródło: GUS „Rynek wewnętrzny 2023", Warszawa 2024

**Udział działalności handlowej w tworzeniu PKB w 2023 roku stanowił 12,9%. Rok wcześniej było to 13,8%, dwa lata wcześniej – 13,9%**

bazarów zniknęło niemal 800 punktów sprzedaży detalicznej, a ok. 3,2 tys. firm tego typu zawiesiło działalność. Sprzedawcy mówią wprost, że klienci coraz częściej przenoszą się z zakupami do Internetu. Jednocześnie, jak podaje GUS, liczba targowisk w Polsce rośnie – w 2021 r. było ich 2116, w 2023 r. – już 2560.

Sukcesywnie spada natomiast liczba niezależnych sklepów FMCG. Portal wiadomoscispozywcze.pl alarmuje, że „z dnia na dzień z rynku znikają kolejne niezależne sklepy". Potwierdzają to dane GUS: „Udział sprzedaży detalicznej zrealizowanej w 2023 r. przez podmioty o liczbie pracujących do 9 osób wyniósł 25,7%". Gdzie więc odbywa się sprzedaż żywności? Przede wszystkim w sklepach sieciowych średniego formatu: hipermarketach, supermarketach i dyskontach, które w ostatnim czasie niemal zdominowały rynek polski. Rynek jest podzielony ściśle między trzy marki: Biedronkę, która dysponuje największą liczbą sklepów (na koniec I kwartału 2024 r. miała 3596 placówek w 1300 miejscowościach), Lidl (ponad 900 sklepów) i jedyny z polskim kapitałem, błyskawicznie rozwijający się Dino (30 września 2024 r. sieć liczyła 2572 markety). Istotnym graczem na rynku jest też lider formatu convenience store, czyli Żabka, która ma w Polsce już ponad 10 tys. punktów. Liczby te składają się na ponad 70-proc. udział sieci w polskim rynku spożywczym (dane firmy CPS GfK za 2023 r.).

W swojej dorocznej analizie rynku wewnętrznego GUS podaje, że na koniec 2023 r. działało w Polsce blisko 327 tys. sklepów, co oznacza wzrost o 0,2% w porównaniu do roku poprzedniego. Jednocześnie łączna powierzchnia sprzedażowa wszystkich sklepów zwiększyła się o 1,4% i osiągnęła 39 102,6 tys. m². Największy wzrost powierzchni sprzedażowej zaobserwowano w sklepach średniej wielkości (400–999 m²), co pokrywa się z intensywnym rozwojem sieci dyskontów i dużych (powyżej 1000 m²). Sklepy o powierzchni 400–999 m² powiększyły swoją powierzchnię o 581,8 tys. m², co stanowi wzrost o 6,8%. W tej samej kategorii odnotowano również największy wzrost liczby sklepów (o 6,4%). Z kolei sklepy o powierzchni powyżej 1000 m² zwiększyły swoją powierzchnię o 275,9 tys. m² (wzrost o 2,5%).

Przeciwną tendencję zaobserwowano w przypadku najmniejszych sklepów (do 99 m²), gdzie powierzchnia sprzedażowa zmniejszyła się o 410,9 tys. m² (spadek o 2,8%). Zbiega się to z osłabieniem pozycji przedsiębiorców niebędących franczyzobiorcami oraz generalnymi trendami. Wysoka inflacja w 2023 r. znacząco utrudniła funkcjonowanie europejskiej branży spożywczej. Rosnące ceny produktów spowodowały, że konsumenci zaczęli ograniczać wydatki na żywność, co przełożyło się na spadek sprzedaży. Mniejsze zarobki również ograniczyły siłę nabywczą Europejczyków. Porównując inflację artykułów spożywczych w Europie (12,8%) ze wzrostem wielkości sprzedaży (8,6%), wyraźnie widać, że rzeczywista wartość sprzedaży, skorygowana o inflację, spadła o 4,5% w porównaniu z rokiem 2022.

W odpowiedzi na tę sytuację konsumenci częściej zaczęli wybierać tańsze produkty, takie jak marki własne (+1,8%). Również dyskonty zyskały na znaczeniu, zwiększając swój udział w rynku. W Polsce wzrost popularności marek własnych był jeszcze bardziej widoczny, osiągając 1%. Mimo zwiększenia udziału dyskontów i marek własnych supermarkety wciąż utrzymywały dominującą pozycję na rynku, kontrolując 37,2% sprzedaży.

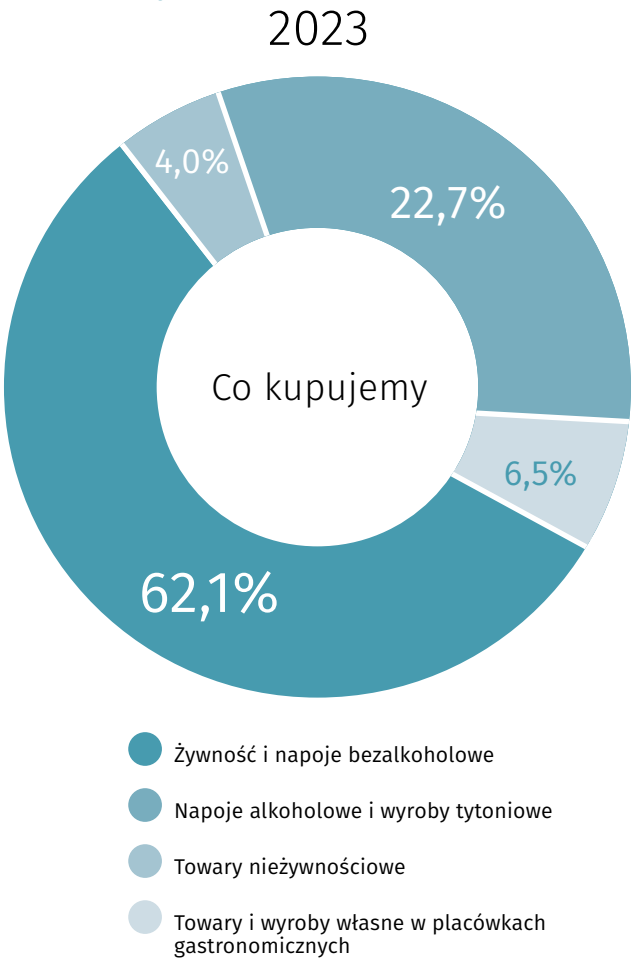
Największe szkody w handlu odnotowano w sektorze spożywczym. Były one spowodowane głównie przestępstwami sklepowymi. Co ciekawe, aż 50,4% odnotowanych przestępstw sklepowych przypada właśnie na sklepy spożywcze. Nie dziwi więc fakt, że przestępcy, którzy jak dotąd wielokrotnie dokonywali kradzieży, w momencie pojawienia się kas samoobsługowych dostrzegli szansę na nowe możliwości oszustw i wykorzystali lukę w zabezpieczeniu.

W ciągu zaledwie kilku lat Polska stała się liderem w Europie pod względem liczby kas samoobsługowych. W roku 2021 ich liczba wzrosła o ponad 90% w porównaniu do roku poprzedniego. W Polsce Biedronka chwali się instalacją 15 tysięcznej kasy samoobsługowej. Inne sieci również zainstalowały tysiące takich urządzeń, co pozwala sprzedawcom na redukcję kosztów i rozwiązanie problemu deficytu pracowników.

Tymczasem brak bezpośredniego nadzoru sprawia, że sklepy odnotowują większe straty z powodu kradzieży – nawet o 31% więcej niż w przypadku tradycyjnych kas. Klienci, czując się anonimowi, częściej decydują się na oszustwa, takie jak skanowanie tańszych produktów zamiast droższych.

Aby przeciwdziałać tego typu problemom, sklepy inwestują w zaawansowane systemy monitoringu i zabezpieczeń. Polscy sprzedawcy detaliczni wydają ok. 1,1% swoich obrotów na kwestie bezpieczeństwa. Zaliczają się do nich tradycyjne systemy sygnalizacji włamania i ochrona fizyczna stała lub doraźna, dozór wizyjny oraz systemy przeciwkradzieżowe, elektroniczne zabezpieczenia towarów

Struktura przychodów netto ze sprzedaży produktów, towarów i materiałów w przedsiębiorstwach handlowych (ceny bieżące)




Źródło: GUS „Rynek wewnętrzny 2023", Warszawa 2024

Konsumenci oczekują perfekcyjnej obsługi, a to oznacza m.in. dobrej jakości towar, błyskawiczną i niedrogą przesyłkę, sprawny proces reklamacyjny i łatwy kontakt ze sprzedawcą.

## Z dyskontu do e-commerce

Świeża żywność jest tą kategorią, której sprzedaż w Internecie nie cieszy się dużym zainteresowaniem. Sprzedaż niemal wszystkich innych, ze szczególnym naciskiem na odzież, obuwie, ale także artykuły RTV/AGD, książki jest bardzo dobra. Mimo że obecnie polski e-handel znajduje się w fazie stagnacji (mBank, *Handel detaliczny 2024*), a jego dynamika rozwoju w 2024 r. spadła w porównaniu z analogicznym okresem w roku poprzednim (PAP), nadal jest to jedna z najlepiej rozwijających się branż w kraju. Dla ścisłości – czwarta najszybciej rozwijająca się branża w Polsce pod względem liczby nowych firm rejestrowanych w Krajowym Rejestrze Sądowym. (Pierwsze trzy to działalność związana z oprogramowaniem, prace wykończeniowe oraz fryzjerstwo). Tutaj nie dotarł jeszcze trend ze stacjonarnej strony lustra, który sprawia, że najwięksi gracze zmiatają z planszy mniejszych – w polskim Internecie jest miejsce i dla światowych (bądź krajowych) gigantów, i dla średniaków, i dla maluczkich.

Średnio dziennie zakładanych jest 20 nowych firm, które jako podstawowy zakres swojej działalności wskazują sprzedaż internetową. Do końca czerwca br. powstało takich firm 7,2 tys.; do końca roku ich łączna liczba przekroczy 70 tys. Dla porównania: w zeszłym roku przebijaliśmy barierę 60 tys. Nawet biorąc poprawkę na te przedsiębiorstwa, które zamknęły swoje wirtualne podwoje (3,9 tys.) lub zawiesiły działalność (4,5 tys.), nadal jesteśmy jednym z największych rynków e-commerce w Europie. Co więcej, ich sytuacja finansowa jest zwykle dobra lub bardzo dobra.

Najlepiej radzą sobie podmioty średnich rozmiarów, o rocznych przychodach między 10 a 250 mln zł. Najsłabiej – firmy młode i małe, te z rocznym dochodem poniżej 10 mln. Sytuacja finansowa aż 52% z nich jest zła lub bardzo zła. Średnio jednak polski sklep internetowy generuje rocznie ok. 8 mln zł przychodu. Z tej kwoty można wyodrębnić średni zysk netto wynoszący ok. 250 tys. zł. Oznacza to, że rentowność takiego sklepu kształtuje się na poziomie ok. 2,7%. Zaznaczmy, że istnieją również znacznie więksi gracze, których roczne przychody sięgają miliardów złotych. Ci zwykle radzą sobie bardzo dobrze (81%), rzadko słabo (19%).

Polscy konsumenci są dobrze zaznajomieni z zakupami w sieci. Co najmniej raz w życiu zrobił je każdy internauta z naszego kraju,

a regularnie z tej formy zaopatrywania się w różne towary korzysta spory odsetek – 37% robi zakupy online co najmniej pięć razy w miesiącu (dane Izby Gospodarki Elektronicznej). 87% zrobiło je co najmniej raz w ciągu minionego półrocza. Rynek e-commerce jest więc nie tylko duży i chłonny, ale też zmienny. Regularnie pojawiają się na nim nowe trendy, które kształtują oblicze handlu elektronicznego. Do największych i najbardziej aktualnych należą:

- transmisje na żywo, pozwalające na interaktywne zakupy i budowanie relacji marek z klientami;
- media społecznościowe przekształciły się w platformy sprzedażowe, umożliwiając łatwiejsze dotarcie do młodszych konsumentów;
- polskie firmy coraz śmielej wychodzą poza granicę kraju, sprzedając swoje produkty na całym świecie. Ekspansją na rynkach europejskich i pozaeuropejskich mogą pochwalić się marki z każdej branży – od producentów skarpet po wytwórców wyrafinowanej elektroniki;
- model subskrypcji, znany z wielu „tradycyjnych" branż, zyskuje na popularności także w e-commerce, oferując klientom wygodę i przewidywalność zakupów. Stosowany w tak różnych dziedzinach, jak kosmetyki, miody, kawy, żywienie zwierząt czy bielizna bądź dobra niematerialne, jak serwisy streamingowe;
- w odpowiedzi na rosnącą świadomość ekologiczną coraz więcej osób decyduje się na zakup używanych produktów, co przyczyniło się do bardzo intensywnego rozwoju rynku *e-commerce*.
- z kolei producenci, chcąc mieć większą kontrolę nad sprzedażą i budować silniejsze relacje z klientami, coraz częściej decydują się na sprzedaż bezpośrednią, omijając pośredników.
- *omnichannel* łączy w sobie różne kanały sprzedaży: sklepy stacjonarne, sklepy internetowe, aplikacje mobilne, a nawet media społecznościowe, tworząc spójne doświadczenie zakupowe.

Handel jest jedną z tych branż, które bardzo szybko przyjmują innowacyjne rozwiązania i zgrabnie zaprzęgają je do swojego użytku. Świadczy o tym chociażby dotychczasowe wykorzystanie sztucznej inteligencji, np. do stworzenia wersji webowych i mobilnych e-sklepów, analityki danych na temat preferencji klientów, optymalizacji procesów wysyłki i zbudowania algorytmów, które zaspokajają, a nawet przewidują pragnienia konsumentów. Jest jednak coś, co przysparza właścicielom niemałych kłopotów, a w czym sztuczna inteligencja uparcie się nie sprawdza. Brak rąk do pracy, brak pracowników z umiejętnościami cyfrowymi, duży wskaźnik rotacji i malejący średni staż pracy.

Konsumenci też nie pozostają już wyłącznie bierni, oni także mają swoje preferencje, które wpływają na kształt współczesnego handlu. Oczekują, to jasne, perfekcyjnej obsługi, a to oznacza m.in. dobrej jakości towar, błyskawiczną i niedrogą przesyłkę, sprawny proces reklamacyjny i łatwy kontakt ze sprzedawcą. Coraz częściej są to też innego rodzaju wymagania – dotyczące już nie wyłącznie wymiernych parametrów towaru i sklepu, ale także „miękkich" jakości, takich jak transparentność firmy (tj. gdzie i w jakich warunkach odbywa się jej produkcja), odpowiedzialność społeczna (redystrybucji zysków w środowiskach defaworyzowanych), innowacje uwzględniające środowisko i dobro – także psychiczne – użytkowników. Raport *Meaningful Brands 2024* (EAS), a także nowoczesne metody zabezpieczeń towarów, takie jak etykiety RFID, które pozwalają nie tylko zabezpieczać towary przed kradzieżą, ale także umożliwiają bieżące monitorowanie stanów magazynowych. Najnowsze projekty wykorzystują sztuczną inteligencję do rozpoznawania produktów i ułatwiają klientom samodzielne skanowanie towarów. Sztuczna inteligencja identyfikuje produkty umieszczone na wadze, rozróżniając jabłko Granny Smith od odmiany „polskie jabłko luzem", i uniemożliwia zeskanowanie melona jako dyni. W przypadku próby oszukania systemu sztucznej inteligencji nadal istnieje możliwość wykrycia nieuczciwego działania. Automatyczny monitoring zapamiętuje twarze klientów, którzy dokonali nadużyć, co może skutkować konsekwencjami prawnymi. Przykładowo, w sądzie w Zielonej Górze klient, który podmienił kod kreskowy na perfumach o wartości 120 zł, został ukarany grzywną w wysokości 1500 zł i trzema miesiącami pozbawienia wolności w zawieszeniu. Sąd zakwalifikował ten czyn jako kradzież, a oszustwo.

**Sztuczna inteligencja**

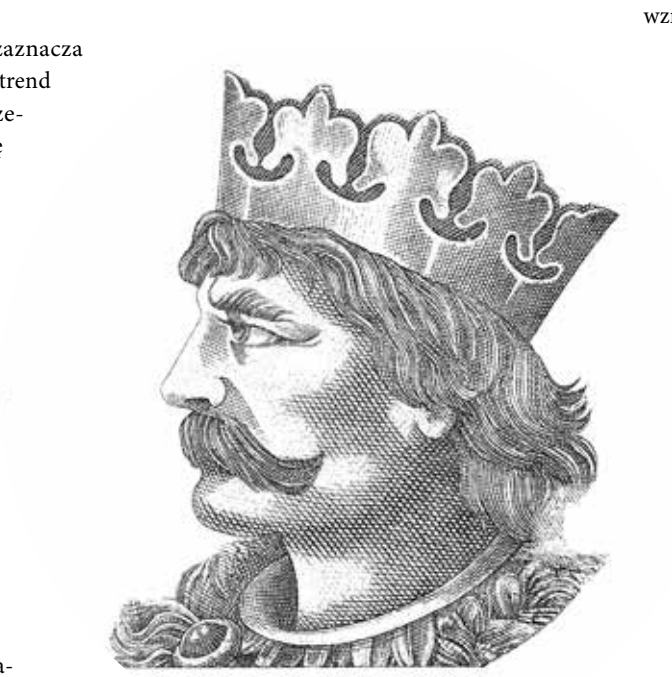
Pomimo zmieniających się taktyk kradzieży, istnieją skuteczne metody przewidywania incydentów. Technologia bezpieczeństwa, w tym analityka podejrzanych zachowań oraz generatywna sztuczna inteligencja, staje się coraz bardziej efektywna w identyfikacji wzorców i dostarczaniu informacji o anomaliach, umożliwiając pracownikom proaktywne reagowanie. Wzmacnianie strategii bezpieczeństwa przez sprzedawców detalicznych można osiągnąć poprzez trzy główne trendy: niezawodną analitykę

*The Rise of the Change Makers* przeprowadzony przez firmę Havas wskazuje, że klienci przestali traktować firmy jako zwykłych wytwórców i/lub sprzedawców dóbr codziennego użytku, ale mają wobec nich dużo większe oczekiwania, jak wobec aktywnych i, co ciekawe, obdarzonych świadomością, aktorów życia społecznego. Marki muszą być dziś empatyczne i zaangażowane w problemy świata, a także brać za nie część odpowiedzialności, np. organizować wydarzenia sportowe, finansować profilaktykę zdrowotną, prowadzić akcje edukacyjne, aktywnie przeciwdziałać zanieczyszczeniu środowiska, wspierać różne społeczności.

## Z e-commerce do butiku

Zamiast podsumowania przyjrzyjmy się najbardziej nieoczekiwanemu trendowi w handlu, a mianowicie zainteresowaniu produktami klasy premium, które w Polsce jest nawet wyższe niż w Europie (14% wg danych firmy McKinsey, za portalem: www.dlahandlu.pl).

Chociaż w naszym kraju zaznacza się on wyjątkowo silnie, jest to trend ogólnoświatowy. Od zakończenia pandemii obserwuje się dynamiczny wzrost sprzedaży artykułów luksusowych. Analitycy z Bain & Company i Altagamma przewidywali, że w 2024 roku sprzedaż detaliczna w sektorze premium wzrośnie o 4% w stosunku do 2023 roku i osiągnie poziom 390 miliardów euro.



Trend ten napędzany jest przez kilka czynników. Pierwszy, podstawowy, to ten, że konsumenci, pomimo inflacji i ograniczeń budżetowych, są skłonni płacić więcej za produkty wysokiej jakości. Ten trend obserwowany jest w różnych branżach, od mody i biżuterii po restauracje i hotele.

Drugi trend – pomimo licznych ograniczeń w ostatnich latach, europejscy konsumenci zgromadzili dodatkowe oszczędności o wartości prawie 1 biliona euro. Marki luksusowe wykorzystują tę siłę nabywczą, zachęcając klientów do wydawania oszczędności.

Kolejny trend to tzw. efekt niezapomnianych wrażeń, który łączy w sobie wyjątkowe doświadczenia zakupowe w sklepach zarówno stacjonarnych, jak i internetowych. Marki premium inwestują w różnego rodzaju ekskluzywne inicjatywy, takie jak organizowanie specjalnych wydarzeń, spotkań z wyjątkowymi ludźmi czy tworzenie limitowanych edycji produktów. W sukurs przychodzi im sztuczna inteligencja, która pozwala jeszcze lepiej dopasowywać oferty do indywidualnych potrzeb zamożnych klientów.

Ciekawym zagadnieniem w tym kontekście wydaje się zmiana na rynku nieruchomości handlowych. Wszystko wskazuje na to, że do przeszłości odchodzą domy towarowe, których pozostało w kraju już tylko 229 (dane za 2021 rok). Jednocześnie od roku 2010 ich liczba zmniejszyła się aż o 38% (dane: Bank Pekao S.A. za: wiadomoscihandlowe.pl). Mimo okresowego spadku liczby odwiedzających oraz obrotów centrów handlowych w ubiegłych latach w pierwszym kwartale 2024 r. obroty były na sześcioprocentowym plusie w stosunku do roku ubiegłego.

W raporcie Polskiej Rady Centrów Handlowych Rynek obiektów handlowych w Polsce podano, że w bieżącym roku powierzchnia nowoczesnych obiektów handlowych w Polsce osiągnęła 13,5 mln m2 GLA (Gross Leasable Area – powierzchnia użytkowa do wynajęcia), co oznacza wzrost o 190 tys. m2 GLA w porównaniu do poprzedniego okresu. Otwarto 15 nowych obiektów handlowych, a 5 zostało rozbudowanych lub zmodernizowanych. Największe z nich są zlokalizowane w Koszalinie, Lesznie i Bytomiu, co pokrywa się z obserwacją, iż najwięcej nowych powierzchni handlowych powstało w miastach liczących poniżej 100 tys. mieszkańców. W budowie jest jeszcze 28 obiektów, które mają zostać otwarte do końca 2024 r. Centra handlowe wciąż stanowią największą część nowoczesnej powierzchni handlowej, choć udział parków handlowych rośnie. Największa część powierzchni handlowej (52%) znajduje się w 8 największych aglomeracjach, w miastach liczących 100–400 tys. mieszkańców znajduje się 24%, pozostałe 24% w miastach najmniejszych.

Według najnowszych danych Polskiej Rady Centrów Handlowych, polski rynek nieruchomości handlowych przeżywa intensywny rozwój. W ciągu najbliższych trzech lat planowane jest otwarcie lub rozbudowa aż 123 obiektów handlowych, co przełoży się na wzrost całkowitej powierzchni handlowej o blisko 1,2 mln m2 GLA.

podejrzanych zachowań z wykorzystaniem rozwiązań predykcyjnych, platformy integrujące systemy bezpieczeństwa z POS i IoT oraz zmianę sposobu prezentowania danych na bardziej intuicyjny.

Scentralizowane operacje i zintegrowane systemy są kluczowe dla nowoczesnego bezpieczeństwa w handlu detalicznym. Ujednolicone platformy bezpieczeństwa, które integrują różne technologie i dane, takie jak dozór wizyjny, urządzenia IoT i POS, umożliwiają zespołom szybkie i efektywne reagowanie na incydenty. Dzięki takiej platformie można łatwo przeszukiwać nagrania wideo i dopasowywać je do podejrzanych transakcji, co zwiększa skuteczność stosowanych zabezpieczeń.

**Rozwiązania chmurowe w handlu**

Platformy, które integrują sygnały z systemów alarmowych z nadzorem wideo, zmniejszają liczbę fałszywych alarmów, umożliwiając szybką i efektywną reakcję. Ponadto wykorzystanie chmury obliczeniowej zapewnia zarządzanie systemem bezpieczeństwa z dowolnego miejsca i o każdej porze, co znacznie zwiększa elastyczność i efektywność operacyjną. Istotne jest również zastosowanie takich rozwiązań w zyskujących popularność sklepach samoobsługowych, nastawionych na wygodę, bezpieczeństwo i automatyzację operacji.

Rozwiązania oparte na chmurze, takie jak nadzór wideo jako usługa (VSaaS) i kontrola dostępu jako usługa (ACaaS), umożliwiają zdalne monitorowanie i zarządzanie bezpieczeństwem, eliminując potrzebę fizycznych serwerów i skomplikowanych instalacji na miejscu. Dzięki chmurze dane są bezpiecznie przechowywane i łatwo dostępne, a systemy są skalowalne i elastyczne. Aplikacje chmurowe są również tworzone z myślą o intuicyjnej obsłudze, znacząco różniąc się od interfejsów wdrażanych *on-prem*, które często wymagają przeszkolenia.

Wykorzystanie AI pozwala zbierać i analizować dane dotyczące ruchu klientów, obłożenia sklepu i innych kluczowych wskaźników. To umożliwia podejmowanie lepszych decyzji, a także optymalizację obsługi klienta oraz strategii sprzedaży. ●

# Podziel obiekt na pięć stref, by skutecznie przeciwdziałać kradzieżom

Przestępczość w handlu detalicznym pozostaje znaczącym wyzwaniem dla branży. Sieciowe rozwiązania do dozoru wizyjnego firmy Axis pomagają w ograniczeniu kradzieży i oszustw oraz działają odstraszająco, chroniąc klientów i pracowników przed przemocą. Podział obiektu handlowego na pięć logicznych stref ułatwia walkę z przestępcami.

Przestępczość w handlu detalicznym jest kwestią złożoną. Trudne warunki ekonomiczne, rosnące koszty życia i zwiększająca się liczba przestępstw dokonywanych przez zorganizowane grupy stanowią wielkie wyzwanie dla osób zajmujących się ochroną obiektów handlu detalicznego. Celem, jaki powinien im przyświecać, jest wdrażanie rozwiązań bezpieczeństwa i ochrony w sposób efektywny, a to wymaga starannego planowania opartego na danych. Pomocna będzie metodologia Pięciu Stref Wpływu opracowana przez działającą na Uniwersytecie Florydy Radę Badań Zapobiegania Stratom (*Loss Prevention Research Council,* LPRC). Zgodnie z propozycją LPCR każdy obiekt można podzielić na pięć kluczowych obszarów. Taki podział ułatwi m.in. obserwowanie sposobu, w jaki poruszają się obecne w danym miejscu osoby, a następnie wizualizację ich przemieszczania się. To z kolei oznacza łatwiejsze wytypowanie miejsc narażonych na działanie przestępców i nie tylko poprawia świadomość sytuacyjną, ale także pomaga podjąć odpowiednie kroki.

**Pięć stref w obrębie nieruchomości handlowej to:**
**STREFA 5. Cały obiekt**
**STREFA 4. Parking i najbliższe otoczenie**
**STREFA 3. Wejście/wyjście ze sklepu**
**STREFA 2. Powierzchnia sprzedaży**
**STREFA 1. Punkty wysokiego ryzyka**

W każdej z tych pięciu stref powinny działać, dostosowane do jej funkcji, rozwiązania dozorowe. Ważne, by zastosowany w obiekcie handlowym system umożliwiał tworzenie inteligentnych scen, dopasowanych do każdej ze stref, by możliwe było gromadzenie danych i błyskawiczna reakcja na incydenty oraz, co nie mniej ważne, zapis nagrań służących jako materiał dowodowy.
Przyjrzyjmy się zatem Pięciu Stefom Wpływu zdefiniowanym przez LPRC i temu, jakie rozwiązania można zastosować w każdej nich, by zapobiegać dokonywaniu przestępstw na terenie obiektów handlowych lub ograniczyć ich konsekwencje.

## STREFA 5. CAŁY OBIEKT

Jedną z najlepszych metod zapobiegania m.in. kradzieżom jest współpraca sklepów, które w danym obiekcie działają. Bardzo często padają one łupem gangów wyspecjalizowanych w okradaniu konkretnych placówek. Sklepy zlokalizowane tuż obok siebie mają często problemy z tymi samymi przestępcami. Dzieje się tak szczególnie, gdy są to zorganizowane szajki. Współpraca sklepów oraz udostępnianie danych organom ścigania i centrom operacji bezpieczeństwa (SOC) pozwoli opracować wzorzec takich ataków. Z kolei dane z nagrań wideo z całego obiektu umożliwiają profesjonalistom ds. zapobiegania stratom (LP/AP) przeszukanie nagrań i wsparcie organów ścigania w trwających śledztwach, umożliwiając skoordynowaną odpowiedź ze strony społeczności.

## STREFA 4. PARKING I JEGO OTOCZENIE

Rejestrowanie i analiza danych w tym miejscu są niezwykle ważne zarówno dla aktywnej profilaktyki, jak i szybkiej reakcji. Inteligentne systemy dozoru wizyjnego mogą umożliwiać prewencję, jeśli dzięki narzędziom rozpoznawania twarzy system „zauważy" twarz rejestrowanego wcześniej przestępcy i dyskretnie zaalarmuje ochronę. Kiedy ta osoba przekroczy granicę tej strefy, ochrona będzie mogła prewencyjnie ją obserwować, zapobiegając tym samym dokonaniu kradzieży lub aktów wandalizmu. W strefie 4. doskonale sprawdza się także oprogramowanie do rozpoznawania tablic rejestracyjnych.

## STREFA 3. WEJŚCIE/WYJŚCIE ZE SKLEPU

Umieszczenie kamer przy wejściach z jednej strony jest jasną informacją o obecności monitoringu, z drugiej – daje klientom poczucie bezpieczeństwa, wiedzą bowiem, że są chronieni. W przypadku jakiegokolwiek incydentu, gdy sytuacja eskaluje, rozwiązania kontroli dostępu mogą uniemożliwić wejście i wyjście, a system audio pozwala przekazać obecnym we wnętrzu stosowne komunikaty od ochrony. Poza godzinami otwarcia wykrywanie obecności osób przy wejściach może służyć jako wczesne ostrzeżenie przed kradzieżą lub wandalizmem, wyzwalając alarmy odstraszające i oświetlenie, aby odstraszyć intruzów.

## STREFA 2. POWIERZCHNIA SPRZEDAŻY

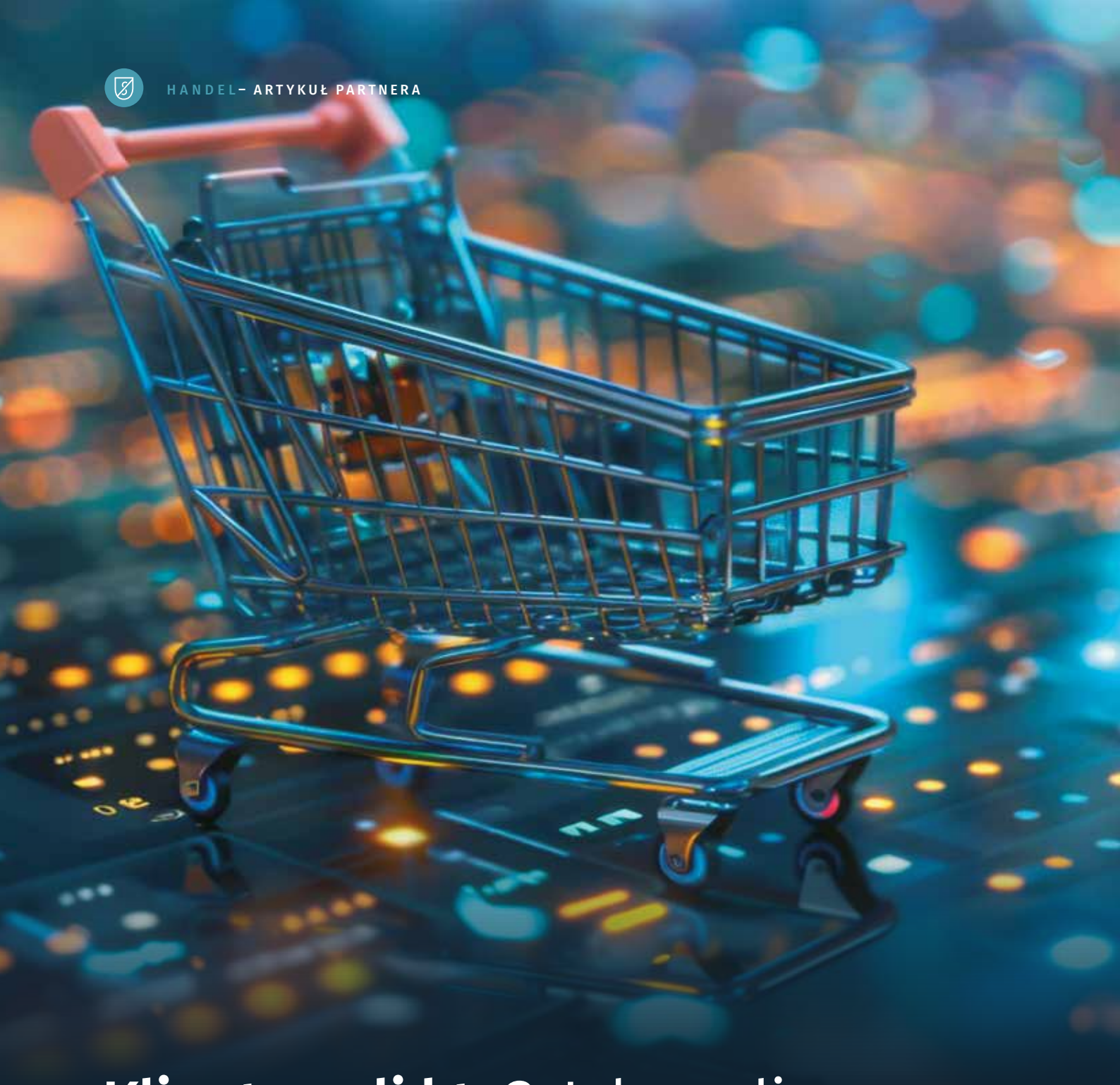
Ze względu na to, że w dużych obiektach sprzedaż jest często prowadzona na bardzo dużym, skomplikowanym pod względem architektonicznym terenie, szczególnie w okresach wzmożonego ruchu trudno utrzymać całkowitą świadomość sytuacyjną. Niełatwy może być monitoring różnych zaułków, zwłaszcza gdy ochrona próbuje się skupić na konkretnym osobniku lub grupie. Możliwość monitorowania wszystkich obszarów pozwala na interwencję w czasie rzeczywistym i przegląd nagrań po incydencie. Nagrania wideo we wszystkich strefach są niezbędne do skutecznego ścigania przestępstw w handlu detalicznym. Zawsze potrzebne są dowody w postaci nagrań wideo, które bez żadnej wątpliwości pozwolą zidentyfikować sprawcę od momentu jego wejścia w obszar zainteresowania.

## STREFA 1. PUNKTY WYSOKIEGO RYZYKA

W każdym obiekcie można zidentyfikować miejsca, które wymagają dodatkowej uwagi. Strategiczne umieszczanie urządzeń dozoru wizyjnego w strefach wysokiego ryzyka ułatwi obserwację, szczególnie jeśli zostaną zlokalizowane w pobliżu towarów o wysokim potencjale kradzieży (np. sprzętów elektronicznych lub półek i gablot z biżuterią bądź luksusowymi kosmetykami), a także w okolicy kas samoobsługowych. Tworzenie spójnego systemu łączącego kamery dozorowe z analizą wideo i rozwiązaniami nasobnymi może być niezwykle przydatne w dostarczaniu szczegółowych i krytycznych informacji dotyczących wszelkiego rodzaju wydarzeń. Połączenie uzyskanych w ten sposób danych z nagraniami dokumentującymi przebieg zdarzenia daje pełny obraz sytuacji.

Rozwijanie i utrzymywanie skutecznej strategii zapobiegania przestępstwom, zazwyczaj kradzieżom, ale też aktom wandalizmu, jest niekończącym się procesem. Wymaga gruntownego zrozumienia celu, jaki powinien przyświecać organizacji chroniącej dany obiekt, i jej ciągłego doskonalenia się. System dozoru dostarczony przez sprawdzonego dostawcę pozwala na gromadzenie i analizowanie danych, które nie tylko służą do prowadzenia ochrony w czasie rzeczywistym, ale także będą bazą działań predykcyjnych. Dozór wideo zapewne pozostanie jednym z najpotężniejszych narzędzi w zapobieganiu przestępstwom, zapewniając, że w razie potrzeby organy ścigania otrzymają niezbędne materiały dowodowe. Równie ważne jest to, że łącząc urządzenia dozorowe z aplikacjami do analizy wizyjnej, można skrócić czas oczekiwania w kolejkach, udoskonalić układ sklepu, kierować personel tam, gdzie jest potrzebny – w konsekwencji zwiększając zyski. Można nawet wykorzystać urządzenia do dozoru jako narzędzia do tworzenia przyjaznego środowiska, które przyciągnie gości i zainspiruje pracowników. Połączenie urządzeń Axis z aplikacjami naszych partnerów pozwoli poprawić bezpieczeństwo, ograniczyć braki towaru i jeszcze bardziej zwiększyć wydajność operacyjną. •

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



# **Klient, czyli kto?** Jak analiza materiału wizyjnego pomaga zrozumieć zachowania klientów

W dzisiejszych czasach sprzedawcy nie wyobrażają sobie prowadzenia biznesu bez gromadzenia i zarządzania danymi pomagającymi zidentyfikować potrzeby klientów. Kluczowe jest pozyskiwanie takich informacji, dzięki którym mogą zwiększyć liczbę klientów, poprawić współczynnik konwersji i interakcji oraz efektywność kampanii marketingowych i reklamowych, wskaźnik *user experience* itp.

**Armen Moska**

Rzecz w tym, że na razie dotyczy to przede wszystkim e-commerce. Sytuacja w sklepach stacjonarnych wygląda nieco odmiennie. Wspomniane dane i wskaźniki, które są absolutnym standardem w prowadzeniu biznesu e-commerce, stosunkowo rzadko są gromadzone w przypadku placówek stacjonarnych. Dlaczego tak się dzieje? Być może jest to związane z brakiem doświadczenia w zakresie analizy danych i umiejętności wyciągania na ich podstawie konstruktywnych wniosków. Z pewnością ograniczona liczba zasobów ludzkich jest tutaj również pewnym utrudnieniem. A i świadomość możliwości związanych z pozyskiwaniem informacji za pomocą analizy materiału wizyjnego mogłaby być jeszcze wyższa. Właściwie to nie wiedząc, jak i dlaczego, przeskoczyliśmy szybciutko ponad prostymi, dostępnymi i efektywnymi analitykami wizyjnymi do zaawansowanych algorytmów sztucznej inteligencji, której wdrażanie w obszarze wideo nadal pozostaje dość żmudne i kosztowne. Tymczasem sklepy mogą korzystać ze sprawdzonych, skalowalnych i niedrogich rozwiązań, które są dostępne od lat i potrafią efektywnie pomagać w poznaniu wzorców zachowań osób przebywających na terenie sklepu.

## Liczniki odwiedzin

Chcąc ocenić liczbę klientów, sklepy sięgają najczęściej po najbardziej podstawową informację, jaką jest liczba wystawionych paragonów. I faktycznie, w przypadku sklepów spożywczych takie podejście wydaje się uzasadnione. Trudno bowiem wyobrazić sobie sytuację, w której odwiedzający taki sklep klient, nie znalazłszy swojej ulubionej marki cukru czy soli, wychodzi głęboko wstrząśnięty i niczego nie kupuje. Zupełnie inaczej wygląda sytuacja sklepów z odzieżą, elektroniką lub DIY. Tutaj stosunkowo często zdarza się, że odwiedzający nie znajdują produktu, który spełnia ich oczekiwania w zakresie rodzaju, koloru, rozmiaru czy potrzebnych funkcji. W takim wypadku liczba wystawionych paragonów żadną miarą nie odzwierciedla liczby osób, które odwiedziły sklep. A to informacja bardzo ważna, pozwala bowiem obliczyć współczynnik konwersji. Znajomość współczynnika konwersji może przynieść lawinę pytań: co spowodowało, że ktoś wszedł do sklepu i nic w nim nie kupił? Czy wiązało się to z brakiem towaru, czy brakiem pożądanego produktu w ofercie? A może trudno było go znaleźć? Analiza materiału wizyjnego pozwoli odpowiedzieć na te pytania i wdrożyć odpowiednie działania, co realnie pomoże w podniesieniu przychodów.

Świetnym rozwiązaniem dla placówek znajdujących się w galeriach handlowych, pasażach czy pieszych ciągach komunikacyjnych jest funkcja *pass-by*. Pozwala ona nie tylko policzyć osoby, które sklep odwiedziły, ale także te, które przeszły obok, nie wchodząc. Pozwala to w prosty sposób oszacować potencjał sprzedażowy konkretnej placówki.

Analiza zapisów materiału wizyjnego z wnętrza sklepu pozwala nie tylko na dokładne policzenie liczby odwiedzających, ale także udostępni informacje o czasie ich przebywania w placówce. Można je wówczas połączyć w bardzo efektywny sposób z licznikiem wejść, liczbą i wartością wystawionych paragonów, strukturą koszyka czy sezonowością.

## Zakupowe ścieżki

Dzięki analizie materiału wizyjnego dla każdego sklepu można opracować tzw. heatmapę. Heatmapa pokazuje, w jaki sposób nabywcy poruszają się po sklepie, które miejsca najczęściej odwiedzają, a do jakich w ogóle nie zaglądają. Heatmapa może mieć formę grafiki lub raportu. To prawdziwa skarbnica wiedzy. Dzięki pozyskiwaniu danych tego typu można z łatwością identyfikować obszary o największym i najmniejszym potencjale marketingowym w sklepie, planować rozłożenie towaru zgodnie z rzeczywistymi ścieżkami poruszania się odwiedzających i – wreszcie – testować wpływ pozycjonowania produktów, zarządzania personelem placówki czy jego całościowym konceptem w oparciu o konkretne i miarodajne statystyki.

## Analiza sprzedaży

Znajomość liczby klientów w sklepie lub liczbie osób przechodzących obok, czasu przebywania w placówce i o tym, jak ludzie przemieszczają się po sklepie, w których jego obszarach jest ich najwięcej, a w których najmniej, przy których regałach klienci najczęściej przystają i na jak długo, a także jak długo trwa ich zainteresowanie konkretnymi produktami jest zatem bezcenna. To zaś oznacza, że można m.in.:

- zwiększyć współczynniki konwersji zarówno w przypadku klientów odwiedzających sklep, jak i tych, którzy obok niego przechodzą,
- zoptymalizować ofertę produktową,
- zarządzać w sposób optymalny merchandisingiem całego sklepu, bądź poszczególnych towarów lub ich grup,
- szybko reagować na wszelkiego rodzaju wahania sezonowe,
- obniżyć koszty operacyjne funkcjonowania placówki,
- optymalizować zasoby sprzedażowe,
- planować wsparcie sprzedaży i marketing,
- efektywnie zarządzać liczbą osób obsługi, dzięki lepszemu dostosowaniu np. grafików pracy.

Jednocześnie wszystkie dane pozyskane na drodze analizy materiału wizyjnego po połączeniu z konkretnymi systemami sklepowymi mogą posłużyć do błyskawicznej reakcji, wręcz w czasie rzeczywistym, do podjęcia konkretnych działań, będących odpowiedzią na to, jak w wygląda sytuacja w placówce. Może to być np.:

- zarządzanie kolejką do kas w zależności od liczby osób oczekujących,
- automatyzacja otwierania kolejnych kas lub uruchomienie mobilnego kasjera,
- wywoływanie komunikatów systemu audio zapraszających klientów do skorzystania z kas samoobsługowych,
- zarządzanie muzyką tła w sklepie w zależności od natężenia ruchu w placówce,
- zarządzanie systemem *Digital Signage* i treścią wyświetlanego materiału wizyjnego w zależności od liczby klientów, ich charakterystyki czy interakcji z konkretnymi produktami.

Jak widać możliwości, których dostarcza analiza materiału wizyjnego, jest naprawdę dużo. Niekoniecznie trzeba stosować algorytmy sztucznej inteligencji i kosztujące setki tysięcy złotych narzędzia analityczne, by wykorzystać potencjał drzemiący w danych łatwych do pozyskania dzięki analizie nagrań. Dziś tak naprawdę można zaprojektować kompleksowy system analizy wizyjnej za naprawdę niewielkie pieniądze. Wystarczy tylko zastanowić się, jakie informacje są istotne, jakich jeszcze brakuje, jak z nich korzystać i jak nimi zarządzać.

Systemy służące do tego typu analizy są na rynku dostępne od lat, ale ta technologia nadal ma ogromny, niewykorzystany jeszcze potencjał, aby znacząco odmienić metodę działania sprzedawców detalicznych. Sposoby prowadzenia sprzedaży cały czas ewoluują, ale rozwój technologii sklepowych chyba za tą ewolucją nie nadąża. Analiza może zatem odegrać znaczącą rolę w kształtowaniu przyszłości handlu detalicznego, umożliwiając sprzedawcom rozwój w coraz bardziej cyfrowym i skoncentrowanym na danych świecie. ●

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

# Raz, dwa, trzy... security patrzy i liczy

Dawno minęły czasy, kiedy liczbę osób obecnych w danym miejscu oceniało się „na oko", a o ostatecznej frekwencji kupujących świadczył stan kasy pod koniec dnia. Informacja o liczbie klientów odwiedzających sklep lub choćby podziwiających wystawy jest zbyt cenna, i to dosłownie, by stosować tę niedokładną miarę.

Monika Żuber-Mamakis

Obecnie firmy chętnie korzystają z systemów pozwalających na precyzyjne liczenie ludzi pojawiających się w centrach handlowych, biurowcach, halach targowych itp. Każda taka osoba, nawet jeśli należy do mało popularnej kategorii wizytujących, lecz nie kupujących, jest przecież potencjalnym nabywcą.

Informacja o liczbie wizytujących to coś więcej niż tylko określenie, ile osób odwiedziło jakieś miejsce. To wiedza pozwalająca określić częstotliwość odwiedzin, sprawdzić, jakie są wzorce zakupowe klientów, ułatwiająca określenie skuteczności kampanii marketingowej. Dzięki systemom liczącym firmy, szczególnie te z sektora handlu detalicznego, mogą zoptymalizować ułożenie towaru na półkach, modyfikować decyzje dotyczące zatowarowania, dostosować grafik pracowników. Innymi słowy, zwiększyć przychody. Równie ważne jest to, że szczególnie w sklepach wielkopowierzchniowych i galeriach handlowych dokładna znajomość liczby obecnych w nich ludzi służy zapewnieniu im bezpieczeństwa. Łatwiejsza jest ewakuacja, gdy po pierwsze, wiadomo, ile osób było w środku, a po drugie, czy wszyscy wyszli.

Liczenie osób może się odbywać na dwa sposoby. Jednym z nich jest zastosowanie specjalnych urządzeń elektronicznych (np. czujników, a nawet radarów) przeznaczonych wyłącznie do tego celu. Drugim wykorzystanie funkcji oprogramowania służącego do obsługi systemów zabezpieczeń funkcjonujących w budynku. Przy czym od strony fizycznej różne są sposoby realizacji tego zadania. Może być to wiązka podczerwieni, obrazowanie termiczne, sygnały wizyjne albo nawet maty wykrywające nacisk. Bardzo często do liczenia osób są też wykorzystywane kamery dozoru wizyjnego.

Jak wyjaśnia Bogumił Szymanek, Axis Communications, *kamery wykorzystują zaawansowane algorytmy analizy obrazu pozwalające na dokładne policzenie osób wchodzących i wychodzących z określonych obszarów. Przy czym kamery dwusensorowe mogą uzyskać widok 3D i dzięki temu dokonują analizy głębi obrazu, co zwiększa precyzję liczenia, eliminując błędy związane z refleksami, cieniami i zmianą oświetlenia.*

Pracę kamer ułatwia oczywiście sztuczna inteligencja. Według Marcina Walczuka z BCS, dzięki zastosowaniu AI w kamerach IP urządzenia te uzyskują 98% dokładność, jeśli chodzi o rozpoznawanie ludzkiej sylwetki. Z równą precyzją alarmują, gdy osoba niepowołana przekroczy granicę wyznaczonej strefy. I jak podkreśla M. Walczuk: *Im skuteczniejsze rozpoznawanie sylwetki, czyli „mądrzejsze" AI, tym lepszą skuteczność samego liczenia jesteśmy w stanie uzyskać.*

Bogumił Szymanek zauważa też, że *ostatnie lata zaowocowały wzrostem możliwości analizy obrazu opartej na głębokim uczeniu, dzięki czemu możliwe jest liczenie osób przebywających w polu widzenia kamery lub przekraczających wirtualną linię. Całość przetwarzania odbywa się w kamerze i nie ma potrzeby stosowania serwerów, co pozwala na optymalizację kosztów zakupu i utrzymania.*

Finansowy zysk, będący skutkiem całkiem nieubocznym, z zastosowania liczenia osób ma z pewnością niebagatelny wpływ na wzrost zainteresowania systemami oferującymi tę możliwość. Druga strona medalu jest jednak taka, że liczenie osób bazujące na monitoringu wizyjnym otwartym pozostawia pytanie o ochronę prywatności liczonych. Ta obawa oraz rozwój branży e-commerce nieco ograniczają popyt na systemy liczące. Niezależnie jednak od tego, według najnowszego badania firmy MarketsandMarkets, globalny rynek systemów do liczenia osób na koniec 2024 r. ma osiągnąć wartość 1 196,9 mln USD, w do roku 2029 r. ma być to 2 070,0 mld USD, przy CAGR na poziomie 11,6%.

## Pasażerów potok czy tylko strużka?

Wprawdzie to firmy handlowe są tymi, które z oczywistych powodów najchętniej stosują systemy liczące, to nie wolno zapominać, że są one również przydatne w transporcie, szczególnie publicznym. Na ten aspekt zwraca uwagę Marcin Trzmiel, Senior Business Development Manager Transportation z Vivotek: *W transporcie publicznym dane dotyczące liczby osób z nich korzystających (tzw. potoków pasażerskich) są od dawna zbierane za pomocą różnych technologii (systemy biletowe, automatyczne systemy zliczania, dane z telefonów komórkowych), badań ankietowych i zliczania manualnego. Pozyskane w ten sposób informacje służą do optymalizacji rozkładów jazdy, planowania nowych linii i tras, rozliczeń operatora transportu z odbiorcą usługi itp. Kamery monitoringu wizyjnego, które teraz są standardowym wyposażeniem pojazdów transportu publicznego, oprócz swojej podstawowej funkcji (ochrona mienia i zwiększanie poczucia bezpieczeństwa pasażerów) dostarczają dodatkowych danych dotyczących np. liczby pasażerów korzystających z wózków inwalidzkich czy podróżujących z większym bagażem.*

Każdy, kto listopadową porą korzysta z autobusu miejskiego, a ten przyjeżdża na czas, powinien zatem z wdzięcznością pomyśleć o systemach liczących. To m.in. dzięki nim nie trzeba marznąć na przystanku i podróżować w zatłoczonym autobusie.

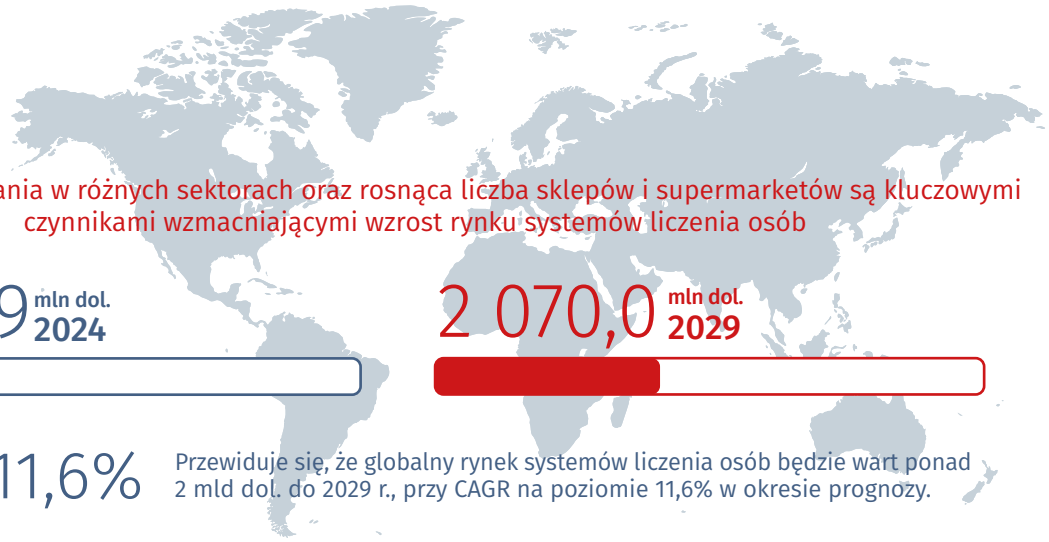
## Kto liczy najszybciej?

Najszybciej rozwijają się rynki Azji i Pacyfiku ze względu na rosnące gospodarki i pojawiające się możliwości w różnych sektorach, takich jak handel detaliczny, transport i hotelarstwo. Wzrost można również przypisać rosnącemu rozmieszczeniu średnich i dużych sklepów stacjonarnych, rosnącym możliwościom płynącym z rynków wschodzących w Chinach i Indiach oraz coraz większej populacji w regionie.

Natomiast największy udział w światowym rynku systemów liczenia osób w 2024 r. będzie miała Ameryka Północna. W tym przypadku głównym powodem jest obecność dużej liczby centrów handlowych i sklepów detalicznych oraz wczesne przyjęcie technologii liczenia odwiedzających i śledzenia natężenia ruchu w miejscach publicznych.

W Europie krajami o największej liczbie wdrożonych systemów są Niemcy, Francja i Wielka Brytania. Urządzenia służące do liczenia liczby osób odwiedzających stosowane są głównie w handlu, transporcie i dużych przedsiębiorstwach.

→



Nowe zastosowania w różnych sektorach oraz rosnąca liczba sklepów i supermarketów są kluczowymi czynnikami wzmacniającymi wzrost rynku systemów liczenia osób

**1 196,9** mln dol. **2024**

**2 070,0** mln dol. **2029**

**CAGR 11,6%** Przewiduje się, że globalny rynek systemów liczenia osób będzie wart ponad 2 mld dol. do 2029 r., przy CAGR na poziomie 11,6% w okresie prognozy.

Rosnąca troska o bezpieczeństwo i ochronę ludzi w miejscach publicznych jest odpowiedzialna za zwiększenie zapotrzebowania na systemy liczenia osób.

Oczekuje się, że wprowadzanie na rynek i rozwój produktów stworzy lukratywne możliwości rozwoju dla graczy rynkowych w ciągu najbliższych pięciu lat.

Wiele wskazuje, że w 2024 r. segment oparty na monitoringu wizyjnym będzie miał największy udział w systemie zliczania osób (48,8%).

Większe zastosowanie technologii, takich jak marketing cyfrowy, liczenie osób, sprzedaż wielokanałowa i sztuczna inteligencja w sklepach stacjonarnych i centrach handlowych, będzie wspierać wzrost rynku.

Źródło: Secondary Research, Industry Journals, Interviews with Experts, and MarketsandMarkets Analysis

*» Największym wyzwaniem wydaje się efektywne wykorzystanie zgromadzonych danych. Kluczowe jest opracowanie strategii ich analizy w celu osiągnięcia wymiernych korzyści, takich jak poprawa jakości obsługi, zwiększenie liczby klientów oraz, co najważniejsze, wzrost sprzedaży. «*

## Klient jest zadowolony

To zrozumiałe, że systemy liczenia osób są najchętniej stosowane w sklepach, hotelach, bankach, na stadionach i w szpitalach. Coraz częściej korzystają z nich również muzea i parki. Systemy zliczania osób pomagają firmom w płynnym prowadzeniu działalności dzięki optymalnemu wykorzystaniu personelu i przestrzeni fizycznej. Istnieją już funkcje, które umożliwiają użytkownikom połączenie konta Google Analytics z własnym oprogramowaniem, pozwalając przy tym na porównanie ruchu na stronie internetowej z odwiedzinami w sklepach stacjonarnych.

Na pytanie, czego zatem w przyszłości można się spodziewać po systemach liczenia ludzi, odpowiedział nam m.in. Karol Radzajewski, Project Manager Retail & Logistics Technology Solutions Department z Hikvision. W jego ocenie *liczenie osób już jest jedną ze sprawnie prowadzonych analityk. Najbardziej znanym rozwiązaniem wykorzystującym kamery dwuobiektywowe, które umożliwiają przetwarzanie obrazu 3D, jest system pozwalający na szacowanie wzrostu osób (pozwala nam to odfiltrowywać np. dzieci). Co istotne, rozwiązanie to jest odporne na błędy w zliczaniu w sytuacjach, gdy przez przejście jednocześnie przechodzi wiele osób, które mogą się wzajemnie zasłaniać. Pod tym względem można uznać, że firmy oferujące takie rozwiązania spełniają oczekiwania klientów, rezultaty pracy takich systemów są bowiem więcej niż zadowalające* – wyjaśnia. Co nie zmienia faktu, że, jak podkreśla, największym wyzwaniem wydaje się efektywne wykorzystanie zgromadzonych danych. Kluczowe jest opracowanie strategii ich analizy w celu osiągnięcia wymiernych korzyści, takich jak poprawa jakości obsługi, zwiększenie liczby klientów oraz, co najważniejsze, wzrost sprzedaży.

Chodzi bowiem nie tylko o to, by liczyć, ale by liczyć mądrze. I z tego wyciągać wnioski. ●

# Monitoring wizyjny w nowoczesnym handlu

**Monitoring wizyjny w sklepach i centrach handlowych jest czymś więcej niż tylko narzędziem ochrony. Obecnie jest kluczem do poprawy bezpieczeństwa, analityki i jakości obsługi.**

Systemy monitoringu wizyjnego ewoluowały w wielofunkcyjne platformy, które dbają o bezpieczeństwo i jednocześnie ułatwiają zarządzanie obiektem, wpływają na poprawę doświadczenia klienta i optymalizują procesy sprzedażowe.

## Monitoring wizyjny jako narzędzie analityczne

Nowoczesne systemy monitoringu wizyjnego są wyposażone w zaawansowaną analitykę, która umożliwia analizowanie zachowań klientów, tego jak długo klient zatrzymuje się w określonych miejscach, co pozwala na lepsze rozłożenie towaru w sklepie, a tym samym zwiększenie efektywności sprzedaży.

– *Analiza wspiera zarządzanie ruchem klientów, w tym rozładowywanie kolejek w godzinach szczytu* – mówi Grzegorz Wojtasik, wiceprezes PZP Ochrona. – *Systemy automatycznie powiadamiają personel o konieczności uruchomienia kolejnej kasy, co jest szczególnie ważne w okresach wzmożonego ruchu, takich jak weekendy czy święta.*

## Bezpieczeństwo na pierwszym miejscu

Podstawowym zadaniem monitoringu wizyjnego jest zapewnienie bezpieczeństwa. Nowoczesne systemy monitoringu oferują funkcje detekcji zdarzeń, takich jak upadki osób, przebywanie klientów w niedozwolonych miejscach czy gromadzenie się wielu osób np. w wąskim korytarzu. Dzięki temu możliwe jest zapobieganie aktom wandalizmu, blokowaniu wyjść ewakuacyjnych czy innym zagrożeniom.

## Monitoring jako wsparcie jakości obsługi

Systemy monitoringu wizyjnego znajdują zastosowanie także w obszarze kontroli jakości obsługi klienta. – *Dzięki integracji z analityką mogą ułatwiać nadzór nad przestrzeganiem standardów przez personel, weryfikować uniformy pracowników, obecność logotypów marki czy liczbę aktywnych kas. Ponadto umożliwiają audyty zdalne, np. weryfikację procesu przyjmowania dostaw czy rozmieszczania produktów w przestrzeni sklepowej* – wskazuje G. Wojtasik.

Monitoring może być również stosowany do kontroli sposobu prezentacji produktów, co jest szczególnie ważne w sklepach odzieżowych i sieciach handlowych, gdzie kluczowa jest dbałość o estetykę ekspozycji.

## Rola ochrony fizycznej w dobie zaawansowanych technologii

Chociaż nowoczesne systemy monitoringu znacząco wspierają ochronę obiektów handlowych, fizyczna obecność pracowników ochrony jest nadal kluczowa. W mniejszych placówkach obserwuje się redukcję zatrudnienia ochrony fizycznej na rzecz rozbudowy systemów technologicznych. W takich przypadkach ochrona skupia się na działaniach interwencyjnych.

Warto pamiętać, że każdy system monitoringu pełni funkcję prewencyjną – obecność kamer działa odstraszająco na potencjalnych sprawców przestępstw. Wiele sklepów wprowadza dodatkowe środki bezpieczeństwa, takie jak oznakowanie produktów systemami antykradzieżowymi.

Nowoczesne systemy monitoringu wizyjnego integrują funkcje ochrony i zarządzania obiektem. Umożliwiają nie tylko rejestrowanie incydentów, ale także analizę przepływu klientów czy tworzenie „map ciepła". Dane te są nieocenione dla zarządców obiektów handlowych, pomagając w tworzeniu ofert dla najemców czy planowaniu procesów merchandisingowych. – *Sprawne funkcjonowanie systemów monitoringu wymaga regularnego serwisowania i integracji z centrami zarządzania operacyjnego. To pozwala szybko reagować na zagrożenia i koordynować działania w sytuacjach awaryjnych* – podsumowuje G. Wojtasik.

Monitoring wizyjny staje się filarem nowoczesnego handlu. Jego wszechstronność – od zapewniania bezpieczeństwa, przez optymalizację sprzedaży, aż po kontrolę jakości obsługi – sprawia, że inwestycja w zaawansowane systemy jest niezbędna dla skutecznego zarządzania obiektami handlowymi. Połączenie technologii z ochroną fizyczną tworzy kompleksowy system, który pozwala na zwiększenie efektywności operacyjnej i poprawę doświadczenia klienta. ●

**Polski Związek Pracodawców Ochrona**
ul. Koszykowa 61, 00-667 Warszawa
www.pzpochrona.pl
biuro@pzpochrona.pl

# głos branży

Bezpieczeństwo w handlu detalicznym odgrywa kluczową rolę w ochronie zarówno klientów, jak i personelu, a także w zapobieganiu stratom finansowym. Eksperci branżowi podkreślają, że skuteczne systemy zabezpieczeń nie tylko minimalizują ryzyko kradzieży, ale również budują zaufanie klientów i wzmacniają wizerunek sklepu.

Adam Suliga
EKSPERT POLSKIEJ IZBY HANDLU

## Minimalizacja ryzyka kradzieży

Niezmiennie od wielu lat zarządzający placówkami handlowymi zrzeszonymi w Polskiej Izbie Handlu podejmują szereg działań, które mają na celu zminimalizowanie ryzyka kradzieży. W obszarze tzw. Triady Bezpieczeństwa wyróżniamy te, które najskuteczniej ograniczają niepożądane skutki tych zdarzeń:

- zabezpieczenia techniczne,
- ochronę fizyczną,
- procedury.

Kluczowym elementem jest monitoring wizyjny (kamery CCTV), który pozwala na bieżąco kontrolować zachowanie klientów i pracowników, a także zbierać dowody w razie potrzeby. Kolejnym działaniem jest szkolenie pracowników w zakresie rozpoznawania podejrzanych zachowań, co pozwala im skutecznie reagować w sytuacjach zagrożenia. Wdrażane procedury obejmują zarówno aspekty organizacyjne, jak i techniczne oraz opisują sposoby postępowania w sytuacjach zagrożenia. Ponadto wprowadzane są rozwiązania technologiczne typu RFID *(Radio Frequency Identification)*, które pozwalają na identyfikację towarów i zapobiegają ich kradzieży, a także wykrywają nieopłacone towary przy kasach. Działania te są wspierane przez kontrolę dostępu do pomieszczeń magazynowych czy biurowych. Ważnym aspektem jest także organizacja pracy personelu w taki sposób, aby obecność pracowników w sali sprzedaży była widoczna i utrzymywała porządek w sklepie, co działa prewencyjnie.

Obecnie w wielu placówkach handlowych inwestuje się przede wszystkim w systemy zabezpieczeń technicznych, ponieważ oferują

one większą efektywność w prewencji i reakcji na kradzież. Technologie takie jak monitoring CCTV, systemy alarmowe, kontrola dostępu czy czytniki RFID pozwalają na stałe monitorowanie i analizowanie sytuacji w sklepie, co zmniejsza potrzebę fizycznej obecności ochrony. Dzięki nowoczesnym systemom możliwa jest szybka reakcja na incydenty, a także zbieranie dowodów w przypadku wykrycia kradzieży.

Jednocześnie ochrona fizyczna nadal odgrywa ważną rolę, zwłaszcza w placówkach o dużym natężeniu ruchu lub w miejscach, gdzie kradzieże mogą być szczególnie uciążliwe (placówki z towarami o szczególnie wysokiej wartości). Choć jej koszt jest wyższy, często uzupełnia ją zaawansowana technologia, tworząc kompleksowy system zabezpieczeń. Współczesne podejście zakłada zatem równowagę pomiędzy inwestycjami w technologie, nieustannym dostosowywaniem procedur do istniejących warunków i obecnością ochrony fizycznej przy uwzględnieniu specyfiki placówki i poziomu ryzyka.

Czy bez przeszkolenia personelu warto montować bramki antykradzieżowe, skoro pracownicy lekceważą lub nie znają procedur? Czy ma uzasadnienie montaż słabej jakości kamer, z których nikt nie weryfikuje nagrań? Mogłoby się wydawać, że jest to odpowiedź na pytanie, czy zarządzający placówkami powinni inwestować więcej w systemy zabezpieczeń technicznych, czy w ochronę fizyczną? Odpowiedź nie jest jednoznaczna. Informację, jak zabezpieczyć daną placówkę handlową, uzyskamy, analizując zagrożenia występujące w danej lokalizacji. W bezpiecznej dzielnicy wystarczą szkolenia personelu i systemy antykradzieżowe, lecz na obszarach o zwiększonej liczbie zdarzeń konieczne będzie dodatkowo okresowe lub stałe korzystanie z ochrony fizycznej.

Długookresowo, w mojej opinii, dzięki sztucznej inteligencji zabezpieczenia techniczne zyskają dominującą rolę w walce ze złodziejami. Musimy zdawać sobie jednak sprawę, że przed nami jeszcze sporo wyzwań natury prawnej i organizacyjnej, aby móc w pełni wykorzystać możliwości systemów zabezpieczeń technicznych w połączeniu z AI.

Robert Kujawa
RETAILSECURITYACADEMY.PL

## Kluczowe działania

Analizując sytuację związaną z kradzieżami, łatwo dostrzec, że znaczna ich część nie jest odnotowywana w żadnych statystykach. Z danych policji wynika, że w rekordowym pod względem kradzieży roku 2023 zgłaszany był co dziesiąty przypadek. Obecnie, opierając się na doświadczeniach moich klientów, mogę stwierdzić, że wskaźnik kradzieży wygląda znacznie gorzej. Jakie działania podjąć, aby zminimalizować ryzyko kradzieży?

Po pierwsze, nie wystarczy kilka zdań w czasie pierwszego dnia pracy i odesłanie pracownika do procedur (jeśli istnieją). Szkolenie pracowników z zagadnień związanych z kradzieżami to inwestycja nie tylko w bezpieczeństwo, ale także w ich zdrowie i być może życie. Po drugie, należy dopracować współpracę placówki handlowej z ochroną obiektu co do działań zarówno w obszarze sklepu, jak i poza nim. Kolejnym ważnym aspektem jest znalezienie złotego środka pomiędzy zadaniami procesowymi realizowanymi przez pracowników a rolą sprzedawcy – doradcy, który jest w stanie obserwować newralgiczne strefy sklepu, np. strefa wejścia–wyjścia. Zalecam także włączenie w tematykę kradzieży działów VM w celu znalezienia kompromisowego rozwiązania pomiędzy minimalizowaniem strat a wzrostem sprzedaży.

Na koniec warto wspomnieć o polityce bezpieczeństwa. Mając na uwadze rosnące koszty osobowe, ale także koszty zabezpieczeń, należy przeanalizować obszary i towary, które musimy szczególnie chronić. Powinniśmy skupić się na zasadności ponoszonych wydatków, bo ilość nie zawsze oznacza jakość. Warto się zastanowić, jakie zabezpieczenia w danej placówce odegrają swoją rolę.

Wojciech Kawa
EKSPERT DS. BEZPIECZEŃSTWA

## Złapać złodzieja!

Obecnie w zabezpieczaniu handlu przed działaniami przestępczymi trwa swoisty wyścig zbrojeń. Zawołanie „Łap złodzieja!" nabiera nowego znaczenia. Najczęściej dokonuje się kradzieży/wykroczeń i przestępstw. Często zdarzają się też oszustwa tzw. przemetkowań, traktowane ostatnio jako wykroczenie kradzieży lub przestępstwo kradzieży. Dodatkowo obiekty handlowe są zagrożone kradzieżami z włamaniem lub kradzieżami zuchwałymi, kradzieżami rozbójniczymi.

Z najnowszych danych Komendy Głównej Policji wynika, że liczba kradzieży w sklepach znacząco spadła w pierwszych trzech kwartałach 2024 r. Statystyki mogą jednak ulec zmianie wraz z nadejściem okresu przedświątecznego, który tradycyjnie przynosi wzrost incydentów kradzieży. Straty powstałe wskutek kradzieży z włamaniem nie kończą się na wyniesionych przez złodziei przedmiotach. Równie kosztowne potrafią być zniszczenia powstałe w czasie nielegalnego wejścia do biura, magazynu, sklepu, np. uszkodzone drzwi, sprzęty wewnątrz, zniszczona instalacja elektryczna, infrastruktura informatyczna. Ubezpieczenie co prawda nie uchroni przed włamaniem, ale zapewni finansową pomoc po szkodzie.

Zabezpieczenie firmy przed kradzieżą z włamaniem wymaga zrównoważonego podejścia, które obejmuje zarówno środki techniczne, jak i procedury operacyjne. Inwestycja w systemy monitoringu, alarmowe oraz oświetlenie zewnętrzne może zapewnić dodatkową warstwę ochrony dla biznesu. Warto również regularnie przeglądać i aktualizować zabezpieczenia, aby dostosować się do zmieniających się potrzeb i zagrożeń.

Człowiek jest najsłabszym ogniwem w całym systemie bezpieczeństwa, ale trzeba też pamiętać, że technologie nie zawsze zastępują, ale często uzupełniają tradycyjne usługi ochrony fizycznej, tworząc bardziej skuteczne i zintegrowane systemy bezpieczeństwa. Ostatecznym czynnikiem ochrony, przynajmniej na razie, pozostaje człowiek i jego decyzje.

Grunt to doskonale przeszkolony i zmotywowany do pracy zespół ochrony, który wnikliwie oraz przy wsparciu odpowiednich narzędzi technicznych, takich jak inteligentna analityka obrazu, obserwuje otoczenie i natychmiast reaguje na zdarzenia oraz współpracuje przy tym z centrum monitoringu.

Podsumowując, zapewnienie bezpieczeństwa obiektów handlowych to proces złożony, który wymaga starannej analizy, zastosowania odpowiednich środków ochrony oraz wdrożenia dobrych praktyk. Systematyczne monitorowanie i doskonalenie działań w zakresie bezpieczeństwa są kluczowe dla skutecznego zapobiegania stratom wynikającym z kradzieży.

Michał Badke
EKSPERT DS. BEZPIECZEŃSTWA

## Zapobieganie stratom

Pomimo stale rosnącego udziału e-commerce w handlu detalicznym sprzedaż bezpośrednia zarówno w obszarze produktów i usług luksusowych, jak i artykułów pierwszej potrzeby nadal odgrywa istotną rolę. Skuteczne zapewnienie bezpieczeństwa klientom i pracownikom oraz unikanie strat w tym sektorze było i będzie sporym wyzwaniem. Nieodzowne jest tu holistyczne, przemyślane i praktyczne podejście osób odpowiedzialnych, ponieważ właściwe określanie aktualnych ryzyk oraz dobieranie i wdrażanie skutecznych metod zapobiegania im gwarantuje bezpieczeństwo.

Należy przy tym pamiętać, aby metody te jednocześnie:

- nie wpływały negatywnie na odczucia konsumenta (w konsekwencji zrażając go do marki),
- nie nadwyrężały bilansu finansowego biznesu poprzez nadmierne „zbrojenia",
- były zrozumiałe dla personelu, a przy tym nie generowały dodatkowego obciążenia nowymi procedurami.

Także skokowy rozwój technologii, którego doświadczamy, stawia przed branżą nieznane wcześniej wyzwania. Na szczęście, w ramach wyścigu miecza i tarczy ta zmienna może wydatnie przysłużyć się podniesieniu bezpieczeństwa i ułatwić zapobieganie stratom. Oparte na AI rozwiązania pozwalają dziś na automatyzację wielu procesów – to wręcz generacyjna zmiana jakości i skuteczności pozyskiwania oraz obróbki danych operacyjnych! A – co każdy specjalista od *loss prevention* potwierdzi bez wahania – uwielbiamy dane! To one bowiem pozwalają nam ustalić oraz zrozumieć źródła i przyczyny powstawania strat, a to pierwszy krok do ich ograniczenia. Sowicie „nakarmione" danymi systemy pozwalają nam dziś na szczegółową analizę tysięcy parametrów, które jeszcze kilka lat temu „ginęły w tłumie" jako *grey data*.

To już nie tylko usprawnienie klasycznego monitoringu poprzez wykrywanie nietypowych zachowań konsumentów w sali sprzedaży lub pracowników magazynu, ale również precyzyjne śledzenie przepływu i monitorowanie stanu zasobów dzięki malejącym kosztom i rosnącej popularności rozwiązań opartych choćby na RFID czy termowizji.

Bogumił Szymanek
AXIS COMMUNICATIONS

## Bezpieczeństwo i komfort dzięki kamerom

Kamery wspierające bezpieczeństwo sklepów odgrywają kluczową rolę w ochronie towarów, personelu oraz klientów. Dzięki zaawansowanej technologii monitoringu możliwe jest skuteczne zapobieganie kradzieżom oraz szybkie reagowanie na wszelkie incydenty. Kamery pozwalają na stałe monitorowanie przestrzeni sklepowej, co zwiększa poczucie bezpieczeństwa zarówno wśród pracowników, jak i klientów. Ponadto nagrania z kamer mogą być wykorzystywane jako dowody w przypadku dochodzeń, co ułatwia identyfikację sprawców i rozwiązywanie sporów.

Obecne urządzenia mogą być zintegrowane i wyposażone w inteligentne algorytmy, które wykryją zdarzenia potencjalnie niebezpieczne, np. nieautoryzowane otwarcie drzwi, wejście pod prąd, podejrzanie długie przebywanie w określonym miejscu. Pomocne okaże się też wykrywanie krzyku lub hałasu realizowane za pomocą Axis Audio Analytics, które przy zachowaniu zasad zachowania prywatności (bez rejestracji dźwięku) wygeneruje alarm dla ochrony o niebezpiecznym zdarzeniu.

Pracownicy handlu detalicznego często są również ofiarami agresywnego zachowania klientów, zatem docenią możliwość noszenia kamery na sobie. Takie urządzenie, widoczne dla innych, zmniejsza prawdopodobieństwo agresywnych zachowań. Natomiast gdy już dojdzie do sytuacji konfliktowej, stanowi doskonałe źródło obiektywnego materiału dowodowego. Pomimo realizowania wielu zaawansowanych funkcji obsługa systemu nie powinna być skomplikowana i do tego w Axis dążymy, oferując system zarządzania materiałem wizyjnym oraz kontroli dostępu Axis Camera Station. W efekcie systemy monitoringu wizyjnego przyczyniają się do poprawy ogólnego bezpieczeństwa i komfortu w sklepach.

Marcin Walczuk
BCS

# Zabezpieczenie branży handlowej

Zabezpieczenie obiektów handlowych, począwszy od małych sklepów po ogromne centra handlowe, już dawno przestało opierać się na prostym systemie alarmowym czy systemie telewizji dozorowej. Niejednokrotnie, a w przypadku dużych obiektów praktycznie zawsze, są to wysoce skomplikowane centralnie zarządzane systemy zabezpieczenia obiektu, w których skład, obok wspomnianych systemów SSWiN i CCTV, wchodzą również systemy przeciwpożarowe czy kontroli dostępu.

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

Wykorzystanie różnych funkcji zaawansowanej analizy wideo pozwala znacząco ograniczyć liczbę fałszywych alarmów i reagować na sytuacje, które faktycznie mogą stanowić zagrożenia. Funkcja wykrywania pozostawionych obiektów pomoże odpowiednio szybko namierzyć taki przedmiot i podjąć wobec niego odpowiednie działania. Dzięki skróceniu czasu reakcji zwiększa się również szansa na odnalezienie osoby odpowiedzialnej za całe zdarzenie. Z kolei funkcja monitorowania zachowania tłumu czy poszczególnych osób pozwoli zapobiec panice bądź wychwycić z otoczenia osoby zachowujące się w sposób podejrzany.

O ile bezpieczeństwo jest najważniejsze, o tyle nowoczesny system CCTV może już służyć nie tylko do zabezpieczenia obiektu. Zaczyna stanowić coraz potężniejsze narzędzie analityczne, które szczególnie w handlu może podnieść skuteczność sprzedaży. Dane spływające z kamer w postaci map cieplnych, obrazujące największy ruch, pozwoli w lepszy sposób pozycjonować produkty, na których sprzedaży klientom najbardziej zależy. Raporty z kamer zliczających ludzi dają informacje, ile osób odwiedziło sklep, które można powiązać np. z liczbą wystawionych paragonów w danym okresie. Metadane, które pozyskujemy z kamer identyfikujących twarze czy inteligentnych rejestratorów, określające płeć, przedział wiekowy czy nastrój, pozwolą lepiej ukierunkować działania marketingowe skierowane do docelowej grupy odbiorców.

Jasno pokazuje to, że rozwój technologii zabezpieczeń jest ściśle powiązany z sektorem handlowym. Z jednej strony należy zapewnić bezpieczeństwo i to w dalszym ciągu powinien być cel nadrzędny każdego systemu, z drugiej – nowoczesne rozwiązania pozwalają na zwiększenie przychodów. Dlatego m.in. BCS, jako wiodąca marka rozwiań security w Polsce, blisko współpracuje z odbiorcami końcowymi, którymi są największe sieci handlowe w naszym kraju.

Armen Moska
HIKVISION

# Analityka wizyjna nie tylko do zabezpieczeń

Sklepy detaliczne w dzisiejszych czasach stają przed wieloma wyzwaniami, które zmieniają się bardzo dynamicznie. Coraz trudniej jest im utrzymać stabilną rentowność, w czym z pewnością nie pomagają straty powodowane przez kradzieże, stosunkowo wysoka inflacja i ciągła pogoń za zmieniającymi się upodobaniami klientów.

W mojej opinii wiele mogłoby w tym obszarze zmienić szersze zastosowanie możliwości, jakie daje analityka wizyjna w sklepach. Temat ten jest ciągle jeszcze bardzo mało wyeksploatowany. Dzięki analityce sklepy mogłoby otworzyć sobie drogę do pozyskiwania bardzo dużej wartości dodanej wynikającej wprost z konkretnych informacji analitycznych. Pozyskane dane można z łatwością wykorzystać do zwiększania współczynnika konwersji, wzmocnienia merchandisingu i optymalizacji pracy całej placówki.

Przez wiele lat systemy monitoringu wizyjnego były traktowane wyłącznie jako elementy systemów zabezpieczeń i kojarzyły się w głównej mierze z czynnikiem kosztowym. To koszt, który trzeba było ponieść, ale najlepiej, żeby był on jak najniższy. Tymczasem dziś analityka wizyjna to tanie i skuteczne maszynki do generowania konkretnych i mierzalnych zysków. Wystarczy otworzyć się na nowe możliwości i poszukać nowych wartości tam, gdzie nikt ich do tej pory nie szukał, w ten sposób spowodować, by dotychczasowy system zapobiegania stratom stał się równocześnie generatorem przychodów.

Cieszę się, że coraz więcej dużych sieci handlowych inwestuje w podobne rozwiązania, przyczynia się to bowiem do dynamicznego rozwoju całej branży w tym obszarze. I oby tak dalej. ●

# Rozwiązania Synology Surveillance Solutions dla firmy Q-Park

Firma Q-Park, jeden z największych dostawców usług parkingowych w Europie, uznała, że nadszedł czas na zmodernizowanie systemu swojego monitoringu. Wyzwaniem było znalezienie łatwego w zarządzaniu, przyszłościowego systemu monitoringu. Sprostało mu rozwiązanie Synology Surveillance Solutions.

Starsze urządzenia zabezpieczające stosowane przez Q-Park osiągnęły kres swojej żywotności, czego wyraźnie dowiodły m.in. częste przestoje podczas aktualizacji oprogramowania. Dodatkowym problemem był brak wsparcia dla Windows 7, co wiązało się z ryzykiem bezpieczeństwa i uniemożliwiało pełną ochronę danych i monitoring parkingów.

Poprzedni system, choć spełniał swoje funkcje, nie umożliwiał redundancji dysków i zasilania. Oznaczało to, że w przypadku awarii urządzenia Q-Park był narażony na utratę cennych danych, a brak odpowiedniej konfiguracji zasilaczy zapasowych groził przerwami w działaniu systemu w wyniku awarii prądu. Q-Park stanął przed potrzebą wdrożenia nowoczesnego, niezawodnego i łatwego w zarządzaniu rozwiązania. Wybór padł na Synology.

## Nieprzerwane działanie i przechowywanie danych

Firma Q-Park, po dokładnym sprawdzeniu możliwości oferowanych przez Synology Surveillance Station, uznała, że to właśnie ten system może sprostać wymaganiom. W centrali firmy w Leeds w Wielkiej Brytanii zainstalowano jednostkę centralną RackStation, która stała się hostem dla lokalnych serwerów monitoringu. System wdrażano stopniowo na poszczególnych parkingach, rozbudowując go o kolejne serwery RackStation z Surveillance Station, aż do osiągnięcia liczby 2000 kamer w różnych lokalizacjach.

Jednym z kluczowych elementów, który wyróżniał Synology, było stosowanie podwójnych zasilaczy gwarantujące nieprzerwane działanie systemu. Dzięki temu ryzyko zakłóceń w monitoringu spowodowanych awarią zasilacza lub przypadkowym odłączeniem energii zostało skutecznie wyeliminowane. To innowacyjne rozwiązanie pozwala Q-Park na utrzymanie wysokiej niezawodności systemu, co jest szczególnie istotne w miejscach o dużym natężeniu ruchu i wymagających ciągłego monitoringu.

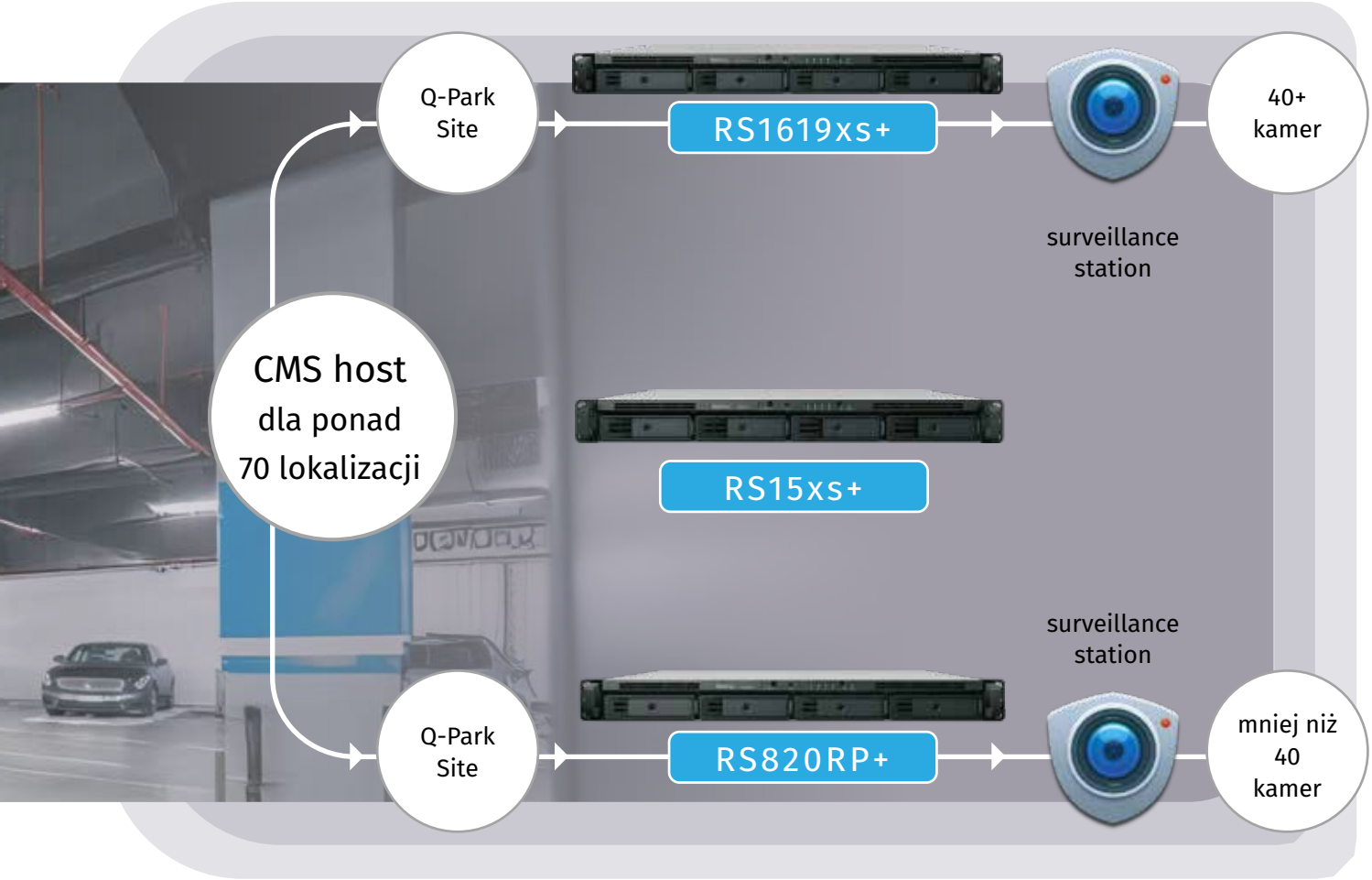
Konfiguracja RAID zastosowana w urządzeniach Synology to kolejny aspekt, który przyciągnął uwagę Q-Park. Redundancja dysków zapewnia dostępność kopii zapasowych, co jest kluczowe w przypadku awarii któregoś z dysków. Dzięki zastosowaniu tej technologii Q-Park może być pewny, że uszkodzenie pojedynczego dysku nie spowoduje utraty danych. To dodatkowe zabezpieczenie pozwala na nieprzerwaną pracę systemu i zwiększa jego ogólną niezawodność.

Ponadto wykorzystano specjalistyczne dyski z serii HAT3000 Plus, które zapewniają jeszcze większą niezawodność przechowywania danych. W sytuacjach awaryjnych Synology może szybko autoryzować wymianę dysku, minimalizując czas przestoju i ograniczając ryzyko utraty danych. Dzięki temu firma Q-Park zyskała większą pewność w zakresie bezpieczeństwa przechowywanych nagrań, co bezpośrednio wpływa na poprawę jakości usług oferowanych klientom.

## Centralizacja zarządzania systemem

Synology oferuje zaawansowany Centralny System Zarządzania (CMS) ułatwiający zarządzanie rozbudowaną infrastrukturą monitoringu. Dzięki niemu zespoły zarządzające mogą nadzorować wszystkie serwery monitoringu z poziomu głównego hosta. Pracownicy Q-Park mają możliwość podglądu transmisji na żywo oraz archiwalnych nagrań z dowolnej lokalizacji, co znacząco podnosi jakość i wygodę monitoringu. W sytuacjach awaryjnych można szybko wdrożyć odpowiednie działania i ograniczyć potencjalne straty.

Zdalne zarządzanie jest szczególnie przydatne w sytuacjach, gdy konieczne jest szybkie zaktualizowanie oprogramowania układowego w celu poprawy zabezpieczeń. Dzięki CMS, Q-Park może w dowolnym momencie wdrażać aktualizacje na wielu urządzeniach jednocześnie, co znacząco skraca czas potrzebny na utrzymanie bezpieczeństwa systemu. Aplikacje mobilne na systemy iOS i Android ułatwiają




pracownikom Q-Park zdalne monitorowanie parkingów, nawet gdy są poza biurem. To nowoczesne rozwiązanie umożliwia podgląd na żywo z kamer, wysyłanie powiadomień e-mail oraz szybką reakcję w przypadku wykrycia incydentu. Dzięki tej funkcji Q-Park może skuteczniej zarządzać bezpieczeństwem obiektów oraz minimalizować ryzyko zdarzeń wymagających interwencji.

## Integracja kamer Synology ze sztuczną inteligencją

Kamery Synology BC500, które Q-Park wdrożył w swoich obiektach, zostały zintegrowane z systemem bez konieczności dodatkowych licencji. Wprowadzenie zaawansowanych funkcji opartych na sztucznej inteligencji, takich jak wykrywanie osób i pojazdów, znacząco zwiększa skuteczność monitoringu. Automatyczne wykrywanie zagrożeń i błyskawiczne wyszukiwanie nagrań pozwalają na szybsze reagowanie na potencjalne zagrożenia.

Dzięki kompatybilności z innymi systemami platforma Synology umożliwia Q-Park zintegrowanie monitoringu z rozwiązaniami dostarczonymi przez zewnętrznych dostawców, co zwiększa elastyczność systemu. Inteligentne funkcje AI pozwalają na skuteczniejszy nadzór nad parkingami i szybki dostęp do nagrań, znacząco wpływając na efektywność działania służb monitorujących.

## Niezawodny nadzór i zachowanie integralności danych

Aby zapewnić maksymalną dostępność systemu i pełną ciągłość działania monitoringu, Q-Park wdrożył klaster wysokiej dostępności (SHA) dla swoich serwerów hostujących CMS. Dzięki temu rozwiązaniu, w przypadku awarii serwera głównego, automatycznie aktywuje się serwer zapasowy, który przejmuje wszystkie funkcje monitoringu. To innowacyjne rozwiązanie eliminuje ryzyko przerw w nagrywaniu i zabezpiecza dane przechowywane w systemie. Implementacja SHA jest dowodem na zaangażowanie Q-Park w nieprzerwaną ochronę danych i zapewnienie pełnego bezpieczeństwa obiektów. Wprowadzenie tego rozwiązania podkreśla dążenie Q-Park do utrzymania najwyższych standardów bezpieczeństwa i jakości usług.

## Q-Park: lider nowoczesnych usług parkingowych

Q-Park, jako jeden z największych dostawców usług parkingowych w Europie, stawia na rozwiązania innowacyjne, które mają na celu zapewnienie komfortu i bezpieczeństwa swoim klientom. Firma została założona w 1998 r. w Holandii i od tego czasu rozszerzyła swoją działalność na 70 miast w siedmiu krajach, obsługując ponad 200 obiektów parkingowych, w tym ponad 70 w Wielkiej Brytanii.

Wyróżnikiem Q-Park na tle konkurencji jest dbałość o jakość życia miejskiego i odpowiedzialność społeczna. Firma inwestuje w nowoczesne technologie, które mają na celu poprawę doświadczeń użytkowników parkingów. Poza standardowymi usługami Q-Park oferuje także ładowanie pojazdów elektrycznych, możliwość rezerwacji miejsc online, a także dodatkowe udogodnienia, jak wypożyczanie parasoli czy wózków dziecięcych.

Firma Q-Park dzięki rozwiązaniom Synology Surveillance Solutions nie tylko zmodernizowała swoje podejście do monitoringu, ale także zyskała narzędzie do zarządzania bezpieczeństwem na najwyższym poziomie. Wysoka niezawodność systemu, redundancja zasilania i dysków oraz wsparcie techniczne Synology umożliwiają Q-Park oferowanie usług, które przekładają się na zadowolenie klientów i spokój właścicieli obiektów. ●

**Synology**
Grafenberger Allee 295,
40237 Düsseldorf, Niemcy
www.synology.com/pl-pl/


# Systemy parkingowe DSS Professional

**Oprogramowanie do zarządzania systemami dozoru wizyjnego już dawno przestało być wyłącznie elementem systemu bezpieczeństwa. Potrzeba integracji z innymi rozwiązaniami spowodowała, że obecnie umożliwia ono obsługę systemów alarmowych, systemów liczenia osób, kontrolę dostępu i wielu innych, w tym także systemów parkingowych.**

W ofercie Dahua Technology za obsługę parkingów odpowiada aplikacja serwerowa DSS Professional. Z poziomu jednej platformy operator może zarządzać wszystkimi urządzeniami zaangażowanymi w funkcjonowanie konkretnej przestrzeni, a także ich logicznymi powiązaniami. Łatwo konfigurowalna wizualizacja miejsc parkingowych, monitorowanie w czasie rzeczywistym ich obłożenia, wygodne wyszukiwanie pojazdów, kontrola wjazdów i wyjazdów na podstawie wcześniej zdefiniowanych list, statystyki czasu przebywania na parkingu, alerty powiązane z przedłużającym się pobytem i wiele więcej zaawansowanych funkcji pokazuje, jak bardzo elastyczne podejście do zarządzania przestrzenią parkingową proponuje DSS Professional.

Jednakże systemy z tej kategorii to nie tylko warstwa programowa. *Clou* każdej takiej instalacji stanowi zespół urządzeń odpowiedzialnych za wjazdy na parkingi i wyjazdy z nich, kontrolę obecności pojazdów na danych miejscach parkingowych oraz za bezpieczne, szybkie i ukierunkowane przemieszczanie się pojazdów w celu możliwie bezproblemowego dostania się do danego miejsca.

**Z tego też względu w ofercie Dahua Technology znalazły się:**

- kamery ANPR pozwalające na błyskawiczne odczytywanie numerów rejestracyjnych oraz cech danego pojazdu, takich jak kolor, marka, typ pojazdu;
- kamery kontrolujące obecność pojazdów badające 2, 3 lub 6 miejsc postojowych;
- szlabany;
- tablice LED wyświetlające informacje na temat liczby wolnych miejsc oraz kierujące ruchem pojazdów;
- akcesoria montażowe, m.in. zabezpieczające przed przypadkowym zamknięciem szlabanu.

DSS Professional pozwala na obsługę aż 50 tys. pojazdów w jednym systemie, które można zebrać w 500 różnych grup. Parkingów głównych w ramach jednego systemu może funkcjonować aż 16, a do każdego z nich można przypisać kolejnych 16 tzw. parkingów podrzędnych. To oznacza, że DSS Professional sprawdzi się doskonale w przypadku organizacji zarządzających obiektami o bardzo rozbudowanej strukturze. System łącznie jest w stanie obsłużyć do 128 punktów wjazdowych/wyjazdowych. Obsługę skomplikowanych pod względem architektonicznym, wielopoziomowych parkingów ułatwia możliwość zastosowania e-map, przedstawiających wizualizację poziomów parkingu.

Jeżeli wymagania dotyczące obsługi i zarządzania danym obiektem nie ograniczają się tylko do kwestii podglądu obrazu z kamer, ale oznaczają także konieczność interakcji z systemem kontroli dostępu czy systemem parkingowym, to DSS Professional będzie doskonałym wyborem. Pełna integracja wielu różnych systemów, praca wieloserwerowa, wygodna aplikacja mobilna, możliwość wygenerowania licencji testowej, by sprawdzić system w boju jeszcze przed jego zakupem, to niewątpliwe atuty tej platformy. ●

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

alhua TECHNOLOGY

# WIZCOLOR

## AS BRIGHT AS DAYLIGHT


Technologia Dahua WizColor to połączenie zaawansowanych algorytmów sztucznej inteligencji w ramach technologii przetwarzania obrazu AI-ISP, z dużą matrycą światłoczułą oraz szerokim otworem przysłony kamery.

To wyjątkowe połączenie umożliwia kamerom bezproblemowe rejestrowanie obrazów wysokiej jakości o naturalnych żywych kolorach w warunkach nocnych, gwarantując zachowanie szczegółowości obrazu i minimalizacji rozmycia ruchu.

- **Precyzyjne i wyraźne szczegóły**
- **Mniejsze rozmycie ruchu**
- **Korekcja zniekształceń obrazu**
- **Bardziej realistyczne obrazy**
- **Długi zasięg monitorowania**
- **Wyraźne tablica rejestracyjne**

* Wygląd oraz specyfikacja urządzeń może ulec zmianom bez uprzedniego powiadomienia

Wer. 1, 10.2024

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

# Kasa automatyczna PAY FRAME 600 Narodziny gwiazdy!

**Odkryj zalety nowej minimalistycznej kasy automatycznej PAY FRAME 600. Ten nowoczesny system parkingowy zmienia jakość korzystania z obiektów użyteczności publicznej.**

To przyszłościowe rozwiązanie koncentrujące się na elastyczności, wydajności i łatwości użytkowania. Jego innowacyjność upraszczająca procesy sprawia, że znalezienie miejsca parkingowego staje się szybkie i bezstresowe.

## Nowoczesność, łatwość użytkowania i wygoda

Kasa PAY FRAME 600 rewolucjonizuje bezgotówkowe płatności w obiektach parkingowych. Elegancka, montowana na ścianie konstrukcja łączy zaawansowaną funkcjonalność z intuicyjnymi cechami użytkowymi.

## Intuicyjna obsługa

Wyposażona w duży 27-calowy kolorowy ekran dotykowy TFT kasa PAY FRAME 600 umożliwia użytkownikom łatwą obsługę opłat parkingowych, od skanowania biletów po dokonywanie płatności za pomocą kart zbliżeniowych.

## Wszechstronne możliwości płatności

PAY FRAME 600 oferuje wiele metod płatności – od zbliżeniowych kart płatniczych po kody QR, płatności kartami z użyciem PIN i technologii zbliżeniowych NFC, co sprawia, że płatność jest szybka i prosta. Modułowa konstrukcja PAY FRAME 600 umożliwia wszechstronną personalizację, pozwalając operatorom na dostosowanie funkcji kasy do potrzeb obiektu, w którym kasa funkcjonuje.

## Nowoczesna opcja *pay-by-plate* – koniec z biletami

Użytkownicy mogą płacić, wpisując numer rejestracyjny pojazdu, korzystając z opcji *pay-by-plate*, co zapewnia w pełni bezbiletowe doświadczenie – idealne dla nowoczesnych obiektów parkingowych.

## Unikatowa elegancja

Podświetlana ramka LED dodaje nowoczesnego stylu, a możliwość dostosowania kolorów pozwala dopasować urządzenie do identyfikacji wizualnej obiektu. Ta możliwość personalizacji sprawia, że urządzenie staje się nie tylko narzędziem praktycznym, ale także stylowym elementem aranżacji przestrzeni parkingowej.

Dzięki uproszczonym procesom płatności oraz elastycznym opcjom instalacji kasa PAY FRAME 600 oferuje nowoczesne rozwiązanie zapewniające sprawne, bezpieczne i nowoczesne płatności bezgotówkowe w obiektach parkingowych. ●

**DESIGNA AXESS POLSKA**
plac Konesera 12, 03-736 Warszawa
https://designa.com/
Konrad.Jaworski@designa.com

ALNET SYSTEMS

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


**www.alnetsystems.com**

# blueEvo
# Nowy elektroniczny system kontroli dostępu Winkhaus

Kontrola dostępu w obiektach to działania, procedury oraz technologie zarządzające dostępem do określonego miejsca lub jego zasobów. W kontekście bezpieczeństwa to konkretne mechanizmy, które pozwalają na identyfikację i autoryzację osób mających prawo dostępu do obiektów lub informacji.

O nowym elektronicznym systemie kontroli dostępu, który opracowała firma Winkhaus, rozmawiamy z **Krzysztofem Ratajczakiem,** dyrektorem handlowym Winkhaus Polska.

### Zacznijmy od początku, czyli od historii firmy Winkhaus w branży elektronicznych systemów kontroli dostępu.

Jesteśmy obecni od początku rozwoju branży, kiedy do systemów kontroli dostępu zaimplementowano technologie IT. Pierwsze systemy KD wykorzystujące technologie elektromagnetyczne pojawiły się w latach 60. XX wieku, by – rozwijając się w kolejnych dekadach – wykorzystywać dostępne rozwiązania, takie jak karty zbliżeniowe RFID, a później systemy biometryczne. Wprowadzenie mikroprocesorów i zaawansowanych technologii informatycznych w latach 90. pozwoliło na tworzenie skomplikowanych systemów zarządzania dostępem, obejmujących zdalne zarządzanie uprawnieniami, monitoring i integrację z innymi systemami bezpieczeństwa. Na bazie tych zmian w 1999 r. na rynku zadebiutował pierwszy system elektronicznej kontroli dostępu Winkhaus, jakim był blueChip.

### Jak ewoluowała technologia elektronicznego systemu kontroli dostępu Winkhaus?

Od premiery systemu blueChip minęło ćwierć wieku. W odniesieniu do nowoczesnych technologii to wręcz kosmos zmian, często rewolucja. W firmie Winkhaus inwestycje w dział R&D, podążanie za światowymi trendami i rozwojem technologii oraz dopasowanie do wymogów rynku przyniosły rezultaty w postaci nowych rozwiązań: w 2011 r. wprowadzono na rynek system blueSmart, a w 2015 – blueCompact.

Rynek zabezpieczeń rozwija się, na szczęście, szybciej od zaangażowania w techniki ich łamania, a Winkhaus należy do europejskiej czołówki producentów branży zabezpieczeń, bacznie obserwując jej zmiany i potrzeby. W tym roku w Europie Zachodniej, w Polsce na początku 2025, zadebiutujemy z najnowszym produktem naszego działu rozwoju z Münster, systemem blueEvo.

### blueEvo – ewolucja inspirowana tradycją – czyli...

Czyli nowoczesna technologia bazująca na doświadczeniu, wiedzy, badaniach i testach, inspirowana także wnioskami i obserwacjami klientów i – na drodze ewolucji – łącząca najnowocześniejsze usprawnienia technologiczne. Wywodzi się z systemu blueSmart i bazuje na tej technologii, a co najważniejsze została zaprojektowana i jest produkowana w 100% w naszym zakładzie w Münster. W telegraficznym skrócie: system składa się z elektronicznych wkładek i obsługujących je kluczy. Nie wymaga okablowania. To znaczący wyróżnik systemu. Komunikacja odbywa się za pomocą fal radiowych w momencie kontaktu klucza z wkładką. Do komunikacji między komponentami a oprogramowaniem służą czytniki online montowane z reguły przy głównych wejściach do budynków.

### Dlaczego warto inwestować w elektroniczny system kontroli dostępu blueEvo?

Bo to inwestycja w bezwzględne bezpieczeństwo. Ma to przełożenie na szereg korzyści. Zaletami elektronicznej kontroli dostępu są przede wszystkim niezależność i elastyczność nadawania uprawnień. W odróżnieniu od wariantu mechanicznego prawa dostępowe mogą tu być nadawane na czas nieokreślony lub w ściśle określonych ograniczeniach czasowych i na każdym etapie eksploatacji systemu. W przypadku zgubienia klucza nie ma potrzeby przekodowania wkładek elektronicznych ani ich wymiany. Większość dostępnych na rynku elektronicznych systemów zabezpieczeń wymaga specjalnego okablowania, które trzeba zaplanować już na etapie projektu instalacji elektrycznej. Późniejszy montaż bowiem wiąże się z nieplanowanymi kosztami przeróbek i remontu obiektu.

Rozwiązaniem niemal idealnym jest zatem system działający niezależnie od zasilania sieciowego, bez konieczności montowania urządzeń podtrzymujących napięcie i akumulatorów, czyli blueEvo.

## Co odróżnia system blueEvo od wcześniejszych wersji elektronicznej kontroli dostępu Winkhaus?

Przełomowa koncepcja blueEvo dotyczy kompleksowej architektury bezpieczeństwa obejmującej zarówno sprzęt, jak i oprogramowanie oraz procedury i standardy, które razem tworzą spójny system zabezpieczeń. Do tego dochodzą bogata oferta komponentów oraz intuicyjna obsługa sprzętu i oprogramowania. Dzięki temu system spełnia różnorodne wymagania w kwestii zabezpieczeń, a jego zastosowania są rozległe.

Najważniejszą cechą systemu jest koncepcja bezpieczeństwa, która zapewnia stałą ochronę poufności, integralności i autentyczności danych systemowych oraz danych dostępowych. O całość zadbali nasi specjaliści w Niemczech wraz z ekspertami z dziedziny Cyber Physical Systems i Security Management. Akcesorium blueEvo zostało zabezpieczone przed atakami mechanicznymi i hakerskimi. Gwarantuje to technologia Mifare® DESFire® EV3 zastosowana we wszystkich komponentach. Jak dotąd tylko firmie Winkhaus udało się pomyślnie zintegrować te technologie w niewielkich urządzeniach, jakimi są wkładka elektroniczna i klucze.

## Jakie są inne ważne funkcje systemu blueEvo?

Ciekawą funkcją jest Virtual Network Hubs (czytniki z funkcją aktualizacji praw dostępu i rejestracji), dzięki której zmiana uprawnień jest aktywowana natychmiast, gdy tylko identyfikator, głównie elektroniczny klucz, zostanie przystawiony do czytnika, bez potrzeby ręcznego wprowadzania zmian. Zwykle instalowane są one przy głównych drzwiach i w tle zapisują aktualne informacje o uprawnieniach na dostępnych identyfikatorach: kluczach czy brelokach. Równocześnie przesyłają do sieci wirtualnej informacje o zdarzeniach zamknięcia, użycia nieuprawnionego klucza czy ostrzeżenia o niskim poziomie naładowania baterii.

System blueEvo korzysta również z funkcji czasowych uprawnień, które automatycznie wygasają (można ustawić wymóg codziennego aktywowania), co zapewnia wysoki poziom bezpieczeństwa również w przypadku utraty klucza.

## Jak programuje się system blueEvo?

Programowanie systemu i jego komponentów odbywa się w oprogramowaniu BE blueControl. Winkhaus skupił się tu na łatwości obsługi również dla mniej doświadczonych administratorów. Stworzono zatem nowatorską matrycę nadawania uprawnień. Wprowadzono nową w dziedzinie organizacji dostępu funkcję Power-Search, która pozwala przejść bezpośrednio do odpowiedniego pola funkcji aplikacji. Aplikacja przeglądarkowa jest responsywna i optymalnie zorganizowana, by umożliwić szybkie i proste wprowadzanie zmian przez administratora systemu. W przypadku zgubienia klucza można go natychmiast zablokować kilkoma kliknięciami myszy.

## Czy blueEvo można zintegrować w ramach systemu zarządzania budynkiem BMS?

Oprócz funkcji podstawowej, jaką jest kontrola dostępu do pomieszczeń, czyli zapewnienie bezpieczeństwa użytkownikom, system blueEvo posiada funkcje dodatkowe. Architektura oprogramowania jest specjalnie zaprojektowana i pozwala, opierając się na API, na integrację z innymi systemami, których programiści mogą łatwo połączyć blueEvo z istniejącymi narzędziami i platformami, zapewniając pełną kompatybilność i automatyzację procesów.

Rozwiązanie blueEvo można zatem zintegrować z takimi systemami jak stacja ładowania pojazdów elektrycznych i baterii akumulatorowych, rejestracji czasu pracy, z istniejącymi systemami kontroli dostępu, a także różnym sprzętem biurowym.

## Czy system blueEvo wpisuje się w nowe przepisy Unii Europejskiej dotyczące bezpieczeństwa sieci i informacji?

Unia Europejska dostrzegła potrzebę ochrony infrastruktury krytycznej i stworzyła kompleksowe ramy regulacyjne za pomocą dyrektywy NIS 2. Dyrektywa ta wzmacnia odporność sieci i systemów informatycznych oraz rozszerza swój zakres na łącznie 18 sektorów, w których system elektronicznej kontroli dostępu blueEvo powinien stać się swoistym *must have*.

Jedną z podstawowych funkcji każdego systemu kontroli dostępu jest zarządzanie ryzykiem. System powinien więc pozwolić na szybkie reagowanie na sytuacje kryzysowe, takie jak kradzież, sabotaż, pożar, zagrożenie terrorystyczne czy wypadek, umożliwiając natychmiastowe ograniczenie dostępu, rewizję aktywności lub ewakuację określonych obszarów. To wszystko gwarantuje blueEvo.

Zainteresowanych współpracą z Winkhaus Polska w dziedzinie zabezpieczeń i kontroli dostępu zachęcamy do kontaktu z naszymi specjalistami. ●

**Winkhaus Polska Beteiligungs**
ul. Przemysłowa 1, 64-130 Rydzyna
Tel. 538 818 723, 65 52 55 784
www.blueevo.com

# Kryteria wyboru systemu *master key*

**W dobie rosnących zagrożeń bezpieczeństwa obiektów kultury wybór odpowiedniego systemu master key do muzeum jest zadaniem wymagającym i kluczowym dla zachowania wartościowych zbiorów.**

**Artur Bogusz**, kierownik Działu Bezpieczeństwa w Muzeum Historii Polski oraz rzeczoznawca Polskiej Izby Ochrony, dzieli się swoim doświadczeniem i podpowiada, jak zapewnić ochronę przed nieautoryzowanym dostępem, a jednocześnie umożliwić sprawne funkcjonowanie personelu i bezproblemowe zwiedzanie ekspozycji.

Wybór systemu *master key* do nowego obiektu to kluczowa decyzja wpływająca na bezpieczeństwo obiektu i komfort jego użytkowania. System musi być precyzyjnie dopasowany do specyfiki funkcjonowania muzeum. Hierarchiczny system dostępu, w którym jeden klucz otwiera wiele drzwi, pozwala na efektywne zarządzanie dostępem do różnych stref, co jest szczególnie istotne w instytucji, w której ochrona eksponatów ma kluczowe znaczenie.

Podczas wyboru systemu należy określić wszystkie strefy dostępu oraz wymagania różnych grup użytkowników. Dlatego współpraca z doświadczonym doradcą, szefem ds. bezpieczeństwa jest nieoceniona. Pomoże on zdefiniować uprawnienia użytkowników, a także zidentyfikować potencjalne zagrożenia. W muzeum znajdują się przecież nie tylko drzwi, ale także inne chronione miejsca: gabloty, okna czy systemy alarmowe, które należy uwzględnić w planie ochrony. Bardzo istotne jest zabezpieczenie dostępu do gablot z eksponatami – to element wyróżniający system klucza w instytucji kultury. Alarm pożarowy, ogłoszenie ewakuacji obiektu, potrzeba ewakuacji zbiorów to kwestie związane z otwieraniem czy zamykaniem określonych pomieszczeń, w tym szczególnie chronionych.

Kolejnym aspektem, jaki należy uwzględnić, jest elastyczność systemu. Dobrze zaprojektowany system powinien umożliwiać dostosowanie dostępu w zależności od zmieniających się potrzeb muzeum, a także odwzorowywać strukturę organizacyjną. Każda grupa pracowników, od kuratorów, konserwatorów, pracowników ochrony po techników, powinna mieć przypisany klucz tylko do pomieszczeń, do których jest uprawniona.

Przy wyborze producenta ważne jest zwrócenie uwagi na jakość i niezawodność produktu. Należy wybierać renomowanych producentów z miarodajnymi referencjami i długoletnim doświadczeniem w branży. Równie istotne jest zapewnienie odpowiednich standardów ochrony danych, gdyż proces tworzenia systemu zamknięć często wymaga udostępnienia wrażliwych informacji, np. planów budynków. Z punktu widzenia osób zarządzających bezpieczeństwem w instytucjach kultury ważny jest także dobry kontakt z dostawcą i obsługa posprzedażowa. Praktyka w tym zakresie pokazuje, że sama sprzedaż przebiega bez zakłóceń, a problemy zaczynają się na etapie faktycznego użytkowania systemu.

Odpowiednia eksploatacja oraz regularna konserwacja są kluczowe dla sprawności systemu. W przypadku muzeum intensywne użytkowanie niektórych drzwi wymaga regularnych przeglądów i konserwacji, aby zapewnić ciągłość bezpieczeństwa. Zarządzanie kluczami także ma znaczenie. Właściwe procedury dotyczące inwentaryzacji kluczy oraz postępowania w przypadku ich utraty powinny być jasno określone. Ich brak może prowadzić do nieprzyjemnych konsekwencji.

Wybór odpowiedniego systemu *master key* to inwestycja w bezpieczeństwo muzeum na wiele lat. Dobrze zaplanowany i solidnie wykonany system dostępu, współpraca z doświadczonymi specjalistami oraz regularna konserwacja to elementy zapewniające jego długotrwałe funkcjonowanie. System *master key* nie tylko chroni wartościowe zbiory, ale także wpływa na efektywność funkcjonowania muzeum, co w dzisiejszych czasach jest kluczowe dla sukcesu każdej instytucji kultury. ●

**EVVA Polska**
ul. Rzemieślnicza 12
05-082 Blizne Łaszczyńskiego
www.evva.pl

# CREDO ID – nowość na rynku polskim


**CREDO ID to opracowana ponad 10 lat temu na Litwie otwarta platforma kontroli dostępu. Dzięki niezawodności, funkcjonalności oraz prostocie instalacji i obsługi znalazła zastosowanie zarówno w małych obiektach handlowych, jak w dużych instalacjach.**

CREDO ID to mało wymagająca sprzętowo platforma kontroli dostępu działająca w środowisku Windows lub Linux, dostępna również jako Docker bądź usługa w chmurze. Bardzo ważną jej cechą jest działanie na kontrolerach różnych producentów, co pozwala na wysoką elastyczność ich doboru przy nowych instalacjach i niespotykaną dotychczas możliwość modernizacji istniejących systemów kontroli dostępu. CREDO ID współpracuje z czytnikami HID, STid oraz innych producentów stosujących protokół OSDP, gwarantując najwyższy dostępny poziom niezawodności, bezpieczeństwa i szyfrowania.

Platforma wspiera mobilne poświadczenia HID lub STid, co pozwala na bezpieczne i wygodne użycie smartfonów zamiast kart, obniżając koszty. Obsługuje również mobilne czytniki umożliwiające identyfikację użytkowników w dowolnym miejscu nawet poza obiektem, np. podczas pożaru i zbiórki. System powiadomi, ile osób pozostało w budynku oraz gdzie i kiedy po raz ostatni odnotowano ich obecność. Mogą być także obsługiwane bezprzewodowe zamki, kłódki elektroniczne, zamki do szaf serwerowych i wkładki z kluczem mechaniczno-elektronicznym CLIQ. Dzięki temu za pomocą CREDO ID można kontrolować wiele rozwiązań różnych dostawców. Dostępna jest też rejestracja czasu pracy oferująca wbudowane raporty przydatne w każdej firmie po integracje ze Splan.

CREDO ID może także się integrować z wieloma systemami VMS obecnymi na rynku oraz z parkingowymi systemami LPR, lub bezpośrednio z kamerami AXIS z funkcją rozpoznawania tablic rejestracyjnych. Integracja z SATEL pozwala na sterowanie systemem alarmowym za pomocą map obecnych w CREDO ID. Możliwe jest także wyświetlanie alarmów i zmiana scenariuszy działania systemu kontroli dostępu.

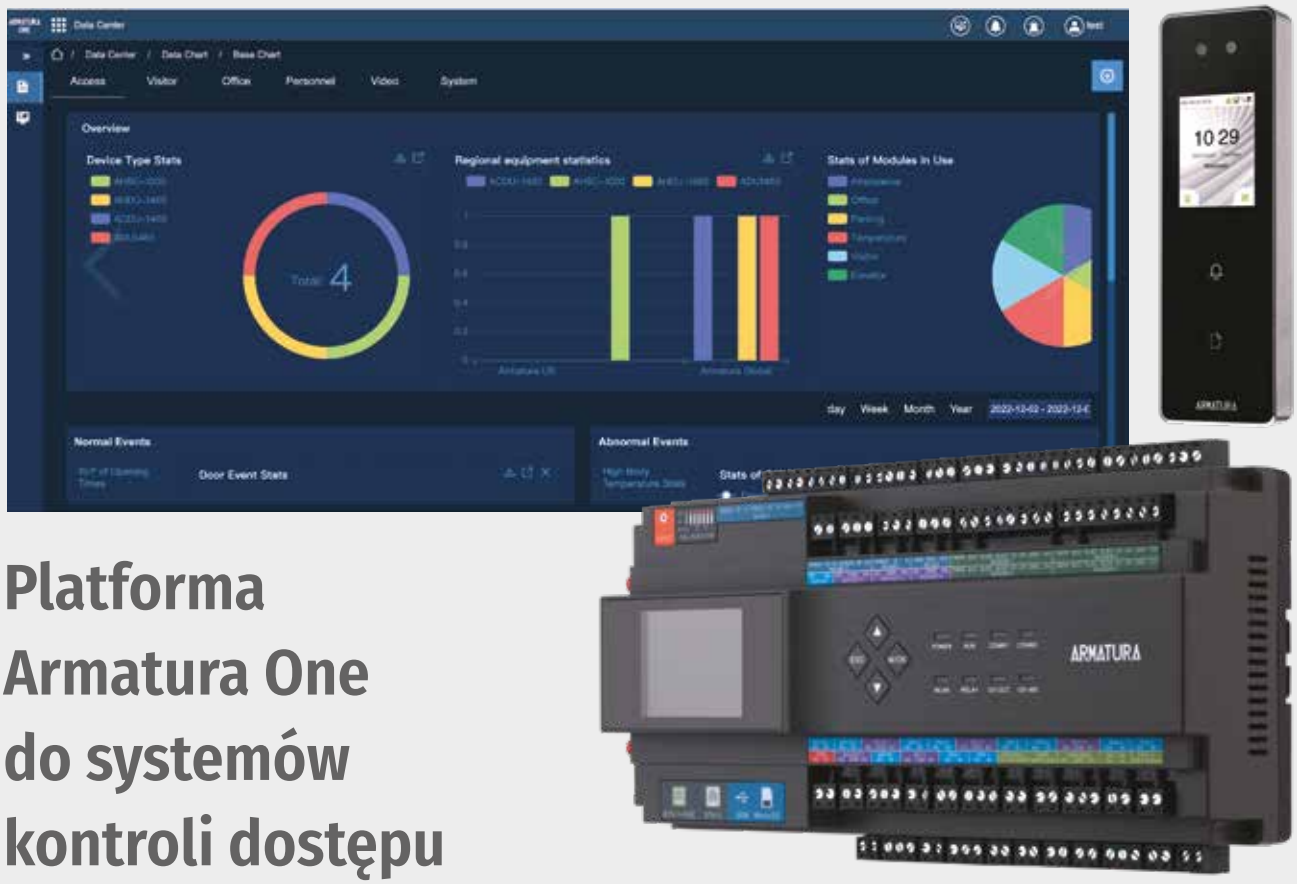
Dzięki zgodności z najnowszymi wymaganiami bezpieczeństwa, m.in. NIS2, jesteśmy w stanie stworzyć bezpieczny, nie tylko cyfrowo, system kontroli dostępu spełniający wymagania określone w normie Grade 4. Klientom zapewniamy bezpłatny dostęp do REST API, które umożliwia samodzielne wykonanie integracji z działającymi już w firmie rozwiązaniami.

Przykładamy dużą wagę do tego, by każdy z naszych klientów mógł lokalnie liczyć na pełne przed- i posprzedażowe wsparcie. Aby móc je zapewnić, podpisaliśmy umowę dystrybucyjna z EST Polska (European Security Trading Polska).

Zapraszamy do kontaktu z firmą EST Polska (www.security-trading.pl/credoid) lub bezpośrednio z naszym przedstawicielem:

j.kazmierczak@midpoint-security.com ●

**Midpoint Systems**
Zalgirio 88,
LT 09303 Wilno, Litwa
www.midpoint-security.com




# Platforma Armatura One do systemów kontroli dostępu

**Rosnące zapotrzebowanie na coraz lepsze rozwiązania w zakresie bezpieczeństwa doprowadziło do opracowania przez inżynierów z Doliny Krzemowej w USA dla firmy ZKTeco platformy Armatura One.**

**Marek Piotrowski**

Armatura One to internetowa platforma „wszystko w jednym" zaprojektowana w celu zapewnienia wysoce bezpiecznego, przyjaznego dla użytkownika i zintegrowanego systemu kontroli dostępu o szerokiej funkcjonalności.

Priorytetowo potraktowano w niej prywatność i bezpieczeństwo. Wszystkie dane są szyfrowane przy użyciu zaawansowanych 256-bitowych protokołów kryptograficznych *Advanced Encryption Standard* (AES) i *Transport Layer Security* (TLS). Ma certyfikaty ISO27001, ISO27701 i ISO27017.

Platforma Armatura One oferuje uwierzytelnianie wielopoziomowe za pomocą takich technik, jak biometria, uwierzytelnianie mobilne, szyfrowane dynamiczne kody QR i wiele standardów kart RFID.

Na elementy platformy oprócz systemu zarządzającego składają się: kilka rodzajów kontrolerów kompatybilnych z najnowszym protokołem OSDP 2.2 wyposażonych w PUE (802.3at), RS-485, Wi-Fi, opcjonalny Bluetooth oraz samodzielne terminale i czytniki.

Jedną z istotnych cech platformy jest wsparcie dla automatyki budynkowej, dzięki czemu można ją łatwo zintegrować z systemami zarządzania budynkiem (BMS) i systemami zarządzania nieruchomością (PMS).

Funkcja mapy cyfrowej integruje się z różnymi narzędziami do tworzenia map, takimi jak Google Maps, GIS Maps i SuperMap. Umożliwia tworzenie map 2D dla poszczególnych pięter, map 3D dla budynków wielopiętrowych oraz map obiektów znajdujących się w wielu oddalonych lokalizacjach.

Platforma obsługuje większość scenariuszy dla aplikacji kontroli dostępu obejmujących zaawansowane, wielofunkcyjne powiązania z ponad 200 warunkami. Ponadto obsługuje połączenia z urządzeniami klasy przemysłowej, np. czujnikami jakości powietrza, klimatyzatorami, czujnikami wycieku wody i wieloma innymi.

Armatura One powstała z myślą o skalowalności. Wykorzystuje innowacyjny protokół komunikacyjny MQTT, dzięki czemu zapewnia wydajną komunikację z ponad 10 000 urządzeniami końcowymi (kontrolery, terminale, czytniki, czujniki) i zarządzanie ponad milionem użytkowników w prostym środowisku sieciowym.

Jedną z wyróżniających się funkcji platformy jest system powiadomień, który umożliwia użytkownikom otrzymywanie wiadomości za pośrednictwem poczty elektronicznej, SMS-ów lub komunikatorów internetowych, takich jak WhatsApp czy Amazon SNS.

Aby zapewnić łatwość integracji z systemami zabezpieczeń innych firm, Armatura One oferuje pełne API i SDK. Platforma integruje się już z rozwiązaniami takich firm, jak BOSCH, Risco, Honeywell, Schindler, Mitsubishi, Kone, Hitachi, Otis, Milestone, Arteco, Digifort, Assa Abloy Aperio. Obsługuje wiele form integracji w oparciu o Armatura Restful Web API, Microsoft Active Directory, Microsoft Excel i automatyczny import CSV.

Podsumowując, Armatura One to wysoce bezpieczne, elastyczne i skalowalne rozwiązanie spełniające najwyższe wymagania dotyczące bezpieczeństwa, oferujące szeroki zakres funkcji i możliwości integracji. ●

**ZKTeco Polska**
aleja Niepodległości 18
02-653 Warszawa
marek.piotrowski@zkteco.eu

# Pierwsza linia ochrony:
## systemy detekcji i alarmowania

**Jednym z filarów ochrony obiektów firmowych i obszarów, na których się znajdują, są systemy obwodowe, składające się najczęściej z mariażu systemów zabezpieczeń mechanicznych z różnego rodzaju systemami zakopywanymi, mocowanymi do ogrodzeń, umieszczanymi za liniami ogrodzeń czy systemami detekcji wizyjnej.**

Wiele przedsiębiorstw powiela znane rozwiązania, nie zwracając uwagi na cele, którym mają one służyć. Istotna jest pełna świadomość tego, w jakim celu stosowane są systemy ochrony obwodowej, czyli wydłużenie czasu niezbędnego na sforsowanie fizycznego ogrodzenia z jednoczesnym powiadomieniem odpowiednich służb. Nawet najdoskonalsze systemy nie zatrzymają napastnika, ale spowolnią go i pozwolą na wysłanie patrolu, który może fizycznie zneutralizować zagrożenie.

Dlatego ważna jest budowa systemu w sposób adekwatny do potrzeb zabezpieczanego obiektu. Często wystarczy sygnalizator dźwiękowy, snop światła z reflektora czy komunikat głosowy, żeby zniechęcić napastnika. Jednak widok patrolu potrafiącego zastosować środki przymusu bezpośredniego jest właśnie najczęściej czynnikiem wymuszającym ucieczkę intruza.

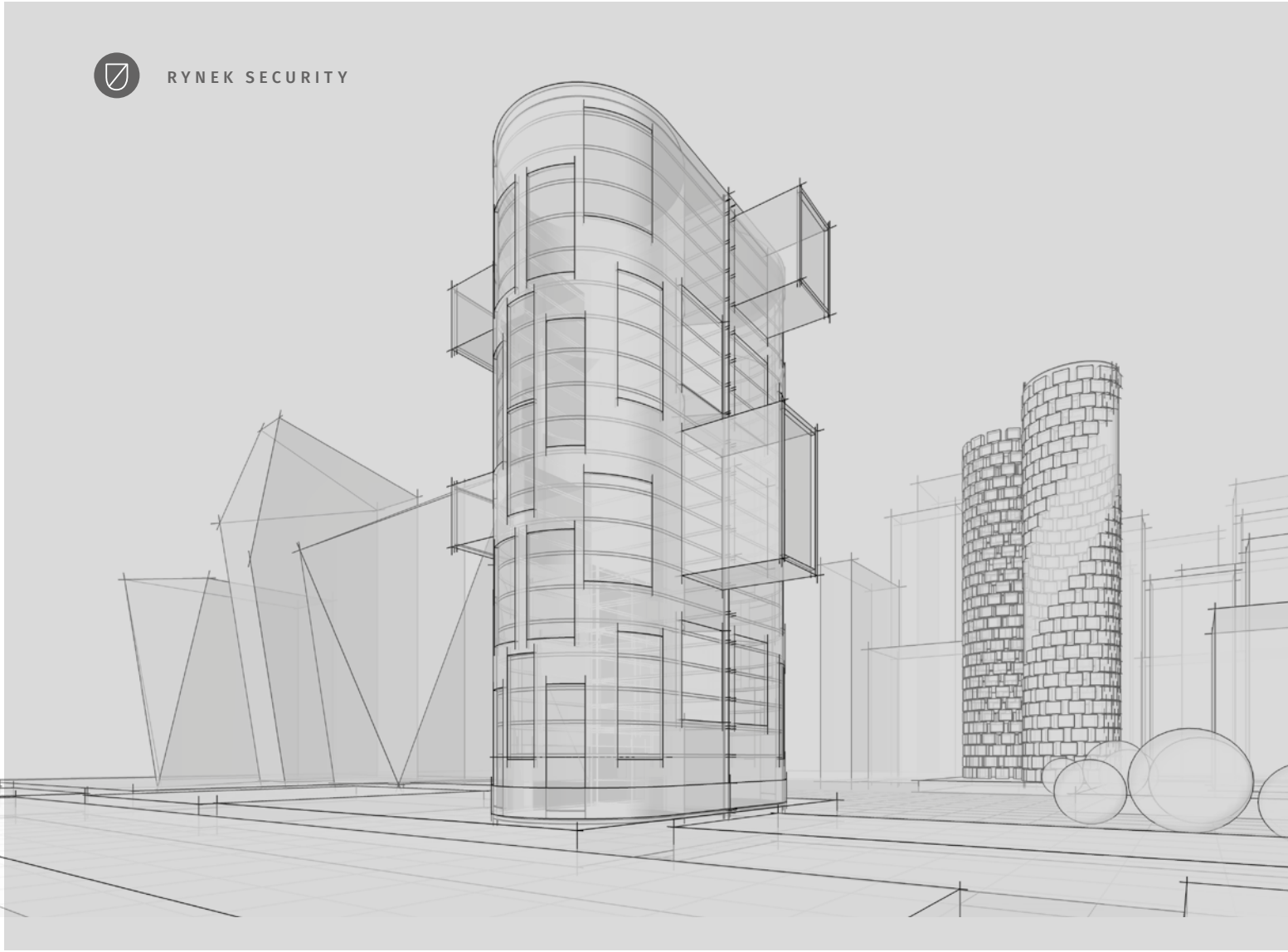
Taki intruz potrafi dokonać wielu szkód. Znajdując się na drodze startowej lotniska, może nie tylko sparaliżować na pewien czas plan operacji lotniczych, co może generować znaczne koszty dla operatora lotniska, ale też może spowodować katastrofę lotniczą zagrażającą życiu pasażerów i obsługi. Podobnie na terenach zakładów zajmujących się przesyłem paliwa czy energii elektrycznej albo produkcją chemikaliów lub innych niebezpiecznych i strategicznych materiałów. Nawet drobny incydent jest w stanie spowodować awarię czy katastrofę ekologiczną o dużym zasięgu w skali kraju i ogromnych kosztach, nie tylko finansowych, ale i społecznych.

Inne podejście należy zastosować w przypadku ochrony obwodowej obszarowej, z terenami rozległymi, jakimi są np. granice państwowe. Z uwagi na czas potrzebny na dotarcie do miejsca penetracji strefy stosowane są tam systemy pozwalające na ostrzeganie o jej naruszeniu z największym wyprzedzeniem. Już prealarmy ze stref podejścia są sygnalizowane w centrach nadzoru, a dalej, przez efektywne połączenie systemów detekcyjnych z obrazami z kamer termowizyjnych i światła widzialnego za pomocą oprogramowania PSIM, odbywa się weryfikacja zdarzeń przez operatorów i zostaje podjęta decyzja o przesunięciu grupy interwencyjnej w dany sektor.

Ochrona obwodowa dużych i zróżnicowanych obszarów jest ogromnym wyzwaniem z uwagi na zmienność terenu (cieki wodne, zbiorniki wodne, tereny podmokłe, lasy, pola, przewyższenia terenu etc.) oraz przestrzenie podlegające zabezpieczeniu. Dlatego, w takich warunkach, do weryfikacji zdarzeń oraz ewentualnego śledzenia intruzów poza kablami detekcyjnymi pokrywającymi duże obszary wykorzystywane są systemy dodatkowych czujników oraz detekcja wizyjna w postaci kamer termowizyjnych, łącznie z kamerami PTZ dalekiego zasięgu.

W obecnych czasach warto również wziąć pod uwagę zabezpieczenie przestrzeni powietrznej nad obiektami. W celu uszczelnienia zabezpieczeń do wykrywania zagrożeń z powietrza coraz częściej zaczynają być stosowane systemy wykrywania bezzałogowych statków powietrznych. Na razie kwestią problematyczną są tylko metody neutralizacji unoszących się w przestrzeni dronów, mogących stanowić zagrożenie. ●

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



# Mapa inwestycji

Koniec roku wcale nie oznacza spowolnienia na rynku inwestycji. W całej Polsce trwają przygotowania do prac budowlanych lub już rozpoczynają się nowe inwestycje, na które umowy podpisano jesienią. Jak zwykle przedstawiamy wybór największych projektów prowadzonych przez renomowane firmy. To m.in. budynki cywilne, takie jak akademiki czy kompleksy handlowo-usługowe, a także obiekty przemysłowe, elementy infrastruktury morskiej oraz przesyłowej. Przekrój „tematyczny" jest więc spory, podobnie jak geograficzny. Jednocześnie zachęcamy do korzystania z map inwestycji zamieszczonych w poprzednich numerach „a&s Polska" – zawsze bowiem przygotowujemy je z dużym wyprzedzeniem, pilnując, aby daty zakończenia kontraktów wypadały nie wcześniej niż za trzy kwartały.

Adela Prochyra, a&s Polska


## ATREM

**Co:** KOMPLEKSOWA MODERNIZACJA ROZDZIELNI 110 KV
**Gdzie:** Przechowo
**Kiedy:** 31.12.2025
1

## BUDIMEX

**Co:** BUDOWA FALOCHRONÓW OSŁONOWYCH, STANOWIĄCYCH WODNĄ INFRASTRUKTURĘ DOSTĘPOWĄ DO PORTU ZEWNĘTRZNEGO W PORCIE GDYNIA, W FORMULE ZAPROJEKTUJ I WYBUDUJ
**Gdzie:** Gdynia
**Kiedy:** 490 dni od podpisania umowy (2.10.2024) + 819 dni na prace budowlane od dnia uzyskania pozwolenia na budowę
2

## ELEKTROTIM

**Co:** WYMIANA ROZDZIELNIC WRAZ Z TRANSFORMATORAMI
**Gdzie:** Lubin
**Kiedy:** 120 tygodni licząc od dnia podpisania umowy (22.10.2024)
3

## ENERGOAPARATURA

**Co:** PRZEBUDOWA ROZDZIELNI SN 15KV WRAZ Z WYMIANĄ TRANSFORMATORÓW 110/15 KV
**Gdzie:** Żnin
**Kiedy:** 9 miesięcy od dnia zawarcia umowy (17.10.2024)
4

## ERBUD

**Co:** ROBOTY BUDOWLANE PODWYKONAWCZE W RAMACH BUDOWY ZESPOŁU URZĄDZEŃ SŁUŻĄCYCH DO WYPROWADZENIA MOCY Z MORSKIEJ FARMY WIATROWEJ MFW BAŁTYK III
**Gdzie:** Pęplino k. Ustki
**Kiedy:** 30.07.2027
5

**Co:** BUDOWA INFRASTRUKTURY QRA DLA F-35 – DOMEK PARY DYŻURNEJ ORAZ 4 HANGARY TYPU PÓŁCIĘŻKIEGO
**Gdzie:** Świdwin – lotnisko
**Kiedy:** 30.01.2026
6

**Co:** BUDOWA INFRASTRUKTURY QRA DLA F-35 – DOMEK PARY DYŻURNEJ ORAZ 4 HANGARY TYPU PÓŁCIĘŻKIEGO
**Gdzie:** Poznań
**Kiedy:** 27.11.2025
7

## PJP MAKRUM

**Co:** WYBUDOWANIE BUDYNKU B5
**Gdzie:** Ujeździec Mały
**Kiedy:** 30.06.2025
8

## PEKABEX

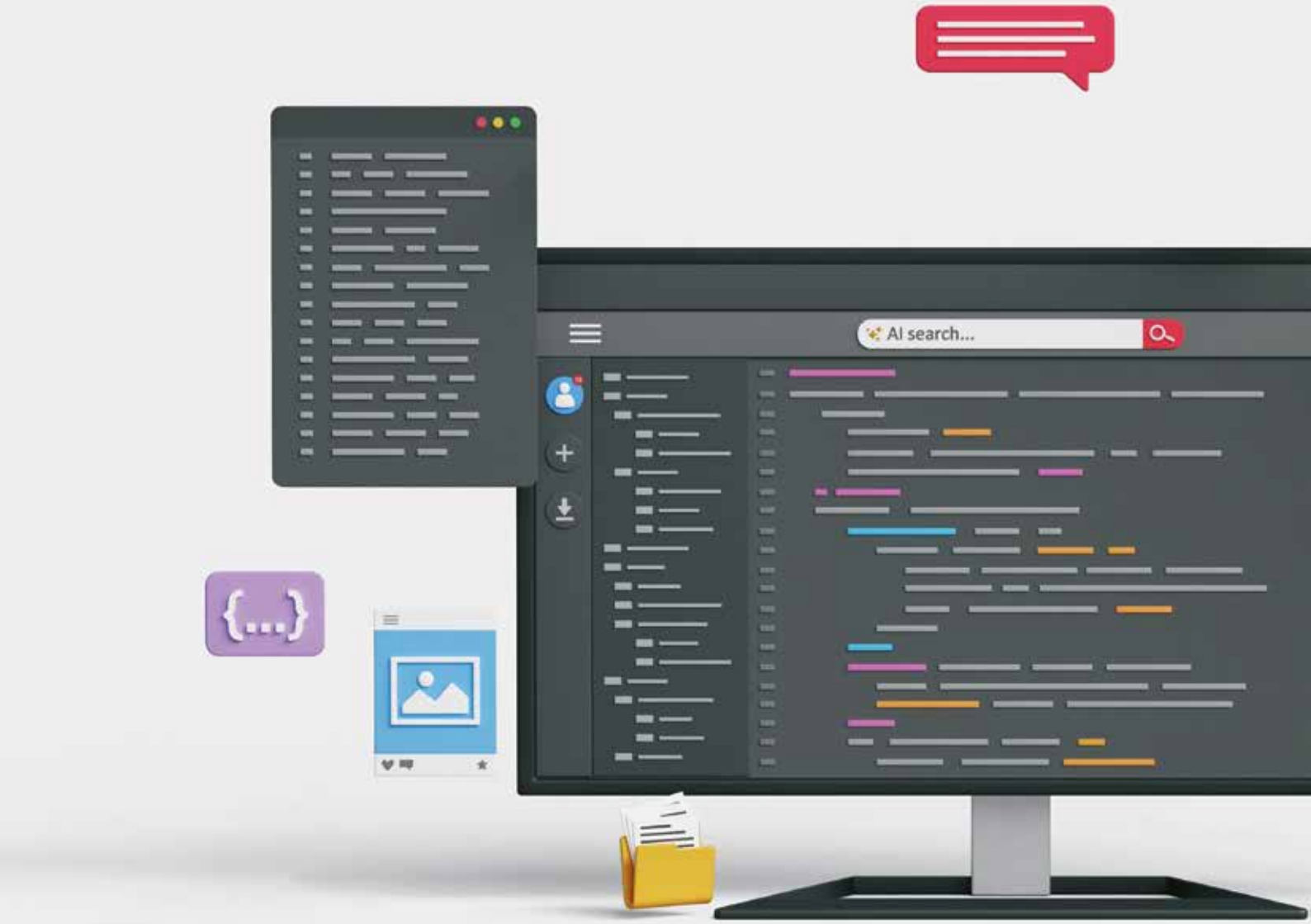
**Co:** BUDOWA ZAKŁADU PRZETWÓRSTWA MLECZNEGO
**Gdzie:** Bieruń
**Kiedy:** 28.02.2026
9

**Co:** BUDOWA ZESPOŁU BUDYNKÓW HANDLOWO-USŁUGOWYCH Z ZAGOSPODAROWANIEM TERENU ORAZ NIEZBĘDNĄ INFRASTRUKTURĄ TECHNICZNĄ I TOWARZYSZĄCĄ ORAZ PYLONAMI REKLAMOWYMI
**Gdzie:** Nowogard
**Kiedy:** Nie później niż 12 miesięcy od dnia wezwania spółki do rozpoczęcia robót
10

**Co:** BUDOWA BUDYNKU U1 – CENTRUM WSPARCIA DYDAKTYKI UNIWERSYTETU MEDYCZNEGO W ŁODZI W FORMULE „ZAPROJEKTUJ I WYBUDUJ"
**Gdzie:** Łódź
**Kiedy:** 14.03.2026
11

**Co:** BUDOWA BUDYNKU PROCESOWEGO NR P1C WCHODZĄCEGO W SKŁAD ZAKŁADU PRODUKCYJNEGO
**Gdzie:** Powiat nyski w woj. opolskim
**Kiedy:** 15.04.2026
12

**Co:** ROZBUDOWA ZAKŁADU PIEKARNI O NOWĄ HALĘ PRODUKCYJNO-MAGAZYNOWĄ WRAZ Z ROZBUDOWĄ CZĘŚCI SPEDYCYJNEJ ORAZ PRZEBUDOWĄ UZBROJENIA I UTWARDZEŃ TERENÓW ZEWNĘTRZNYCH I ROZBIÓRKĄ MYJNI SAMOCHODÓW DOSTAWCZYCH
**Gdzie:** Ożarów Mazowiecki – obszar wiejski
**Kiedy:** 10.08.2025
13




# Projekt IT dla systemów bezpieczeństwa

Przenikanie się obszarów bezpieczeństwa fizycznego oraz IT na stałe wpisało się w nasze codzienne obowiązki. Czy tego chcemy, czy nie, prędzej czy później na naszej drodze pojawią się aspekty związane z każdym z nich. Dlatego warto przyjrzeć się zbieżności, która przejawia się tym, że dla każdego projektu dotyczącego bezpieczeństw należy przygotować także... odpowiednią dokumentację IT. I tu bardzo często pojawiają się pewne wyzwania.

Tomasz Dacka

Dojrzałe środowiska wypracowały swoje standardy oraz wytyczne, jak sobie z tymi wyzwaniami radzić. Mimo to nawet jeśli owa dokumentacja została przygotowana z dbałością i starannością, to realizacją zadań zajmują się ludzie, którzy z definicji nie lubią robić tego, na czym się dobrze nie znają. Dlatego bardzo często na etapie przygotowywania projektów pojawiają się ludzie-mosty, łączący ze sobą świat security i IT.

## Dwa światy, dwie dokumentacje? Dwa podejścia?

Dokumentacja projektowa prowadzona przez obszar bezpieczeństwa fizycznego skupia się na aspektach stricte z nimi związanych. Można tam znaleźć analizę ryzyka, opis funkcjonalny, rzuty z rozmieszczeniem urządzeń, tabele z zestawieniem danych związanych z urządzeniami typu kamery, kontrolery, NVR-y czy oprogramowanie. Niemniej żadne z tych urządzeń nie pracuje w próżni, są one osadzone w architekturze IT, bardzo często połączone z innymi systemami, usługami IT. Rodzi to potrzebę sporządzenia dokumentacji z obszaru informatycznego, a te z reguły wymagają od nas szerszej wiedzy i dużej dokładności w przedstawianiu danych. Tu pojawiają się pytania: czy zatem potrzebne będą dwie dokumentacje? Najprawdopodobniej tak. Czy mój wkład będzie wymagany w obydwu? Oczywiście. Jak mam sobie z tym poradzić?

## Zainteresowane strony

Jeśli musimy upiec naprawdę duży tort i przyozdobić go tzw. *compliance* (rozumianym jako zapewnienie zgodności działalności z normami, zaleceniami lub stosownymi praktykami), staje się oczywiste, że sami zrobić tego nie możemy. Dlatego tak ważne, aby wskazać (to wcale nie jest proste zadanie) oraz zebrać (kolejne żmudne działanie) wszystkich zainteresowanych. To pierwszy krok do koordynacji dwóch (lub więcej) obszarów. I gdyby tutaj kończyły się tzw. schody, byłoby dobrze, najtrudniejsze jednak jest rozdzielenie obowiązków pomiędzy dane komórki, zespoły. Bardzo często jest to nawet niewykonalne, a powodów jest mnóstwo. Warto jednak takie spotkania organizować, aby poznać możliwości, a przede wszystkim oczekiwania wszystkich zainteresowanych. Dowiemy się wtedy, jakie konkretne dane/aktywności będą potrzebne z naszej strony, kto może nas wspierać i kiedy (oraz jak często) będziemy się spotykać, aby zsynchronizować zadania. W mojej ocenie takie otwierające spotkanie z branżą IT powinno nastąpić jak najszybciej. Dlaczego? Ponieważ zyskujemy świadomość i z tą wiedzą możemy wykonać kolejne kroki podczas następnych aktywności:

- spróbować swoich sił,
- zatrudnić do pomocy kompetentne osoby spoza działu (z wewnątrz lub zewnątrz organizacji),
- przerzucić wymagania np. na wykonawcę, integratora (należy tu jednak pamiętać, że koordynacja wciąż jest po naszej stronie).

→

W momencie tworzenia dokumentacji przetargowej, zakupowej itp., uzbrojeni w nabytą wiedzę jesteśmy w stanie stworzyć wymagania ściśle nawiązujące do obszaru IT. Nie oznacza to (znam to z własnego doświadczenia), że instalator/integrator zrobi wszystko za nas, otwiera to jednak pole do dyskusji oraz punkt do wsparcia w niektórych aspektach wdrożenia systemów.

## Gra do jednej bramki

Wymagania IT będą do nas spływać zazwyczaj równolegle do prowadzonych prac fizycznych, a bardzo często nawet jeszcze przed ich rozpoczęciem. Może nawet wystąpić sytuacja, że nie będziemy mogli uruchomić wiertarki przed spełnieniem szeregu wymagań IT. Projekty informatyczne są zazwyczaj prowadzone wedle pewnych metodologii, bez względu na to, jaki konkretny model wykorzystują. Na tym etapie warto przygotować się do tego, że możemy zmierzyć się z modelem, który został stworzony stricte na potrzeby *Software Development Lifecycle* (SDLC – cykl życia oprogramowania, czyli proces, z którego korzystają programiści do tworzenia i dostarczania aplikacji w ramach uzgodnionego terminu i budżetu), podczas gdy nasze projekty rzadko zakładają tworzenie własnego oprogramowania, raczej bazują na rozwiązaniach już gotowych, z tzw. półki. Mimo to będziemy musieli się do tego dostosować, co nie powinno stanowić problemu przy naszej jasnej deklaracji na samym początku koordynacji.

Najistotniejszą kwestią na początku jest podzielenie się naszymi wymaganiami biznesowymi co do samej aplikacji, czyli generalnie rzecz ujmując, wytłumaczenie, dlaczego i w jakim zakresie wdrażamy dany system. Pomoże to ustalić wspólny mianownik i da punkt referencyjny do dalszych dyskusji.

Powinniśmy również być gotowi na to, że cały proces wdrożeniowy zostanie podzielony na pewne etapy, bramki. Przy każdym etapie będą wymagane różne informacje oraz inny poziom ich szczegółowości. Ogólnie proces można podzielić na trzy główne bramki:

- **BRAMKA NR 1.** Przedstawienie założeń biznesowych oraz koncepcji rozwiązania
- **BRAMKA NR 2.** Przedstawienie architektury rozwiązania (to, jak chcemy budować system)
- **BRAMKA NR 3.** Przedstawienie systemu gotowego do oddania (to, jak zbudowaliśmy system)

Ważne jest również, że przez wszystkie bramki przechodzi się wspólnie jako zespół. Każda bramka wymaga innego zaangażowania i położenia nacisku na inne aspekty, jednak koordynacja zapewniająca przepływ informacji odgrywa tutaj ważną rolę.

Przejście przez poszczególne bramki będzie możliwe po uzyskaniu pewnych zgód interesariuszy. Uzyskuje się je przeważnie poprzez prezentację zaawansowania swoich prac oraz zgodność z obowiązującymi politykami IT.

## Czego się spodziewać?

System zarządzania materiałem wizyjnym (VMS) czy system kontroli dostępu (SKD) jako systemy IT podlegają dokładnie takim samym wymaganiom jak inne systemy ze świata informatycznego, nawet jeśli projektowane i wdrażane są w trochę inny sposób. Generalnie każdy z systemów musi zmierzyć się z wymaganiami IT z trzech różnych dziedzin:

1. architektury IT,
2. cyberbezpieczeństwa, bezpieczeństwa informacji,
3. utrzymania i oddania do użytku.

Każda z wymienionych dziedzin będzie miała swoje wymagania, wspomniany wcześniej *compliance* oraz dokumenty do uzupełnienia.

Architektura będzie od nas wymagała informacji na temat, w jaki sposób chcemy wdrażać system. Mogą tutaj paść pytania o wykorzystanie sieci korporacyjnej lub wdrożenie na zupełnie oddzielnej sieci. Wszystkie interfejsy łączące dane segmenty sieci muszą zostać wskazane i opisane. Mniej ważny będzie tu typ kamery czy NVR, a ważniejszy może być łańcuch dostaw, informacje na temat producenta (czy np. wykonuje testy penetracyjne, czy posiada własny system zarządzania ryzykiem itp.).

Istotną kwestią jest fakt, czy chcemy łączyć się z innymi systemami, usługami korporacyjnymi, takimi jak Active Directory czy systemy ticketowe (utrzymaniowe).

Ważna jest także odpowiedź na pytanie, na jakiej architekturze będzie bazować nasz projekt:

1. *on-premise:* wszystkie urządzenia oraz dostępy zamkną się w naszej własnej architekturze w danym miejscu;
2. wykorzystanie usług chmurowych: być może chcemy, aby system (z wyjątkiem urządzeń końcowych) pracował w chmurze;
3. hybryda: chcemy połączenia dwóch powyższych punktów, dzieląc system na część pracującą w danym obiekcie oraz część wyniesioną do chmury (np. interfejs użytkownika).

Każdy wybór będzie pociągał za sobą inny zbiór wymagań i trochę inną drogę do ich spełnienia. Dlatego jest tak kluczowy już na samym początku koordynacji.

Nie unikniemy też różnego rodzaju szacowań ze strony zespołów cyberbezpieczeństwa. Niekiedy jest to naprawdę długa lista wymagań, co do których musimy się ustosunkować. Dlatego tak ważne, aby docelowego dostawcę wybierać uważnie, ponieważ wsparcie producenta/dostawcy będzie tutaj odgrywać kluczową rolę.

Zazwyczaj weryfikacji poddaje się dostawcę, łańcuch dostaw oraz samo rozwiązanie i aplikację danego rozwiązania.

Utrzymanie aplikacji w środowisku IT to proces złożony. Zwykle jest to zbiór wielu aktywności (a zatem i dokumentów) składających się na obraz całości. Jako specjaliści od bezpieczeństwa fizycznego/technicznego, ale i biznesowi właściciele projektu będziemy tutaj obarczeni dużą odpowiedzialnością za wkład merytoryczny. Najczęściej zadawane pytania mogą brzmieć następująco:

1. Kto jest odpowiedzialny za utrzymanie danego segmentu systemu?
2. Czy mamy wdrożone umowy SLA (*Service Level Agreement,* SLA – umowa o gwarantowanym poziomie świadczenia usług)?
3. Czy system został zintegrowany z system ticketowym?
4. Jaki jest model obsługi zgłoszeń serwisowych?
5. Jaki jest model wprowadzania zmian?
6. Pomoc przy wdrożeniu systemu badającego stan techniczny systemu (monitoring systemu).
7. Pomoc przy wdrożeniu dokumentu dotyczącego reagowania na incydenty i zachowania ciągłości działania.
8. Jaki jest model dostępu do systemu?

## Detale

Organizacja infrastruktury IT nie leży po stronie działów bezpieczeństwa fizycznego, niemniej jednak wkład merytoryczny z naszej strony bywa kluczowy, szczególnie jeśli niejako „dołączamy się" do sieci już istniejącej. Koordynacja oraz transparentność w przekazywaniu danych jest tutaj wskazana, m.in. przy:

1. Określaniu zapotrzebowania na liczbę portów – sprawa, która na pierwszy rzut oka wydaje się banalnie prosta, w rzeczywistości

może okazać się problematyczna. Szczególnie systemy CCTV lubią wykorzystywać dużą liczbę portów w przełącznikach. Sieci IT natomiast są budowane w oparciu o konkretne modele z dedykowaną konfiguracją. Domówienie nowych urządzeń w trybie ad hoc może być niemożliwe. Pociąga to za sobą nie tylko koszty, ale także długi czas oczekiwania na dostawę.

2. Wskazaniu przepustowości rozwiązania – tutaj sprawa wygląda podobnie do tej omawianej powyżej. Kamery o wysokiej rozdzielczości, nawet przy wykorzystaniu nowoczesnych kodeków obrazu, generują strumień danych, który z punktu widzenia sieci jest „ciężki". Gdy liczba kamer się zwiększa, wyzwanie gwałtownie wzrasta. I jakkolwiek ruch wewnętrzny w sieci zazwyczaj da się okiełznać, to ten na zewnątrz (np. przy rozwiązaniach czysto chmurowych lub hybrydowych) zaczyna być problematyczny. W czasach pędu do chmury, nie zawsze podpartego technicznymi analizami, takie podejście może okazać się niewykonalne.
3. Wskazaniu wszystkich interfejsów – większość producentów rozwiązań proponuje swoje usługi, które w części są dostępne przez instancje chmurowe. Z punktu widzenia cyberbezpieczeństwa jest niezwykle ważne, aby wskazać dokładną architekturę naszego rozwiązania tak, aby można było zidentyfikować wszystkie potencjalne wektory ataku.
4. Omówieniu szyfrowania oraz przepływu danych – idąc krok dalej, niezmiernie istotne jest opisanie tego, w jaki sposób dane od urządzeń końcowych, tj. kamery czy karty kontroli dostępu, trafiają do serwerów, instancji chmurowych, użytkowników końcowych. Jakich protokołów używamy, ruch jest jedno- czy dwustronny, jakie mechanizmy szyfrowania zostały wprowadzone w naszej aplikacji?
5. Omówieniu segmentacji oraz segregacji sieci – zazwyczaj systemy bezpieczeństwa powinny pracować w oddzielnych podsieciach wraz z opisanymi i wdrożonymi regułami omawiającymi, w jaki sposób odbywa się komunikacja pomiędzy nimi.

W odniesieniu do wszystkich omówionych kwestii kluczowe znaczenie ma nasz wkład merytoryczny. Zdaję sobie sprawę, że nie jest to zadanie proste ani przyjemne i wymaga od nas wyjścia poza pewną strefę komfortu. Pozwala jednak świadomie budować rozwiązania, które mają szansę się obronić i to nie tylko przed audytem. Uważam również, że to nam, jako właścicielom biznesowym, powinno najbardziej zależeć na zgodności z wymaganiami oraz na jak najkrótszym czasie wdrożenia. Faza przygotowania do projektu jest kluczową, aspekty ściśle związane ze światem IT mogą zostać łatwo pominięte ze względu na natłok informacji „z naszego podwórka". Należy jednak pamiętać, że są one tak samo istotne przy wdrożeniu, jak wybór odpowiednich kamer czy oprogramowania, stanowią przecież fundament, na którym każdy system jest budowany. ●


## Tomasz Dacka

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

# Powszechne błędy w podejściu do cyberbezpieczeństwa

Wiele firm popełnia błędy, które narażają je na poważne cyberzagrożenia. Przedstawiamy najczęściej występujące oraz sposoby ich unikania.

**Maciej Cieśla**

**LEKCEWAŻENIE RYZYKA.** Wiele małych i średnich przedsiębiorstw uważa, że hakerzy koncentrują się tylko na dużych firmach. To błędne przekonanie prowadzi do niedostatecznych inwestycji w zabezpieczenia. Cyberprzestępcy często kierują swoje ataki na małe i średnie przedsiębiorstwa, które nie mają odpowiednich polityk bezpieczeństwa. Warto zauważyć, że najczęściej stosowanymi metodami ataków są ataki socjotechniczne, takiej jak *phishing* (e-maile), *vishing* (telefony) czy *smishing* (SMS).

**BRAK PRZYGOTOWANIA NA ZAGROŻENIA WEWNĘTRZNE.** Wiele incydentów bezpieczeństwa wynika z błędów pracowników, takich jak przypadkowe kliknięcie w złośliwy link. Dlatego istotne jest wdrożenie narzędzi do monitorowania pracy z danymi oraz zarządzania urządzeniami mobilnymi. Pracownicy powinni być również edukowani w zakresie rozpoznawania zagrożeń.

**BRAK EDUKACJI PRACOWNIKÓW.** Nie organizuje się szkoleń z zakresu cyberbezpieczeństwa, a nawet jeśli już są, to po ich przeprowadzeniu okazuje się, że 25% „wyedukowanych" pracowników nadal popełnia błędy i niewłaściwie udostępnia dane firmowe. Szkolenia powinny być regularnie aktualizowane i dostosowywane do zmieniającego się obszaru zagrożeń w kontekście danej organizacji.

**SŁABE HASŁA I BRAK WIELOSKŁADNIKOWEJ AUTORYZACJI.** To kolejny słaby punkt w zabezpieczeniach wielu przedsiębiorstw. Organizacje często lekceważą te podstawowe środki ochrony, co ułatwia cyberprzestępcom dostęp do systemów. Warto wprowadzić politykę silnych haseł oraz wymagać dodatkowych form uwierzytelnienia.

**BRAK STRATEGII OCHRONY DANYCH.** W wyniku tego zazwyczaj dochodzi do naruszeń. Firmy często nie mają jasno określonej strategii ich protekcji, co prowadzi do chaosu w zarządzaniu informacjami. Niezbędne jest określenie, które dane są najbardziej wrażliwe i wymagają szczególnej ochrony, oraz przeprowadzenie szczegółowej analizy ryzyka. Wdrożenie systemów DLP *(Data Loss Prevention)* i szyfrowania danych to kluczowe kroki w zabezpieczaniu informacji.

**NIEPRAWIDŁOWE ZARZĄDZANIE UPRAWNIENIAMI DOSTĘPU.** Nadmierna liczba kont administratorów oraz aktywne konta byłych pracowników mogą prowadzić do poważnych naruszeń bezpieczeństwa. Regularne przeglądanie uprawnień dostępu oraz stosowanie zasady najmniejszych uprawnień jest kluczowe, aby zminimalizować ryzyko naruszenia bezpieczeństwa.

**BRAK KOPII ZAPASOWYCH.** Bezpieczeństwo nie może być zbudowane solidnie, jeśli w organizacji nie tworzy się kopii zapasowych. Brak takich kopii lub ich nieregularne tworzenie to kolejny błąd, który może prowadzić do utraty danych. Kopie zapasowe powinny być tworzone regularnie i przechowywane w bezpiecznym miejscu. Należy także testować ich odtworzenie zgodnie z planami przywracania ciągłości działania.

**SPOCZYWANIE NA LAURACH.** W niektórych firmach nadal panuje przekonanie, że po wdrożeniu podstawowych zabezpieczeń są już bezpieczne. Jednak cyberzagrożenia ewoluują, dlatego ważne jest ciągłe monitorowanie trendów i aktualizacja polityk bezpieczeństwa. Regularne audyty bezpieczeństwa mogą pomóc w identyfikacji luk i zagrożeń. W obliczu rosnących zagrożeń cybernetycznych organizacje muszą być świadome najczęstszych błędów popełnianych w zakresie cyberbezpieczeństwa. Edukacja pracowników, wdrażanie odpowiednich narzędzi oraz ciągłe monitorowanie sytuacji to kluczowe elementy skutecznej strategii ochrony przed cyberatakami. Ignorowanie tych kwestii może prowadzić do poważnych konsekwencji finansowych i obniżenia reputacji dla firmy, w tym do utraty kluczowych danych.

**Polski Związek Pracodawców Ochrona**
ul. Koszykowa 61, 00-667 Warszawa
www.pzpochrona.pl
biuro@pzpochrona.pl

# Akademia Bezpieczeństwa

Instytucje finansowe są celem nieustających ataków cyberprzestępców. Jak wynika z raportu CERT*, to właśnie one stanowią 25% wszystkich odnotowanych cyberincydentów. W całym 2023 r. było ich niemal 19 tys. i to m.in. dlatego mBank jako jeden z liderów bankowości w Polsce zorganizował wydarzenie, które miało na celu przybliżyć pracownikom banku, jakie zagrożenia czyhają na nich i na ich klientów. O wnioskach z Akademii Bezpieczeństwa rozmawialiśmy z **Jarosławem Górskim**, dyrektorem departamentu bezpieczeństwa mBanku.

**Banki są najlepiej zabezpieczonymi podmiotami, jeśli chodzi o cyberbezpieczeństwo – takie zdanie wielokrotnie padło ze sceny. Co dla banku jest największym wyzwaniem w przestrzeni wirtualnej?**

Infrastruktura banków i bankowość elektroniczna mają wysoki poziom zabezpieczeń technologicznych. Przestępcy szukają słabych punktów u użytkowników, a hakerzy przeprowadzają ataki socjotechniczne, dzwoniąc i podszywając się pod pracownika banku czy służby mundurowe. Niestety, protokoły związane z identyfikacją dzwoniącego są archaiczne, dlatego staramy się edukować klientów. Ważne jest, żeby zadać sobie pytanie: czy dzwoni do mnie bank? Jeżeli dzwoni do nas pracownik banku, to w aplikacji mBanku otrzymamy komunikat z imieniem i nazwiskiem pracownika. W przypadku wiadomości mailowej, jeżeli korzystamy ze skrzynek pocztowych, to przy wiadomościach nadanych z mBanku znajduje się oznaczenie „sprawdzony nadawca", co gwarantuje autentyczność e-maila. Jeżeli otrzymaliśmy e-maila bez takiego oznaczenia, nadawca podszywa się pod mBank. Należy to zgłosić na infolinię i nigdy nie klikać w linki w wiadomości, nie otwierać załączników. O tym, jak rozpoznawać ataki i jak sobie z nimi radzić, mówimy w naszych kampaniach dotyczących bezpieczeństwa w sieci.


**Jak wygląda system regulacji w sektorze finansowym, jeśli chodzi o cyberbezpieczeństwo?**

Obowiązuje nas cały szereg regulacji krajowych, europejskich i światowych. Do tego dochodzą rekomendacje i komunikaty KNF, które miejscami są bardzo wymagające. Ostatnio wszystkie banki pracują nad implementacją wymagań DORA, która wchodzi w życie na początku 2025 roku. DORA skupia się na bezpieczeństwie i systemie zarządzania dostawcami. Wynika to z faktu, że coraz więcej ataków odbywa się przez łańcuchy dostaw. Jest tego dużo, ale dostosowując bank do regulacji, lepiej spełniamy wysokie standardy cyberbezpieczeństwa.

**Co powinno się znaleźć w polskich procedurach zabezpieczeń instytucji finansowych jako kluczowych dla funkcjonowania państwa?**

Gwarancja niezbędnych do realizacji procesów kluczowych zasobów. Do utrzymania usług bankowości potrzebne są zasoby i to nie tylko w postaci wyszkolonych pracowników. Składa się na to cały ekosystem, czyli wykwalifikowani pracownicy, infrastruktura IT, łączność, sprzęt, energia czy paliwo. Bez tego bank nie będzie w stanie realizować procesów kluczowych, co spowoduje zatrzymanie systemu płatniczego. Dlatego tak ważne jest ustalenie już teraz, w czasie pokoju, na co banki mogą liczyć w razie konfliktu i czy zostaną im zagwarantowane dostępy do zasobów niezbędnych do funkcjonowania. Jakie są priorytety i jakim organizacjom przysługują, w jakiej kolejności. Wszystko to powinno być poparte odpowiednimi gwarancjami. Dziś rozmawiamy podczas podobnych wydarzeń jak nasze Dni Bezpieczeństwa, niewątpliwie jest jeszcze sporo do zrobienia w tym zakresie. ●

Rozmawiała: Aleksandra Czapska

* Raport CERT z 2024 r. https://www.parkiet.com/oszczedzanie/art41249301-instytucje-finansowe-w-polsce-sa-niemal-codziennie-narazone-na-cyberataki

# Systemy VMS a cyberbezpieczeństwo

W dobie dynamicznie zmieniających się regulacji prawnych oraz rosnących wymagań w zakresie cyberbezpieczeństwa, szczególną uwagę warto poświęcić systemom VMS *(Video Management System)*. Współczesne wersje systemów do zarządzania materiałem wizyjnym coraz częściej oferują możliwość zdalnego dostępu uprawnionym użytkownikom. Takie rozwiązania, choć wygodne, rodzą jednak pytania o bezpieczeństwo i ryzyko nieautoryzowanego dostępu.
O wyzwania i przyszłość systemów VMS Aleksandra Czapska zapytała Piotra Łancewicza, eksperta ds. bezpieczeństwa.

## Jakie wyzwania stoją dziś przed producentami systemów VMS, a na jakie kwestie powinien zwrócić uwagę użytkownik?

Akurat systemy VMS to mój konik w branży security, bo to taki centralny punkt dowodzenia w wielu obiektach. Sporo czasu spędzam na testowaniu nowych systemów zarządzania materiałem wizyjnym. Jedną z moich obserwacji jest to, że to liderzy rynkowi wyznaczają ścieżki, którymi podąża większość branży. Moim zdaniem obecnie kluczowe tematy to: cyberbezpieczeństwo, otwartość oraz wykorzystanie sztucznej inteligencji.

## Co zmieniło się w kontekście cyberbezpieczeństwa, jeśli chodzi o systemy VMS?

Cyberbezpieczeństwo to kluczowy element, nawet jeśli brzmi to jak tautologia. Przez lata obserwowałem, jak systemy zabezpieczeń funkcjonowały jako odrębne byty, często nieobjęte polityką IT organizacji. Było to zazwyczaj spowodowane tym, że eksperci od technicznych systemów zabezpieczeń, kamer czy kontroli dostępu, rzadko są też specjalistami od bezpieczeństwa IT. W procesie projektowania rozwiązań bezpieczeństwa natomiast rozwiązanie powinno spełniać wymogi zarówno bezpieczeństwa technicznego, jak IT. Wiele kamer i systemów VMS dostępnych na rynku nie spełnia założeń cyberbezpieczeństwa, co utrudnia ich wdrożenie. W takich sytuacjach pojawia się pytanie: czy lepiej wybrać tańsze rozwiązanie, które IT będzie musiało dodatkowo zabezpieczyć kosztownymi narzędziami, czy droższe, ale w pełni pasujące do firmy czy szerzej obiektu.

## A jak ma się do tego rozwój technologii chmurowych?

Usługi chmurowe w branży security rozwijają się stosunkowo powoli, co wynika z obaw przed udostępnianiem ich w Internecie. Słyszałem wiele opinii, że podłączenie systemu do sieci to otwarcie drzwi każdemu potencjalnemu intruzowi. To mit. Wszystko zależy od odpowiedniego zabezpieczenia i specyfiki obiektu. Przykładowo, firma Milestone zaprezentowała niedawno usługę XProtect Remote Manager – świetne narzędzie, które umożliwia administratorom zdalne zarządzanie systemem i jego monitorowanie przez przeglądarkę internetową, bez konieczności instalacji dodatkowego oprogramowania. To właśnie jest przykład podejścia *single pane of glass* – wszystko w jednym miejscu, dostępne w prosty sposób. Dodatkowo Milestone wprowadza rozwiązanie *Kite* – system umożliwiający zapis obrazu w chmurze. To innowacyjne rozwiązanie, a chmura to przyszłość, której nie należy się obawiać.

## Otwartość systemu – jak rozumieć to w kontekście VMS?

Otwartość to wolność – ma ona moim zdaniem dwa kluczowe aspekty. Pierwszy to *security by openness* – bezpieczeństwo przez otwartość. Polega ono na stosowaniu znanych technik, jak algorytmy szyfrowania. Ich otwartość oznacza, że są stale testowane przez ekspertów na całym świecie. Jeśli któraś technika się nie sprawdzi, branża szybko reaguje, co podnosi poziom bezpieczeństwa. Przeciwieństwem tego podejścia jest *security through obscurity*, czyli ukrywanie mechanizmów działania systemu. Moim zdaniem to mało efektywne i wymaga od działów IT dodatkowej pracy, np. na własne testy penetracyjne. Drugi aspekt otwartości to integracja. Systemy muszą wymieniać informacje – najlepiej dwukierunkowo. Milestone jest liderem w tym zakresie, oferując bogate narzędzia do integracji, dokumentację i wsparcie dla deweloperów. Na przykład Milestone PS Tools to narzędzie pozwalające na zarządzanie VMS za pomocą linii komend, co otwiera możliwość automatyzacji, np. migracji dużych systemów. Migracja 10 kamer ręcznie to nic wielkiego, ale 500? Automatyzacja to oszczędność czasu i pieniędzy.

## Wspominałeś o wykorzystaniu sztucznej inteligencji. Jaką rolę odgrywa w VMS?

Sztuczna inteligencja zmienia zasady gry. Milestone działa na wielu frontach – od udziału w pracach legislacyjnych, aby nie naruszać praw człowieka, po współpracę z firmami takimi jak Nvidia, które wykorzystują GPU do najnowocześniejszych modeli AI. Kilka lat temu Milestone przejął firmę BriefCam, lidera w analityce wideo. Proces ich integracji trwa, a już teraz systemy AI pozwalają na wyszukiwanie obiektów według określonych kryteriów czy wykrywanie nietypowych zachowań. To tylko kwestia czasu, może 2-4 lat, zanim będziemy mogli wydawać polecenia typu „znajdź złodzieja" i system zrobi to za nas. Największa zaleta AI to jednak oszczędność czasu. Przy setkach godzin nagrań wideo to bardzo ważne. Na przykład w australijskim mieście Hobart, dzięki rozwiązaniom Milestone czas wyszukiwania materiału skrócił się o 95%. Dodając do tego narzędzia, takie jak Video Synopsis opracowane przez BriefCam, możliwe jest przeglądanie 24 godz. nagrań w zaledwie 10-15 minut – i to bez przyspieszania wideo. To prawdziwa rewolucja. ●


**Milestone Systems**
Banemarksvej 50 C, DK-2605 Brondby, Denmark
Tel. +45 88 300 300
www.milestonesys.com

# W grupie na grubie!*

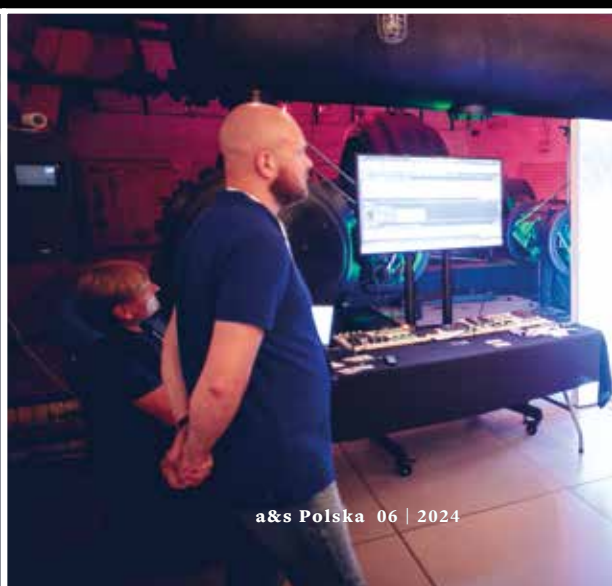
**Jesienna edycja Security Bootcamp odbyła się 9-10 października w Zabrzu, w absolutnie wyjątkowej scenerii. Security managerowie tym razem spotkali się... 320 metrów pod ziemią, w korytarzach zabytkowej kopalni „Guido". Tam rozwiązywali zadania przygotowane przez partnerów, wymieniali się wiedzą i nawiązywali nowe kontakty.**

Niemal 60 uczestników podzielono na drużyny, które rywalizowały ze sobą w konkurencjach przygotowanych na poszczególnych stoiskach. Stawką były atrakcyjne nagrody ufundowane przez partnerów dla najlepszych teamów. Intensywnie rozpoczął się pierwszy dzień. Goście zjechali głęboko pod ziemię autentyczną szolą górniczą. Mieli chwilę na zwiedzanie zabytkowych korytarzy i pomieszczeń kopalni, w tym pubu położonego najgłębiej względem poziomu morza. Posileni tradycyjnym śląskim obiadem ruszyli do zadań, które czekały na nich na stoiskach pięciu partnerów tego wydarzenia: Genetec, Hanwha Vision, Novatel, Roger i Securitas.

Securitas zaprosił do gry w ciemności, nawiązując do naturalnych warunków w kopalni. Celem było zlokalizowanie obiektów o niskiej i wysokiej temperaturze. Z pomocą termowizji uczestnicy przekonali się, jak różne rozwiązania technologiczne sprawdzają się w ekstremalnych warunkach. – *Chcieliśmy pokazać, że choć niektóre technologie nie sprawdzają się, inne działają niezawodnie, zapewniając bezpieczeństwo i skuteczność w trudnych sytuacjach. Nasze rozwiązania zawsze odpowiadają na realne potrzeby* – podkreślił **Marek Skowronek**.

Genetec zaproponował zaprojektowanie systemu bezpieczeństwa, który, oparty na najnowszych rozwiązaniach chmurowych, bezszwowo łączy monitoring wizyjny, kontrolę dostępu i rozpoznawanie tablic. – *Uczestnicy mogli przejść przez cały proces rejestracji nowej kamery w chmurze, przejrzeć system pod kątem monitorowania obszaru dzięki wtyczkom restricted security area oraz wziąć udział w całym procesie przygotowania instalacji* – wyjaśnił, na czym polega ich zadanie, **Bartłomiej Bzymek**.

* Gruba w gwarze śląskiej oznacza kopalnię.





Hanwha Vision przygotowała dla odwiedzających grę z wykorzystaniem najnowszych modeli kamer firmy, wyposażonych w AI i MQTT. Kamery te umożliwiają integrację z różnymi elementami wykonawczymi i rejestrującymi, co przekłada się na poprawę bezpieczeństwa w obiektach zarówno przemysłowych, jak i prywatnych. – *Przygotowaliśmy pewną historię inżyniera bezpieczeństwa w kopalni, który zaginął w niewyjaśnionych okolicznościach. Zadaniem uczestników było – na podstawie jego notatek – uzyskanie informacji, co się z nim stało, oraz odtworzenie projektu monitoringu wizyjnego, który wykonywał w kopalni* – zachęcał do udziału **Łukasz Lik**.

Novatel przyjął natomiast inną strategię i na swoim stoisku przedstawił bardzo bogaty wybór interkomów. Największe zainteresowanie wśród odwiedzających wzbudziły pętle indukcyjne. – *Wisienką na torcie jest kwestia dostępności – pokazujemy pętlę indukcyjną. Myślę, że systemy radiowe i interkomowe także były czymś takim, co było oceniane jako potencjalnie przydatne. Ciekawe były też reakcje na moje pytanie, czy firmy już się dostosowują do potrzeb osób słabosłyszących i stosują pętlę indukcyjną* – zdradził **Tomasz Jaeschke**.

Roger, który po raz pierwszy gościł na Security Bootcampie, ograniczył się do jednego, ale jakże przydatnego elementu. – *Przyjechaliśmy pokazać nasze oprogramowanie VISO SMS. To platforma służąca do monitorowania, wizualizacji i zarządzania bezpieczeństwem w obiektach. VISO SMS współpracuje z systemem kontroli dostępu RACS 5 i umożliwia integrację z innymi systemami zabezpieczeń. Pokazaliśmy również, jak w prosty sposób skopiować kartę o niskim stopniu zabezpieczenia* – powiedział **Łukasz Kanarek**.


**Marcin Przondziono**
Aptiv

Pochodzę z Katowic, jestem Ślązakiem z dziada pradziada. W branży pracuję ponad 20 lat, a to mój pierwszy Bootcamp. Jeśli chodzi o konkurencje, były bardzo, bardzo fajne. Przekraczacie oczekiwania!

**Aneta Sadach**
Uniwersytet Łódzki

Bootcamp jest fantastycznym spotkaniem, gromadzi wielu uczestników, z którymi można porozmawiać i wymienić się doświadczeniami. Są tu fantastyczni przedstawiciele firm, od których można wiele się dowiedzieć. Skorzystałam dzisiaj z oferty jednego z wystawców, która dała mi do myślenia, co powinnam u siebie poprawić. Bardzo serdecznie polecam, to fantastyczna impreza, fantastyczna energia, fantastyczni ludzie.

**Łukasz Obiedziński**
Ruch

Najbardziej podobały mi się dwa stanowiska – Genetec i Hanwha – dlatego że to są rzeczy, którymi się interesuję, czyli telewizja dozorowa i wszelkie nowe rozwiązania oraz integracja, unifikacja ich w jedną całość.

**Tomasz Grzelak**
DHL Supply Chain

W takim gronie i z taką liczbą ekspertów od bezpieczeństwa jesteśmy jak najbardziej bezpieczni. Konkurencje na Bootcampie świetne, superzabawa, adrenalina, emocje. Mogliśmy się zintegrować i dobrze bawić.

**Dawid Karczewski**
Grupa LipCo Foods

Od 12 lat jestem w branży security, cały czas rozwijam swoją pasję. Na Bootcampie jestem po raz pierwszy. Wydarzenie było zorganizowane bardzo profesjonalnie: świetni ludzie, wymiana informacji, zwłaszcza na temat innowacji, które mogę przełożyć na działalność Grupy.

Drugi dzień był już mniej intensywny – po śniadaniu uczestnicy udali się na omówienie case study, które poprowadził zastępca redaktor naczelnej „a&s Polska" Jan T. Grusznic. Po warsztacie na chętnych czekała ostatnia niespodzianka: możliwość wzięcia udziału w kameralnej wycieczce po zakamarkach nieczynnej kopalni.
Jakie były wrażenia gości i uczestników tego wyjazdu? Bardzo pozytywne! W rozmowach kuluarowych podkreślano zwłaszcza wagę tych spotkań na rzecz integracji branży i możliwości wymiany doświadczeń, a także, co nie mniej istotne, nawiązania nowych kontaktów zawodowych. Bootcamp to także niepowtarzalna okazja do zapoznania się z najnowszymi technologiami poszczególnych producentów i przetestowania ich w praktyce oraz, co równie ważne, w wyjątkowo przyjaznej atmosferze i bardzo atrakcyjnych okolicznościach.

PZPO

# Konferencja Branży Ochrony już po raz 25.

**29–30 października 2024 roku Polska Izba Ochrony zorganizowała 25. Jubileuszową Konferencję Branży Ochrony, która odbyła się w hotelu Windsor w Jachrance. Wydarzenie zgromadziło specjalistów z sektora ochrony oraz przedstawicieli instytucji państwowych i firm prywatnych. Głównym tematem konferencji było „Branża ochrony w zapewnieniu bezpieczeństwa infrastruktury krytycznej w obliczu podwyższonego zagrożenia państwa".**

Prelegenci omówili kluczowe zagadnienia, takie jak cyberbezpieczeństwo i ochrona infrastruktury krytycznej oraz zaprezentowali nowoczesne technologie ochronne. Wystąpienia wzbogacono panelem dyskusyjnym z udziałem zaproszonych ekspertów. Uczestnicy konferencji mieli również możliwość odwiedzenia strefy wystawców z najnowszymi rozwiązaniami technologicznymi w branży ochrony.

Spotkanie zwieńczyła gala jubileuszowa z okazji 30-lecia Polskiej Izby Ochrony połączona z aukcją charytatywną na rzecz Fundacji „Ochrona i Pomoc", podczas której można było wylicytować m.in. obraz z wizerunkiem Julii Szeremety, srebrnej medalistki w boksie podczas tegorocznych Igrzysk Olimpijskich w Paryżu.

Drugiego dnia odbył się trening charytatywny z mistrzem, podczas którego uczestnicy mieli okazję wykonać ćwiczenia sprawnościowe wprowadzające w tajniki sztuki pięściarskiej. Każdy uczestnik treningu samą swoją obecnością wsparł Fundację „Ochrona i Pomoc".

Konferencja okazała się wyjątkową okazją do wymiany doświadczeń i wzmocnienia współpracy w branży ochrony, szczególnie w kontekście współczesnych wyzwań, a samo wydarzenie odnotowało rekordową w historii tej imprezy liczbę uczestników i partnerów. ●

SHRACK SECONET

# Wszystko o bezpieczeństwie pożarowym

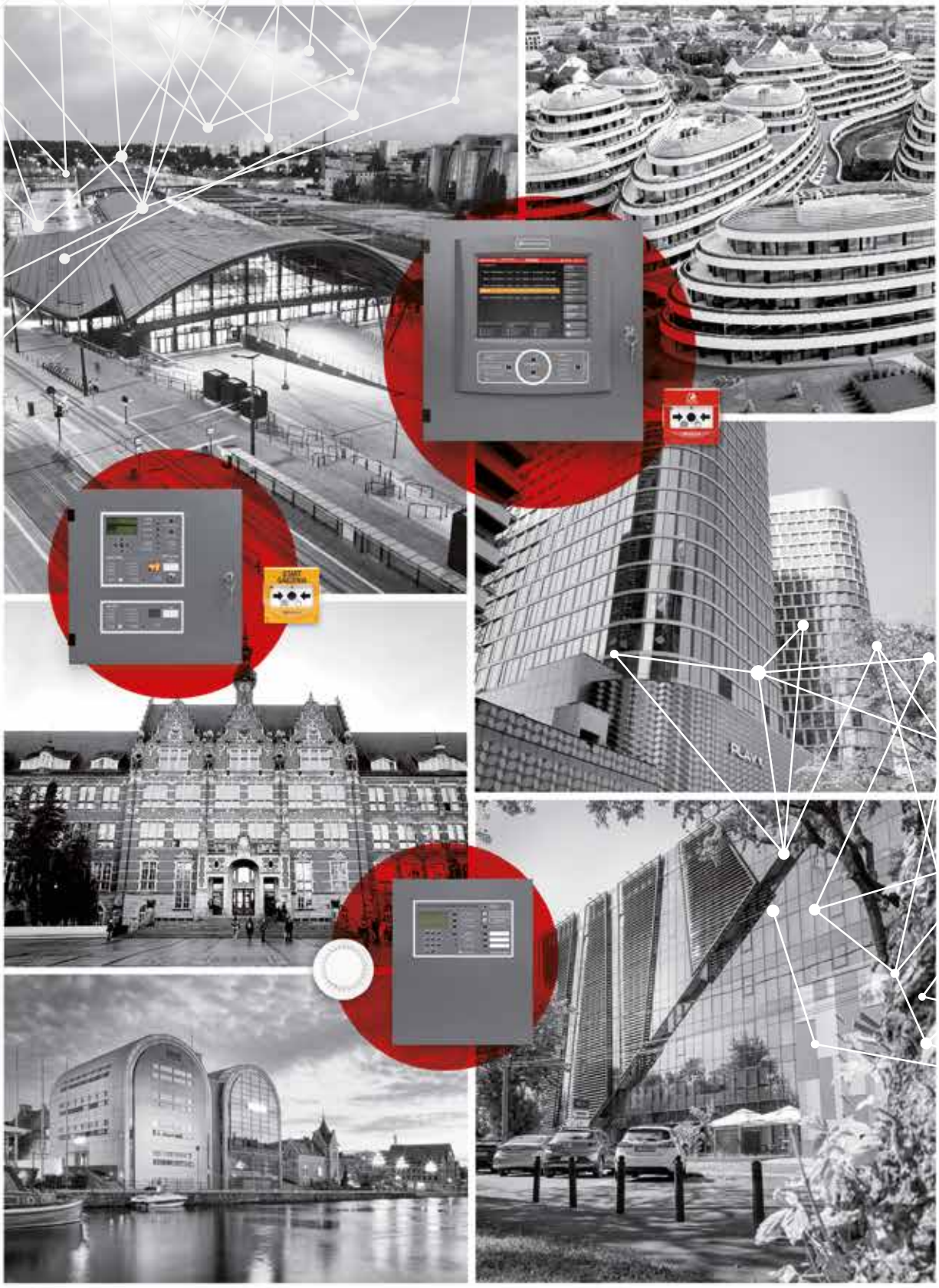
**XI edycja Ogólnopolskich Dni Zintegrowanych Systemów Bezpieczeństwa Pożarowego – Schrack Seconet i Partnerzy odbyła się w dniach: 9-10 października 2024 r. w hotelu Windsor w Jachrance. Wydarzenie zorganizowała firma Schrack Seconet Polska, światowy producent zaawansowanych technologicznie systemów bezpieczeństwa pożarowego, we współpracy z innymi liderami branży (11 Partnerów Technologicznych!) oraz najlepszymi ekspertami reprezentującymi najbardziej opiniotwórcze instytuty w kraju.**

Tegoroczna edycja pozostała w formule merytorycznych spotkań. Uczestnicy mieli okazję zapoznać się ze wszystkimi produktowymi nowościami, z aktualnymi wytycznymi i dobrymi praktykami w zakresie projektowania, realizacji i eksploatacji systemów bezpieczeństwa. Nie zabrakło szczegółowo omówionego współdziałania systemów bezpieczeństwa i instalacji technicznych dla różnych typów zagrożeń w obiektach budowlanych. Przeanalizowano studia przypadków, polecając zalecenia dla projektantów, instalatorów, inwestorów i użytkowników w zakresie integracji systemów bezpieczeństwa.

Podczas dwóch dni wydarzenia słuchacze zapoznali się z najnowszymi wytycznymi dotyczącymi projektowania, instalacji oraz użytkowania takich systemów, jak: sygnalizacji pożarowej, sterowania gaszeniem, DSO, kontroli rozprzestrzeniania dymu i ciepła, integracji urządzeń przeciwpożarowych (SIUP), sterowania urządzeniami przeciwpożarowymi i innymi instalacjami użytkowymi obiektu, dozoru wizyjnego, kontroli dostępu, okablowania strukturalnego i przemysłowych rozwiązań infrastruktury sieciowej.

Wsparcie merytoryczne podczas tegorocznej edycji szkolenia zapewnili Partnerzy Merytoryczni: Stowarzyszenie Inżynierów i Techników Pożarnictwa – Izba Rzeczoznawców, Polska Izba Systemów Alarmowych, Instytut Bezpieczeństwa Pożarowego NODEX, HESTIA Loss Control, VdS Schadenverhütung oraz eksperci reprezentujący Centrum Naukowo-Badawcze Ochrony Przeciwpożarowej – Państwowy Instytut Badawczy. ●

POLON-ALFA



*tradycyjnie* KOMPLEKSOWA OCHRONA

tysięcy obiektów w kraju i za granicą

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

AXIS COMMUNICATIONS

# Kamery typu turret o doskonałej jakości obrazu do 4K

**Axis Communications przedstawia nową generację kamer z serii AXIS M31. Te kompaktowe i dyskretne kamery zapewniają wygodną instalację zarówno wewnątrz, jak i na zewnątrz.**

Kamera AXIS M3125-LVE oferuje rozdzielczość 2 Mpix, a AXIS M3126-LVE i AXIS M3128-LVE zapewniają odpowiednio 4 Mpix i 8 Mpix. WDR zachowuje szczegóły, gdy w scenie znajdują się zarówno jasne, jak i ciemne obszary, a technologia OptimizedIR umożliwia dozór w całkowitej ciemności.

Te kamery oparte na sztucznej inteligencji, wyposażone w procesor głębokiego uczenia (DLPU), umożliwiają przeprowadzanie zaawansowanych analiz na brzegu sieci. Przykładowo, w systemie znajduje się AXIS Object Analytics, preinstalowany program do wykrywania, klasyfikowania, śledzenia i liczenia obiektów, takich jak ludzie i pojazdy. DLPU dostarcza również cennych metadanych, ułatwiając szybkie, łatwe i wydajne wyszukiwanie kryminalistyczne w wideo na żywo lub nagranym wcześniej.

Dzięki wszechstronnemu zestawowi akcesoriów montażowych, te płaskie kopuły można montować na ścianach lub sufitach. Kompaktowe i dyskretne, są dostępne w kolorze czarnym lub białym. Ponadto, Axis Edge Vault, sprzętowa platforma cyberbezpieczeństwa, zabezpiecza urządzenie i chroni poufne dane przed nieautoryzowanym dostępem. Kamery te oferują certyfikat FIPS 140-3 poziomu 3, bezpieczne przechowywanie i obsługę kluczy kryptograficznych.

Ponadto każda kamerą oferuje:

- doskonałą jakość obrazu w rozdzielczości do 4K,
- WDR, Lightfinder i OptimizedIR,
- obudowę w kolorze czarnym lub białym
- analitykę materiału wizyjnego opartą na sztucznej inteligencji,
- wbudowane funkcje cyberbezpieczeństwa dzięki Axis Edge Vault. ●

SAFETY PROJECT

# VII Międzynarodowy Kongres Naukowo-Techniczny SAFE PLACE 2024

**Za nami niezwykle intensywna i merytoryczna VII edycja Międzynarodowego Kongresu Naukowo-Technicznego Safe Place 2024. Tegoroczna edycja zgromadziła rekordową liczbę uczestników blisko 450 osób. To dowód na rosnące zainteresowanie zagadnieniami bezpieczeństwa obiektów i przestrzeni.**

Kongres otworzyły wystąpienia ekspertów, które rzuciły nowe światło na aktualne wyzwania związane z zagrożeniami hybrydowymi, kryminalnymi oraz implementacją kluczowych dyrektyw, takich jak NIS-2, CER i DORA. Nie zabrakło praktycznych rekomendacji, podanych z międzynarodowej perspektywy przez wybitnych specjalistów, w tym dyrektora RCB Zbigniewa Muszyńskiego, gen. dyw. w st. spocz. prof. Bogusława Packa czy Itaya Levina, reprezentującego Intelligence Driven Security. Uwagę uczestników przyciągnęły:

- Debata ekspercka na temat przygotowania do wojny oraz zagrożeń hybrydowych i kryminalnych, moderowana przez jednego z organizatorów Kongresu.


- Zawody strzeleckie organizowane we współpracy z Militaria.pl i Safety Project, które zakończyły się uroczystym wręczeniem nagród.
- Dynamiczny pokaz Grupy TAURUS OCHRONA, który dostarczył niezapomnianych emocji.
- Warsztaty praktyczne, podczas których uczestnicy mogli ćwiczyć reagowanie na zamachy, poznawać innowacje technologiczne oraz doskonalić umiejętności z zakresu pierwszej pomocy.

Dzień warsztatowy okazał się jednym z największych sukcesów tegorocznej edycji. Równolegle odbywały się cztery moduły praktyczne, w tym prezentacje rozwiązań takich firm, jak Bosch Security and Safety Systems, GINA Software czy IntelexVision.

Podczas sesji finałowej zaprezentowano wnioski oraz rekomendacje do raportu dotyczącego stanu bezpieczeństwa obiektów i przestrzeni, podkreślając konieczność budowania odporności infrastruktury krytycznej.

– *Nie byłoby tak spektakularnego Kongresu bez zaangażowania naszych partnerów: technicznych, merytorycznych, medialnych oraz partnera motoryzacyjnego. Ich wkład w jakość i prestiż wydarzenia jest nieoceniony. Wielkie podziękowania kierujemy również do uczestników, którzy swoją aktywnością i zaangażowaniem uczynili Safe Place 2024 niezapomnianym wydarzeniem* – powiedział mjr rez. dr hab. inż. Jarosław Stelmach (na zdjęciu obok).

Organizatorzy już teraz zapraszają do udziału w Safe Place 2025! ●

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 szyfrowaną transmisję przy użyciu TLS1.2. Dostępne urządzenia oferują od 8 do 32 kanałów IP w wersji PLUS.**

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

Obsługa kamer 8 MP (4K) z kompresją H.265 HEVC to już standard w tego typu urządzeniach. Jednak dzięki zwiększonym wymogom bezpieczeństwa rejestratory są zgodne z NDAA, doskonale wpisują się też w najnowsze wymagania związane z certyfikatami PCI DSS. Zastosowanie modułu TPM zapewnia kompleksowe szyfrowanie strumieni i poleceń za pomocą zintegrowanych kluczy kryptograficznych. Wybierając rozwiązania z serii 35 Honeywell, wchodzimy na wyższy poziom cyberbezpieczeństwa.

Urządzenia są dostępne w portfolio Linc Polska. ●

ROGER

# Integracja systemu RACS 5 z kamerami LPR MOBOTIX

**MOBOTIX to uznany producent zaawansowanych systemów monitoringu wizyjnego, należący do grupy Konica Minolta. W ofercie firmy znajdują się m.in. kamery LPR, które są przystosowane do współpracy z systemami kontroli dostępu, w tym również z systemem RACS 5.**

Integracja RACS 5 z kamerami LPR MOBOTIX pozwala na automatyzację procesu kontroli dostępu dla pojazdów. Dzięki współpracy tych rozwiązań możliwe jest uzyskanie pełnej kontroli nad dostępem do obiektów przy wykorzystaniu zaawansowanego monitoringu wizyjnego.

Integracja tych rozwiązań niesie ze sobą liczne korzyści. Do najważniejszych z nich zaliczyć można:

- automatyczne otwieranie bram na podstawie odczytu tablic rejestracyjnych;
- zwiększenie bezpieczeństwa dzięki precyzyjnej identyfikacji i wyeliminowaniu możliwości wjazdu nieupoważnionych pojazdów;
- elastyczne reguły dostępu dostosowane do indywidualnych potrzeb;
- automatyzowane raporty i alerty dotyczące zdarzeń kontrolnych.

Możliwość automatyzacji kontroli dostępu dla pojazdów przy jednoczesnym zwiększeniu poziomu bezpieczeństwa sprawia, że rozwiązanie to sprawdzi się w wielu obszarach i sektorach rynkowych. Integracja systemu RACS 5 z kamerami LPR MOBOTIX znajduje swe zastosowanie m.in. w parkingach i garażach, obiektach przemysłowych, firmach i biurach oraz obiektach logistycznych. ●

HANWHA VISION

# Wielokierunkowe kamery AI

**Wielokierunkowe kamery AI łączą kilka kamer w jednym urządzeniu, oferując korzyści trzech, czterech, a nawet pięciu kamer AI bez związanych z tym kosztów obsługi kilku urządzeń. Główną zaletą wielokierunkowych kamer AI jest opłacalność, ponieważ firmy inwestują tylko w jeden zestaw sprzętu, okablowanie i jedną licencję VMS (systemu zarządzania materiałem wizyjnym).**

Wielokierunkowe kamery AI są idealne do monitorowania dużych i złożonych obszarów, w tym centrów miast, lotnisk, skrzyżowań i ruchliwych placów logistycznych. Przykładowo 5-kanałowy model PNM-C34404RQPZ zapewnia operatorom rozległy zasięg przy użyciu kamer PTZ i kamer stacjonarnych w jednym połączeniu, ze szczegółową jakością obrazu do 4K i zaawansowanym pakietem analityki AI.

Kamery te mogą być również dobrze dostosowane do środowisk wewnętrznych, takich jak handel detaliczny, biura i przestrzenie o niskim suficie. Modele AI Mini są kompaktowe i dyskretne, co oznacza, że można je bezproblemowo zainstalować w miejscach o niskim suficie lub tam, gdzie priorytetem jest estetyka. Urządzenia te dostarczają do czterech

różnych strumieni wideo, dzięki czemu operatorzy mogą łatwo monitorować scenę bez konieczności przełączania się między kamerami przy zachowaniu szerszego pola widzenia w porównaniu do pojedynczej kamery.

Skuteczność dozoru przy słabym oświetleniu może spadać, ale nowoczesne kamery wielokierunkowe są wyposażone w niezależne strefy podczerwieni (IR) i funkcje dalekiego zasięgu IR, zapewniając wyraźny obraz nawet w całkowitej ciemności. W całej gamie kamer wielokierunkowych Hanwha Vision dostępne są opcje, umożliwiające operatorom ręczną regulację intensywności każdej strefy podczerwieni, co zapobiega odbiciom i optymalizuje jakość obrazu, zapewniając wyraźny obraz miejsc niezależnie od warunków oświetleniowych.

Wielokierunkowe kamery AI są idealnym rozwiązaniem dla firm potrzebujących kompleksowego i inteligentnego dozoru, bez kosztownej i czasochłonnej instalacji i konserwacji większej liczby kamer ●

# Może to przeziębienie, a może covid?

**Listopadowy poranek, a w zasadzie prawie noc. Piąta rano nie była ulubioną porą dnia Krzysztofa Jastrzębskiego, menedżera agencji ochrony strzegącej – m.in. kilkunastu sklepów wielkopowierzchniowych, należących do dużej międzynarodowej sieci sprzedaży. Nie było jednak wyboru. Czas do roboty.**

*Matko jedyna, psa by nie wygonił, powiedział do siebie w duchu Krzysztof, patrząc na wredny deszcz lejący za oknem. Na zewnątrz było ciemno i ponuro. Zgniły wyż okazał się niestety trafną prognozą pogody.*
*– Chodź, Fafik, pójdziemy na spacer. – Głos Krzysztofa pobrzmiewał sztucznym entuzjazmem. Fafik, przygarnięty w chwili Krzysztofowej słabości mieszaniec jamnika i owczarka niemieckiego, z charakteru wredna bestia, nie dał się na to nabrać. Z niejednej miski jadł w poprzednim życiu obierki z pomyjami, żeby go teraz na dwór w taką pogodę wyganiać. Łypnął groźnym wzrokiem na widok ręki ze smyczą, więc Krzysztof szybko zrezygnował z planu wyprowadzenia psa.*
*– No nic, pańcia z tobą wyjdzie. – Krzysztof uznał, że naleganie nie ma sensu. Mogło się to skończyć źle albo jeszcze gorzej. Oczywiście dla niego. On jednak nie miał wyboru. Trzeba było ruszać do roboty.*

*Z rozmyślań nad własnym ciężkim losem (dlaczego nie urodziłem się psem?) wyrwał go dzwonek telefonu.*
*– Panie Krzysztofie, przepraszam, że tak wcześnie, mam nadzieję, że nie obudziłam – głos Krystyny Dzwoneczek, kierowniczki sklepu, brzmiał trochę niepokojąco – ale pan Jarek nie przyszedł, a to ten, no kłopot, bo sam pan wie...*

– Pan Jarek, ten ochroniarz.

– Pracownik ochrony, pani Krystyno. Ochroniarz to w klubie nocnym szopenfeldziarzy przegania. – Krzysztof pilnował kwestii formalnych, bo wiedział, że ludzie lubią lekceważyć jego ciężko pracujących ludzi. Ileż razy spotkał się z mocno krzywdzącą opinią, że stoi taki, nic nie robi, a pieniądze bierze. A dobrze wiedział, że jak trwoga, to do… no właśnie, pracownika ochrony. Należał im się zatem szacunek.

– Wiem, wiem, ale to nie zmienia faktu, że pan Jarek nie zjawił się w pracy. A tu za chwilę sklep rusza. – Krystyna Dzwoneczek, której głos przypominał raczej solidny spiżowy dzwon, brzmiała na zmartwioną.

– Pani kierownik, damy radę, mamy ludzi. Już jadę. Do zobaczenia. – Krzysztof zakończył rozmowę, starając się nie dać po sobie poznać, że mocno się zmartwił.

Z tymi ludźmi wcale nie było tak dobrze. Ostatnie rekrutacje nie wyglądały zachęcająco. Młodzi sensowni ludzie nie garnęli się do pracy w agencji ochrony. Robota była ciężka, często bezpośrednio z klientem bez krawata, w dzikich porach, cały dzień na nogach. A przecież jako agencja nie mogli oferować ani owocowych czwartków, ani casual piątków, a karta sportowa dla kogoś, kto miał po całym dniu chodzenia kilkanaście kilometrów na liczniku, też nie była wystarczającą zachętą. Potrzebowali młodych, rzutkich, wysportowanych ludzi, a zgłaszali się emeryci z grupą inwalidzką. Nic to, trzeba działać.

Dariusz Wielki, od niedawna pracownik ochrony, miał tego dnia w planach pospać do południa, a potem zaszyć się w przydomowym warsztacie, gdzie hobbystycznie strugał z drewna różne krasnale i zabawne ludziki, które zresztą coraz lepiej się sprzedawały na popularnym portalu z rękodziełem. Plany diabli wzięli, bo zadzwonił kierownik Krzysztof. Dariusz siedział teraz naburmuszony w samochodzie, jadąc do pracy.

– Panie Darku, to zobaczymy jak tam na miejscu, ale nie powinno być kłopotów. Zastępstwo jest dzisiaj, grafik sprawdzę, żeby pan nie był poszkodowany.

Po dotarciu na miejsce obaj panowie zastali może nie armegedon, ale mały chaosik. Za pięć minut powinno nastąpić otwarcie sklepu. Już przestępują przed nim z nogi na nogę osiedlowe „wózkowe", jak mówiła o nich kierownik Dzwoneczek, czyli starsze panie z wózkami w kratę, tymczasem w pomieszczeniu ochrony zamiast planowania pracy odbywała się dziwna narada. Jadwiga, starsza sprzedawczyni zawiadująca działem nabiału, gorączkowo tłumaczyła, że *przecież Jarek to już wczoraj był dziwny, ani chybi się pochorował, zresztą mówił, że go coś rozbiera i nie wie, czy przyjdzie. Może to covid, a może zwykła grypa.* No tak mówił. Kierowniczka Dzwoneczek z oburzeniem przyjęła tę wiadomość, bo *nikt mi nigdy nic nie mówi i dlaczego ja zawsze dowiaduję się ostatnia?!* Pani Wanda, sprzątająca od lat w placówce znienacka zauważyła, że *ludzie, kamery włączta, bo przecież zaraz tu tłum wejdzie i nas pookradają.* Kierownik Dzowneczek przewróciła oczami, Krzysztof westchnął ciężko, widząc, że Wanda ma rację, bo monitory były czarne jak listopadowa noc, za to Dariusz Wielki ze stoickim spokojem oznajmił, że on to się idzie przebrać i się rozejrzy, bo *coś mu tu śmierdzi.*

– Jakże śmierdzi! – Wanda nie kryła wzburzenia. – Ja tu na kolanach wszystko szoruję! Spójrz Pan – teatralnym gestem wskazała na pomieszczenie – na błysk! A na wędlinach i serach to nawet ufały świecą nocą. Co też Pan gadasz. – Mało brakowało, a przejechałaby młodzianowi szmatą przez grzbiet.

– W sensie, że sytuacja dziwna – pracownik ochrony Dariusz zaczął tłumaczyć – bo u nas taki zwyczaj, że jak ktoś nie może przyjść, to wcześniej pana kierownika powiadamia. – Mówiąc to, Dariusz wskazał na Krzysztofa Jastrzębskiego.

– Tak że ten, ja się przejdę po obiekcie. – I cofając się rakiem do wyjścia, dyskretnie się oddalił. Krzysztofa zmartwiły tak naprawdę nie kłopoty kadrowe, ale fakt, że dziwnym trafem nieobecność jednego pracownika zbiegła się z niedziałającym system CCTV. Dlaczego nie działa? Oto jest pytanie.

Dariusz Wielki przeszedł przez sklep, potem obszedł parking, potem jeszcze raz przeszedł przez sklep, a potem raz jeszcze wyszedł na parking. Niby nic się nie działo, ale dlaczego o 6.30, w listopadowy poranek siedzi na parkingu w samochodzie czterech dziwnych typów, którzy nie wyglądają na takich, którym w głowie świeże bułeczki i mleko dla kota? Hm, zastanawiające. Dyskretnie zerknął na tablicę rejestracyjną, ale ta była umazana błotem, jakby samochód brał udział w rajdzie „Paryż–Dakar. Po bezdrożach Amazonii". I już miał wejść do środka, gdy zauważył, że do samochodu, tak jakby chyłkiem podchodzi…

Krzysztofowi udało się uruchomić system CCTV. Zerknął na monitory i zobaczył to samo co Dariusz. Do samochodu, z którego wyszło czterech solidnie wyglądających mężczyzn, podszedł ktoś mu znajomy. Jakie interesy, które nie pozwalają wejść do ciepłego jasnego wnętrza sklepu, można mieć w mroczny listopadowy poranek? Co takiego załatwia się akurat tego dnia, gdy ochrona miała działać w osłabionym składzie, a monitoring wizyjny odmówił współpracy z idiotycznego powodu, powiedzmy, że uszkodzonego kabelka?

Gdy Krzysztof zastanawiał nad całą sytuacją, do pomieszczenia wszedł Dariusz Wielki i oznajmił:
– Widziałem coś dziwnego. – Krzysztof wskazał głową na monitory. Razem w nie spojrzeli.
– Tak, panie Darku, miał pan rację, coś tu zdecydowanie śmierdzi.

Kto podszedł do samochodu? Co „śmierdziało" pracownikowi ochrony Dariuszowi i jego zwierzchnikowi Krzysztofowi Jastrzębskiemu? Jak sprytnie unieruchomić system CCTV i jak temu zapobiec? I czy naprawdę ktoś się rozchorował, czy raczej wolał danego dnia w pracy się nie pojawić? Odpowiedzi na te pytania poznali uczestnicy ostatniego w tym roku Security Forum. Udzielił ich nasz ekspert Jacek Grzechowiak. Odpowiedzi znajdują się też na naszej stronie „a&s Polska".

Opracowała Monika Żuber-Mamakis na bazie scenariusza Jacka Grzechowiaka

Robert Głażewski, Checkpoint Systems

*Na Security Forum najbardziej podoba mi się przede wszystkim aspekt warsztatowy spotkania. Szkolenie to nie jest prezentacja, tylko rozmowa, a ludzie biorą w niej aktywny i bezpośredni udział. Często prowadzący na innych warsztatach chcieliby osiągnąć taki efekt, ale mówią zbyt sztywno, trzymając się slajdów. Tu wszyscy korzystają. Każdy jest inny, każdy ma coś innego w głowie i robi się ciekawe sprzężenie. Dodatkowo, tu nie ma osób z przypadku, to są profesjonaliści, którzy chcą się rozwijać i zależy im, żeby ta branża szła do przodu.*

Mateusz Gintrowicz, Securitas Polska

*Podczas spotkania zwróciliśmy uwagę na kluczową rolę odpowiednio przygotowanych procedur. To one wyznaczają działania, jakie pracownik ochrony powinien podjąć w przypadku wystąpienia incydentu. Ich opracowanie leży po stronie menedżera i ma na celu zapewnienie, że pracownik dokładnie wie, co robić w konkretnej sytuacji. Nawet chwilowe zawahanie może skutkować wysokimi kosztami związanymi z incydentem. Przeprowadzona gra symulacyjna dodatkowo wykazała, że pracownicy ochrony powinni być odpowiednio przeszkoleni z uwzględnieniem specyfiki branży, którą obsługują.*

Magdalena Wiśniewska, CH Pruszków

*Z tego Security Forum wyniosłam dla siebie przede wszystkim wiedzę, że należy uważnie przyglądać się osobom współpracującym. Ponadto jeszcze większą uwagę będziemy zwracać na wszystkie firmy, które prowadzą różne prace w naszym budynku, np. bezpośrednio dla najemców. Mamy procedurę awizacyjną, więc każdą taką osobę znamy z imienia i nazwiska, ale – jak pokazuje dzisiejsze szkolenie – nawet to może być złudne, bo podwykonawca może nie wiedzieć, że ktoś się u niego zatrudnił na potrzeby prac w konkretnym miejscu. Zamierzam się temu dokładniej przyjrzeć.*

Andrzej Łukianowicz, Allegro

*Najciekawsze w tym szkoleniu było omówienie genezy kradzieży. Dało to na pewno dużo do myślenia zarówno uczestnikom z branży e-commerce, jak i ze sklepów wielkopowierzchniowych, którzy nie mieli wiedzy na temat metod działania sprawców dokonujących kradzieży w ich obiektach. Ja akurat spotkałem się z tym wcześniej, ale zawsze warto odświeżyć i uporządkować tę wiedzę. Co chwilę wchodzą nowe metody kradzieży, a takie spotkanie to też okazja do wymiany poglądów. To zdecydowanie poszerza horyzonty.*

Monika Turek, Dino Market

*Największymi wyzwaniami dla nas są kradzieże oraz powstające ich nowe formy. Zagadnienia na listopadowym Security Forum były naprawdę bardzo interesujące. Bardzo mi się podobało, że prowadzący omówił właśnie konspekt kradzieży i pokazał, od czego zaczynać ich rozpracowywanie, i przeszedł od weryfikacji po końcowe ustalenia. Równie cenna była wymiana doświadczeń z innymi security managerami z branży retail.*


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 Koczwara
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

BCS®

*dla profesjonalistów*

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

# *Wesołych Świąt*

i Szczęśliwego Nowego Roku

Życzy BCS