01 (49) / 2025

CZASOPISMO RYNKU SECURITY

a&S POLSKA

www.aspolska.pl

PODSUMOWANIE ROKU 2024 I PROGNOZY NA 2025

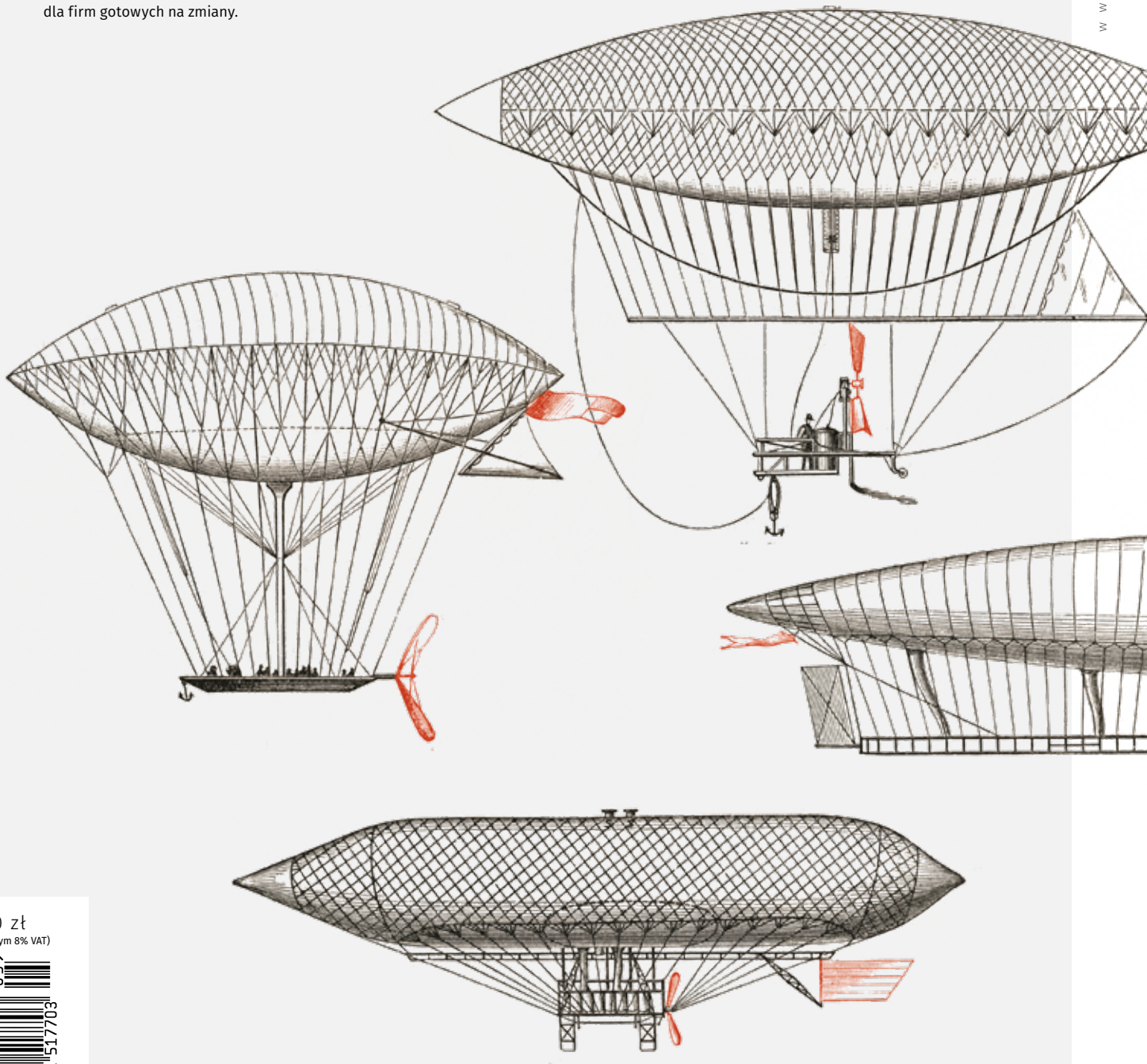
Rok 2024 w branży zabezpieczeń okazał się czasem dynamicznych przemian i intensywnych wyzwań. Wypowiedzi przedstawicieli firm security dają obecny i przyszły obraz sytuacji na polskim rynku.

STARE, ALE JARE? NIEKONIECZNIE

Bezpieczeństwo urządzeń IoT to proces wymagający ciągłej uwagi, aktualizacji i adaptacji do zmieniających się zagrożeń. Technologia ma wspierać organizację, a nie być jej najsłabszym ogniwem.

RAPORT: TRANSPORT I LOGISTYKA 2025

Dekoniunktura z perspektywą trwałego wzrostu to obecna sytuacja polskiej branży TSL. To dobry czas dla firm gotowych na zmiany.



20 zł
(w tym 8% VAT)

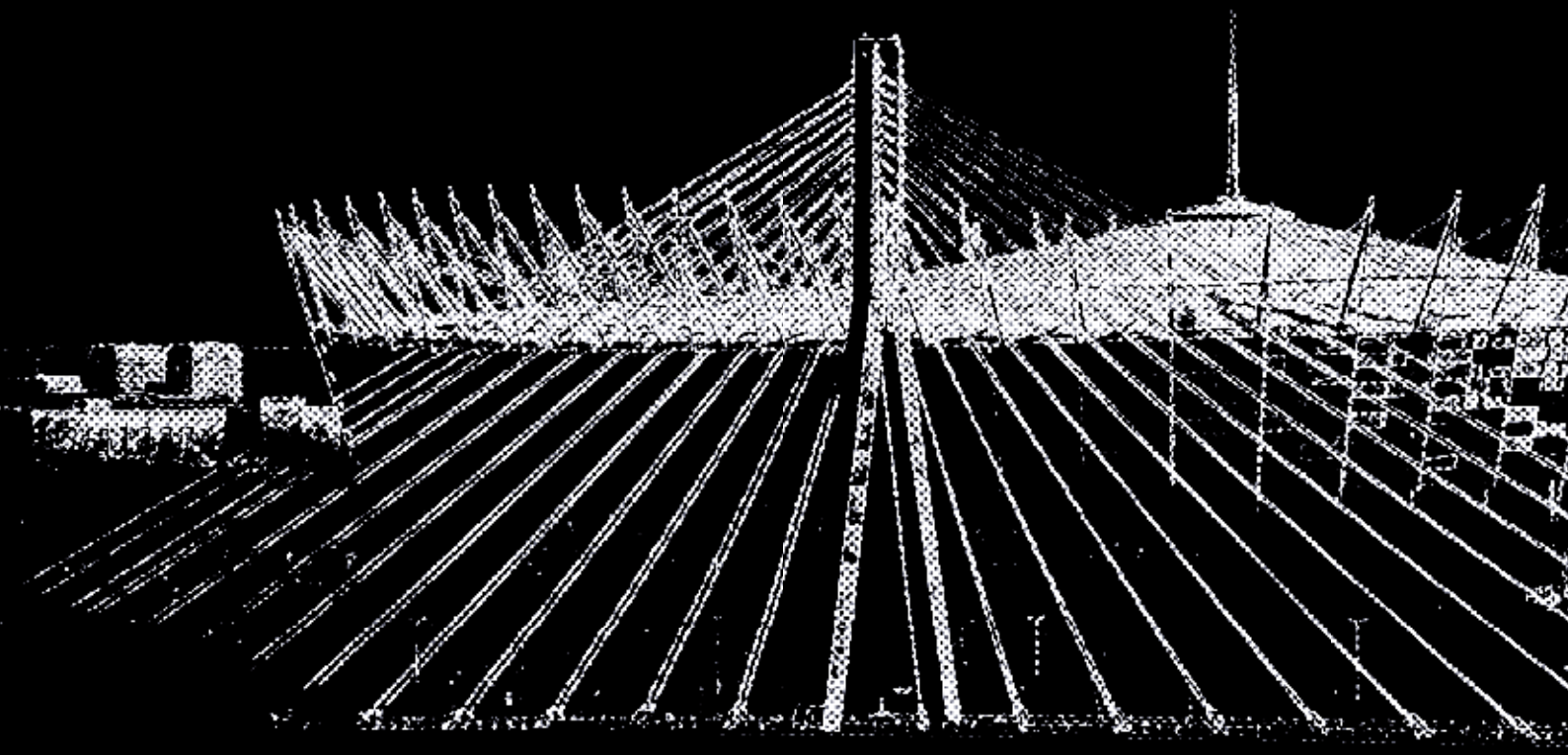
ISSN 2451-5175

SAVE THE DATE

13 CZERWCA 2025

WARSAW SECURITY SUMMIT

PGE NARODOWY



WarsawSecuritySummit.online

W zdrowym ciele zdrowy duch

Gospodarka jest jak organizm. Ważny jest każdy element. Gdyby chcieć przyrównać gospodarkę do ludzkiego ciała, to transport i logistyka byłyby odpowiednikiem wszystkich naczyń krwionośnych: tętnic, żył i naczyń włosowatych. Wszystkich tak samo ważnych. I tak jak one doprowadzają krew do najbardziej odległych zakątków ciała, tak transport i logistyka odpowiedzialne są za sprawne dostarczenie wszystkiego, co potrzebne, by dobrze funkcjonował cały gospodarczy organizm.

W tym porównaniu nasza branża, czyli security, byłaby oczywiście systemem immunologicznym.

Zapewne wielu czytelników się zgodzi, że do dobrego człowiek szybko się przyzwyczaja i fakt, że półki sklepowe są pełne towarów, a zatankowanie samochodu nie sprawia żadnej trudności, poza bólem portfela, jest oczywistą oczywistością. Czasami jednak, jak w każdym organizmie, coś przestaje funkcjonować idealnie albo sobie radzi nieco gorzej, niż byśmy chcieli. Pojawia się jakiś dyskomfort. O takim delikatnie zauważalnym dyskomforcie dotyczącym właśnie branży TSL piszemy w raporcie na str. 12.

Cóż takiego dolega branży TSL? Niższe przychody, mniejsze marże, problemy z utrzymaniem płynności finansowej, zadłużenie, niewypłacalność – to jeszcze nie stan krytyczny, ale wyraźne symptomy, że organizm (czyli gospodarka) cierpi z powodu jakiejś dolegliwości. Najczęściej jest to spowolnienie gospodarcze – choroba o skomplikowanej etiologii. Mimo kłopotów TSL wykazuje zaskakującą odporność, między innymi wspomaganą przez security, i broni się na przykład za pomocą inwestycji. To właśnie firmy z sektora TSL inwestują znacząco więcej niż średnia przedsiębiorstw w Polsce. Polecamy uwadze ten raport, bo podobnie jak system immunologiczny, który nieustannie monitoruje organizm, reagując na najmniejsze zagrożenia, tak branża security czuwa nad bezpieczeństwem całego łańcucha dostaw. A inwestycje prowadzone przez TSL dotyczą przecież nie tylko infrastruktury, ale także jej ochrony.

Gdy TSL niedomaga, rola security staje się jeszcze bardziej kluczowa. Nasza branża stale rozwija „terapie" i „szczepionki" – od fizycznych zabezpieczeń po zaawansowane systemy AI – by wspierać odporność branży TSL na wszelkie „choroby". Nie można jednak zapomnieć, że tak jak odporność organizmu wymaga stałego wzmacniania i modernizacji, tak i systemy bezpieczeństwa muszą ewoluować, by skutecznie odpowiadać na coraz to nowe zagrożenia. Tak twierdzą też eksperci zapytani o prognozy na rok 2025 (str. 32).

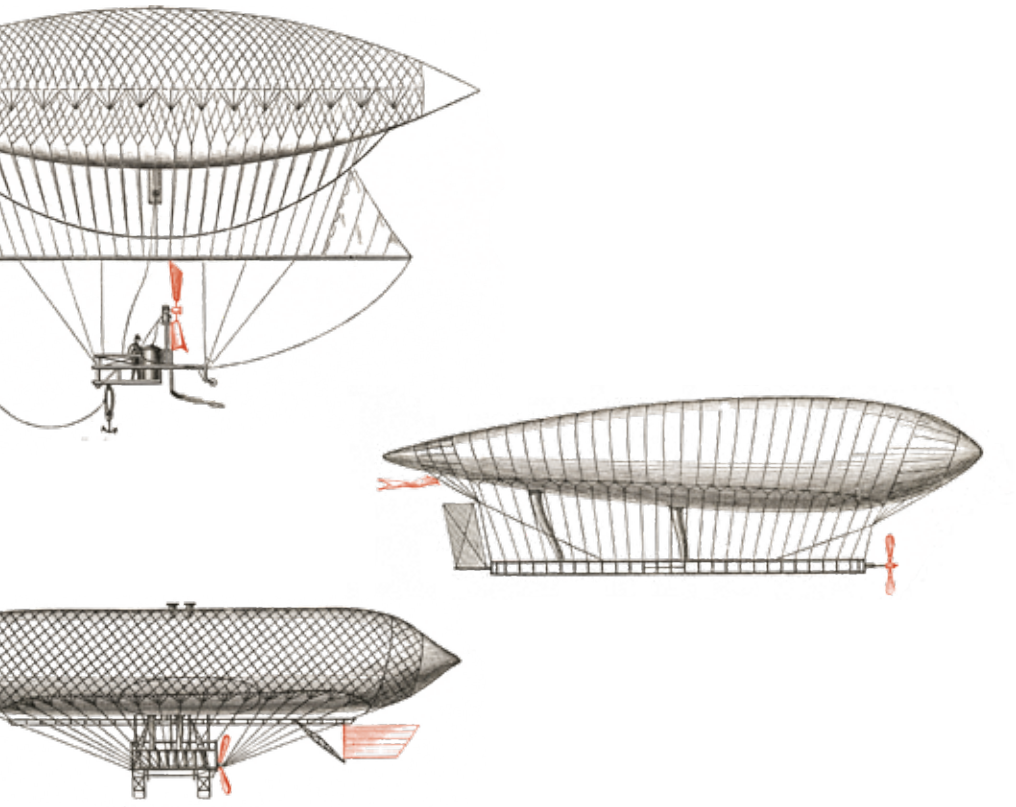
Sięgając po innowacyjne rozwiązania, jak zastosowanie systemów monitoringu wizyjnego do detekcji dymu i płomienia (str. 52 i 57) czy sztucznej inteligencji do optymalizacji procesów (str. 26), branża security skutecznie wspiera „odporność" branży TSL. To właśnie o tych nowoczesnych „terapiach" piszemy w bieżącym numerze. Zapraszamy do lektury artykułów, życząc przy okazji zarówno Państwu, jak i całej gospodarce, dużo, dużo zdrowia.

Redakcja

CZASOPISMO RYNKU SECURITY

a&S POLSKA

01 (49) / 2025



Spis treści

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

BCS®

dla profesjonalistów

BCS POINT ITC

Najwyższa skuteczność w każdym… znaku

Zgodność
z wymaganiami **NDAA**

Czarna i biała lista
do **20 tyś.** pozycji

» Więcej przeczytasz na stronie 8

POLSKA MARKA BCS

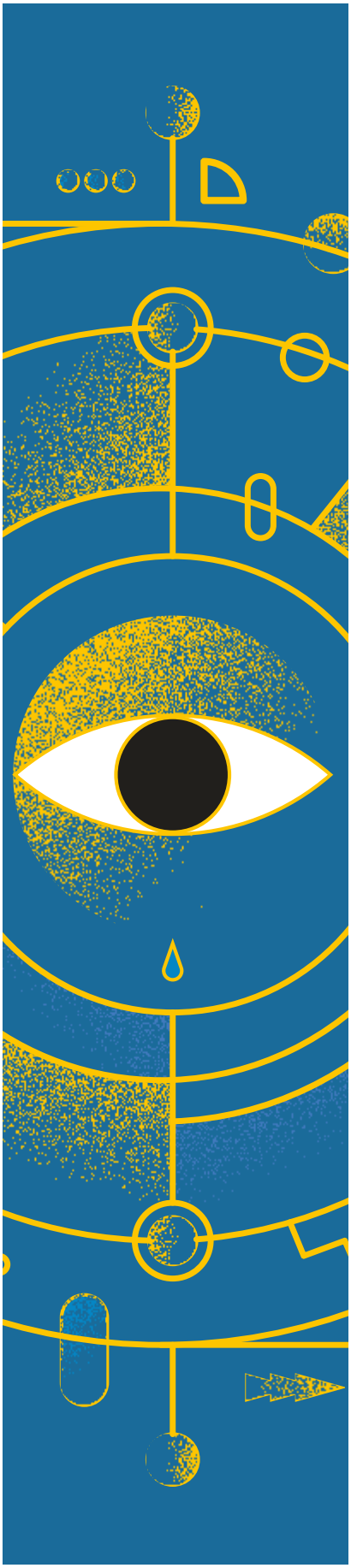
www.bcs.pl
www.facebook.com/bcspl

CZASOPISMO RYNKU SECURITY

a&S POLSKA

01 (49) / 2025

Spis treści



ALNET SYSTEMS

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

www.alnetsystems.com

Prezentujemy najnowsze urządzenia z oferty firm

BCS, HIKVISION, LINC POLSKA, SQUARETEC, TP-LINK





BCS

Nowe kamery LPR z serii BCS Point

4-Mpix kamery LPR *(Licence Plate Recognision)* z serii BCS Point są przeznaczone do automatycznego odczytywania numerów tablic rejestracyjnych pojazdów. Doskonale sprawdzają się na parkingach do kontroli ruchu (wjazdów/wyjazdów) oraz rejestracji czasu postoju pojazdu.

Nowe modele kamer LPR z serii BCS Point mają obiektywy z motozoomem w różnych zakresach ogniskowych. Do obserwacji z odległości do 10 m (np. wjazdy/wyjazdy z parkingów), sprawdzi się model **BCS-P-TIP74VSR5-ITC-2812,** który ma ogniskową w zakresie od 2,8 do 12 mm. Natomiast drugi model **BCS-P-TIP74VSR5-ITC-0832** charakteryzuje się większą ogniskową, w zakresie od 8 do 32 mm i jest przeznaczony gównie do obserwacji ruchu z większych odległości (np. bramki nad drogą). Umożliwiają odczyt tablicy z pojazdu, poruszającego się z prędkością do 80 km/h.

Urządzenia mają też opcję tworzenia białej i czarnej listy, czyli list samochodów uprawnionych do wjazdu bądź do niego nieuprawnionych. Listy, które mogą mieć do 20 tys. wpisów, można zintegrować z systemami szlabanowymi i zdarzeniami alarmowymi, np. pojawienie się samochodu z czarnej listy.

Kamery wyposażono w funkcje: **WDR, White Balance, ręczne ustawienia migawki czy promiennika IR**. Ponadto mają dwa wejścia i wyjście alarmowe, za pomocą których można sterować zewnętrznymi urządzeniami, oraz wejście i wyjście audio, które w razie potrzeby umożliwia prowadzenie dwukierunkowej komunikacji głosowej.

Kamery LPR z serii BCS Point umożliwiają stworzenie bezpiecznego systemu kontroli ruchu, zgodnego z wymaganiami NDAA *(National Defense Authorization Act)*.

Więcej na: www.bcs.pl

HIKVISION

Nowa seria kamer Hikvision ColorVu 3.0 IPC 2XX7G3 z technologią HIKAI-ISP

Firma Hikvision wprowadziła serię kamer ColorVu 3.0 2XX7G3, które wyznaczają nowe standardy w monitoringu wizyjnym. Dzięki zastosowaniu zaawansowanych technologii, takich jak HikAI-ISP, Smart Hybrid Light, F1.0 Super Confocal Lens, 3D LUT Color Correction oraz AI WDR, kamery tej serii gwarantują doskonałą jakość obrazu w każdych warunkach oświetleniowych.

Technologia HikAI-ISP zapewnia niezrównaną wydajność dzięki redukcji szumów wspieranej przez AI, dynamicznej redukcji smużenia oraz zaawansowanemu procesowi automatycznej regulacji parametrów, co przekłada się na stabilność algorytmu i doskonałą jakość obrazu, nawet w słabym oświetleniu.

F1.0 Super Confocal Lens to precyzyjnie zaprojektowany obiektyw, który dzięki dużej aperturze zapewnia wyraźne i jasne obrazy w trybach dziennym i nocnym. Wysoki współczynnik LPPM wraz z korekcją do pracy w podczerwieni gwarantuje doskonałą jakość obrazu niezależnie od warunków.

Smart Hybrid Light pozwala na wybór trybu oświetlenia: IR, światła białego lub trybu inteligentnego, który automatycznie przełącza się na obraz kolorowy po wykryciu zdarzenia.

3D LUT Color Correction wyrównuje poziom jasności obrazu oraz wiernie odwzorowuje kolory, dzięki czemu obraz z trybu nocnego dorównuje jakością dziennemu. **WDR** wspierany algorytmami **AI** zapewnia idealny balans między jasnymi i ciemnymi obszarami, eliminując prześwietlenia i zachowując szczegóły w miejscach zacienionych.

Więcej na: www.hikvision.com/pl

camect

INTELIGENTNY REJESTRATOR
efektywna i skuteczna detekcja zagrożenia

SZTUCZNA INTELIGENCJA
wbudowana, zaawansowana sztuczna inteligencja

ROZRÓŻNIA PONAD 30 TYPÓW OBIEKTÓW
ludzi, pojazdy, zwierzęta

WSPÓŁDZIAŁANIE
z różnymi kamerami IP

KOMPATYBILNOŚĆ
z SAFESTAR

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.

LINC POLSKA

AVUTEC | Innowacyjność w kamerach ANPR

Rozpoznawanie tablic rejestracyjnych (LPR) lub automatyczne rozpoznawanie tablic rejestracyjnych (ANPR) to technologie wykorzystywane do automatycznej identyfikacji pojazdów.

Technologia LPR, wykorzystywana głównie do celów bezpieczeństwa i monitorowania ruchu, znalazła szerokie zastosowanie w poborze opłat, zarządzaniu parkingami i egzekwowaniu prawa, umożliwiając tym sektorom wydajniejsze i skuteczniejsze działanie.

Na dokładność i skuteczność **technologii ANPR** wpływa wiele czynników: warunki środowiskowe, różnorodność tablic rejestracyjnych, prędkość pojazdu, rozmieszczenie kamer i stabilność sieci. Rozpoznawanie tablic rejestracyjnych w terenie jest bardziej złożone, niż mogłoby się początkowo wydawać. Chociaż tworzenie systemów rozpoznawania tablic rejestracyjnych (LPR) dla kontrolowanych środowisk może być proste, prawdziwym wyzwaniem jest opracowanie technologii, która umożliwia dokładny odczyt tablic rejestracyjnych w zmiennych warunkach.

Wybierając system ANPR warto zwrócić uwagę na następujące kwestie:

- **Precyzja działania** – rozpoznawalność na najwyższym poziomie w każdych warunkach.
- **Kompatybilność** – możliwość integracji z innymi systemami.
- **Wysoka jakość** produktów, serwisu i wsparcia.
- **Innowacyjność** połączona z wysoką wydajnością.

Dzięki wieloletniemu doświadczeniu w terenie, głębokiej wiedzy w zakresie technologii sztucznej inteligencji i ciągłym wysiłkom AVUTEC stworzył kompletny system ANPR, który skutecznie radzi sobie z wyzwaniami świata rzeczywistego. Zachęcamy do jego przetestowania.

Więcej na: www.linc.pl

SQUARETEC

Przełączniki sieciowe BAROX

Przełączniki sieciowe BAROX oferują zaawansowane funkcje, które doskonale odpowiadają współczesnym wymaganiom w zakresie zwiększania bezpieczeństwa systemów ochrony.

Dzięki funkcji automatycznego sprawdzania PoE przełączniki mogą rutynowo „pingować" podłączone urządzenia i automatycznie ponownie uruchamiać połączenie w przypadku braku odpowiedzi, co eliminuje konieczność interwencji inżyniera. Graficzny interfejs zarządzania (DMS) dostarcza informacji o monitorowanych urządzeniach oraz diagnostyce w całej sieci bezpieczeństwa, znacznie skracając czas diagnozowania i usuwania usterek.

Przełączniki BAROX wspierają najnowsze standardy i funkcje cyberbezpieczeństwa, takie jak szyfrowanie komunikacji, zabezpieczenia portów, zarządzanie logowaniem, wyłączanie niezajętych portów, obszerna lista kontroli dostępu, TACACS+, kontrola wielu użytkowników, serwer Radius, TLS i SSL, a także wbudowane funkcje zapory sieciowej. Funkcja Non-Stop PoE umożliwia portom PoE pozostanie aktywnymi i przesyłanie strumieni podczas aktualizacji systemu. Monitorowanie przepływu danych w czasie rzeczywistym, ustawianie progów przepływu danych oraz monitorowanie poboru mocy z kamery pozwalają na proaktywne identyfikowanie potencjalnych problemów z podłączonymi urządzeniami.

Przełączniki BAROX integrują się z systemami VMS i PSIM renomowanych dostawców, zapewniając kompleksowe zarządzanie i monitorowanie sieci. Te zaawansowane rozwiązania sieciowe, gwarantujące niezawodność, bezpieczeństwo oraz łatwość zarządzania, dostępne są w ofercie firmy squareTec.

Więcej na: www.squaretec.pl

TP-LINK

Insight S445ZI i Insight S345ZI – nowe kamery VIGI z motozoomem

TP-Link rozszerza ofertę rozwiązań VIGI, wprowadzając kamery Insight z zaawansowanym zoomem optycznym, które łączą nowoczesną technologię i inteligentną analizę z wygodą montażu i przyjaznym wzornictwem.

Insight S445ZI i Insight S345ZI to 4-megapikselowe kamery Super HD z 5-krotnym zoomem optycznym (długość ogniskowej 2,7-13,5 mm) i inteligentnymi funkcjami analityki. Zmotoryzowany obiektyw zmiennoogniskowy w obu modelach pozwala użytkownikowi dostosować pole widzenia (FOV) do wybranego obszaru, co pomaga ograniczyć liczbę nieprawidłowych stref wykrywania i zwiększyć wyraźność celu. Kamery typu turret S445ZI i typu bullet S345ZI są odporne na warunki atmosferyczne (klasa szczelności IP67) i uszkodzenia mechaniczne (klasa wytrzymałości mechanicznej IK10), a zasięg doświetlenia w podczerwieni do 60 m gwarantuje wyraźny obraz również nocą.

Funkcje, takie jak **klasyfikacja ludzi i pojazdów, rozbudowane algorytmy wykrywania Smart czy inteligentna korekcja wideo** pomagają uzyskać szczegółowy podgląd nawet w wymagających lokalizacjach. Oparte na kodowaniu H.265+ rozwiązania umożliwiają optymalne wykorzystanie pasma i przestrzeni dyskowej, co jest szczególnie istotne w większych instalacjach monitorujących.

Seria VIGI jest skierowana do użytkowników oczekujących profesjonalnego monitoringu w domach i firmach, a przy tym ceniących prostą, wygodną obsługę. Zdalny podgląd P2P działa dzięki chmurze TP-Link ID oraz mobilnej aplikacji VIGI, którą można zainstalować na urządzeniach z iOS lub Androidem.

Więcej na: www.tp-link.com/pl

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

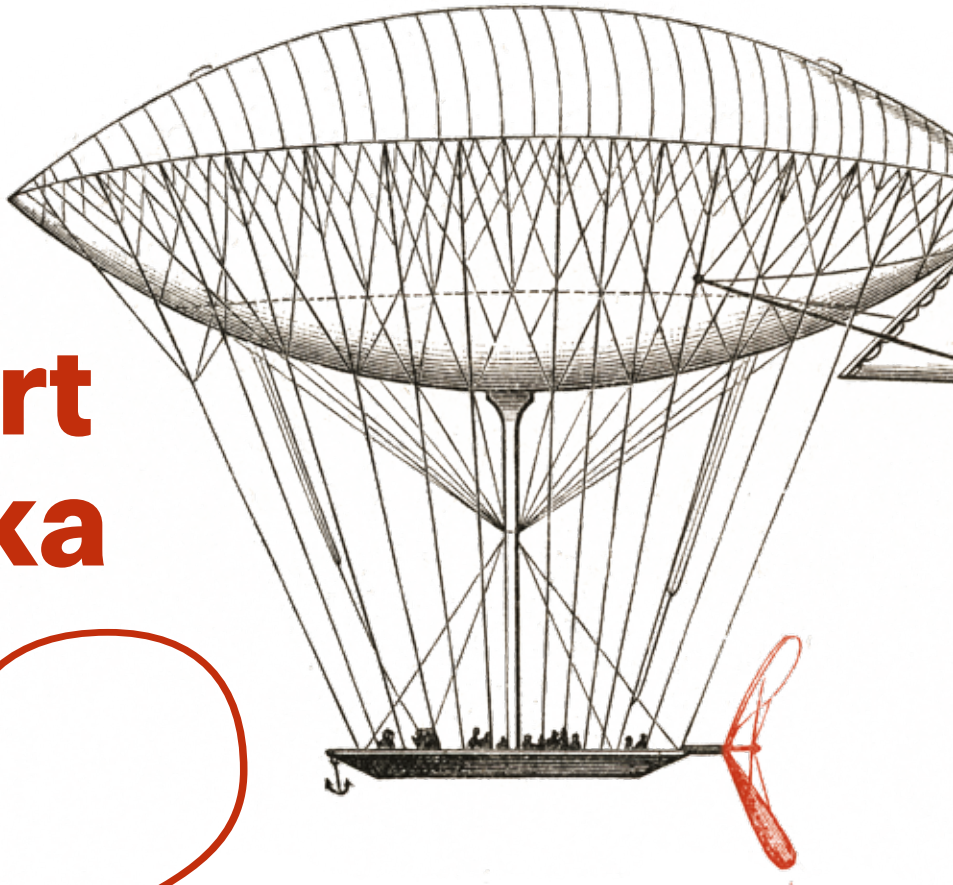
www.linc.pl

WIĘCEJ O NAS:

Linc Polska Sp. z o.o.

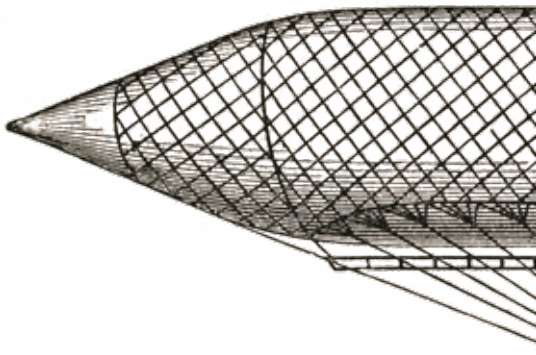
Dekoniunktura z perspektywą trwałego wzrostu – tak w telegraficznym skrócie można opisać sytuację polskiej branży TSL. W zeszłym roku doświadczyła najgłębszego kryzysu od dwóch dekad, a mimo to oczekuje się, że długofalowo będzie się rozwijać. Paradoks? Nie, to moment w cyklu koniunkturalnym. Moment być może zwrotny.

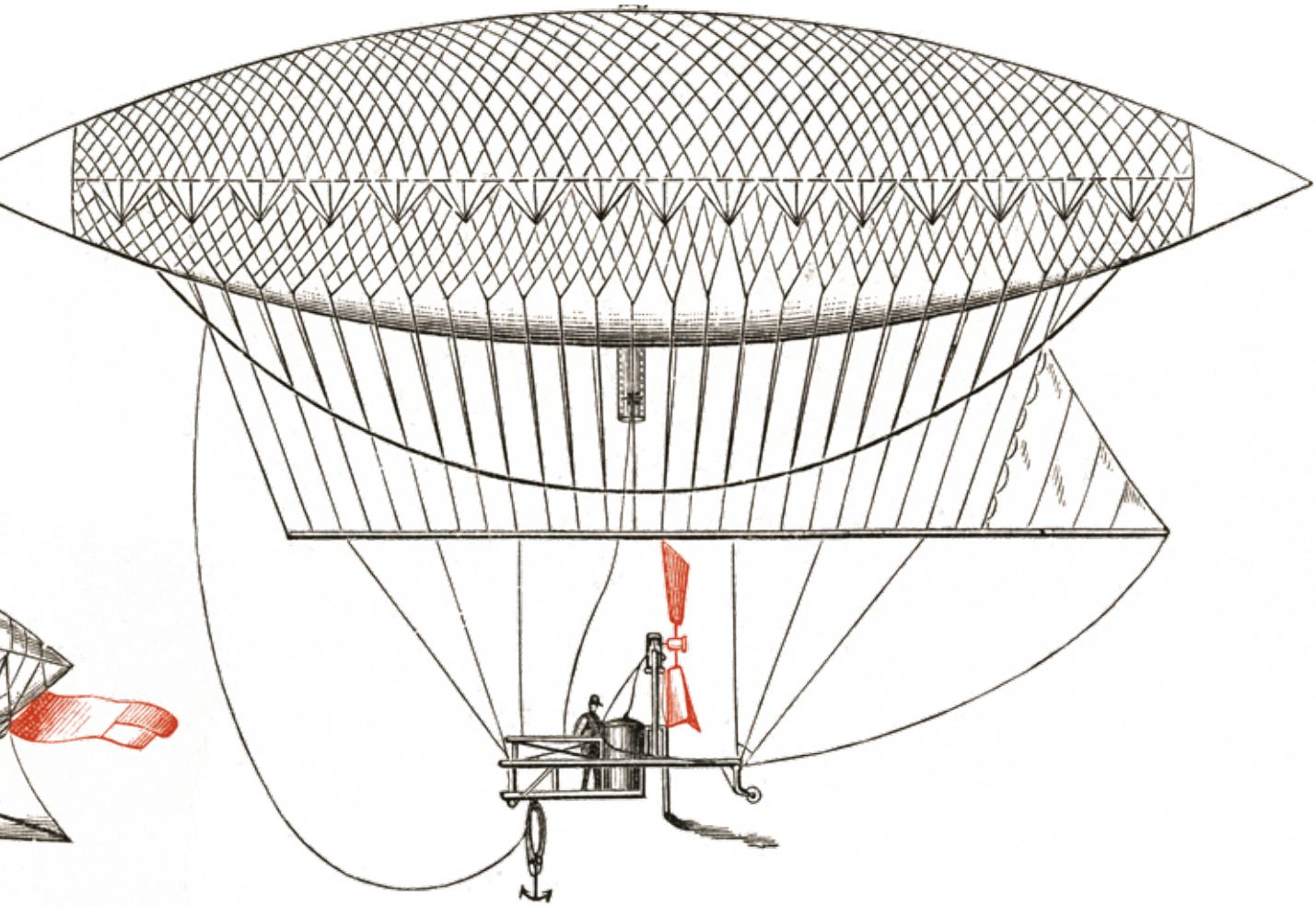
Adela Prochyra

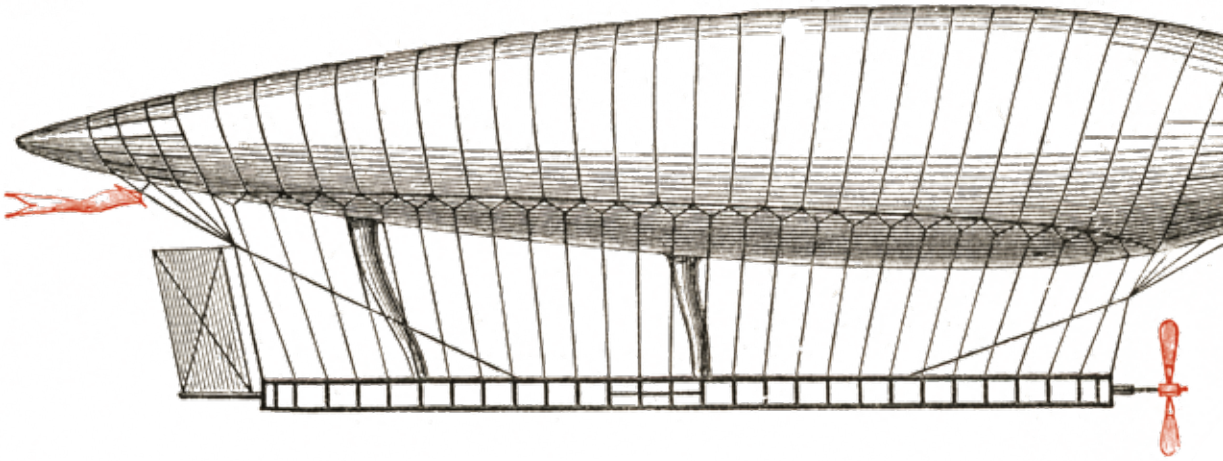


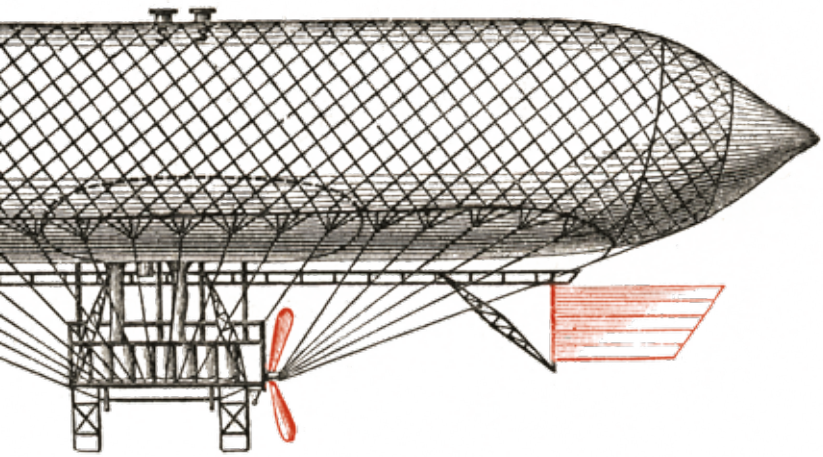
RAPORT

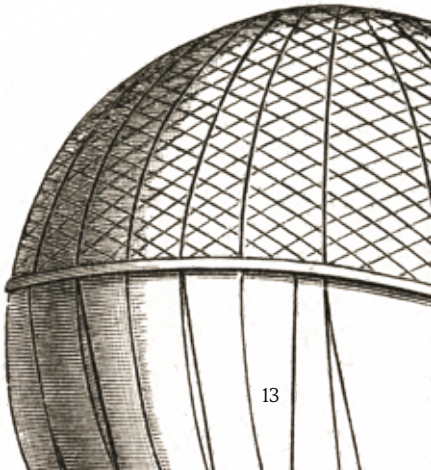
Transport i logistyka 2025



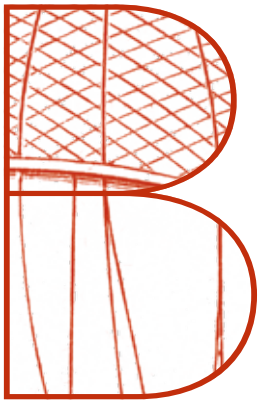








Ilustracje: rawpixel



Branża transportu i logistyki jest kluczową częścią gospodarki i podlega jej regułom, w tym regule cykliczności koniunktury. Eksperci i pracownicy tego sektora, komentując bieżącą sytuację finansową, często w swoich wypowiedziach odnoszą się do „historycznych wyników". Mają wówczas na myśli złoty okres obejmujący lata 2010–2019, kiedy to średnia wzrostu wynosiła 4,9% (możemy przyjąć, że 2000–2019 to okres srebrny ze średnią wzrostu 3,8%). To były lata „tłuste", po których nieuchronnie nadchodzą lata „chude", czyli moment obecny. Portal Business Insider podaje co prawda, że średnioroczny wzrost w 2024 roku wyniósł dla całej branży 4,3%, a dla transportu drogowego i rurociągowego 6,1% (dostęp: 22.01.2025), powołując się na dane Eurostatu dotyczące produkcji usług w Europie, za okres styczeń–październik 2024 roku. Warto jednak pamiętać, że szczegółowa analiza sytuacji przedsiębiorstw transportu drogowego (obejmująca finanse, zatrudnienie, wynagrodzenia, nakłady inwestycyjne) jest przygotowywana przez GUS co dwa lata. Dane za 2024 i 2025 rok będą dostępne dopiero pod koniec 2026 roku.

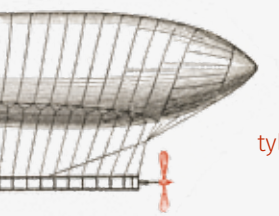
Co wiemy już teraz z całą pewnością? Zeszłoroczne prognozy zakładające delikatny optymizm (por. *Raport: Transport i logistyka w Polsce 2024*) się nie sprawdziły. Branża transportowa w Polsce jest obecnie w fazie ostrego spowolnienia, które jest efektem m.in. dynamicznego rozwoju w poprzednim, bardzo dobrym okresie. Firmy, które w latach boomu zbyt szybko powiększały flotę czy zatrudniały zbyt wielu nowych pracowników, teraz zmagają się z problemami finansowymi. Na ich obecną, kiepską sytuację wpływają także czynniki makroekonomiczne: wysoka inflacja, wzrost kosztów paliwa i dekarbonizacji, wzrost wynagrodzeń, spadki produkcji oraz generalny spadek popytu na usługi transportowe w Europie. Trend zniżkowy widać było już w 2023 roku: transportem samochodowym przewieziono wtedy 1942,8 mln ton ładunków, tj. o 1,7% mniej niż rok wcześniej, i wykonano pracę przewozową na poziomie 400,6 mld tonokilometrów, czyli 1,5% mniej niż w 2022 roku (GUS, *Transport drogowy w Polsce w latach 2022 i 2023*). Dalej GUS: „W roku 2023 w porównaniu z rokiem poprzednim odnotowano spadek przewozów krajowych (w tonach – o 1,0%, w tonokilometrach – o 3,7%). Przewozy międzynarodowe były mniejsze odpowiednio o 0,9% w tonach i o 0,8% w tonokilometrach. Udział transportu międzynarodowego w ogólnych przewozach w tonach kształtował się na tym samym poziomie co w 2022 roku i wyniósł 21,4%, natomiast w tonokilometrach wzrósł – z 63,6% do 64,3%".

Polscy przewoźnicy – to już Eurostat – mimo wszystko utrzymali pierwszą pozycję w Europie w przewozach drogowych. W roku 2023 przejechali 20,3% ogólnej liczby tonokilometrów. Dla porównania drudzy na podium Niemcy – 15,4 %, a trzecia Hiszpania – 14,2%.

Niewinne z pozoru spadki doprowadziły jednak do sytuacji trudnej wcześniej do wyobrażenia. Głównym zagadnieniem w firmach przewozowych w 2024 roku nie były już rozwój i wzrost, ale coraz częściej utrzymanie płynności finansowej. Niektóre z nich musiały zredukować flotę, zwolnić część załogi, a w skrajnych przypadkach mierzyły się także z kwestiami restrukturyzacji, upadłości czy wręcz likwidacji. W marcu 2024 roku firma Transcash przeprowadziła ankietę na temat sytuacji finansowej firm spedycyjnych. Aż 70% badanych wskazało, że w ciągu ostatnich 12 miesięcy ta się pogorszyła, a tylko 9% – że się polepszyła (trade.gov.pl, dostęp: 22.01.2025). Na to samo wskazują wyniki badania ankietowego przeprowadzonego na 105 przedsiębiorcach z branży transportu przez Centrum Analiz SpotData na zlecenie i przy merytorycznej współpracy ze związkiem pracodawców Transport i Logistyka Polska. Ponad połowa badanych przyznała, że w ciągu ostatnich dwóch lat ich przychody się obniżyły, a w zdecydowanej większości przypadków spadek wyniósł ponad 5%. Jedna trzecia zadeklarowała, że przychody ich firm wzrosły. W 13% przypadków przychody nie uległy zmianie.

O słabej koniunkturze świadczy gwałtowny wzrost liczby postępowań restrukturyzacyjnych w ostatnich dwóch latach. W roku 2021 przeprowadzono ich w transporcie 87. W roku 2024, tylko do końca września, było ich 430 (dane: Centralny Ośrodek Informacji Gospodarczej). Z jednej strony świadczy to o skali zadłużenia

Transport i logistyka w liczbach



7%
tyle PKB wytwarza sektor TSL

6,5%
tyle zatrudnionych pracuje w TSL

457 mld zł
przychody sektora z 2023 r. (przybliżone)

Zeszłoroczne prognozy zakładające delikatny optymizm (por. *Raport: Transport i logistyka w Polsce 2024*) nie sprawdziły się. Branża transportowa w Polsce jest obecnie w fazie ostrego spowolnienia, które jest efektem m.in. dynamicznego rozwoju w poprzednim, bardzo dobrym okresie.

i niewypłacalności firm, ale wynika także ze zmian ustawowych, które obecnie znacząco utrudniają ogłoszenie upadłości i likwidację firmy, a ułatwiają restrukturyzację. Jednocześnie branża „Transport drogowy towarów" (PKD 4941Z) była absolutną rekordzistką pod względem liczby prowadzonych postępowań restrukturyzacyjnych w kraju. Łącznie było ich 3396, co daje 12,6% branży transportowej. Drugi wynik – 165 – należy do kategorii „Uprawy rolne połączone z chowem i hodowlą zwierząt (działalność mieszana)". Dla porównania w 2021 roku postępowania restrukturyzacyjne w transporcie drogowym stanowiły 5% całości, w roku 2022 – 8%, a w 2023 – 10%. Kolejne alarmujące dane, które świadczą o zapaści branży, to lawinowo rosnąca liczba zawieszenia wykonywania transportu drogowego. W porównaniu z rokiem 2021 (63) do września 2024 (327) wzrosła ponadpięciokrotnie.

Branża TSL – czynniki kryzysu i bariery rozwoju

A więc mamy kryzys. Niższe przychody, mniejsze marże, problemy z utrzymaniem płynności finansowej, zadłużenia, niewypłacalność – to chleb powszedni dużej części, jeśli nie większości firm transportowych. Pytanie, co jest przyczyną takiego stanu rzeczy. Jak zwykle, odpowiedź może być tylko jedna: to krajobraz złożony z różnych czynników i przenikających się trendów obejmujący obszar znacznie większy niż lokalny, polski rynek przewozów. Pierwsza z przyczyn to wspomniany już moment w cyklu koniunktury. Na niekorzyść branży zadziałał (zbyt?) szybki jej rozwój w ubiegłych latach. Poniekąd to naturalny etap życia każdej dziedziny – po okresie intensywnego wzrostu następuje okres spowolnienia, a koszty poczynionych wcześniej inwestycji oraz koszty pracy stają się trudne do utrzymania w okresie dekoniunktury. To jednak nie tłumaczy całości procesu, jedynie wyznacza punkt, w którym się znajdujemy.

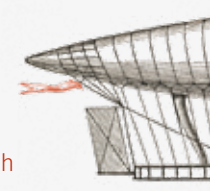
Przyjrzyjmy się teraz pokrótce najważniejszym czynnikom wpływającym negatywnie na branżę TSL. Zaznaczamy, że wiele tych problemów dotyczy całego rynku europejskiego.

- **Hamowanie całej europejskiej i światowej gospodarki** – cały czas odczuwalne są długofalowe konsekwencje wydarzeń ostatnich lat: pandemii COVID-19, wybuchu wojny w Ukrainie, kryzysu na rynku energii, wybuchu wojny na Bliskim Wschodzie. Boom na dostawy online okazał się o tyle nietrwały, że społeczeństwa trawione niepewnością, podwyżkami cen żywności i inflacją teraz obniżają konsumpcję, a firmy produkcję. To oznacza mniejsze zapotrzebowanie na transport towarów.

0,1%
długookresowe tempo rozwoju przewozów pasażerskich

10%
długookresowe tempo rozwoju przewozu towarów

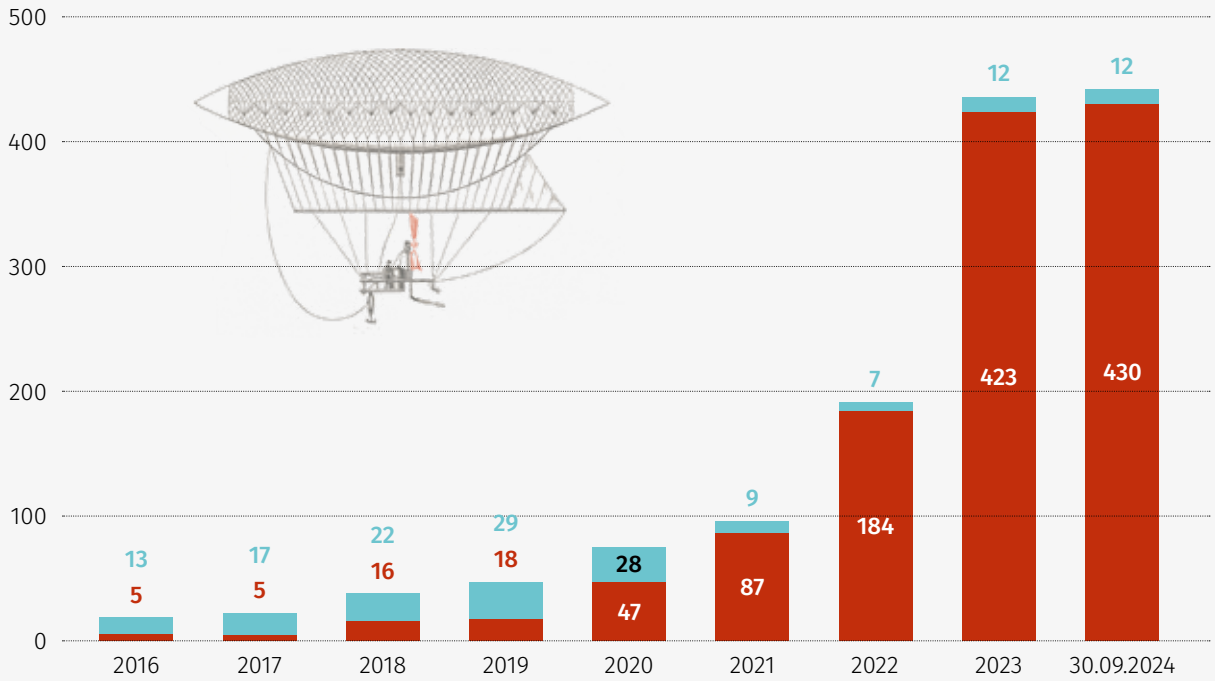
20%
długookresowe tempo rozwoju usług magazynowych



Źródło: *Transport drogowy w Polsce 2024/2025*, Centrum analiz SpotData na zlecenie i przy merytorycznej współpracy ze związkiem pracodawców Transport i Logistyka Polska

- **Kryzys na rynku niemieckim** – to zarówno istotne spowolnienie tamtejszej gospodarki, jak i wprowadzone w ubiegłym roku myto, które znacznie zwiększyło koszty przewozów na tamtejszym obszarze. Dla polskiego sektora transportowego to prawdziwy cios, ponieważ zachodni sąsiad to niezmiennie nasz największy partner handlowy, a wielu polskich przewoźników było podwykonawcami firm niemieckich. W zeszłorocznym raporcie pisaliśmy: „Dla rynków takich jak Polska i inne kraje Europy Środkowo-Wschodniej osłabienie niemieckiej dominacji może stanowić szansę na rozwój". Wygląda na to, że to założenie okazało się błędne.
- **Zmiany strukturalne** – to szereg zmiennych, które kształtują branżę w określony sposób, m.in. pakiet mobilności z 2022 roku, który obniża konkurencyjność polskich firm na arenie międzynarodowej. Obserwuje się w związku z tym spadek przewozów między krajami i wzrost liczby przewozów wewnętrznych (od 2019 roku średnioroczny wzrost wynosi 9,7%). Do tego podpunktu należy także zaliczyć zmiany w strukturze polskiej gospodarki – produkcja, będącą dotąd potężną siłą napędową, ustępuje miejsca usługom, które nie generują takiego popytu na transport.
- **Wzrost cen energii** – przekłada się na ceny właściwie każdego produktu i usługi.
- **Koszty dekarbonizacji w Polsce** – zmiany w regulacjach prawnych, w tym konieczność redukcji emisji gazów cieplarnianych, oznaczają dla przewoźników konieczność inwestowania w pojazdy elektryczne. Polska flota wciąż nie jest na to gotowa, przeważają w niej pojazdy spalinowe, w większości kilkunastoletnie. Wymiana pojazdów wymaga ogromnych nakładów finansowych, a więc mogą skorzystać na niej największe firmy dysponujące dużym kapitałem. Polska branża jest jednak bardzo rozdrobniona i składa się w większości z małych i mikroprzedsiębiorstw – ponad 50% proc. firm zatrudnia do 10 osób (patrz: raport z 2023 roku).
- **Inflacja i wysokie stopy procentowe** – średnia inflacja za rok 2024 to 3,6%, jednak już w styczniu 2025 roku wyniosła powyżej 5% (szacunek na 25.01.2025). Po rekordowo trudnym pod tym względem 2023 roku taki wzrost może nie wydawać się duży, jednak podwyżki cen liczone są od cen z poprzedniego miesiąca lub roku, a te już były wysokie. Stopy procentowe powodują, że koszt pieniądza w Polsce jest na najwyższym poziomie od lat, a to hamuje popyt na towary.
- **Wzrost kosztów pracy** – wynagrodzenia kierowców w Polsce nadal są niższe niż średnie płace w krajach Unii, lecz różnica ta szybko się zmniejsza. Obecnie koszt godziny pracy w sektorze TSL w Polsce to 13,7 euro, czyli 53,3% średniej unijnej. W roku 2020 stosunek ten wynosił 40,5% (dane: Eurostat za 2023 rok). Za wzrostem kosztów pracowniczych stoi też pakiet mobilności wprowadzony w 2022 roku. Miał on poprawić komfort pracy kierowców, ale niesie też skutki finansowe dla firm. To główne przyczyny spadku konkurencyjności polskiego transportu w Europie.
- **Niedobór pracowników w branży TSL** – to stary problem, który w powiązaniu z poprzednim punktem może wydawać się nielogiczny. Przyjrzyjmy się temu. Wykwalifikowani, doświadczeni

Restrukturyzacje i likwidacje



Źródło: opracowanie własne SpotData i TLP na podstawie danych CDIG

> Polska nadal jest europejską potęgą na rynku przewozów, z 20-procentowym udziałem w rynku. Być może tego pułapu nie uda się przeskoczyć, na razie jest to pozycja nie do pobicia. Jeśli chodzi o kabotaż na terenie Niemiec, nadal bijemy na głowę inne nacje. W 2023 roku polskie firmy przewiozły tam 45,6 mln ton, co stanowiło 56,4% masy przewożonych towarów. Dla porównania: ładunek przewieziony przez wszystkie inne nacje z Unii Europejskiej razem wzięte wyniósł 35,3 mln ton, czyli o 22,6% mniej niż nasz udział.

pracownicy to podstawa działalności firm. W związku z ograniczeniem imigracji i wzrostem kosztów pracy pracodawcy TSL mają ogromny problem z zapełnieniem wakatów. W roku 2023 w odniesieniu do liczby wakatów generalnie na całym rynku pracy ich wskaźnik był najwyższy w historii. Liczba zatrudnianych w branży w 2024 roku zmalała o 0,5% r/r, a jednocześnie liczba ofert pracy dla kierowców wzrosła o 4% r/r, dla magazynierów o 7% r/r. To sygnał poważnego niedopasowania popytu i podaży.

- **Konkurencja ze strony firm ukraińskich oraz południowych** – to w zasadzie dwa różne zagadnienia, lecz sprowadzają się do jednego wniosku: polscy przewoźnicy są zastępowani innymi. Na trasach z Europy Zachodniej na południe kontynentu coraz częściej jeżdżą przewoźnicy z południa, ale także z Czech, Węgier czy Rumunii. Z kolei firmy ukraińskie były dopuszczane do rynku na preferencyjnych zasadach. Skutkowało to m.in. 30-proc. spadkiem udziału polskich przewoźników na trasie Polska–Ukraina w ciągu dwóch lat (2021–23).

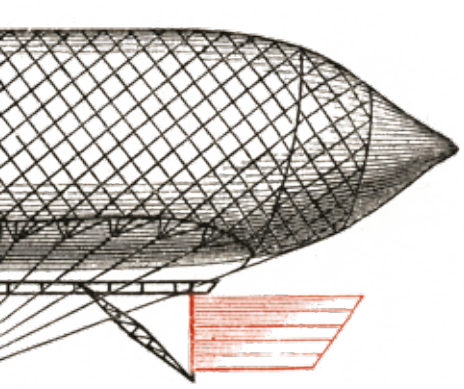
Perspektywy polskiej branży przewozowej w roku 2025

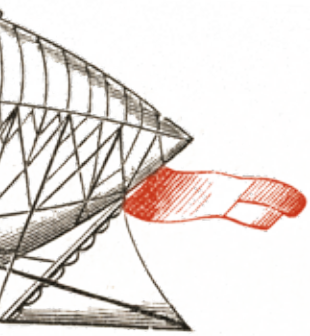
Zachowując w pamięci wszystkie informacje o liczbie restrukturyzacji, a także likwidacji firm transportowych itp., warto podkreślić kilka faktów. Polska nadal jest europejską potęgą na rynku przewozów, z 20-proc. udziałem w rynku. Być może tego pułapu nie uda się przeskoczyć, ale na razie jest to pozycja nie do pokonania. Jeśli chodzi o kabotaż na terenie Niemiec, nadal bijemy na głowę inne nacje. W roku 2023 polskie firmy przewiozły tam 45,6 mln ton, co stanowiło 56,4% masy przewożonych towarów. Dla porównania: ładunek przewieziony przez wszystkie inne nacje z Unii Europejskiej razem wzięte wyniósł 35,3 mln ton, czyli o 22,6% mniej niż nasz udział. Nadal mamy przewagę konkurencyjną w postaci niższych kosztów i wysokiej jakości świadczonych usług. W perspektywie czasu, to już wiadomo, będzie się ona kurczyć, a naszą markę trzeba będzie zbudować na czymś innym.

Nastroje w branży są... wyrównane: w badaniu zleconym przez Transport i Logistyka Polska ankietowani poproszeni o określenie spodziewanych przychodów w ciągu najbliższych dwóch lat aż w 27% wskazali, że spadną one o ponad 5%, a w 10% przypadków, że spadną maksymalnie o 5%, 14% odpowiedziało, że przychody się nie zmienią. Druga połowa oczekiwała jednak wzrostów: 20% ankietowanych – do 5% rocznie, 15% ankietowanych – 5–10% rocznie, a 14% ankietowanych – powyżej 10% rocznie.

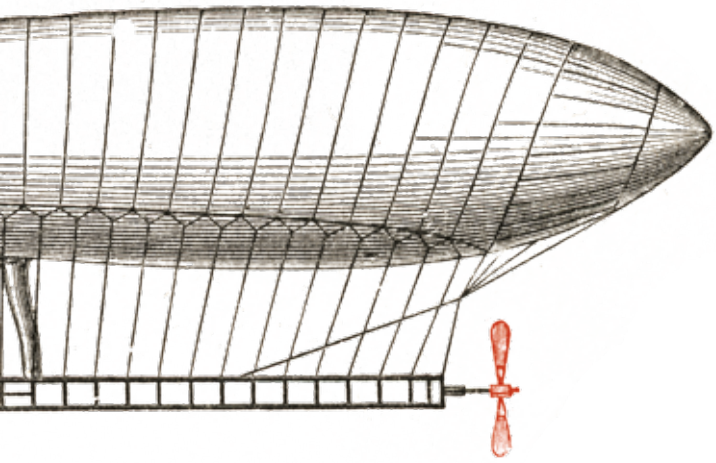
Choć obecna sytuacja na rynku jest wymagająca, to nie jest beznadziejna. Mimo trudności, które obserwujemy w ostatnich latach, branża transportowa wykazuje niezwykłą odporność. **Zmieniające się otoczenie gospodarcze wymusza na firmach transportowych konieczność adaptacji do nowych warunków.** W obliczu rosnących kosztów pracy, coraz bardziej restrykcyjnych przepisów dotyczących emisji spalin oraz wzmożonej konkurencji ze strony podmiotów zagranicznych czas poszukać nowych rozwiązań. Innymi słowy: zmiany stwarzają również nowe możliwości. Konkurencja ze strony ukraińskich przewoźników może okazać się... korzystna. W obliczu tego, że średnie pensje tam są niemal dwukrotnie niższe niż w Polsce, a firm ze Wschodu nie obowiązują regulacje unijne, takie jak postanowienia Zielonego Ładu, przewoźnicy ukraińscy mogą w przyszłości pełnić funkcję podwykonawców przewoźników polskich.

Polskie firmy aktywnie wybiegają w przyszłość. W 2023 roku nakłady inwestycyjne tego sektora przekroczyły 34 mld zł, co stanowi wzrost o 3 mld zł w porównaniu z rokiem poprzednim (mowa tu o firmach, które zatrudniają do 10 osób, które stanowią gros branży TSL). Szczególnie dynamicznie rozwija się transport drogowy, gdzie inwestycje sięgnęły około 16,5 mld zł, co oznacza wzrost o 7 mld zł rok do roku. Dodać należy, że **firmy z sektora TSL inwestują znacząco więcej niż średnia przedsiębiorstw w Polsce.** Stosunek nakładów inwestycyjnych do przychodów w sektorze TSL wynosi 11%, podczas gdy dla całej gospodarki jest to zaledwie 4%. Średnie nakłady inwestycyjne na





> Mimo znaczącego pogorszenia koniunktury w branży TSL perspektywy na przyszłość nie rysują się wyłącznie w czarnych barwach. (...) Firmy, które inteligentnie wykorzystają ten moment na zmiany mogą na tym bardzo skorzystać.



pracownika w sektorze TSL wynoszą 65 tys. zł, co jest znacznie wyższe niż średnia dla wszystkich przedsiębiorstw, a to bardzo dobry prognostyk.

Ważnym trendem jest rosnące znaczenie inwestycji w nieruchomości. Udział nakładów na budynki w ogólnych nakładach na środki trwałe w sektorze TSL systematycznie rośnie, w roku 2023 osiągnął poziom 57,4%. Świadczy to o dynamicznym rozwoju rynku magazynowego i wzroście znaczenia usług okołotransportowych, które przyczyniają się do zwiększenia wartości dodanej i efektywności sektora. Wysokie nakłady inwestycyjne, zwłaszcza w obszarze nieruchomości i technologii, mogą świadczyć o tym, że firmy z tej branży są przygotowane na dynamiczne zmiany zachodzące na rynku i chcą zwiększać swoją konkurencyjność. Poza, nazwijmy to, biznesową zwinnością mają też wiele innych atutów, a na korzyść długotrwałego wzrostu branży TSL będzie działać szereg czynników, do których należą przede wszystkim:

- **Wysokie tempo wzrostu gospodarczego** – przewiduje się, że Polska będzie się rozwijać szybciej niż średnia w krajach Unii Europejskiej (wg Międzynarodowego Funduszu Walutowego w najbliższych pięciu latach ma to być przyrost 3,4% w porównaniu do 1,5%). Oznacza to większą aktywność gospodarczą, a co za tym idzie, większe zapotrzebowanie na usługi transportowe.
- **Wysoki udział przemysłu w PKB** – silny sektor przemysłowy generuje duże ilości towarów, które muszą być transportowane. Im większa produkcja, tym większa potrzeba usług logistycznych.
- **Silny eksport** – mimo zanotowanego w 2024 roku niewielkiego spadku (1,2%) Polska pozostaje dużym europejskim i światowym eksporterem. Zwyżkowe są zwłaszcza kierunki: Wielka Brytania, Stany Zjednoczone, Wschód. Więcej na ten temat w naszym raporcie *Handel się liczy* („a&s Polska", 6/2024).
- **Korzystne położenie geograficzne** – bliskość kluczowych tras handlowych to bezwzględny atut Polski. Nasz kraj jest atrakcyjnym miejscem dla firm logistycznych, a dodatkowo korzystają na nim firmy przewozowe.
- **Rozwój nearshoringu, reshoringu i friendshoringu** – po pandemii przenoszenie produkcji do regionów bliższych geograficznie i kulturowo stało się trendem globalnym. Zwiększa to zapotrzebowanie na transport regionalny i lokalny.
- **Rozwój eksportu usług transportowych** – ten trend jest ściśle powiązany z dwoma powyższymi i wiele firm w nim znajduje swoją niszę.

Mimo znaczącego pogorszenia koniunktury w branży TSL perspektywy na przyszłość nie rysują się wyłącznie w czarnych barwach. Obecna sytuacja być może nieszczególnie na to wskazuje: otoczenie prawno-gospodarcze jest pewną stałą – koszty pracy będą wyższe, podaż pracowników niższa, a regulacje prawne coraz bardziej wymagające. Eldorado się skończyło, a firmy będą musiały się do tego dostosować. To jednak nie koniec rozgrywki. Firmy, które inteligentnie wykorzystają ten moment na zmiany i np. zaczną świadczyć bardziej złożone, kompleksowe usługi zamiast tych najprostszych, mogą na tym bardzo skorzystać.

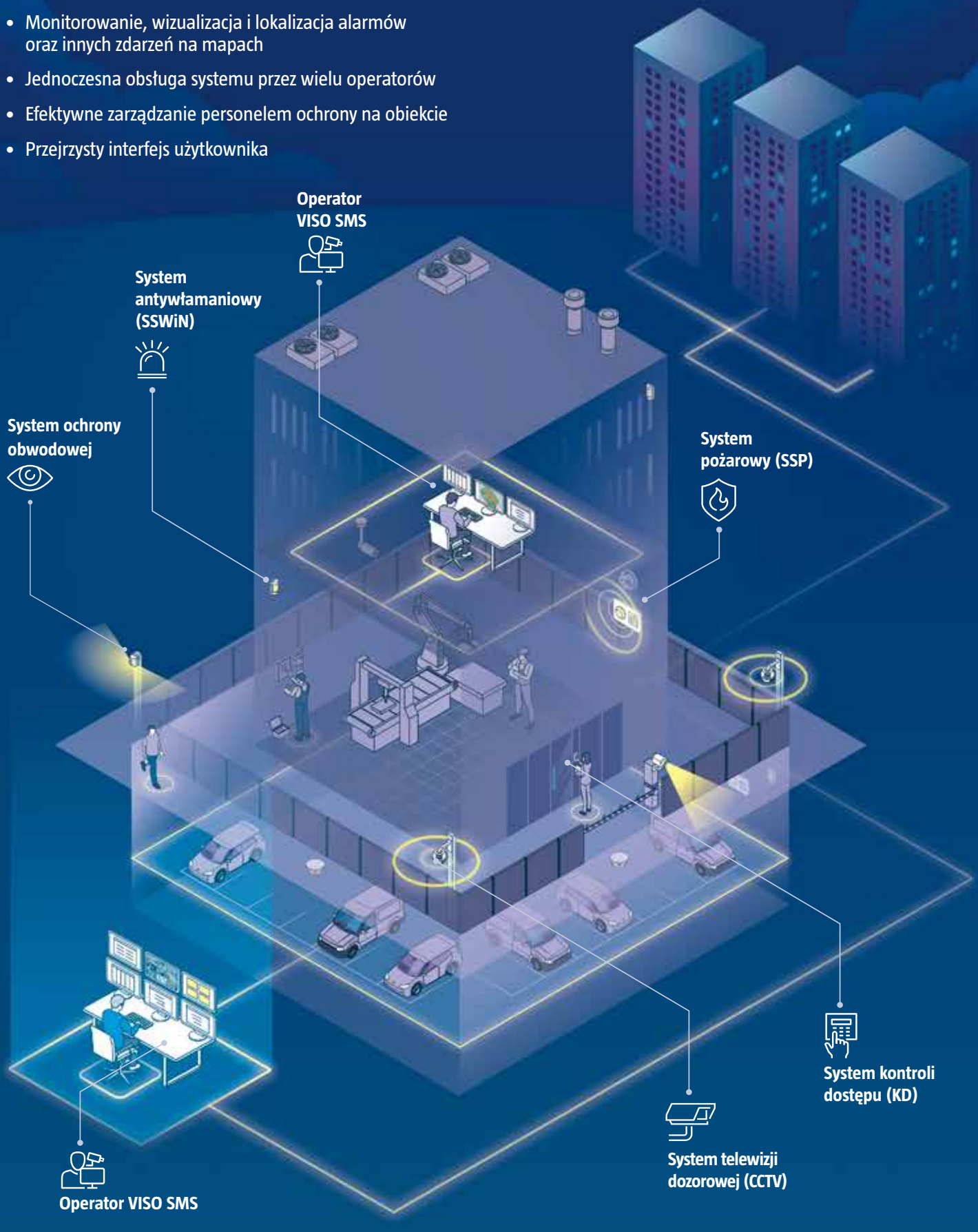
Adela Prochyra
redaktorka „a&s Polska"

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



HIKVISION dla logistyki – trendy na 2025 r.

Początek roku to idealny moment, aby przyjrzeć się trendom, które będą kształtować przyszłość logistyki. Zwiększanie efektywności i elastyczności oraz dążenie do zrównoważonego rozwoju pozostaną kluczowymi kierunkami w logistyce.

Bartłomiej Skórski

Jak wynika z raportu Związku Pracodawców „Transport i Logistyka Polska", aż 70% przedsiębiorstw planuje w ciągu najbliższych pięciu lat rozbudowę floty, cyfryzację procesów, a 28% przymierza się do rozwoju usług logistycznych. Hikvision trzyma rękę na pulsie, ułatwiając tym firmom osiągnięcie ambitnych celów.

Automatyzacja i robotyzacja to jedne z najważniejszych trendów w logistyce. Urządzenia AMR *(Autonomous Mobile Robots)* mogące poruszać się swobodnie po obiektach magazynowych oraz realizować zlecenia od systemów nadrzędnych zastępują ludzi w powtarzalnych czynnościach. Hikvision oferuje gamę robotów AMR, również z certyfikatem TiSAX, dostępnych w różnych wariantach – FMR, CTU, LMR oraz CMR/HMR. Firma zapewnia kompleksowe rozwiązania zawierające oprogramowanie iWMS-100 oraz akcesoria, takie jak stacje ładujące i dokujące. Przykładem udanego wdrożenia robotów Hikvision jest firma Superdry z branży retail, która wykorzystuje ponad 60 robotów w dwóch centrach dystrybucyjnych w Europie. Dzięki nim aż 99% zamówień jest realizowane w ciągu pierwszych 24 godzin od złożenia, z dokładnością operacyjną na poziomie 99%. To imponujące osiągnięcie!

Generatywna sztuczna inteligencja, cyfryzacja, Big Data oraz uczenie maszynowe stają się kluczowymi elementami, w które firmy z branży logistycznej będą inwestować, aby utrzymać swoją przewagę konkurencyjną. Technologie te pozwalają na zwiększenie wydajności oraz precyzji w zarządzaniu łańcuchem dostaw. Pomagają w redukcji zapasów, optymalizacji łańcuchów dostaw i poprawie dystrybucji zasobów. Istotnym celem jest także doskonalenie prognozowania popytu oraz realizacji zamówień poprzez łączenie IoT ze sztuczną inteligencją i Big Data. Takie podejście pomoże w rozwiązywaniu coraz bardziej skomplikowanych wyzwań w logistyce.

Zgodnie z prognozami IDC globalne wydatki na sztuczną inteligencję mają przekroczyć 301 mld USD do 2026 r., co stanowi ponaddwukrotny wzrost w porównaniu do obecnych wydatków na AI wynoszących 125 mld USD rocznie. Firmy coraz częściej zwracają się ku AI, aby poprawić wydajność operacyjną, jakość obsługi klienta, produktywność pracowników i innowacyjność.

Innowacje oparte na sztucznej inteligencji, takie jak analityka danych, robotyka i uczenie maszynowe, umożliwiają doskonalenie procesów i podejmowanie bardziej trafnych decyzji. Przykłady rozwiązań Hikvision pokazują, że AI może wzbogacić nowoczesną działalność logistyczną i przyczynić się do zwiększenia efektywności operacyjnej.

AI dla magazynów oraz placów manewrowych

Automatyczne rozpoznawanie tablic rejestracyjnych (ANPR) do zarządzania pojazdami: Technologia ANPR firmy Hikvision pomaga w rozpoznawaniu pojazdów i zarządzaniu ich ruchem poprzez automatyczne odczytywanie znaków i cech tablic rejestracyjnych za pomocą algorytmów oprogramowania kamer stosowanych przy wjazdach i wyjazdach lub na drogach. Dzięki temu zarządzanie przepływem pojazdów jest sprawniejsze, co jest szczególnie ważne w obiektach logistycznych o dużym natężeniu ruchu wjazdowego i wyjazdowego. Rozwiązanie to zapewnia również, że do danego miejsca mogą wjechać wyłącznie pojazdy upoważnione, co znacząco poprawia bezpieczeństwo.

Inteligentne zarządzanie dokami: Ponieważ klienci oczekują coraz szybszej realizacji zamówień, efektywne zarządzanie dokami stało się kluczowe. Sztuczna inteligencja może pomóc zautomatyzować proces, wykorzystując dane w czasie rzeczywistym i algorytmy AI do koordynowania ruchu ładowania i rozładowywania towarów, minimalizując opóźnienia i zwiększając produktywność. Systemy AI firmy Hikvision umożliwiają monitorowanie załadunku i rozładunku w czasie rzeczywistym, optymalizując operacje na dokach, minimalizując czas realizacji i redukując błędy.

Rozpoznawanie twarzy: Technologia rozpoznawania twarzy umożliwia wejście wyłącznie upoważnionym osobom, co wpływa na ogólne bezpieczeństwo obiektu. Dzięki systemom wykorzystującym algorytmy AI możliwe jest sprawne nadzorowanie przepływu osób w obiekcie, wyznaczanie stref zastrzeżonych, obsługa obecności gości. To zaś pozwala udoskonalać ogólne protokoły bezpieczeństwa.

Termowizja i zapobieganie pożarom: Incydenty pożarowe mogą być katastrofalne dla operacji logistycznych. Sztuczna inteligencja może odegrać kluczową rolę w zapobieganiu pożarom, wykorzystując do tego technologię obrazowania termicznego służącą do wykrywania nieprawidłowych wzrostów temperatury. W przypadku wykrycia nieprawidłowości oprogramowanie uruchamia środki zapobiegawcze, minimalizując tym samym ryzyko eskalowania pożaru. Technologia obrazowania termicznego Hikvision wykrywa nieprawidłowe wzrosty temperatury przed wystąpieniem pożaru, uruchamiając wczesne systemy ostrzegawcze i minimalizując potencjalne szkody.

Wykrywanie środków ochrony osobistej: Wprowadzanie zasad bezpieczeństwa i higieny pracy jest stosunkowo łatwe, ale ich egzekwowanie może być znacznie trudniejsze. Systemy Hikvision skutecznie promują zgodność z przepisami bezpieczeństwa, rozpoznając, czy pracownicy noszą wymagany sprzęt ochrony osobistej (np. kaski), czy nie. Problemy są wykrywane automatycznie, co oszczędza czas firm i daje pewność, że potencjalne naruszenia bezpieczeństwa i higieny pracy nie zostaną przeoczone.

Zautomatyzowane rozwiązania obsługi kierowców, pojazdów oraz towarów

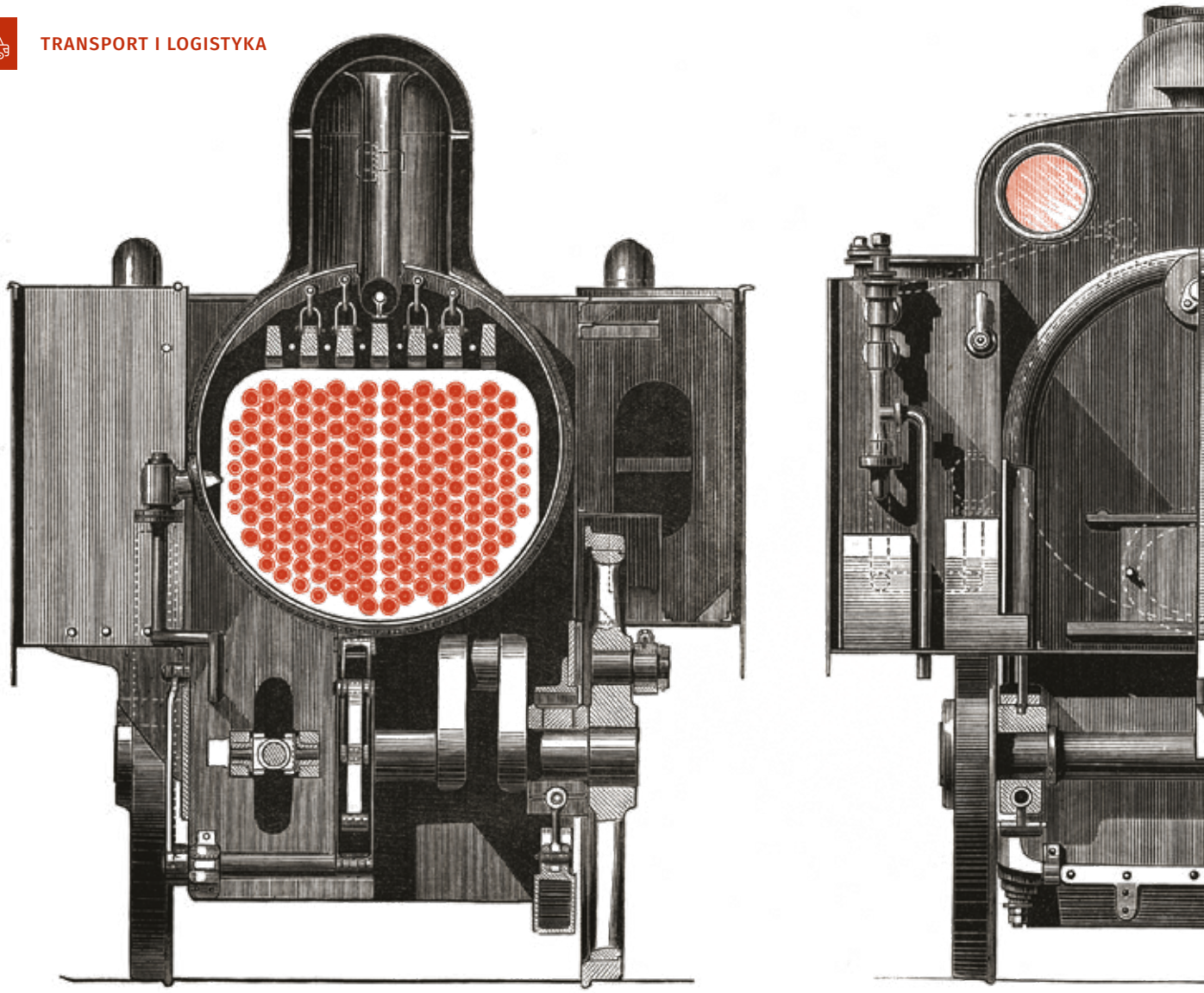
Zarządzanie transportem w czasie rzeczywistym: Dzięki centralizacji podstawowych funkcji w rozwiązaniu oferowanym przez Hikvision, m.in. takich jak inteligentna rejestracja i odtwarzanie materiału wizyjnego, a także pozycjonowanie pojazdu w czasie rzeczywistym, kluczowe dane dotyczące transportu są widoczne na jednym pulpicie. Dzięki temu praktycznie w czasie rzeczywistym operator ma wszystkie informacje dotyczące transportu liniowego, co podnosi wydajność mniejszym nakładem kosztów. Platforma Hikvision pozwala także na wygenerowane wielu różnych raportów, dających szczegółowy obraz sieci transportowych, co jest przydatne w sytuacjach awaryjnych i ułatwia podejmowanie decyzji.

Ochrona kierowcy dzięki inteligentnemu systemowi ADAS: Kierowcy samochodów ciężarowych często muszą radzić sobie z nieoczekiwanymi zagrożeniami na drodze, niesprzyjającą pogodą, ale też monotonią jazdy czy próbami kradzieży ładunku. Hikvision zdaje sobie sprawę, że jest to praca ciężka, a każda przeszkoda może oznaczać zagrożenie dla kierowcy, ładunku i bezpieczeństwa drogowego w ogóle. Dlatego Hikvision opracował i cały czas udoskonala inteligentne systemy wspomagania jazdy, które obejmują ostrzeżenie o ryzyku zderzenia czołowego (FCW), ostrzeżenie o opuszczeniu pasa ruchu (LDW), ostrzeżenie o kolizji z pieszymi (PCW), wykrywanie martwego pola (BSD), monitorowanie odstępu między pojazdami (HMW) i analizę jazdy. Jednocześnie rozwiązanie Hikvision dzięki różnym czujnikom takim jak czujniki drzwi kontenera, temperatury i poziomu paliwa ułatwia zapobieganiu kradzieży paliwa i towaru.

Rozwiązania AI dla dostaw na etapie ostatniej mili

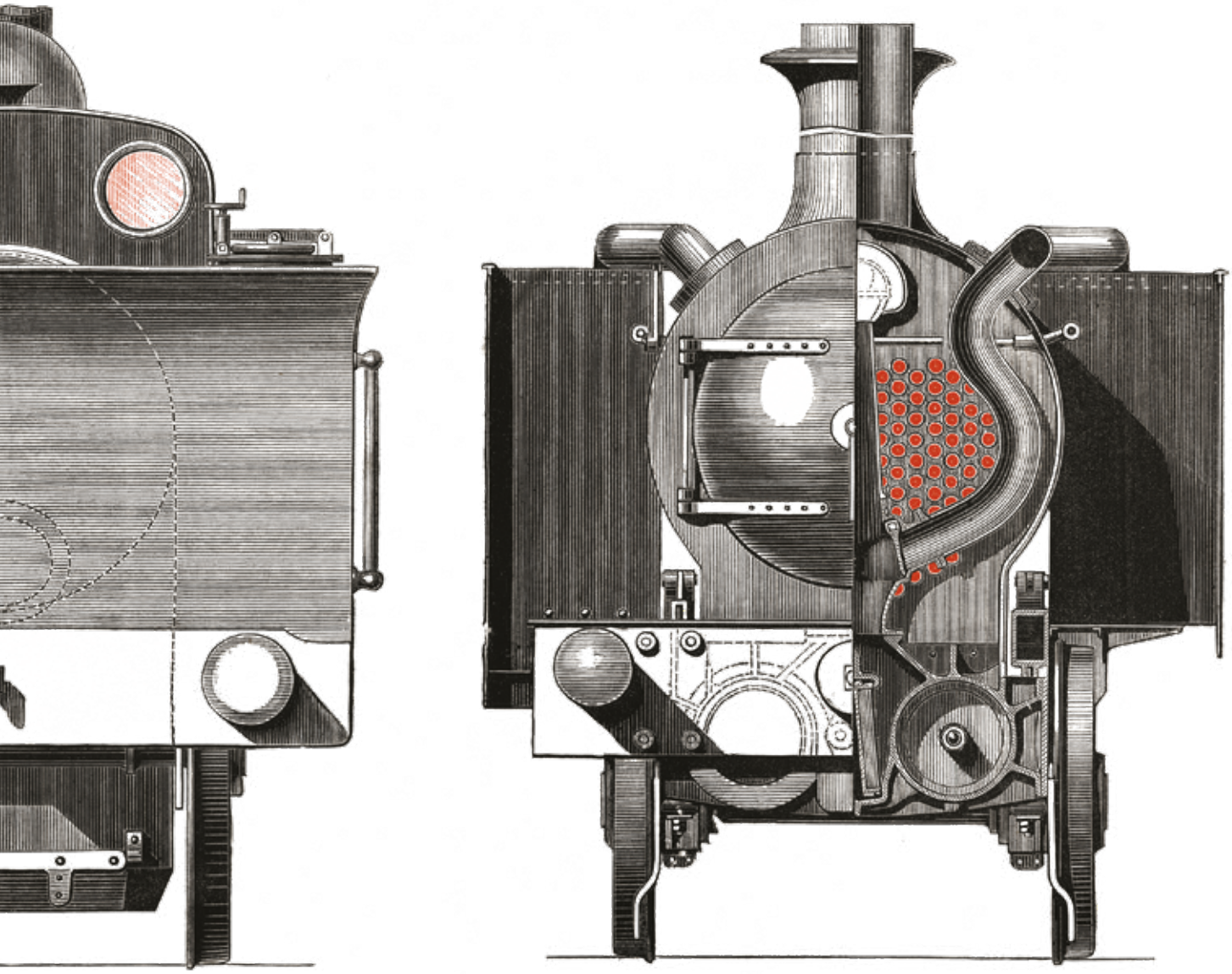
Hikvision zapewnia potężne, kompleksowe, wizualizowane rozwiązanie śledzenia przesyłek, które łączy dane z systemów monitoringu wizyjnego i zewnętrznych systemów odczytu kodów kreskowych. W ten sposób pomaga firmom poprawić jakość obsługi, reagować szybciej, zapewnić przejrzystość i poprawić ogólną satysfakcję klienta. W przeciwieństwie do RFID wdrożenie systemu *parcel tracking*, działającego na kamerach, wiąże się ze znacznie niższymi, można powiedzieć, marginalnymi kosztami w porównaniu do RFID. Dla firm kurierskich, które obsługują dużą liczbę paczek, może to być kosztowne. Z kolei technologie śledzenia paczek, takie jak kody kreskowe czy GPS, mogą być bardziej ekonomiczne i łatwiejsze do wdrożenia w skali masowej. •

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



POCIĄGI

pod (nie)specjalnym nadzorem



Niepokojące są wnioski wynikające z kontroli przeprowadzonej przez Najwyższą Izbę Kontroli w dwunastu instytucjach odpowiedzialnych za transport kolejowy.

Monika Żuber-Mamakis

Główne pytanie kontrolne brzmiało: czy systemy zarządzania kryzysowego na kolei zapewniały właściwą ochronę infrastruktury krytycznej oraz bezpieczeństwo osób przebywających na obszarze kolejowym, na dworcach i w pojazdach kolejowych, a także mieszkańców miejscowości położonych na szlakach przewozów towarów niebezpiecznych? Raport *Funkcjonowanie systemów zarządzania kryzysowego na kolei*, opublikowany w listopadzie ubiegłego roku, jednoznacznie wskazuje – odpowiedź brzmi: nie. Dokument ujawnia poważne braki w zarządzaniu kryzysowym, które mogą mieć katastrofalne skutki dla pasażerów i przewoźników, a sytuację dodatkowo pogarszają przestarzałe systemy sterowania ruchem oraz nadużywanie procedur awaryjnych.

Ale po kolei...

Urząd Transportu Kolejowego informuje, że Polacy chętnie korzystają z transportu kolejowego. W podsumowaniu roku przygotowanym przez UTK czytamy, że rok 2024 okazał się wyjątkowo udany dla przewozów pasażerskich – koleje przewiozły ponad 407,5 mln podróżnych, co stanowi wzrost o 8,8% (33,1 mln osób) w stosunku do roku 2023. Warto zauważyć, że ostatni raz tak wysoką liczbę pasażerów odnotowano w 1997 roku, kiedy z usług kolei skorzystało 416,6 mln osób. Znacząco wzrosła również praca przewozowa, która osiągnęła prawie 28,5 mld pasażerokilometrów

Ilustracje: rawpixel

– o 10,2% więcej niż w poprzednim roku. Również praca eksploatacyjna wzrosła o 7,5%, osiągając poziom 205,6 mln pociągokilometrów. Statystyczny pasażer w 2024 roku pokonywał średnio 69,9 km, co stanowi niewielki wzrost w porównaniu do 69,1 km w 2023 roku. Prezes UTK, Ignacy Góra, cytowany przez UTK.gov.pl, podkreślił, że rosnąca popularność kolei to efekt działań podejmowanych przez przewoźników i uczestników rynku, dodając, że statystycznie każdy Polak skorzystał z kolei prawie 11 razy w ciągu roku.

Jednak nie wszystkie sektory kolejowe mogą pochwalić się tak dobrymi wynikami. Transport towarowy odnotował spadek o 3,5% w porównaniu z rokiem poprzednim, osiągając poziom 223,5 mln ton przewiezionych towarów – wynik zbliżony do sytuacji z pandemicznego roku 2020. Według prezesa UTK na wyniki tego sektora wpłynęła przede wszystkim sytuacja geopolityczna związana z wojną w Ukrainie.

Pozytywnym sygnałem jest wzrost średniej odległości podróży pasażerskich do 69,9 km. W przypadku przewozów towarowych średnia odległość transportu jednej tony ładunku wyniosła 260,7 km, co stanowi niewielki spadek w porównaniu z rekordowym rokiem 2023.

Dla przewoźników, szczególnie tych zajmujących się przewozami pasażerskimi, rok 2024 był zatem udany, a statystyki zgromadzone przez UTK brzmią krzepiąco. Czy jednak są to przewozy bezpieczne? Najwyższa Izba Kontroli ma co do tego poważne wątpliwości.

Co kontrolerzy NIK znaleźli na torach?

Listopadowy raport NIK *Funkcjonowanie systemów zarządzania kryzysowego na kolei* wskazuje, że zarządzanie sytuacjami kryzysowymi w transporcie kolejowym pozostawia wiele do życzenia. Wśród głównych problemów wymieniono:

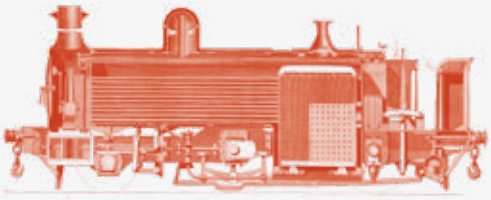
- Brak jednoznacznych procedur współpracy między Ministerstwem Infrastruktury a spółkami kolejowymi.
- Niedostateczne włączenie Prezesa Urzędu Transportu Kolejowego (UTK) w procesy decyzyjne.
- Nadużywanie procedury powoływania zespołów kryzysowych, często bez realnych przesłanek.
- Niewystarczające szkolenia i braki sprzętowe w zespołach ratownictwa technicznego.

Awaria – sygnał większego problemu

17 marca 2022 roku polska kolej doświadczyła jednej z największych awarii systemu sterowania ruchem. Błąd w oprogramowaniu firmy Alstom ZWUS sparaliżował zarządzanie ruchem na terenie 13 zakładów linii kolejowych, co poskutkowało:

- odwołaniem 457 pociągów,
- opóźnieniem 1 155 pociągów pasażerskich o 63 809 minut,
- opóźnieniem 173 pociągów towarowych o 64 770 minut,
- łącznym opóźnieniem wynoszącym 128 579 minut.

Firma Alstom przyznała, że przyczyną awarii był błąd w formatowaniu czasu, który wpłynął na funkcjonowanie sieci kolejowej i zakłócił transport w Polsce. Podkreślono jednak, że incydent nie był wynikiem cyberataku ani nie stanowił bezpośredniego zagrożenia dla pasażerów. W ramach działań naprawczych wdrożono plan przywrócenia sprawności systemów sterowania, mający na celu ograniczenie skutków awarii i minimalizację zakłóceń



Kolej na liczby

Liczba pasażerów w 2024 roku:

407,5 mln

(wzrost o 33,1 mln, czyli +8,8% w stosunku do 2023 roku). Jest to najwyższy wynik od 1997 roku (416,6 mln pasażerów).

Wskaźnik wykorzystania kolei wyniósł

10,8

statystycznie każdy mieszkaniec Polski korzystał z kolei prawie 11 razy w ciągu roku.

Średnia odległość podróży pasażerskiej w 2024 roku:

69,9 km

(wzrost z 69,1 km w 2023 roku).

W sektorze towarowym przewieziono

223,5 mln ton

ładunków – spadek o 8,1 mln ton (-3,5%) w porównaniu z poprzednim rokiem, co odpowiada wynikom z 2020 roku.

Średnia odległość przewozu jednej tony ładunku w 2024 roku:

260,7 km

nieznaczny spadek w porównaniu z 266 km w rekordowym roku 2023.

W grudniu 2024 roku z kolei skorzystało

33,2 mln

pasażerów, co oznacza wzrost o 1,8 mln osób (+5,7%) względem grudnia 2023 roku.

w ruchu kolejowym. Mimo powagi sytuacji Ministerstwo Infrastruktury nie uznało tego incydentu za wymóg uruchomienia oficjalnych procedur zarządzania kryzysowego, co zdaniem ekspertów mogło negatywnie wpłynąć na dalsze funkcjonowanie kolei.

Cyfryzacja kolei na razie na bocznicy

Sygnał radio-stop to awaryjny system zatrzymywania pociągów, działający poprzez nadanie komunikatu radiowego, który powoduje automatyczne uruchomienie hamulców w każdym pociągu w zasięgu sygnału. System ten powinien być kluczowym elementem bezpieczeństwa, wykorzystywanym w sytuacjach kryzysowych, takich jak nagłe zagrożenia na torach, awarie techniczne czy wypadki. Niestety, Polska wciąż korzysta z analogowego systemu sterowania ruchem, co niesie ze sobą poważne ryzyko. Na otwartych, nieszyfrowanych kanałach można swobodnie podsłuchać komunikację między maszynistami a dyżurnymi ruchu, co czyni system podatnym na manipulacje i sabotaż. W nocy z 25 na 26 sierpnia 2023 roku doszło do incydentu, podczas którego zatrzymało się 20 pociągów w czterech województwach – maszyniści usłyszeli w kabinach rosyjski hymn i przemówienie Władimira Putina. Zatrzymanie pociągu przy użyciu sygnału radio-stop jest banalnie proste – eksperci ostrzegają, że do zatrzymania dowolnego składu wystarczy łatwo dostępne urządzenie nadawcze, działające na tej samej częstotliwości co kolejowe systemy łączności. Dowodem tego jest reportaż „Przejazd niestrzeżony" przygotowany przez dziennikarki Olgę Orzechowską i Katarzynę Lazzeri.

W ostatnich latach odnotowano liczne przypadki nieuprawnionego nadania sygnału radio-stop przez osoby spoza kolei, co powodowało opóźnienia i chaos w ruchu pociągów. Modernizacja systemu, na przykład poprzez cyfryzację i zabezpieczenie przed nieautoryzowanym użyciem, jest kluczowa dla poprawy bezpieczeństwa przewozów. Tylko w pierwszym kwartale 2024 roku sygnał radio-stop został nadany w sposób nieuprawniony blisko 200 razy, powodując masowe opóźnienia pociągów zarówno pasażerskich, jak i towarowych. Oto konkretne liczby:

- 2020 r.: 488 przypadków (495 minut opóźnień),
- 2021 r.: 440 przypadków (1785 minut opóźnień),
- 2022 r.: 482 przypadki (560 minut opóźnień),
- 2023 r.: 561 przypadków (1494 minuty opóźnień).

Polska miała obowiązek wdrożyć nowoczesny system sterowania ruchem kolejowym, zgodnie z zobowiązaniami wynikającymi z członkostwa w UE. Projekt cyfryzacji kolei, wart ponad 9 mld złotych, rozpoczął się w 2013 roku, lecz do tej pory nie został zrealizowany. Mimo przeznaczenia środków na infrastrukturę system wciąż nie funkcjonuje w pełni. Były prezes PKP PLK, Ireneusz Merchel, tłumaczył opóźnienia pandemią, wojną w Ukrainie oraz problemami wykonawców. Tymczasem obecne kierownictwo PKP PLK przyznaje, że projekt został wstrzymany i nie wiadomo, kiedy zostanie ukończony.

Co dalej? Rekomendacje NIK

Nie wszystko na kolei działa źle. Raport NIK wskazuje na pozytywne i negatywne aspekty funkcjonowania podmiotów rynku kolejowego w sytuacjach kryzysowych. Choć istnieje rozbudowany system przepisów i regulacji kryzysowych, diabeł tkwi w szczegółach – niektóre procedury są niejasne, inne traktowane zbyt swobodnie. Potrzebne są kompleksowe rozwiązania oraz skuteczne mechanizmy kontroli. Spółki muszą regularnie weryfikować swoje procedury, a organy nadzoru – pilnować przestrzegania przepisów. Kluczowe jest, aby zalecenia pokontrolne nie pozostały jedynie na papierze, lecz przełożyły się na realne zmiany w funkcjonowaniu kolei. W końcu chodzi nie tylko o spełnienie formalnych wymogów, ale przede wszystkim o bezpieczeństwo systemu kolejowego w sytuacjach kryzysowych.

Czy polska kolej jest gotowa na przyszłe kryzysy? Raport NIK jednoznacznie pokazuje, że system wymaga pilnych zmian. Opóźnienia, awarie, niekontrolowane sygnały alarmowe oraz brak koordynacji działań mogą w doprowadzić do jeszcze poważniejszych konsekwencji. Rosnąca liczba pasażerów świadczy o popularności kolei – ale nie chodzi o to, by wsiąść do pociągu byle jakiego, lecz by ten pociąg bezpiecznie dotarł do celu.

Wnioski z kontroli – zalecenia NIK

Dla Prezesa Rady Ministrów:

- Włączenie UTK do systemu zarządzania kryzysowego – podjęcie działań nadzorczych w celu formalnego uwzględnienia Prezesa UTK w strukturach zarządzania kryzysowego na kolei, jako organu odpowiedzialnego za bezpieczeństwo ruchu kolejowego.
- Ujednolicenie planów zarządzania kryzysowego – inicjatywa legislacyjna doprecyzowująca zakres i zawartość planów kryzysowych opracowywanych przez ministrów oraz kierowników urzędów centralnych, zgodnie z ustawą o zarządzaniu kryzysowym. Obecne przepisy są niespójne i różnie interpretowane na poszczególnych szczeblach administracji, co utrudnia skuteczną koordynację działań.

Dla Ministra Infrastruktury:

- Stworzenie i wdrożenie szczegółowych procedur zarządzania kryzysowego na kolei – opracowanie kompleksowych zasad regulujących funkcjonowanie systemu zarządzania kryzysowego w sektorze kolejowym.
- Uregulowanie roli kluczowych uczestników systemu – uwzględnienie w nowych regulacjach specyfiki działalności wszystkich podmiotów zaangażowanych w zarządzanie kryzysowe, w tym spółek kolejowych oraz Prezesa UTK.

Monika Żuber-Mamakis
redaktorka „a&s Polska"

Głos branży

Bezpieczeństwo w transporcie i logistyce odgrywa kluczową rolę, ponieważ wpływa zarówno na ochronę życia ludzkiego, jak i na sprawność łańcuchów dostaw. Właściwe zabezpieczenie towarów minimalizuje ryzyko strat wynikających z uszkodzeń lub kradzieży. O tym, jak zapewnić właściwy poziom bezpieczeństwa w tym sektorze mówią przedstawiciele branży.

Zarządzanie bezpieczeństwem w centrach dystrybucyjnych

NATALIA BRZOZOWSKA, BCS

Współczesne centra dystrybucyjne i logistyczne to miejsca, w których odpowiednie zarządzanie bezpieczeństwem stanowi klucz do sprawnego ich funkcjonowania. Wymagają zaawansowanych rozwiązań technicznych, które zapewniają ochronę przed zagrożeniami i umożliwiają skuteczne administrowanie obiektem.

Dzięki integracji systemów w centralnym oprogramowaniu zarządzającym, operatorzy mogą łatwo śledzić obrazy z wielu kamer, przeglądać nagrania archiwalne oraz na bieżąco reagować na sytuacje alarmowe. Dzięki zastosowaniu nowoczesnych kamer IP, operatorzy nadzorują każdy zakątek obiektu w czasie rzeczywistym. Rozwiązania te oferują obraz wysokiej jakości, co pozwala na łatwą identyfikację osób, pojazdów oraz potencjalnych zagrożeń. W dużych obiektach, takich jak centra logistyczne, możliwość podglądu na żywo z kilkudziesięciu kamer jednocześnie znacząco zwiększa efektywność dozoru. Dodatkowo nowoczesne systemy przeciwpożarowe mogą współpracować z monitoringiem wizyjnym, co umożliwia szybkie zlokalizowanie źródła zagrożenia. Natomiast oprogramowanie zarządzające pozwala na połączenie systemów sygnalizacji włamania i napadu, umożliwiając zdalne sterowanie stanem uzbrojenia lub rozbrojenia centrali alarmowej bądź automatycznym kierowaniem kamer w stronę miejsca, w którym wykryto podejrzaną aktywność. W ten sposób operatorzy mogą skuteczniej koordynować działania ratunkowe lub inne, właściwe dla sytuacji.

Współczesne centra logistyczne korzystają z zaawansowanych rozwiązań, które łączą systemy CCTV, PPOŻ i SSWiN w jedną, zintegrowaną platformę. Taka integracja zapewnia szybszą reakcję na zagrożenia, ponieważ zgłoszenia alarmowe pochodzą z konkretnych kamer i czujek, co daje szybszy wgląd w sytuację na terenie obiektu. Dzięki centralnemu oprogramowaniu zarządzającemu, wykorzystując wysoką skalowalność i elastyczność systemu, można go dostosować do wielkości i specyfiki obiektu dystrybucyjnego.

W czasach, gdy bezpieczeństwo staje się jednym z kluczowych wymagań operacyjnych, centra logistyczne wyposażone w zaawansowane rozwiązania, które są w stanie zintegrować różne systemy, zyskują znaczną przewagę konkurencyjną. Dlatego marka BCS, aktywnie uczestnicząc w rozwoju rynku, stworzyła kompleksowe oprogramowanie, które spełnia potrzeby nawet najbardziej wymagających klientów centrów logistycznych.

Nowoczesne zabezpieczenia w logistyce

ADAM SAWICKI,
ekspert ds. bezpieczeństwa

Bezpieczeństwo w transporcie i logistyce jest kluczowe dla stabilności łańcucha dostaw. Kradzieże, cyberataki i nieautoryzowany dostęp wymagają wdrożenia nowoczesnych systemów ochrony, które zwiększają bezpieczeństwo i efektywność operacyjną. Z mojego już prawie 25-letniego doświadczenia wynika, że najważniejszymi aspektami bezpieczeństwa w transporcie i logistyce są:

- **Monitoring wizyjny i analiza obrazu** – telewizja dozorowa z inteligentną analizą obrazu umożliwia wykrywanie zagrożeń w czasie rzeczywistym. Systemy rozpoznawania twarzy, analiza zachowań i detekcja ruchu pozwalają szybko reagować na wtargnięcia i manipulowanie przy ładunku. Algorytmy sztucznej inteligencji rozpoznają odbiegający do wzorca ruch i przewidują potencjalne zagrożenia. Automatyczne alerty pozwalają służbom ochrony na szybsze działanie, minimalizując ryzyko strat.
- **Kontrola dostępu i ochrona infrastruktury** – ochrona magazynów, terminali i pojazdów wymaga zaawansowanych systemów autoryzacji: biometrycznych skanerów, RFID i inteligentnych kart dostęp. Integracja tych rozwiązań z systemem monitoringu wizyjnego pozwala na obserwowanie przemieszczania się osób i wykrywanie nieprawidłowości. Automatyczne alarmy zwiększają bezpieczeństwo i ograniczają ryzyko nieautoryzowanego dostępu.
- **Cyberbezpieczeństwo w transporcie** – systemy zarządzania transportem są narażone na cyberataki, które mogą powodować zakłócenia i straty. Wdrożenie szyfrowania danych,

wielopoziomowego uwierzytelniania (MFA) i systemów wykrywania zagrożeń (IDS/IPS) jest kluczowe dla ochrony cyfrowej. Regularne audyty i szkolenia pracowników ograniczają ryzyko ataków socjotechnicznych, takich jak phishing. Stosowanie zasady „zero trust" dodatkowo wzmacnia ochronę wrażliwych systemów. Inwestowanie w nowoczesne technologie minimalizuje ryzyko, zwiększa efektywność operacyjną i buduje zaufanie klientów.

Przedsiębiorstwa nie mogą sobie pozwolić na straty

TOMASZ GRZELAK,
DHL Exel Supply Chain (Poland)

Bezpieczeństwo w logistyce i transporcie stanowi jeden z kluczowych filarów sprawnego funkcjonowania łańcucha dostaw. Rosnące zagrożenia, takie jak kradzieże, sabotaże czy nieautoryzowany dostęp do stref załadunku i magazynów, zmuszają firmy do inwestowania w coraz bardziej zaawansowane systemy zabezpieczeń. W 2025 r. można spodziewać się intensyfikacji tych działań, ponieważ skala problemu rośnie, a przedsiębiorstwa nie mogą sobie pozwolić na straty wynikające z niewystarczającej ochrony.

Jednym z najważniejszych elementów skutecznego zabezpieczenia pozostaje monitoring wizyjny, który dzięki nowoczesnym technologiom umożliwia całodobową kontrolę zarówno nad pojazdami, jak i magazynami. Kamery o wysokiej rozdzielczości wspomagane przez analizę obrazu opartą na sztucznej inteligencji pozwalają na błyskawiczne wykrywanie takich zachowań, jak wtargnięcie na teren chroniony czy manipulacja przy ładunku.

Nie można zapominać o podstawowych, ale niezwykle skutecznych środkach ochrony, takich jak odpowiednie oświetlenie terenu, które pełni funkcję prewencyjną, znacząco ograniczając ryzyko włamań i aktów wandalizmu. W nowoczesnych centrach logistycznych coraz częściej stosuje się również systemy nagłośnieniowe, pozwalające na odstraszanie intruzów.

Kolejnym istotnym aspektem jest zabezpieczenie samego transportu. W ostatnich latach wzrosła liczba kradzieży towarów na postojach i w trakcie przeładunków, dlatego coraz więcej firm decyduje się zmiany dotychczasowych przyzwyczajeń. Bezpieczne strefy postojowe, parkingi wyposażone w monitoring i kontrolę dostępu, stają się standardem, zwłaszcza na kluczowych trasach międzynarodowych.

W przypadku transportu drogowego standardowe plomby mechaniczne często nie zapewniają wystarczającego poziomu ochrony, dlatego firmy inwestują w plomby elektroniczne z GPS i czujnikami otwarcia. W przypadku próby manipulacji system generuje alarm i powiadamia centrum monitoringu.

Patrząc na rok 2025, można spodziewać się dalszego wzrostu inwestycji w bezpieczeństwo fizyczne i techniczne. Cieszy mnie to, iż coraz więcej firm dostrzega zagrożenia oraz konsekwencje jakie z nich wynikają. Zwiększona liczba incydentów związanych z kradzieżami oraz wprowadzanie bardziej rygorystycznych regulacji prawnych sprawią, że kompleksowe systemy zabezpieczeń staną się nie tyle wyborem, co koniecznością.

Budowanie świadomości w zakresie bezpieczeństwa

ANDRZEJ CZAPLA, Orlen Paczka

Uważam, że dzisiejsza sytuacja geopolityczna, jak i w dalszym ciągu dynamicznie rozwijający się rynek sektora transportowo-logistycznego wymaga budowania świadomych i konsekwentnych procedur bezpieczeństwa. Wystarczy spojrzeć na dane statystyczne, które podaje TAPA *(The Transported Asset Protection Association).* Wynika z nich, że: „jedynie w grudniu 2024 r. dokonano kradzieży za kwotę 36,8 mln euro produktów w łańcuchu dostaw w regionie EMEA (Europa, Bliski Wschód i Afryka) zgłoszonych do systemu TIS (TAPA EMEA Intelligence System). Taka dwucyfrowa kwota utrzymywała się niezmiennie w czwartym kwartale 2024 r. Co prawda w tym zestawieniu zajmujemy jedno z ostatnich miejsc (zgłoszono jedynie pojedyncze przestępstwo z Polski) i pomimo tego, że pod względem przestępstw cargo „świecimy się" na zielono, to nie jesteśmy wolni od tego typu zagrożeń.

W mojej ocenie zabezpieczenia osobowe, mechaniczne czy elektroniczne to „minimum" w kwestii szeroko pojętego bezpieczeństwa i nie wyobrażam sobie funkcjonowania firmy logistycznej bez tych podstawowych narzędzi. Oczywiście, zawsze warto być na bieżąco z nowinkami technologicznymi, trendami w branży, ale najważniejszą kwestią jest budowanie świadomości bezpiecznego postępowania w branży kurierskiej zgodnie z wypracowanymi i ciągle aktualizowanymi zasadami. Jedynie w ten sposób jesteśmy wstanie skutecznie wdrożyć reguły prewencji i przeciwdziałać otaczającym nas zagrożeniom.

Dlatego w mojej ocenie bardzo ważnym aspektem jest prowadzenie szkoleń, przewidujących dużą aktywność uczestników i pracę na konkretnych przykładach. Takie szkolenia powinny być regularnie powtarzane i dotyczyć nie tylko nowoprzyjętych osób, ale i długoletnich pracowników. Nieświadomy zagrożeń w kwestii szeroko pojętego bezpieczeństwa pracownik zawsze będzie stanowił najsłabsze ogniwo wśród elementów security. Z drugiej strony odpowiedzialny w kwestii zagrożeń będzie stanowił o świadomej i konsekwentnej polityce bezpieczeństwa firmy logistycznej.

Skuteczna strategia bezpieczeństwa

MICHAŁ BADKE, Allegro

Zapewnienie odpowiedniego poziomu bezpieczeństwa w transporcie i logistyce wymaga podejścia łączącego aspekty fizyczne i cyfrowe. Kluczowe jest zabezpieczenie zarówno przepływu towarów, jak i informacji na każdym etapie łańcucha

Ilustracje: rawpixel

dostaw – od transportu surowców, przez produkcję, aż po dostarczenie gotowych produktów do odbiorcy.

W dobie dynamicznego rozwoju technologii i narzędzi opartych na sztucznej inteligencji przewagę zyskają ci, którzy potrafią je skutecznie wykorzystać. Dane gromadzone w postaci procedur, instrukcji, opisów incydentów czy raportów – wcześniej często stanowiące *gray data* trudne lub realnie niemożliwe do analizy – mogą dziś, dzięki nowoczesnym modelom przetwarzania informacji, zostać przekute w realne *know-how* i przełożyć się na realną poprawę bezpieczeństwa.

Kluczowymi elementami, które należy uwzględnić przy tworzeniu skutecznej strategii bezpieczeństwa są:

- **Zarządzanie ryzykiem** – stała analiza zagrożeń i zdolność do szybkiego reagowania w sytuacjach kryzysowych.
- **Procedury i standardy** – ich właściwe wdrażanie oraz ciągłe doskonalenie na wszystkich szczeblach organizacji.
- **Świadomość pracowników** – systematyczne szkolenia i budowanie kultury bezpieczeństwa.
- **Nowoczesne zabezpieczenia** – integracja technologii AI, systemów monitoringu i narzędzi analizy danych.

Współczesne zagrożenia obejmują nie tylko tradycyjne ryzyka operacyjne, ale także

- **Cyberprzestępczość** – ataki na systemy IT zarządzające logistyką.
- **Terroryzm** – zagrożenie dla infrastruktury krytycznej.
- **Nieuczciwą konkurencję** – kradzieże danych i sabotaż gospodarczy.
- **Zmienną sytuację polityczną i społeczną** – konflikty wpływające na globalne łańcuchy dostaw.

Tylko połączenie nowoczesnych technologii, analizy przeszłych zdarzeń oraz świadomego podejścia pracowników z właściwie zbudowanymi i ustawicznie kontrolowanymi systemami zabezpieczeń pozwoli skutecznie przeciwdziałać tym zagrożeniom i zapewnić stabilność oraz bezpieczeństwo sektora transportu i logistyki.

Automatyzacja i optymalizacja procesów logistycznych

ARTUR NOWAKOWSKI, Linc Polska

We współczesnych centrach logistycznych stosowane są zaawansowane technologie poprawiające efektywność i bezpieczeństwo procesów magazynowych. Jednym z kluczowych rozwiązań są roboty typu ARM *(Automated Robotic Manipulators),* które odgrywają istotną rolę w automatyzacji i optymalizacji procesów logistycznych.

Roboty ARM są wykorzystywane do wielu zadań, takich jak automatyczne przenoszenie, sortowanie i układanie towarów. Dzięki zastosowaniu zaawansowanej sztucznej inteligencji oraz czujników wizyjnych, roboty potrafią precyzyjnie wykonywać operacje, eliminując błędy ludzkie oraz przyspieszając procesy logistyczne.

Aby zapewnić bezpieczną współpracę ludzi i maszyn, w nowoczesnych centrach logistycznych wdraża się rygorystyczne procedury bezpieczeństwa. Roboty wyposażone są w czujniki i systemy wykrywania kolizji, a także system *geofencing,* który pozwala ograniczać ich przemieszczanie się w granicach wyznaczonych stref. Nowoczesne technologie pozwalają również na minimalizowanie ryzyka wypadków w magazynach. Inteligentne oprogramowanie wspomagane sztuczną inteligencją przewiduje sytuacje awaryjne i zapobiega kolizjom robotów.

Jednocześnie system kamer wspomagany przez rozwiązania AI, jak np. Camect Smart Hub umożliwia monitorowanie całej przestrzeni centrum logistycznego. Dzięki „umiejętności" rozróżniania obiektów alarm będzie aktywowany dopiero, gdy w strefę przeznaczoną dla robotów wkroczy człowiek.

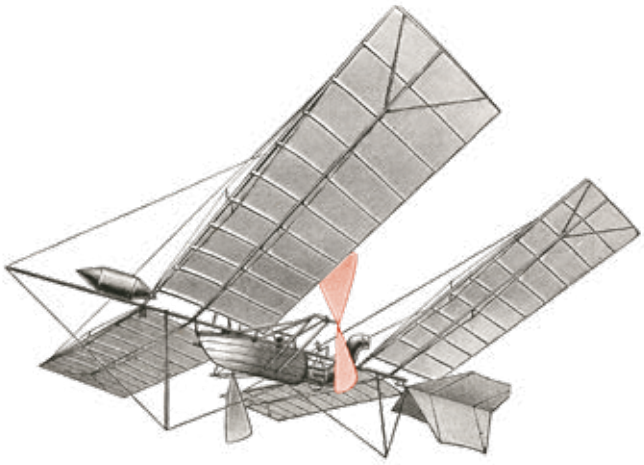
Wdrożenie nowoczesnych technologii w centrach logistycznych pozwala na znaczne usprawnienie procesów operacyjnych oraz poprawę bezpieczeństwa pracy. Rozwiązania sztucznej inteligencji stanowią przyszłość logistyki, zwiększając wydajność i minimalizując ryzyko błędów oraz wypadków.

Wszyscy odpowiadamy za bezpieczeństwo na kolei

MIROSŁAW LUKOWSKI,
ekspert ds. bezpieczeństwa

Zapewnienie bezwzględnego bezpieczeństwa pasażerom, pracownikom i całej infrastrukturze jest warunkiem niezbędnym, by transport kolejowy mógł funkcjonować sprawnie. Kolej jest jednym z najbezpieczniejszych środków transportu, ale aby tak było, wymaga ciągłego monitorowania i doskonalenia procedur bezpieczeństwa.

Nowoczesne systemy bezpieczeństwa na kolei obejmują m.in. monitoring wizyjny, detektory dymu i ognia oraz systemy alarmowe. W przypadku wykrycia zagrożenia informacje są natychmiast przekazywane do centrali, co umożliwia szybką interwencję. Takie działanie to gwarancja bezpieczeństwa. Motorem napędowym zmian przepisów i wymogów w dzisiejszym niestabilnym świecie jest szeroko pojęte zrozumienie zagrożeń wynikających zarówno z działań wojennych w Ukrainie, jak i z niestabilnej sytuacji na Bliskim Wschodzie. Tak prozaiczne rozwiązania, jak przezroczyste kosze na śmieci, są tylko jednym z podstawowych elementów struktury bezpieczeństwa wspieranej nowoczesną technologią.



Dziś w dobie AI systemy telewizji dozorowej są wspierane zaawansowaną analityką, która pozwala na wykrycie pozostawionego bagażu czy przekroczenia bezpiecznej strefy. To standard. Kamery są w stanie rozpoznać niepożądane zachowanie (np. próby samobójcze lub włamania) i przekazać informację o nim właściwym służbom. Aby było to możliwe, niezbędne są precyzyjne procedury i standardy pracy, nie pozwalające na obniżenie jakości instalowanych systemów czy zastosowanych materiałów. Przestrzeganie tych regulacji jest kluczowe dla utrzymania wysokiego poziomu bezpieczeństwa.

Wszystkie firmy związane z transportem kolejowym mają świadomość, iż każdego dnia od standardu ich pracy zależy bezpieczeństwo pasażerów oraz infrastruktury tak ważnej dla bezpieczeństwa państwa. Zmieniająca się rzeczywistość, wojna hybrydowa i cyfrowy świat oznaczają, że każdego dnia pojawiają się nowe zagrożenia. Dlatego dla utrzymania wysokiego standardu bezpieczeństwa tak ważne jest, by personel kolejowy, składający się z maszynistów, konduktorów i obsługi stacji był dobrze przeszkolony. Regularne szkolenia z zakresu bezpieczeństwa, pierwszej pomocy oraz procedur awaryjnych są niezbędne. Ważne jest, aby personel potrafił szybko i skutecznie reagować na sytuacje kryzysowe. Perfekcyjna obsługa i znajomość wszystkich systemów zabezpieczeń pozwala przeciwdziałać takim sytuacjom i minimalizować ich skutki, a czasami nawet nie dopuścić do pojawienia się groźnej sytuacji.

Musimy mieć świadomość, że za bezpieczeństwo kolei odpowiadają nie tylko odpowiednie służby, ale i my wszyscy, jako pasażerowie i obywatele. Promowanie kultury bezpieczeństwa wśród pracowników i pasażerów jest kluczowe. Obejmuje to edukację na temat bezpiecznego zachowania na stacjach i w pociągach, a także kampanie informacyjne dotyczące przestrzegania zasad.

Odpowiedni dobór systemu kontroli dostępu

ŁUKASZ GLINIECKI, Roger

System kontroli dostępu w obiektach sektora transportu i logistyki pełni kluczową rolę w zapewnieniu bezpieczeństwa, ochrony zasobów oraz optymalizacji procesów operacyjnych. Odpowiedni dobór tego systemu wpływa nie tylko na redukcję ryzyka nieuprawnionego dostępu, ale także na zwiększenie efektywności operacyjnej i sprawność funkcjonowania całej infrastruktury.

W branży transportowej i logistycznej obiekty, takie jak magazyny, terminale przeładunkowe, porty czy centra dystrybucyjne, są narażone na zagrożenia związane z kradzieżami, sabotażem oraz niekontrolowanym ruchem osób i pojazdów. Zastosowanie zaawansowanych technologii, takich jak wieloetapowa weryfikacja, odpowiednio skonfigurowane karty oraz czytniki RFID, pozwala na precyzyjną weryfikację tożsamości pracowników i dostawców, co znacznie podnosi poziom bezpieczeństwa.

Kolejnym aspektem jest zgodność z regulacjami prawnymi i normami branżowymi. Wdrożenie odpowiedniego systemu kontroli dostępu umożliwia spełnienie wymagań dotyczących ochrony infrastruktury krytycznej, a także zabezpiecza dane i towary przed dostaniem się w niepowołane ręce.

Zaawansowane systemy kontroli dostępu integrujące się z innymi rozwiązaniami, np. systemami telewizji dozorowej umożliwiają ciągłe monitorowanie chronionego obiektu, minimalizują ryzyko nieautoryzowanego dostępu oraz pozwalają na szybką weryfikację poruszających się w nim osób.

Automatyzacja procesów związanych z zarządzaniem dostępem umożliwia szybsze i bardziej efektywne przeprowadzanie operacji logistycznych. Pracownicy, kontrahenci i dostawcy mogą łatwiej uzyskać dostęp do niezbędnych stref w odpowiednich godzinach, co skraca czas oczekiwania i przyspiesza realizację zamówień. Odpowiedni dobór systemu kontroli dostępu w obiektach transportowych i logistycznych to nie tylko kwestia bezpieczeństwa, ale także kluczowy element optymalizacji operacji i spełnienia wymogów regulacyjnych. Inwestycja w nowoczesne rozwiązania przekłada się na większą kontrolę, mniejsze ryzyko strat oraz lepszą organizację pracy.

Cyberzagrożenia w sektorach transportu i logistyki

DANIEL KAMIŃSKI, Orange

Jednym z najdotkliwszych zagrożeń w sektorze transportu i logistyki są ataki ransomware, głównie dlatego, że powodują przerwy w dostawach. Przestój może trwać od kilku tygodni do nawet 3 miesięcy. Obecnie Polska zajmuje 7 miejsce na liście najczęściej atakowanych krajów za pomocą tego złośliwego oprogramowania. Szczególnie duża aktywność była w drugiej połowie 2024 r., gdzie według danych ESSET odnotowano 37% wzrost ataków w stosunku do pierwszego półrocza.

Historia uczy nas pokory, dlatego warto wrócić do największych ataków ransomware w historii, czyli WannaCry i NotPetya. WannaCry zainfekował dużą liczbą komputerów, ponieważ wiele osób nie instalowało poprawek w oprogramowaniu. Podobnie z NotPetya, który dotknął największe firmy transportowe i agencje rządowe. Maersk ocenił straty na 300 mln USD, Fedex na 400 mln USD. Szacuje się że całkowite szkody wywołane przez atak wyniosły 10 mld USD.

Problem dotyczył również Polski. Poszkodowane były m.in. firmy z branży motoryzacyjnej, transportowej i logistycznej. Cyberatak potraktowano jak działania wojenne, z tego powodu ubezpieczyciele odmówili wypłaty ubezpieczenia. Sprawy o odszkodowania utknęły w sądach, dopiero po kilku latach ubezpieczyciele i poszkodowani podpisali ugody. Tamte wydarzenia wpłynęły na obecne ubezpieczenia wykluczające cyberataki, w których aktywność hakerów sponsorują obce kraje.

Atak NotPetya był na tyle poważny, że pierwszy raz w Polsce Rządowy Zespół Zarządzania Kryzysowego, podjął decyzję o współpracy z CERT-ami, szkoleniach pracowników, kwestiach wykonywania kopii bezpieczeństwa oraz aktualizacji systemów.

Kluczowe trendy globalnego rynku bezpieczeństwa

Raport przygotowany przez amerykańskie stowarzyszenia ASIS International oraz Security Industry Association (SIA) przy wsparciu brytyjskiej firmy analityczno-doradczej Omdia przedstawia najważniejsze trendy, które wpływają na rynek bezpieczeństwa fizycznego. To sztuczna inteligencja, chmura obliczeniowa oraz mobilne poświadczenia będą miały na branżę największy wpływ.

Rynek już jest wart miliardy dolarów, a przecież...

...wiele wskazuje, że branża nie powiedziała jeszcze ostatniego słowa. W roku 2022 wartość globalnego rynku urządzeń do ochrony fizycznej wyniosła 51 mld USD. A już w przyszłym 2026 roku, według prognoz ekspertów, wartość ta ma wzrosnąć do 70 mld USD, co przekłada się na średnioroczny wzrost na poziomie 8,2%.

Jeszcze lepiej radzą sobie usługi bezpieczeństwa. W roku 2022 wartość rynku tych usług oszacowano na 298 mld USD, a do 2026 r. ma być to 389 mld USD. To łącznie niemal pół biliona dolarów w sektorze, który odgrywa kluczową rolę w gospodarce globalnej.

Innowacje zmieniają krajobraz branży

Sztuczna inteligencja, integracja systemów chmurowych oraz analiza danych zwiększają możliwości rozwiązań bezpieczeństwa. Jednocześnie nieco łagodzą skutki zmian demograficznych, ale też społecznych, bolesnych szczególnie dla krajów europejskich. Globalnie branża angażuje ponad 30 mln osób, z czego 7,87 mln pracuje w sektorze usług, 210 tys. zajmuje się produkcją urządzeń, a 22,6 mln to użytkownicy końcowi. To całkiem spora społeczność osób dbających o to, by świat był bezpieczniejszy: producentów, instalatorów, pracowników ochrony i menedżerów ds. bezpieczeństwa. Czy mogłoby tych osób być więcej? Zapewne tak, ale nie tylko Polska zmaga się z brakiem chętnych do pracy. Dlatego coraz więcej firm inwestuje w rozwiązania techniczne. Do roku 2027 ponad 60% przychodów z kamer sieciowych i rejestratorów ma pochodzić z urządzeń wyposażonych w algorytmy sztucznej inteligencji lub głębokiego uczenia. Na znaczeniu zyskuje też chmura hybrydowa, szczególnie w Ameryce Północnej.

Rynki regionalne – liderzy i nowi gracze
Pod względem finansowym najlepiej radzą sobie firmy z Ameryki Północnej, Europy i Chin. Łącznie odpowiadają za 75% globalnych przychodów. Chiny dominują w segmencie produkcji urządzeń, podczas gdy Ameryka Północna przoduje w usługach. Nie zmienia to faktu, że nieźle radzą sobie też organizacje funkcjonujące w Ameryce Łacińskiej, na Bliskim Wschodzie i Afryce oraz w regionie Azji i Oceanii.

Europa – niedostatecznie mocny łańcuch dostaw
Podobnie jak inne regiony naszego globu Europa długo zmagała się z problemami związanymi z niepewnością dostaw. Kolejnym wyzwaniem była inflacja. Wiele jednak wskazuje, że największą inflację mamy już za sobą. Konflikt w Ukrainie nie pozwala na długoterminowe prognozy polityczne, a co za tym idzie na przewidywania dotyczące gospodarki.

ESG wpływa na branżę
Audyty związane z ochroną środowiska, odpowiedzialnością społeczną i zarządzaniem (ESG) stają się coraz ważniejsze, zwłaszcza na rynku zachodnioeuropejskim. W sektorze kontroli dostępu obawy dotyczące zgodności z RODO oraz kwestie higieniczne tradycyjnych czytników linii papilarnych z zastosowaniem dotyku przyczyniły się do spadku popytu w Europie na ten rodzaj urządzeń.

Zauważalny jest wzrost rozwiązań ochrony perymetrycznej, powszechnie stosuje się je w krajach południowej Europy, takich jak Hiszpania i Włochy. W wielu krajach zachodnioeuropejskich zwiększa się średni rozmiar instalacji, a w miarę wzrostu zapotrzebowania są dodawane dodatkowe akcesoria.

Najbardziej dynamicznie w Europie rozwija się sektor centrów danych, związanych z koniecznością obsługi olbrzymiej ilości danych gromadzonych m.in. przez urządzenia stosowane w ochronie. Rozwój budownictwa napędza też instalację systemów zabezpieczeń w budynkach komercyjnych i mieszkaniowych. Zauważalny jest również wzrost nakładów na systemy zabezpieczeń w sektorze handlu detalicznego.

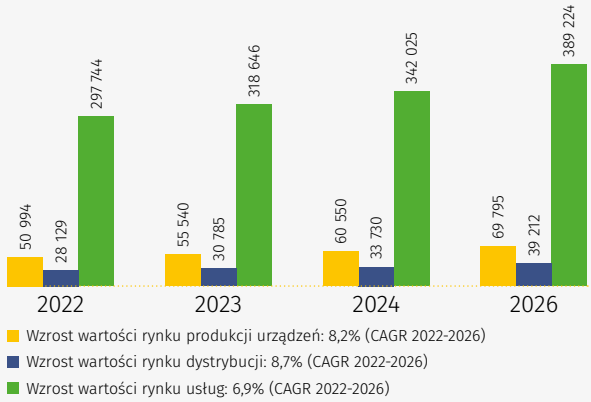
Przyszłość branży bezpieczeństwa
Im więcej techniki, tym mniejsza zależność od tradycyjnych metod ochrony, takich jak patrole, coraz częściej zastępowane przez zautomatyzowane urządzenia wykorzystujące robotykę i analitykę wideo. Systemy integrujące zarządzanie budynkami (BMS) z rozwiązaniami bezpieczeństwa dają nowe możliwości optymalizacji zużycia energii i koordynacji procesów operacyjnych. Kluczowe również będzie dostosowanie się do globalnych trendów, takich jak zrównoważony rozwój, poprzez wdrażanie ekologicznej alternatywy, np. mobilnych poświadczeń zamiast plastikowych kart.

Wnioski z raportu wskazują, że branża bezpieczeństwa będzie nadal ewoluować, dostosowując się do nowych wyzwań i potrzeb rynku globalnego. Zrównoważony rozwój, innowacje technologiczne oraz skuteczna adaptacja do lokalnych warunków rynkowych okażą się kluczowe dla przyszłego sukcesu sektora.

Redakcja „a&s Polska"

Ilustracje: freepik

Światowy rynek security 2022-2026
Rynek urządzeń i usług związanych z zabezpieczeniami



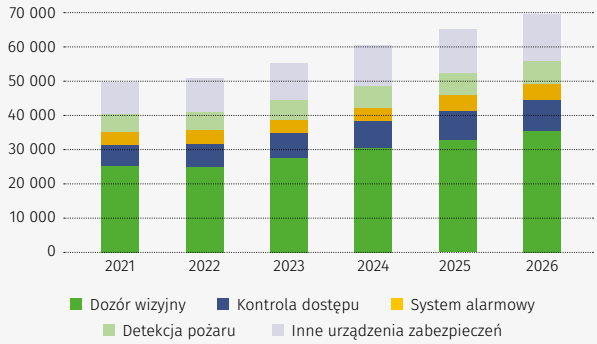
Szacunkowa liczba osób w sektorze security

210 000 produkcja urządzeń

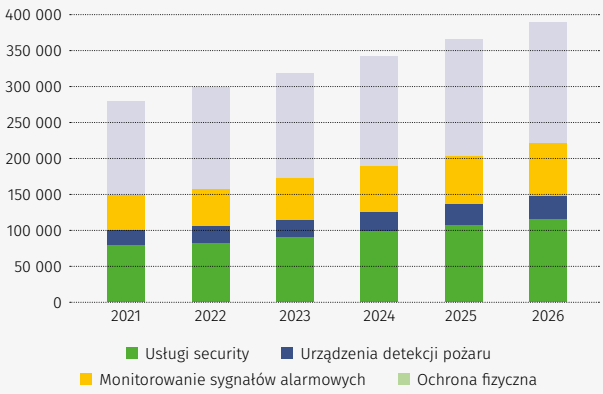
7 865 000 usługi

22 600 000 użytkownicy końcowi

Rynek usług zabezpieczeń w podziale na typy



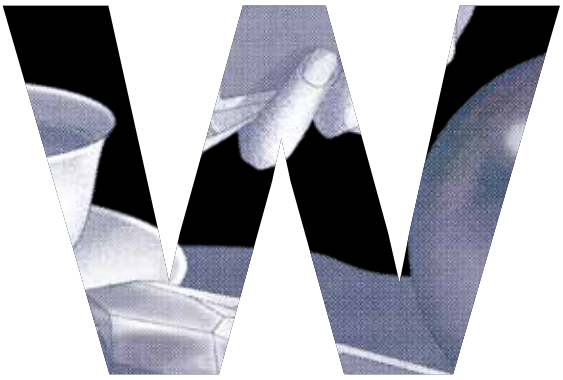
Rynek urządzeń zabezpieczeń w podziale na typy



Podsumowanie roku 2024 **i prognozy** na 2025

Rok 2024 okazał się czasem dynamicznych przemian, intensywnych wyzwań oraz nowatorskich rozwiązań w branży zabezpieczeń. Zarówno producenci, jak i klienci branży muszą się mierzyć z nowymi regulacjami. Jak firmy security poradziły sobie z tymi wyzwaniami i jakie mają plany na ten rok?

Monika Żuber-Mamakis



Wypowiedzi przedstawicieli firm branżowych dają pewien obraz sytuacji na polskim rynku. Oczywiście, każda z tych osób patrzy na rynek ze swojej perspektywy, a dokładnie z perspektywy reprezentowanej przez siebie firmy, ale przecież wszystkie zmagają się z podobnymi wyzwaniami i każda z nich ma też nadzieję, że rok 2025 będzie lepszy.

Krzysztof Bartuszek, Prezes Zarządu spółek Securitas w Polsce, przedstawił rok 2024 jako okres intensywnej pracy, w którym firma musiała zmierzyć się z licznymi wyzwaniami rynkowymi. Zwrócił uwagę, że oprócz oczywistej polaryzacji rynku – gdzie z jednej strony pojawiali się klienci stawiający na jakość, a z drugiej ci poszukujący oszczędności kosztem bezpieczeństwa – istotną rolę odegrały zmiany strukturalne oraz systemowe. Podkreślił, iż firma zainwestowała w rozwój zespołu oraz wdrożenie nowoczesnych narzędzi, takich jak globalny system ERP i wyspecjalizowane aplikacje wspomagające zarządzanie ochroną. Jak sam stwierdził, rok 2024 był dla Securitas Polska okresem, w którym *klienci coraz bardziej doceniali wartość długoterminowej jakości, mimo iż część kontrahentów decydowała się na rozwiązania oszczędnościowe, co wiązało się z większym ryzykiem operacyjnym.* W swoich uwagach Bartuszek przekazał, że firma konsekwentnie rozwijała swoje kompetencje, stawiając na szkolenia kadry oraz inwestycje w technologie umożliwiające szybsze reagowanie na potrzeby rynku.

Reprezentujący **Axis Communications Poland Konrad Badowski** zajmujący w firmie stanowisko **Business Relationships Managera** za najważniejsze dla firmy w zeszłym roku uznał wdrożenie układu ARTPEC 9. generacji, co miało fundamentalne znaczenie dla rozwoju technologii monitoringu. Firma wprowadziła szereg ulepszeń, w tym lepszą analitykę wspomaganą sztuczną inteligencją oraz zaawansowane mechanizmy cyberbezpieczeństwa. Jak podkreślił, *wdrożenie wsparcia dla standardu AV1 – nowoczesnego sposobu kodowania wideo – umożliwiło uzyskanie najwyższej jakości obrazu przy jednoczesnej optymalizacji przepływu danych.* Zauważył, że zmiany te nie tylko poprawiły jakość produktów, ale także umożliwiły firmie poszerzenie oferty w zakresie zaawansowanych rozwiązań dozorowych. *– Wsparcie dla AV1, czyli nowoczesnego standardu kodowania wideo, zapewnia najwyższą jakość obrazu przy zachowaniu optymalnej*

KONRAD BADOWSKI
Axis Communications Poland

W 2025 roku Axis skupi się na wzmacnianiu współpracy z partnerami oraz organizacji szkoleń, takich jak Meet Axis czy „Śniadanie z Axis". Intensyfikowane będą spotkania z klientami, z dedykowanymi szkoleniami i demoshow, a także obecność na wydarzeniach branżowych, takich jak Security BootCamp, Warsaw Security Summit 2025 i POLSECURE. Firma planuje także współpracę ze stowarzyszeniami branżowymi, szczególnie w przemyśle i infrastrukturze krytycznej. Sztuczna inteligencja w dozorze wizyjnym pozostaje kluczowym obszarem, z nowymi funkcjami, jak wykrywanie odzieży ochronnej. Axis rozwija innowacje w układach SoC ARTPEC oraz wprowadza kamery termowizyjne z AI i zabezpieczeniami kryptograficznymi, które zapewniają niezawodne wykrywanie przy minimalnych fałszywych alarmach.

KRZYSZTOF BARTUSZEK
Securitas Polska

Ubiegły rok był czasem dalszej polaryzacji rynku. Część klientów stawia na jakość i bezpieczeństwo, inni szukają oszczędności kosztem ryzyka. Niespodzianką było za to kolejne odroczenie zmian dotyczących umów zleceń. My skupiliśmy się na inwestycjach – w zespół, nowe struktury i technologie, m.in. globalny system ERP oraz aplikacje Guarding Platform, MySecuritas i Advisor. W 2025 roku planujemy pełne wykorzystanie wdrożonych narzędzi, rozwój kadry i zwiększenie udziału w rynku poprzez nowoczesne produkty i intensyfikację działań sprzedażowych. Otwieramy się także na potencjalne przejęcia. Skuteczny system ochrony opiera się na czterech filarach: ludziach, technologii, procedurach i danych. Kluczowa jest analiza ryzyka – tu pomaga nasza aplikacja Advisor, pozwalająca na precyzyjne prognozowanie zagrożeń i budowanie efektywnych strategii bezpieczeństwa.

Przedsiębiorstwa z sektora zabezpieczeń obecne na polskim rynku przez wiele lat zdążyły wypracować strategie, które pozwolą im sprostać nadchodzącym wyzwaniom. Prognozy na rok 2025 wskazują, że kluczowymi trendami będą rozwój sztucznej inteligencji, integracja systemów oraz wdrażanie innowacyjnych rozwiązań biometrycznych. Ciągły rozwój to podstawa.

HARALD DINGEMANS
Linc Polska

Niestabilna sytuacja geopolityczna wymusza nowe podejście do polityki bezpieczeństwa w skali zarówno makro, jak i mikro. Jako Linc Polska od lat promujemy wielowarstwowe zabezpieczenia, łącząc nowoczesne technologie z doświadczeniem w ochronie infrastruktury krytycznej i przemysłowej. Cały czas rozwijamy technologie wykrywania i neutralizacji dronów, które stają się coraz większym zagrożeniem. A oferowane przez Linc Polska mobilne wieże monitoringu iTower oraz systemy nadzoru zasilane ogniwami EFOY Pro wpisują się w koncepcję elastycznych i autonomicznych rozwiązań zabezpieczeń. Patrząc w przyszłość, kluczowe pozostają sprawdzone relacje z partnerami i klientami, którzy reprezentują najwyższy poziom w swoich branżach. Dzięki tej współpracy możemy stale rozwijać ofertę i reagować na nowe wyzwania.

ROBERT GAWROŃSKI
TP-Link

Rok 2024 był pełen wyzwań, ale zakończył się pozytywnie. Pierwsza połowa roku przyniosła spowolnienie rynku i niepewność co do zamówień, jednak druga połowa to powrót do wzrostów. Kluczowe było szybkie dostosowanie się do zmian i rozwój rozwiązań chmurowych, w tym Omada SDN. Dużym sukcesem było także poszerzenie oferty systemów monitoringu VIGI z zaawansowaną analizą obrazu. W bieżącym roku planujemy dalszy rozwój Omada SDN, nowe modele kamer VIGI z AI oraz intensyfikację działań edukacyjnych dla klientów i partnerów. Jako sygnatariusz „Secure by Design" stawiamy na cyberbezpieczeństwo – nasze rozwiązania, jak szyfrowanie WPA3-Enterprise czy VLAN, są dostępne bez dodatkowych opłat. Edukacja w zakresie bezpieczeństwa pozostanie jednym z naszych priorytetów.

Ilustracje: envato

przepływowości bitowej – stwierdził K. Badowski, podkreślając, że wdrożone rozwiązania techniczne będą miały długofalowy wpływ na rozwój systemów monitoringu zarówno lokalnie, jak i w chmurze.

Robert Gawroński, B2B Channel Manager w firmie TP-Link, przedstawił rok 2024 jako okres złożony, w którym pierwsza jego część upłynęła pod znakiem pewnego spowolnienia wzrostu i opóźnienia w realizacji projektów. W swoich analizach zauważył, że rynek wykazywał tendencję do wyhamowywania, co było związane m.in. z niepewnością dotyczącą zamówień publicznych. Druga połowa roku przyniosła jednak znaczące ożywienie. – *Firma TP-Link, wykorzystując rosnące zainteresowanie rozwiązaniami chmurowymi, podjęła działania zmierzające do rozwoju funkcjonalności platformy Omada SDN, umożliwiającej zdalne zarządzanie siecią. Elastyczne podejście i szybkie dostosowanie się do zmieniających się warunków rynkowych pozwoliły na realizację założonych celów biznesowych.*

Z kolei **Wojciech Weissenberg, CTO squareTec**, zwrócił uwagę na wyzwania mijającego roku, podkreślając, że *zbyt wcześnie jest na prawdziwe podsumowanie, rok nie należał do łatwych z uwagi na zawirowania w istotnym dla nas sektorze publicznym.* Choć wiele firm z branży ochrony osób i mienia zmagało się z tymi trudnościami, **Miwi Urmet** wypracowało stabilną pozycję. Jak zauważył **dyrektor handlowy Mariusz Garbacz**, *rok 2024 to dla Miwi Urmet w dużej mierze kontynuacja działań w zakresie dostaw do obiektów resortu obrony narodowej.* Każda z tych firm ma więc inne doświadczenia z sektorem publicznym. Niezależnie jednak od tego, zawsze warto stawiać na dywersyfikację odbiorców. Ubiegły rok pokazał, że użytkownicy coraz bardziej świadomi są swoich potrzeb i wybierają funkcjonalne, bezpieczne i niezawodne rozwiązania.

Na problematyce regulacyjnej oraz rosnącej roli sztucznej inteligencji w swojej wypowiedzi skupił się **Jarosław Grzybowski, Channel Team Director w Hikvision Poland.** Zauważył, że w 2024 roku pojawiło się wiele nowych przepisów, które często były źle interpretowane przez rynek, co utrudniało wdrażanie nowoczesnych systemów zabezpieczeń. Podkreślił, że firmy z sektora musiały inwestować nie tylko w cyberbezpieczeństwo, ale

MARIUSZ GARBACZ
Miwi Urmet

Rok 2024 to dla Miwi Urmet kontynuacja dostaw dla resortu obrony narodowej, ale także przełamanie dotychczasowego trendu związanego z dostawami do tego typu instytucji głównie urządzeń z zakresu telewizji dozorowej. Skutecznie rozszerzyliśmy te dostawy o system Protege klasy Grade 4, realizujący funkcje kontroli dostępu oraz wizualizację zdarzeń. Klienci coraz częściej wybierali też rozwiązania Milesight, w tym oprogramowanie VMS. W 2025 roku planujemy dalsze dostawy do sektora infrastruktury krytycznej, w tym energetycznego i medycznego. Kluczowe będą integracja systemów i zaawansowana analiza obrazu oparta na AI, które podnoszą skuteczność ochrony i usprawniają obsługę w wielosystemowych wdrożeniach.

JAROSŁAW GRZYBOWSKI
Hikvision Poland

Nie możemy narzekać na minione miesiące. Rok 2024 zakończył się dla Hikvision Poland bardzo pozytywnie. Dynamiczny rozwój rynku zabezpieczeń technicznych, wzrost zapotrzebowania na systemy monitoringu i rozwój AI stworzyły duże możliwości. Trudnością były nowe regulacje oraz rosnąca presja na cyberbezpieczeństwo, wymagająca inwestycji w ochronę danych. Sukcesem było poszerzenie oferty o kamery 4K, rozwiązania AI i produkty non-video, a także rozwój sieci lojalnych partnerów. Zaskoczeniem okazało się przyspieszenie postępu technologicznego, zwłaszcza w AI i IoT. Teraz Hikvision skupi się na dalszym rozwoju AI i analizie obrazu, podnoszeniu standardów cyberbezpieczeństwa oraz rozwoju dedykowanych rozwiązań dla branż wertykalnych, takich jak retail, transport czy logistyka. Ważnym elementem strategii będzie edukacja rynku poprzez intensyfikację szkoleń. Innowacje w monitoringu, w tym AI i analiza obrazu, rewolucjonizują branżę, podnosząc efektywność, automatyzację i integrację systemów. Hikvision planuje dalsze inwestycje w te technologie, rozwój rozwiązań chmurowych oraz wzmacnianie poziomu bezpieczeństwa i prywatności w swoich produktach.

również w integrację systemów monitoringu wizyjnego z innymi rozwiązaniami technologicznymi. Jego zdaniem rosnąca potrzeba centralizacji zarządzania bezpieczeństwem stała się impulsem do rozwoju platform chmurowych, takich jak Hik-Central, które umożliwiają scentralizowaną analizę danych. – *Producenci muszą inwestować w cyberbezpieczeństwo, a jednocześnie zapewniać innowacje, które zwiększą skuteczność monitoringu i zarządzania infrastrukturą miejską* – wyjaśnił, wskazując na konieczność połączenia tradycyjnych systemów dozorowych z nowoczesnymi rozwiązaniami bazującymi na sztucznej inteligencji.

Łukasz Kanarek, Dyrektor Sprzedaży Krajowej i Obsługi Klienta w firmie **Roger,** przedstawił perspektywę sektora kontroli dostępu, podkreślając rosnące znaczenie cyberbezpieczeństwa w kontekście integracji systemów. Zauważył, że firma planowała wprowadzenie nowych produktów, które będą obsługiwać najnowsze standardy technologiczne, takie jak MIFARE® DESFire®, a także rozwijać rozwiązania dedykowane dla coraz bardziej wymagających projektów. Jego wypowiedź miała charakter prognostyczny, gdyż podkreślił, że rosnące wymagania klientów będą stymulowały dalszy rozwój oferty firmy, a integracja systemów zabezpieczeń stanie się kluczowym elementem budowania kompleksowych rozwiązań. Natomiast **Kinga Zarzycka, Distribution BU General Manager z ZKTeco Europe,** pytana o plany, skupiła się na przyszłości biometrii oraz roli nowatorskich narzędzi w obszarze kontroli dostępu. W swoich analizach stwierdziła, że technologia *palm-vein*, oparta na analizie kształtu i naczyń krwionośnych dłoni, stanowi nowoczesną metodę identyfikacji, która spełnia europejskie normy dotyczące sztucznej inteligencji. Przekazała, że system ten jest nie tylko bezkontaktowy, ale również zapewnia wysoki poziom bezpieczeństwa, co jest szczególnie ważne w dobie rosnących zagrożeń cybernetycznych. Wyjaśniła też, że ZKTeco Europe dynamicznie rozwija markę premium Armatura, dedykowaną projektom wymagającym najwyższych standardów zabezpieczeń.

– *To nowoczesna, bezkontaktowa metoda identyfikacji, zgodna z europejskimi regulacjami dotyczącymi sztucznej inteligencji* – podkreśliła **Kinga Zarzycka**, dodając, że rozwój tej technologii oraz wdrożenie nowej marki stanowią fundament przyszłych innowacji w sektorze.

Jaki będzie 2025 rok? To się okaże...

Każdy kolejny rok wydaje się... ciekawszy od poprzedniego, w rozumieniu chińskiego przysłowia o ciekawych czasach. W biznesie nie mówi się o problemach, lecz o wyzwaniach. Tych, zdaniem branżowych ekspertów, w roku 2025 raczej nie zabraknie. Częściowo ze względu na sytuację geopolityczną na całym świecie, częściowo ze względu na zbliżające się w kraju wybory prezydenckie, a po troszę ze względu na rozpychające się kolejne wersje sztucznej inteligencji. Próba destabilizacji sytuacji w naszym kraju może odbić się na firmach nie tylko reprezentujących infrastrukturę krytyczną. Rykoszetem mogą „oberwać" też mniejsze firmy.

To, co obecnie dzieje się na świecie, ale i w kraju, to żadną miarą nic pożądanego, ale... dla branży ochrony osób i mienia to rodzaj biznesowej szansy. Szansy, której wykorzystanie ułatwić może między innymi rozwój technologii chmurowych, integracja systemów zabezpieczeń oraz wdrażanie rozwiązań opartych na sztucznej inteligencji. Każda z omawianych firm zaprezentowała swoje plany na nadchodzący rok, wskazując na konieczność dalszej profesjonalizacji usług oraz inwestycji w nowoczesne narzędzia technologiczne.

ŁUKASZ KANAREK
Roger

Pomimo wyzwań w branży budowlanej, rok 2024 zakończył się dla firmy Roger zgodnie z planowanym wzrostem sprzedaży. Dywersyfikacja przychodów pozwoliła na realizację projektów w sektorze publicznym, takich jak służba zdrowia, więziennictwo czy uczelnie. Wzrosło także zainteresowanie platformą VISO SMS, umożliwiającą zarządzanie i integrację systemów bezpieczeństwa na obiektach. W 2025 roku firma planuje premierę nowego kontrolera dostępu, dostosowanego do najbardziej wymagających projektów. Wprowadzi także nową linię czytników zbliżeniowych obsługujących MIFARE® DESFire® oraz identyfikację mobilną BLE/NFC. Popularność elektronicznych depozytorów kluczy RKD32 skłoniła firmę do rozszerzenia oferty o model RKD64, umożliwiający deponowanie większej liczby kluczy. Przełomowym wydarzeniem było dołączenie Rogera do Grupy ASSA ABLOY w grudniu 2024 roku, co otwiera nowe możliwości rozwoju i wzmacnia pozycję firmy na rynku krajowym i międzynarodowym.

Krzysztof Bartuszek zapowiedział, że **Securitas Polska** zamierza w 2025 roku w pełni wykorzystać potencjał nowych narzędzi i technologii wdrożonych w mijającym roku. Firma planuje kontynuować inwestycje w rozwój zespołu, a także poszerzyć zakres szkoleń dla kadry zarządzającej. Podkreślił też, że przedsiębiorstwo otwiera się na możliwość przejęć, co mogłoby wzmocnić pozycję rynkową oraz umożliwić szybszy rozwój. W jego ocenie, kluczowe będzie utrzymanie wysokich standardów jakości i bezpieczeństwa, co przełoży się na dalszy wzrost konkurencyjności firmy.

Axis Communications Poland, reprezentowane przez **Konrada Badowskiego,** postawiło na wzmacnianie relacji z partnerami biznesowymi oraz organizację dedykowanych szkoleń i spotkań. Firma planuje regularne wydarzenia, takie jak cykle Meet Axis czy organizowany przez „a&s Polska" Security Bootcamp, które mają na celu wymianę wiedzy oraz prezentację najnowszych rozwiązań technologicznych. Podkreślił, że rozwój kompetencji partnerów będzie miał bezpośredni wpływ na sukcesy sprzedażowe oraz ekspansję na rynki międzynarodowe.

Robert Gawroński z TP-Link wskazał, że nadchodzący rok będzie kontynuacją intensywnych działań rozwojowych w obszarze rozwiązań chmurowych. Firma zamierza rozbudowywać platformę Omada SDN, wprowadzając kolejne funkcje związane z zarządzaniem siecią oraz bezpieczeństwem. Zauważył, że zwiększenie liczby warsztatów technicznych i szkoleń dla klientów pozwoli na pełniejsze wykorzystanie możliwości oferowanych rozwiązań, co w efekcie przełoży się na poprawę efektywności operacyjnej i konkurencyjności oferty.

Jarosław Grzybowski z Hikvision podkreślił, że w 2025 roku intensyfikacja działań w zakresie sztucznej inteligencji i integracji systemów stanie się priorytetem. To jasne, że nie tylko jego firma planuje dalszy rozwój systemów analityki wideo oraz wdrożenie nowych narzędzi umożliwiających automatyzację procesów monitoringu. A kluczowym trendem będzie integracja systemów zabezpieczeń z urządzeniami IoT, co pozwoli na szybsze wykrywanie zagrożeń i bardziej efektywne zarządzanie infrastrukturą. W jego ocenie rozwój otwartych platform zarządzania bezpieczeństwem umożliwi scentralizowaną kontrolę nad wszystkimi elementami systemu, co znacząco podniesie poziom ochrony.

Nawet najlepiej skonstruowana oferta nie pomoże, jeśli zawiedzie odbiorca usługi lub dostawca rozwiązań. Takiego zdania jest **Harald Dingemans, CEO Linc Polska**, który wprost mówi: *Oceniając poprzedni rok i patrząc w przyszłość, uważam, że dobrze jest mieć sprawdzonych klientów oraz partnerów. Nasi grają w pierwszej lidze w swoim obszarze biznesowym. Jesteśmy z tego dumni i dziękujemy im za możliwość współpracy*. Myśląc o przyszłości, dobrze jest mieć w pamięci te słowa.

Z kolei **Łukasz Kanarek** zapowiedział, że firma **Roger** w 2025 roku wzbogaci swoją ofertę o nowe rozwiązania z zakresu

WOJCIECH WEISSENBERG
squareTec

Rok 2024 nie należał do najłatwiejszych z powodu zawirowań w sektorze publicznym, ale pomimo trudności firma zrealizowała swoje cele. Udało się zwiększyć udział w projektach zagranicznych, a współpraca z Gentec i AXIS w zakresie rozwoju oprogramowania nabrała tempa. Z dumą rozwijany jest system Broker, który integruje systemy zarządzania wideo (VMS) od różnych dostawców w jeden spójny system. Na 2025 rok firma skupi się na dalszej ekspansji zagranicznej, dążąc do jeszcze większego wzrostu przychodów z projektów międzynarodowych, a także na wdrożeniu rozwiązań chmurowych w zakresie swojej oferty. Planowana jest także retrospektywna analiza metadanych z systemów bezpieczeństwa oraz zaawansowane analizy oparte na sztucznej inteligencji. Efektywność systemów bezpieczeństwa zależy od zabezpieczeń, szczególnie w kontekście IoT. SquareTec kładzie nacisk na uwierzytelnianie urządzeń, kontrolę wersji oprogramowania, szyfrowanie komunikacji i budowę architektur odpornych na ataki. Wdrożenie systemu zarządzania bezpieczeństwem informacji, zgodnego z ISO 27001 miało na celu ujednolicenie procesów zapewniających bezpieczeństwo w firmie, wzorując się na procedurach ochrony informacji niejawnych. Certyfikacja ISO 27001 zwiększa zaufanie klientów, potwierdzając, że systemy zarządzania bezpieczeństwem informacji spełniają najwyższe standardy.

KINGA ZARZYCKA
ZKTeco Europe

Mamy za sobą sporo zmian i osiągnięć, między innymi prowadzenie nowej marki premium Armatura oraz otwarcie biura w Polsce. To ważne kroki w rozwoju firmy. Nowoczesny showroom umożliwi klientom praktyczne zapoznanie się z rozwiązaniami ZKTeco i Armatura. Mimo trudności wynikających z sytuacji polityczno-gospodarczej w Europie firma zdołała utrzymać, a w niektórych krajach nawet zwiększyć swój udział w rynku. Wzrost zainteresowania biometrią i systemami opartymi na AI otworzył nowe możliwości, które ZKTeco jako lider w tej technologii planuje w pełni wykorzystać. W 2025 roku kluczową rolę odegra marka Armatura, dedykowana projektom o najwyższym poziomie bezpieczeństwa (Grade IV). W planach jest również uruchomienie nowej strony internetowej i portalu dla klientów, który ułatwi dostęp do informacji o produktach i zwiększy interakcję z marką. Jednym z najważniejszych kierunków rozwoju będzie konsolidacja technologii *palm-vein*, która spełnia europejskie standardy AI i zapewnia bezpieczną, bezkontaktową weryfikację. Terminale FT10CMQ z linii Armatura, wyróżniające się elegancją i wszechstronnością, znajdą zastosowanie m.in. w bankach, centrach danych i szpitalach.

Według raportu „Branża ochrony w Polsce. Kondycja, prognozy, wyzwania. 2024" opracowanego przez Polski Związek Pracodawców Ochrona aż 80% respondentów oceniło stan krajowej gospodarki pozytywnie, co stanowi znaczący wzrost w porównaniu z 2022 rokiem. Wówczas jedynie 18% było tego zdania. Natomiast aż 90% firm z branży ochrony oceniło swoją kondycję jako dobrą, co oznacza wzrost o 27 punktów procentowych w porównaniu z poprzednimi latami. Ponad połowa firm odnotowała wzrost obrotów większy niż 10%.

W konsekwencji wartość rynku ochrony osób i mienia szacowana jest przez twórców raportu na 12 do 14 miliardów złotych. Inna rzecz, że obrót nie równa się zysk. Ankietowane firmy ochrony, podobnie jak wszystkie inne polskie organizacje, muszą się liczyć z rosnącymi kosztami operacyjnymi, wynikającymi choćby ze wzrostu płacy minimalnej, a negocjacje dotyczące waloryzacji stawek wynagrodzeń nie należą do najłatwiejszych. Wprawdzie 62% ankietowanych przez PZPO firm z pozytywnym dla siebie skutkiem przeprowadziło waloryzację u ponad 80% swoich klientów to, jak piszą twórcy raportu „reakcje zleceniodawców w większości nie były pozytywne. Aż 58% klientów wykazało niezadowolenie z wprowadzanych podwyżek, co może prowadzić do napięć w relacjach biznesowych". Nie ma co kryć – wzrost cen dotyka wszystkich.

Jednakże, jak wynika z raportu Polskiego Związku Pracodawców Ochrona, aż 77% firm inwestuje w nowoczesne technologie, aby sprostać rosnącym wymaganiom rynku oraz zapewnić najwyższy poziom bezpieczeństwa swoim klientom.

kontroli dostępu. Wyjaśnił, że w najbliższych miesiącach planowane jest wprowadzenie nowego kontrolera dostępu oraz linii czytników, które będą obsługiwać najnowsze standardy technologiczne. Według przedstawiciela firmy inwestycje te mają na celu nie tylko podniesienie poziomu bezpieczeństwa, ale również umożliwienie lepszej integracji systemów zabezpieczeń w obiektach o wysokich wymaganiach operacyjnych.

ZKTeco Europe postrzega rok 2025 jako punkt zwrotny w rozwoju technologii zabezpieczeń. Firma zamierza wdrażać innowacyjne rozwiązania, wśród których kluczową rolę odegra technologia biometryczna oparta na rozpoznawaniu układu naczyń krwionośnych dłoni. Według **Kingi Zarzyckiej** właśnie ta metoda, dzięki swojej bezkontaktowości oraz zgodności z europejskimi regulacjami ma zyskać na popularności w sektorze zarówno publicznym, jak i prywatnym. A rozwój marki Armatura, oferowanej przez firmę, ma na celu zaspokojenie potrzeb najbardziej wymagających klientów, którzy oczekują najwyższych standardów zabezpieczeń.

Technologiczne kierunki rozwoju i wyzwania integracji systemów

Zanosi się na to, że 2025 rok będzie rokiem SI. Wszyscy eksperci pytani o to, jakie narzędzie zdominuje najbliższych kilkanaście miesięcy, jednomyślnie podkreślali, że dalszy rozwój technologii odbywać się będzie głównie za sprawą rozwoju algorytmów sztucznej inteligencji. Dotyczyć będzie to także analizy w systemach dozoru wizyjnego oraz integracji systemów zabezpieczeń. Firmy inwestują w rozwój kamer termowizyjnych, systemów do analizy obrazu w każdych warunkach oraz rozwiązań chmurowych umożliwiających scentralizowane zarządzanie. **Konrad Badowski** zwrócił uwagę, że rozwój nowych technologii kodowania obrazu przyczyni się do poprawy jakości monitoringu, co w dłuższej perspektywie pozwoli na bardziej precyzyjne wykrywanie zagrożeń.

Natomiast **przedstawiciel Hikvision** podkreślił, że integracja różnych systemów – od kontroli dostępu, przez monitoring, po sygnalizację alarmową – jest jednym z najważniejszych wyzwań, przed którymi stoi branża. Zauważył, iż rozwój otwartych platform, takich jak Hik-Central, umożliwia pełną automatyzację procesów oraz szybką reakcję na zagrożenia. W jego ocenie integracja pozwoli na redukcję kosztów operacyjnych i zmniejszenie liczby błędów wynikających z ręcznego przetwarzania danych.

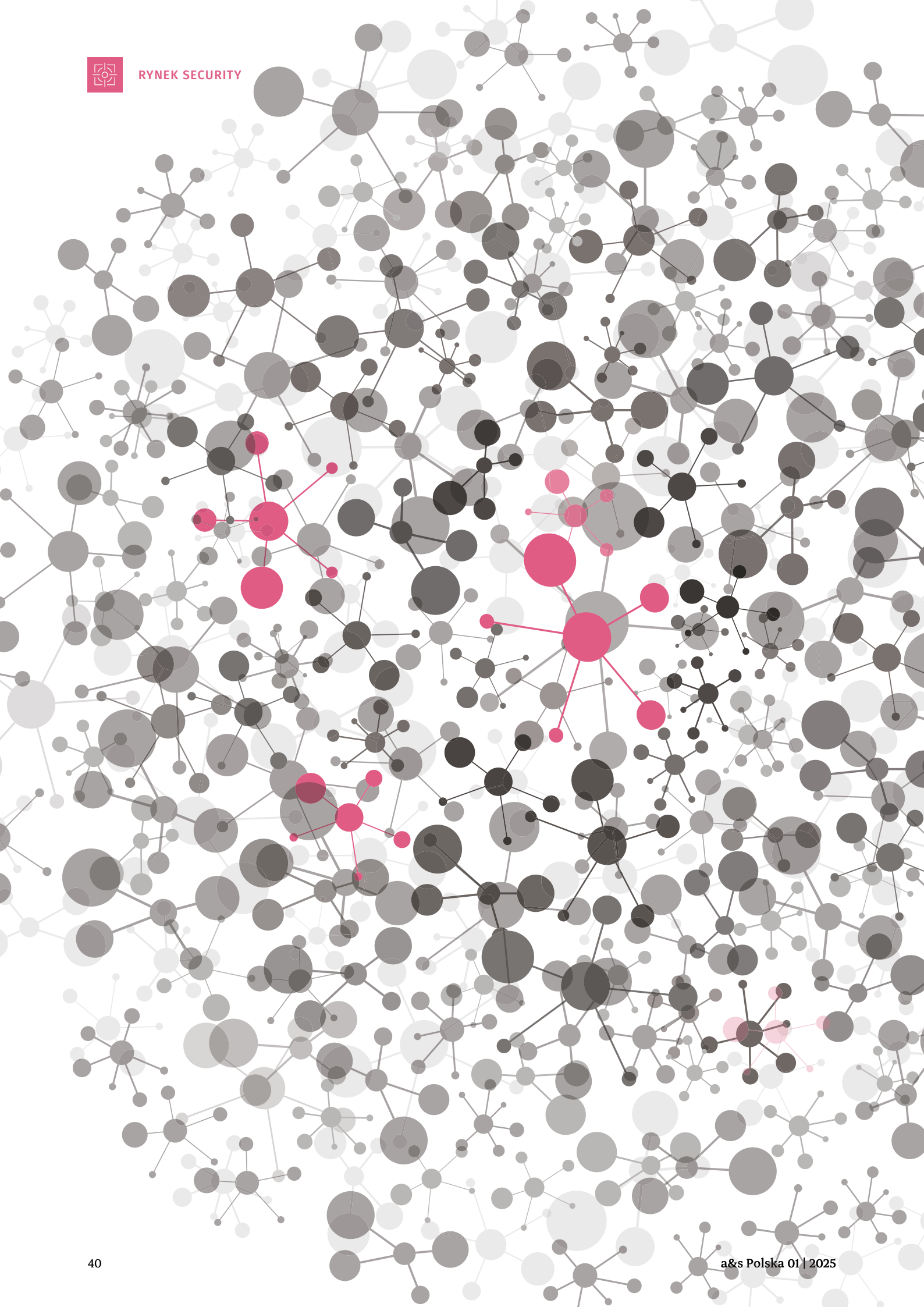
Linc Polska stawia na bezzałogowe statki powietrzne: *Chcemy wykorzystywać w systemach zabezpieczeń bezzałogowe statki powietrzne. Są elementem większej układanki tworzącej naszą koncepcję ochrony obiektów. Mamy oczywiście świadomość, że drony mogą być zagrożeniem, więc częścią naszej oferty będzie możliwość zwalczania dronów nielegalnie przekraczających granicę chronionych obiektów* – podkreślił **Harald Dingemans.**

Faktycznie, firmy chroniące mienie i ludzi muszą działać na dwa fronty. Z jednej strony chroniąc powierzone im dobra, z drugiej równie aktywnie zwalczając wszelkie możliwe zagrożenia.

Ten rok zapowiada się zatem jako czas, kiedy kluczowym elementem będzie dalsza integracja nowoczesnych technologii z tradycyjnymi systemami zabezpieczeń. Firmy stawiają na innowacyjność, automatyzację oraz rozwój kompetencji zarówno własnych zespołów, jak i partnerów biznesowych. Wspólnym celem jest stworzenie spójnych, zintegrowanych systemów ochrony, które umożliwią efektywne zarządzanie bezpieczeństwem w obliczu rosnących wyzwań współczesnego świata.

Przedsiębiorstwa z sektora zabezpieczeń obecne na polskim rynku przez wiele lat zdążyły wypracować strategie, które pozwolą im sprostać nadchodzącym wyzwaniom. Prognozy na rok 2025 wskazują, że kluczowymi trendami będą rozwój sztucznej inteligencji, integracja systemów oraz wdrażanie innowacyjnych rozwiązań biometrycznych. Ciągły rozwój to podstawa. Z tej prostej przyczyny, że kto się nie rozwija, ten się cofa. Branża to wie i nieustająco prze do przodu.

Monika Żuber-Mamakis,
redaktorka „a&s Polska"

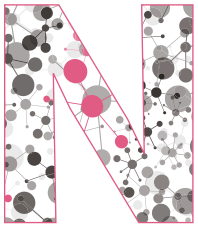


BRANŻOWE FUZJE I PRZEJĘCIA

Co oznaczają dla rynku security

Rok 2024 na rynku elektronicznych systemów zabezpieczeń był okresem fuzji i przejęć. Kto przejął kogo i z jakiego powodu? Jakie firmy się zwijają, a jakie rozwijają? Jaki skutek dla rynku security przyniosą te działania? Przyjrzyjmy się tym zmianom dokładniej.

Jan T. Grusznic



Najpierw Silent Sentinel zostało przejęte przez Motorolę. Potem rynek dowiedział się o połączeniu sił Milestone'a i BriefCam. Ta ostatnia informacja zrobiła spore wrażenie, ponieważ BriefCam, będący liderem w dziedzinie analizy materiału wizyjnego, był traktowany jako producent niezależny od platform systemów telewizji dozorowej. Jeszcze nie opadły emocje, a Milestone potwierdził, że po pewnej przerwie ponownie połączy się z Arcules. Naprawdę ciekawie zrobiło się w grudniu, kiedy się okazało, że biznes elektronicznych systemów zabezpieczeń Boscha zostanie przejęty przez firmę Triton, zaś ASSA ABBLOY potwierdziło informację o przejęciu firmy Roger.

Niektóre z tych organizacyjnych roszad nie były zaskoczeniem. Przecież już podsumowując w „a&s Polska" rok 2023 i zastanawiając się nad tym, co przyniesie kolejnych 12 miesięcy, informowaliśmy o możliwych konsolidacjach na rynku elektronicznych systemów zabezpieczeń. Wówczas pretekstem do tych dywagacji była wiadomość, że Bosch zamierza pozbyć się części swojego biznesu związanego z elektronicznymi systemami zabezpieczeń, co mogło trochę dziwić, skoro wcześniej firma sięgnęła po Paladin Technologies, wiodącego dostawcę rozwiązań w zakresie bezpieczeństwa i ochrony życia, a także usług integracji systemów. A jednak w październiku 2023 r. plan wszedł w życie. Bosch zdecydował się pozbyć większej części działu Building Technologies,

Ilustracje: freepik

w tym systemów dozoru wizyjnego, kontroli dostępu, sygnalizacji włamania i napadu oraz części audio (BSCT – Bosch Security and Communications Technology Product Business). Działalność dotycząca alarmów przeciwpożarowych miała pozostać w firmie i stać się istotną częścią przyszłościowej działalności Bosch Building Technologies w zakresie integracji systemów, oferując rozwiązania i usługi dotyczące bezpieczeństwa budynków, efektywności energetycznej i automatyki budynkowej.

Branżowych ekspertów zżerała ciekawość: kto kupi? Tym bardziej że warunkiem stawianym nabywcy było przejęcie tych wcześniej wymienionych trzech jednostek biznesowych, zatrudniających 4300 osób w ponad 90 lokalizacjach na całym świecie. Spekulacjom nie było końca, co w pewnym momencie stało się dla firmy Bosch niewygodne. Każda taka niepewność może się bowiem przełożyć na wyniki finansowe. Choć jak się ostatecznie okazało, sprzedaż w 2024 r. okazała się rekordowa, co zdradził nam Michał Małek, przedstawiciel Bosch Building Technologies w Polsce.

Po co funduszowi Triton firma z branży security?

Triton Partners to londyńska firma *private equity* koncentrująca się na inwestowaniu i wspieraniu średnich przedsiębiorstw, głównie europejskich. W obszarze jej zainteresowania są firmy dostarczające towarów o znaczeniu krytycznym dla organizacji świadczących usługi biznesowe innym podmiotom, oferującym sprzęty i usługi niezbędne dla przemysłu i instytucji związanych z opieką zdrowotną. Opisywana transakcja nie jest pierwszą tego typu. Triton Partners w 2013 r. kupił Bosch Rexroth Pneumatics. W roku 2014 firma zmieniła nazwę na Aventics i pod taką nazwą została sprzedana przez fundusz w roku 2018. Czy tak samo będzie z BSCT? Podobno w planach jest uczynienie z przejętych oddziałów pełnowymiarowej samodzielnej firmy z zachowaniem głównej siedziby firmy w niemieckim Grasbrunn i utrzymaniem zatrudnienia.

Sfinalizowanie umowy z Boschem pokazuje, że Triton Partners konsekwentnie powiększa swoje portfolio podmiotów zajmujących się bezpieczeństwem. W ubiegłym roku fundusz zainwestował w Wavelynx Technologies, dostawcę bezpiecznych i otwartych rozwiązań w zakresie tożsamości i kontroli dostępu na urządzeniach mobilnych, a w 2021 r. w Acre i jego podmioty zależne: Matrix Systems Inc., Communication Networks Inc., Feenics Inc., Open Options Corporation, Security Identification Systems Corporation, RS2 Technologies, LLC, Razberi Technologies Inc., REKS, TDS (Time Data Security) Limited. Ciekawostką jest, że Acre było właścicielem Mercury Security, producenta sprzętu OEM używanego przez firmy kontroli dostępu, od 2013 r. do momentu sprzedaży HID Global (marka Assa Abbloy) w 2017 r. Przypadek? Hm...

Otóż Oliver Philippou, starszy kierownik ds. badań i analiz w niezależnej agencji badawczej Omdia specjalizującej się w rynku zaawansowanych technologii, uważa, że Bosch i Acre po prostu do siebie pasują ze względu na profil prowadzonej działalności. Czyżby nowy ALARM.COM? Czas pokaże. Na pewno marka i logo Bosch szybko nie znikną z produktów BSCT. Rebranding ma zacząć się nie wcześniej niż w 2026 r. Natomiast Bosch Building Technologies czeka reorganizacja i nowa rola: regionalnego

integratora oferującego rozwiązania i usługi w zakresie bezpieczeństwa budynków, efektywności energetycznej i automatyki budynkowej. Skąd ta zmiana? Po prostu...

lepiej integrować niż produkować

Rynek integratorów systemów jest bardziej dochodowy i zapewnia wyższe marże niż rynek producentów urządzeń. Pokazują to wyniki finansowe takich dużych integratorów jak Siemens, Covergint, Stanley (obecnie Securitas Technology), ale też mniejszych, takich jak T4B i Sprint. Oferta tych firm jest skierowana do inwestorów zajmujących się wysokobudżetowymi projektami, z założenia potrzebującymi kompleksowego podejścia, zaawansowanej wiedzy technicznej i umiejętności zarządzania projektami. Celem jest uzyskanie kompleksowego systemu ochrony, więc oczywiste jest, że inwestor oczekiwać będzie integracji sprzętu, oprogramowania, sieci telekomunikacyjnych i innych technologii. Przy takim podejściu marża musi być wyższa niż narzut, na jaki może liczyć producent. Producentom życia nie ułatwia też konkurencja z Dalekiego Wschodu. Jest tak skuteczna, że nawet zwiększenie obrotu nie zawsze przekłada się na wzrost zysków. Dużym firmom, rozrastającym się choćby w wyniku różnego rodzaju fuzji i przejęć, łatwiej walczyć z dalekowschodnią konkurencją, ale łatwiej też o przygotowanie kompleksowej oferty dla klienta.

Producentom życia nie ułatwia konkurencja z Dalekiego Wschodu. Jest tak skuteczna, że nawet zwiększenie obrotu nie zawsze przekłada się na wzrost zysków. Dużym firmom, rozrastającym się choćby w wyniku różnego rodzaju fuzji i przejęć, łatwiej walczyć z dalekowschodnią konkurencją, ale łatwiej też o przygotowanie kompleksowej oferty dla klienta.

W kupie siła

Silne przenikanie się rynku elektronicznych systemów zabezpieczeń z ochroną danych wymusza na producentach większe zaangażowanie w procesy związane z bezpieczeństwem informacji i przetwarzaniem danych oraz wykorzystywaniem mechanizmów uznanych w cyfrowym świecie za standard. Utrzymanie tego standardu jest po pierwsze czasochłonne, po drugie kosztowne i wcale nie musi się przekładać na wprowadzanie nowych funkcji, czego nabywcy oczekują. A rozpaskudzeni przez AI oczekiwania mają niemałe. Analiza obrazu dokonywana przez AI już spowszedniała, oczekiwania zatem rosną, dlatego związanie się z większym graczem, dysponującym odpowiednim kapitałem oraz zasobami jest sensownym wyjściem. Zrozumieli to zarządzający firmą Roger, która od 30 lat oferuje klientom systemy kontroli dostępu. Od wielu lat Roger zaznaczał swoją obecność na zagranicznych targach w Europie, Dubaju i Azji. Obecnie może poszczycić się licznymi partnerami i dystrybutorami poza granicami Polski. Firma od lat rozwijała swoje produkty, aktywnie słuchając głosu instalatorów, użytkowników i śledząc trendy rynkowe. Dzięki temu dzisiaj oferuje rozwiązania z zakresu kontroli dostępu niemal dla każdego segmentu rynku: od typowych rozwiązań przeznaczonych dla przemysłu, przez obiekty sportowe i rekreacyjne, po sektor mieszkaniowy, szpitale i hotele. Nie dziwi więc, że wpadła w oko takiemu graczowi jak ASSA ABLOY. Zainteresowanie jest wzajemne, bo utrzymanie pozycji lidera wymaga potężnego wsparcia. Roger więc na tym mariażu zyska wsparcie potężnego protektora. ASSA ABLOY też zyskuje, gdyż Roger dysponuje takimi technologiami, które wręcz wyznaczają trendy w SKD. I wydaje się, że na to też liczy inwestor, gdyż jak mówi Achim Haberstock, SVP & Head of ASSA ABLOY Central Europe: *Przejęcie firmy Roger wzmacnia naszą pozycję w Europie Środkowej i Wschodniej, uzupełniając nasze portfolio o sprawdzone kompetencje w zakresie elektronicznych systemów kontroli dostępu oraz innowacyjne rozwiązania, takie jak bezprzewodowe zamki Aperio, elektromechaniczne systemy zamków inteligentnych CLIQ (bazujące na technologii smart key), bezbateryjne zamki PULSE oraz wiele innych. Ta współpraca jest dowodem naszego zaangażowania w innowacje i dostarczanie rozwiązań dostosowanych do zróżnicowanych potrzeb klientów w regionie. Jesteśmy wdzięczni za zaufanie założycieli Grzegorza i Dariusza Wenskerów, którzy powierzyli ASSA ABLOY przyszłość firmy, by pomóc wynieść ją na kolejny poziom.*

Czy konsolidacja oznacza monopolizację?

W ostatnich latach branża zabezpieczeń elektronicznych odnotowała liczne przejęcia, które zmieniają i konsolidują rynek. Główni gracze przejmują kolejne firmy, aby zwiększyć udział w rynku, zdywersyfikować ofertę, rozwinąć technologie i szybko zwiększyć zyski. Ale fuzje i przejęcia są spowodowane także rosnącym popytem na nowe technologie w rozwiązaniach bezpieczeństwa dla sektorów prywatnego i publicznego, któremu mogą sprostać tylko duże podmioty. Nic nie wskazuje na to, by trend związany z konsolidacją miał w najbliższym czasie osłabnąć.

Rynek systemów kontroli dostępu fizycznego przez wiele był uznawany za stabilny, mało dynamiczny, jeśli chodzi o obecne na nim firmy. Jednak okres pandemii zmienił sposób korzystania z przestrzeni chronionych, wymusił zwiększoną dostępność do systemów, to zaś spopularyzowało rozwiązania takie jak choćby SaaS. Obecnie systemy kontroli dostępu fizycznego przeżywają największą przemianę technologiczną od czasu opracowania protokołu Wieganda! Czy zmiany właścicielskie okażą się równie rewolucyjne?

Jan T. Grusznic
redaktor „a&s Polska"

Mapa inwestycji

Prezentujemy wybór inwestycji prowadzonych przez takie firmy, jak Atrem, Dekpol, Elektrotim, Energoaparatura, Mostostal Warszawa, Mostostal Zabrze, Polimex Mostostal, Poznańska Korporacja Budowlana Pekabex, Prochem i Unibep. Projekty te obejmują m.in. budowę i modernizację infrastruktury energetycznej (np. stacje 110/15 kV, magazyny energii, podstacje trakcyjne), przemysłowej (np. centra dystrybucyjne, zakłady produkcyjne), medycznej (np. budynek zakładu medycyny nuklearnej) oraz transportowej (np. oświetlenie nawigacyjne lotniska, płyta postojowa samolotów). Inwestycje te są planowane na najbliższe miesiące i lata. Zakończenie najkrótszej z nich przewidywane jest na koniec sierpnia bieżącego roku, a najdłuższej na 2028 rok.

Atrem

1	**Co:**	Budowa stacji 110/15 kV Gdańska przy EC Szczecin
	Gdzie:	Szczecin
	Kiedy:	nie więcej niż 24 miesiące od dnia zawarcia umowy (28.11.2024)

Dekpol

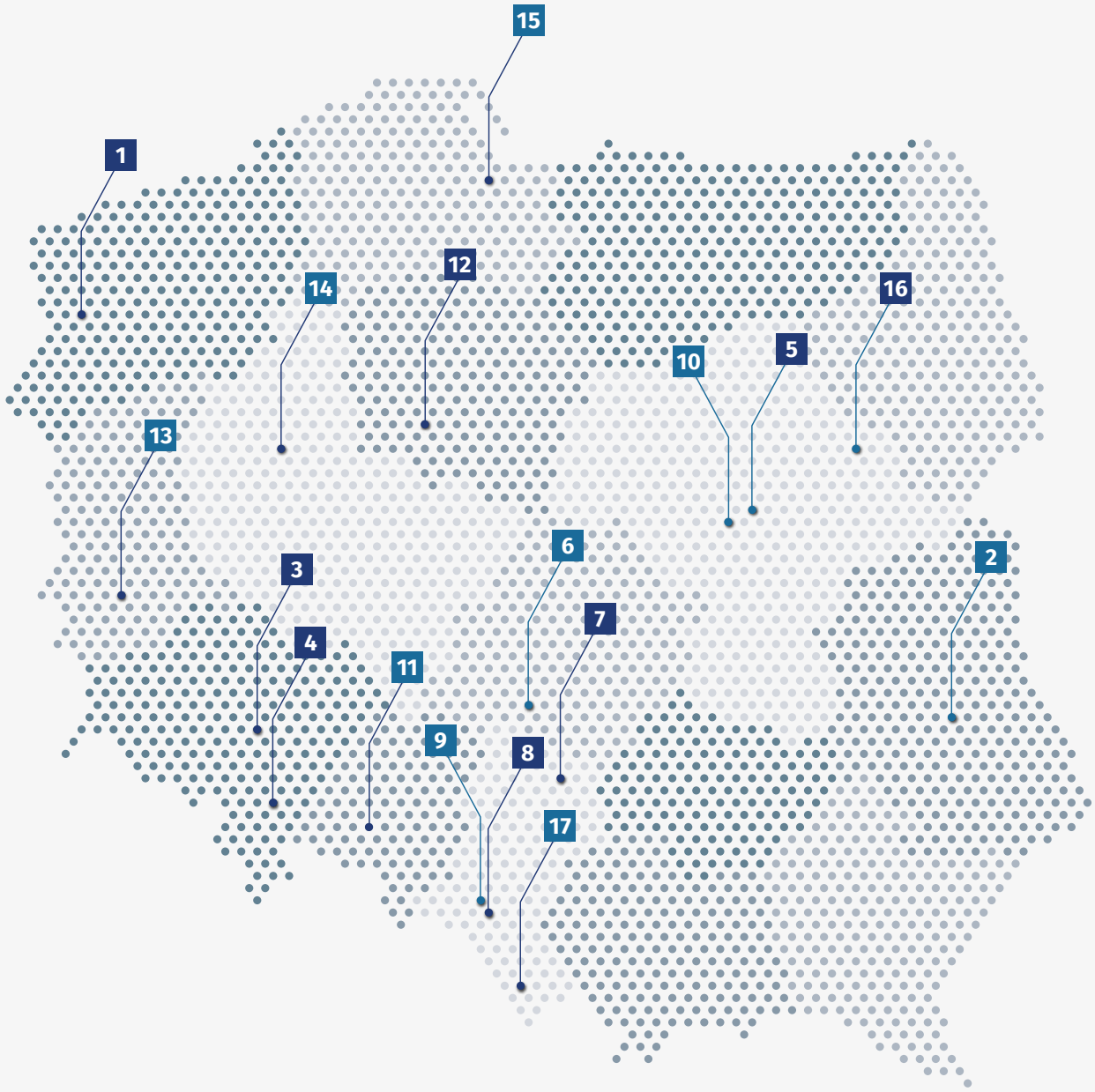
2	**Co:**	Multifunkcyjne Centrum Rozwoju
	Gdzie:	Świdnik
	Kiedy:	III kwartał 2026

Elektrotim

3	**Co:**	Oświetlenie nawigacyjne dla Portu Lotniczego we Wrocławiu
	Gdzie:	Wrocław
	Kiedy:	Październik 2026
4	**Co:**	Budowa wielkoskalowego magazynu energii
	Gdzie:	Stary Grodków
	Kiedy:	Grudzień 2025
5	**Co:**	Budowa budynku podstacji trakcyjnej „Jasna" wraz z modernizacją urządzeń elektroenergetycznych
	Gdzie:	Warszawa
	Kiedy:	42 tygodnie licząc od dnia zawarcia umowy (06.12.2024)
6	**Co:**	Kompleksowe prace projektowo-montażowe na GPZII
	Gdzie:	Trębaczew
	Kiedy:	31.12.2025

Mostostal Warszawa

7	**Co:**	Modernizacja systemu transportu paliwa w Elektrociepłowni Częstochowa
	Gdzie:	Częstochowa
	Kiedy:	29.01.2027
8	**Co:**	Budowa siedziby prokuratur różnego szczebla
	Gdzie:	Katowice
	Kiedy:	30.06.2028



Mostostal Zabrze

9	**Co:**	Budowa Budynku Zakładu Medycyny Nuklearnej i Endokrynologii Onkologicznej – Oddziału Terapii Izotopowej dla Narodowego Instytutu Onkologii im. Marii Skłodowskiej-Curie – Państwowego Instytutu Badawczego Oddziału w Gliwicach
	Gdzie:	Gliwice
	Kiedy:	I kwartał 2026
10	**Co:**	Wykonanie płyty postojowej samolotów wraz z pracami towarzyszącymi
	Gdzie:	Lotnisko Chopina w Warszawie
	Kiedy:	20 miesięcy od dnia podpisania umowy (15.11.2024)
11	**Co:**	Wykonanie prac mechanicznych, montaż urządzeń i rurociągów technologicznych
	Gdzie:	Radzikowice k. Nysy
	Kiedy:	31.03.2026

Polimex Mostostal

12	**Co:**	Budowa Elektrowni Fotowoltaicznej Marulewy o łącznej mocy 47,39 MWp
	Gdzie:	Marulewy
	Kiedy:	30.09.2027

Poznańska Korporacja Budowlana Pekabex

13	**Co:**	Budowa zakładu produkcyjnego z funkcją biurową, usługami wraz z parkingiem
	Gdzie:	Nowa Sól
	Kiedy:	18.05.2026
14	**Co:**	Nadbudowa 5 kondygnacji biurowych na magazynie HoReCa
	Gdzie:	Poznań
	Kiedy:	11 miesięcy od dnia zawarcia umowy (10.01.2025)
15	**Co:**	Budowa zakładu przetwórstwa i magazynowania ryb
	Gdzie:	Gdańsk
	Kiedy:	31.08.2025

Prochem

16	**Co:**	Generalna realizacja inwestycji na terenie Zakładu Przetwórstwa Nasion Oleistych
	Gdzie:	Kosów Lacki
	Kiedy:	Luty 2027

Unibep

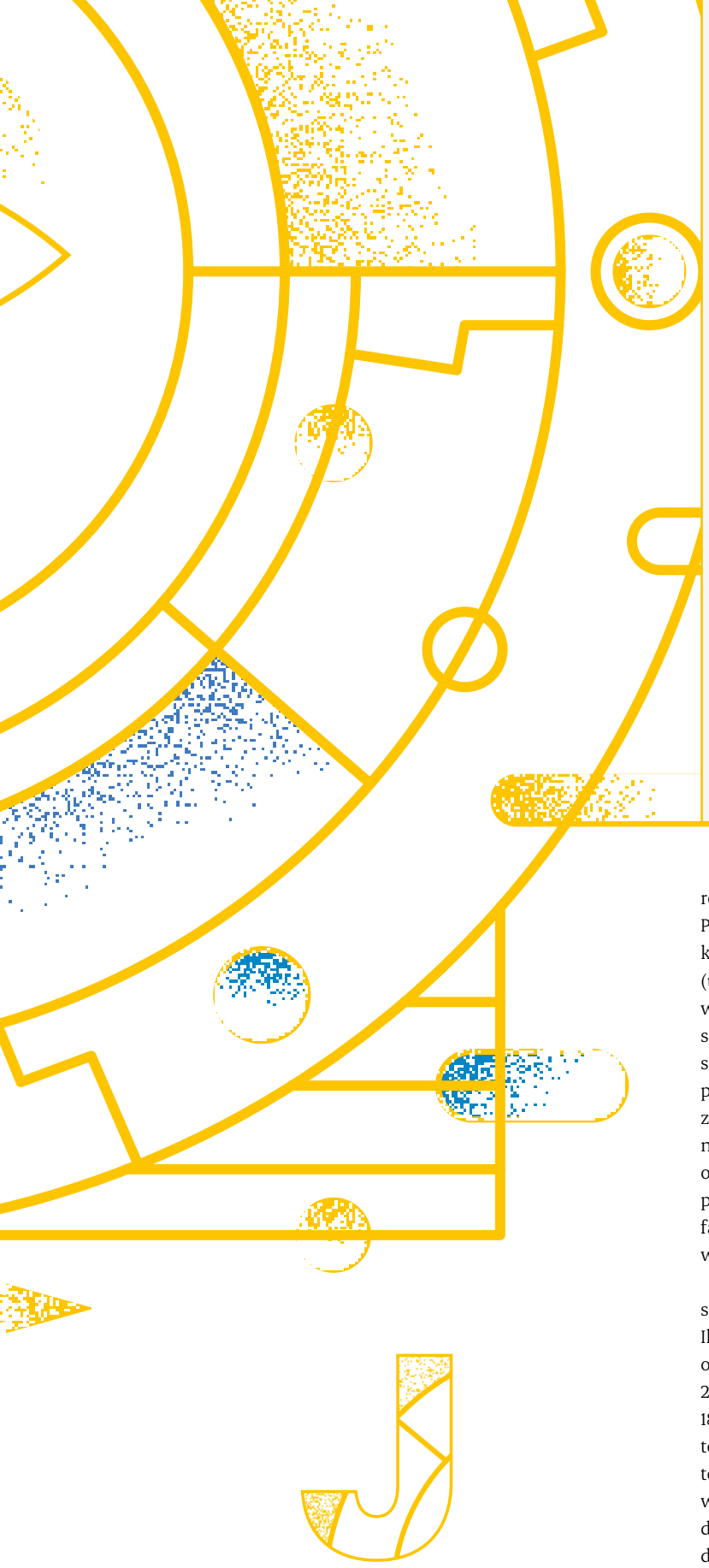
17	**Co:**	Przebudowa kotłowni Rejonowej „Pod Grapą”
	Gdzie:	Żywiec
	Kiedy:	I kwartał 2026

Ilustracje: freepik / Mapa: Jan Kurzawa

Stare, **ale jare?** Niekoniecznie

Urządzenia security działające w ramach Internetu rzeczy bezwzględnie potrzebują regularnej aktualizacji oprogramowania. Jeśli producent jej nie oferuje lub odstępuje od wsparcia dla jakiegoś modelu bądź całej serii produktów, to warto rozważyć ich wymianę. Dlaczego? Z bardzo prostej przyczyny: takie urządzenia są wymarzonym celem ataków hakerskich.

Monika Żuber-Mamakis



Botnet Mirai, którego nazwa pochodzi od japońskiego słowa „przyszłość", stanowi jeden z najbardziej znaczących przypadków złośliwego oprogramowania w historii cyberbezpieczeństwa. Stworzony w 2016 roku, specjalizował się w infiltracji urządzeń Internetu rzeczy (IoT), wykorzystując domyślne hasła do przejmowania kontroli nad kamerami internetowymi, rejestratorami wideo i ruterami.

W szczytowym momencie Mirai zainfekował około 2,5 mln urządzeń na całym świecie. Jego największym atakiem było uderzenie w serwery firmy Dyn, co doprowadziło do zakłócenia działania wielu popularnych serwisów internetowych. Botnet atakował głównie słabo zabezpieczone urządzenia IoT, od kamer po inteligentne lodówki, generując ruch sieciowy przekraczający 1 Tb/s. Przypadek Mirai pokazał, jak krytyczne znaczenie ma właściwe zabezpieczanie urządzeń IoT i regularne aktualizaowanie ich oprogramowania.

Jeszcze nie tak dawno temu dziesięcioletnia lodówka była urządzeniem w sile wieku, a pięcioletnia pralka w zasadzie była uznawana za nową. Wspomniane urządzenia to oczywiście nie nasza branża, ale dobrze pokazują, jak bardzo zmieniły się czasy, jeśli chodzi o kwestię życia produktu. Współczesne lodówki, pralki, telewizory, ale i kamery dozorowe są naszpikowane zaawansowaną elektroniką. Na czas ich życia wpływa po pierwsze, gwałtowny rozwój techniki, w tym coraz chętniej stosowane algorytmy AI. Po drugie, wielce naganna praktyka producentów (przede wszystkim urządzeń AGD i biurowych) celowego postarzania urządzeń (unijna dyrektywa ograniczająca ten proceder weszła w życie w roku 2021, jest więc na rynku sporo produktów, które jeszcze się jej wymykają). Po trzecie, nie mniej ważne jest to, że niepostrzeżenie zaczęliśmy żyć w świecie Internetu rzeczy. I to właśnie połączenie urządzeń w ramach IoT ma chyba największe dla nas znaczenie, jeśli chodzi o kwestię bezpieczeństwa. Czas fizycznego życia (i zużycia) produktu to jedno. Drugim jest czas jego odporności na zagrożenia cyfrowe. Warto sobie bowiem zadać pytanie, jakie skutki dla bezpieczeństwa fizycznego powoduje fakt, że urządzenia służące do ochrony obiektów funkcjonują w internetowej sieci.

Internet rzeczy (*Internet of Things*, IoT) to sieć połączonych ze sobą urządzeń, które mogą komunikować się i wymieniać dane. Ile sprzętów już teraz tworzy IoT? To zależy, kto liczy, ale mowa o miliardach. Według raportu serwisu IoT Business News w roku 2024 liczba połączonych urządzeń IoT wzrosła o 13%, osiągając 18,8 mld na całym świecie. Największy wzrost odnotowano w sektorze transportu, gdzie liczba urządzeń IoT wzrosła o 25%. Sektor zdrowia również wykazuje dynamiczny rozwój, z rosnącym wykorzystaniem urządzeń monitorujących i telemedycyny. Za dziesięć lat w ramach Internetu rzeczy ma funkcjonować prawie dwukrotnie więcej urządzeń, bo aż 30 mld, tak z kolei uważają eksperci serwisu Statista. Oczywiście, może być tych urządzeń więcej, bo nieostre są kryteria tego, co uważamy za urządzenie IoT. Zasadniczo to te, które mają zdolność do komunikacji przez Internet i mogą przesyłać dane do innych urządzeń lub systemów bez potrzeby ingerencji człowieka. Należy przy tym pamiętać, że Internet rzeczy tworzą nie tyle „poważne" urządzenia IT, ile cała ta drobnica, którą otaczamy się na co dzień, czyli odkurzacze samojezdne, telewizory, smartwatche, pralki, lodówki, ekspresy do

Ilustracje: freepik

kawy, domofony oraz, *last but not least*, urządzenia security, takie jak kamery dozorowe czy urządzenia dostępowe, zazwyczaj nierzucające się w oczy, ale niezbędne, by zapewnić bezpieczeństwo. Gdyby tylko jedna trzecia z nich stała się przestarzała w ciągu pięciu lat, oznaczałoby to, że ponad 5,6 mld urządzeń mogłoby się stać podatnych na cyberatak – nie od razu, ale w miarę wygaszania wsparcia prawdopodobieństwo wzrasta.

Nic nie jest wieczne

To właśnie urządzenia takie jak kamery dozoru wizyjnego czy bramki dostępowe są doskonałymi przykładami zastosowań IoT. Monitorują otoczenie, cały czas przesyłając dane do centralnych systemów zarządzania, co umożliwia zdalne nadzorowanie i kontrolowanie różnych procesów. W miarę ich udoskonalania rola w zapewnieniu bezpieczeństwa i efektywności staje się coraz bardziej istotna, dlatego tak ważna jest aktualizacja ich oprogramowania. Regularne aktualizowanie oprogramowania jest niezbędne, aby urządzenia mogły działać zgodnie z najnowszymi standardami i były odporne na nowe zagrożenia, bez tego urządzenia mogą utracić zdolność współpracy z innymi systemami lub będą narażone na ataki hakerów. To ostatnie jest nawet bardziej niż pewne.

Wsparcie techniczne producentów urządzeń IoT jest kluczowe, ponieważ to oni odpowiadają za dostarczanie aktualizacji. W przypadku starszych urządzeń, które nie mogą liczyć na regularne aktualizacje, należy pamiętać, że wcześniej czy później pojawią się poważne problemy związane z bezpieczeństwem.

Tymczasem producenci często kończą wsparcie po kilku latach, co może prowadzić do sytuacji, w której fizycznie sprawne urządzenie stanie się „niesprawne" cyfrowo, a co się z tym wiąże – niebezpieczne. Czemu tak czynią? Z kilku względów. Jednym z najważniejszych jest zakończenie cyklu życia produktu. Kiedy urządzenie osiąga status *end of life* (EOL), producenci przestają oferować jakiekolwiek wsparcie techniczne, w tym aktualizacje oprogramowania. Utrzymanie go w odniesieniu do starszych urządzeń może bowiem wymagać znacznych zasobów finansowych i ludzkich, a koszty z tym związane przewyższą ewentualne korzyści, szczególnie jeśli firma, dążąc do konkurencyjnej atrakcyjności, wprowadza na rynek nowe, lepsze modele i to funduje im intensywną promocję. Inna rzecz, że bywa też tak, iż konkretne modele zostały zaprojektowane w sposób, który uniemożliwia ich skuteczną ochronę, nawet mimo aktualizacji. Zostały np. zbudowane z wykorzystaniem chipsetu, w którym wykryto lukę krytyczną.

Luka krytyczna to poważna podatność w oprogramowaniu, które mogą prowadzić do zdalnego wykonania kodu (RCE) lub innych nieautoryzowanych działań. Takie luki są szczególnie niebezpieczne, ponieważ mogą być wykorzystywane przez cyberprzestępców do ataków bez konieczności interakcji ze strony użytkownika, co czyni je trudnymi do wykrycia i obrony.

Drobne rzeczy tworzą duże sieci

Nie zawsze celem przestępców jest wdarcie się do wnętrza firmy. Bardzo często takie urządzenia mogą stać się częścią botnetu. Botnet to złożona sieć zainfekowanych komputerów, które są kontrolowane przez cyberprzestępców. Termin „botnet" powstał z połączenia słów „robot" i „network", co wskazuje na automatyzację i zdalne zarządzanie tymi urządzeniami. Komputery wchodzące w skład botnetu, często nazywane „zombie", działają bez wiedzy ich właścicieli, co czyni je idealnym narzędziem dla przestępców.

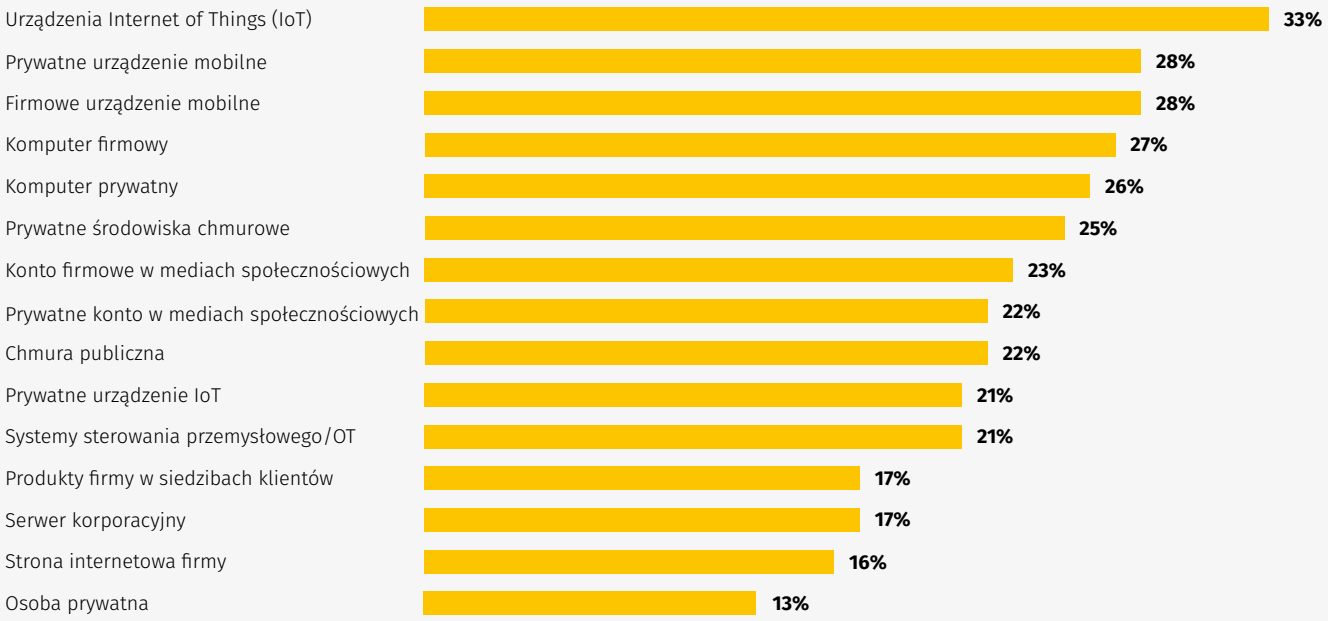
Tworzenie botnetu zazwyczaj rozpoczyna się od infekcji urządzeń. Cyberprzestępcy wykorzystują różne metody, aby zainstalować złośliwe oprogramowanie na komputerach ofiar. Może to obejmować wysyłanie złośliwych linków w wiadomościach e-mail, umieszczanie szkodliwego oprogramowania na stronach internetowych lub dołączanie wirusów do nielegalnie pobranych aplikacji. Zainfekowane urządzenia łączą się z serwerem kontrolnym (tzw. serwerem C&C – *Command and Control*), gdzie oczekują na dalsze instrukcje od cyberprzestępcy. Gdy boty są już pod kontrolą, mogą być wykorzystywane do przeprowadzania różnych działań przestępczych na rozkaz ich operatora.

Botnety są wykorzystywane w różnych celach, m.in. do:

- ataków DDoS (*Distributed Denial of Service*) – celem ataku jest wywołanie przeciążenia serwerów, co powoduje, że są niedostępne legalnym użytkownikom. Ataki te polegają na wysyłaniu dużej liczby żądań jednocześnie z wielu urządzeń;
- rozsyłania spamu – zainfekowane komputery mogą masowo wysyłać e-maile spamowe, co pozwala przestępcom omijać filtry antyspamowe;
- kradzieży danych;
- przeprowadzania ataków phishingowych;
- manipulowania algorytmami internetowymi poprzez generowanie sztucznego ruchu.

Brak wsparcia oznacza, że wiele urządzeń IoT, jeszcze przecież fizycznie bardzo żwawych i nadal doskonale się spisujących, może paść ofiarą ataku hakerskiego. Wówczas w najlepszym przypadku zasilą armię komputerów – zombii.

Najczęstsze cele zewnętrznych cyberataków na świecie w 2023 r.



Źródło: Statista

Brak wsparcia oznacza, że wiele urządzeń IoT, jeszcze przecież fizycznie bardzo żwawych i nadal doskonale się spisujących, może paść ofiarą ataku hakerskiego. Wówczas w najlepszym przypadku zasilą armię zombi. Przykładem może być atak botnetowy Mirai, który wykorzystywał niezabezpieczone urządzenia IoT z przestarzałym oprogramowaniem do stworzenia jednej z największych sieci botnetów. W najgorszym – posłużą jako brama, którą wypłyną dane firmowe.

W roku 2022 odnotowano ponad 20 mln cyberataków na urządzenia Internetu rzeczy (IoT). Z danych FortiGuard Labs wynika, że ataki te były realizowane z prawie 122 tys. unikalnych adresów IP, z czego blisko jedna trzecia pochodziła z Chin, 10% ze Stanów Zjednoczonych, a 9% z Korei Południowej. Ataki na urządzenia IoT często mają na celu uzyskanie dostępu do nich lub przejęcie nad nimi kontroli, co może prowadzić do ich wykorzystania w dalszych atakach. Wiele z tych urządzeń nie ma wbudowanych funkcji zabezpieczających, co czyni je łatwym celem dla cyberprzestępców. W roku 2022 większość aktywnych botnetów IoT bazowała na oprogramowaniu Mirai (patrz ramka: *Botnet Mirai*), które wykorzystuje domyślne dane logowania do infekcji systemów.

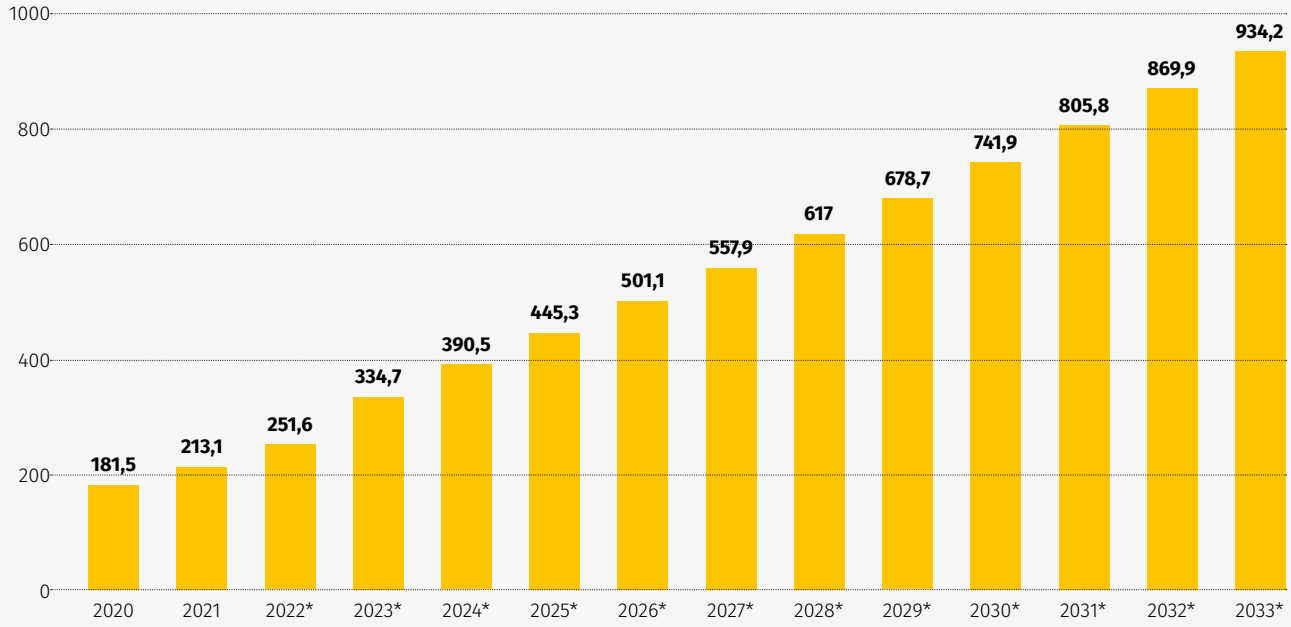
Zgromadzone dane telemetryczne dowodzą, że średnio wykrywano 80 tys. naruszeń dziennie, a w szczytowych momentach liczba ta sięgała 160 tys. Warto zauważyć, że ataki skanowania portów stanowiły 56% wszystkich zidentyfikowanych incydentów związanych z urządzeniami IoT.

Jakie sprzęty są najbardziej wrażliwe?

Według ekspertów firmy Netgear w 2023 r. najwięcej luk ułatwiających atak odkryto w telewizorach (34%), inteligentnych wtyczkach (18%), cyfrowych rejestratorach wideo (13%) i ruterach (12%). Luki w zabezpieczeniach telewizorów okazują się dość powszechne. Te urządzenia zazwyczaj są używane wiele lat i bywa, że użytkownicy z premedytacją nie pozwalają na dokonywanie automatycznych aktualizacji, a odbiorniki zwykle działają znacznie dłużej niż okres oferowanego dla nich wsparcia. Rutery są zdecydowanie lepiej zabezpieczone i strzeżone, ale to one są przez hakerów wybierane najchętniej. Według autorów raportu opublikowanego przez Fortinet Threat Landscape to właśnie rutery są najczęstszym celem ataku, co zrozumiałe. Jeśli haker wedrze się do rutera, to sieć stoi przed nim otworem. Przejęcie kontroli nad urządzeniem pozwala na monitorowanie i przechwytywanie ruchu sieciowego ze wszystkich podłączonych urządzeń. Poza tym powodzeniem cieszą się: inteligentne kamery i rejestratory wizyjne (atakowane ze względu na ich popularność w systemach monitoringu; w 2023 r. obserwowano wzrost liczby ataków, które wykorzystywały zainfekowane kamery do przeprowadzania ataków DDoS), inteligentne głośniki i asystenci głosowi, a także inteligentne lodówki, odkurzacze, termostaty i żarówki.

Natomiast według informacji przygotowanych przez Check Point organizacje europejskie doświadczały średnio prawie 70 ataków IoT na organizację tygodniowo, co podkreśla skalę zagrożenia w tym regionie. Z danych wynika, że ok. 80% wszystkich urządzeń IoT jest podatne na różnorodne ataki. Cyberprzestępcy wykorzystują ich luki do przeprowadzania ataków DDoS, kradzieży danych oraz szpiegowania użytkowników. W związku z rosnącą liczbą ataków na te technologie ważne, aby użytkownicy dbali o bezpieczeństwo swoich urządzeń IoT poprzez regularne aktualizacje oprogramowania i stosowanie silnych haseł. O ile z używaniem silnych haseł może sobie poradzić odpowiednia polityka bezpieczeństwa, o tyle gorzej jest z aktualizacjami, gdy skończy się czas wsparcia oferowany przez producenta. Co to oznacza dla

Całkowity roczny przychód z Internetu rzeczy (IoT) na świecie w latach 2020–2033



Źródło: Statista

organizacji? Konieczność zachowania czujności i przygotowania się na fakt, że w pewnym momencie konkretna liczba urządzeń bezpieczeństwa będzie musiała zostać wymieniona, nawet jeśli fizycznie nic im dolegać nie będzie. To z kolei oznacza konkretny koszt. Moment ten można przesunąć w czasie, wybierając takich dostawców, którzy deklarują długi czas wsparcia dla swoich urządzeń, i przewidując w budżecie konieczność wymiany.

Warto również wspomnieć o rozwijających się regulacjach prawnych w zakresie IoT. Oprócz wspomnianej dyrektywy UE z 2021 r. dotyczącej postarzania produktów kluczowe znaczenie ma *Cyber Resilience Act (CRA)* z 2024 ro., który nakłada na producentów urządzeń IoT konkretne wymagania dotyczące cyberbezpieczeństwa. Obejmują one m.in. minimalny okres wsparcia technicznego, obowiązek informowania o lukach w zabezpieczeniach oraz konieczność zapewnienia regularnych aktualizacji zabezpieczeń. W Stanach Zjednoczonych podobną rolę odgrywa *IoT Cybersecurity Improvement Act,* który ustanawia standardy bezpieczeństwa dla urządzeń IoT używanych przez agencje rządowe.

Strategia bezpieczeństwa IoT – dobry plan to podstawa

Regularne monitorowanie stanu aktualizacji, audyty bezpieczeństwa oraz uwzględnienie w budżetach faktu, że niektóre z używanych urządzeń dotrą do kresu swojego życia (przynajmniej wg definicji ich producentów), powinny być zatem elementem praktyk operacyjnych. Firmy muszą inwestować w rozwiązania, które pozwalają na szybkie identyfikowanie przestarzałych lub podatnych na ataki urządzeń, a także rozwijać politykę zarządzania infrastrukturą IoT. Jednocześnie istotne jest nawiązywanie współpracy z dostawcami, którzy oferują długoterminowe wsparcie techniczne i gwarantują bezpieczeństwo swoich produktów przez cały ich cykl życia. Ryzyko związane z wykorzystaniem niezabezpieczonych urządzeń IoT nie dotyczy wyłącznie potencjalnych strat finansowych czy operacyjnych – jest to także kwestia ochrony danych i integralności całego systemu organizacji. Dbałość o cyfrową odporność infrastruktury staje się nie tylko środkiem zapobiegawczym, ale wręcz koniecznością.

Aby skutecznie zaplanować wymianę urządzeń IoT w organizacji, warto wdrożyć następujące praktyki:

- Stworzenie i regularne aktualizowanie inwentaryzacji wszystkich urządzeń IoT w organizacji, wraz z datami zakończenia wsparcia technicznego
- Wdrożenie systemu monitorowania wieku urządzeń i alertów o zbliżającym się końcu wsparcia (min. 12 mies. przed terminem)
- Opracowanie trzyletniego planu budżetowego uwzględniającego koszty wymiany urządzeń
- Priorytetyzacja wymiany urządzeń według ich krytyczności dla bezpieczeństwa organizacji
- Wprowadzenie polityki zakupowej preferującej dostawców oferujących minimum 5-letnie wsparcie techniczne
- Regularne testy bezpieczeństwa starszych urządzeń IoT, szczególnie zbliżających się do końca terminu wsparcia

Bezpieczeństwo IoT to nie jednorazowe działanie, ale proces wymagający ciągłej uwagi, planowania i adaptacji do zmieniających się zagrożeń. Jak pokazują liczby i przykłady botnetów takich jak Mirai, zaniechanie w tej kwestii może skutkować konsekwencjami na skalę globalną. Dlatego priorytetem powinno być budowanie środowiska, w którym technologia wspiera organizację, zamiast być jej najsłabszym ogniwem.

Monika Żuber-Mamakis
Redaktor „a&s Polska"

Ataki DDoS
Jak się przed nimi bronić?

Z raportu Cloudflare wynika, że w minionym roku na świecie liczba i skala ataków DDoS osiągnęły rekordowe poziomy. W Polsce dochodzi rocznie do tysięcy tego typu ataków. Ich celem jest zakłócenie funkcjonowania firmy lub całkowity jej paraliż.

Ataki typu DDoS (*Distributed Denial of Service*) polegają na wysyłaniu ogromnej liczby zapytań lub wywołań służących zajęciu wszelkich zasobów serwerów i uniemożliwieniu działania systemów lub usług w sieci. Są w stanie skutecznie sparaliżować działanie firm i instytucji.

Atak polega na zdalnym wykorzystaniu przez atakujących komputerów „zombie", rozmieszczonych na całym świecie, zainfekowanych złośliwym oprogramowaniem (m.in. trojany, malware). Do infekcji dochodzi najczęściej poprzez otwarcie przez użytkownika złośliwego załącznika do poczty, kliknięcie w spreparowane linki z poczty i komunikatorów internetowych, co powoduje automatyczną instalację złośliwego oprogramowania. Szkodliwy plik zagnieżdża się w zasobach komputera i na wydany przez atakującego rozkaz, bez wiedzy użytkownika, wysyła żądania połączenia ze stroną lub serwisem ofiary. Zainfekowanych w ten sposób komputerów mogą być tysiące. Tworzą wówczas tzw. botnet. Jeśli liczba wysyłanych zapytań jest większa od możliwości odpowiedzi serwisu, ten może zawiesić swoje działanie. Urządzeniami wykorzystywanymi do ataków DDoS mogą być nie tylko komputery, ale także smartfony i tablety, a nawet urządzenia IoT (kamery IP, telewizory, routery, inteligentne czujniki i inne tego typu urządzenia).

Ataki DDoS – wielowektorowe i rekordowo silne

Cloudflare, amerykańskie przedsiębiorstwo informatyczne, poinformowało o rekordowym wzroście liczby i skali ataków w 2024 r. Tylko w czwartym kwartale zneutralizowano 6,9 mln ataków, co oznacza wzrost o 83% w porównaniu z analogicznym okresem poprzedniego roku. Uwagę zwraca zwiększenie liczby ataków o hiperwolumetrycznej charakterystyce – 420 z nich przekroczyło prędkość 1 Tb/s. Największy odnotowany atak osiągnął szczytowy wolumen 5,6 Tb/s i był wymierzony w dostawcę usług internetowych w Azji Wschodniej. Trwał zaledwie 80 sekund i został przeprowadzony przez wariant botnetu Mirai, w którego skład wchodziło aż 13 tys. urządzeń IoT. Analizy CERT Orange Polska wskazują, że trendem są mocne, ale krótkotrwałe ataki. Zdecydowana większość z nich nie przekracza 10 minut. Eksperci obserwują także ataki złożone, wielowektorowe oraz długie. To tzw. *Web DDoS Tsunami,* które potrafią trwać wiele godzin lub nawet dni. Wówczas dochodzi do wielokrotnie ponawianych ataków na usługę DNS. Zaobserwowano tzw. *DNS Water Torture,* które osiągały między 50 a 300 tys. zapytań na sekundę.

Przeciwko komu ta broń?

Najczęściej atakowane są firmy hostingowe, serwisy aukcyjne i brokerskie, duże sklepy i firmy spedycyjne, strony WWW firm i instytucji. Cyberprzestępcom często chodzi o to, aby spowolnić działanie danej strony lub usługi, a czasem całkowicie ją wyłączyć. Bywa, że właściciele systemów lub stron są wcześniej szantażowani tego typu atakami. Groźba paraliżu firmy ma skłonić do zapłaty okupu. Niemal rok temu na celowniku cyberprzestępców znalazł się polski transport. Ofiarą ataków padły m.in. strony lotnisk, metra czy systemu poboru opłat za przejazd autostradą.

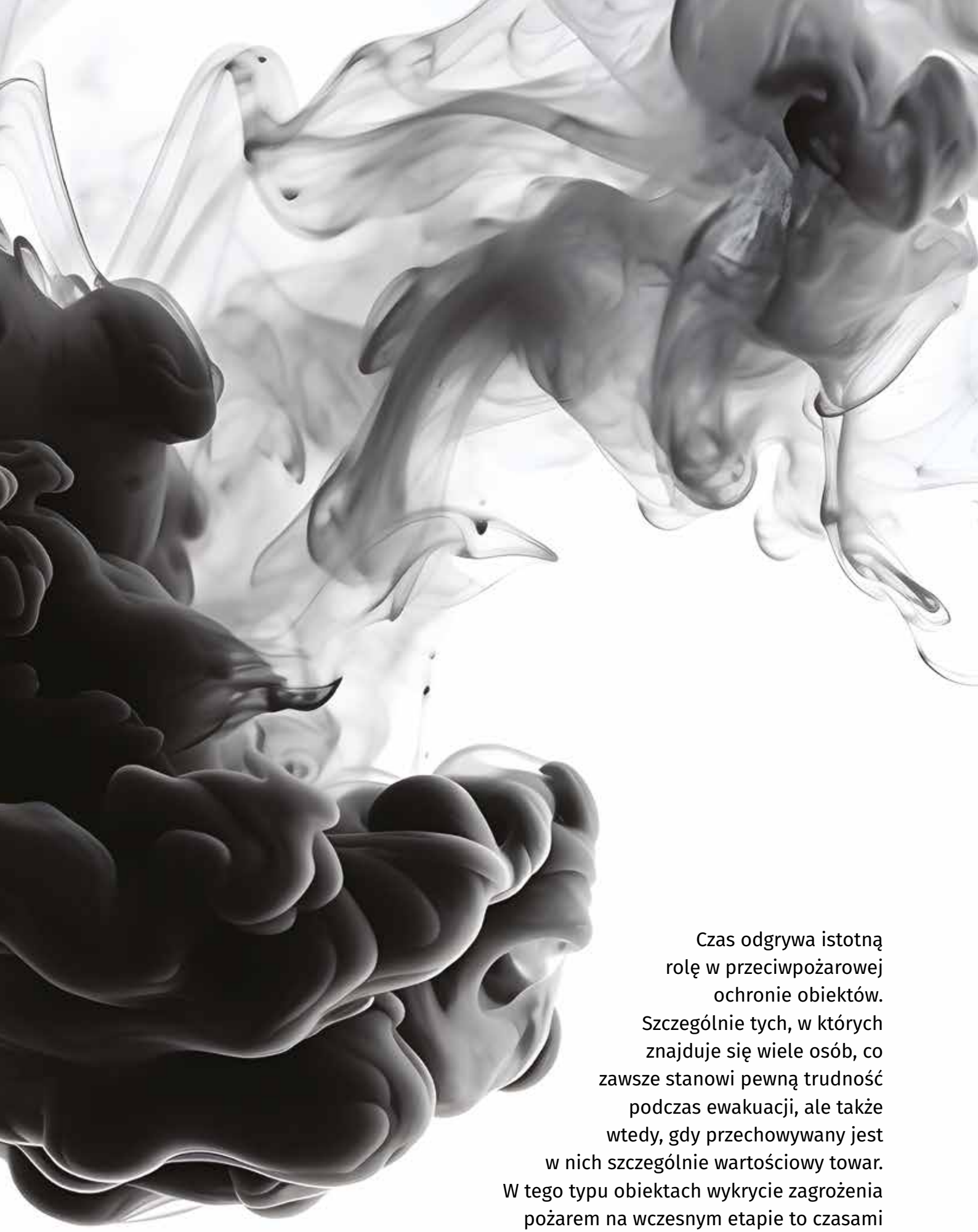
Jak się chronić?

Korzystając z usługi **Orange Internet Protection.** Ochrona przed atakami jest realizowana wewnątrz sieci Orange, dzięki czemu ataki są odpierane jeszcze przed dotarciem złośliwego ruchu do infrastruktury klienta. W przypadku ataku klient otrzymuje drogą elektroniczną informację o automatycznym uruchomieniu ochrony https://www.orange.pl/duze-firmy/orange-internet-protection. Aby zyskać większe bezpieczeństwo firmowego internetu, warto także zwrócić uwagę na usługę **Zarządzany UTM.** To kompleksowe rozwiązanie, które wykorzystuje profesjonalny sprzęt – instalowany i konfigurowany w lokalizacji klienta, do ochrony nie tylko przed niebezpieczeństwem z internetu, ale także co istotne zabezpiecza dane przekazywane między oddziałami firmy oraz dostęp do zasobów https://www.orange.pl/duze-firmy/zarzadzany-utm. •

Orange Polska
https://www.orange.pl/duze-firmy/cyberbezpieczenstwo

DYM BEZ OGNIA,

czyli o systemach wizyjnej detekcji pożaru i ważnych normach



Czas odgrywa istotną rolę w przeciwpożarowej ochronie obiektów. Szczególnie tych, w których znajduje się wiele osób, co zawsze stanowi pewną trudność podczas ewakuacji, ale także wtedy, gdy przechowywany jest w nich szczególnie wartościowy towar. W tego typu obiektach wykrycie zagrożenia pożarem na wczesnym etapie to czasami kwestia życia lub śmierci.

Jan T. Grusznic

Ilustracje: envato

Hale magazynowe i wysokiego składowania to obiekty, które nie mogą się obejść bez systemu wczesnego wykrywania pożarów. Duże wysokości oraz możliwość pojawienia się ognia w dowolnym miejscu powodują, że taki system musi wykrywać dym na różnej wysokości, ale też w miejscach najbardziej prawdopodobnego pojawienia się ognia.

Podobną specyfikę mają wszystkie wysokie i jednocześnie rozległe obiekty, np. hale sportowe. Niższe, typu magazyn, można zabezpieczyć czujkami liniowymi albo punktowymi, ale nie zapewnią detekcji dymu w czasie umożliwiającym stłumienie zarzewia pożaru i uratowanie składowanych towarów.

Im wyżej sufit, tym więcej czasu trzeba, by dym lub ciepło z pożaru tlącego się na podłodze dotarły do wysoko umieszczonego czujnika. Może się też zdarzyć, że dym i ciepło nie dotrą do wysoko zamontowanych detektorów ze względu na zjawisko zwane stratyfikacją termiczną. Dym ochładza się w miarę unoszenia, zmniejszając swoją wyporność w stosunku do otaczającego powietrza. Stygnący dym przestaje się unosić, nie może więc dostać się do czujników.

Większość stosowanych obecnie systemów sygnalizacji pożaru wykorzystuje jednocześnie różne sposoby detekcji. Technologie te obejmują detektory jonizacji punktowej i fotoelektrycznej, zasysające powietrze czujki dymu czy np. liniowe detektory z wiązką projekcyjną, ale też optyczne czujki pożaru. Wszystkie te metody wykrywania dymu są stale ulepszane. Idea przyświecająca tym ulepszeniom jest oczywista – zapewnienie jak najszerszego zasięgu systemom przeciwpożarowym i szybszej reakcji na rzeczywiste źródła pożaru przy jednoczesnym wyeliminowaniu fałszywych alarmów. Ważna jest także optymalizacja kosztów instalacji takiego systemu – im łatwiejsza jego instalacja, testowanie i późniejsza konserwacja, tym taniej.

Zastosowanie systemów wizyjnych do wykrywania pożarów wydaje się idealne, ale takie rozwiązania mogą być traktowane wyłącznie jako pomocnicze. Niestety, nie mogą być jedynym systemem wykrywającym pożar, gdyż nie ma dla nich stosownych norm, co uniemożliwia podłączenie ich do SSP na takich samych prawach jak typowe czujki. A szkoda, bo systemy wizyjnego wykrywania pożarów mają znacznie więcej zalet niż rozwiązania konwencjonalne.

Systemy wizyjnego wykrywania pożarów

Wraz z pojawieniem się technologii systemów wizyjnego wykrywania pożaru (VFD – *Video Fire Detectors*) branża bezpieczeństwa i ochrony przeciwpożarowej odkryła nowy i skuteczny sposób wykrywania dymu i ognia na bardzo wczesnym etapie. VFD staje się coraz bardziej popularne w tych miejscach, dla których nie powstał dotychczas niezawodny system wykrywania pożaru. Mowa o obiektach o wysokim stopniu zagrożenia, często wysokich lub pozbawionych sufitu, ale też takich, gdzie występują różnego rodzaju utrudnienia, takie jak składowane środki chemiczne, kurz czy wilgoć. Nałożenie się kilku takich warunków powoduje, że użycie konwencjonalnych czujek liniowych, wiązkowych lub punktowych nie sprawdzi się, co oznacza olbrzymie trudności z wykryciem dymu lub ognia.

VFD wykorzystuje kamery dozoru wizyjnego i inteligentną analizę wideo, które są w stanie rozpoznać inicjujący dym lub ogień. Choć są do tego wykorzystywane kamery dozoru wizyjnego, to ich ustawienie i kadr muszą być zgodne z celem ich instalacji. Dym i ogień to zupełnie inne zjawiska w porównaniu z działalnością człowieka, co przekłada się również na specyficzne wymagania dla tych kamer. Po pierwsze, pole widzenia i kierunek obserwacji służące wykrywaniu dymu lub ognia są różne. Pole widzenia kamer VFD jest zoptymalizowane pod kątem dostrzegania ognia w najwcześniejszym możliwym stadium pożaru. Po drugie, dzięki swojej konstrukcji pozwalają na objęcie obserwacją całego obiektu bądź jego większej części, a nie tylko jego małego fragmentu, co ma miejsce w przypadku detektorów dymu lub ciepła, które siłą rzeczy działają punktowo.

VFD może być też instalowane poza obszarem zagrożonym pożarem, co znacznie ułatwia dostęp w celu wykonania konserwacji. Kamery VFD mogą być instalowane w niemal każdym środowisku, ponieważ produkowane są dla nich różne obudowy ochronne, umożliwiające ich stosowanie w środowiskach agresywnych, także tam, gdzie występuje potencjalnie łatwopalna atmosfera lub otoczenie niosące ryzyko korozji. Produkowane są też obudowy iskroszczelne wymagane w strefach ATEX, gdzie istnieje wysokie ryzyko zagrożenia wybuchem.

Wizyjna detekcja pożaru w naturalny sposób zapewnia objęcie nadzorem obszaru od podłoża po powałę budynku. Dym nie musi pojawić się w zasięg detektora, by system mógł go wykryć. System wizyjny po prostu dym „widzi". Według wielu badań VFD wykrywa dym i ogień szybciej niż konwencjonalne systemy detekcji. Nawet jeśli są to tylko sekundy, to może mieć to znaczenie. Szczególnie, jeśli chodzi o wykrywanie pożaru w miejscach, w których występują materiały lotne lub wybuchowe. To sprawia, że systemy wizyjne są dobrym wyborem w miejscach takich jak magazyny, wewnętrzne składowiska i sortownie odpadów, hale produkcyjne, laboratoria, zakłady chemiczne, rafinerie i kotłownie.

Systemy wizyjnego wykrywania pożaru są już na tyle dojrzałe, że wskaźnik fałszywych alarmów jest stosunkowo niski. Skutecznie analizują obraz wideo, aby odróżnić dym lub ogień od innych nieprawidłowości, takich jak osoby poruszające się w polu widzenia, zwierzęta, pojazdy lub przedmioty. Operatorzy mogą monitorować obrazy w czasie rzeczywistym i reagować, gdy system aktywuje alarm. Zapewnienie dozoru zdalnego jest nie do przecenienia – operatorzy mogą dzięki temu ocenić charakter i wielkość pożaru, a także etap jego rozwoju bez narażania zdrowia i życia. Na podstawie nagrań sprzed incydentu mogą sprawdzić czy w miejscu zdarzenia znajdowali się ludzie i lepiej ocenić sytuację. W ten sposób mogą również lepiej wykorzystać posiadane zasoby. Po incydencie materiał wizyjny można wykorzystać do analizy i zapobiegania przyszłym zdarzeniom, a także do celów ubezpieczeniowych.

Bez normy nie ma odbioru

Stosownych polskich norm dla opisanych wcześniej rozwiązań nie ma, a bez tego, jak już wcześniej wyjaśniłem, nie mogą być

VFD wykrywa dym i ogień z prędkością porównywalną lub większą niż konwencjonalne systemy detekcji

podłączone do SSP tak samo jako czujki konwencjonalne. Co w takim razie powinien zrobić projektant lub konsultant proponujący takie rozwiązanie? Najlepsze moim zdaniem jest sięgnięcie po normy EN54-10, ale też ISO 7240 – 29, FM3232, UL268B oraz VdS 3878 i VdS 3847. Wszystkie jednocześnie? Oczywiście, nie. Należy uwzględniać te pasujące do specyfiki konkretnych urządzeń.

Większość systemów detekcji opartych na kamerach wykorzystuje obrazy widma widzialnego w celu wykrywania dymu lub ognia. Niektóre rozwiązania są połączone z oświetlaczami podczerwieni, aby działać w ciemności. Inne korzystają z obrazów termowizyjnych do detekcji podwyższonej temperatury. Dla każdego z tych rozwiązań stosuje się inne metody badań i certyfikacji. W Polsce obowiązują europejskie normy zharmonizowane z dyrektywą 89/106/EWG, w których na próżno szukać wytycznych dla VFD.

EN 54-10 *(Systemy sygnalizacji pożarowej. Część 10: czujki płomienia – czujki punktowe)* określa wymagania, metody badań oraz kryteria działania punktowych, kasowalnych czujek płomienia, które funkcjonują z wykorzystaniem promieniowania płomienia (czujki podczerwieni IR, czujki nadfioletu UV i czujki wielopasmowe), przeznaczonych do stosowania w systemach sygnalizacji pożarowej, instalowanych w budynkach. Nie jest to jednak dokument jasno wskazujący na wykorzystanie kamer. Jest on na tyle ogólny, że kamery termowizyjne można jednak uznać za czujki płomienia, pracujące w systemie podczerwieni, reagujące tylko na promieniowanie o długości fali większej niż 850 nm, pod warunkiem że są wyposażone w indywidualny, zintegrowany optyczny wskaźnik działania, umożliwiający identyfikację wysyłającej alarm czujki. Czujka taka podczas testów musi wysłać sygnał alarmowania w czasie 30 s po narażeniu jej na promieniowanie pochodzące od dwóch pożarów testowych (tacka zawierająca n-heptan i tacka zawierająca spirytus skażony). W ramach EN 54-10 wyróżnione zostały 3 klasy:

Klasa 1	Jeśli wszystkie próbki reagują na oba rodzaje pożaru przy odległości co najmniej 25 m
Klasa 2	Jeśli wszystkie próbki reagują na oba rodzaje pożaru przy odległości co najmniej 17 m
Klasa 3	Jeśli wszystkie próbki reagują na oba rodzaje pożaru przy odległości co najmniej 12 m

Jeśli wszystkie testowane czujki wyślą alarm, test kończy się wynikiem pozytywnym. Wystarczy, by zawiodła jedna, a test nie zostanie zaliczony. Co warto zaznaczyć, EN 54-10 dotyczy wyłącznie rozwiązań stosowanych wewnątrz pomieszczeń.

Normy opracowane po sąsiedzku

Niemiecki instytut VdS Schadenverhütung w 2022 r. wprowadził w ramach normy VdS 3878 precyzyjne wytyczne dotyczące charakterystyki działania kamer termowizyjnych w zastosowaniach pożarowych oraz metod ich testowania. Zgodnie z wytycznymi VdS kamery te nie są (!) czujkami pożarowymi. Przy okazji warto wiedzieć, że nie ma dla nich innych norm europejskich.

Kamery czułe na podczerwień wykrywają nieprawidłowości temperatury w monitorowanym obszarze i na wczesnym etapie, a tym samym służą jako uzupełnienie systemów wykrywania pożaru i systemów alarmowych. Norma VdS 3878 wyraźnie wskazuje, jak ma być przeprowadzony test na zgodność urządzenia z jej wytycznymi, w którego ramach jednym z zadań jest podgrzanie urządzenia emitującego ciepło o 10 stopni Kelvina powyżej progu alarmowego. Urządzenie referencyjne jest następnie umieszczane w obszarze przechwytywania i sprawdzane, czy został uruchomiony sygnał alarmowy. Wykonywane są również testy

Zestawienie pożarów testowych (z podziałem na rodzaj spalanego materiału) oraz dominujące czynniki towarzyszące (zgodnie z ISO/TS 7240-9)

Test	TF1	TF2	TF3	TF4	TF5	TF6	TF8
Rodzaj pożaru testowego	płomieniowe spalanie drewna	rozkład termiczny (piroliza) drewna	pożar tlewny bawełny	płomieniowe spalanie tworzywa (poliuretanu)	spalanie cieczy (n-heptan) wydzielającej dym	spalanie cieczy (alkohol etylowy) nie-wydzielającej dymu	spalanie cieczy (dekalina) wydzielającej dym
Dominujące czynniki pożarowe	otwarty płomień, dym słabo widoczny, silny wzrost temperatury	jasny dym rozpraszający, o małej prędkości wznoszenia	jasny dym rozpraszający, o bardzo małej prędkości wznoszenia	bardzo ciemny dym, wzrost temperatury	bardzo ciemny dym, wzrost temperatury	silny wzrost temperatury	ciemny dym, niewiel-ki wzrost temperatury

temperatury reakcji statycznej polegające na wprowadzeniu alarmu przy zwiększającej i zmniejszającej się temperaturze źródła promieniowania i zakres progów alarmowych. Niestety, nie jest testowana czułość na zmieniające się warunki środowiskowe (np. zmiany temperatury, wilgotności, wstrząsy itp.). Urządzenie nie musi, ale może mieć wbudowany czerwony wskaźnik optyczny, który może być używany do wskazywania ogólnego stanu alarmowego do momentu zresetowania.

VdS 3878 również wprowadza 3 klasy produktów, przy czym są to klasy środowiskowe:

Klasa I	Urządzenia, instalowane w budynkach komercyjnych/przemysłowych, ale w przypadku których należy unikać ekstremalnych warunków środowiskowych
Klasa II	Urządzenia instalowane w budynkach komercyjnych/przemysłowych we wszystkich obszarach
Klasa III	Urządzenia instalowane na zewnątrz budynków

Usterka systemu musi być przekazana za pośrednictwem złącza wyjścia usterki najpóźniej w ciągu 3 min. Z kolei awaria głowicy uchylno-obrotowej (która może stanowić element VFD) systemu chłodzącego lub ścieżki transmisji musi zostać zgłoszona w ciągu 100 s.

Natomiast dla systemów pracujących w zakresie widma widzialnego VdS opracował inną normę – 3847 – dotyczącą kamer wideo do wizualnego monitorowania pożarów wewnątrz budynków.

I podobnie jak w przypadku VdS 3878 również ta norma określa, że kamery wideo nie są czujkami pożarowymi, a jedynie wspomagają wykrywanie dymu lub płomieni. Mogą więc być uzupełnieniem systemów sygnalizacji pożaru, nawet jeśli w zamyśle projektanta miałyby być systemem głównym.

VdS 3847 dzieli VFD na trzy typy pod kątem oceny parametru pożarowego:

Typ 1	widoczny płomień (TF1, TF5, TF6, TF8)
Typ 2	dym (TF2, TF3, TF4, TF8)
Typ 3	widoczny płomień i dym (TF1, TF2, TF3, TF4, TF6, TF8)

Pomiar czasu reakcji jest wykonywany przez wykonanie pożarów testowych (od TF1 do TF8) zgodnie z normą EN 54-7 przy średnim natężeniu światła ok. 150 luksów. Testowy pożar jest rejestrowany za pomocą kamery z odległości ok. 4 m przy szerokości obszaru pola widzenia kamery wynoszącym 70 st. Tak zarejestrowany obraz jest następnie wyświetlany na ekranie wysokiej rozdzielczości umieszczonym na wprost obiektywu kamery, tak by ekran wypełniał cały obszar widzenia kamery. Zadaniem takiego zabiegu jest utrzymanie jak największej powtarzalności procesu dla testowanych urządzeń. Z kolei czułość na rzeczywiste pożary wykonywana jest przy najbardziej niekorzystnym ustawieniu kamery do badania. Czas sygnalizacji nie może przekraczać 30 s. Interesujące jest, że VdS 3847 zakłada wykonanie ponownych testów po badaniach środowiskowych.

W styczniu 2024 r. została opublikowana norma ISO 7240-29 – *Systemy wykrywania i sygnalizacji pożaru – Część 29: Wizyjne czujki detekcji pożaru*. Norma określa wymagania, metody testowania i kryteria wydajności dla wizyjnych czujek pożarowych, działających w paśmie światła widzialnego. Ogólnie rzecz biorąc, normy produktowe określają minimalne oczekiwania dotyczące wydajności i testują spójność reakcji urządzeń na warunki stresowe.

ISO 7240-29 wymaga, by czułość urządzenia wystawianego na szczególne warunki (np. zimno, wibracje, SO2 i EMC) była potwierdzana okresowo powtarzanymi testami. Ocena czułości polega m.in. na sprawdzeniu, ile dymu lub płomienia potrzeba, aby uruchomić alarm. Stosowany jest też zestaw testów pożarowych dających odpowiedź na pytanie, czy czujka reaguje na „typowe" pożary, które powinna wykrywać (patrz tabela: *Typy pożaru*). Norma wprowadza wyraźne rozróżnienie między detekcją dymu (typ A) i płomienia (typ B) przez odpowiednio reagujące urządzenia, definiując jedne jako czujki typu A, a drugie jako czujki typu B. Co istotne, uwzględnia także czujki reagujące na oba zjawiska (typ AB).

Podobnie jak inne normy EN 54 i ISO 7240 część 29 nie podaje żadnych wytycznych dotyczących fałszywych alarmów. Zawiera jednak klauzulę stwierdzającą, że „czujniki powinny być odporne na zjawiska, które mogą powodować niepożądane alarmy". Odnosi się to jednak do szeregu krytycznych usterek, które mogą uniemożliwić działanie VFD. Mogą to być np. utrata ostrości, zanieczyszczenie środowiska optycznego (np. obiektywu,

szyby obudowy itp.), zasłonięcie pola widzenia lub zamknięcie przysłony obiektywu. ISO 7240-29 wymaga pracy przy poziomach oświetlenia 15–10 tys. luksów. Górna granica dotyczy zastosowań zewnętrznych. Badany jest również wpływ sztucznego światła na VFD, w tym np. światło fluorescencyjne, halogenowe, wysokociśnieniowe i niskociśnieniowe światło sodowe, LED, laserowe, a nawet spawanie łukowe. We wszystkich przypadkach VFD nie może sygnalizować pożaru ani usterki.

Zgodnie z normą alarm musi być sygnalizowany za pomocą czerwonej diody LED. Jest to standardowa cecha wszystkich urządzeń detekcyjnych z serii EN 54 i ISO 7240. Jednakże wyjątkowo w przypadku VFD czerwona dioda LED nie jest wymagana, jeśli obraz jest dostarczany na bieżąco użytkownikom. To ustępstwo zostało poczynione przy założeniu, że oprogramowanie użytkownika wyświetla obraz z kamery z wyraźnym wskazaniem stanu pożaru i jego lokalizacją.

System wizyjnego wykrywania pożarów ma wiele zalet, których brakuje technologiom konwencjonalnym:

- może wykrywać pożar bezpośrednio u źródła, praktycznie z dowolnej odległości. Dzięki systemom wizyjnym alarm jest wzbudzany zanim dym dosięgnie czujki;
- generuje mniej fałszywych alarmów. Systemy „przewrażliwione" stają się bezużyteczne, gdyż ludzie mają tendencję do ignorowania alarmów, jeśli te zbyt często są nieprawdziwe. Im mniej fałszywych alarmów, tym większą czujność zachowują operatorzy, traktujący wówczas każde powiadomienie z należytą powagą;
- daje operatorowi pole do interpretacji. Ponieważ detekcja jest tak szybka i umożliwia weryfikację wizualną, VFD zapewnia operatorowi cenny czas na podjęcie uzasadnionej decyzji.

Coraz więcej specjalistów ds. bezpieczeństwa pożarowego przyznaje, że VFD wypełnia lukę na rynku, ponieważ oferuje sposób na zabezpieczenie obszarów, dla których do tej pory nie było rozwiązania. Niemniej pewną niedogodnością tego rozwiązania jest brak wyraźnie określonych, choćby przez Polski Komitet Normalizacyjny, norm dla urządzeń i systemów przez nie tworzonych. Projektanci mogą podpierać się normami opracowanymi przez naszych zachodnich sąsiadów, co nie zmienia faktu, że nawet zaawansowany system VFD musi być uzupełniony o konwencjonalne czujki dymu i ognia. Mimo braku norm liczne systemy VFD funkcjonują z dużym powodzeniem. Wdrożenia bez norm są, jak widać, równie możliwe, jak dym bez ognia.

Jan T. Grusznic
redaktor „a&s Polska"

WIZYJNE SYSTEMY DETEKCJI DYMU I PŁOMIENIA

BCS

Systemy detekcji dymu i płomienia na obrazie wideo

Tradycyjne metody detekcji pożarów oparte na czujkach dymu i ciepła mają swoje ograniczenia. Systemy detekcji dymu i płomienia na obrazie wideo oferują nową jakość w identyfikacji zagrożeń pożarowych. Wykorzystują algorytmy sztucznej inteligencji do analizy obrazu, co umożliwia szybkie wykrywanie dymu i płomienia. Dzięki temu są one bardziej precyzyjne i efektywne w porównaniu do tradycyjnych metod.

Kamery, takie jak np. BCS-L-TIP242FR3-TH-Ai1(0403) z analizą obrazu stosuje się do monitorowania określonych obszarów i analizowania zapisanych danych w czasie rzeczywistym. Mogą być instalowane w różnych lokalizacjach, w tym na zewnątrz budynków, w halach produkcyjnych, magazynach, biurowcach czy na obszarach leśnych.

Detekcja dymu polega na identyfikacji specyficznych wzorców zmieniających się w czasie, takich jak kształt, kolor i ruch dymu. Z kolei rozpoznanie płomienia bazuje na analizie parametrów świetlnych, np. intensywności światła, koloru i migotania.

BCS-L-EIP242FR3-TH-AI(0202)

BCS-L-TIP242FR3-TH-Ai1(0403)

BCS-L-TIP542FR5-THT-Ai1(0807)

Algorytmy zastosowane w kamerze BCS-L-EIP242FR3-TH-AI(0202) są w stanie wychwycić nawet najmniejsze oznaki pożaru, co pozwala na wczesne ostrzeżenie i podjęcie działań prewencyjnych.

Pomimo licznych zalet, systemy detekcji dymu i płomienia na obrazie wideo nie są doskonałe. Jednym z głównych wyzwań jest fałszywe alarmowanie wynikające z obecności innych źródeł dymu czy światła, które mogą być błędnie zinterpretowane jako oznaki pożaru. Jednak dzięki ciągłemu rozwojowi technologii i algorytmów, systemy te stają się coraz bardziej zaawansowane i niezawodne.

Obecnie najbardziej niezawodną metodą wykrycia zagrożenia jest pomiar temperatury, który oferują kamery termowizyjne, np. BCS-L-TIP542FR5-THT-Ai1(0807). Zapewniają możliwość dokładnego określenia poziomu temperatury, przekroczenie którego uznawane jest za niebezpieczne dla otoczenia.

Więcej na: **www.bcs.pl**

LINC POLSKA

Teledyne FLIR – FH-Series R kamera do wczesnego wykrywania pożaru

FH-Series R marki Teledyne FLIR to kamery stałopozycyjne, integrujące obraz termowizyjny z pomiarem temperatury z obrazem widzialnym 4K. Koncepcja ta umożliwia wizualizację i weryfikację punktów o podwyższonej temperaturze, pozwalając na szybkie wykrycie źródła pożaru. W przypadku zidentyfikowania „gorącego" punktu lub zmiany temperatury (bezdotykowy pomiar temperatury), sygnał jest automatycznie wysyłany do operatora w celu oceny sytuacji i podjęcia natychmiastowych działań.

FH-Series R Teledyne FLIR oferuje:

- **Szybką detekcję i wideoweryfikację**
  Integracja przetwornika termowizyjnego z tradycyjnym o wysokiej rozdzielczości umożliwia wykrywanie przekroczenia określonej temperatury i wideoweryfikację zagrożenia przy użyciu jednego urządzenia.
- **Inteligentne alarmy**
  Zminimalizowanie liczby fałszywych alarmów jest możliwe dzięki zastosowaniu dwóch przetworników i wbudowanej analizie wideo. Łącząc skuteczność wykrywania podwyższonej temperatury na danym obszarze z inteligentnym wykrywaniem pojazdów, można radykalnie ograniczyć liczbę fałszywych alarmów powodowanych przez gorące rury wydechowe.
- **Indywidualną konfigurację**
  Korzystając z wbudowanego narzędzia do planowania istnieje możliwość indywidualnego skonfigurowania kamery odpowiednio do pory dnia, godzin pracy czy innych okresów czasu.
- **Łatwą integrację**
  Kamery z serii FH marki Teledyne FLIR, mogą stanowić część kompleksowego rozwiązania tego producenta lub mogą działać w połączeniu z innymi preferowanymi rozwiązaniami firm trzecich.

Kamera termowizyjna umożliwiająca pomiar temperatury w połączeniu z przetwornikiem światła widzialnego i wbudowaną wideoanalityką, to ekonomiczne rozwiązanie pozwalające na szybkie wykrycie źródła ognia, zanim dojdzie do pożaru. Dzięki tej integracji uzyskujemy możliwość oceny i eliminacji zagrożeń w czasie rzeczywistym.

Więcej na: **www.linc.pl**

VIVOTEK

Nowe kamery termowizyjne w ofercie VIVOTEK

Z końcem 2024 roku oferta VIVOTEK poszerzyła się o nowe kamery termowizyjne, w tym kamery termowizyjne typu bullet, TB9332-E w rozdzielczości 640x512 oferującą czułość termiczną na poziomie NETD < 40 mK @ F1.0; dostępne w czterech wariantach ogniskowych (9, 15, 35 oraz 50mm), a także kamery bispektralne, dostępne w obudowach kopułowych (TT9333-E) oraz obudowach typu bullet (TB9333-E) oferujące rozdzielczość 256x192 skalowalną aż do 704x576 (dla termowizji) i czułość termiczną na poziomie NETD < 50 mK @ F1.0 oraz rozdzielczość 2880x1620 (dla światła widzialnego). Kamery bispektralne dostępne są w wersjach z ogniskową 3.5 oraz 7mm.

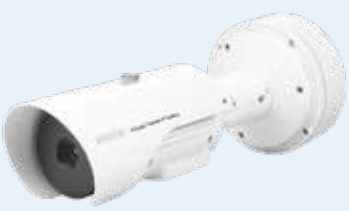
Kamery termowizyjne to specjalistyczne rozwiązania pozwalające nie tylko na obserwację monitorowanego obszaru w całkowitej ciemności poprzez tworzenie obrazów na bazie ciepła emitowanego przez obiekty, ale również pozwalające na pomiar temperatury tych obiektów. W połączeniu z zaawansowanymi funkcjami analizy obrazu są w stanie m.in. wykrywać pożary w ich wczesnym stadium, wykrywać wzrost lub spadek temperatury monitorowanych obiektów, ale również wykrywać np. dym czy osoby palące papierosy w miejscach niedozwolonych.

Dzięki możliwości integracji danych z kamer termowizyjnych z zewnętrznymi systemami, użytkownicy otrzymują wysokiej jakości rozwiązania pozwalające na minimalizowanie strat w przypadku wystąpienia niepożądanych wzrostów lub spadków temperatury obserwowanych obiektów poprzez np. uruchomienie systemów gaszenia czy awaryjne odcięcie zasilania.

Poza wykorzystaniem kamer termowizyjnych w ochronie obwodowej, przemyśle czy do monitorowania obiektów infrastruktury krytycznej, urządzenia te są coraz częściej wykorzystywane w gospodarstwach domowych chociażby do monitorowania przydomowych magazynów energii czy garaży posiadaczy samochodów elektrycznych. Również firmy ubezpieczeniowe coraz częściej zaczynają wymagać stosowania kamer termowizyjnych w przypadku chociażby instalacji fotowoltaicznych.

Więcej na: **www.vivotek.com**

TB9333-E



TB9332-E

TT9333-E

Wczesne wykrywanie dymu i płomieni – niezawodna ochrona ludzi, obiektów i dóbr

Twoje bezpieczeństwo to nasz priorytet. Wyobraź sobie rozwiązanie, które niezawodnie wykrywa zagrożenia pożarowe na wczesnym etapie, chroniąc życie, mienie i inwestycje. Mobotix oferuje innowacyjną technologię, która zapewnia spokój ducha dzięki precyzyjnemu monitorowaniu i zgodności z najwyższymi standardami bezpieczeństwa.

Kamera Mobotix to przełomowe rozwiązanie w dziedzinie monitoringu i ochrony przeciwpożarowej. To jedyna kamera na świecie, która może być bezpośrednio podłączona do systemów alarmowych przeciwpożarowych dzięki zgodności z rygorystycznym **certyfikatem EN54-10.**

Wczesne wykrywanie dymu oraz płomieni jest kluczowym elementem ochrony przeciwpożarowej, umożliwiającym szybką interwencję i minimalizację szkód. Dzięki zaawansowanym rozwiązaniom termowizyjnym MOBOTIX można monitorować nawet te obszary, które są poza zasięgiem tradycyjnych systemów wykrywania pożaru.

MOBOTIX, jako pierwszy producent systemów wideo, uzyskał potrójną certyfikację w zakresie ochrony przeciwpożarowej, co potwierdza jakość i niezawodność jego produktów. Certyfikowane systemy MOBOTIX mogą indywidualnie i precyzyjnie monitorować do 20 obszarów w jednym polu widzenia, co pomaga uniknąć fałszywych alarmów.

Certyfikacja CNPP – niezawodne wykrywanie dymu i płomieni

Francuskie Narodowe Centrum Zapobiegania i Ochrony (CNPP) certyfikowało rozwiązania MOBOTIX do integracji z systemami alarmowymi przeciwpożarowymi. Pakiet rozwiązań składa się z kamery (M73, S74) oraz dedykowanej aplikacji. Możliwe jest również użycie dodatkowych czujników optycznych i modernizacja istniejących kamer.

Certyfikacja EN 54-10 – zgodność z systemami alarmowymi p.poż.

Europejski Komitet Normalizacyjny (CEN) opracował wytyczne dotyczące systemów alarmowych w serii norm EN 54. Pakiety rozwiązań MOBOTIX, składające się z kamer IoT (M16, M73, S74) i akcesoriów, spełniają wymagania rozporządzenia dotyczącego wyrobów budowlanych UE. Dodatkowo mogą być one wyposażone w dodatkowe czujniki optyczne.

Certyfikacja VdS – uznanie w branży ochrony przeciwpożarowej

VdS Schadenverhütung GmbH, największy w Europie instytut ds. bezpieczeństwa korporacyjnego, przyznał certyfikację rozwiązaniom MOBOTIX. Termowizyjne kamery MOBOTIX z kalibrowanym sensorem mogą wywoływać alarmy i przesyłać wiadomości sieciowe, gdy zostaną przekroczone zdefiniowane progi temperatur. Systemy te są oparte na kamerach Mobotix M16 wraz z interfejsami (ochrona przed przepięciami, zasilanie, połączenie z centrum sterowania).

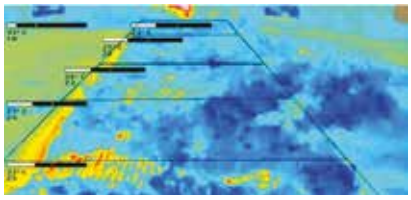
Gwarancja jakości

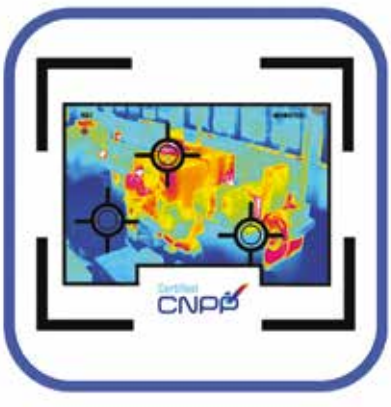
Wszystkie certyfikowane kamery termowizyjne MOBOTIX są produkowane w Niemczech, a firma oferuje 5-letnią gwarancję na swoje produkty, co dodatkowo potwierdza ich jakość i niezawodność.

Dzięki zaawansowanym technologiom MOBOTIX, wczesne wykrywanie pożarów stało się bardziej precyzyjne i skuteczne, co pozwala na szybszą interwencję i ochronę ludzi, budynków oraz mienia.

Postaw na bezpieczeństwo i niezawodność

Kamera Mobotix to narzędzie innowacyjne, które łączy nowoczesną technologię z najwyższymi standardami certyfikacyjnymi. Dzięki niej masz pewność, że Twoje obiekty są skutecznie chronione przed zagrożeniami pożarowymi. •





Mobotix – Twoje bezpieczeństwo w najlepszych rękach!

Konica Minolta Business Solutions Polska
ul. Krakowiaków 44
02-255 Warszawa
www.konicaminolta.pl

Perspektywy i kierunki rozwoju branży security

WAT

4 lutego 2025 r. odbyła się wyjątkowa, jubileuszowa 10. edycja Seminarium Branży Elektronicznych Systemów Bezpieczeństwa (SBESB), połączona z konkursem o tytuł Mistrza Elektronicznych Systemów Bezpieczeństwa. Tegoroczne wydarzenie miało szczególny charakter, ponieważ wpisywało się w obchody 50-lecia działalności Instytutu Systemów Elektronicznych. Organizatorem seminarium był Instytut Systemów Elektronicznych Wydziału Elektroniki Wojskowej Akademii Technicznej, we współpracy z czołowymi firmami z branży security, a merytorycznym partnerem przedsięwzięcia była Polska Izba Systemów Alarmowych.

Tematem przewodnim tegorocznej edycji były „Kierunki i perspektywy rozwoju elektronicznych systemów bezpieczeństwa". Uczestnicy seminarium mieli okazję wysłuchać prelekcji ukazujących osiągnięcia ostatnich 10 lat w zakresie projektowania i wdrażania nowoczesnych rozwiązań w systemach zabezpieczeń. Wydarzenie stało się również platformą do wymiany doświadczeń między środowiskiem akademickim a przedstawicielami branży, podkreślając znaczenie współpracy na rzecz podnoszenia jakości kształcenia w specjalności Inżynieria Systemów Bezpieczeństwa.

Integralną częścią SBESB był tradycyjny konkurs o tytuł Mistrza Elektronicznych Systemów Bezpieczeństwa, skierowany głównie do studentów kierunku Elektronika i Telekomunikacja. W tym roku rywalizacja wyłoniła sześciu laureatów. Zwycięzcą został inż. Mateusz Koperski, student studiów II stopnia, który otrzymał statuetkę oraz nagrody ufundowane przez partnerów wydarzenia. Pierwsze i drugie miejsce w konkursie zajęli odpowiednio inż. Filip Zalewski oraz inż. Marek Ledworowski. Wyróżnienia przyznano Bartoszowi Lechowi, Kacprowi Bodeckiemu i Albertowi Kobyłce.

Jubileuszowe SBESB cieszyło się dużym zainteresowaniem ze strony zarówno studentów – w tym wojskowych – jak i przedstawicieli firm z branży. Spotkanie po raz kolejny pokazało, jak ważne jest wspólne działanie na rzecz kształcenia specjalistów w dziedzinie ESB. Przemysłowi partnerzy seminarium od lat wspierają Instytut, nie tylko organizując praktyki i staże, ale także wyposażając laboratoria w nowoczesny sprzęt.

Tradycyjnie finałem wydarzenia był konkurs strzelecki na strzelnicy WAT, którego wyniki zadecydowały o kolejności wystąpień podczas przyszłorocznej edycji seminarium.

Kamera z podwójnym obiektywem i czytnikiem kodów kreskowych

Hanwha Vision

Hanwha Vision, światowy lider rozwiązań wizyjnych, prezentuje przełomowe urządzenie – kamerę z podwójnym obiektywem i wbudowanym czytnikiem kodów kreskowych, dostępną w trzech wersjach: TNS-9040IBC, TNS-9050IBC i TNS-9060IBC. To pierwsze na rynku rozwiązanie łączące funkcje skanera kodów kreskowych i kamery monitoringu wizyjnego. W połączeniu z platformą Vision Logistics Tracking Software w czasie rzeczywistym umożliwia śledzenie przesyłek i dozór wizyjny, co usprawnia pracę magazynu, eliminuje błędy wysyłkowe i redukuje liczbę zwrotów.

Nowa kamera Hanwha Vision wyróżnia się możliwością jednoczesnego skanowania wielu kodów kreskowych w kadrze. Zastosowana technologia AI do wykrywania etykiet w trybie monochromatycznym radzi sobie nawet z szybko poruszającymi się przesyłkami na taśmociągach. A aplikacja WiseBCR daje natychmiastowy dostęp do danych o zeskanowanych kodach wraz z pełną historią operacji.

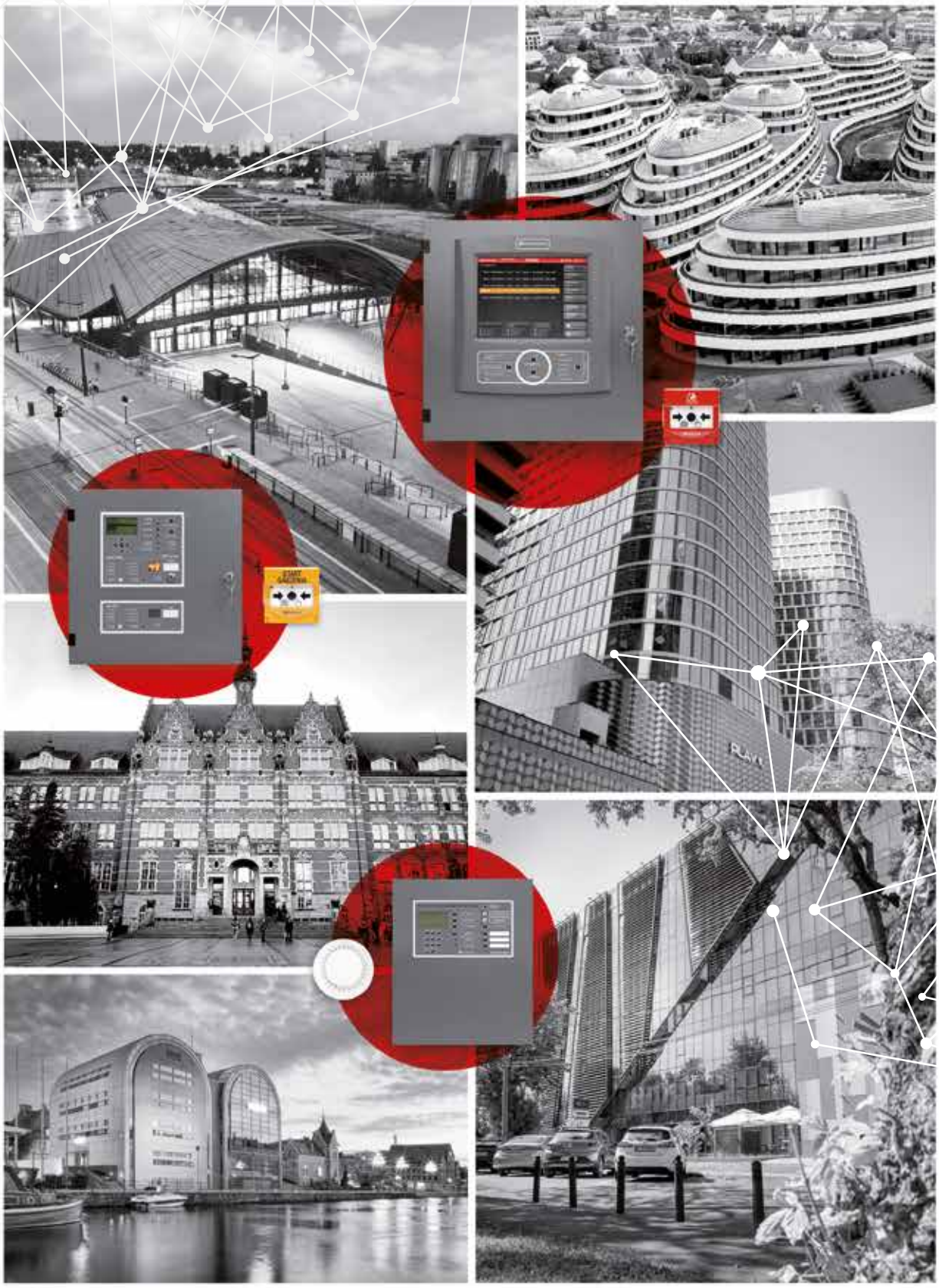
Oba przetworniki kamery pracują w rozdzielczości 4K, zapewniając krystalicznie czysty obraz. Do wyboru są trzy warianty obiektywów (16, 25 lub 35 mm), co pozwala na dopasowanie pola widzenia do konkretnych potrzeb i warunków w magazynie.

W przeciwieństwie do tradycyjnych rozwiązań wymagających osobnych instalacji czytników kodów i kamer CCTV nowy model Hanwha Vision to znacząca oszczędność. Personel zyskuje wygodne narzędzie do szybkiej weryfikacji przesyłek i analizy zdarzeń w jednym interfejsie. Solidna konstrukcja ze złączami M12, potwierdzona certyfikatami IP66/67 i IK10, gwarantuje niezawodność nawet w trudnych warunkach przemysłowych.

Kamera współpracuje z zaawansowaną platformą Vision Logistics Tracking Software (VLTS), zapewniającą pełną kontrolę nad operacjami. System wspiera również integrację ze skanerami ręcznymi różnych producentów, co jest szczególnie przydatne w centrach dystrybucyjnych.

Dzięki temu rozwiązaniu kierownicy logistyki mogą znacząco podnieść wydajność pracy, zoptymalizować koszty i zwiększyć bezpieczeństwo operacji, jednocześnie minimalizując ryzyko strat i kradzieży.

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

Linc Polska

Camect jest po prostu smart!

Camect Smart Hub to rejestrator wykorzystujący analizę bazującą na algorytmach AI z zastosowaniem sieci neuronowych. Oferuje skuteczną wideoanalitykę, która jest ciągle udoskonalana. Najnowsze aktualizacje są dostępne dla wszystkich urządzeń i oferują szereg praktycznych funkcjonalności. Jedną z nich jest obsługa audio w trzech torach. Głośniki można podłączyć do analogowego wyjścia w urządzeniu, wyjścia audio w kamerze. Trzecią opcją jest użycie dedykowanych głośników IP. Każdy z nich może nadawać inny komunikat głosowy, można je przypisać do określonych kamer czy stref alarmowych. Operator może również rozmawiać na żywo z osobą przebywającą na obiekcie.

Drugą istotną zmianą jest wprowadzenie dedykowanej aplikacji Camect Viewer działającej z systemami Android i iOS. Aplikacja umożliwia sprawną obsługę systemu na żywo, jak i przeglądanie zdarzeń. Dzięki niej z poziomu telefonu można ustawić indywidualne powiadomienia alarmów. Rozróżnianie ponad 30 typów obiektów umożliwia ustawienie indywidualnych powiadomień, np. o kurierze, który przywiózł paczkę, czy kocie, który niszczy rabatkę.

Camect to niezawodne rozwiązanie do wideoanalizy, oferujące skuteczność detekcji na poziomie około 99,7%. Wybierając jeden z 3 modeli Camect 24, Camect 60 lub Camect 96, można zapewnić niemal bezbłędne wykrywanie intruzów.

Te i inne funkcjonalności znajdziesz w Camect, bo Camect jest po prostu smart!

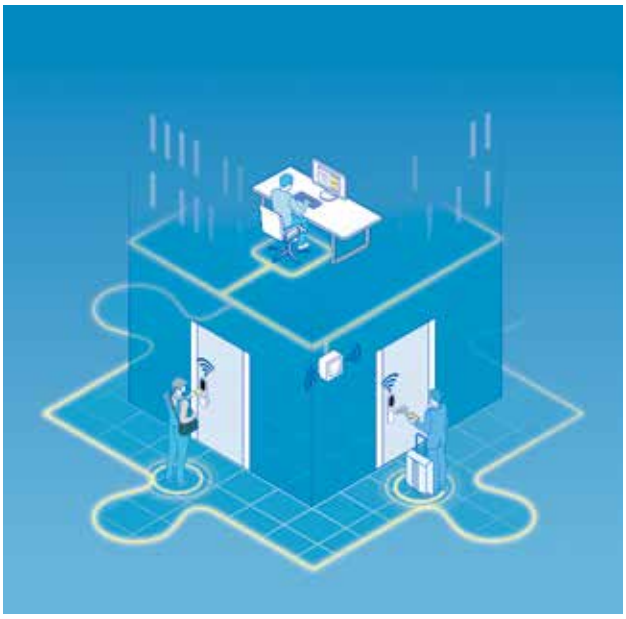
Roger

Integracja systemu kontroli dostępu RACS 5 z zamkami bezprzewodowymi Aperio firmy ASSA ABLOY

Zamki Aperio to rozwiązania bezprzewodowe umożliwiające łatwą modernizację istniejących systemów drzwiowych i ich dostosowanie do standardów elektronicznej kontroli dostępu. Integracja systemu kontroli dostępu RACS 5 z zamkami Aperio przynosi inwestorowi liczne korzyści. Do najważniejszych z nich zaliczyć można:

- Zarządzanie wszystkimi punktami dostępu z poziomu jednego centralnego systemu (VISO), co upraszcza administrację i zwiększa efektywność.
- Zabezpieczenie dostępu w miejscach, gdzie standardowa kontrola dostępu (KD) nie może być zastosowana np. ze względu na brak możliwości doprowadzenia okablowania.
- Możliwość połączenia rozwiązania bezprzewodowego z przewodową kontrolą dostępu, co pozwala na dostosowanie do specyficznych potrzeb.
- Łatwa modyfikacja uprawnień dostępu oraz możliwość integracji z innymi systemami zabezpieczeń.
- Redukcja kosztów związanych z okablowaniem i konserwacją oraz szybszy proces instalacji.

Zamki Aperio zintegrowane z systemem RACS 5 mogą być wykorzystywane w różnych środowiskach, takich jak biura, obiekty przemysłowe, placówki edukacyjne czy szpitale. Współpraca pozwala na uzyskanie zaawansowanego i elastycznego rozwiązania, które spełnia współczesne wymagania systemów zabezpieczeń i zapewnia wygodę użytkowania. Wdrożenie wspomnianej integracji w organizacji umożliwia efektywne zarządzanie dostępem do obiektów, co pozwala na minimalizację ryzyka oraz optymalizację procesów administracyjnych.




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 MANAGER

MONITORING W CENTRACH LOGISTYCZNYCH

1000

Pełna kontrola nad monitoringiem wizyjnym w dużych lub mniejszych centrach przemysłowych – obsługa do 1000 urządzeń BCS lub innych producentów oraz obsługa wielu monitorów podłączonych do stacji roboczej.

64

Podgląd na żywo z 64 kanałów (na jednej karcie podglądu) – tworzenie własnych podziałów, zadań i sekwencji z automatycznym wywoływaniem po zalogowaniu się do aplikacji.

36

Odtwarzanie kanałów z rejestratorów podłączonych do aplikacji max. do 36 kamer jednocześnie.

∞

Zarządzanie użytkownikami – nielimitowana ilość kont użytkowników z możliwością określenia dostępu do kanałów, interfejsu, zadań, eksportu danych innych czynności.

Tworzenie i obsługa eMAP i integracją alarmów z urządzeń.

Obsługa kamer specjalnych – sterowanie kamerami PTZ, FishEye (dewarping na stacji roboczej w podglądzie na żywo i odtwarzaniu), obsługa dwukierunkowego audio.

Integracje z zewnętrznymi systemami

- Systemy sygnalizacji pożarowej
- Systemy sygnalizacji włamania i napadu

Sprawdzanie trasy przesyłek, śledzenie zamówień

POLSKA MARKA BCS

www.bcs.pl

www.facebook.com/bcspl