CZASOPISMO RYNKU SECURITY

a&S POLSKA

50. WYDANIE „a&s Polska”

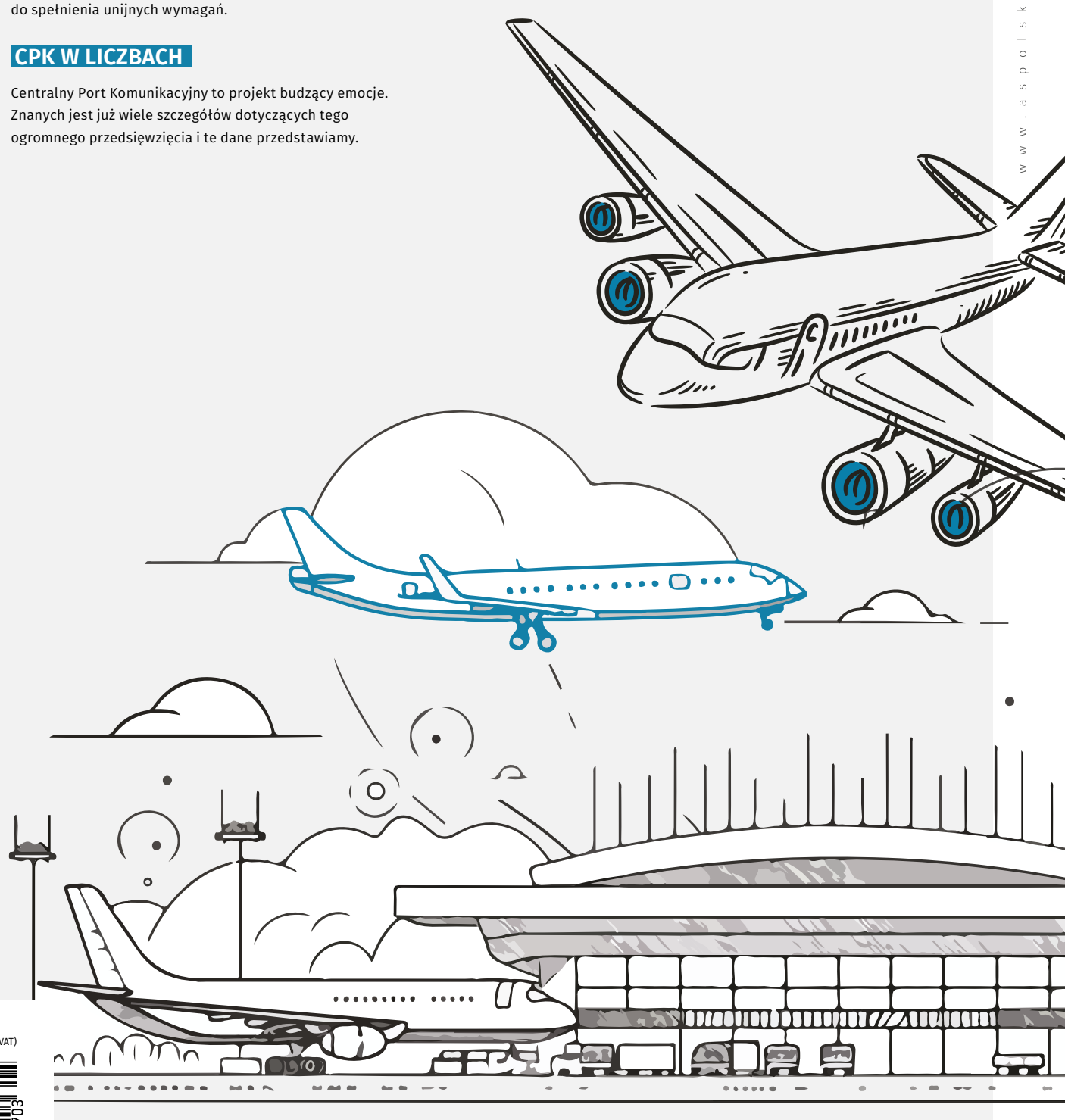
Zaczynaliśmy osiem lat temu w zupełnie innej rzeczywistości. To dobry moment, aby zerknąć wstecz i przekonać się, jak zmienił się rynek zabezpieczeń technicznych.

WDROŻENIE NIS2 I CER CO JUŻ WIADOMO?

Przedsiębiorstwa, które będą podlegały pod nowe regulacje, powinny niezwłocznie zacząć przygotowania do spełnienia unijnych wymagań.

CPK W LICZBACH

Centralny Port Komunikacyjny to projekt budzący emocje. Znanych jest już wiele szczegółów dotyczących tego ogromnego przedsięwzięcia i te dane przedstawiamy.



www.aspolska.pl

20 zł
(w tym 8% VAT)

ISSN 2451-5175 05
9 772451 517703

blue**Evo**

Ewolucja inspirowana tradycją

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

Pełna kontrola,
prostota i bezpieczeństwo
w nowoczesnym wydaniu.

blueEvo.com

WINKHAUS

Dyrektywa NIS-2

Dowiedz się więcej o znaczeniu dyrektywy NIS-2 dla kontroli dostępu w przedsiębiorstwach i instytucjach publicznych.

Dawno, dawno temu, a dokładnie...

...w 2017 roku, czyli raptem przed ośmiu laty, w artykule *Coś się zmieniło, czyli o... zaletach życia w ciekawych czasach* pisaliśmy: „Wydaje się, że dotychczasowy porządek międzynarodowy kruszeje, jakby tracił swoją spoistość i spójność. Gdy dodać do tego niestabilność gospodarczą i demograficzną, migracje i niestabilność energetyczną, to uzyskujemy obraz sytuacji, w której musimy poradzić sobie z nowymi zagrożeniami przy użyciu starych narzędzi".

Dziś już wiemy, że te „ciekawe czasy" nie są przejściowym zaburzeniem, chwilową nieprzyjemnością, lecz rzeczywistością, która być może zostanie z nami na dłużej (czego ani sobie, ani Czytelnikom nie życzymy). Państwa demokratyczne zmagają się z presją systemów autorytarnych, dezinformacja zatruwa debatę publiczną, a wojna – ta realna, tuż obok nas – przypomniała, że bezpieczeństwo to nie teoria. Jeśli chcemy je zachować, musimy zadbać o konkret. Ochronić linię energetyczną, most, lotnisko, stację uzdatniania wody, szpital i urząd skarbowy. Nigdy bowiem nie wiadomo, czy nie stanie się coś, co utopi naszą utopię w potopie (jak w *Hydropiekłowstąpieniu* Lao Che). A jak piszemy w bieżącym numerze, *Bezpieczeństwo wymaga czujności* (str. 28).

Infrastruktura krytyczna stała się dziś nie tylko celem ataków, ale także testem sprawności państwa. Czy potrafimy przewidzieć, które elementy naszej codzienności mogą być sparaliżowane jednym ruchem? Czy potrafimy chronić to, bez czego nie da się zapewnić obywatelom ani bezpieczeństwa, ani elementarnej stabilności?

W 50. numerze „a&s Polska" przyglądamy się temu, jak nasz kraj radzi sobie z tym wyzwaniem. Czy budujemy odporność systemowo, czy tylko reagujemy po fakcie? Czy tworzymy prawo, które zabezpiecza, czy raczej mnożymy przepisy, które uspokajają sumienie? (Więcej w artykule *Wdrożenie dyrektyw NIS2 i CER w Polsce – daleko jeszcze?*, str. 22). Czy wielkie projekty infrastrukturalne faktycznie mogą być odpowiedzią na ewentualne geopolityczne perturbacje? Czy mamy plan nie tylko na rozwój, ale i na ochronę tego, co rozwinięte? I ile może nas to kosztować? W artykule *Centralny Port Komunikacyjny – wszystko, co chcielibyście wiedzieć, ale boicie się o to zapytać* (str. 16) sięgamy zatem po konkretne liczby, które, jak wiadomo, nie kłamią.

Pięćdziesiąty numer naszego dwumiesięcznika to dobra okazja, by przypomnieć, że bezpieczeństwo publiczne nie jest ideologicznym konstruktem, ale fundamentem realnej wolności. Dziś nie wystarczy mówić o zagrożeniach – trzeba budować państwo, które je rozumie, które nie zapomina o sprawności i odpowiedzialności, które potrafi połączyć strategię z praktyką. To również dobra okazja, by podziękować Wam, Szanowni Czytelnicy, za to, że z nami jesteście. •

Redakcja

CZASOPISMO RYNKU SECURITY

a&S POLSKA

02 (50) / 2025

Spis treści

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

BCS®

dla profesjonalistów

tworzyMY

FLEX

BCS Flex to zupełnie nowe rozwiązanie w portfolio marki BCS

BCS-F-NVR7004 • BCS-F-NVR3504

intel inside · ONVIF · P2P Praca w chmurze · 4K HDMI · Max. 24TB

• Autorskie oprogramowanie tworzone przez markę BCS • System operacyjny Linux • Procesory intel i5 / i7
• Obsługa 35 / 70 kanałów • Brak ograniczenia dla rozdzielczości kamer • Bitrate ograniczony interfejsem sieciowym
• Możliwość instalacji do 4 dysków o pojemności 20TB każdy • Funkcje: eMapa, POS, analizy obrazu z kamer
• Synchroniczne szybkie odtwarzanie (4× 128) • Odtwarzanie w podglądzie

POLSKA MARKA BCS

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

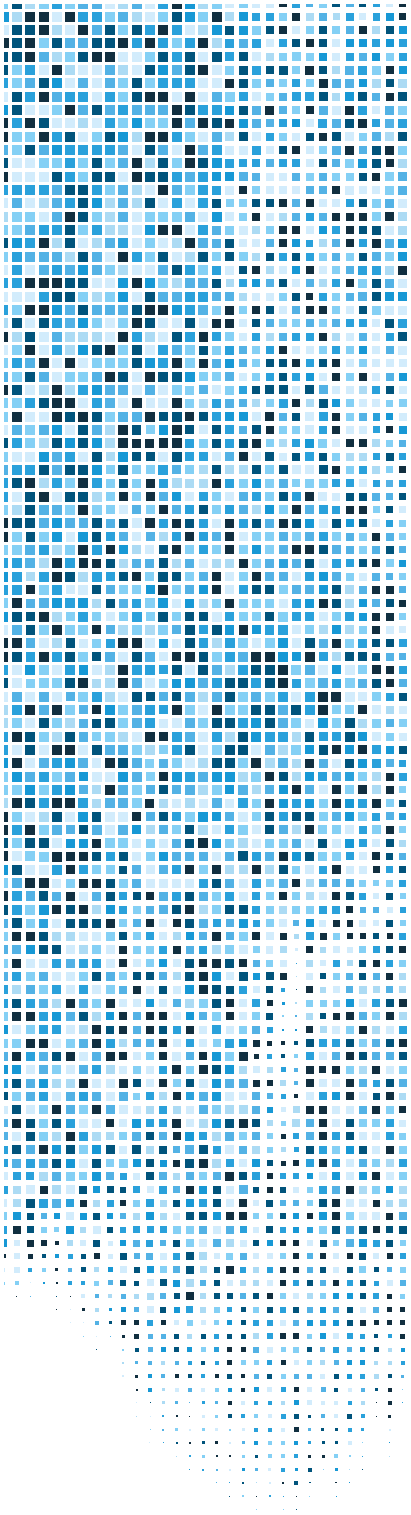
tworzyMY
rejestratory
dostosowane
do potrzeb klienta

IN EU MANUFACTURED

CZASOPISMO RYNKU SECURITY

a&S POLSKA

02 (50) / 2025



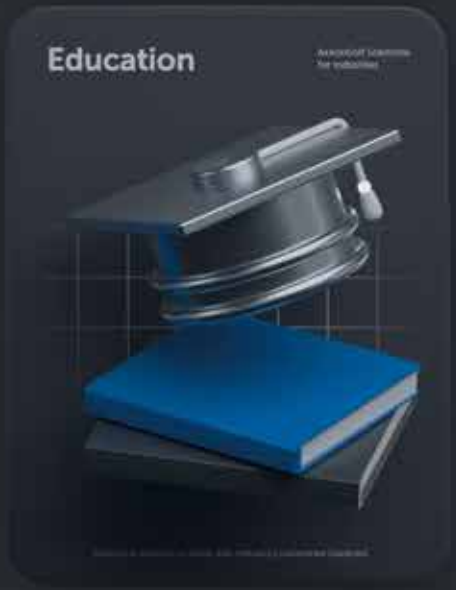
Spis treści

Drive Your Business & Maximize Security

with AxxonSoft Tailored Solutions

axxon ONE

ALL-in-ONE SOLUTIONS



A world's leading developer of intelligent VMS and PSIM software

axxonsoft.com

axxonSOFT

BCS

Stacja monitorowania BCS-F-STATION

Nowy produkt firmy BCS jest rozwiązaniem typu CMS *(Central Monitoring Station)*. Służy do budowy kompleksowego systemu zabezpieczeń obiektów i zarządzania nim.

Stacja BCS-F-STATION umożliwia nadzór nad rozległym obszarem lub wieloma obiektami znajdującymi się w różnych lokalizacjach z jednego, centralnego stanowiska. Zebranie w jednym miejscu spływających w czasie rzeczywistym alarmów z kamer, rejestratorów, systemów alarmowych i systemów sygnalizacji pożarowej pozwala na szybkie reagowanie na pojawiające się zagrożenia. Prowadzi to do zwiększenia bezpieczeństwa i zminimalizowania kosztów ochrony.

Stacja współpracuje ze wszystkimi rejestratorami z oferty BCS, a także opcjonalnie z rejestratorami innych producentów. Można do niej podłączyć dowolne kamery IP firmy BCS oraz kamery z protokołem ONVIF innych marek.

W trybie podglądu każdy z maks. czterech monitorów może wyświetlać obraz z 64 kamer. Przeglądanie zapisu z rejestratorów jest wygodne i intuicyjne, a obraz odtwarzany jednocześnie z wielu kamer może być zsynchronizowany. Moduł e-mapy pozwala na lokalizację miejsca wystąpienia alarmu i ocenę zagrożenia dzięki podglądowi obrazu z najbliższych kamer.

Podczas wirtualnych obchodów operator cyklicznie sprawdza stan obiektu przez analizę obrazu z wybranych kamer i udzielenie odpowiedzi na pytania kontrolne.

Stacja BCS-F-STATION pracuje na systemie operacyjnym Linux, korzysta z autorskiego oprogramowania firmy BCS i – jak wszystkie produkty z linii FLEX – jest zgodna z wymaganiami NDAA (*National Defense Authorization Act*). •

Więcej na: www.bcs.pl

EVVA

EMZY EVVA – rozwiązanie dla infrastruktury krytycznej

Chcesz mieć pewność, że drzwi w obrębie infrastruktury krytycznej (zewnętrzne i wewnętrzne) będą automatycznie zamykane i otwierane? Umożliwia to zaawansowana wkładka motoryczna EMZY EVVA, która zapewnia niezawodność i pełną kontrolę nad bezpieczeństwem obiektu.

W przypadku obiektów IK kluczowe jest zastosowanie systemów, które automatycznie blokują lub odblokowują drzwi prowadzące do stref o wysokim ryzyku. Elektroniczna wkładka motoryczna EMZY oferuje szereg funkcji, takich jak możliwość zdalnego otwierania, elastyczność w zakresie adaptacji momentu obrotowego oraz integracji z innymi systemami zabezpieczeń.

EMZY współpracuje z różnymi typami zamków drzwiowych, nie wymagając dużej ingerencji w istniejącą infrastrukturę drzwiową. To rozwiązanie wykorzystuje dokładnie tyle siły, ile potrzeba, aby zminimalizować ryzyko uszkodzeń zamka czy drzwi, a jednocześnie zapewnia wystarczającą „moc" do obsługi nawet ciężkich i wysokich drzwi (adaptacyjny moment obrotowy do 2 Nm). Podczas pierwszego uruchomienia system automatycznie dostosowuje się do charakterystyki zamka i drzwi, co pozwala na optymalne działanie w różnych warunkach.

Dzięki EMZY możliwe jest pełne monitorowanie statusu drzwi oraz zdalne sterowanie ich funkcjami. Wkładka motoryczna może być zintegrowana z innymi systemami, np. ppoż., alarmowymi, a także ewakuacyjnymi i sterowania technicznego budynku. EMZY EVVA stanowi idealne rozwiązanie dla zapewnienia wysokiego poziomu bezpieczeństwa w obiektach wymagających stałej kontroli dostępu. •

Więcej na: www.evva.pl

HIKVISION

Hikvision Mobile Access – nowoczesna kontrola dostępu

Hikvision Mobile Access to innowacyjne rozwiązanie, które zapewnia bezpieczny, elastyczny i wygodny dostęp do nieruchomości dzięki dynamicznym kodom QR i tymczasowym kodom PIN. Jest to idealne rozwiązanie dla krótkoterminowego wynajmu, hoteli czy biur.

Dynamiczne kody QR zmieniają się automatycznie zgodnie z ustalonym harmonogramem lub manualnie przez użytkownika, ograniczając ryzyko dostępu przez osoby nieuprawnione. Można również ustawić okres ważności każdego kodu, co zapewnia dostęp tylko w wyznaczonym czasie. System pozwala także na określenie liczby użyć kodu – po ich przekroczeniu dostęp zostaje automatycznie zablokowany.

W jednym systemie zintegrowano funkcje kontroli dostępu oraz domofonu, co ułatwia zarządzanie nieruchomością. W przypadku problemu z uzyskaniem dostępu do nieruchomości użytkownik może jednym przyciskiem zadzwonić z terminala na stację wewnętrzną, do centrum zarządzania lub aplikację HikConnect zainstalowaną na telefonie administratora nieruchomości. Administrator po weryfikacji gościa może zdalnie otworzyć drzwi. Zarządzanie dostępem jest wyjątkowo proste dzięki intuicyjnej konfiguracji zarówno online, jak i lokalnie w trybie AP. Wbudowana kamera 2 Mpix z szerokim kątem widzenia gwarantuje wyraźny obraz, a obsługa kodeków H.264 i H.265 zapewnia wysoką jakość przesyłanego obrazu, przy niewielkiej zajętości pasma.

System umożliwia zdalną konserwację i aktualizację oprogramowania, dzięki czemu instalatorzy mogą monitorować urządzenia i przeprowadzać ich konfigurację bez konieczności wizyty na miejscu. •

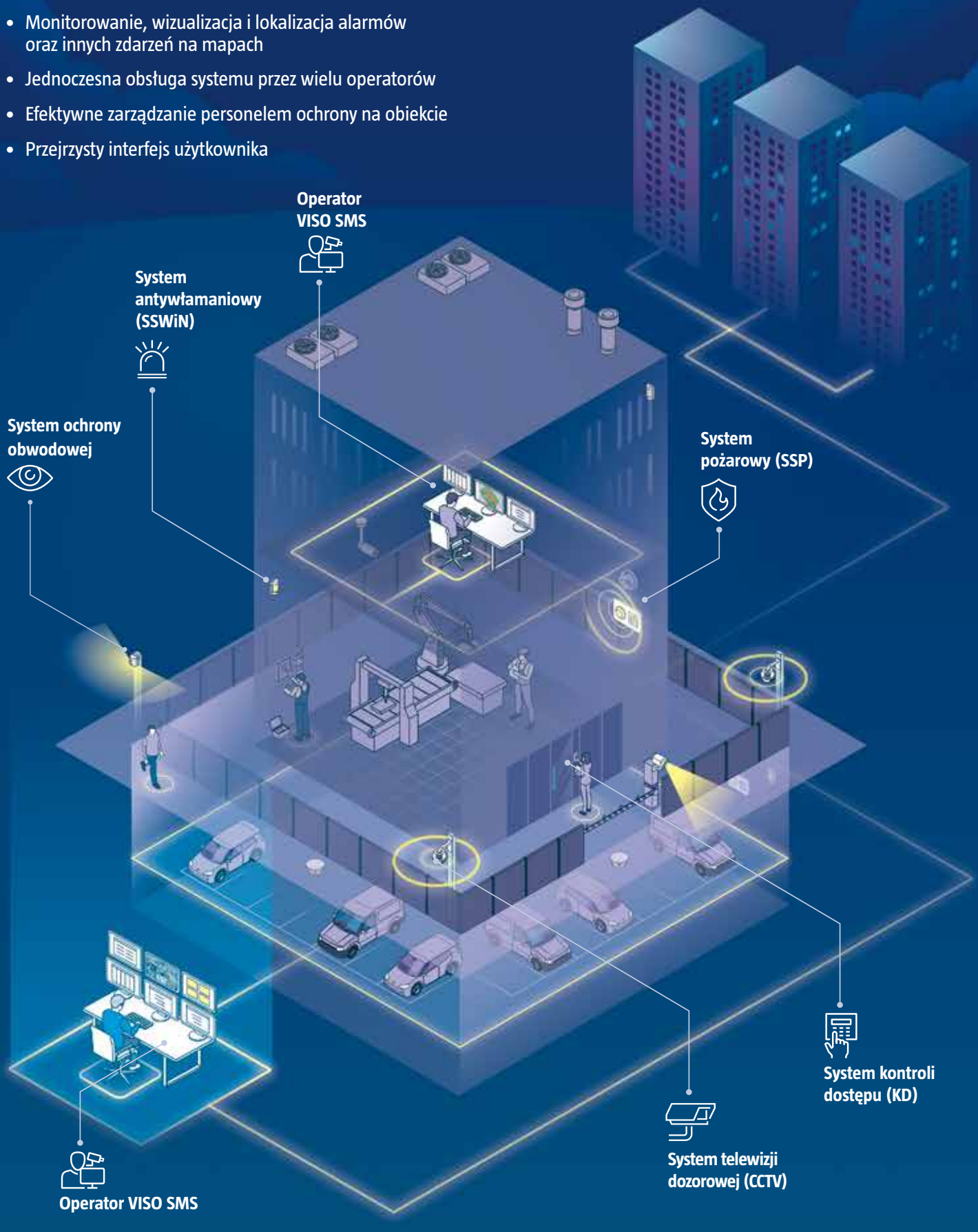
Więcej na: www.hikvision.com/pl/

VISO SMS

Monitorowanie i wizualizacja systemów bezpieczeństwa

roger
Intelligence for Building

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



LINC POLSKA

Radary Echodyne jako element systemu antydronowego

Dron to urządzenie, które daje ogromne możliwości zastosowania w różnych sektorach. Wraz ze wzrostem ich popularności rosną również zagrożenia związane z niewłaściwym ich wykorzystaniem. Aby móc przeciwstawić się takim zagrożeniom, trzeba je w pierwszej kolejności zidentyfikować, a w tym zadaniu najlepiej sprawdzają się radary.

Rozwiązania radarowe Echodyne potrafią wykrywać drony już od kilkuset metrów w przypadku EchoGuard, do nawet kilku kilometrów w modelach EchoShield. Co ważne, radary „widzą" nie tylko to, co dzieje się z przodu, ale też u góry. Mając do dyspozycji 90° kąt pokrycia w pionie, wykrywają obiekty lecące bardzo wysoko, bezpośrednio nad obiektem.

Cechą unikalną radarów Echodyne jest to, że potrafią skutecznie rozróżniać bezzałogowe statki powietrzne UAV od innych obiektów, takich jak ptaki czy ludzie. Ponadto najnowsza wersja oprogramowania EchoShield wprowadza szereg zmian w rozróżnianiu obiektów. Oprócz samego rozpoznania dronów radary wyróżnia podział na modele wielowirnikowe i „latające skrzydło". Umożliwiają również rozróżnianie ludzi, pojazdów czy samolotów, co znacząco poprawia świadomość sytuacyjną i eliminuje niepożądane alarmy, np. detekcje ptactwa.

Dzięki temu, że radar jest definiowany programowo, możliwe jest jego ciągłe udoskonalanie i wprowadzanie nowych funkcjonalności. Możliwości, jakie oferuje sztuczna inteligencja, sprawiają, że radar może być dynamicznie modyfikowany pod najnowsze zagrożenia i scenariusze działań. •

Więcej na: www.linc.pl

TP-LINK

TP-Link Omada Cloud Essentials – bezpłatna wersja kontrolera Omada w chmurze

TP-Link wprowadza Omada Cloud Essentials, bezpłatne i intuicyjne rozwiązanie, które rewolucjonizuje sposób zarządzania sieciami. Dzięki prostocie i funkcjonalności platforma pozwala użytkownikom domowym, małym firmom i administratorom sieci monitoringu cieszyć się scentralizowanym zarządzaniem bez dodatkowych kosztów i skomplikowanej infrastruktury.

Omada Cloud Essentials jest wygodną alternatywą dla sprzętowego i programowego kontrolera Omada. Rozwiązanie jest całkowicie darmowe i w pełni oparte na chmurze. Ponadto pozwala na obsługę dowolnej liczby urządzeń w sieci.

Dzięki funkcji Zero-Touch Provisioning i adopcji urządzeń poprzez skanowanie numerów seryjnych konfiguracja i wdrażanie nowych urządzeń stają się dziecinnie proste – cały proces można przeprowadzić bez konieczności wysyłania technika na miejsce. Administrator może skonfigurować urządzenia bez rozpakowywania sprzętu, a następnie wysłać je do siedziby klienta. Jest to niezwykle wygodne dla mniejszych przedsiębiorstw, ponieważ nie generuje dodatkowych kosztów.

Omada Cloud Essentials, hostowane na serwerach Amazon Web Services (AWS), zapewnia wysoką dostępność, niezawodność i bezpieczeństwo danych. Obsługuje szeroką gamę produktów TP-Link, takich jak bramy sieciowe, punkty dostępowe i przełączniki. Możliwość rozbudowy sieci i przejścia na bardziej zaawansowaną wersję Omada Cloud Standard bez wymiany sprzętu czyni to rozwiązanie wyjątkowo elastycznym, zapewniającym pełne wsparcie zarówno dla małych firm, jak i większych przedsiębiorstw. •

Więcej na: www.tp-link.com/pl/

VIVOTEK

Nowa seria kamer 4K od VIVOTEK

VIVOTEK IB9399-EHTV to jedna z pięciu kamer nowej serii 99, która wyróżnia się nowoczesnymi funkcjami i wysoką jakością obrazu. Dzięki rozdzielczości 4K oraz takim technologiom, jak RealSight Engine czy Deep Learning AI, IB9399-EHTV jest idealnym wyborem do monitorowania lotnisk, centrów handlowych czy przestrzeni publicznych.

Dzięki zastosowaniu sztucznej inteligencji RealSight Engine pozwala uzyskać wyraźny, pozbawiony rozmyć obraz zarówno w dzień,

odwzorowując rzeczywiste kolory monitorowanej sceny, jak i w nocy.

W serii 99 znajduje się również stałogniskowa kamera typu bullet oraz trzy kamery kopułowe, w tym jedna wewnętrzna ze złączem HDMI. Te modele oferują podobną jakość obrazu oraz szerokie możliwości instalacyjne, co czyni je doskonałym rozwiązaniem do monitorowania zewnętrznego. Kamery serii 99 rozpoznają takie obiekty, jak ludzie oraz pojazdy cztero- i dwukołowe, umożliwiając zapisywanie informacji w formie metadanych w celu późniejszego wyszukania zdarzeń. Urządzenia wyposażone w Smart Motion Detection są dostarczane z licencją Smart VCA umożliwiającą m.in. wykrywanie tłumów, wałęsania, intruza, przekroczenia linii. Ich funkcjonalność można też rozszerzyć o wykrywanie biegu czy zaparkowanego pojazdu.

Za bezpieczeństwo danych odpowiedzialny jest układ TPM 2.0, który zapewnia szyfrowanie sprzętowe w celu ochrony danych poufnych i zapobieganiu nieautoryzowanemu dostępowi. Gwarantuje także integralność systemu w celu zapewnienia długoterminowego bezpieczeństwa. •

Więcej na: www.vivotek.com

ALNET SYSTEMS

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

www.alnetsystems.com

50 wydań temu

Ilustracje: freepik

Od lat dostarczamy ekspertom branży security najważniejsze informacje, przedstawiamy analizy i omawiamy trendy, opisując rozwój innowacyjnych technik i strategii bezpieczeństwa. Każdy z 50 numerów „a&s Polska” to efekt pracy fachowców, którzy dbają o to, by merytoryczne artykuły o najwyższej jakości podane były w atrakcyjnej formie. Jest to zatem dobry moment, aby zerknąć wstecz i przekonać się, jak zmienił się rynek zabezpieczeń technicznych.

Jan T. Grusznic

Pięćdziesiąt wydań temu, czyli przed ośmiu laty, branża elektronicznych systemów zabezpieczeń wyglądała zupełnie inaczej. Niby to tylko osiem lat, ale... zmiany są znaczące. Otóż w 2017 r. rynek był zdominowany przez dalekowschodnich producentów, takich jak Hikvision i Dahua, którzy swoją strategią marketingową i niskimi cenami skutecznie wyparli inne marki. Według niektórych analiz w tamtym czasie aż 80% całej sprzedaży należało do tych dwóch firm. Dziś, po latach dominacji, oferta rynkowa ponownie stała się bardziej różnorodna, jeśli chodzi o dostawców, choć odnotowaliśmy pewne konsolidacyjne działania (o czym można przeczytać w artykule ***Branżowe fuzje i przejęcia. Co oznaczają dla rynku security?*** z pierwszego numeru w roku 2025). Wiadomo, duży może więcej.

Trening czyni mistrza, czyli o edukacji klientów

Jednym z kluczowych czynników wpływających na zmianę rynku był fakt, że klienci końcowi przez tych osiem lat stali się bardziej świadomi różnych zagrożeń. W dużej mierze to efekt takich wydarzeń, jak choćby organizowane przez naszą redakcję tzw. security bootcampy (**relację z pierwszej edycji Security Bootcamp znaleźć można w nr. 4/2019**). Ich uczestnicy zawsze mieli i mają okazję spotkać się z praktyką w najlepszym mistrzowskim wydaniu. O popularności tej formy szkoleniowej niech świadczą fakty, że po pierwsze, nasze bootcampy mają wielu naśladowców, a po drugie, organizowane są teraz dwa razy do roku – a mogłyby być i częściej, bo chętnych nie brak.

Żegnajcie targi, witajcie webinary

Osiem lat temu największym wydarzeniem branżowym były targi Securex. Setki wystawców i tysiące odwiedzających szczelnie wypełniały cztery hale wystawowe. Pandemia zdecydowanie zmieniła oblicze całej branży wystawienniczej, choć już wcześniej dało się zauważyć, że klasyczne targi przeżywają pewien kryzys tożsamości. Pandemia po prostu przyspieszyła ten trend, zmieniając sposób organizacji i uczestnictwa w wydarzeniach. W kalendarzach wielu specjalistów na dobre zagościły webinary, które teraz stanowią jedną z bardziej popularnych metod edukacji, oraz podcasty prowadzone przez branżowych specjalistów. Tym bardziej cieszy, że nie maleje zainteresowanie Warsaw Security Summit (**zobacz relację z pierwszego WSS w nr. 4/2017 – Warsaw Security Summit – DUŻY SUKCES!**). To wydarzenie zorganizowane po raz pierwszy w 2017 r. na zawsze odmieniło sposób organizacji branżowych eventów.

Kabel, kabel i po kablu. Czas na IP

Pięćdziesiąt wydań temu duże zainteresowanie budziły technologie przesyłania obrazu o wysokiej rozdzielczości za pomocą kabli koncentrycznych, takich jak AHD, Turbo-HD, HD-CVI i HD-TVI. Mimo że przesyłanie przez IP było już dobrze znane, to wielu instalatorów nadal preferowało stare, sprawdzone rozwiązania (czyli kabel), choć w nowej odsłonie (w pierwszym numerze z roku 2017 twierdziliśmy, że ***Zmiana kursu receptą na przetrwanie***). To zrozumiałe, lubimy to, co znamy. Ostatecznie kable, w tych przypadkach, w których tylko można to było zrobić, zostały zastąpione przez IP. Branża nie przespała tej zmiany, co widać po kolejnych nowościach produktowych, o których piszemy.

Co ja widzę?

Osiem lat temu analiza obrazu w systemach monitoringu wizyjnego była nadal w powijakach. Bazując na uczeniu maszynowym, zaczynała co prawda odgrywać coraz większą rolę, jednak jej ograniczenia były zauważalne, a liczba fałszywych alarmów poddawała w wątpliwość sens jej stosowania. Dopiero wprowadzenie algorytmów sztucznej inteligencji pozwoliło na przełom w skuteczności analizy wideo. W tamtym czasie nikt nie wyobrażał sobie, że kamery staną się podstawowym narzędziem ochrony obszarów zewnętrznych. A teraz, 50 numerów „a&s Polska" później? Sprzedaż tradycyjnych czujek zewnętrznych dramatycznie

spadła, a kamery z inteligentną analityką stały się standardem w ochronie perymetrycznej.

Integracja systemów, czyli luksus dla każdego

Pięćdziesiąt wydań temu integracja była luksusem dostępnym tylko dla największych graczy. Systemy bazowały na zamkniętych protokołach, a dostęp do API i SDK był ograniczony. Dziś, patrząc na rynek, trudno nawet wyobrazić sobie wdrożenie jakiegoś rozwiązania bez możliwości jego integracji z innymi funkcjonującymi w firmie rozwiązaniami, za pomocą otwartych protokołów jak MQTT czy http (pisaliśmy o tym w artykule ***Dynamiczny rozwój wielkie wyzwania***, 6/2017). Nowe pokolenie instalatorów wręcz żąda od dostawców intuicyjnych aplikacji i interfejsów użytkownika, a systemy zabezpieczeń coraz częściej łączą się z urządzeniami IoT, automatyką budynkową, a nawet sprzętem AGD. Integracja przestała być luksusem, a stała się oczywistością.

Gdzie ci mężczyźni?

Dynamiczny wzrost płacy minimalnej w ostatnich latach miał ogromny wpływ na branżę ochrony, co pośrednio odbiło się także na rynku elektronicznych systemów zabezpieczeń. Wzrost kosztów pracy spowodował, że wielu klientów zaczęło poszukiwać alternatyw w postaci automatyzacji pracy pracowników ochrony. Skutek? Profesjonalne firmy ochrony, zamiast zwiększać liczbę pracowników, inwestują w zaawansowane systemy monitoringu, analizę obrazu i sztuczną inteligencję, aby zoptymalizować koszty operacyjne. Trend ten zmienia model funkcjonowania całej branży, przyspieszając rozwój technologii zastępujących tradycyjne formy ochrony fizycznej.

Wespół zespół, czyli ochrona pod rękę z IT

Osiem lat temu, kiedy startował magazyn „a&s Polska", firmowe działy IT, zajmujące się przecież także bezpieczeństwem, a dokładnie jego cyfrową wersją, nie za bardzo współpracowały z ludźmi odpowiedzialnymi za fizyczną ochronę obiektów. Każdy miał swoją działkę i o nią dbał. Ta sytuacja diametralnie się zmieniła – nowe zagrożenia, regulacje (np. NIS2 i CER) oraz rosnąca świadomość cyberzagrożeń sprawiły, że departamenty bezpieczeństwa w instytucjach publicznych i korporacjach zaczęły traktować systemy zabezpieczeń na równi z IT (***Wskazówki dla integratorów systemów, by rozwijali się wraz z branżą*** opublikowaliśmy w numerze drugim z 2017 r.). Niestety, rosnącej świadomości cyfrowych zagrożeń towarzyszą od lat te same błędy – używanie tych samych haseł, brak aktualizacji oprogramowania czy lekceważenie podstawowych zasad cyberhigieny. Upływ czasu w tym przypadku niczego nie zmienił.

Dajcie mi branżę, a przepis się znajdzie

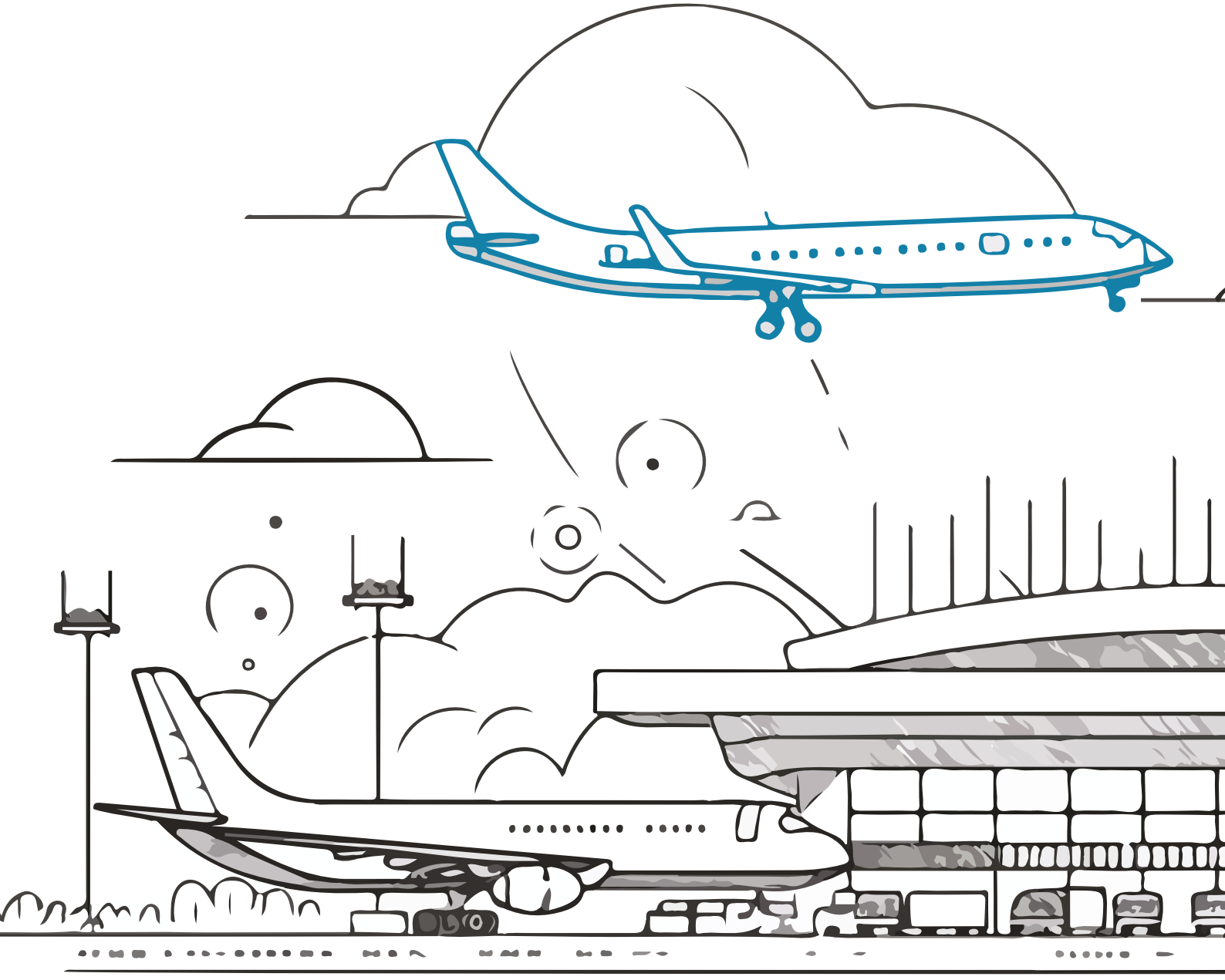
Pięćdziesiąt wydań temu sen z powiek wielu osobom spędzało wprowadzenie przepisów RODO. Co to są dane wrażliwe? Kto je może przechowywać i jak długo? Legitymować wszystkich czy tylko tych, którzy się zgodzą? Co może zawierać przepustka, a czego absolutnie nie wolno umieścić na drzwiach gabinetu? Pytań było wówczas więcej niż osób i instytucji, które mogłyby na nie odpowiedzieć. Jednym z największych wyzwań było z góry skazane na niepowodzenie dostosowanie systemów dozoru wizyjnego do art. 17 (prawa do bycia zapomnianym). Dziś podobną rewolucję przynoszą dyrektywy NIS2 i CER, które redefiniują podejście do bezpieczeństwa w sektorze zabezpieczeń elektronicznych. O czym przy okazji piszemy na stronie 22, bo „a&s Polska" zawsze trzyma rękę na pulsie.

Patrząc wstecz, zmiany w branży zabezpieczeń na przestrzeni ostatnich 50 wydań „a&s Polska" są ogromne. Minęło wprawdzie tylko osiem lat, ale świat i rynek branży security zmieniły się w tym czasie znacząco. Jedni gracze zeszli ze sceny, inni troszkę się na niej posunęli, na dobre upowszechnił się protokół IP, sztuczna inteligencja i uczenie maszynowe. Wystarczyło tylko osiem lat, a rynek przeszedł gruntowną transformację – z pewnością duży wpływ miała pandemia. Jedno pozostaje niezmienne – branża zabezpieczeń to dynamiczny ekosystem, który nieustannie ewoluuje, dostosowując się do nowych wyzwań i technologii. „a&s Polska" jest czujnym tych zmian kronikarzem. •

Jan T. Grusznic
redaktor „a&s Polska"

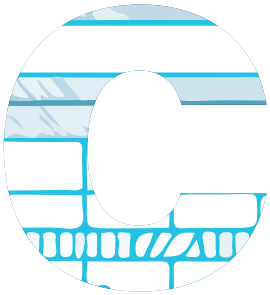
Centralny Port Komunikacyjny

wszystko, co chcielibyście wiedzieć, ale boicie się zapytać



To nie będzie tekst o tym, na ile budowa nowego portu lotniczego w Polsce jest w ogóle zasadna, ani o tym, która frakcja polityczna podjęła w tej sprawie słuszne decyzje. Nie odnosimy się w nim do tego, czy wybrana lokalizacja jest najbardziej korzystna, a przygotowanie terenu pod budowę odbywa się zgodnie z zasadami sprawiedliwości społecznej. Zostały podjęte kluczowe decyzje i port powstanie. Znanych jest już wiele szczegółów dotyczących tego ogromnego przedsięwzięcia i te dane przedstawiamy.

Adela Prochyra



CPK w liczbach

LOKALIZACJA, POWIERZCHNIA

Wieś Stanisławów, gmina Baranowice, powiat grodziski, województwo mazowieckie – to tam w ciągu siedmiu najbliższych lat powstanie gigantyczny intermodalny węzeł transportowy, łączący lotnisko o charakterze huba – Port Lotniczy Solidarność – i podziemny węzeł kolejowy, do którego ma być poprowadzony dogodny i szybki dojazd drogowy z największych polskich miast. Port będzie oddalony 37 km od Warszawy i 78 km od Łodzi. Z głównymi miastami w kraju połączy go sieć Kolei Dużych Prędkości, dzięki której czas przejazdu między Warszawą a największymi miastami w Polsce wyniesie do 2,5 godz.

Kompleks zajmie ok. 30 km^2, a oprócz lotniska i węzła kolejowego całe aerotropolis – obszar bezpośredniego otoczenia CPK – będzie się składać także z:

- **systemu dróg publicznych** – inwestycja obejmuje budowę i modernizację infrastruktury drogowej w celu zapewnienia efektywnego transportu do i z CPK;
- **Cargo City** – specjalnej strefy przeznaczonej na obsługę transportu towarowego, magazynowanie i logistykę;
- **Airport City** – tereny przeznaczone pod działalność związaną z przemysłem lotniczym, parki biurowe, przestrzenie wystawiennicze, centra badawcze oraz ośrodki innowacji do użytku zarówno komercyjnego, jak i publicznego;
- **inwestycji towarzyszących,** takich jak:
  - sieć przesyłowa i dystrybucyjna energii elektrycznej,
  - system kanalizacyjny,
  - urządzenia i obiekty do obsługi ruchu lotniczego.

Całość projektu ma być zgodna z europejskimi planami rozwoju transportu intermodalnego oraz celami klimatycznymi Unii Europejskiej.

Przepustowość

Planowana przepustowość lotniska „Solidarność" to ponad 32 mln pasażerów rocznie w pierwszym etapie. „Projekt terminala w perspektywie długoterminowej pozwoli na jego elastyczną rozbudowę zgodnie z bieżącymi potrzebami i prognozami rozwoju rynku", napisano na stronie cpk.pl (dostęp: 6.03.2025), aż do 60 mln, jak podaje Monitor Polski z 31 grudnia 2024 r. IATA (International Air Transport Association – Międzynarodowe Zrzeszenie Przewoźników Powietrznych) przewiduje, że w początkowej fazie działalności CPK obsłuży ok. 200 tys. ton ładunków rocznie, a wolumen będzie rósł aż do 1,5 mln ton w 2060 r.

Dla porównania: największy obecnie port lotniczy w Polsce, Lotnisko Chopina w Warszawie, w rekordowym 2024 r. przyjął 21,3 mln pasażerów. Rekordowy okazał się także tonaż odprawionego cargo w 2024 r., który wyniósł ponad 117 tys. ton (+13% r/r). Eksperci podkreślają, że zbliża się on do granicy przepustowości, a zbyt bliskie położenie dzielnic mieszkalnych i dużych tras szybkiego ruchu, limity hałasu i ograniczenia środowiskowe uniemożliwiają jego istotną rozbudowę. Portal rynek-lotniczy.pl zauważa (dostęp: 5.03.2025), że „skala ruchu transferowego na Lotnisku Chopina w ostatnich latach spadła". W roku bieżącym ma on stanowić 24% ruchu, a później 27% (lata 2027–29), aż do 29% w 2032 r. IATA prognozuje, że na PCK ma on stanowić ok. 40%. Dużego potencjału upatruje się zwłaszcza w relacjach: Europa – Azja, Europa – Ameryka Północna i Ameryka Północna – Azja. Chociaż lotnisko będzie obsługiwać wszystkie rodzaje połączeń, z naciskiem na długie dystanse, ta kategoria pasażerów jest kluczowa dla jego rentowności.

Polskie lotniska regionalne także zanotowały znakomite wyniki, obsługując w minionym roku blisko 38 mln pasażerów (co łącznie z wynikiem Chopina daje niemal 60 mln podróżnych). To wzrost o ponad 14% w porównaniu do roku 2023, a także o ponad 26% w stosunku do 2019 r. Dodajmy, że obecnie lotniska regionalne obsługują 64% ruchu lotniczego w Polsce. Dla porządku odnotujmy też, że oprócz 15 portów lotniczych obsługujących ruch pasażerski, z czego pięć obsługuje również transport cargo (patrz: *Mapa lotnisk w Polsce*), mamy w kraju także szereg lotnisk wojskowych i sportowych.

Wzrost liczby pasażerów odnotowany na polskich lotniskach w ub.r. jest zgodny z globalnymi trendami. W roku 2024 w całej Europie lotniska odnotowały wzrosty: 2,5 mld podróżnych, co oznacza „wzrost o 7,4% w porównaniu do 2023 r. i o 1,8% w stosunku do 2019 r.", jak podaje portal lotnisko-chopina.pl (dostęp: 5.03.2025). Trzeba mieć jednak na uwadze, że rynek europejski, który obecnie odpowiada aż za ¼ rynku (26% w 2023 r.), w nadchodzących dekadach obniży swój udział do 1/5. W roku 2043 ma on wygenerować już tylko 19,5% ruchu powietrznego (dane IATA „Air Passenger Market analysis", za: rynek-lotniczy.pl, dostęp: 6.03.2025). Mimo to prognozy IATA dla CKP zakładają, że m.in. ze względu na swoje centralne położenie i dobre skomunikowanie z miastami będzie to liczący się hub w regionie i 12. pod względem wielkości lotnisko w Europie.

Największy w Polsce port lotniczy, Lotnisko Chopina jest na 31. miejscu w Europie pod względem wielkości. Inne ważne lotniska z regionu CEE są jeszcze mniejsze – Port lotniczy Praga im. Václava Havla odprawia do 18 mln pasażerów rocznie, a Lotnisko im. Ferenca Liszta w Budapeszcie obsługuje do 15 mln pasażerów rocznie, a więc oba plasują się bliżej 40. miejsca.

CKP w perspektywie globalnej

Prognozy wskazują, że w najbliższych dekadach zarówno ruch pasażerski, jak i lotniczy transport cargo będą systematycznie rosnąć, choć tempo tego wzrostu może się różnić w zależności od przyjętych założeń. Rozwój lotnictwa do 2060 r. będą napędzać m.in. czynniki demograficzne (wzrost klasy średniej, szczególnie w Azji i Afryce), postęp technologiczny (nowe samoloty i paliwa), polityka regulacyjna dotycząca zrównoważonego rozwoju oraz sytuacja geopolityczno-ekonomiczna.

Według prognoz IATA światowy ruch pasażerski będzie rósł średnio o 3,6–3,8% rocznie w perspektywie najbliższych dwóch dekad. Oznacza to, że liczba obsługiwanych podróżnych może się zwiększyć ponaddwukrotnie – z ok. 4,5 mld w 2019 r. do nawet

Mapa lotnisk w Polsce

10 mld pasażerów rocznie do 2050 r. Już w 2043 roku w powietrzu ma znaleźć się ośmiomiliardowy pasażer. Zresztą, po co wybiegać tak daleko w przyszłość! W bieżącym roku IATA spodziewa się ruchu na poziomie 5,2 mld (za: rynek-lotniczy.pl, dostęp: 6.03.2025). W optymistycznym scenariuszu (szybki rozwój PKB i brak większych kryzysów gospodarczych) do 2060 r. globalna liczba pasażerów mogłaby nawet potroić się względem poziomu z 2019 r. W scenariuszu pesymistycznym – wzrost wyniesie prawdopodobnie od 1,5 raza do 2 razy.

Równolegle z ruchem pasażerskim będzie się rozwijać lotniczy transport towarów. Choć pod względem masy stanowi on poniżej 1% światowego wolumenu, odpowiada za ok. 35% wartości globalnego handlu, gdyż przewozi głównie towary wysokowartościowe i wymagające szybkiego transportu takie jak elektronika, części zamienne, dobra luksusowe, farmaceutyki. Te sektory będą się rozwijać wraz ze wzrostem zamożności społeczeństw. Prognozy długoterminowe Boeinga zakładają średni wzrost ruchu cargo rzędu 4% rocznie na głównych szlakach handlowych. Oznacza to potencjalne podwojenie światowego tonażu cargo co 18–20 lat. Do jego wzrostu przyczyni się wiele czynników: rozwój e-commerce, zintensyfikowanie handlu między Afryką a Azją Wschodnią (ten do 2050 r. ma się potroić), rozwój technologii i zastosowanie samolotów bezzałogowych czy dronów towarowych. Mówi się wręcz o tym, że w perspektywie dwóch–trzech najbliższych dekad każdy większy sklep będzie dysponował własnym dronem towarowym. Nawet w przypadku ziszczenia się negatywnych scenariuszy (m.in. koszty paliw, regulacje środowiskowe, kryzysy gospodarcze i polityczne) transport lotniczy cargo ma przed sobą perspektywę lepszego rozwoju niż loty pasażerskie.

CKP. Koszt inwestycji, harmonogram budowy

Jak czytamy w otwarciu Monitora Polskiego z 9 stycznia 2025 r.: „Okres realizacji Programu Wieloletniego ustala się na lata 2024–2032" oraz „Łączny limit zaangażowania środków Skarbu Państwa na realizację Programu Wieloletniego wynosi 62 901 000 000 zł (sześćdziesiąt dwa miliardy dziewięćset jeden milionów złotych)". Program nie obejmuje wydatków z budżetu państwa. Budowa CPK ma być finansowana także z funduszy unijnych, długów zaciągniętych w bankach oraz obligacji emitowanych przez spółkę CPK. Łączny koszt do 2032 r. ma wynieść 131,7 mld zł. 17 marca 2025 r. spółka została dokapitalizowana kwotą 1,9 mld zł. Środki te zostaną przeznaczone na realizację zadań bieżących, obejmujących przede wszystkim podprogramy związane z infrastrukturą lotniskową, kolejową, nieruchomościami, rozwojem otoczenia oraz inwestycjami rozwojowymi. W pierwszej transzy (grudzień 2024) wypłacono 3,5 mld zł. *CPK jako spółka celowa realizuje ustawowe zadania inwestycyjne, które wymagają nakładów z budżetu państwa. Bez przekazanych środków ich wykonanie nie byłoby możliwe* – skomentował Maciej Lasek, pełnomocnik rządu ds. CPK, sekretarz stanu w Ministerstwie Infrastruktury.

Etap II projektu, czyli zaplanowany na lata 2024–32, uwzględnia zakończenie budowy do 2031 r. i uruchomienie portu do końca 2032 r. Oznacza także przeniesienie ruchu z Lotniska Chopina do Baranowa. Budowa i cały koncept CPK są zaprojektowane etapowo i modułowo, co oznacza, że gdy prognozy okażą się trafne, a zapotrzebowanie na przepustowość wzrośnie, port lotniczy będzie można rozbudować, i taka możliwość jest uwzględniona w projekcie.

Port Lotniczy „Solidarność" – projekt

Pod koniec czerwca 2019 r. z inicjatywy Ambasady Zjednoczonego Królestwa Wielkiej Brytanii i Irlandii Północnej oraz spółki CPK odbyły się międzynarodowe warsztaty architektoniczne, które miały przybliżyć wizję portu w Stanisławowie. Swoje koncepcje przedstawiły zaproszone do udziału renomowane pracownie

Ilustracje: freepik

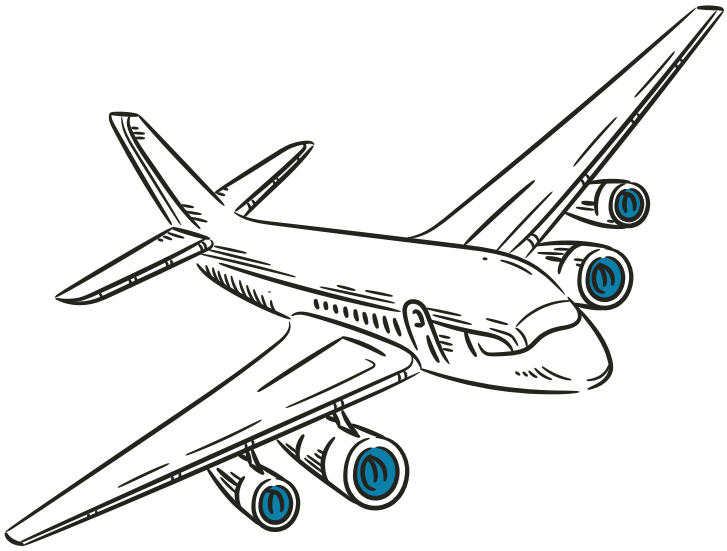
architektoniczne: Zaha Hadid Architects, Foster + Partners, Chapman Taylor, Grimshaw Architects, Benoy oraz Pascall + Watson. Ostatecznie projekt architektoniczny Centralnego Portu Komunikacyjnego został powierzony brytyjskiej pracowni Foster + Partners, znanej z realizacji nowoczesnych i funkcjonalnych obiektów na całym świecie. Współpracując z firmą Buro Happold, architekci opracowali koncepcję, której centralnym elementem jest przestronne atrium, pełniące funkcję węzła komunikacyjnego integrującego transport lotniczy, kolejowy i drogowy.

Sercem portu ma się stać atrium zwieńczone dachem przypominającym diament, gdzie pasażerowie będą mogli swobodnie przemieszczać się między różnymi środkami transportu. Dzięki zastosowaniu dużych połaci ze szkła wnętrze zostanie wypełnione naturalnym światłem, co ma stworzyć przyjazną i komfortową atmosferę. Projekt zakłada również wykorzystanie nowoczesnych technologii i rozwiązań proekologicznych, takich jak systemy oszczędzania energii czy zarządzania wodą deszczową, co wpisuje się w globalne trendy zrównoważonego rozwoju. Ponadto elastyczność konstrukcji umożliwi przyszłą rozbudowę portu w zależności od rosnących potrzeb transportowych.

Doradcą strategicznym CPK pod koniec 2020 r. został Port Lotniczy Incheon z Seulu, główne międzynarodowe lotnisko w Korei Południowej. Współpraca została nawiązana w celu zapewnienia wiedzy operacyjnej i komercyjnej niezbędnej do efektywnego zarządzania dużym lotniskiem przesiadkowym, jakim ma być CPK. Incheon International Airport to jedno z najlepiej ocenianych lotnisk na świecie, zajmujące czwarte miejsce w rankingu Skytrax pod względem jakości obsługi. Jego doświadczenie w zarządzaniu dużym portem przesiadkowym jest kluczowe dla sukcesu projektu CPK. Umowa z Portem Lotniczym Incheon została podpisana na trzy lata, a jej wartość wyniosła 3,5 mln euro. W ramach współpracy koreańscy eksperci mieli dostarczyć wiedzę i doświadczenie, których brakuje w Polsce, ponieważ tak duży projekt nie był wcześniej realizowany w naszym kraju. Dzięki tej współpracy CPK ma szansę stać się jednym z czołowych portów lotniczych na świecie, czerpiąc z najlepszych praktyk i innowacyjnych rozwiązań stosowanych na lotnisku Incheon.

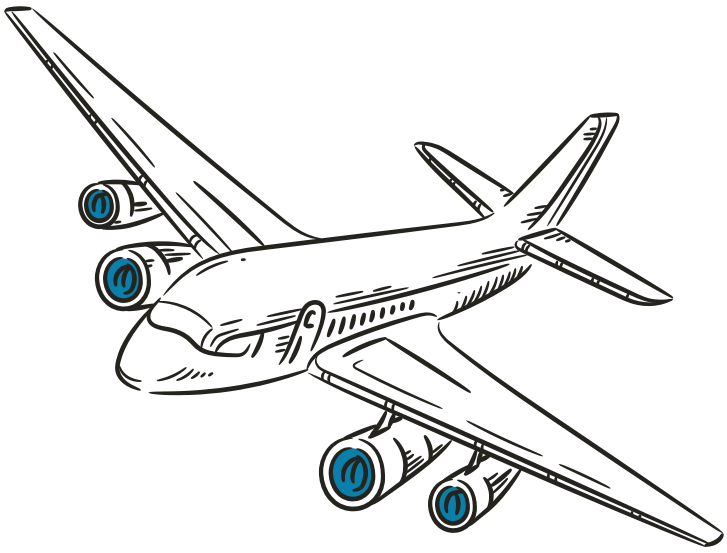
Kolej Dużych Prędkości

Równocześnie z budową lotniska CPK powstanie 140-kilometrowa linia kolejowa umożliwiająca szybkie połączenie na odcinku Warszawa – CPK – Łódź Fabryczna. Przejazd z CPK do Warszawy ma trwać ok. 15 min, a do Łodzi Fabrycznej – 25. W tym samym czasie będą prowadzone zaawansowane prace budowlane na odcinkach do Wrocławia i Poznania. Docelowo, dzięki programowi „Polska w 100 minut", czas przejazdu z Warszawy do tych miast ma wynosić ok. 100 min. Główna linia „Y" połączy Warszawę, CPK, Łódź, Wrocław i Poznań, stanowiąc szkielet nowej sieci Kolei Dużych Prędkości. Planowane są także dodatkowe odgałęzienia do Trójmiasta, Krakowa, Katowic, a skrócenie czasu przejazdu między Warszawą a miastami południa i zachodu wpłynie pozytywnie także na wzrost ruchu z Lublina, Białegostoku czy Szczecina. Sieć KDP ma liczyć łącznie ok. 2 tys. km nowych linii kolejowych, które zostaną wybudowane etapami do 2040 r. Skorzystają na niej także mniejsze miejscowości położone na trasie: Grudziądz, Sieradz czy Kalisz, w którym wzrost liczby podróżnych ma wynieść ponad 400%.



„Duże porty lotnicze są impulsem do rozwoju gospodarczego, oddziałując bezpośrednio i pośrednio na rynek regionalny i krajowy, i wpływają pozytywnie na zatrudnienie, wartość dodaną oraz wpływy budżetowe".

źródło: Monitor Polski z dnia 31.12.2024 r.



KDP ma na celu stworzenie zintegrowanego systemu transportowego, w którym będzie współdziałać z transportem lotniczym i drogowym, zapewniając płynne przesiadki i skracając czas podróży między kluczowymi miastami. Nowe linie KDP zostaną przystosowane do prędkości projektowej do 320 km/h i zelektryfikowane w systemie 25 kV prądu przemiennego. Przy tak dużych prędkościach konieczne będzie zastosowanie nowych technologii sterowania ruchem (Europejski System Sterowania Pociągiem ERTMS/ETCS). Nowoczesny będzie także tabor, w którego skład wejdą pociągi zaprojektowane zgodnie z duchem czasu: z komfortowymi wagonami, wyposażonymi w ergonomiczne fotele i z dostępnym stabilnym Internetem.

Koszt komponentu kolejowego, w tym budowy linii „Y" łączącej Warszawę, CPK, Łódź, Wrocław i Poznań, ma wynieść ponad 76,8 mld zł. Finansowanie inwestycji ma pochodzić, podobnie jak reszty projektu CPK, ze środków Skarbu Państwa, funduszy unijnych oraz źródeł zewnętrznych, takich jak dług bankowy czy emisja obligacji przez spółkę CPK.

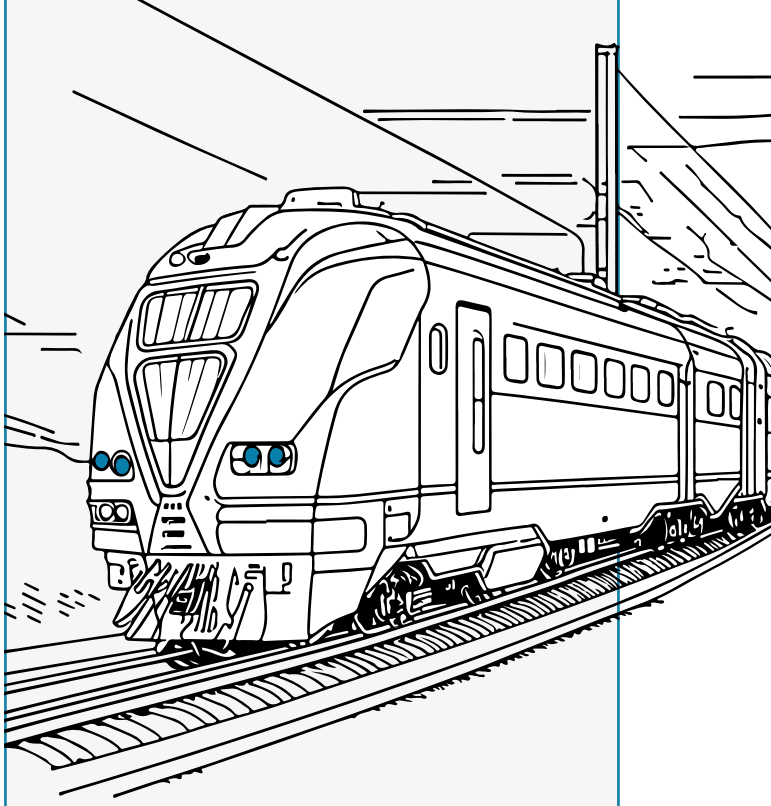
CPK jako nowoczesny hub transportowy

CPK to jedno z największych przedsięwzięć infrastrukturalnych w historii Polski. Jego celem jest nie tylko usprawnienie polskiego transportu lotniczego, ale także stworzenie nowoczesnego węzła kolejowego i logistycznego, który znacząco wpłynie na polską gospodarkę i mobilność obywateli. W założeniu projektantów CPK ten port ma być impulsem dla polskiej gospodarki w myśl zasady, że jedno miejsce pracy w sektorze lotniczym tworzy trzy nowe miejsca pracy w innych dziedzinach gospodarki. Według raportu firmy Kearney z 2020 r. w szczytowym okresie realizacji inwestycji, przypadającym na rok 2026, przewiduje się utworzenie ok. 95,2 tys. nowych miejsc pracy. W podziale na sektory inwestycje kolejowe mają wygenerować 57 tys. miejsc pracy, lotnicze – 28,4 tys., a drogowe – 9,8 tys. W latach 2020–34, dzięki inwestycjom w lotnisko i kolej, polska gospodarka zyska dodatkowe 126,6 mld zł. Największy wpływ na ten wzrost będą miały inwestycje kolejowe (61%), lotnicze (22%) i drogowe (17%).

Budowa CPK przyniesie największe korzyści branży budowlanej, która otrzyma ponad 80% środków przeznaczonych na ten projekt. Produkcja globalna w tym sektorze wzrośnie o ok. 162 mld zł, a wartość dodana brutto – o 94 mld zł. W roku 2026, szczytowym okresie budowy, w sektorze tym powstanie 72 tys. nowych miejsc pracy (źródło: cpk.pl, dostęp: 6.03.2025).

Projekt ma kluczowe znaczenie dla sektora transportu i logistyki, ale może również stanowić kamień milowy w rozwoju branży security. Nowoczesne lotnisko i hub kolejowy oznaczają nowe wyzwania w zakresie ochrony pasażerów i ładunków oraz infrastruktury krytycznej. CPK będzie punktem strategicznym pod względem zarówno ekonomicznym, jak i bezpieczeństwa narodowego. Jak podkreślał dyrektor komunikacji Konrad Majszyk w wywiadzie udzielonym aspolska.pl w 2020 r.: *Kwestie bezpieczeństwa są absolutnie kluczowe dla funkcjonowania CPK w przyszłości. Dlatego bierzemy pod uwagę szeroki wachlarz zagadnień, takich jak bezpieczeństwo pasażerów, bezpieczeństwo statków powietrznych, zabezpieczenia cyfrowe itd.* Ze względu na charakter przedsięwzięcia, *szczegóły dotyczące planów zabezpieczenia, stosowanych sił i środków, a także przewidywanych scenariuszy zagrożeń dla Centralnego Portu Komunikacyjnego z oczywistych względów nie mogą być przedmiotem publicznej dyskusji* – przekazało nam w marcu 2025 r. Biuro Prasowe CPK. Zapewniono nas jednak, że za wskazówkę przy projektowaniu systemów zabezpieczeń ma służyć doświadczenie istniejących portów lotniczych: *CPK korzysta oczywiście z doświadczeń funkcjonujących portów lotniczych, ale także stara się przewidywać nowe zagrożenia wynikające zarówno ze specyfiki CPK, jak i obecnej sytuacji geopolitycznej.*

Kiedy faktycznie powstanie i jaki kształt ostatecznie przybierze CPK? To, co możemy wyczytać w oficjalnych komunikatach i rozporządzeniach, należy traktować z pewną rezerwą. Prognozy przepustowości CPK, którymi posługiwałam się w niniejszym artykule, mają zostać powtórzone jeszcze dwukrotnie. Ich wyniki zapewne będą miały wpływ na kolejne decyzje dotyczące portu. Na kilka godzin przed oddaniem artykułu media obiegła informacja o niedostatecznym przygotowaniu Lotniska Chopina do rozbudowy, która miała rozpocząć się wiosną 2026 r. i potrwać do 2029. Ten krok jest kluczowy dla powstania CPK, ponieważ ma umożliwić rozwój Polskim Liniom Lotniczym LOT i zwiększenie funkcji huba polskiego lotniska. W związku z opóźnieniem na Okęciu może przesunąć się w czasie także oddanie Centralnego Portu Komunikacyjnego. Z początkiem tego roku pod znakiem zapytania stanęła także nazwa Portu. Pojawiły się głosy za tym, aby lotnisko na CPK nosiło imię Fryderyka Chopina. Mimo wszystkich niewiadomych... to CPK stoi przed wyjątkową szansą wybudowania huba od podstaw i szytego na miarę, zgodnie z zapotrzebowaniem i wymaganiami użytkowników. •



Przetargi związane z zabezpieczeniem i ochroną Spółki oraz jej obiektów są uruchamiane sukcesywnie w miarę potrzeb i zatwierdzanych koncepcji oraz planów.

Informacje o kolejnych przetargach dotyczących CPK można znaleźć na stronie:
https://portal.smartpzp.pl/cpk

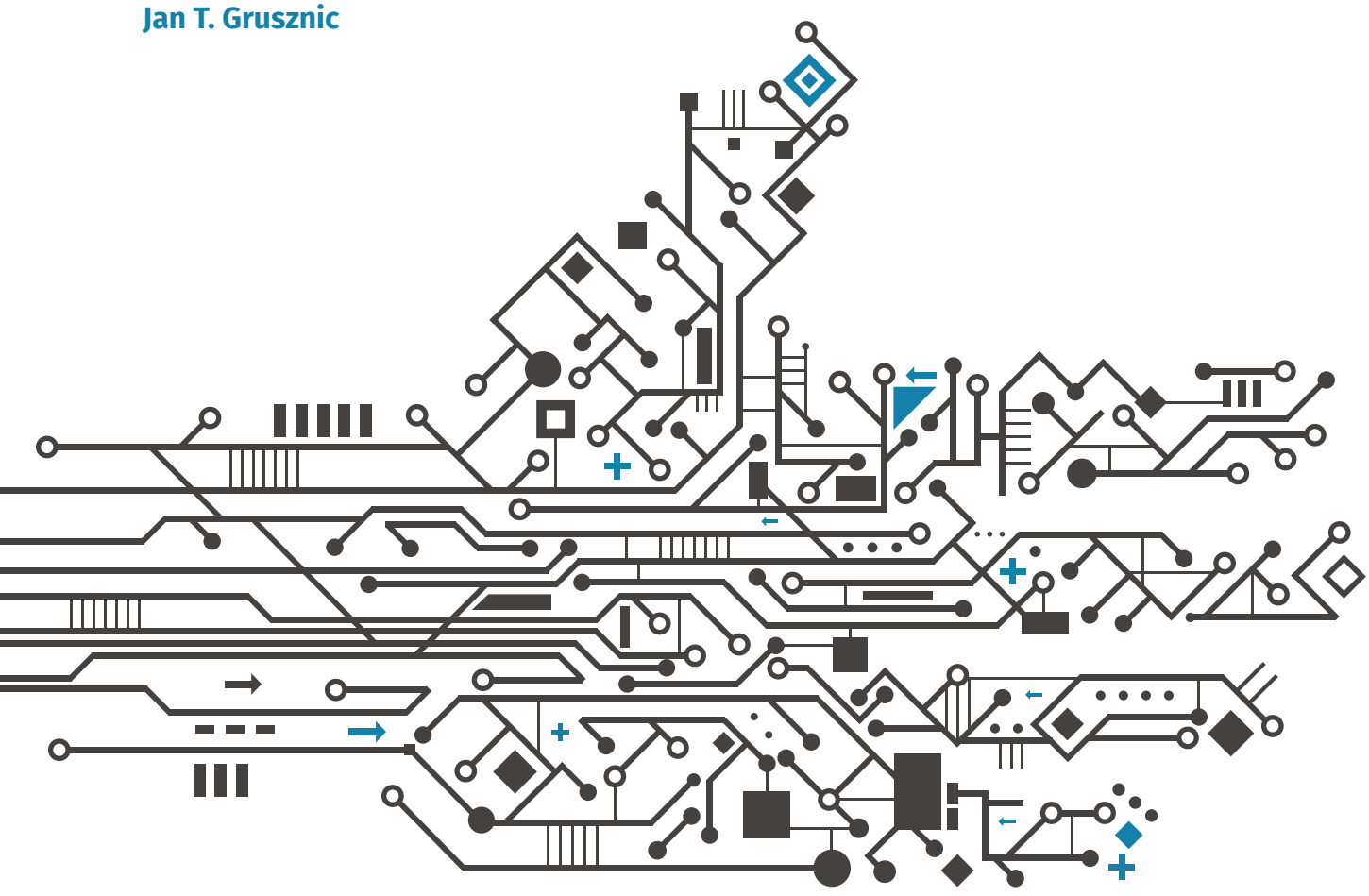
Adela Prochyra
redaktorka „a&s Polska"

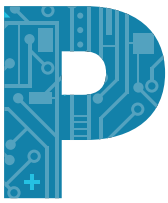
Wdrożenie dyrektyw NIS2 i CER w Polsce

Daleko jeszcze?

Dyrektywy NIS2 i CER stanowią fundament europejskiego systemu cyberbezpieczeństwa, zapewniając ochronę obywateli, przedsiębiorstw oraz usług publicznych przed różnorodnymi zagrożeniami. W Polsce Ministerstwo Cyfryzacji przygotowuje nowelizacje dwóch ustaw: o krajowym systemie cyberbezpieczeństwa (UKSC) oraz o zarządzaniu kryzysowym, które wdrażają te dyrektywy. Prace cały czas trwają – czy ustawodawca zdąży? Oto jest pytanie.

Jan T. Grusznic





Zgodnie z harmonogramem do 17 października zeszłego roku Polska miała wdrożyć dyrektywę NIS2 do prawa krajowego. Jesteśmy wśród 23 państw, które nie dopełniły obowiązku pełnej transpozycji dyrektywy. Kolejnym kamieniem milowym jest 17 kwietnia – do tego czasu państwa członkowskie muszą zidentyfikować podmioty kluczowe i ważne oraz poinformować te podmioty o spoczywających na nich obowiązkach. Najpewniej i ten termin nie zostanie dochowany. Do 17 stycznia 2026 r. kraje muszą sporządzić i przekazać Komisji Europejskiej pierwszą ocenę ryzyka zagrożeń dla podmiotów krytycznych – to wynika z dyrektywy CER, a do 17 października 2026 r. przekazać listę podmiotów objętych regulacją NIS2.

Piąta wersja projektu nowelizacji Ustawy o krajowym systemie cyberbezpieczeństwa pojawiła się na stronie Rządowego Centrum Legislacji 7 lutego. I ta wersja została przekazana Stałemu Komitetowi Rady Ministrów. Zapewne nie jest to wersja ostatnia, ponieważ konsultacje prowadzone przez Ministerstwo Cyfryzacji dotyczące ujednolicania przepisów nowelizacji UKSC z ustawą wdrażającą dyrektywę CER sugerują, że przed skierowaniem projektu do parlamentu czekają nas kolejne zmiany. Tym bardziej że 24 lutego br. w siedzibie Ministerstwa Cyfryzacji (MC) odbyło się spotkanie zespołów MC i Rządowego Centrum Bezpieczeństwa (RCB), którego założeniem było zidentyfikowanie potencjalnych rozbieżności w projektach nowelizacji oraz wypracowanie sposobu na ich eliminację.

Rozmowy dotyczyły w szczególności:

- rodzajów sektorów i podmiotów wchodzących w ich zakres,
- kontroli nad podmiotami kluczowymi i krytycznymi,
- właściwości organów sprawujących nadzór nad podmiotami kluczowymi i krytycznymi,
- audytów doraźnych (zlecanych decyzją o rygorze natychmiastowej wykonalności),
- screeningu kandydatów do zatrudnienia w zakresie weryfikowania niekaralności,
- kar za tożsame naruszenia w celu uniknięcia podwójnego karania.

Wśród propozycji pojawiających się w nowelizacji wywołującą jak do tej pory najwięcej dyskusji było wykreślenie bezpośredniego odwołania do norm ISO/IEC 27001 oraz ISO/IEC 22301 dla zgodności systemu zarządzania bezpieczeństwem informacji z regulacjami w przypadku, gdy system ten spełniał wymogi owych norm. Obecnie wymagane jest wdrożenie systemu zarządzania bezpieczeństwem informacji w systemie informacyjnym wykorzystywanym w procesach wpływających na świadczenie usługi. Podmioty kluczowe będą musiały przeprowadzić pierwszy audyt w ciągu 24 miesięcy od wejścia w życie ustawy (lub spełnienia kryteriów uznania za podmiot kluczowy), natomiast podmioty ważne będą zwolnione z tego obowiązku. Wydłużono czas do 3 miesięcy, jaki podmioty kluczowe i ważne będą miały na samodzielne przeprowadzenie analizy, której celem ma być sprawdzenie, czy podlegają pod regulacje, a jeśli tak, to dokonanie rejestracji w wykazie. Kolejną z kluczowych zmian jest nowa klasyfikacja podmiotów publicznych na kluczowe i ważne:

- **Podmioty publiczne kluczowe** – administracja centralna, istotne instytucje publiczne oraz wybrane podmioty jednostek samorządu terytorialnego.
- **Podmioty publiczne ważne** – samorządowe jednostki budżetowe, instytucje kultury oraz spółki prawa handlowego wykonujące zadania o charakterze użyteczności publicznej z wykorzystaniem systemów informatycznych.

Podmioty publiczne ważne będą miały uproszczone obowiązki w zakresie cyberbezpieczeństwa. Zamiast wdrażania rozbudowanego systemu zarządzania bezpieczeństwem informacji będą zobowiązane do wdrożenia uproszczonego systemu zgodnego z nowym załącznikiem nr 4 do Ustawy o krajowym systemie cyberbezpieczeństwa. Ponadto będą musiały wyznaczyć tylko jedną osobę do kontaktu z krajowym systemem cyberbezpieczeństwa oraz zgłaszać jedynie incydenty poważne, bez konieczności przekazywania wczesnych ostrzeżeń, sprawozdań okresowych i końcowych.

Kompetencje organów właściwych do spraw cyberbezpieczeństwa zostały rozszerzone. Teraz mogą samodzielnie decydować o wstrzymaniu koncesji, działalności regulowanej lub cofnięciu zezwolenia na prowadzenie działalności gospodarczej. Środki nadzoru nie będą stosowane dłużej niż 14 dni od daty doręczenia decyzji, lecz mogą być przedłużane aż do czasu usunięcia uchybień.

Nowy projekt doprecyzowuje również procedury stosowania środków nadzoru, aby zapewnić ich większą przejrzystość oraz egzekwowalność. Mowa m.in. o doraźnych kontrolach prowadzonych w celu sprawdzenia, czy podmiot usunął wcześniej stwierdzone uchybienia albo wykonał zalecenia pokontrolne oraz o publikacji w Biuletynie Informacji Publicznej (właściwym dla organu nadzorczego) decyzji o zastosowanych środkach nadzoru, z wyjątkiem informacji prawnie chronionych.

Wśród innych zmian znalazła się także propozycja zmniejszenia maksymalnego wymiaru kary pieniężnej dla osób zarządzających podmiotami kluczowymi i ważnymi. Obecnie wynosi ona maks. 300% (wcześniej 600%) wynagrodzenia ukaranego, obliczanego według zasad obowiązujących przy ustalaniu ekwiwalentu pieniężnego za urlop.

Zmieniona została również przesłanka, w wyniku której dostawca sprzętu lub oprogramowania może zostać uznany za dostawcę wysokiego ryzyka (DWR) z „zagrożenie dla obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego, lub życia i zdrowia ludzi" na „zagrożenia dla podstawowego interesu bezpieczeństwa państwa". Warto przypomnieć, że decyzja o uznaniu za dostawcę wysokiego ryzyka zawiera m.in. wskazanie typów produktów, rodzajów usług lub konkretnych procesów ICT pochodzących do dostawcy uwzględnionych w postępowaniu. Decyzja o uznaniu za dostawcę wysokiego ryzyka podlega natychmiastowemu wykonaniu i nie przysługuje ponowne rozpatrzenie sprawy, ale można ją zaskarżyć do sądu administracyjnego.

Procedura dotycząca uznania firmy za dostawcę wysokiego ryzyka jest złożona i wymaga czasu. Decyzja oparta jest w głównej mierze na opinii Kolegium do Spraw Cyberbezpieczeństwa, która rozważa aspekty nietechniczne, czyli sprawdza:

- czy istnieją zagrożenia bezpieczeństwa narodowego o charakterze ekonomicznym, wywiadowczym i terrorystycznym oraz

Ilustracje: freepik

zagrożenia realizacji zobowiązań sojuszniczych i europejskich, jakie stanowi dostawca,
- czy dostawca jest w jakiś sposób kontrolowany przez władze państw spoza terytorium UE lub NATO,
- czy dostawca ma powiązania z podmiotami określonymi w załączniku 1 do rozporządzenia 2019/796 z 17 maja 2019 r. w sprawie środków ograniczających w celu zwalczania cyberataków zagrażających Unii lub jej państwom członkowskim. (Załącznik zawiera wykaz osób fizycznych i prawnych, podmiotów i organów odpowiedzialnych za przeprowadzenie lub usiłowanie przeprowadzenia cyberataków)

oraz aspekty techniczne:
- liczbę i rodzaje wykrytych podatności i incydentów dotyczących typów produktów lub rodzajów usług bądź konkretnych procesów ICT, sposobu i czasu ich eliminowania,
- tryb i zakres, w jakim dostawca sprawuje nadzór nad procesem wytwarzania i dostarczania sprzętu lub oprogramowania dla wskazanych w ustawie podmiotów,
- ryzyko dla procesu wytwarzania i dostarczania sprzętu lub oprogramowania,
- wyniki badania podatności sprzętu lub oprogramowania.

Skutkiem uznania za dostawcę wysokiego ryzyka jest zakaz wprowadzania do użytkowania sprzętu lub oprogramowania tego dostawcy oraz obowiązkowe wycofanie sprzętu lub oprogramowania w ciągu 7 lat (4 lata dla przedsiębiorców komunikacji elektronicznej lub dla kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług) od momentu ogłoszenia w Monitorze Polskim.

CER, czyli dyrektywa o odporności podmiotów krytycznych

Niewątpliwie NIS2 ma lepsze *public relations* niż CER. Zapewne na zainteresowanie rynku wpływają liczby. Przepisom NIS ma podlegać kilkanaście tysięcy podmiotów. W przypadku CER będzie ich około tysiąca. Tymczasem to CER, patrząc z perspektywy branży ochrony osób i mienia, wydaje się ważniejszy. CER bowiem skupia się na odporności fizycznej infrastruktury krytycznej na różne zagrożenia, takie jak klęski żywiołowe, ataki terrorystyczne, sabotaż czy zagrożenia wewnętrzne. NIS2 koncentruje się na cyberbezpieczeństwie sieci i systemów informacyjnych. Obydwa akty współgrają ze sobą choćby w zakresie kategoryzacji podmiotu. Podmiot uznany za krytyczny w myśl dyrektywy CER staje się podmiotem kluczowym w myśl NIS2. A pełne wdrożenie dyrektyw NIS2 i CER wzmocni krajową cyberodporność, zapewniając skuteczną ochronę przed zagrożeniami cyfrowymi i zwiększając przejrzystość oraz efektywność działań nadzorczych.

Dyrektywa CER nakłada na państwa członkowskie obowiązek zapewnienia niezakłóconego świadczenia kluczowych usług społecznych i gospodarczych. Wymaga zatem najpierw zidentyfikowania podmiotów krytycznych, by móc wspierać ich odporność na zakłócenia. Ta dyrektywa rozszerza zakres ochrony infrastruktury krytycznej, obejmując jedenaście sektorów, w tym energię i transport, uznane przez Komisję Europejską za niewystarczające dla pełnej ochrony rynku wewnętrznego UE. Do tej pory przepisami unijnej dyrektywy objęte były tylko podmioty krytyczne z sektorów energii i transportu.

Dyrektywa CER wprowadza szczególną kategorię podmiotów krytycznych – podmioty krytyczne o szczególnym znaczeniu europejskim. Za takie uznaje się te, które są 1. podmiotem krytycznym w państwie członkowskim oraz 2. świadczą takie same lub podobne usługi kluczowe na rzecz co najmniej sześciu państw. Organizację, która została uznana za podmiot krytyczny o szczególnym znaczeniu europejskim należy o tym fakcie powiadomić.

Wyznaczanie podmiotów krytycznych o szczególnym znaczeniu europejskim odbywa się dopiero po konsultacjach, w których biorą udział: KE, właściwy organ państwa członkowskiego, właściwy organ innych zainteresowanych państw członkowskich oraz określony podmiot krytyczny. W trakcie konsultacji każde państwo członkowskie informuje Komisję o tym, czy uważa, że usługi świadczone na jego rzecz przez podmiot krytyczny stanowią usługi kluczowe w rozumieniu dyrektywy. Dopiero po tym KE uznaje dany podmiot za mający szczególne znaczenie europejskie, co wiąże się z określonymi w dyrektywie obowiązkami.

Co ważne państwa mają obowiązek **wspierać podmioty krytyczne w zwiększaniu ich odporności.** Obejmuje to m.in. opracowywanie materiałów zawierających wytyczne oraz metodyk, pomoc w organizacji ćwiczeń mających na celu sprawdzenie odporności tych podmiotów, czy zapewnianie doradztwa i szkoleń dla personelu podmiotów krytycznych. Jeżeli jest to konieczne i uzasadnione celami interesu publicznego, państwa mogą również przekazywać zasoby finansowe podmiotom krytycznym. Na ten cel stworzona zostanie w budżecie państwa rezerwa celowa.

Każde państwo musi wdrożyć strategię odporności do 17 stycznia 2026 r. i aktualizować ją co trzy lata. Państwa są również zobowiązane do przeprowadzenia krajowej oceny ryzyka (tzw. KOR) w tym samym terminie, którą także muszą aktualizować co trzy lata. Ocena ta pomaga organom identyfikować podmioty krytyczne i wspierać je zgodnie z dyrektywą. Do 17 lipca 2026 r. państwa mają obowiązek wyznaczyć te podmioty w sektorach wymienionych w załączniku.

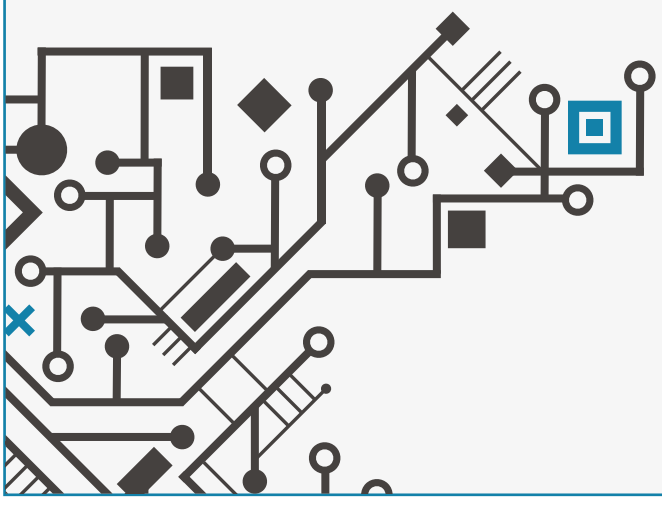
W dyrektywie zawarte zostały kryteria, które muszą być spełnione łącznie, aby dany podmiot mógł zostać uznany za krytyczny dla funkcjonowania danego sektora (lub państwa):
1. świadczy przynajmniej jedną usługę kluczową,
2. prowadzi działalność na terytorium państwa członkowskiego i jego infrastruktura krytyczna znajduje się na terytorium tego państwa,
3. ewentualny incydent miałby istotne skutki zakłócające świadczenie co najmniej jednej usługi kluczowej.

Identyfikując podmioty krytyczne państwo musi wziąć pod uwagę wyniki przeprowadzonej wcześniej oceny ryzyka KOR oraz przyjętą strategię odporności podmiotów krytycznych. Podmiot uznany za krytyczny zobowiązany jest wykonać obowiązki określone w ustawie po 9 miesiącach od daty powiadomienia. Państwo ma również obowiązek prowadzenia wykazu podmiotów krytycznych, który aktualizowany ma być co najmniej co dwa lata, a w stosownych przypadkach – częściej.

Jednym z głównych celów dyrektywy CER jest podniesienie odporności podmiotów krytycznych na wszelkiego rodzaju zagrożenia. Mają być one w stanie zwiększyć swoje zdolności do zapobiegania incydentom mogącym zakłócić świadczenie usług kluczowych, ochrony przed takimi incydentami i odpowiedzi na nie, stawiania im oporu, łagodzenia i absorbowania ich oraz adaptacji i odtworzenia po takich incydentach. Dlatego też w dyrektywie

PROCEDURA DOTYCZĄCA UZNANIA FIRMY ZA DOSTAWCĘ WYSOKIEGO RYZYKA

1	**Wszczęcie postępowania przez ministra właściwego ds. informatyzacji**	Z urzędu	Na wniosek Kolegium do Spraw Cyberbezpieczeństwa
2	**Zawiadomienie o wszczęciu postępowania**	Strony postępowania	Prokurator Generalny
3	**Opublikowanie informacji o wszczęciu postępowania w BIP właściwego ministra**	Niezwłocznie po doręczeniu zawiadomienia	W przypadku strony z siedzibą poza UE, Szwajcarią, EFTA albo EOG – udostępnienie zawiadomienia w BIP po 14 dniach ma skutki identyczne jak doręczenie
4	**Przedstawienie stanowisk przez organizacje społeczne**	Fakultatywnie w terminie 14 dni od opublikowania informacji	Minister właściwy do spraw informatyzacji publikuje w BIP raport ze złożonych w terminie stanowisk, wskazując w szczególności główne uwagi zawarte w stanowiskach
5	**Zasięgnięcie opinii Kolegium do Spraw Cyberbezpieczeństwa**	Termin na dostarczenie opinii: 3 miesiące	Przygotowuje zespół opiniujący powoływany przez przewodniczącego Kolegium, w jego skład może wejść także przedstawiciel Prezesa UOKiK
6	**Wydanie decyzji o uznaniu za dostawcę wysokiego ryzyka**	Dotyczy dostawcy sprzętu i oprogramowania oraz podmiotów wchodzących w skład grupy kapitałowej	Obowiązek wycofania dotyczy wyłącznie typów sprzętu i oprogramowania wskazanych w decyzji
7	**Ogłoszenie decyzji w Dzienniku Urzędowym Monitor Polski oraz udostępnienie w BIP i na stronie internetowej urzędu obsługującego właściwego ministra**		



Strony postępowania ws. uznania za DWR

- każdy, wobec kogo zostało wszczęte postępowanie
- fakultatywnie na prawach strony także przedsiębiorca telekomunikacyjny, spełniający określone ustawowo warunki:
  - ma siedzibę na terytorium Polski
  - jest wpisany do rejestru przedsiębiorców telekomunikacyjnych
  - w poprzednim roku obrotowym (roku, przed którym wszczęto postępowanie) uzyskał przychód z tytułu działalności telekomunikacyjnej w wysokości co najmniej dwudziestotysięcznej krotności przeciętnego wynagrodzenia wskazanej w ostatnim ogłoszonym przed wszczęciem postępowania komunikacie Prezesa GUS

cały rozdział poświęcony został mechanizmowi wzmacniania odporności podmiotów krytycznych. W jego ramach mieści się:
- ocena ryzyka podmiotu krytycznego,
- środki w zakresie odporności podmiotów krytycznych,
- sprawdzenie przeszłości osób i podmiotów,
- zgłaszanie incydentów,
- **zachęcanie do stosowania norm i specyfikacji technicznych.**

Zgodnie z projektem ustawy podmioty uznane za krytyczne muszą w ciągu 9 miesięcy od powiadomienia ocenić ryzyko. Kolejne oceny mają być przeprowadzane przynajmniej co trzy lata lub według potrzeb. Analiza obejmuje wszystkie istotne czynniki ryzyka, w tym naturalne, spowodowane przez człowieka, międzysektorowe i transgraniczne. Uwzględnia również wypadki, klęski żywiołowe, zagrożenia zdrowia publicznego, hybrydowe oraz związane z konfliktami międzynarodowymi, w tym terroryzm.

Podmioty powinny również ocenić zależność innych sektorów od świadczonych usług kluczowych oraz swoją zależność od innych podmiotów krytycznych. Incydenty zakłócające świadczenie usług muszą być zgłaszane do organów właściwych wstępnie w ciągu 24 godzin od ich wykrycia, a szczegółowe raporty należy przedłożyć w ciągu miesiąca.

Podobnie jak w NIS2, bazując na informacjach zebranych w ramach KOR i Krajowego Planu Zarządzania Ryzykiem (KPZR) oraz wyników oceny ryzyka podmiotu krytycznego, podmioty te muszą wdrożyć **odpowiednie i proporcjonalne środki, które mają zapewnić im odporność** na wszelkiego rodzaju incydenty w ramach tzw. 6-paku bezpieczeństwa znanego z Narodowego Programu Ochrony Infrastruktury Krytycznej (NPOIK), czyli:

a) bezpieczeństwa fizycznego, w tym ochrony fizycznej oraz zabezpieczeń technicznych uwzględniających kontrolę dostępu,
b) bezpieczeństwa technicznego,
c) bezpieczeństwa osobowego dotyczącego pracowników i dostawców zewnętrznych,
d) cyberbezpieczeństwa,
e) bezpieczeństwa prawnego,
f) ciągłości działania i odtwarzania, w tym utrzymywania własnych systemów rezerwowych zapewniających bezpieczeństwo i podtrzymujących funkcjonowanie infrastruktury krytycznej do czasu jej pełnego odtworzenia;

Ustawodawca przewidział 9 miesięcy na wdrożenie powyższych rozwiązań przez operatora infrastruktury krytycznej od dnia otrzymania informacji o dokonaniu wpisu do wykazu, a użyte środki muszą być opisane w planie zwiększania odporności podmiotu krytycznego. Minimalne wymagania w zakresie bezpieczeństwa fizycznego, technicznego, osobowego, cyberbezpieczeństwa, prawnego oraz ciągłości działania, niezbędne do wdrażania rozwiązań, o których mowa, zostaną określone na bazie rozporządzenia do ustawy. Z kolei zestawienie certyfikatów wymaganych od podmiotów zapewniających wdrożenie rozwiązań, potwierdzających posiadanie odpowiednich kompetencji i uprawnień ma być opracowane przez ministra kierującego działem administracji rządowej, właściwego terytorialnie wojewodę lub Komisję Nadzoru Finansowego, po zasięgnięciu opinii właściwych sektorowych rad do spraw kompetencji i udostępnione na stronie podmiotowej Biuletynu Informacji Publicznej. Należy spodziewać się odniesienia do norm branżowych i specyfikacji technicznych.

Podmioty krytyczne

ENERGIA

- Energia elektryczna
- System ciepłowniczy i chłodniczy
- Ropa naftowa
- Gaz
- Wodór

TRANSPORT

- Transport lotniczy
- Transport kolejowy
- Transport wodny
- Transport drogowy
- Transport publiczny

BANKOWOŚĆ

WODA PITNA

ADMINISTRACJA PUBLICZNA

INFRASTRUKTURA RYNKÓW FINANSOWYCH

ŚCIEKI

PRZESTRZEŃ KOSMICZNA

ZDROWIE

INFRASTRUKTURA CYFROWA

ŻYWNOŚĆ

Sektorowe rady do spraw kompetencji

Państwa członkowskie będą zachęcać podmioty krytyczne, nie narzucając ani nie faworyzując stosowania określonego rodzaju technologii, do stosowania europejskich i międzynarodowych norm oraz specyfikacji technicznych istotnych dla środków w zakresie bezpieczeństwa i odporności mających odniesienie do podmiotów krytycznych.

System rad ds. kompetencji w Polsce wspiera współpracę między biznesem, edukacją i administracją publiczną. Rady sektorowe analizują potrzeby rynku pracy i tworzą rekomendacje dotyczące kształcenia oraz doskonalenia zawodowego. W rezultacie programy szkoleniowe są lepiej dostosowane do rzeczywistych potrzeb rynku, co zwiększa szanse na znalezienie pracy oraz ułatwia rekrutację kompetentnych pracowników.

Rady pełnią funkcję opiniodawczo-doradczą przy Prezesie Polskiej Agencji Rozwoju Przedsiębiorczości (PARP) i składają się z przedstawicieli pracodawców, pracowników, instytucji edukacyjnych oraz organizacji branżowych. Ich zadania obejmują:

- analizowanie potrzeb kompetencyjnych w sektorze,
- opracowywanie rekomendacji dotyczących kształcenia i szkolenia zawodowego,
- monitorowanie zmian w sektorze i ich wpływu na wymagane kompetencje,
- upowszechnianie informacji o potrzebach kwalifikacyjno-zawodowych,
- inicjowanie współpracy przedsiębiorców z uczelniami i innymi podmiotami w celu integracji edukacji i pracodawców.

Lista sektorów, którym Prezes PARP powierzy podmiotom organizację i prowadzenie sektorowych rad ds. kompetencji została określona przez Prezesa PARP, na podstawie pozytywnej opinii Rady Programowej ds. kompetencji. Obecne trwa jeszcze nabór wniosków w konkursie na powierzenie organizacji i prowadzenia sektorowych rad ds. kompetencji. Wniosek o powierzenie organizacji i prowadzenia Sektorowej Rady ds. Kompetencji w sektorze Ochrony i Bezpieczeństwa Mienia i Osób złożony przez Zakład Rozwoju Technicznej Ochrony Mienia TECHOM Sp. z o.o. wraz z partnerami: Polską Platformą Bezpieczeństwa Wewnętrznego, Polskim Towarzystwem Bezpieczeństwa Narodowego i Stowarzyszeniem POLALARM uzyskał pozytywną opinię Prezesa PARP. Rada ta jest w procesie organizacji i zacznie działać w najbliższych tygodniach.

Organy właściwe na podstawie projektowanej ustawy otrzymały możliwość skorzystania z dwóch rodzajów **środków nadzoru:**

1. kontroli
2. audytów – prowadzonych samodzielnie lub zlecanych

Zakresem kontroli objęta jest infrastruktura krytyczna (obiekt, urządzenie, instalacja, sieć, system oraz usługa lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje, sieci, systemy oraz usługi niezbędne do świadczenia usługi kluczowej) oraz budynki i tereny wykorzystywane przez podmiot krytyczny do świadczenia usług kluczowych. W tej grupie środków znalazło się także uprawnienie do prowadzenia zdalnego nadzoru nad środkami w zakresie odporności stosowanymi przez podmioty krytyczne.

Oprócz tego organy właściwe wyposażone zostały w środki egzekwowania przepisów. Należą do nich:

- zobowiązanie podmiotów zidentyfikowanych jako podmioty krytyczne do przekazania w rozsądnym terminie,
- informacji niezbędnych, by ocenić, czy działania podjęte przez nie w celu zapewniania ich odporności spełniają wymogi określone w dyrektywie,
- dowodów potwierdzających skuteczne wdrożenie tych środków, w tym wyników audytu przeprowadzonego na koszt tego podmiotu przez wybranego przez niego niezależnego i wykwalifikowanego audytora,
- po przeprowadzeniu działań nadzorczych nakaz podjęcia przez podmioty krytyczne koniecznych i proporcjonalnych działań w celu wyeliminowania wszelkiego stwierdzonego naruszenia dyrektywy w rozsądnym terminie ustalonym przez te organy oraz poinformowania tych organów o podjętych działaniach.

Podmiot krytyczny będzie zobowiązany przeprowadzić audyt systemu zarządzania bezpieczeństwem świadczenia usługi kluczowej co najmniej raz na trzy lata, który obejmie: bezpieczeństwo informacji, ciągłość działania usługi, bezpieczeństwo fizyczne budynków i terenów oraz zabezpieczenia techniczne, w tym kontrolę dostępu. Audyt może prowadzić jednostka certyfikująca lub dwóch audytorów, w tym jeden z ukończonym szkoleniem audytora wiodącego, mający odpowiednie certyfikaty i spełniający wymagania bezpieczeństwa osobowego i przemysłowego. Wykaz wymaganych certyfikatów uprawniających do przeprowadzania audytów, uwzględniających zakres wiedzy specjalistycznej wymaganej od osób lub podmiotów legitymujących się poszczególnymi certyfikatami oraz wymagane doświadczenie zostanie określony w rozporządzeniu.

W dyrektywie znalazł się również zapis o możliwości nakładania przez państwa członkowskie sankcji, mających zastosowanie w przypadku naruszeń przepisów krajowych przyjętych na podstawie dyrektywy CER. W przypadku projektu z dnia 24 marca 2025 r. najwyższa kara wynosi 200 000 zł za brak audytu lub uchylanie się od wdrożenia zaleceń pokontrolnych. Kary nadawane są jednak za **uchybienia**, zatem ich wysokość w skrajnych przypadkach może przekroczyć milion zł. Karze finansowej tej wysokości może podlegać zarząd spółki za uporczywe naruszanie przepisów ustawy.

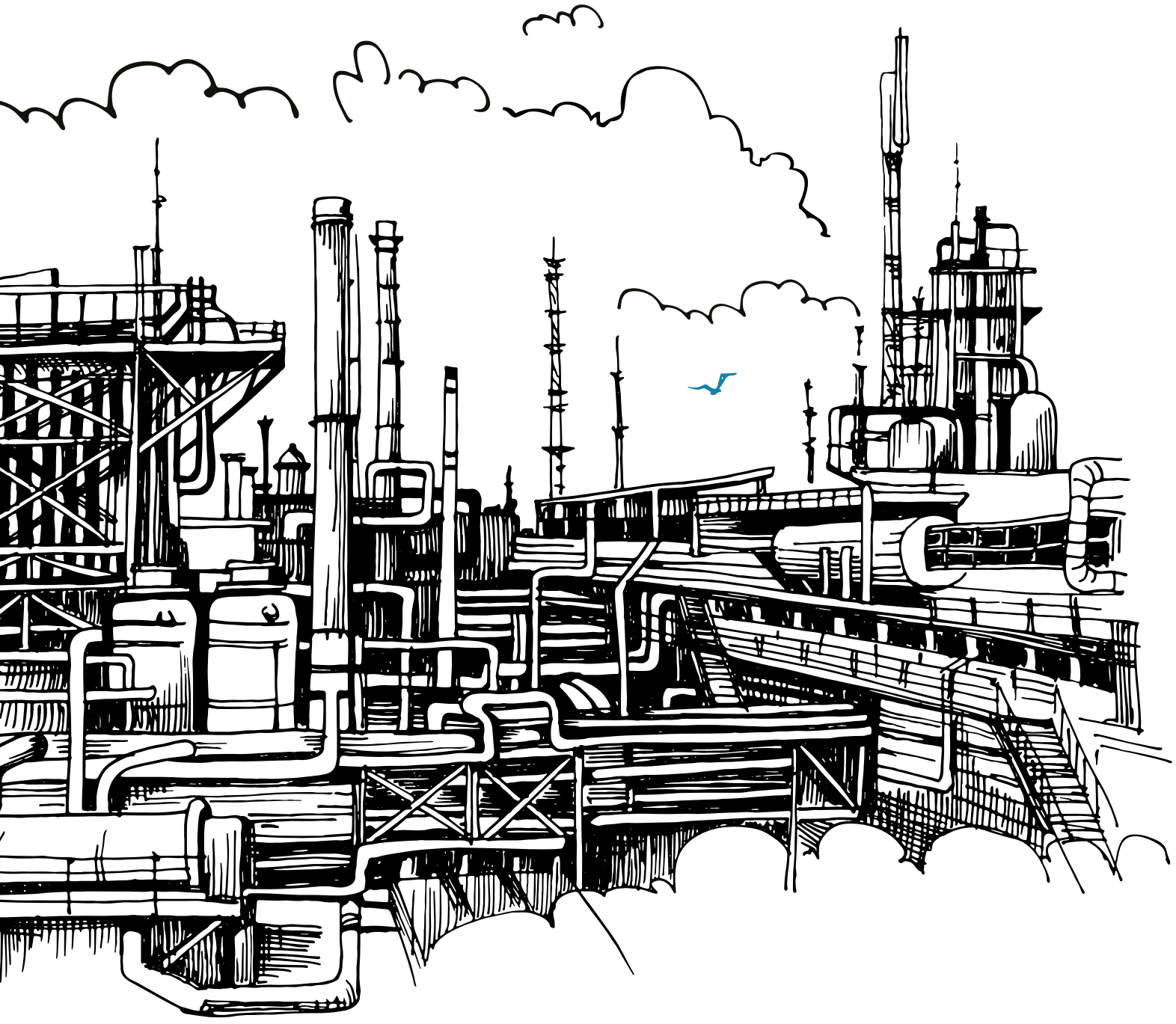
Interesującym mechanizmem, mającym wzmocnić odporność podmiotów krytycznych, jest umożliwienie **weryfikacji przeszłości osób, które pełnią newralgiczne funkcje w podmiocie krytycznym** lub na jego rzecz bądź mają dostęp do budynków i terenów podmiotu krytycznego, jego informacji lub systemów kontroli. Może to również dotyczyć osób, które są brane pod uwagę przy rekrutacji na określone stanowiska.

Pełne wdrożenie dyrektyw NIS2 i CER oraz nowelizacja UKSC mają na celu wzmocnienie cyberbezpieczeństwa w Polsce, zapewniając skuteczną ochronę przed zagrożeniami cybernetycznymi i zwiększając przejrzystość oraz efektywność działań nadzorczych.

Można oczekiwać, że w niedługim czasie projekty obu ustaw zostaną skierowane do parlamentu. W związku z czym przedsiębiorstwa, które będą podlegały pod tę regulację, powinny już teraz zacząć przygotowania do spełnienia nowych wymagań. •

Jan T. Grusznic
redaktor „a&s Polska”

Bezpieczeństwo wymaga **czujności**



Współczesne zagrożenia nie epatują bronią, nie wjeżdżają czołgami. Udają incydenty, niegroźne usterki, przypadki – aż wreszcie w najmniej oczekiwanym momencie uderzają z pełną siłą. Polska, znajdująca się na styku kluczowych szlaków geopolitycznych, stała się obiektem rosnącej presji – od cyberataków po działania hybrydowe.

Jakub Sobek

W odpowiedzi na te wyzwania wprowadzono system stopni alarmowych określonych w Ustawie o działaniach antyterrorystycznych z 10 czerwca 2016 r. (Dz.U. 2016 poz. 904), które mają mobilizować służby i administrację do wzmożonej czujności. To zrozumiałe, że rośnie znaczenie ochrony perymetrycznej – systemów zabezpieczeń stosowanych na obwodzie chronionych obiektów – która w dynamicznej sytuacji zagrożeń musi ściśle współdziałać z pozostałymi systemami.

Ochrona perymetryczna a stopnie alarmowe

Ochrona perymetryczna to zespół środków ochrony fizycznej stosowanych na granicy (obwodzie) chronionego terenu lub obiektu. Obejmuje m.in. ogrodzenia, bariery, czujniki ruchu, kamery dozoru wizyjnego i systemy detekcji wtargnięć. Jej zadaniem jest odstraszanie intruzów, wczesne wykrywanie próby wtargnięcia i uniemożliwienie intruzowi dotarcia do chronionych zasobów albo choć opóźnienie jego działania, by ochrona zdążyła przybyć z odsieczą. Sprawna ochrona perymetryczna jest pierwszą linią obrony przed atakiem fizycznym lub sabotażem.

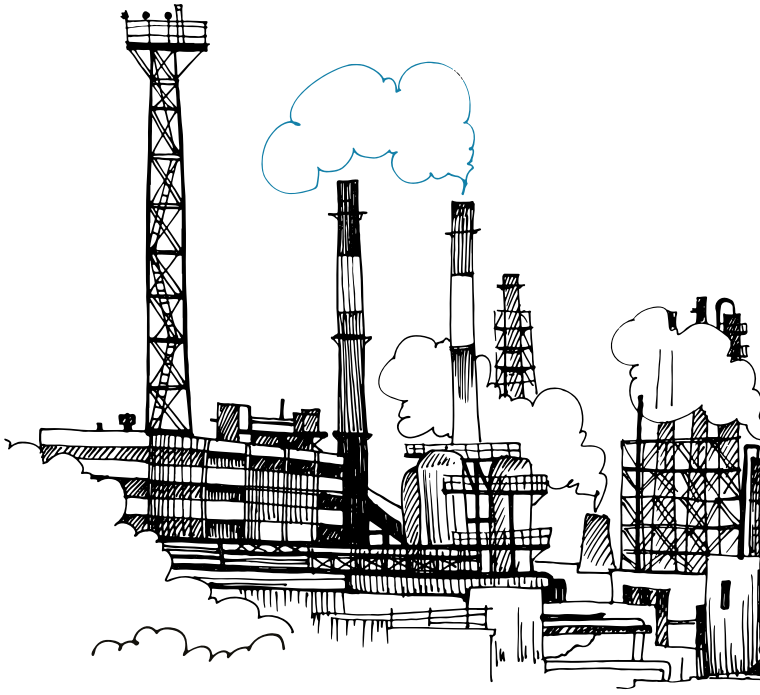
Zgodnie z polskim prawem w naszym kraju obowiązują cztery stopnie alarmowe: ALFA, BRAVO, CHARLIE i DELTA (oraz analogiczne cztery stopnie CRP dotyczące cyberprzestrzeni). Każdy z tych alarmów może zostać wprowadzany w części kraju lub na całym terytorium. Może też dotyczyć konkretnych obiektów infrastruktury krytycznej w drodze zarządzenia Prezesa Rady Ministrów (lub w pilnych przypadkach – Ministra Spraw Wewnętrznych). Każdy kolejny stopień oznacza wyższy poziom zagrożenia terrorystycznego lub sabotażowego i wiąże się z rozszerzeniem wachlarza przedsięwzięć ochronnych, także w obszarze ochrony fizycznej obiektów.

Stopień ALFA (najniższy) ma charakter ogólnego ostrzeżenia – jest wprowadzany, gdy pojawiają się niepokojące sygnały o możliwości wystąpienia zdarzenia o charakterze terrorystycznym, gdy brak konkretnych informacji o celach ataku. Jego ogłoszenie obliguje administrację i służby do wzmożonej czujności, m.in. poprzez kontrolę obiektów użyteczności publicznej, monitoring miejsc zgromadzeń oraz gotowość personelu do działań ochronnych. Na terenie chronionych obiektów zwiększa się częstotliwość patroli i kontroli pojazdów oraz osób, sprawdzane są systemy alarmowe i monitoring wizyjny. W praktyce ALFA ma utrzymywać służby w stanie gotowości przez czas nieograniczony – tak, by mogły natychmiast reagować na ewentualną eskalację zagrożenia.

Stopień BRAVO jest ogłaszany, gdy pojawiają się bardziej konkretne przesłanki zagrożenia terrorystycznego lub sabotażowego – np. zwiększone i przewidywalne ryzyko ataku, choć bez zidentyfikowanego celu. Ogłoszenie stopnia BRAVO oznacza wzmocnienie środków ochrony perymetrycznej, zwiększenie liczby posterunków i patroli przy obiektach wrażliwych, dodatkowe kontrole pojazdów, osób i budynków w rejonach zagrożonych. Następuje także podniesienie zabezpieczeń obiektów kluczowych, takich jak choćby ograniczenie dostępu osób postronnych do budynków publicznych, wzmacniana jest ochrona transportu publicznego i infrastruktury komunikacyjnej. Z perspektywy ochrony perymetrycznej stopień BRAVO oznacza uruchomienie rezerw personalnych niezbędnych do wsparcia ochrony obwodowej obiektów oraz intensywniejsze monitorowanie stref wokół nich.

Stopień CHARLIE jest trzecim poziomem alarmowym, ogłaszanym, gdy doszło do konkretnego zdarzenia (ataku terrorystycznego lub sabotażu), bądź uzyskano wiarygodne informacje o przygotowaniach do takich działań. CHARLIE wprowadza całodobowe dyżury ważnych instytucji, ogranicza dostęp do niektórych budynków użyteczności publicznej, powoduje jeszcze częstsze i bardziej skrupulatne kontrolowanie osób i pojazdów przy wjazdach na teren obiektów, a także zamknięcie stref obecnych w pobliżu granic obiektów, mowa np. o zakazie parkowania w pobliżu chronionych budynków. W razie potrzeby wydawana jest broń i sprzęt ochronny dodatkowym siłom, a miejsca dotąd nieobjęte nadzorem są włączane pod ciągłą obserwację. To znaczy, że np. obiekt infrastruktury krytycznej po ogłoszeniu alarmu

Ilustracje: freepik



CHARLIE może zostać otoczony dodatkowymi posterunkami na całym obwodzie, z kontrolą każdego pojazdu i osoby wchodzącej.

Stopień DELTA (najwyższy) ogłaszany jest w sytuacji bezpośredniego zagrożenia lub po ataku terrorystycznym. Oprócz pełnego zakresu działań wynikających z zasad obowiązywania niższych stopni alarmowych DELTA wprowadza pełną mobilizację, m.in. możliwość zamknięcia dróg i wprowadzenia ograniczeń komunikacyjnych w rejonie zagrożonym, dokładną identyfikację i ewakuację pojazdów z otoczenia obiektów, kontrolę absolutnie wszystkich osób i pakunków wnoszonych na teren chroniony, częste kontrole zewnętrzne i patrolowanie parkingów. Celem wprowadzenia stopnia DELGA jest uniemożliwienie kolejnego ataku. Ochrona perymetryczna jest wówczas zaangażowana na sto procent swoich możliwości, a dostęp na teren obiektu chronionego jest drastycznie ograniczony.

Lepiej zapobiegać

W pierwszych miesiącach 2022 r., w związku z narastającym napięciem wokół Ukrainy, kilkukrotnie ogłaszano ALFA-CRP w całej Polsce. Bezpośrednio przed inwazją Rosji na Ukrainę, 21 lutego 2022 r., podniesiono alarm cybernetyczny do stopnia CHARLIE-CRP na terenie całego kraju, a następnie (po wybuchu wojny i masowym napływie uchodźców) wprowadzono drugi stopień BRAVO w województwach przygranicznych (lubelskim i podkarpackim) oraz wkrótce potem BRAVO w całej Polsce. Od tego momentu przez w latach 2022–2023 przez większość miesięcy obowiązywał co najmniej stopień ALFA lub BRAVO, a dla cyberprzestrzeni często BRAVO-CRP. W połowie 2024 r. rząd przedłużył obowiązywanie BRAVO oraz BRAVO-CRP na obszarze całego kraju (oraz dodatkowo BRAVO dla polskiej infrastruktury energetycznej za granicą) – z zamiarem utrzymania ich do końca sierpnia 2024 r. Wobec utrzymywania się zagrożeń hybrydowych ze strony Rosji i Białorusi alarmy te były ponownie przedłużane. Najnowszą decyzją obowiązywać będą do maja 2025 r. To skutek charakteru zagrożeń i tego, że przynajmniej na razie, nie ma mowy o ich wygaśnięciu. Przedłużenie obowiązywania tych stopni wymaga permanentnego utrzymania wzmocnionej ochrony perymetrycznej wielu obiektów strategicznych, wzmocnienia ochrony lotnisk i dworców kolejowych, uszczelnienia granic (również w odpowiedzi na kryzys migracyjny na granicy z Białorusią w 2021 r.), ale też wzmocnienie ochrony elektrowni i magazynów paliw po agresji Rosji na Ukrainę (w obawie przed dywersją). Konieczność bezproblemowego przejścia od sytuacji, w której zagrożeń brak, do stanu alarmowego (ALFA/BRAVO/CHARLIE) powoduje, że infrastruktura krytyczna musi być tak chroniona, by być odporna na pojawiające się incydenty i dostosowana do wprowadzenia kolejnych stopni alarmowych. Począwszy od stopnia ALFA, czysto prewencyjnego aż po stopień DELTA, wymagający pełnej mobilizacji sił ochrony.

Incydenty w Polsce

Polska w ostatnich latach doświadczyła rosnącej liczby incydentów sabotażowych i ataków cyfrowych wymierzonych w strategiczne obiekty przemysłowe oraz infrastrukturę krytyczną. Działania te najczęściej są przypisywane podmiotom powiązanym z Rosją lub Białorusią i wpisują się w szerszą kampanię destabilizacji regionu:

- Sabotaż na kolei (sierpień 2023 r.). W drugiej połowie sierpnia 2023 r. doszło do serii zakłóceń na polskiej kolei wywołanych przez nieuprawnione nadawanie sygnałów stop w systemie radiołączności pociągów. 25 sierpnia nieznani sprawcy nadali przez sieć kolejową sygnał awaryjnego zatrzymania (tzw. radio-stop), co spowodowało unieruchomienie ponad 20 pociągów w okolicach Szczecina.
- Operacja sabotażowa rosyjsko-białoruska (wrzesień 2024 r.). We wrześniu 2024 r. polskie służby ogłosiły neutralizację siatki sabotażystów działających na terenie kraju, kierowanej przez służby Rosji i Białorusi. Wiceminister ds. cyfryzacji Krzysztof Gawkowski poinformował o rozbiciu grupy, której celem było zdestabilizowanie Polski w odwecie za jej wsparcie dla Ukrainy. Sabotażyści działali z terytorium Białorusi, współpracując z rosyjskim wywiadem; infiltrowali instytucje państwowe i spółki z sektora obronnego wykonujące zamówienia wojskowe. Ich zadaniem było wykradanie danych, szantażowanie osób oraz prowadzenie cyberwojny de facto przeciw Polsce. Wcześniej, bo w roku 2023 ABW zatrzymała dziewięciu członków innej siatki szpiegowsko-dywersyjnej działającej na zlecenie Rosji.
- Próby podpaleń i ataki bombowe na infrastrukturę pocztową (2023–2024). Przejawem sabotażu hybrydowego były przesyłki z materiałami zapalającymi wysyłane do instytucji w Polsce i krajach sojuszniczych. Kulminacją tych działań było odkrycie w 2023 r. spisku polegającego na podkładaniu ładunków zapalających do przesyłek kurierskich z zamiarem wywołania pożarów na pokładach samolotów cargo lecących do USA i Kanady. ABW we współpracy z sojusznikami zidentyfikowała osoby zaangażowane w ten plan. W październiku 2023 r. aresztowano cztery osoby podejrzane o udział w międzynarodowej siatce sabotażu wykorzystującej firmy kurierskie. Incydenty z przesyłkami wykazały, że infrastruktura krytyczna to nie tylko obiekty stacjonarne, ale także logistyka i łańcuchy dostaw – lotnicze cargo, centra kurierskie – które również stały się celem kreatywnych form ataku. W odpowiedzi wzmocniono kontrolę bezpieczeństwa przesyłek i monitoring transportów w newralgicznych węzłach.

Wszystkie te przypadki mają wspólny mianownik: są elementem szerszej kampanii wojny hybrydowej prowadzonej przez

Polska, podobnie jak inne państwa NATO, znalazła się w ostatnich latach w obliczu bezprecedensowej fali zagrożeń hybrydowych. Ataki terrorystyczne, akcje sabotażowe i ataki hakerskie – często inspirowane lub bezpośrednio prowadzone przez nieprzyjazne służby – wymusiły rozbudowę krajowego systemu ochrony. Ochrona perymetryczna obiektów, np. infrastruktury krytycznej, stała się nie tylko kwestią ochrony fizycznej, ale także elementem szerszej układanki budowania odporności.

nieprzyjazne państwa przeciwko Polsce i Zachodowi. Wojna hybrydowa to strategia prowadzenia konfrontacji, która łączy metody konwencjonalne (militarne) z działaniami poniżej progu regularnej wojny – takimi jak cyberataki, sabotaż, dezinformacja, presja ekonomiczna czy prowokacje polityczne. Celem wojny hybrydowej jest osłabienie przeciwnika od wewnątrz i osiągnięcie przewagi bez formalnego wypowiedzenia wojny.

Znaczenie ochrony perymetrycznej

Bezpieczeństwo antyterrorystyczne i ochrona infrastruktury krytycznej w Polsce są uregulowane w kilku kluczowych aktach prawnych. Wśród nich najważniejsze to: ustawa z 10 czerwca 2016 r. o działaniach antyterrorystycznych (wprowadzająca m.in. stopnie alarmowe) oraz ustawa z 26 kwietnia 2007 r. o zarządzaniu kryzysowym (definiująca infrastrukturę krytyczną i obowiązki jej ochrony, wielokrotnie nowelizowana, m.in. w 2018 r. i 2023 r.). Dodatkowo istnieją akty wykonawcze, np. rozporządzenie Prezesa Rady Ministrów z 25 lipca 2016 r. określające szczegółowe przedsięwzięcia w poszczególnych stopniach alarmowych (Dz.U. 2016 poz. 1101) oraz Narodowy Program Ochrony Infrastruktury Krytycznej przyjmowany przez rząd.

Infrastruktura krytyczna (IK), zgodnie z definicją w ustawie o zarządzaniu kryzysowym, to systemy i powiązane obiekty kluczowe dla bezpieczeństwa państwa i obywateli, których zakłócenie funkcjonowania spowodowałoby poważne konsekwencje (m.in. systemy energetyczne, zaopatrzenia w wodę, łączność, transport, finansowe, ochrony zdrowia itd.). Ustawa ta nakłada na organy administracji różne obowiązki w zakresie ochrony IK, a przede wszystkim zobowiązuje właścicieli i operatorów infrastruktury krytycznej do jej ochrony. Art. 5 ust. 5 tej ustawy stanowi, że „właściciele oraz posiadacze samoistni i zależni obiektów, instalacji lub urządzeń infrastruktury krytycznej mają obowiązek ich ochrony", w szczególności przez przygotowanie i wdrożenie planów ochrony infrastruktury krytycznej stosownie do potencjalnych zagrożeń. W praktyce każdy operator (np. spółka energetyczna zarządzająca siecią elektroenergetyczną, przedsiębiorstwo wodociągowe, port lotniczy, itd.) identyfikuje swoje obiekty zaliczone do IK i opracowuje Plan Ochrony IK.

Z punktu widzenia ochrony perymetrycznej plany ochrony IK zazwyczaj szczegółowo opisują, jakie środki fizycznej ochrony są zastosowane na obwodzie obiektu i jakie obowiązują procedury dostępu. Co więcej, ustawa zobowiązuje operatorów do bieżącej współpracy z centrami zarządzania kryzysowego i służbami, np. mają informować o wszelkich poważnych awariach i incydentach bezpieczeństwa, by można było skoordynować reakcję. Tak więc prawo tworzy platformę wymiany informacji między sektorami publicznym a prywatnym w zakresie ochrony IK.

Polska, podobnie jak inne państwa NATO, znalazła się w ostatnich latach w obliczu bezprecedensowej fali zagrożeń hybrydowych. Ataki terrorystyczne, akcje sabotażowe i operacje cybernetyczne – często inspirowane lub bezpośrednio prowadzone przez nieprzyjazne służby – wymusiły rozbudowę krajowego systemu ochrony. Ochrona perymetryczna obiektów, np. infrastruktury krytycznej, stała się nie tylko kwestią ochrony fizycznej, ale także elementem szerszej układanki budowania odporności. Ochrona perymetryczna – od granic państwa po ogrodzenie pojedynczej elektrowni – pozostaje fundamentalną częścią tej odpowiedzi, lecz dopiero w połączeniu z inteligentnymi systemami i solidnymi ramami prawnymi tworzy efektywną tarczę przeciw zagrożeniom XXI wieku. •

Jakub Sobek

Absolwent Politechniki Poznańskiej na Wydziale Robotyki i Automatyki, specjalność Systemy wizyjne i multimedialne. Od 2012 r. trener techniczny systemów wizyjnych IP oraz rozwiązań termowizyjnych. Od 2015 r. pracownik dydaktyczny PISA, a od 2019 r. członek Zarządu PISA. Od 2022 r. współpracuje z firmą RCS Engineering jako Kierownik Wsparcia Technicznego. Autor wielu publikacji w prasie branżowej dotyczących termowizji, systemów perymetrycznych oraz analizy wideo.

Jak skutecznie dbać o bezpieczeństwo obiektów infrastruktury krytycznej

Szybka reakcja odpowiednich służb chroniących obiekty infrastruktury krytycznej, zapobiegająca nieprzyjemnym w skutkach incydentom, jest możliwa przede wszystkim dzięki zastosowaniu najlepszej jakości urządzeń i oprogramowania, takich jak kamery bispektralne oferowane przez firmę Hikvision, która nieustająco rozwija techniki termowizyjne.

Nie tylko zakłady będące obiektami infrastruktury krytycznej powinny ze stosowania kamer bispektralnych uczynić fundament swojej ochrony, ale także wszystkie firmy, którym zależy na zapewnieniu jak największego poziomu bezpieczeństwa. To bowiem kamery bispektralne zapewniają obraz doskonałej jakości, bez przekłamań związanych z refleksami światła czy zniekształceniami biorącymi się z niskiego poziomu oświetlenia.

Hikvision w ostatnim czasie wprowadził na rynek rodzinę kamer bispektralnych Heat Pro o podwyższonej czułości termicznej wynoszącej 35 mK i z ulepszonym systemem analizy wideo – VCA 3.0. Skutkiem tych zmian jest zdecydowanie mniejsza liczba fałszywych alarmów, co ma niewątpliwe znaczenie dla wiarygodności informacji o incydencie i sprzyja właściwej reakcji służb bezpieczeństwa. Nowy system analizy wideo VCA 3.0 bardzo dobrze sobie radzi w niekorzystnych warunkach atmosferycznych, a jego kalibracja została znacznie uproszczona w porównaniu ze wcześniejszą wersją.

Kamera bispektralna typu bullet

Kamery bispektralne są dostarczane również w formie głowic szybkoobrotowych PTZ oraz pozycjonerów PTZ. Hikvision w ostatnim czasie wprowadził na rynek pozycjonery PTZ dalekiego zasięgu, o czułości termicznej 25 mK i rozdzielczości 1280 x 1024 pikseli. Dzięki oprogramowaniu do analizy wideo urządzenia te potrafią wykryć obiekt z odległości prawie 3 km, rozpoznając, czy jest nim człowiek. Dostępne są też rozwiązania z laserem z pomiarem odległości i GPS, dzięki czemu można określać położenie GPS wykrytego obiektu.

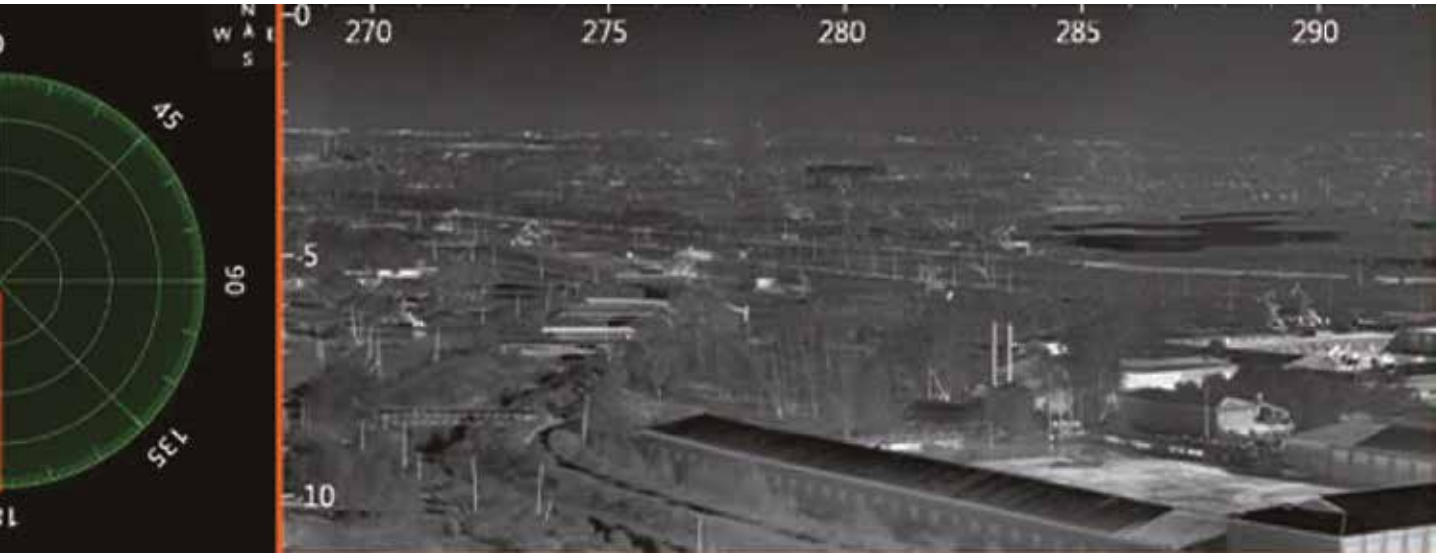
Bispektralna kamera PTZ dalekiego zasięgu

Termowizja może być też wykorzystywana do wykrywania dronów. Przykładem jej zastosowania jest wirujący pozycjoner, który obracając się, skanuje całe otoczenie wokół

Kamera bispektralna typu bullet

Bispektralna kamera PTZ, wyposażona w laser i GPS do namierzania pozycji obiektu

Bispektralna kamera PTZ dalekiego zasięgu



własnej osi, podobnie jak to czyni radar. Urządzenie po wykryciu obiektu naprowadza inne urządzenia lub kamerę PTZ, która dokonuje zbliżenia i weryfikacji.

Termowizyjny skaner 360 stopni

Urządzeniami naprowadzającymi inne kamery PTZ mogą być też typowe radary security. Hikvision w zeszłym roku powiększył ofertę o wyjątkowo odporny na warunki atmosferyczne model, który umożliwia rozpoznanie człowieka z odległości 1800 m przy kącie detekcji 90°. Ponadto radar przekazuje bardzo szczegółowe informacje o trajektorii ruchu wykrytego obiektu. Kamera PTZ naprowadzana tego typu radarem pozwala na precyzyjną weryfikację zagrożenia i szybką reakcję na naruszenia strefy chronionej, nawet jeśli jest ich kilka w tym samym czasie.

System kamer bądź radarów może być sprzężony z systemem zewnętrznych głośników IP. Komunikaty mogą być uruchamiane automatycznie w momencie dostrzeżenia intruza naruszającego strefę chronioną. Taki komunikat ma aspekt informujący, ale też mocno odstraszający. W wielu przypadkach wystarczy, by zniechęcić intruza do wtargnięcia do strefy chronionej.

Poza udoskonalaniem urządzeń wykorzystujących termowizję oraz systemami radarowymi Hikvision zajmuje się rozwojem oferty związanej z zastosowaniem światłowodów. W ubiegłym roku firma wprowadziła do sprzedaży zaawansowane analizatory kabla światłowodowego stosowanego w ochronie perymetrycznej na ogrodzeniach oraz umieszczanych w gruncie. Analizatory wykrywają zmiany parametrów kabla światłowodowego wywołanych drganiami, które mogę wystąpić przy forsowaniu bariery (płotu) czy w wyniku przechodzenia w bliskiej odległości kabla umieszczonego w ziemi.

Połączenie kabla sensorycznego lub radaru z systemami kamer wizyjnych albo bispektralnych powoduje synergiczne wzmocnienie systemu zabezpieczeń. Urządzenia te wzajemnie się uzupełniają, zatem razem są mniej podatne na wpływ środowiska czy próby obejścia systemu dozoru. Może się to przełożyć na istotne podwyższenie jakości pracy takiego systemu i skuteczności służb. Niezależnie jednak od stosowanej technologii należy przede wszystkich sprawdzać stan faktyczny zainstalowanego systemu. Warto regularnie kontrolować, czy system jest w pełni sprawny, czy został prawidłowo dobrany i skonfigurowany, a także czy liczba urządzeń detekcyjnych wystarczy, by objąć nadzorem cały obszar. •

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

Termowizyjny skaner 360 stopni

Głośnik IP

Analizator do ochrony perymetrycznej dla kabla światłowodowego

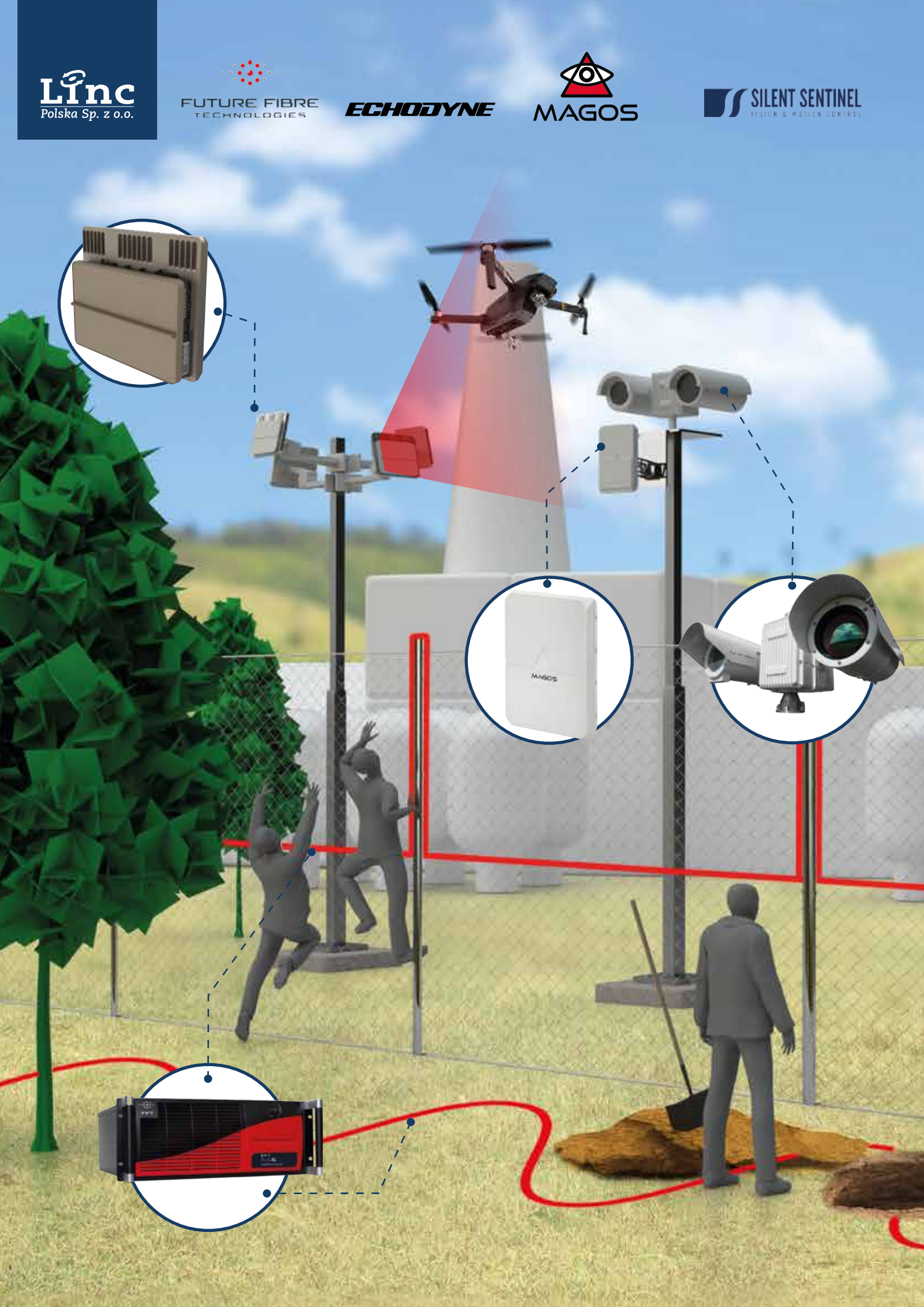
Linc Polska Sp. z o.o.

FUTURE FIBRE TECHNOLOGIES

ECHODYNE

MAGOS

SILENT SENTINEL
VISION & MOTION CONTROL



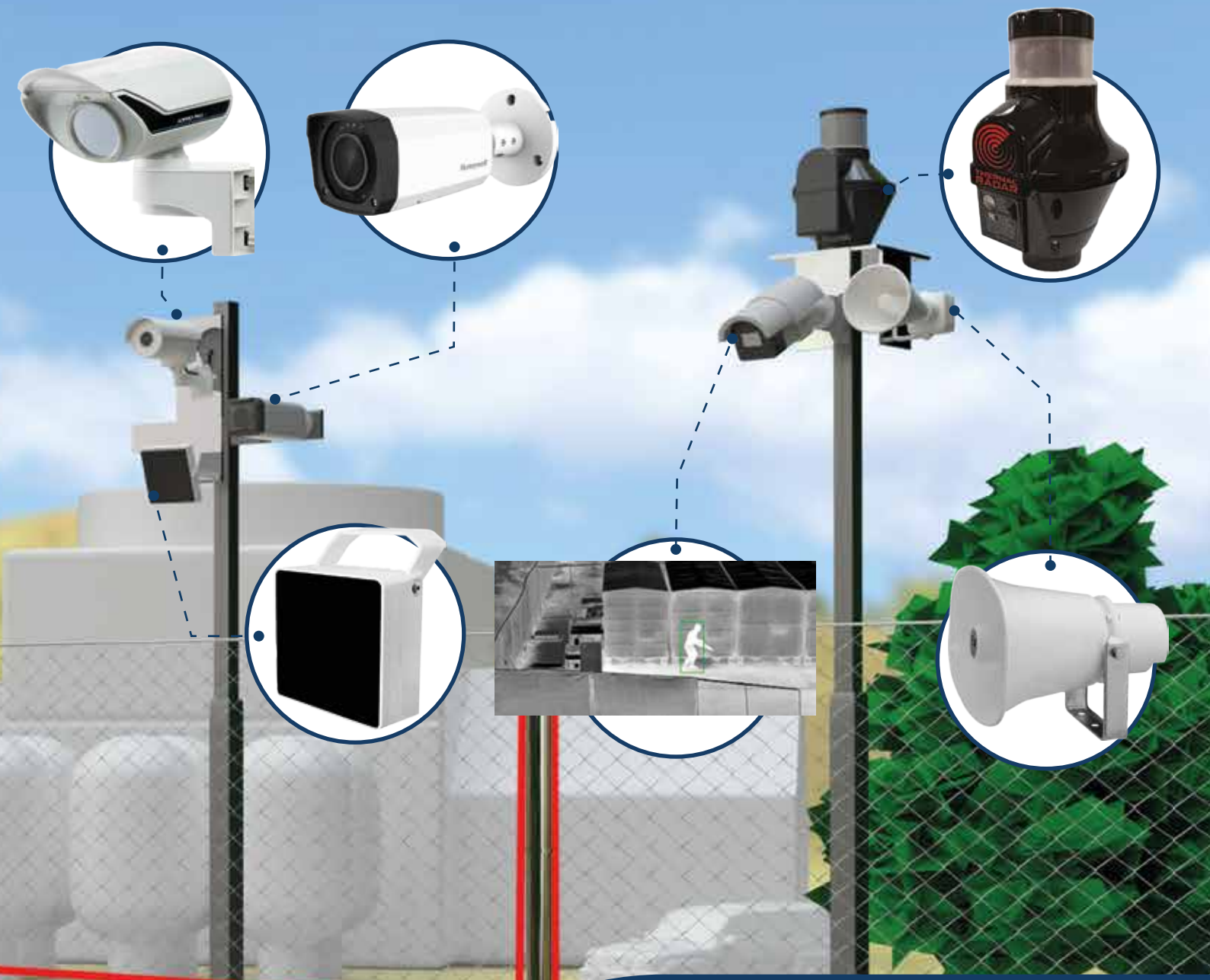
xtralis is now a part of Honeywell

EMITLIGHT

TELEDYNE FLIR

TOA

THERMAL RADAR



Automatyczna detekcja zagrożenia

Sztuczna Inteligencja

Daleki zasięg

Integracja

Niezawodność i skuteczność

www.linc.pl

Bezpieczeństwo na lotniskach z wykorzystaniem nowoczesnych technologii

Infrastruktura krytyczna, w tym lotniska, wymaga szczególnej ochrony, a bezpieczeństwo transportu towarów i pasażerów stanowi jedno z kluczowych wyzwań operatorów tych strategicznych obiektów oraz władz.

Skuteczna ochrona wymaga zastosowania jednocześnie wielu zaawansowanych systemów zabezpieczeń, co pozwala na efektywne przeciwdziałanie zagrożeniom i zapewnienie nieprzerwanego, bezpiecznego funkcjonowania portów lotniczych.

Bezpieczne i sprawne zarządzanie ruchem na parkingach lotniskowych

Wszystko zaczyna się już na parkingu przed terminalem, gdzie seria czujników parkingowych OVS wykrywa obecność pojazdów i aktywowania bram oraz szlabanów. OVS to naziemne rozwiązania stosowane na parkingach lotniskowych. Pomagają zapobiegać wypadkom i ułatwiają płynne kierowanie ruchem. Dzięki temu przyczyniają się do efektywnego zarządzania parkingami lotniskowymi oraz zwiększenia ich bezpieczeństwa.

Ochrona ogrodzeń i obszarów otaczających lotniska

Dzięki systemom światłowodowym, zapewniającym pełną detekcję prób wtargnięcia poprzez wykrywanie wibracji wzdłuż ogrodzenia, cały obwód lotniska może być skutecznie chroniony. W newralgicznych miejscach wymagających szczególnej ochrony, takich jak bramy wjazdowe, magazyny paliwa czy hangary lotnicze, dodatkowo są rozmieszczone detektory laserowe REDSCAN, wspierane monitoringiem wizyjnym, pozwalając na jeszcze szybsze i precyzyjniejsze wykrywanie intruzów. Dzięki połączeniu tych systemów możliwe jest skuteczne zabezpieczenie całego obwodu lotniska i uniknięcie powstawania martwych stref.

Systemy światłowodowe, takie jak EchoPoint OPTEX, są niezastąpione na dużych obszarach, gdyż pozwalają na szybką i dokładną lokalizację miejsca wtargnięcia, z dokładnością do 6 m, nawet na dystansach do 100 km. Montowane na ogrodzeniach lub umieszczane pod ziemią, umożliwiają efektywną detekcję wszelkich prób ich przekroczenia, przecięcia czy sforsowania pojazdem. System EchoPoint zapewnia pełną redundancję, co powoduje, że awaria pojedynczego punktu awarii nie wpływa na skuteczność działania całego systemu. Przykładowo, w konfiguracji pętli nawet w przypadku przecięcia światłowodu system dalej działa stabilnie, chroniąc cały obiekt.

Systemy wykrywające przerzucanie paszportów

Zdarza się, że osoby, które przeszły przez kontrolę paszportową, celowo przerzucają swoje dokumenty innym, które jeszcze nie przeszły kontroli. Takie działania stanowią poważne naruszenie procedur bezpieczeństwa. Aby skutecznie je wykrywać i zapobiegać nieuprawnionemu przekraczaniu granic, w obszarze przed i za kontrolą paszportową instalowane są detektory laserowe z serii REDSCAN. Urządzenia z serii REDSCAN Mini umożliwiają wykrywanie nawet niewielkich obiektów i natychmiastową reakcję służb ochrony.

Inne zastosowanie technologii LiDAR na lotniskach to ochrona nieczynnych stanowisk odprawy biletowo-bagażowej tak, aby alarmować o próbach przekroczenia tego krytycznego obszaru przez jakikolwiek przedmiot lub osobę.

Zaawansowana detekcja zagrożeń w strefie oczekiwania przy bramkach

Wejścia do tych miejsc często prowadzą przez schody lub rampy, w których mogą się tworzyć martwe strefy, co ogranicza skuteczność nadzoru. Istnieje ryzyko nieautoryzowanego dostępu do tej przestrzeni poprzez omijanie wcześniejszych punktów kontroli, co może stanowić poważne zagrożenie bezpieczeństwa. Aby skutecznie eliminować takie ryzyko, firma OPTEX rekomenduje instalację

REDSCAN to wielokrotnie nagradzany system ochrony LiDAR, który precyzyjnie identyfikuje rozmiar i odległość poruszających się obiektów.

Wszechstronność detektorów REDSCAN sprawia, że są one wykorzystywane do zabezpieczania różnorodnych obiektów i środowisk przy użyciu niewidzialnych, laserowych ścian lub płaszczyzn obejmujących otwarte przestrzenie, sufity lub dachy.

Wdrożone w tysiącach lokalizacji na całym świecie, odporne na trudne warunki atmosferyczne, zapewniają niezawodność w różnorodnych środowiskach, co czyni je najlepszym rozwiązaniem dla terenów wymagających wysokiego poziomu bezpieczeństwa.

detektorów laserowych wzdłuż schodów i ramp prowadzących do bramek. Pozwalają one na wykrywanie osób próbujących ominąć standardowe procedury, a także szybką reakcję w przypadku incydentów, takich jak upadki pasażerów.

Systemy zapobiegania uszkodzeniom samolotów w hangarach

Hangary lotnicze często charakteryzują się ograniczoną przestrzenią, co wymaga niezwykle precyzyjnego manewrowania samolotami, aby uniknąć kolizji ze ścianami lub innymi obiektami. Instalacja detektorów laserowych znacząco minimalizuje ryzyko takich incydentów. W przypadku zbliżenia samolotu do strefy zagrożenia detektory laserowe uruchamiają alarm, ostrzegając personel i umożliwiając podjęcie odpowiednich działań w celu uniknięcia uszkodzeń.

Systemy wykrywające próby nieautoryzowanego dostępu przez strefę odbioru bagażu

Strefa odbioru bagażu to jednokierunkowy korytarz prowadzący do wyjścia. Zdarzają się próby nielegalnego przedostania się do tej strefy, w chwili otwierania automatycznych drzwi, z ominięciem punktów kontroli bezpieczeństwa. Detektory OPTEX skutecznie rozpoznają takie próby, umożliwiając natychmiastowe uruchomienie alarmu lub powiadomienie służb ochrony. •

OPTEX Security
ul. Sielecka 35, 00-738 Warszawa
optex@optex.com.pl
www.optex.europe.com/pl

PRZYKŁADOWE ROZMIESZCZENIE SYSTEMÓW ZABEZPIECZEŃ NA LOTNISKU

Na grafice przedstawiono schematyczne rozmieszczenie systemów zabezpieczeń stosowanych na lotniskach, obejmujących różne strefy wymagające precyzyjnej detekcji zagrożeń. Skala ilustracji jest poglądowa i może nie oddawać rzeczywistych wymiarów lotniska.

1. EchoPoint DAS

- Zasięg detekcji 100 km
- Analityka klasyfikacji alarmu lub hybrydowy.
- Lokalizacja miejsca naruszenia z dokładnością do 6 m
- Podział na strefy detekcji wielkości od 10 m do 100 km

2. REDSCAN Pro

Czujka LiDAR, detekcja 50 x 100 m, 190 stopni, PoE+, ONVIF, montaż zewnętrzny/wewnętrzny

- Zaawansowane algorytmy zapewniające precyzyjne śledzenie intruzów
- Daleki zasięg, 50 x 100 m, możliwość dostosowania detekcji w pionie lub poziomie
- Wbudowana kamera pomocnicza umożliwiająca podgląd zdarzenia wywołującego alarm
- 8 niezależnych stref detekcji; ustawienia czułości, rozmiaru celu, sygnału wyjściowego

3. REDSCAN mini Pro

Czujka laserowa, wew./zew., 20x20 m, 95°, odporna na trudne warunki środowiskowe.

- Algorytmy rozpoznające rozmiar, położenie, odległość poruszających się obiektów
- Wbudowana kamera Full HD
- Możliwość dostosowania krótkiego zasięgu detekcji w pionie lub poziomie
- 8 niezależnych stref detekcji; ustawienia czułości, rozmiaru celu, sygnału wyjścia.

4. OVS 02-GT

Niezawodny czujnik do wykrywania pojazdów przeznaczony do integracji z systemami otwierającymi bramy i szlabany.

- Montaż nad ziemią
- Detekcja do 35 km/h
- Zasięg detekcji maks. 8 m
- Ignoruje ruch pieszych

Bezpieczne lotniska dzięki Argus PSIM

Telbud S.A. od lat specjalizuje się w tworzeniu zaawansowanych systemów ochrony technicznej (SOT), skutecznie zabezpieczających obiekty infrastruktury krytycznej. Doświadczenie w projektach związanych z bezpieczeństwem granic i ochroną kluczowych instalacji pozwoliło firmie stworzyć rozwiązania idealnie dopasowane do współczesnych wyzwań.

Flagowym produktem firmy jest Argus PSIM, który dzięki wyjątkowym funkcjom sprawdza się również w zabezpieczaniu lotnisk.

Czym wyróżnia się Argus PSIM?

To kompleksowe narzędzie integrujące różnorodne systemy ochrony zostało w pełni opracowane w Polsce. Dzięki temu producent ma absolutną kontrolę nad kodem źródłowym i może dostosować oprogramowanie do potrzeb krajowych odbiorców, w tym polskich Sił Zbrojnych. Siła Argus PSIM tkwi w zdolności łączenia danych z tysięcy czujników – od kamer, przez sensory sejsmiczne i radary, po urządzenia monitorujące ruch radiowy.

Argus PSIM to nie tylko system nadzorujący, ale także inteligentne narzędzie wspomagające podejmowanie decyzji w czasie rzeczywistym. Oprogramowanie integruje i analizuje dane z tysięcy źródeł, z uwzględnieniem uwarunkowań otoczenia, takich jak ukształtowanie terenu czy warunki środowiskowe. Dzięki zaawansowanemu przetwarzaniu informacji system nie tylko nadzoruje rozległe obszary, ale też analizuje zagrożenia i sugeruje optymalne reakcje, co umożliwia operatorom błyskawiczne podejmowanie trafnych decyzji. Te właśnie cechy czynią Argus PSIM idealnym rozwiązaniem dla takich obiektów, jak lotniska, w przypadku których precyzyjna analiza sytuacji i błyskawiczna reakcja na zagrożenie mogą decydować o bezpieczeństwie, zdrowiu i życiu ludzi.

Argus PSIM – ochrona granic państwa i firm

Argus PSIM stanowi fundament rozbudowanych systemów ochrony tworzonych w Telbud S.A. Obecnie system sprawdza się m.in. na granicy z Federacją Rosyjską oraz z obwodem królewieckim. Jest wdrażany także na granicy z Białorusią. Oczywiście Argus PSIM służy również klientom komercyjnym z takich sektorów, jak przemysł paliwowo-energetyczny. Wdrożony w Polskiej Agencji Żeglugi Powietrznej wspiera ochronę obiektów kluczowych dla bezpiecznego ruchu lotniczego w Polsce.

Nowoczesne porty lotnicze to rozległe kompleksy, gdzie sprawne zarządzanie informacją i szybka reakcja bezpośrednio wpływają na bezpieczeństwo pasażerów. Argus PSIM, sprawdzony już w ochronie granic oraz w sektorze energetycznym, doskonale odpowiada na potrzeby obiektów lotniczych. Integracja różnorodnych źródeł danych pozwala nie tylko monitorować przestrzeń powietrzną, ale też wykrywać zagrożenia związane z ruchem dronów, chroniąc kluczowe elementy infrastruktury lotniska – od wież kontroli po terminale.

Co więcej, inteligentne algorytmy Argus PSIM dostosowują się do zmieniających się warunków. System uczy się charakterystyki otoczenia, eliminując nieuzasadnione alarmy i skupiając się na rzeczywistych zagrożeniach. Skalowalność systemu umożliwia jego dopasowanie do konkretnych wymagań – małych lotnisk regionalnych i międzynarodowych hubów.

Integracja z systemami antydronowymi

Telbud S.A., rozwijając swoje narzędzia, łączy dotychczasowe doświadczenie z najnowszymi osiągnięciami w dziedzinie analizy obrazu, sięgając m.in. po algorytmy sztucznej inteligencji oraz zaawansowane metody szyfrowania plików. Połączenie Argus PSIM z systemami antydronowymi może chronić obiekty, takie jak lotniska, przed inwigilacją i ewentualnym atakiem dronów. Takie podejście zapewnia nie tylko wysoki poziom bezpieczeństwa, ale też elastyczność i możliwość ciągłej modernizacji – niezbędne cechy w obliczu dynamicznie zmieniających się zagrożeń.

Sytuacja geopolityczna powoduje, że lotniska są częstym celem różnego rodzaju ataków. Ich ochrona wymaga sprawdzonych narzędzi, takich jak Argus PSIM, będących innowacyjną odpowiedzią na wyzwania związane z bezpieczeństwem obiektów kluczowych dla funkcjonowania państwa i gospodarki. •

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

POLON-ALFA

ADRESOWALNY
KOMPAKTOWY

POLON 3000

SYSTEM SYGNALIZACJI POŻAROWEJ

NIEZAWODNOŚĆ
System szybko wykrywa zagrożenie pożarowe, minimalizując ryzyko strat.

ŁATWOŚĆ INSTALACJI
Kompaktowa budowa pozwala na szybki i nieskomplikowany montaż,
a także oszczędność miejsca.

SKALOWALNOŚĆ
Możliwość dostosowania do specyficznych potrzeb obiektu,
co gwarantuje maksymalną ochronę.

OPŁACALNOŚĆ
POLON 3000 to przystępna inwestycja w bezpieczeństwo,
która zwraca się w postaci bezcennego spokoju.

Zadbaj o bezpieczeństwo swojego obiektu już dziś!

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

Ochrona infrastruktury krytycznej wciąż nie jest doskonała

Nie ma wątpliwości, że żyjemy w czasach, kiedy infrastruktura krytyczna jest narażona na sabotaż. Stopień zagrożenia jest wysoki i nie wystarczy przygotować się na zagrożenia. Trzeba je uprzedzać.

Krzysztof Łuczak


Mobilna wieża do monitoringu

Wprawdzie obiekty o znaczeniu strategicznym są już wyposażone w wielopoziomowe systemy ochrony, jednak zawsze może być lepiej.

Mobilne urządzenia monitorujące mogą zwiększać bezpieczeństwo podczas tymczasowych prac w terenie, poza obszarem dozorowanym przez system kamer. Sprawdzają się podczas napraw gazociągów, sieci elektroenergetycznych, infrastruktury przesyłowej w rafineriach, infrastruktury kolejowej czy portów lotniczych. Mogą również wpływać na podniesienie poziomu bezpieczeństwa w obiektach o dużej dynamice zmian otoczenia. W sytuacji, gdy punkty obserwacyjne trzeba przenieść szybko, ale z zapewnieniem ciągłości pracy systemu.


System Reconeyez

Takie działania potrzebne są np. w portach przeładunkowych z setkami kontenerów czy wagonów. Częsta reorganizacja takich przestrzeni powoduje, że tradycyjna instalacja kamer monitoringu nie spełni swoich zadań.

Mobilna wieża do monitoringu wizyjnego jest w stanie zapewnić monitoring miejsc pozbawionych zasilania, a nieprzerwaną pracę gwarantuje wielopoziomowy, zarządzalny system zasilania (akumulatory, panele solarne, agregaty, turbiny wiatrowe czy ogniwa paliwowe).

Bezdyskusyjną zaletą tego rozwiązania jest **modułowość,** która sprawia, że może być ono platformą dla innych systemów bezpieczeństwa. Oświetlacze LED, kamery termowizyjne, megafony z dwukierunkową komunikacją, radar wspierający, analityka obrazu AI czy zamontowanie **stacji dokującej dla drona** – to kilka z dostępnych opcji. Komunikacja GSM, radiowa lub satelitarna pozwala na stałe połączenie z wieżą, w każdym miejscu w Polsce.

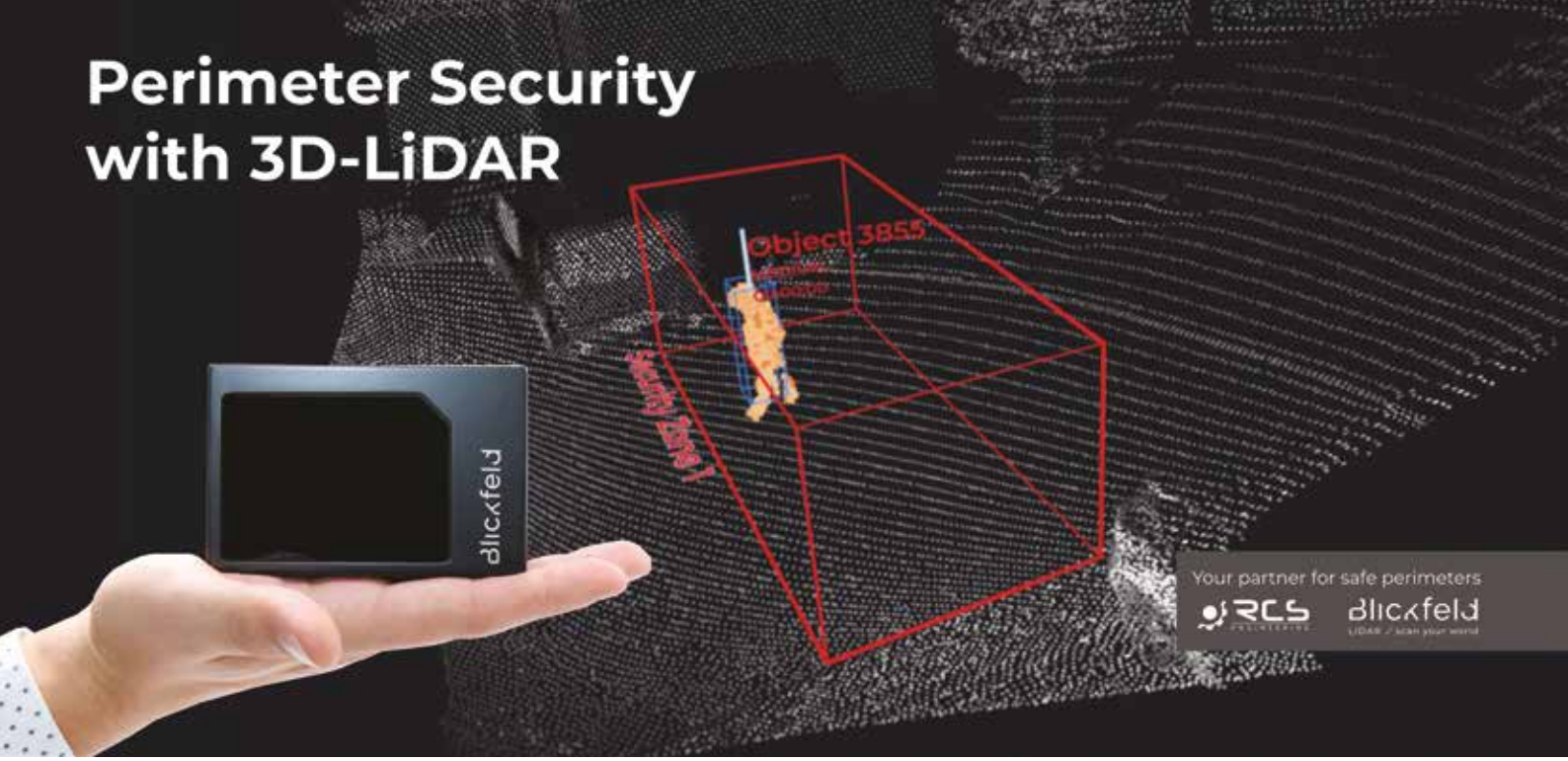
Idealnym przykładem jest mobilna wieża do monitoringu produkowana przez **Uniforce.** Po analizie dotychczasowych rozwiązań dostępnych na polskim rynku powstało rozwiązanie, które łączy zalety wież większości producentów, eliminując przy tym wykryte wady. Ta wersja wieży jest kompromisem między funkcjonalnością a ceną, przy zachowaniu fundamentalnych potrzeb dotyczących jakości obrazu oraz niezależności energetycznej.

Producent zapewnia możliwość dostosowania do różnorodnych potrzeb, a mając wieloletnie doświadczenie w systemach telewizji dozorowej, dronach i nowoczesnych technologiach ochrony w infrastrukturze krytycznej, służbach mundurowych i instytucjach wojskowych, wie dobrze, co doradzić.

A co, jeśli należy zabezpieczyć odcinek obwodu pozbawionego infrastruktury elektrycznej czy ogrodzenia? W takim przypadku sprawdzi się **Reconeyez** – produkowany w Estonii perymetryczny system z czujnikami PIR, kamerami i analityką obrazu, przeznaczony do ochrony infrastruktury krytycznej i obiektów strategicznych. Jest doskonałym uzupełnieniem kilkuetapowego systemu ochrony obwodowej, tworząc sieć czujników w strukturze gwiazdy, lub liniowej, która informuje użytkownika o wykryciu określonych zdarzeń, np. pojawieniu się osoby lub pojazdu. Odbywa się to poprzez wykonanie i przesłanie zdjęć. Niespotykana praca do **400 dni** na akumulatorach to jedno, jednak kluczową zaletą systemu jest analityka obrazu, która z bardzo dużą dokładnością eliminuje fałszywe alarmy.

W Uniforce umożliwiamy przeprowadzenie praktycznych testów, w trakcie których sprawdzane są określone scenariusze działania. •

Uniforce
ul. Bodawska 11
61-309 Poznań
www.uniforce.pl



Świat w chmurach punktów

Szelest liści pod butami. Stawiasz krok, drugi. Patrzysz w dal. Na horyzoncie nic. Szlak wijący się w górę jak niemiecka precyzja. Okazuje się, że twój wzrok to średniowiecze. Nieodporny na mgłę, deszcz i oślepiający blask słońca. Wokół ciebie szczyty Alp Bawarskich, jodły i powietrze, które jeszcze drży od dekretów Ludwika II. Kawałek dalej Monachium, a tam w laboratoriach pełnych laserowego światła i ultradokładnych urządzeń powstaje coś, co widzi więcej, czuje więcej, skanuje rzeczywistość szybciej niż twoje oko.

LiDAR. Taki, co ci powie, czy to w oddali jest miś, czy kamień. Blickfeld. Znaczy „pole widzenia" po niemiecku, ale czy to w ogóle wystarczy? To raczej pole przewidzenia, pole opanowania przestrzeni, pole zmieniania świata w chmurę punktów, które rozumieją więcej. Pole widzenia w praktyce staje się polem dominacji nad otaczającą rzeczywistością. To, co dla ciebie jest ciemnością, dla niego jest mapą.

Lidar Blickfeld Qb2

Qb2 to inteligentny sensor 3D LiDAR, który łączy precyzyjne skanowanie z zaawansowanym przetwarzaniem danych bezpośrednio na urządzeniu. Dzięki wbudowanemu procesorowi oprogramowanie analityczne działa bezpośrednio w skanerze, eliminując potrzebę stosowania dodatkowych komputerów, upraszczając infrastrukturę całego systemu i redukując koszty licencji oraz zasilania.

Qb2 oferuje elastyczne pole widzenia oraz konfigurowalny wzór skanowania, co pozwala na dostosowanie sensora do różnych scenariuszy aplikacyjnych niezależnie od specyfiki monitorowanego obszaru. Qb2 zapewnia wysoką rozdzielczość i dokładność otrzymanych danych. Zaprojektowany z myślą o pracy w trudnych warunkach Qb2 charakteryzuje się solidną konstrukcją z klasą ochrony IP67, co gwarantuje niezawodność. Sensor działa w szerokim zakresie temperatur od -30°C do 60°C, co czyni go idealnym rozwiązaniem w różnych środowiskach pracy – nawet wysoko w górach.

Obszary zastosowania

Tradycyjne systemy, takie jak kamery czy czujniki ruchu, często są ograniczone przez warunki pogodowe lub oświetlenie. Qb2 działa niezależnie od pory dnia, mgły czy opadów atmosferycznych, tworząc trójwymiarową barierę, która wykrywa wszelkie próby wtargnięcia na teren obiektu, ignorując przy tym ruchy nieistotne, np. zwierzęta czy liście poruszane przez wiatr. Qb2 może pełnić funkcję dodatkowego zabezpieczenia przy bramach wjazdowych, wejściach do budynków czy tunelach logistycznych. Współpracując z systemami zarządzania dostępem, jest w stanie wykrywać nieautoryzowane próby przekroczenia bram i szlabanów zarówno przez ludzi, jak i pojazdy.

W świecie, gdzie technologia bezpieczeństwa musi działać szybciej niż zagrożenia, wchodzi Lidar Blickfeld, cały na laserowo. Jego rola to nie tylko wykrywanie, ale też analiza zdarzeń w przestrzeni, gdzie precyzja oznacza najwyższe bezpieczeństwo. To, co dla ciebie jest ciemnością, dla niego jest mapą otoczenia. Tak jak w Alpach Bawarskich, gdzie górskie szlaki prowadzą tych, którzy rozumieją przestrzeń, tak LiDAR Blickfeld prowadzi twój świat ku precyzji i bezpieczeństwu. To więcej niż sensor – to przewodnik w świecie, który nie wybacza błędów. •

Więcej: **https://rcse.pl/lidar/**

RCS Engineering
ul. Topolowa 8
62-030 Luboń
biuro@rcse.pl

AtlasPRO i stacja dokująca AtlasNEST

Drony w ochronie – jeszcze mrzonka czy już fakt?

Na palcach jednej ręki można policzyć branże rozwijające się tak dynamicznie, jak branża producentów dronów i usług z nimi związanych. Są już latające taksówki, drony dostarczające przesyłki kurierskie czy drony patrolowe. Stosowanie tych bezzałogowców mogłoby być bardziej popularne, ale, jak to często bywa, nie technologia, lecz prawo stanowi ograniczenie.

Krzysztof Łuczak

Jednak rynek nie śpi i niczym kropla drążąca skałę, niejednokrotnie wymusza na prawodawcy aktualizacje przepisów. I tak stało się tym razem. Dzięki nowelizacji Ustawy Prawo lotnicze od 2025 r. możliwe jest używanie dronów w zastosowaniach związanych z ochroną infrastruktury krytycznej. Bezzałogowce mogą wykonywać zadania niemożliwe dla najbardziej wyszkolonych pracowników ochrony i patrolować miejsca nieosiągalne dla systemów monitoringu wizyjnego.

Mówiąc o dronach i bezpieczeństwie, nie sposób nie wspomnieć o wątpliwościach związanych z użytkowaniem dronów pochodzących z Chin. Rekomendacje Rządowego Centrum Bezpieczeństwa ostrzegają przed wykorzystywaniem tych urządzeń i zalecają staranny wybór dostawcy. Być może rekomendacja zamieni się w przepis, jak miało to miejsce w przypadku urządzeń telekomunikacyjnych firmy Huawei. Na szczęście rynek dronów w USA i krajach europejskich dynamicznie się rozwija, a producenci odrobili zadanie domowe, stawiając cyberbezpieczeństwo na wysokiej pozycji priorytetów.

Jednym z najbardziej interesujących rozwiązań dronów zza Atlantyku jest model **Skydio X10,** który z powodzeniem sprawdza się w zadaniach związanych z ochroną obiektów oraz w misjach inspekcyjnych. Solidna i przemyślana konstrukcja została opracowana z myślą o służbach mundurowych, jednakże ten model doskonale sprawdza się w ochronie obiektów infrastruktury krytycznej. Poza potwierdzoną w testach umiejętnością samodzielnego unikania przeszkód Skydio X10 jest wyposażony w dualną kamerę (światła widzialnego i termowizję) o bardzo dobrych parametrach. Pozwala to na wykrywanie zdarzeń z kilkuset metrów. Ma możliwość szybkiego startu z ręki i lądowania na niej. Funkcja „Scout" pozwala dronowi utrzymywać stałą pozycję względem aparatury sterującej, nawet jeśli pilot znajduje się w jadącym pojeździe.

Skydio X10 i stacje dokujące

Skydio X10 idealnie sprawdza się również do inspekcji obiektów przemysłowych, infrastruktury telekomunikacyjnej, energetycznej, gazowej czy turbin wiatrowych, czyli tych miejsc, które ze względu na swoją specyfikę są trudne do nadzorowania. Dodatkowa aplikacja 3D Scan umożliwia szybkie i precyzyjne tworzenie modeli trójwymiarowych, co przydaje się bardzo podczas prac inspekcyjnych.

Kolejnym wartym uwagi rozwiązaniem jest zaawansowany system dronowy produkowany przez łotewską firmę **Atlas Aerospace**, która w swojej ofercie ma unikatowe rozwiązanie przeznaczone do ochrony obiektów. To drony **AtlasPRO** współpracujące ze stacją dokującą **AtlasNEST.** Największym wyróżnikiem stacji jest automatyczna wymiana akumulatorów BSP, co pozwala na wznowienie lotu już po 2 minutach. Oszczędza to czas kilkudziesięciu minut ładowania i znacząco podnosi wskaźnik ciągłości misji. Instalacja jednej lub kilku stacji dokujących z dronem pozwala na automatyczną i szybką kontrolę perymetru. Lecący z prędkością do 70 km/h AtlasPRO z łatwością „dogoni" każdego intruza i zapewni obraz na tyle długo, by przejął go patrol.

Już niedługo drony ochrony regularnie patrolujące tereny infrastruktury krytycznej nie będą nikogo dziwić!

Atlas oraz Skydio, a także drony innych sprawdzonych producentów znajdują się w ofercie **Uniforce.** Regularnie organizujemy pokazy, szkolenia oraz testy najnowszych systemów dronowych dla klientów infrastruktury krytycznej, służb mundurowych i Wojska Polskiego. •

Uniforce
ul. Bodawska 11
61-309 Poznań
www.uniforce.pl

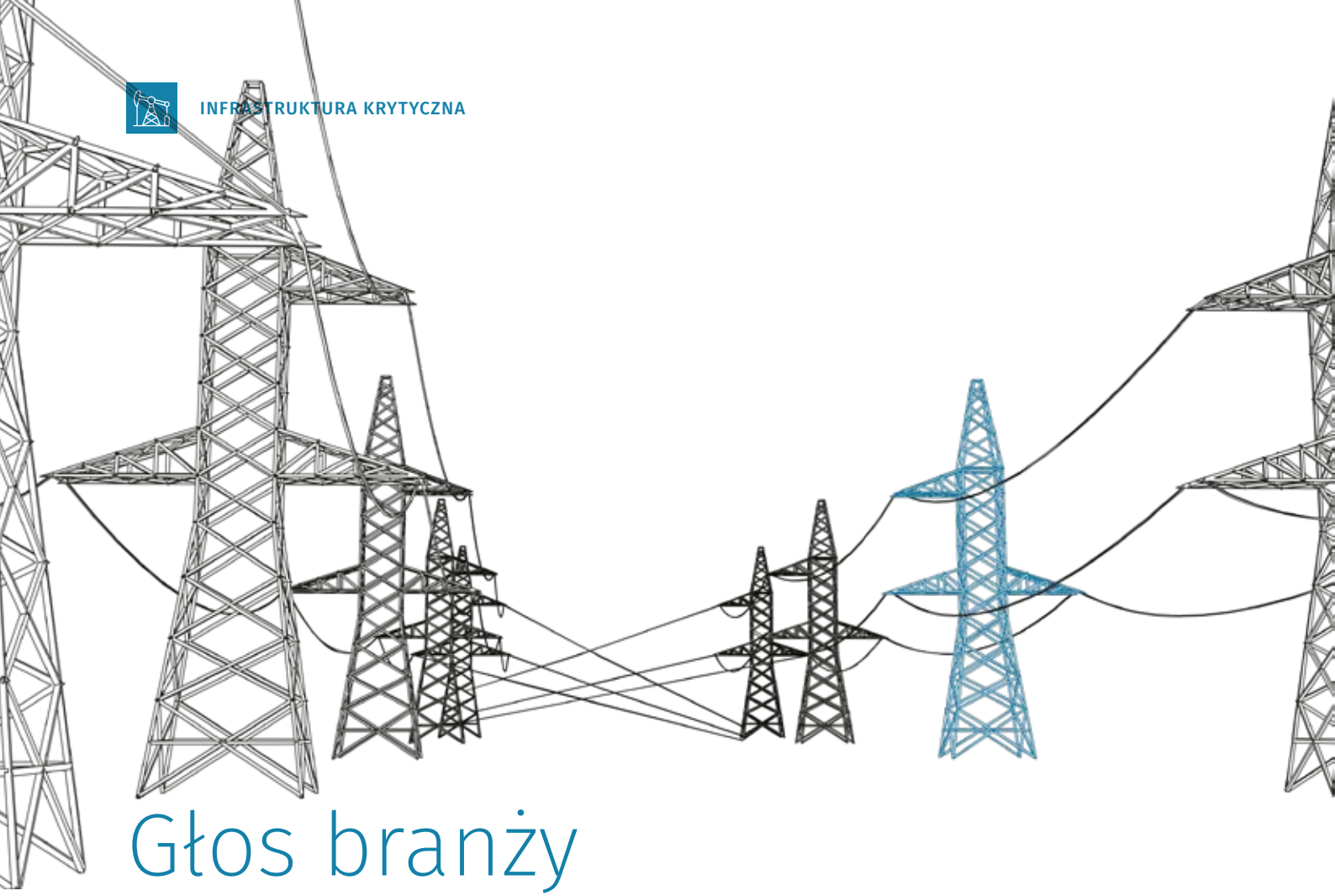
Dahua IVD5148-2I to zaawansowane rozwiązanie do analizy obrazu z użyciem algorytmów sztucznej inteligencji. Do urządzenia możliwe jest podłączenie do 48 dowolnych strumieni wideo i skorzystania z takich funkcji jak detekcja człowieka lub pojazdu, rozpoznawanie twarzy a także szeregu wyspecjalizowanych detekcji z myślą o konkretnej branży.
Wyposażone w 64-bitowy, wysokowydajny procesor wielordzeniowy, zapewnia maksymalną przepustowość do 256 Mbps dla strumieni przychodzących, nagrywania i wychodzących.

- **Analiza AI:** Obsługuje do 32 kanałów inteligentnej analizy wideo jednocześnie.
- **Rozpoznawanie twarzy:** Możliwość zarządzania 100 bazami danych twarzy z łączną pojemnością do 500 000 zdjęć.
- **AcuPick:** Funkcja umożliwiająca szybkie i precyzyjne wyszukiwanie obiektów w dużych zbiorach danych wideo.
- **Kompatybilność:** Współpracuje z kamerami innych producentów poprzez protokoły ONVIF, RTSP, Sony, Panasonic, Axis, Arecont, Pelco, Canon i Samsung.
- **Interfejsy wideo:** 1 wyjście VGA i 2 wyjścia HDMI 4K.

*) Wygląd oraz specyfikacja urządzeń może ulec zmianom bez uprzedniego powiadomienia

Dahua Technology Poland Sp. z o.o.

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



Głos branży

Bezpieczeństwo obiektów infrastruktury krytycznej to jedno z najważniejszych wyzwań współczesnego świata. W dobie rosnących zagrożeń, zarówno cybernetycznych, jak i fizycznych, konieczne jest wdrażanie skutecznych strategii ochrony. Eksperci z branży security dzielą się swoją wiedzą i doświadczeniem, omawiając najlepsze praktyki oraz innowacyjne rozwiązania w zakresie zabezpieczeń.

Odpowiedni dobór systemów zabezpieczeń

NATALIA BRZOZOWSKA, BCS

Współczesny świat opiera się na funkcjonowaniu kluczowych sektorów, takich jak energetyka, transport, łączność czy ochrona zdrowia. Infrastruktura krytyczna jest narażona na różnorodne zagrożenia – od cyberataków, przez akty sabotażu, po katastrofy naturalne. W związku z tym odpowiedni dobór systemów zabezpieczeń jest nie tylko priorytetem, ale wręcz koniecznością dla zapewnienia stabilności i bezpieczeństwa państwa.

Wybór odpowiednich zabezpieczeń dla infrastruktury krytycznej powinien uwzględniać zarówno ochronę fizyczną, jak i cyberbezpieczeństwo. Są to m.in. monitoring wizyjny, bariery mechaniczne, odpowiednio przeszkolony personel, odpowiednie narzędzia cyfrowe, takie jak firewall, szyfrowanie danych oraz mechanizmy wykrywania zagrożeń w czasie rzeczywistym.

Nowoczesne narzędzia to nie tylko zaawansowane mechanizmy ochrony nagranych materiałów, umożliwiające szyfrowanie danych, zabezpieczające przed ich utratą lub zmanipulowaniem, ale także w przypadku awarii jednego elementu możliwość przełączenia się na zapasowy moduł, co gwarantuje ciągłość działania. Oszczędność miejsca na dyskach zapewnia kompresja danych bez utraty jakości nagrań. Ponadto systemy zabezpieczeń są projektowane tak, aby działać w sytuacjach niestabilnej sieci lub awarii zasilania, wykorzystując alternatywne źródła energii oraz mechanizmy automatycznego przełączania na tryb awaryjny.

Równie istotnym aspektem jest wybór dostawcy zabezpieczeń. To od niego zależy jakość rozwiązań, ich niezawodność oraz poziom wsparcia technicznego. Dlatego dokonując tego wyboru, warto zwrócić uwagę na:

1. **doświadczenie i renomę** – firmy z wieloletnim doświadczeniem i referencjami w sektorze bezpieczeństwa mają

sprawdzone rozwiązania i lepiej rozumieją specyficzne zagrożenia,

2. **kompatybilność i skalowalność** – dostawca powinien oferować rozwiązania, które można łatwo dostosować do zmieniających się potrzeb i integrować z istniejącą infrastrukturą,
3. **wsparcie techniczne i serwis** – kluczowe jest zapewnienie ciągłości działania mechanizmów zabezpieczeń, dlatego dostawca powinien gwarantować szybkie wsparcie techniczne oraz regularne aktualizacje oprogramowania,
4. **zgodność z regulacjami prawnymi** – rozwiązania muszą spełniać krajowe i międzynarodowe standardy w zakresie bezpieczeństwa, np. normy ISO czy wytyczne krajowych organów ds. cyberbezpieczeństwa.

Skuteczność ochrony zależy nie tylko od jakości oferowanych przez dostawcę narzędzi czy usług, ale też od tego, czy może on zagwarantować niezawodność swoich rozwiązań, ich zgodność z regulacjami oraz czy oferuje odpowiedni poziom wsparcia technicznego. Integrując linię produktową BCS Ultra z systemami zabezpieczeń, zyskujemy gwarancję ochrony kluczowych zasobów przed rosnącymi zagrożeniami współczesnego świata. •

Długofalowa perspektywa ochrony obiektu

ARTUR NOWAKOWSKI, Linc Polska

Budowa strategicznych obiektów to duże wyzwanie zarówno dla inwestora, projektanta, jak i wykonawcy. Realizacja inwestycji odbywa się tu i teraz, z uwzględnieniem znajomości obecnie dostępnych technik, występujących zagrożeń oraz wiedzy o tym, jak im przeciwdziałać. Proces realizacji takiego przedsięwzięcia jest długotrwały i może się zdarzyć, że to, co na początku tego procesu było rozwiązaniem standardowym, sprawdzonym, po kilku latach będzie niewystarczające. Dobrym tego przykładem jest dynamiczny wzrost cyberataków połączony ze zmianą mechanizmów ich działania. Podobnie wygląda sprawa z zastosowaniem dronów, które jeszcze kilka lat temu były raczej zabawką, a obecnie stanowią poważne narzędzie wykorzystywane w sektorze militarnym.

Podstawą skutecznej ochrony obiektów strategicznych jest jej wielowarstwowość. Wystarczy spojrzeć, jak wygląda ochrona naszych wschodnich granic. Pierwszą warstwę ochronną stanowią systemy detekcyjne, wykrywające zbliżające się obiekty (ludzi). Następną warstwą jest płot, który stanowi rzeczywistą, fizyczną barierę, wyposażoną w dodatkowe sensory informujące o próbach jego sforsowania. Po wewnętrznej stronie strefy chronionej zainstalowanych jest również wiele systemów detekcyjnych. Ich zadaniem jest wykrycie i śledzenie intruza, który sforsował barierę fizyczną. Dopiero połączenie tych wszystkich elementów daje czas na wykrycie niepożądanego obiektu i monitorowanie jego pozycji. Dzięki temu można odpowiednio reagować, a jeżeli intruz przełamie zabezpieczenia, można go śledzić w celu zatrzymania na terenie chronionego obszaru. Tak zaprojektowany system daje pewność ochrony przed nieproszonymi gośćmi.

Kolejna sprawa to dobór odpowiednich urządzeń detekcyjnych tak, aby były one niezależne od warunków oświetleniowych, atmosferycznych i wzajemnie się uzupełniały. Należy mieć na względzie to, że w ciągu kilku lat realizacji planowanej inwestycji mogą pojawić się nowe, doskonalsze rozwiązania. Można to zauważyć, analizując np. zastosowanie sztucznej inteligencji w systemach dozoru wizyjnego i detekcyjnych.

Ochrona przestrzeni powietrznej jest równie istotna. Zagrożenia związane z wykorzystaniem dronów mogą stanowić nie lada wyzwanie dla obiektów infrastruktury krytycznej czy cywilnych, a nawet stanowić bezpośrednie zagrożenie dla zdrowia i życia ludzkiego.

W tym wypadku również konieczna jest wielowarstwowość ochrony. Można zapewnić skuteczny system detekcji oparty m.in. na rozwiązaniach radarowych, które wykryją zagrożenie. Skuteczny system musi być w stanie automatycznie odróżnić dron od np. ptaków i uruchamiać alarm tylko w uzasadnionej sytuacji. Ponadto warto uzupełnić zabezpieczenia o system z detektorem RF do identyfikacji znanych dronów, który umożliwia namierzenie operatora.

Długo wyczekiwaną zmianą była możliwość legalnej neutralizacji bezzałogowego statku powietrznego. Tegoroczna nowelizacja ustawy Prawo Lotnicze reguluje tę kwestię i uprawnia wiele podmiotów do neutralizacji zagrożeń, jakie potencjalnie mogą nieść drony. Dzięki temu obsługa, np. lotniska, wyposażona w odpowiedni sprzęt może podejmować próbę przejęcia i neutralizacji drona, a ewentualna odpowiedzialność za szkody spadnie na operatora.

Warto zaznaczyć, że tylko współpraca z dostawcami, którzy mają wieloletnie doświadczenie, szeroką wiedzę i możliwości techniczne, daje pewność, że wybrane systemy będą skuteczne i dopasowane do zagrożeń. •

Infrastruktura krytyczna w czasach turbulencji

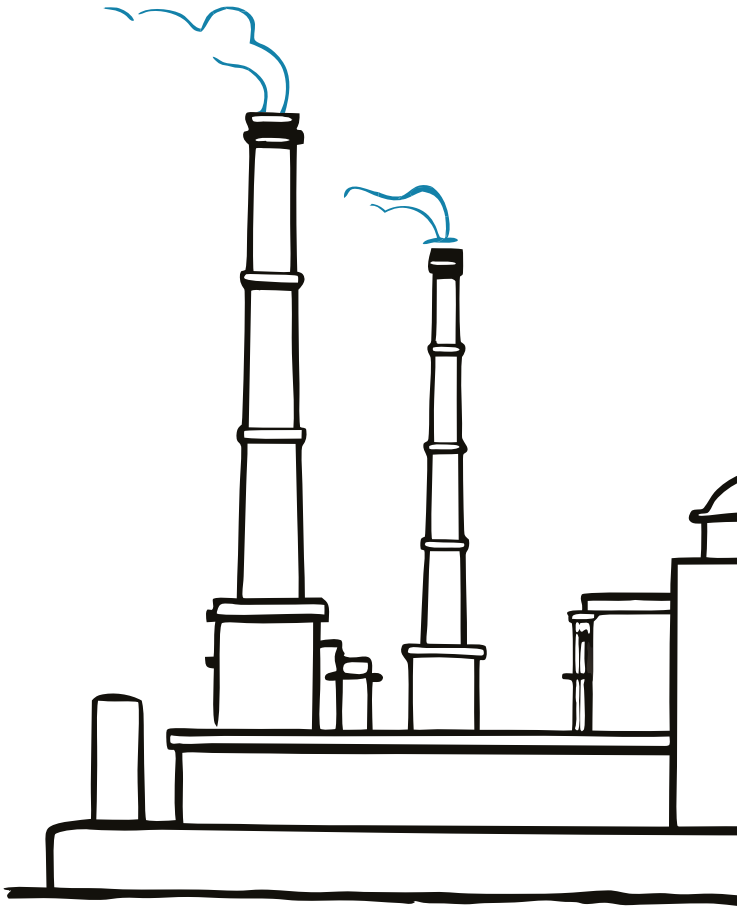
JACEK GRZECHOWIAK, Riskresponse

Sprawne funkcjonowanie wszystkich obiektów infrastruktury krytycznej ma bezpośredni wpływ na życie całego społeczeństwa, ale czy na pewno na to, co jest IK, powinniśmy patrzeć wyłącznie przez pryzmat przepisów? Widzimy przecież wyraźnie, że wektor ataku skierowany jest nie tylko na typowe obiekty IK. Stąd wniosek, że perspektywa naszego przeciwnika jest dużo szersza. Wiemy też, że wektory ataku obejmują zarówno technologie, jak i zachowania człowieka. W naszym przypadku będą to przede wszystkim pracownicy ochrony. A mamy przecież świeże przykłady, że na tym poziomie lokowane są działania obcych służb specjalnych. Przykłady z Berlina i Oslo są wyjątkowo wymowne. Siłą rzeczy – dziś jak nigdy wcześniej – musimy wziąć pod uwagę aktualną sytuację geopolityczną, w której znaleźliśmy się wraz z rozpoczęciem agresji Rosji w Ukrainie, a która powinna skłaniać nas do analizy zagrożeń zarówno wewnętrznych, jak i tych ulokowanych w bliższym i dalszym sąsiedztwie naszych obiektów.

Ilustracje: freepik

Dlatego inwestycje w systemy zabezpieczeń technicznych muszą iść w parze z inwestycjami w świadomość bezpieczeństwa, rozumianą również jako umiejętność rozpoznawania zagrożeń szpiegowskich i sabotażowych. A to dziś jest obszar wciąż niedoceniany, któremu zbyt mało poświęcamy uwagi, zwłaszcza że jest – chyba nawet dość intensywnie – wykorzystywany przez przeciwnika. Ostatnie incydenty identyfikowane jako chuligańskie wcale nie muszą mieć jedynie takiego wymiaru. Zwłaszcza że już same informacje medialne pokazują, że mamy rozpoznanie i przygotowanie, wysoki poziom determinacji (vide: „odbijanie" ujętych grafficiarzy) i wykorzystywanie specjalistycznych narzędzi. A to już nie wygląda amatorsko.

Skoro mamy od lat do czynienia z agenturą proxy, to musimy przyjąć, że zarówno dane z rozpoznania, jak i technologia wejścia na teren, mogą być udostępnione potencjalnym dywersantom, a nawet że w grupie takich „grafficiarzy" już jest agent proxy. Duża część zagrożeń może być ujawniana przez pracowników ochrony i w praktyce tak się dzieje. Jednak te „sukcesy" nie powinny nas usypiać. •



Modernizacja i zastosowanie nowoczesnej technologii

TOMASZ GOLJASZEWSKI,
Hikvision Poland

Ostanie dwa lata pokazały, że powinniśmy dbać nie tylko o zwiększenie skuteczności systemów bezpieczeństwa w obiektach infrastruktury krytycznej, ale także we wszystkich przestrzeniach, gdzie gromadzą się większe grupy ludzi. Podejrzane podpalenia zarówno w naszym kraju, jak i krajach sąsiednich pokazały, że służby odpowiedzialne za bezpieczeństwo muszą zwiększyć czujność i reagować naprawdę szybko. Ataki na takie obiekty, jak sklep IKEA w Wilnie, hale kupieckie na Marywilskiej w Warszawie czy autobusy praskiego transportu publicznego w Czechach, może nie są istotne z punktu widzenia strategicznego dla danego kraju, ale mogą stanowić istotne zagrożenia życia i zdrowia ludzi. A co ważniejsze, stają się niebezpiecznym narzędziem oddziaływania socjotechnicznego na społeczeństwo. W tej sytuacji wymagania w stosunku do systemów zabezpieczeń nigdy nie były tak wysokie jak teraz, a temat sprawności i skuteczności tych systemów powinien być traktowany bardzo poważnie.

Wszystkie systemy, które są tylko straszakami i od wielu lat jedynie udają, że cokolwiek ochraniają, powinny zostać zmodernizowane. Przy okazji modernizacji należy sprawdzić, czy na przestrzeni lat nie powstała potrzeba zapewnienia lepszego pokrycia i zwiększenia rozpoznawalności osób wchodzących w chroniony obszar. W większym stopniu powinno się stosować nowe urządzenia, ponieważ ich cena z roku na rok staje się zdecydowanie bardziej przystępna. Takie rozwiązania, jak kamery bispektralne czy kamery wizyjne oferujące skuteczną analizę obrazu w warunkach zarówno dziennych, jak i nocnych, powinny stać się standardem, aby zapewnić odpowiednie narzędzia operatorom systemów lub służbom bezpieczeństwa. •

Kluczowe aspekty zabezpieczenia IK

MARCIN FRANCZUK,
Zakład Unieszkodliwiania
Odpadów Promieniotwórczych

Bezpieczne funkcjonowanie infrastruktury krytycznej wymaga skoordynowanego podejścia, które łączy aspekty techniczne ze współpracą operacyjną. Istotnym elementem jest systematyczne ocenianie ryzyka, przeprowadzanie regularnych audytów oraz tworzenie i testowanie planów kryzysowych, co umożliwia szybką reakcję na incydenty, zarówno te fizyczne, jak i cybernetyczne.

Wprowadzenie zaawansowanych systemów monitorowania, które wykorzystują sensory, kamery termograficzne oraz światłowody, pozwala na nieprzerwaną obserwację infrastruktury krytycznej. Równocześnie rosnące zagrożenia związane z dronami używanymi do inwigilacji, ataków terrorystycznych czy sabotażu wymagają wprowadzenia systemów zwalczania bezzałogowych statków powietrznych (C-UAS), zdolnych do wykrywania, identyfikacji i neutralizacji nieautoryzowanych dronów.

Równie ważna jest współpraca operatorów infrastruktury z instytucjami wywiadowczymi, takimi jak ABW. Wymiana informacji dotyczących nietypowych zdarzeń oraz analizowanie sygnałów alarmowych umożliwiają wczesne wykrywanie prób szpiegostwa lub sabotażu. Organizowanie wspólnych szkoleń, konsultacji oraz integracja systemów IT/OT przyczyniają się do stworzenia efektywnych procedur reagowania oraz wzmacniają

obronę IK. Podstawy prawne ochrony infrastruktury krytycznej zostały określone w Narodowym Programie Ochrony Infrastruktury Krytycznej oraz w ustawach regulujących działalność ABW, co umożliwia efektywną współpracę pomiędzy służbami a właścicielami infrastruktury.

Najważniejsze zadania zapewniające funkcjonowanie infrastruktury krytycznej to:

- monitorowanie i analizowanie ryzyka w sposób ciągły,
- wdrażanie nowoczesnych rozwiązań, w tym systemów C-UAS,
- ścisła współpraca operacyjna z instytucjami wywiadowczymi,
- aktualizacja przepisów prawnych i integracja systemów ochronnych. •

Zintegrowane podejście do ochrony IK

MAREK BARTKOWSKI, Polpharma

Infrastruktura krytyczna stanowi fundament funkcjonowania nowoczesnych społeczeństw. Jej ochrona jest priorytetem, szczególnie w obliczu rosnących zagrożeń zarówno fizycznych, jak i cyfrowych. W Polsce regulacje dotyczące zarządzania kryzysowego oraz rozporządzenia związane z tworzeniem planów ochrony IK wyznaczają ramy prawne i operacyjne dla jej zabezpieczenia. Aby zagwarantować bezpieczne funkcjonowanie infrastruktury krytycznej, należy zadbać o to, by w organizacji zostały wprowadzone najlepsze praktyki. Są nimi przede wszystkim:

- **Ocena ryzyka i analiza zagrożeń** dla danego obiektów IK – regularne przeprowadzanie ocen ryzyka i ich analiza pozwala na zrozumienie, jakie elementy tej infrastruktury są najbardziej narażone i jakie konsekwencje mogą mieć ewentualnie incydenty.
- **Zabezpieczenia cyfrowe,** czyli m.in. implementacja zaawansowanych systemów ochrony przed cyberatakami, w tym firewalli, systemów detekcji włamań (IDS), szyfrowania danych oraz regularnych aktualizacji oprogramowania.
- **Regularne szkolenia** i podnoszenie świadomości personelu dotyczące najlepszych praktyk w zakresie bezpieczeństwa, rozpoznawania zagrożeń i reagowania na incydenty są kluczowe dla minimalizacji ryzyka błędu ludzkiego. Bardzo ważnym elementem jest też opracowanie i regularne testowanie planów reakcji na incydenty w celu szybkiego odzyskania funkcjonalności po potencjalnym incydencie.
- **Planowanie reakcji na incydenty,** czyli opracowanie i regularne testowanie planów reakcji na incydenty, które umożliwiają szybkie i skuteczne działanie w przypadku wystąpienia zagrożenia.
- **Redundancja i ciągłość działania** umożliwiają szybkie odzyskiwanie funkcjonalności po potencjalnym incydencie.
- **Aktywna współpraca i wymiana informacji** z innymi podmiotami, w tym z agencjami rządowymi, sektorem prywatnym i organizacjami międzynarodowymi, w celu wymiany informacji o zagrożeniach i najlepszych praktykach. Śledzenie najnowszych technologii i inwestowanie w rozwiązania, które mogą poprawić bezpieczeństwo infrastruktury.
- **Monitorowanie systemów** pozwala na szybkie wykrywanie nieprawidłowości i potencjalnych zagrożeń w obszarze zarówno fizycznym, jak i cybernetycznym.
- **Zarządzanie dostawcami**, czyli ocena bezpieczeństwa dostawców i partnerów oraz zapewnienie, że spełniają oni odpowiednie standardy bezpieczeństwa.
- Utrzymanie **zgodności z obowiązującymi regulacjami** i normami bezpieczeństwa, co zapewnia odpowiedni poziom ochrony i minimalizuje ryzyko prawne.

Zintegrowane podejście do ochrony infrastruktury krytycznej oparte na najlepszych praktykach i regulacjach prawnych zapewnia jej bezpieczeństwo i ciągłość działania. Współpraca, innowacje technologiczne oraz regularne szkolenia i oceny ryzyka są kluczowe dla skutecznej ochrony. Dzięki tym działaniom infrastruktura krytyczna może funkcjonować bezpiecznie nawet w obliczu rosnących zagrożeń. •

Cyberzagrożenia wobec infrastruktury krytycznej

JANUSZ SYRÓWKA, EON

Obiekty infrastruktury krytycznej są narażone na ataki hakerskie w takim samym stopniu, jak wszystkie inne. Różnicę stanowią skutki udanego ataku, które w tym przypadku będą miały bardzo poważne konsekwencje. Nie ma znaczenia, w jaki sposób dokonano ataku.

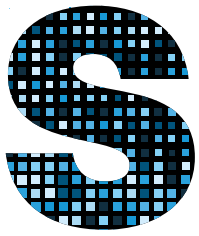
Ostatnio coraz więcej mówi się o cyberatakach. I to dobrze, gdyż każdy incydent to lekcja, którą należy wykorzystać jako impuls do wprowadzenia zmian. Mam nadzieję, że tym razem uwaga zostanie skupiona na bezpieczeństwie automatyki przemysłowej, czyli środowiska OT. Uważam, że jest to obszar, w którym dokonują się ogromne zmiany techniczne, dające wspaniałe możliwości. Jednocześnie mamy do czynienia z często nieuświadomionymi deficytami w obrębie bezpieczeństwa. Coraz większa jest jednak świadomość problemów oraz wola poprawy stanu rzeczy. Dobrym początkiem jest identyfikacja istotnych zasobów, które powinny być chronione. Środowisko OT jest moim zdaniem doskonałym przykładem przenikania się zagrożeń, gdzie granica pomiędzy światem cyfrowym a realnym jest bardzo trudna do zidentyfikowania. Znamy przykłady z Ukrainy, gdzie dokonywano włamań fizycznych do obiektów energetycznych po to, aby zamienić urządzenia na sprzęt odpowiednio zmanipulowany, który miał posłużyć do cyberataków.

Zapewnienie bezpieczeństwa to złożony proces, który niezbyt łatwo poddaje się definicjom. Tworzenie podziałów i współzależności to ta przysłowiowa para, która idzie w gwizdek. Potencjalny atakujący nie zastanawia się nad naszym podejściem do bezpieczeństwa. Skupia się szukaniu najsłabszego punktu i bezwzględnie go wykorzystuje. Jeśli będzie to słabość w systemie cyberbezpieczeństwa, to tak się z pewnością stanie. Nie zapominajmy jednak o mniej wyrafinowanych zagrożeniach, które są równie możliwe i skuteczne, jak choćby ostatnie tajemnicze pożary. •

Kodek kodekowi **nierówny**

Większość systemów dozoru wizyjnego kompresuje obraz za pomocą kodeka H.264. To dobry, sprawdzony kodek. Sęk w tym, że coraz doskonalsze kamery potrzebują bardziej zaawansowanego sposobu kodowania. Takiego, który poradzi sobie z kompresją i dekompresją obrazu ostrego jak żyletka. A H.264 ma już dwadzieścia lat i powoli przestaje wystarczać.

Jan T. Grusznic



Spodziewano się, że po wielu latach funkcjonowania H.264 zostanie zastąpiony przez H.265. Niestety, licencje, jakie dotyczą nowej wersji i ograniczenia kompatybilności powodują, że nowy kodek nie stał się, przynajmniej na razie, popularnym standardem kompresji obrazu.

Czym jest kodek?

Zacznijmy *ab ovo*, czyli od wyjaśnienia, czym jest kodek (ang. **codec,** skrót od **coder-decoder** lub **compressor-decompressor**). Otóż jest to program lub urządzenie służące do kodowania

Ilustracje: freepik

Jak działa kodek?

Kodowanie (kompresja) – kodek przekształca surowe dane multimedialne w bardziej skompresowany format, aby zajmowały mniej miejsca (np. plik wideo o dużym rozmiarze jest konwertowany do mniejszego formatu, np. MP4).

Dekodowanie (dekompresja) – gdy chcesz odtworzyć plik, kodek przekształca skompresowane dane z powrotem na format możliwy do odtworzenia przez odtwarzacz multimedialny.

Rodzaje kodeków:

- **Kodeki wideo** – np. **H.264, H.265 (HEVC), VP9, AV1** – służą do kompresji plików wideo.
- **Kodeki audio** – np. **MP3, AAC, FLAC, Opus** – służą do kompresji dźwięku.
- **Kodeki bezstratne i stratne:**
- **Bezstratne** (np. FLAC, ALAC) – zachowują pełną jakość dźwięku, ale mają większy rozmiar.
- **Stratne** (np. MP3, AAC) – usuwają część danych, aby zmniejszyć rozmiar pliku kosztem jakości.

Co ma ONVIF Profile S do kodeka H.264?

Open Network Video Interface Forum (ONVIF) to międzynarodowa organizacja standaryzacyjna, która opracowuje otwarte standardy dla urządzeń dozorowych (np. kamer IP, rejestratorów NVR). Powstała w 2008 roku, a jej celem jest zapewnienie **kompatybilności** i **interoperacyjności** sprzętu różnych producentów.

Bez ONVIF każda firma mogłaby używać własnych, zamkniętych technologii, co utrudniałoby integrację różnych urządzeń w jednym systemie monitoringu.

ONVIF definiuje **profile,** czyli zestawy funkcji, które urządzenia i oprogramowanie muszą obsługiwać, aby były kompatybilne.

ONVIF Profile S to standard przeznaczony dla **kamer IP i rejestratorów NVR.** Oznacza to, że jeśli kamera i rejestrator obsługują ONVIF Profile S, to będą ze sobą kompatybilne, nawet jeśli pochodzą od różnych producentów.

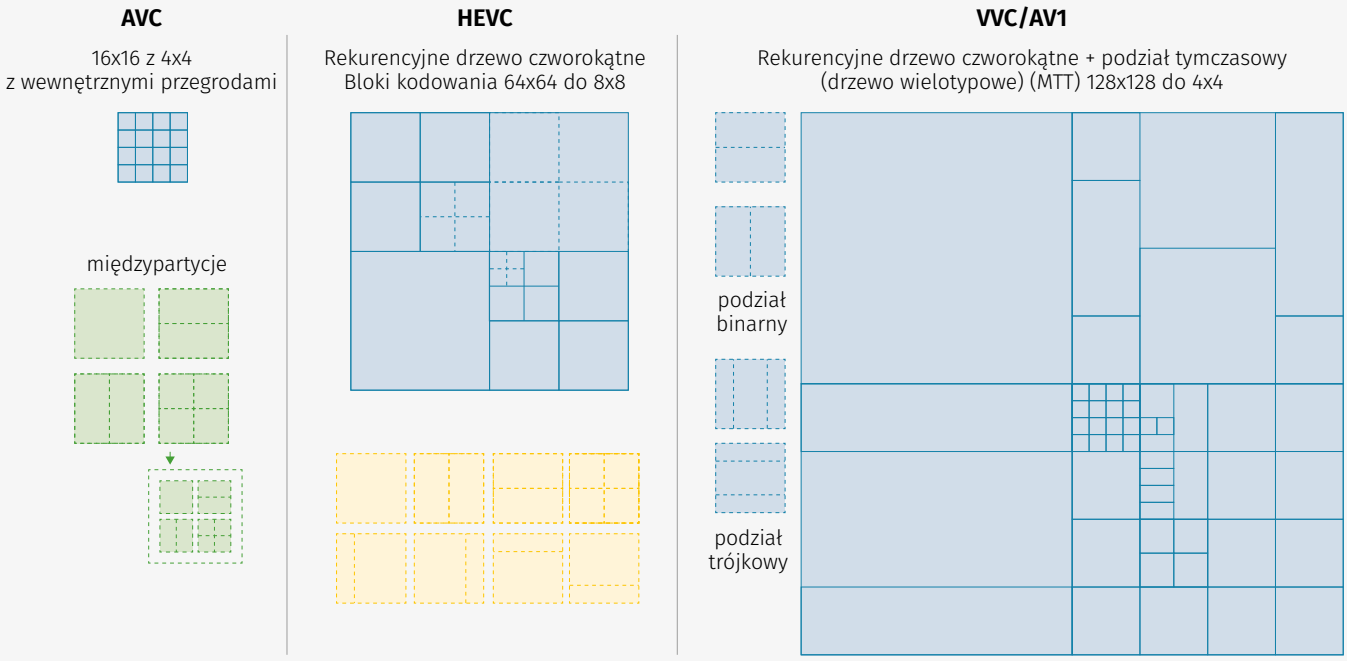
Główne funkcje ONVIF Profile S:

- Strumieniowanie wideo – kamera IP przesyła obraz do rejestratora lub oprogramowania VMS *(Video Management System).*
- Podstawowe sterowanie kamerą – np. zmiana ustawień obrazu, przesyłanie strumienia RTSP.
- Integracja urządzeń różnych producentów – np. kamera firmy A może współpracować z rejestratorem firmy B, jeśli oba obsługują ONVIF Profile S.

H.264 jest standardowym kodekiem wideo używanym w systemach monitoringu. ONVIF Profile S zapewnia, że kamery IP i rejestratory obsługujące ten profil mogą poprawnie przesyłać strumienie wideo w formacie H.264, niezależnie od producenta.

Dzięki temu użytkownik może łatwo budować systemy monitoringu składające się z urządzeń różnych marek, nie będąc zobligowany do kupowania wszystkiego od jednego dostawcy.

Więcej partycji, lepsza kompresja



i dekodowania danych multimedialnych, takich jak dźwięk i wideo. Jego głównym zadaniem jest **kompresja** danych w celu zmniejszenia ich rozmiaru oraz **dekompresja** w celu odtworzenia ich w pierwotnej jakości lub w jak najlepszej wersji.

Kodeki są używane w aplikacjach do odtwarzania i tworzenia plików multimedialnych dla użytkowników, a także do wysyłania plików multimedialnych przez sieć. Kompresują pliki wideo i audio, aby zaoszczędzić miejsce, ale też po to, by dało się je przesłać przez Internet w rozsądnym czasie.

Kodeki składają się z kodera i dekodera. Koder kompresuje plik multimedialny, a dekoder dekompresuje go. Istnieją setki różnych kodeków przeznaczonych do kodowania różnych mediów, takich jak wideo i audio. Dla użytkownika końcowego działanie kodeka jest w zasadzie niewidoczne. Na przykład program Windows Media Player, który jest preinstalowany z każdą wersją systemu Windows, udostępnia ograniczony zestaw kodeków do odtwarzania plików multimedialnych. W przypadku systemów VMS niezbędne kodeki są umieszczane w paczkach instalacyjnych oprogramowania lub paczkach aktualizacyjnych, aby system mógł bezproblemowo współpracować z urządzeniami transmitującymi obraz i/lub dźwięk.

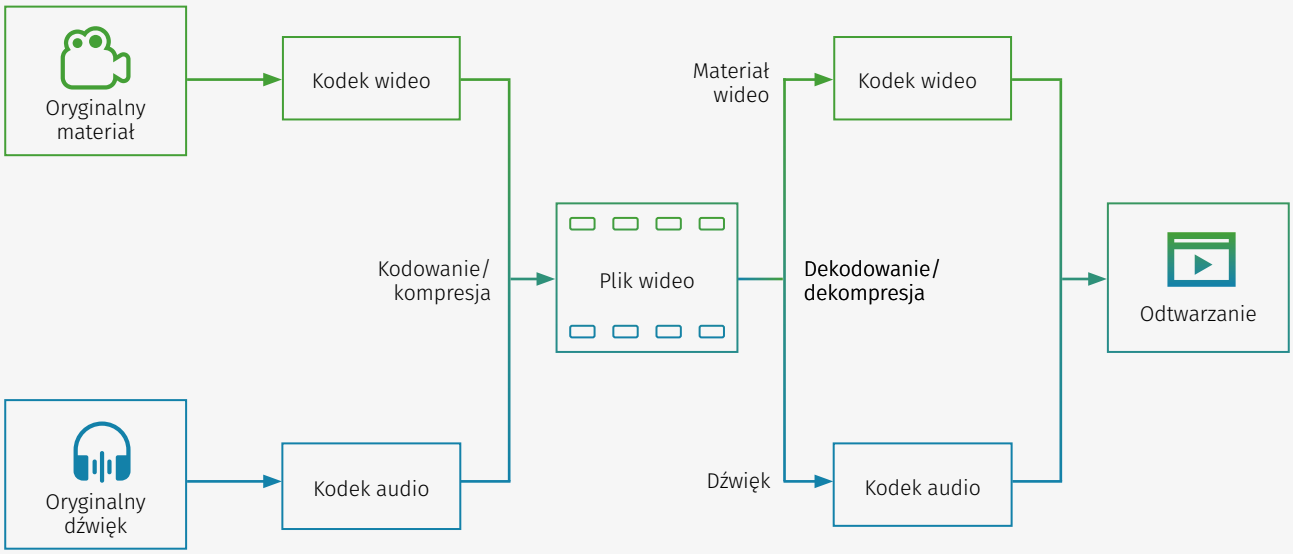
Podczas dekompresji kodek odwraca proces kompresji i rekonstruuje plik wideo. Podczas tego procesu niektóre informacje mogą zostać utracone. Jak wiele – to już zależy od kodeka. Prowadzi to do powstania końcowego pliku wideo, który może nie pasować idealnie do oryginalnie skompresowanego wideo, co może powodować potencjalne różnice w jakości. Wiele zależy od stopnia kompresji oferowanego przez kodek lub wybranego przez użytkownika. Zasada w tym przypadku jest prosta – im większy stopień kompresji, tym większa utrata danych, a końcowo gorsza jakość dekompresowanego pliku. Kodeki są niezbędne do umożliwienia wydajnej obsługi multimediów, zmniejszenia wymagań dotyczących przepustowości i zapewnienia optymalnej jakości w zastosowaniach multimediów cyfrowych.

Ewolucja standardów kompresji obrazu

H.264/AVC *(Advanced Video Coding)* to standard kodowania sekwencji wizyjnych przyjęty w roku 2003 jako 10. część standardu

Podczas dekompresji kodek odwraca proces kompresji i rekonstruuje plik wideo. Podczas tego procesu niektóre informacje mogą zostać utracone. Jak wiele – to już zależy od kodeka.

Proces kompresji i dekompresji kodeka



ISO MPEG-4 oraz jako rekomendacja ITU-T H.264. Mimo że ma już ponad 20 lat, nadal pozostaje najpowszechniej używanym kodekiem w branży dozoru wizyjnego, m.in. dzięki temu, że na nim oparto **ONVIF Profile S,** co znacząco ułatwia integrację urządzeń różnych producentów, wykorzystujących ten właśnie kodek (patrz ramka: *Co ma ONVIF Profile S do kodeka H.264?)*.

H.264 kompresuje wideo, dzieląc najpierw klatkę na kwadraty o stałym rozmiarze 16x16 pikseli, zwane makroblokami. Następnie każdy makroblok jest kompresowany poprzez eliminację nadmiarowych informacji wizualnych w pojedynczych klatkach (kompresja przestrzenna) oraz przechowywanie tylko zmian między kolejnymi klatkami (kompresja czasowa). To podejście pozwala znacząco zmniejszyć rozmiary plików przy zachowaniu akceptowalnej jakości obrazu.

Jednak H.264 ma istotne ograniczenia w kontekście współczesnych wymagań:

- Kodek był optymalizowany głównie dla rozdzielczości Full HD (1080p)
- Teoretycznie wspiera obrazy do 8K, jednak brak obsługi HDR dla wysokich rozdzielczości
- Stała wielkość makrobloków jest nieefektywna w przypadku obrazów o wysokiej rozdzielczości
- Generuje stosunkowo duży transfer danych przy wysokich rozdzielczościach

Czas na zmiany

H.265/HEVC *(High Efficiency Video Coding)* został opracowany jako następca H.264 i jest wspierany przez ONVIF Profile T. Wprowadza on nową strukturę kodowania zwaną CTU *(Coding Tree Units)* – elastyczne jednostki o zmiennych rozmiarach, które mogą być znacznie większe (do 64x64 pikseli) niż makrobloki H.264. Dzięki temu H.265 może skuteczniej zachowywać szczegóły i jakość w krytycznych obszarach wideo.

W teorii H.265 może osiągnąć lepszą jakość obrazu przy tej samej przepustowości lub zmniejszyć rozmiar pliku przy zachowaniu podobnej jakości w porównaniu z H.264. Niemniej jednak jego popularność nie rośnie tak szybko, jak można by się spodziewać, co wynika przede wszystkim z dwóch powodów.

Pierwszym są ograniczenia techniczne. Kodeki wideo nie są kompatybilne krzyżowo – kodek używany do kodowania i przesyłania danych wideo musi być zgodny z kodekiem używanym do ich dekodowania i odtwarzania. Oznacza to, że obraz zakodowany w H.265 nie może być wyświetlony za pomocą dekodera H.264 i odwrotnie. Ten problem jest najbardziej odczuwalny w rozwiązaniach chmurowych oraz aplikacjach webowych. Do dzisiaj tylko wybrane przeglądarki internetowe w pełni obsługują standard HEVC, jak Safari, Samsung Internet czy Baidu. Pozostałe, jak Chrome, Firefox, Edge czy Opera, obsługują go tylko na urządzeniach z odpowiednią akceleracją sprzętową.

Drugim są problemy natury prawnej. HEVC jest formatem zastrzeżonym, obwarowanym wieloma patentami. Licencjonowaniem zarządza Via Licensing Alliance, pobierające opłaty od twórców oprogramowania. Każdy z nich, niezależnie od tego, czy jest producentem VMS, czy producentem kamery do monitoringu wizyjnego, chcąc stosować H.265, musi uiścić opłatę licencyjna wynoszącą 0,20 USD za każde użycie/implementację/jednostkę, o ile produkcja przekracza już 100 tys. jednostek rocznie. Owszem, korzystanie z H.264 również wymagało opłacenia licencji, ale było to 0,10 USD za jednostkę, o ile sprzedaż przekroczyła 5 milionów urządzeń/implementacji. Biorąc pod uwagę, że

w 2024 roku sprzedano ponad 200 milionów kamer dozoru wizyjnego, wartość licencji za stosowanie H.265 w przypadku samych tylko kamer może wynosić około 40 milionów USD, a drugie tyle za oprogramowanie.

Smartkodeki – rozwiązanie pośrednie

Tradycyjne kodeki wideo zapewniają kompresję, usuwając nadmiarowe informacje z klatek wideo, natomiast smartkodeki wykorzystują zaawansowane algorytmy do analizy zawartości strumienia wideo w czasie rzeczywistym i określania, które części obrazu są najważniejsze dla celów nadzoru.

Innymi słowy – **smartkodeki** to zaawansowane algorytmy kompresji wideo, które optymalizują wykorzystanie przepustowości i przestrzeni dyskowej w systemach monitoringu, jednocześnie zachowując wysoką jakość obrazu. Są rozwinięciem standardowych kodeków, ale wprowadzone zostały w nich dodatkowe mechanizmy analizy obrazu.

Koncepcja nie jest nowa – jeszcze przed nastaniem AVC pojawiło się wiele rozwiązań, których celem było zredukowanie informacji powtarzajacych się w pliku wideo, ale z jednoczesnym utrzymaniem jego wysokiej jakości. Do takich rozwiązań należały kompresje MxPEG Mobotixa i MPEG4CCTV firmy Geutebrück. Ponieważ jednak każde z tych rozwiązań pochodziło od konkretnego producenta, to nie stały się obowiązującym w branży standardem, za to stały się bazą dla smartkodeków.

Smartkodeki mogą:

- Znacząco (nawet o 70%) zmniejszyć ilość danych, które muszą być przesyłane i przechowywane.
- Poprawić jakość wideo poprzez selektywne stosowanie kompresji do różnych części obrazu.
- Oznaczać obszary zainteresowania (ROI), które są kompresowane mniej agresywnie.
- Dynamicznie dostosowywać przepustowość w zależności od dostępnych zasobów sieciowych.
- Optymalizować częstotliwość wysyłania klatek kluczowych (I-frame) w zależności od ruchu w scenie.
- Dynamicznie zmieniać liczbę klatek na sekundę w zależności od wykrytej aktywności.

Co istotne, smartkodeki (na ogół) pozostają zgodne z istniejącymi standardami dekodowania, co oznacza, że nie potrzebują dodatkowych dekoderów po stronie oprogramowania klienckiego. Poszczególne standardy dekodera określają jedynie składnię i metodę odtwarzania materiału, nie narzucając samej metody kompresji.

> Wydaje się, że w najbliższej przyszłości będziemy świadkami stopniowej ewolucji, a nie rewolucji w obszarze kodeków wideo dla systemów dozoru wizyjnego.

Przyszłość kodeków wideo w systemach dozoru

Wzrost liczby kamer 4K i 8K stwarza zapotrzebowanie na standardy kodowania wideo, które zapewnią wysoką jakość przy niskich przepustowościach. Na horyzoncie pojawiają się dwa obiecujące kodeki: VVC (H.266) i AV1.

Versatile Video Coding (VVC), znany również jako H.266, to standard kompresji wideo sfinalizowany 6 lipca 2020 r. Jest następcą HEVC i został opracowany z myślą o dwóch głównych celach:

- poprawie wydajności kompresji,
- obsłudze bardzo szerokiego zakresu zastosowań, od obrazów niskiej rozdzielczości po 4K i 16K, a także filmów 360°.

VVC, podobnie jak H.265, podlega złożonym zasadom licencjonowania, co może ograniczać jego przyjęcie przez branżę. AV1 to wprowadzony w 2018 r. przez Alliance for Open Media (AOM) standard kodowania wideo nowej generacji. Członkami założycielami AOM są liderzy branży, tacy jak Amazon, Cisco, Google, Intel, Microsoft, Mozilla i Netflix, którzy postanowili stworzyć alternatywę dla kosztownych rozwiązań licencyjnych HEVC.

Zarówno VVC, jak i AV1 opierają się na koncepcji superbloków o wielkości 128x128 pikseli (dla porównania, w H.264 blok ma rozmiar 16x16 pikseli), co wymaga większej mocy obliczeniowej, ale pozwala zachować wyższą jakość obrazu. Szczególnie interesującą cechą AV1 jest technologia adaptacyjnego przesyłania strumieniowego, która jakość wideo dostosowuje w czasie rzeczywistym do tego, jakiej wydajności łączem sieciowym dysponuje klient. Jest to możliwe dzięki wprowadzeniu nowego typu ramki międzyklatkowej, tzw. ramki S *(switching frame),* która umożliwia przełączanie między różnymi rozdzielczościami bez konieczności stosowania pełnej klatki kluczowej.

Główną wadą AV1 jest jego intensywność obliczeniowa podczas kodowania, co czyni go mniej praktycznym w zastosowaniach wymagających pracy w czasie rzeczywistym, takich jak transmisje na żywo. Jednak sytuacja szybko się poprawia, ponieważ sprzętowa obsługa dekodowania AV1 staje się coraz bardziej powszechna w nowych urządzeniach.

Wydaje się, że w najbliższej przyszłości będziemy świadkami stopniowej ewolucji, a nie rewolucji w obszarze kodeków wideo dla systemów dozoru wizyjnego. Jeszcze przez jakiś czas H.264 będzie dominującym standardem, powoli jednak ustępując czekającym w blokach H.265, VVC i AV1.

Dla użytkowników systemów dozoru wizyjnego oznacza to konieczność zachowania pewnej czujności, szczególnie przy wyborze nowych urządzeń, by uniknąć problemu z kompatybilnością. Jednocześnie nowe kodeki przyniosą znaczące korzyści w postaci zmniejszenia wymagań dotyczących przepustowości i pojemności pamięci masowej, co z pewnością przełoży się na obniżenie kosztów eksploatacji systemów. •

Jan T. Grusznic
redaktor „a&s Polska”

Kamery Provision-ISR z analityką wykorzystującą algorytmy sztucznej inteligencji

Rewolucja sztucznej inteligencji wciąż przyspiesza, a jej zastosowanie w systemach monitoringu wizyjnego staje się coraz bardziej zaawansowane i wszechobecne. Dzięki nowoczesnym algorytmom kamery są zamieniane w inteligentne narzędzia, które nie tylko rejestrują obraz, ale także automatycznie analizują sytuacje w czasie rzeczywistym.

Odpowiednio skonfigurowane kamery są w stanie wyeliminować fałszywe alarmy, rozpoznawać zagrożenia i zapewniać nieprzerwane wsparcie w zarządzaniu bezpieczeństwem. To ewolucja, która zmienia rynek nadzoru wizyjnego – teraz systemy zarówno widzą, jak i rozumieją to, co obserwują.

Analityka wideo bazująca na algorytmach sztucznej inteligencji znajduje zastosowanie w wielu kluczowych obszarach – od monitorowania przestrzeni publicznych, przez ochronę zakładów przemysłowych, po zarządzanie ruchem drogowym i wykrywanie pożarów.

Największym przełomem jest detekcja i rozpoznanie atrybutów ludzi przy wykorzystaniu DDA2™ – opatentowanej technologii Provision-ISR, która wykorzystuje AI do rozpoznawania obiektów na nagraniach. DDA2™ *(Detect, Distinguish, Alert)* nie tylko identyfikuje i rozróżnia osoby, ale także analizuje takie szczegóły jak odzież, akcesoria czy marka pojazdu, eliminując fałszywe alarmy i dostarczając niezwykle precyzyjne analizy.

Flagowa technologia Provision-ISR – analityka wideo DDA™ i DDA2™ – oferuje funkcje takie jak detekcja pożaru, wykrywanie zmian temperatury i zagrożeń pożarowych na długo przed wybuchem ognia. Umożliwia także precyzyjne liczenie ludzi i pojazdów, co jest nieocenione w zarządzaniu ruchem. Z kolei funkcja mapy cieplnej tworzy wizualizację aktywności w danym obszarze, ułatwiając optymalizację przestrzeni.

Od roku 2023 kamery Provision-ISR, wyposażone w Check Point Quantum IoT Nano Agent, oferują zaawansowaną ochronę przed cyberzagrożeniami. Provision-ISR zapewnia również zgodność z wymogami NDAA, gwarantując najwyższe standardy bezpieczeństwa.

Wśród najnowszych modeli Provision-ISR rozszerza gamę kamer termowizyjnych o wersje tubową, a model I6-2120IPEN-MVF-V5, z rozdzielczością 12 Mpix i technologią DDA2™, podnosi poprzeczkę w zakresie zabezpieczeń, oferując nową jakość obrazu i detekcji w najtrudniejszych warunkach. Provision-ISR przesuwa granice możliwości monitoringu wizyjnego, udostępniając rozwiązania, które są inteligentne, niezawodne i podnoszące poziom zabezpieczeń w dziedzinie cyberbezpieczeństwa. •

ICS POLSKA
ul. Poleczki 82, 02-822 Warszawa
www.ics.pl
biuro@ics.pl

Przełączniki sieciowe BAROX

Elektroniczne systemy zabezpieczeń odgrywają kluczową rolę w ochronie osób i mienia. Jednym z najważniejszych elementów tych systemów są przełączniki sieciowe IP, które stanowią fundament nowoczesnych systemów zabezpieczeń technicznych. Dotyczy to w szczególności systemów dozoru wizyjnego, gdzie niezawodność i bezpieczeństwo transmisji danych są priorytetem, a odpowiedni dobór przełączników jest szczególnie istotny.

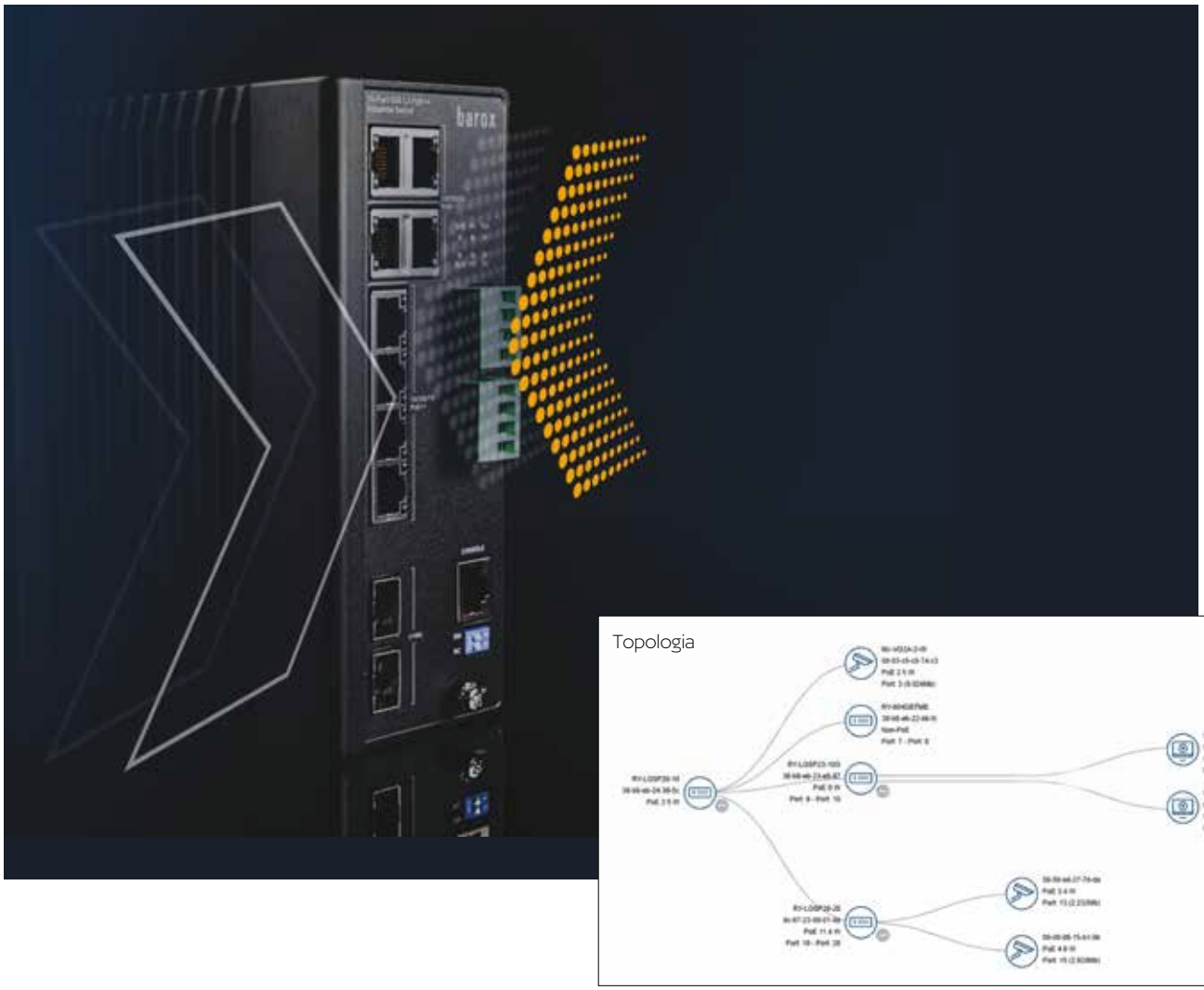
Przełączniki sieciowe IP nie tylko umożliwiają poprawną komunikację między kamerami IP, rejestratorami wideo (NVR) i innymi urządzeniami sieciowymi, ale także muszą posiadać funkcje stanowiące solidną barierę ochronną przed wszelkiego rodzaju próbami ataków cyfrowych oraz zapewniać ciągłość działania nawet w wypadku usterek.

Przełączniki sieciowe IP stosowane w systemach dozoru wizyjnego dla infrastruktury krytycznej powinny zapewniać najwyższy poziom bezpieczeństwa i odporności. Kluczowe technologie dla zapewnienia niezawodności i ochrony przed zagrożeniami cybernetycznymi obejmują zaawansowane mechanizmy szyfrowania, systemy wykrywania i zapobiegania atakom oraz redundancję sprzętową i programową.

Gdy urządzenia elektronicznych systemów zabezpieczeń przestają działać lub zrywają połączenie, wymagają natychmiastowej fizycznej interwencji specjalisty, aby skrócić do minimum czas niedostępności. Przełącznik BAROX można skonfigurować tak, aby sprawdzał obecność podłączonych urządzeń. Jeśli urządzenie nie odpowiada, switch IP automatycznie zrestartuje zasilanie PoE, przywracając działanie systemu.

Poza funkcją PoE Auto Checking przełączniki BAROX oferują także **zaplanowane, sekwencyjne uruchamianie poszczególnych portów** w celu uniknięcia przeciążenia zasilacza. Funkcje te obejmują identyfikację i konfigurowalne powiadomienia o problemach z zużyciem energii, co umożliwia wczesne ostrzeganie o awarii zasilanego urządzenia brzegowego. Natomiast funkcja Non-Stop PoE pozwala **utrzymać zasilanie PoE** (zgodne z IEEE 802.3 bt – nawet 120W na port) **oraz komunikację** podczas aktualizacji oprogramowania układowego przełącznika.

Serię przełączników zarządzalnych BAROX wyposażono w unikalny **bezlicencyjny system zarządzania urządzeniami DMS** (*Devices Management System*). System ten jest dostępny na przełącznikach i może działać samodzielnie lub jako część integracji z takimi platformami, jak Genetec, Milestone, ISM-Genesys, Advancis czy Geutebrück. DMS monitoruje stan całej sieci bezpieczeństwa,



skracając czas diagnozowania i usuwania usterek. Monitoruje wszystkie przełączniki sieciowe, podłączone urządzenia i infrastrukturę.

Topologia sieci oraz wszystkie podłączone końcowe urządzenia IP są prezentowane na diagramie. Jeśli urządzenie końcowe zostanie prawidłowo rozpoznane, to zostanie przedstawione za pomocą odpowiedniego symbolu (kamera, przełącznik, punkt dostępowy itp.). Wszystkie istotne informacje, takie jak nazwa urządzenia, adres IP, szybkość transmisji danych, pobór prądu itp., są wyświetlane obok. Ponadto wszystkie ustawienia mogą być skonfigurowane ręcznie.

Połączenie z urządzeniem można zdiagnozować z dowolnego przełącznika BAROX obecnego w sieci. W przypadku wystąpienia jakichkolwiek zakłóceń w połączeniu lub infrastrukturze kablowej zostanie ono wyświetlone na diagramie, w widoku topologii. Usterki w połączeniach Ethernet mogą zostać zlokalizowane w promieniu 1 m od miejsca wystąpienia problemu.

Funkcja monitorowania umożliwia śledzenie przepływu danych (np. z kamery) w czasie rzeczywistym. Administrator może skonfigurować progi przepływu danych, co pozwala na szybkie określenie, czy połączenie działa zgodnie z oczekiwaniami. Dodatkowo można monitorować pobór prądu przez kamerę oraz ustawiać odpowiednie progi. Oba te parametry mogą być analizowane w celu proaktywnego identyfikowania potencjalnych problemów z podłączonymi urządzeniami, co umożliwia interwencję przed wystąpieniem awarii systemu.

Cyberbezpieczeństwo jest priorytetem. **Ochrona przed atakami cyfrowymi** chroni przełączniki oraz całą sieć przed potencjalnymi zagrożeniami. Przełączniki BAROX spełniają najnowsze normy bezpieczeństwa, są wyposażone w zaawansowane funkcje oprogramowania układowego, których brak w porównywalnych produktach. Są to m.in.:

- szyfrowanie komunikacji typu end-to-end,
- ochrona portów (IEEE 802.1X), w tym blokowanie adresów MAC,
- automatyczne wyłączanie nieobciążonych portów komunikacyjnych,
- funkcja o nazwie *sticky*, która „uczy się sieci" i przechowuje jej „obraz". Jeśli zmieni się adres IP i/lub Mac dowolnego, podłączonego urządzenia, wygeneruje alarm i/lub wyłączy port ethernetowy,
- obsługa list kontroli dostępu (ACL),
- alarmowanie o zmianie topologii sieciowej,
- informowanie o nieudanej próbie logowania do przełącznika,
- zapora sieciowa.

Producent przełączników BAROX posiada akredytację ISO 9001/14001/27001, a produkty są w pełni zgodne z NDAA.

Więcej szczegółów dostępnych jest na stronie producenta www.barox.ch.

Sprzęt testowy jest dostępny u partnera BAROX w firmie squareTec. •

squareTec
ul. Broniewskiego 4,
85-316 Bydgoszcz
www.squaretec.pl

Ratują ŻYCIE, ryzykując WŁASNE

Jak branża security może pomóc w ochronie ratowników medycznych?

Nastąpił niepokojący wzrost liczby ataków na ratowników medycznych w Polsce. Zespoły, które niosą pomoc w stanach zagrożenia życia, coraz częściej same stają się ofiarami agresji. Czy branża security może odegrać kluczową rolę w rozwiązaniu tego narastającego problemu?

W Siedlcach 64-letni ratownik medyczny został śmiertelnie ugodzony nożem przez pacjenta, któremu udzielał pomocy. W podwarszawskim Żółwinie pijana grupa imprezowiczów brutalnie zaatakowała ratowników, zmuszając ich do ucieczki i porzucenia karetki. W Krakowie zespół ratownictwa został pobity przez agresywnego pacjenta, który był pod wpływem narkotyków.

Według danych Ministerstwa Zdrowia tylko w 2024 r. ratownicy medyczni ponad 3 tys. razy prosili o pomoc z powodu agresji pacjentów lub osób postronnych. W tym samym czasie zespoły ratownictwa medycznego wyjechały łącznie do ponad 3 mln 200 tys. zdarzeń. To oznacza, że w czasie jednej na tysiąc interwencji ratownicy potrzebowali wsparcia służb porządkowych, ponieważ ich zdrowie i życie było zagrożone.

Problem ten narasta z roku na rok. Uniwersytet Jagielloński w 2018 r. przeprowadził badania, których wyniki były niepokojące. Aż 96% ratowników medycznych wskazało wówczas, że spotkało się z agresją w pracy, 88% doświadczyło agresji werbalnej, 74% – aktów wandalizmu, a 68% było bezpośrednio atakowanych przez pacjentów lub osoby im towarzyszące.

Krajowa Rada Ratowników Medycznych, która bierze udział w wypracowaniu rozwiązań w celu poprawy ochrony personelu karetki pogotowia, zwraca uwagę na niskie kary za napaść i uszkodzenie sprzętu. Zasądzane dotychczas wyroki sprawcom takich czynów były to najczęściej prace społeczne.

Wzywamy karetkę, a ona ochronę?

Technologie bezpieczeństwa od lat stosowane w innych sektorach – m.in. przy ochronie VIP-ów, transporcie gotówki czy zabezpieczeniu obiektów – mogą stać się skuteczną tarczą ochronną ratowników.

1. MONITORING I SYSTEMY ALARMOWE

- **Kamery nasobne** (*body cameras*) – ich obecność działa prewencyjnie i pozwala rejestrować incydenty. Takie rozwiązanie stosowane jest m.in. w Czechach i Wielkiej Brytanii.

Ilustracje: shutterstock

- **Monitoring karetek** – instalacja kamer wewnętrznych i zewnętrznych ułatwiałaby identyfikację sprawców ataków.
- **Przyciski alarmowe i geolokalizacja** – szybkie wezwanie wsparcia przez system alarmowy skracałoby czas reakcji służb w razie zagrożenia.

2. ŚRODKI OCHRONY OSOBISTEJ

- **Kamizelki nożoodporne** – stosowane przez niektóre zespoły ratownicze w USA i Niemczech, chronią przed atakami ostrymi narzędziami.
- **Hełmy ochronne** – w ekstremalnych przypadkach, np. w miejscach o wysokiej przestępczości, mogą stanowić dodatkowe zabezpieczenie.
- **Systemy samoobrony** – gaz pieprzowy lub paralizatory są przedmiotem dyskusji, ale ich użycie przez ratowników medycznych jest obecnie blokowane przez przepisy prawa.

3. WSPARCIE TECHNOLOGICZNE I AI

- **Systemy predykcji zagrożeń** – analiza zgłoszeń w czasie rzeczywistym pozwala przewidywać, które wezwania mogą się wiązać z agresją.
- **AI w analizie zachowań** – monitoring dźwiękowy w karetkach mógłby wykrywać wzrastający poziom agresji i automatycznie zgłaszać problem w centrali.
- **Automatyczne powiadomienia policji** – szybkie reagowanie służb mundurowych na zagrożenia.

Skuteczny ratownik to bezpieczny ratownik – Wielka Brytania to rozumie

Problem agresji wobec ratowników medycznych występuje nie tylko w Polsce. Wiele krajów na świecie boryka się z podobnym zagrożeniem. Są jednak takie państwa, które wdrożyły skuteczne rozwiązania i w ten sposób znacząco poprawiły bezpieczeństwo personelu medycznego.

Najbardziej spektakularne efekty osiągnęła w tym zakresie Wielka Brytania. W roku 2018 wprowadzono ustawę *Assaults on Emergency Workers (Offences) Act*, która zwiększyła ochronę pracowników służb ratunkowych, w tym ratowników medycznych. Podwoiła ona maksymalną karę za atak na pracowników służb ratunkowych z sześciu miesięcy do roku pozbawienia wolności. Już cztery lata później, w odpowiedzi na stale rosnącą liczbę ataków, rząd zwiększył maksymalny wymiar kary do dwóch lat więzienia. Ponadto wyposażono ratowników w kamery nasobne, które ułatwiają identyfikację sprawców napaści i pociągnięcie ich do odpowiedzialności.

W Niemczech została z kolei usprawniona współpraca medyków z policją podczas interwencji w rejonach podwyższonego

ryzyka. We Francji uwaga rządzących skupiła się na kampaniach społecznych, które mają zbudować szacunek dla służb medycznych i zwiększyć świadomość społeczną problemu.

W całej Europie testowane są na różną skalę również inne rozwiązania technologiczne, takie jak instalacja kamer w pojazdach ratunkowych, które nagrywają obraz wewnątrz i na zewnątrz pojazdu, przyciski alarmowe wszyte w odzież każdego ratownika, aplikacje alarmowe w smartfonach umożliwiające dyskretne wysłanie sygnału alarmowego do odpowiednich służb. Ponadto ratownicy są wyposażani w kamizelki nożoodporne i kuloodporne, hełmy ochronne oraz lekkie tarcze, które mogą być używane w sytuacjach ekstremalnego zagrożenia.

W najbardziej niebezpiecznych rejonach świata (poza Europą) zdarza się, że niektóre grupy pracowników medycznych mają paralizatory elektryczne, gaz pieprzowy i pałki teleskopowe. To jednak rzadkość. Służby medyczne przechodzą wówczas skomplikowane szkolenia dotyczące sytuacji niebezpiecznych i okoliczności, w jakich mogą użyć takich narzędzi.

Co blokuje wprowadzenie zmian w Polsce?

Mimo rosnącej liczby ataków w Polsce nadal obowiązują przepisy, które utrudniają wdrażanie nowoczesnych systemów ochrony:

- **ochrona danych osobowych** – nagrywanie pacjentów przez kamery nasobne wymaga zgody, co może komplikować ich stosowanie;
- **brak podstawy prawnej do użycia narzędzi samoobrony** – ratownicy medyczni w Polsce nie mogą stosować środków, takich jak paralizatory czy gaz pieprzowy, nawet w sytuacji bezpośredniego zagrożenia życia;
- **brak jednoznacznych regulacji dotyczących eskorty policyjnej** – obecnie wsparcie policji jest organizowane sporadycznie i nie jest standardową procedurą w przypadku zgłoszeń z podwyższonym ryzykiem.

Czy rynek security może wypełnić tę lukę?

Branża security ma rozwiązania, które mogą nie tylko zwiększyć bezpieczeństwo ratowników, ale także zmniejszyć liczbę ataków poprzez efekt prewencyjny. Istnieje ogromna nisza rynkowa na produkty skierowane do sektora medycznego – kamery nasobne dostosowane do ochrony danych pacjentów, systemy alarmowe zintegrowane z ratownictwem czy technologie predykcji agresji.

Problem agresji wobec ratowników medycznych wymaga natychmiastowych działań. W obliczu rosnącej liczby ataków polski rynek security ma szansę odegrać kluczową rolę w poprawie bezpieczeństwa służb medycznych. Innowacyjne technologie, wsparcie legislacyjne i współpraca międzysektorowa mogą sprawić, że medycy nie będą już musieli obawiać się o własne życie, niosąc pomoc innym. •

IWO KOŻUCHOWSKI, specjalista ds. obronnych i ochrony Szpitala Czerniakowskiego w Warszawie

Cieszę się, że temat bezpieczeństwa ratowników medycznych podczas wykonywania przez nich trudnej i odpowiedzialnej pracy został poruszony. Pamiętajmy, że pracę tę wykonują ludzie, dla których jest ona pasją. Oczywiście podstawową sprawą jest bezpieczeństwo pacjenta, jednak od pewnego czasu zwraca się też uwagę na bezpieczeństwo osób niosących pomoc. Jest kilka możliwości, które mogą przyczynić się do zwiększenia bezpieczeństwa pracowników zespołów ratownictwa medycznego (ZRM), ale nie wszystkie można wprowadzić w naszym kraju. Przynajmniej na razie.

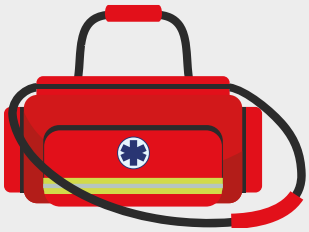
Z pewnością monitoring wizyjny może stanowić ważne uzupełnienie codziennej pracy personelu medycznego (podstawowym aktem prawnym regulującym monitoring wizyjny w placówkach medycznych jest art. 23a ustawy o działalności leczniczej). Umożliwia on dokładną analizę sytuacji i zdarzeń niepożądanych przy udzielaniu świadczeń zdrowotnych, ich przyczyn oraz przebiegu. Decyzja o zastosowaniu monitoringu wizyjnego w podmiocie leczniczym nie może być jednak dowolna i wyłącznie uznaniowa. Kamery dozorowe zawsze muszą być stosowane w sposób odpowiedzialny i zgodny z przepisami prawa, w szczególności z prawami pacjenta i RODO.

Nie ulega wątpliwości, że przy stosowaniu monitoringu wizyjnego konieczne jest pogodzenie kilku kwestii:

- dążenia do poprawy bezpieczeństwa pacjentów,
- efektywności procesu leczniczego,
- korzyści związanych z optymalizacją procesów zarządczych z uwzględnieniem konieczności respektowania praw pacjenta, w szczególności prawa do poszanowania intymności i godności.

I tutaj właśnie pojawia się problem zastosowania kamer nasobnych przez ZRM lub instalowania kamer w ambulansach. Według mnie dopóki przepisy prawne w tych kwestiach nie zostaną zmienione, nie będzie to możliwe. Tak samo jak opcja zatrudnienia pracowników ochrony celem towarzyszenia ZRM podczas udzielania pomocy pacjentom. Przepisy wyraźnie określają, kto może być obecny przy udzielaniu świadczeń medycznych.

Tym, co możemy zrobić już teraz jest: wyposażenie ZRM w systemy pozwalające na szybkie wezwanie wsparcia, zorganizowanie szkoleń dla ratowników medycznych z samoobrony również w ciasnych pomieszczeniach, takich jak np. wnętrze karetki, które będą prowadzili specjaliści w tych kwestiach. Dobrym pomysłem jest również wyposażenie ratowników w kamizelki nożoodporne. Uważam, że polski rynek security z pewnością ma dużo do zaoferowania w kwestii zabezpieczeń ratowników medycznych.



Pracownik ochrony funkcjonariuszem publicznym? Czemu nie

Ostatnie wydarzenia w Warszawie, gdy ochroniarz postrzelił włamywacza, wywołały sporo emocji. Jakie działania są dopuszczalne, a gdzie leżą granice interwencji? Na pytania odpowiada **Jarosław Kur,** wiceprezes Polskiego Związku Pracowników Ochrona.

Pytanie pierwsze i zasadnicze: co może pracownik ochrony, a czego mu nie wolno?
Działalność firm świadczących usługi ochrony osób i mienia bazuje głównie na ustawie z 1997 r. Ustawa jasno określa, w jakich sytuacjach pracownik ochrony może podjąć interwencję. W obiektach chronionych, takich jak zakłady produkcyjne, „obowiązkowej ochrony", zamknięte dla postronnych osób, mamy prawo wylegitymować ludzi, by zweryfikować ich uprawnienia do przebywania w danym miejscu. A gdy ktoś dopuszcza się czynu, który stanowi zagrożenie mienia lub zdrowia i życia – np. w trakcie próby kradzieży czy agresywnego zachowania – możemy zatrzymać taką osobę do czasu przybycia policji. I nic więcej. W centrach handlowych interwencje mogą być podejmowane wobec osób, co do których zachodzi podejrzenie dokonania kradzieży, czy też których zachowanie jest niedopuszczalne typu bójka, niszczenie mienia itp. W tym przypadku możemy zatrzymać taką osobę do czasu przybycia policji.

A co z użyciem środków przymusu bezpośredniego? Czy w sytuacji zagrożenia można stosować takie środki?
Tak, ale z zastrzeżeniem, że muszą być one proporcjonalne do sytuacji, zagrożenia. Obowiązująca ustawa wyraźnie precyzuje, że środki przymusu mogą być stosowane wyłącznie wtedy, gdy istnieje realne zagrożenie dla życia i zdrowia lub utraty mienia. Przykład z Warszawy pokazuje, jak napięta bywa sytuacja – interwencja osoby na posterunku musi być szybka i zdecydowana, jednak zawsze w granicach prawa.

Coraz więcej mówi się o podnoszeniu kwalifikacji pracowników ochrony. Jakie wymagania musi spełnić osoba, która chce pracować w tej branży?
Każdy kandydat na pracownika ochrony musi przejść specjalistyczny kurs trwający zwykle 3-4 miesiące. Po ukończeniu szkolenia odbywają się badania zdrowotne i weryfikacja niekaralności przez odpowiednie służby, np. Komendę Wojewódzką Policji. Jeśli pracownik ma mieć prawo do korzystania z broni lub innych zaawansowanych narzędzi interwencyjnych, musi zdać stosowny egzamin. Dzięki temu mamy pewność, że do akcji interwencyjnych angażujemy osoby odpowiednio przygotowane i przeszkolone.

Wydarzenia ostatniego czasu podkreślają, jak ważne jest nie tylko szkolenie, ale i stosowanie aktualnych procedur. Czy widzi Pan potrzebę wprowadzenia dodatkowych regulacji lub modernizacji przepisów?
Zdecydowanie tak. Agencje ochrony dostosowują procedury do realiów, szczególnie w kwestii współpracy z policją oraz wdrażania nowoczesnych technologii – systemów monitoringu czy rozwiązań alarmowych. Celem firm jest minimalizacja ryzyka zarówno dla pracowników, jak i osób postronnych. Nieustannie też prowadzą szkolenia. Chodzi o to, by pracownicy ochrony zawsze znali swoje uprawnienia, by wiedzieli, jak się zachować w trudnej sytuacji, a także, by ich działania interwencyjne były zgodne z obowiązującymi przepisami. Podstawową zasadą pracy osób zajmujących się ochroną jest odpowiedzialne podejście do kwestii bezpieczeństwa i precyzyjne.

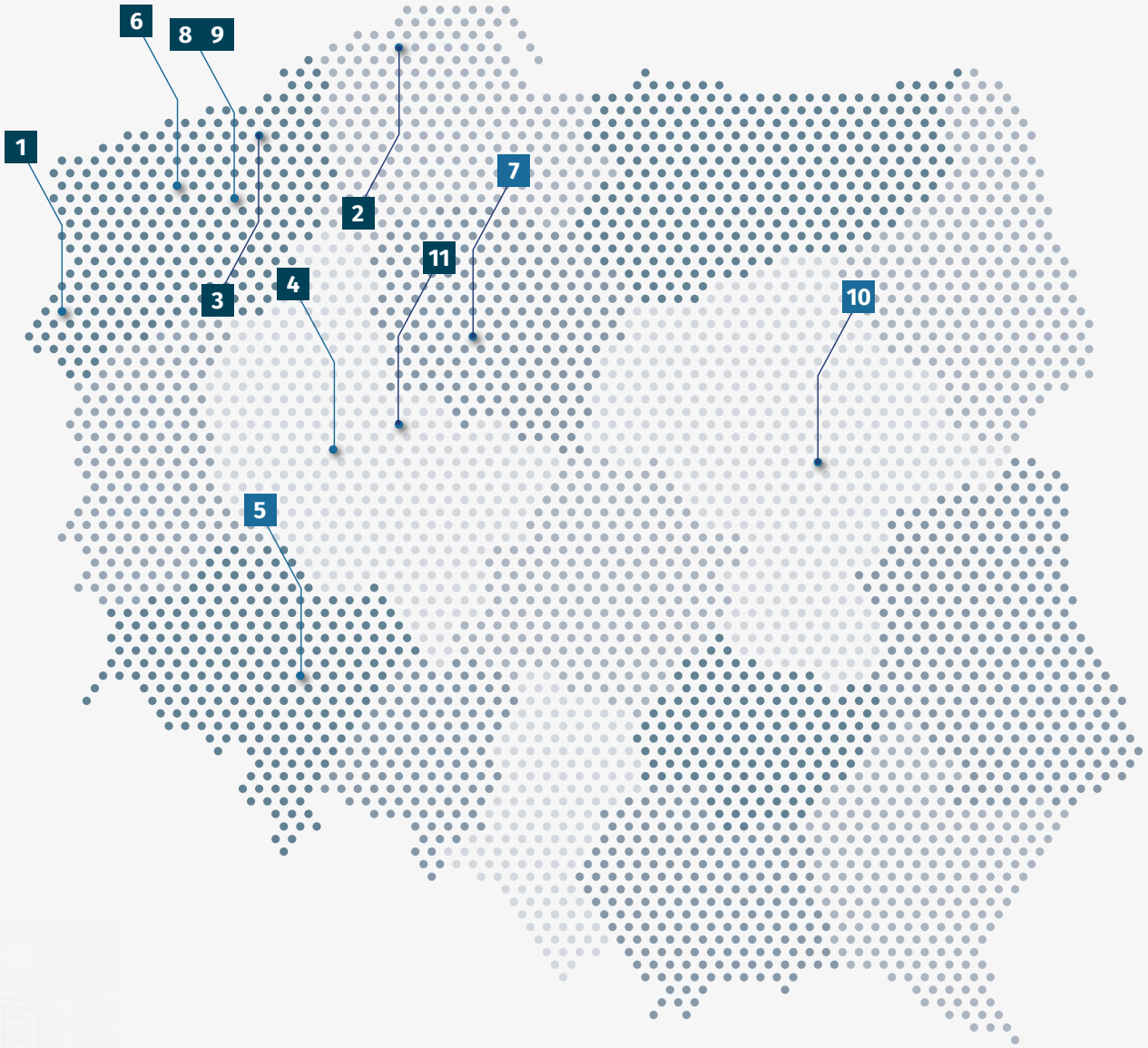
Jednocześnie, jako PZPO widzimy, że w Ustawie o Ochronie Osób i Mienia powinny pojawić się zmiany, dzięki którym pracownik ochrony zyska rangę funkcjonariusza publicznego. Chodzi bowiem o to, by osoba podejmująca interwencję wobec osoby potencjalnie łamiącej prawo była chroniona przez prawo obowiązujące w Polsce. Pracownik ochrony nie może bowiem bać się chronić. •

Ustawa z dnia 10 czerwca 1997 r. o ochronie osób i mienia (Dz.U. 1997 nr 92 poz. 437, z późn. zm.) – reguluje kwestie legitymowania, zatrzymywania oraz stosowania środków przymusu bezpośredniego przez pracowników ochrony w sytuacjach zagrożenia mienia i życia. Przepisy wykonawcze, m.in. rozporządzenia Ministra Spraw Wewnętrznych i Administracji uzupełniają ustawę i określają szczegółowe procedury stosowania środków przymusu.

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

Mapa inwestycji

Prezentujemy wybór inwestycji realizowanych przez firmy takie jak Atrem, DB Energy, Elektrotim, Erbud, Mirbud, Pekabex i Unibep. Projekty te obejmują m.in. modernizację i rozbudowę infrastruktury elektroenergetycznej (np. przebudowa stacji 110/15 kV w Gryfinie, modernizacja stacji przekształtnikowej w Słupsku, budowa GPZ Białogard), inwestycje w sektorze wojskowym (np. budowa budynków koszarowych w Powidzu, infrastruktura lotniska w Świdwinie) oraz projekty medyczne i przemysłowe (np. Centrum Leczenia Dzieci w Bydgoszczy, kompleksowa budowa hangaru obsługi technicznej). Realizowane przedsięwzięcia wpisują się w rozwój kluczowych sektorów gospodarki i infrastruktury. Inwestycje te są planowane na najbliższe lata, a ich zakończenie przewidywane jest od 2026 do 2027 roku.



Atrem

1	**Co:**	Przebudowa stacji 110/15 kV Gryfino
	Gdzie:	Gryfino
	Kiedy:	18 miesięcy od dnia zawarcia umowy (5.03.2025)
2	**Co:**	Modernizacja stacji przekształtnikowej 400 kV AC / 450 kV DC Słupsk – modernizacja SOT oraz budowa ogrodzenia i drogi dojazdowej do bramy
	Gdzie:	Słupsk
	Kiedy:	22 miesiące od dnia zawarcia umowy (3.03.2025)
3	**Co:**	Rozbudowa wraz z przebudową stacji elektroenergetycznej 110/15 kV GPZ Białogard
	Gdzie:	Białogard
	Kiedy:	27 miesięcy od dnia zawarcia umowy (28.02.2025)
4	**Co:**	Przebudowa stacji WN/SN kV Poznań HCP
	Gdzie:	Poznań
	Kiedy:	100 tygodni od dnia zawarcia umowy (7.02.2025)

DB Energy

5	**Co:**	Budowa Głównego Punktu Odbioru energii elektrycznej
	Gdzie:	Wrocław
	Kiedy:	23 miesiące od dnia złożenia zamówienia przez Zamawiającego

Elektrotim

6	**Co:**	Przebudowa stacji 110/15 kV na terenie OD Szczecin: Zadanie nr 4: Przebudowa stacji 110/15 kV Golczewo
	Gdzie:	Golczewo
	Kiedy:	18 miesięcy od daty zawarcia umowy (28.02.2025)

Erbud

7	**Co:**	Budowa obiektu Centrum Leczenia Dzieci Szpitala Uniwersyteckiego nr 1 im. dr. A. Jurasza w Bydgoszczy w formule „zaprojektuj-wybuduj-wyposaż”
	Gdzie:	Bydgoszcz
	Kiedy:	31.10.2027

Mirbud

8	**Co:**	Budowa budynku Naziemnej Obsługi Statków Powietrznych
	Gdzie:	Świdwin
	Kiedy:	30.06.2026
9	**Co:**	Realizacja robót budowlanych dla infrastruktury wojskowej lotniska
	Gdzie:	Świdwin
	Kiedy:	1.09.2026

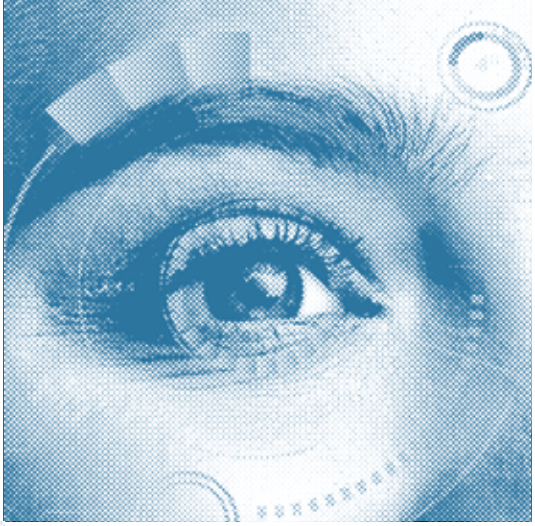
Pekabex

10	**Co:**	Roboty budowlane. Projekt Apart Hotel na nieruchomości położonej w Warszawie
	Gdzie:	Warszawa
	Kiedy:	30.09.2026

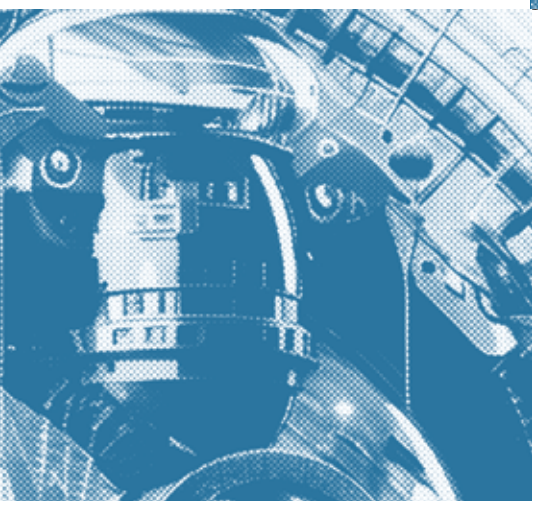
Unibep

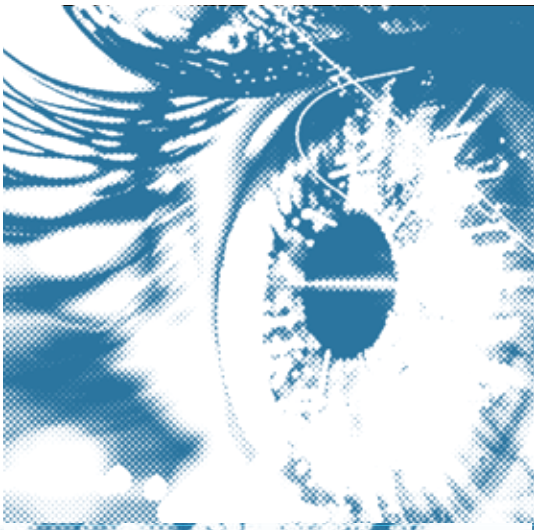
11	**Co:**	Budowa 3 budynków koszarowych i stołówki
	Gdzie:	Powidz
	Kiedy:	IV kwartał 2027

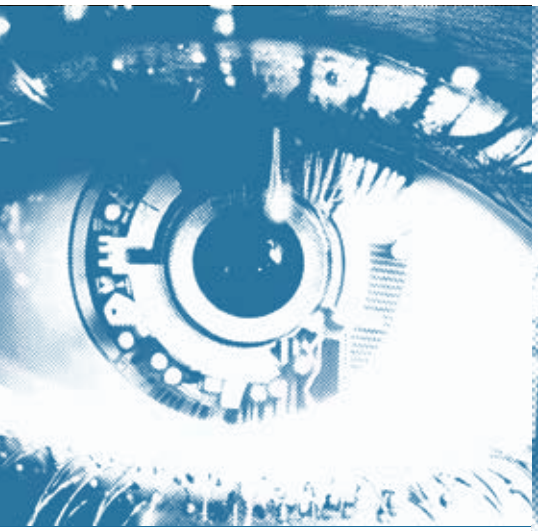
Ilustracje: freepik / Mapa: Jan Kurzawa

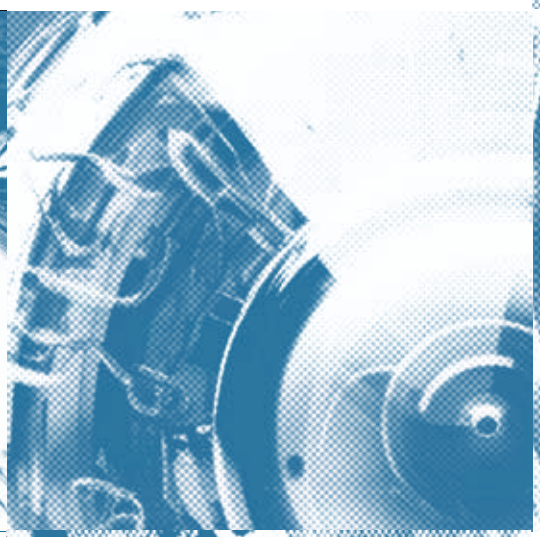


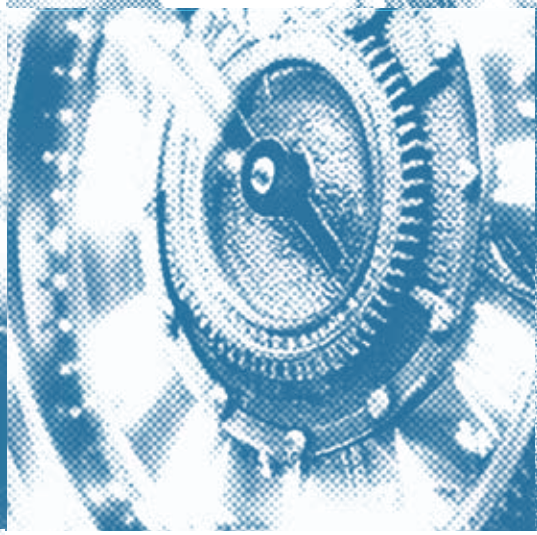
Jak usprawnić pracę security dzięki sztucznej inteligencji

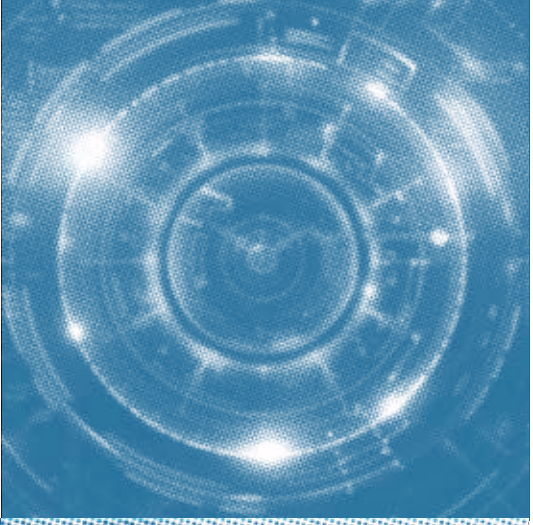


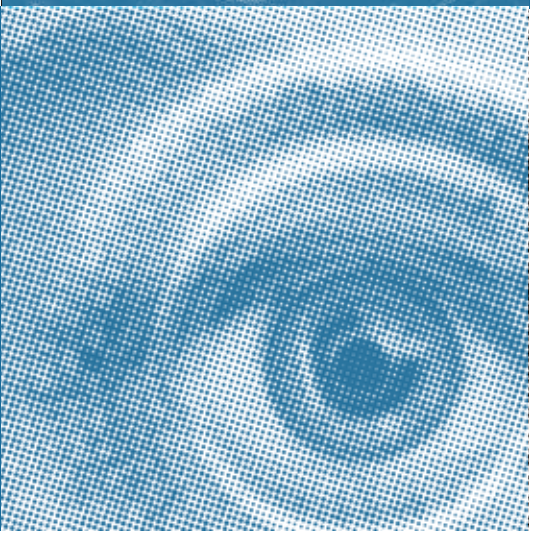






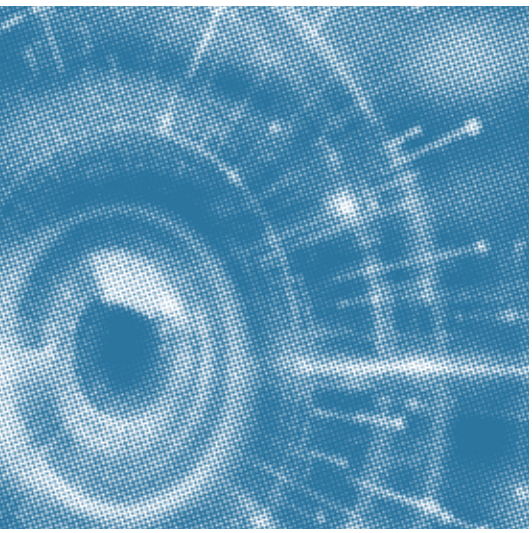


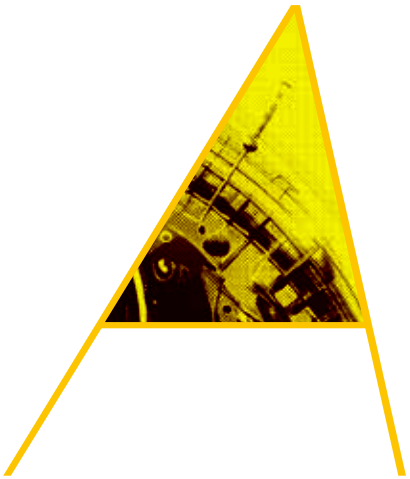




Algorytmy sztucznej inteligencji już jakiś czas temu znalazły zastosowanie w aplikacjach obsługujących urządzenia monitoringu wizyjnego i kontroli dostępu. Z ich mocy, tym razem w generatywnej wersji, wywołującej ostatnio sporo szumu medialnego, mogą korzystać także integratorzy projektujący całe systemy lub potrzebujący porównać różne produkty. Pomocne będą też użytkownikom przymierzającym się do zakupu systemu bezpieczeństwa. W jaki sposób może ich w tym wspomóc na przykład najbardziej popularna SI, czyli ChatGPT?

Monika Żuber-Mamakis





Artificial Intelligence, AI (sztuczna inteligencja, SI) to szeroka dziedzina obejmująca różne technologie inteligentne. W jej ramach wyróżniamy m.in. LLM (*Large Language Model*) – modele skoncentrowane na przetwarzaniu i generowaniu języka naturalnego. Szczególną kategorią jest generatywna SI, która potrafi tworzyć nowe treści na podstawie danych wejściowych, w przeciwieństwie do standardowej SI, która jedynie analizuje podane jej dane. Generatywna SI może tworzyć całkowicie nową treść: tekst, obrazy, wideo czy kod programistyczny na podstawie tzw. promptów, czyli poleceń bądź zapytań użytkowników.

Nowe funkcje ChatGPT-4

Warto dodać, że najnowsza wersja ChatGPT-4 wprowadza szereg nowych funkcji, w tym możliwość analizy obrazów. Użytkownicy mogą teraz przesłać zdjęcie systemu zabezpieczeń i poprosić o analizę jego mocnych i słabych stron.

SI w bezpieczeństwie fizycznym

Branża security już od dłuższego czasu korzysta z możliwości standardowej sztucznej inteligencji. Do tej pory nie służyła ona jednak do tworzenia nowych treści, lecz do analizowania już istniejących. Weźmy np. aplikacje stosowane w monitoringu wizyjnym. Dzięki wprowadzeniu algorytmów SI potrafią nie tylko przeanalizować zapis wideo, ale także spośród wszystkich nagrań wyłuskać te, które dla ludzi wyglądają jak prawdziwe, a w istocie są *deepfake'ami*. Natomiast SI w swojej generatywnej odmianie może uczynić kontrolę dostępu jeszcze bardziej skuteczną dzięki umiejętności opracowywania scenariuszy przewidujących różne próby obchodzenia zabezpieczeń oraz np. udoskonalając odczyty biometryczne.

Ograniczenia ChatGPT

Można by rozwinąć sekcję o ograniczeniach ChatGPT, dodając konkretne przykłady:

- możliwe nieścisłości w specyfikacjach najnowszych produktów,
- brak dostępu do aktualnych cen,
- brak możliwości weryfikacji zgodności z lokalnymi normami bezpieczeństwa.

Sztuczna inteligencja znajduje zastosowanie również w bardziej zaawansowanych systemach bezpieczeństwa fizycznego. Przykładem mogą być autonomiczne roboty patrolujące, które monitorują przestrzeń publiczną i prywatną, korzystając z kamer i czujników. Mogą służyć do inspekcji terenów, szybkiego reagowania na zagrożenia czy śledzenia podejrzanych osób. Innymi przykładami zastosowania SI są analiza zachowań tłumu i wykrywanie potencjalnych zagrożeń. Systemy te mogą wykrywać obecność broni, rozpoznawać twarze w tłumie czy identyfikować agresywne zachowania w czasie rzeczywistym.

ChatGPT jako narzędzie wsparcia

Jedną z najbardziej znanych generatywnych SI jest ChatGPT, który może być pomocny w pracy integratorów bezpieczeństwa. Może być też przydatny osobom potrzebującym porównania różnych produktów, próbującym obliczyć niezbędną ilość pamięci masowej albo chcącym szybko przygotować szczegółową specyfikację jakiegoś rozwiązania.

Jak formułować zapytania do ChatGPT

Jak formułować zapytania do ChatGPT, żeby otrzymać najbardziej przydatne odpowiedzi dotyczące systemów bezpieczeństwa, tzw. *prompt engineering*? Kluczowe jest zadawanie precyzyjnych pytań oraz dostarczanie kontekstu dotyczącego specyfikacji technicznych lub wymagań użytkownika.

Weźmy np. pozornie proste, ale czasochłonne zadanie porównywania różnych urządzeń idealne do powierzenia sztucznej inteligencji. Świetną demonstrację takiego zastosowania można zobaczyć w filmie opublikowanym przez 2DTechBG na YouTubie. ChatGPT został poproszony o porównanie dwóch różnych producentów. Proces trwał mniej niż minutę, a dane wejściowe obejmowały specyfikacje techniczne obu kamer oraz pytania dotyczące ich zastosowań.

Warto zaznaczyć, że ograniczeniem ChatGPT jest dostęp tego narzędzia tylko do informacji zawartych w jego bazie danych, co mogło wpłynąć na dokładność porównania. Po serii kilku pytań ChatGPT przedstawił nie tylko różnice między obydwoma modelami, ale także znalazł inne, podobne modele i podał ich parametry techniczne.

Szybsze przygotowanie specyfikacji

ChatGPT może służyć integratorom systemów jako doradca podczas opracowywania specyfikacji sprzętu. W omawianym przykładzie został poproszony o przygotowanie propozycji specyfikacji dla systemu CCTV, który miał spełniać następujące warunki: cztery kamery, przechowywanie nagrań przez 30 dni oraz interkom. ChatGPT zaproponował dwa modele rejestratorów (NVR), dyski twarde o dwóch różnych pojemnościach (4 lub 8 TB), konkretne modele kamer IP oraz interkomów. Całość obsługiwana za pomocą aplikacji producenta. Przygotowanie tej

Generatywna SI może skutecznie wspierać proces podejmowania decyzji, m.in. w przypadku systemu kontroli dostępu może analizować dane historyczne, by przewidywać potencjalne zagrożenia i rekomendować zmiany w konfiguracji systemu.

specyfikacji zajęło sztucznej inteligencji niecałe trzy minuty, co pokazuje jej skuteczność w analizowaniu i integrowaniu złożonych danych.

Obliczanie pamięci masowej

ChatGPT może pomóc użytkownikom obliczyć wymaganą pojemność pamięci masowej. Na pytanie: „Ile dysków HDD potrzebuję dla systemu CCTV z 10 kamerami 4MP, detekcją ruchu z 30-proc. ruchem dziennie, H.264 dla wszystkich kamer, 15 klatek na sekundę i przechowywaniem nagrań przez 30 dni" ChatGPT najpierw przedstawił pomocny wzór, a następnie wyliczył, że przy takich parametrach wielkość pamięci masowej powinna wynosić ok. 50,6 TB, co można osiągnąć przy użyciu wielu dysków twardych skonfigurowanych w RAID.

Dodatkowe możliwości

Sztuczna inteligencja opracowana przez OpenAI potrafi odpowiadać na różnorodne pytania związane z security. Zapytana o format Wieganda dla numeru karty dostępu 1234567 przedstawiła tę liczbę w postaci 26-bitowego zapisu binarnego z dodatkowym bitem zapewniającym równą liczbę jedynek w całym ciągu tzw. parzysta parzystość (*even parity*). Z kolei na prośbę o obliczenie liczby baterii potrzebnych do zasilenia 10 czujników dymu określonej marki w przypadku dwudniowej przerwy w dostawie prądu, ChatGPT wyjaśnił, że niezbędna byłaby bateria 12 V o pojemności co najmniej 2000 Ah, przy założeniu całkowitego zużycia energii na poziomie 500 W.

Inteligencja sztuczna czy własna – której zaufać?

Korzystanie z SI takich jak ChatGPT jest niewątpliwie wygodne, jednak podejmowanie decyzji zakupowych wyłącznie na podstawie rekomendacji sztucznej inteligencji nie jest rozsądnym rozwiązaniem. Ani integrator, ani użytkownik końcowy nie powinni opierać się wyłącznie na wynikach uzyskanych poprzez odpytywanie generatywnych SI. To znakomite narzędzia usprawniające pracę, ale nie nieomylne – jest wiele przykładów pokazujących, że potrafią przekonująco konfabulować.

Powierzenie decyzji dotyczących bezpieczeństwa wyłącznie maszynie nie jest najlepszym rozwiązaniem. Nie zmienia to jednak faktu, że generatywna SI może skutecznie wspierać proces podejmowania decyzji, m.in. w przypadku systemu kontroli dostępu może analizować dane historyczne, by przewidywać potencjalne zagrożenia i rekomendować zmiany w konfiguracji systemu. Może to obejmować sugerowanie dodatkowych punktów weryfikacji biometrycznej w miejscach o podwyższonym ryzyku lub opracowanie scenariuszy odpowiedzi na nietypowe zachowania użytkowników. Dzięki ChatGPT użytkownik może uzyskać podstawowe informacje o produktach lub rozwiązaniach zabezpieczających oraz inne przydatne dane takie jak długoterminowa wartość produktu i analiza korzyści, ale też kosztów. •

Ilustracje: freepik

Monika Żuber-Mamakis
redaktorka „a&s Polska"

Rośnie rynek **urządzeń ubieralnych**

Urządzenia ubieralne, znane również jako *wearables*, to kategoria elektroniki zaprojektowanej do noszenia. Są to zatem zarówno bardzo proste opaski sportowe, jak i kamery obecne na policyjnych mundurach, ale też inteligentne okulary rozszerzonej lub zaawansowanej rzeczywistości.
Z roku na rok ich liczba rośnie. Branża security powinna mieć je na oku.

Monika Żuber-Mamakis

Urządzenia ubieralne mogą zbierać dane dotyczące parametrów życiowych, snu i aktywności fizycznej. Mogą też służyć do płacenia przez NFC lub uzyskiwania dostępu, ale też, jak w przypadku kamer nasobnych, do rejestrowania wydarzeń. *Wearables* stanowią zatem doskonały przykład implementacji Internetu rzeczy (IoT), łącząc się z innymi urządzeniami i aplikacjami w celu zapewnienia bardziej zintegrowanego doświadczenia użytkownika.

Urządzenia ubieralne – bardzo pojemna kategoria

Kategoria urządzeń ubieralnych jest bardzo pojemna, choć zaawansowanie stosowanej w nich techniki jest różne. Czym innym są bowiem Google Glass oraz HoloLens firmy Microsoft, które oferują doświadczenia w rozszerzonej rzeczywistości (AR) i wirtualnej rzeczywistości (VR), a czym innym prosta fit opaska czy czujnik służący do monitorowania poziomu glukozy. Nie zmienia to faktu, że *wearables*, niezależnie od poziomu skomplikowania, zupełnie niepostrzeżenie zadomowiły się w naszej rzeczywistości, czego dowodem fakt, że w roku 2023 rynek urządzeń ubieralnych został wyceniony na ponad 61 mln USD w 2023 r. i oczekuje się, że osiągnie 152 817,2 mln USD do 2029 r., przy CAGR wynoszącym 16,8% od 2024 do 2029 r.

Jeśli chodzi o polski rynek *wearables*, według danych IDC Poland w 2023 r., sprzedaż urządzeń ubieralnych w Polsce wzrosła o ok. 20% rok do roku. Największą popularnością cieszą się smartwatche i opaski fitness. A jak wynika z badania przeprowadzonego w listopadzie 2024 r. przez SW Research na zlecenie Huawei CBG Polska, z urządzeń ubieralnych, czyli inteligentnych zegarków i opasek, korzysta ponad 1/3 Polaków. Co piąta osoba (20%) ma smartwatch, 12% – opaskę, a 4% ankietowanych – i jedno, i drugie. Smartwatche największą popularnością cieszą się wśród badanych w wieku 25–34 lat – aż 30% z nich ma takie urządzenie.

Główne czynniki powodujące wzrost zainteresowania urządzeniami ubieralnymi to coraz lepsze wyświetlacze, wzrastająca popularność Internetu rzeczy (IoT) oraz integracja rozszerzonej rzeczywistości w technologiach noszonych, co wzmacnia immersyjne doświadczenia kontekstowe. Główne ograniczenia tych urządzeń to ograniczona żywotność baterii oraz, co bardzo ważne, podatność na ataki wymierzone w połączeniach między urządzeniami noszonymi a siecią.

Krytyczne wyzwania stojące przed rynkiem technologii noszonej to potrzeba ciągłego rozwoju urządzeń, nierozwiązane kwestie regulacyjne oraz podatność informacji zdrowotnych, a także osiągnięcie długotrwałego i zrównoważonego zaangażowania klientów.

Urządzenia ubieralne – modne, wygodne, i trochę... niebezpieczne

Smartwatche, opaska fitness czy inteligentne okulary (te są chyba najmniej popularne) nie wydają się urządzeniami szczególnie groźnymi w kontekście firmowego cyfrowego bezpieczeństwa. Niedoszacowanie zagrożeń, z jakimi może się wiązać ich noszenie przez pracowników, to jednak błąd. Urządzenia te są często połączone z siecią i innymi urządzeniami, co czyni je potencjalnymi celami cyberataków. Hakerzy mogą wykorzystać luki w zabezpieczeniach, aby uzyskać dostęp do danych osobowych lub informacji firmowych. Przykłady ataków obejmują wycieki danych z platform takich jak Garmin i Polar, które gromadzą wrażliwe informacje z urządzeń ubieralnych. W roku 2017 doszło do incydentu, w którym dane z aplikacji Strava ujawniły lokalizacje tajnych baz wojskowych USA. Aplikacja, służąca do monitorowania aktywności fizycznej, opublikowała mapy, które pokazywały zagregowane ścieżki biegaczy z miliarda treningów. W wyniku analizy tych danych internauci byli w stanie zidentyfikować miejsca, w których stacjonowali amerykańscy żołnierze, w tym bazy w Turcji, Syrii i Jemenie. Wprawdzie Strava nie publikowała tras konkretnych osób, ale zagregowane dane pozwalały na identyfikację aktywności w miejscach o wysokim stopniu tajności. Wojsko wdrożyło rygorystyczne zasady dotyczące używania technologii przez swoich pracowników oraz przypominania o konieczności ochrony danych osobowych i lokalizacji. O tym incydencie powinny pamiętać firmy, szczególnie te, które spełniają warunki pozwalające je uznać za obiekty infrastruktury krytycznej.

Ponadto urządzenia ubieralne gromadzą różnorodne dane, w tym informacje zdrowotne i lokalizacyjne. W przypadku niewłaściwego zarządzania tymi danymi istnieje ryzyko naruszenia prywatności pracowników oraz wycieków informacji. Firmy muszą być świadome polityki prywatności dostawców tych urządzeń oraz sposobu przechowywania danych.

Wearables nie są bez wad:

- Ograniczona żywotność baterii
- Luki w zabezpieczeniach połączeń sieciowych
- Potrzeba ciągłego rozwoju urządzeń
- Nieuregulowane kwestie prawne i ochrona danych medycznych
- Utrzymanie długoterminowego zaangażowania klientów

Integracja tych urządzeń z systemami IT firmy zwiększa ryzyko, że atak na jedno urządzenie może prowadzić do kompromitacji całego systemu. Wzrost liczby połączeń z Internetem rzeczy (IoT) sprawia, że zabezpieczenia muszą być bardziej zaawansowane. Ponadto niektóre aplikacje używane na urządzeniach ubieralnych mogą zawierać złośliwe oprogramowanie. Użytkownicy mogą przypadkowo pobrać aplikacje spoza oficjalnych źródeł, co stwarza dodatkowe zagrożenie dla bezpieczeństwa danych osobowych i firmowych.

Kolejnym istotnym aspektem jest konieczność regularnych aktualizacji oprogramowania tych urządzeń w celu zapewnienia bezpieczeństwa. Brak takich aktualizacji może prowadzić do pozostawienia luk w zabezpieczeniach, które mogą być wykorzystane przez hakerów. W związku z tym firmy powinny opracować jasne polityki dotyczące używania urządzeń ubieralnych w miejscu pracy oraz przeprowadzać szkolenia pracowników na temat bezpieczeństwa danych oraz prywatności.

Jak chronić firmowe dane przy rosnącej popularności *wearables*?

Urządzenia ubieralne, choć z pozoru niewinne, mogą stanowić furtkę dla cyberataków w środowisku firmowym. Warto przyjrzeć się, jakie działania pomogą zminimalizować to ryzyko. Podstawą jest wprowadzenie **jasnej polityki bezpieczeństwa** określającej zasady korzystania z *wearables* w miejscu pracy. Dokument powinien precyzować, jakie dane mogą być przetwarzane i w jaki sposób należy chronić informacje firmowe.

Kolejny kluczowy element to **edukacja pracowników.** Regularne szkolenia pozwalają pracownikom zrozumieć potencjalne zagrożenia i nauczyć się właściwego korzystania z urządzeń ubieralnych w kontekście firmowym. Istotne jest także bieżące **aktualizowanie oprogramowania.** Regularne instalowanie najnowszych wersji systemu i aplikacji zapewnia aktualną ochronę przed nowymi zagrożeniami. Firmy powinny również **regularnie monitorować wykorzystanie urządzeń ubieralnych** i przeprowadzać audyty bezpieczeństwa. Pozwala to wcześnie wykryć potencjalne luki w systemie ochrony. Ze względu na wymogi RODO, szczególną uwagę należy zwrócić na przetwarzanie danych osobowych. Pracownicy muszą być świadomi, jakie informacje są zbierane i w jakim celu. Warto też pamiętać o ograniczeniu użycia Bluetooth i włączaniu go tylko w razie potrzeby, by ograniczyć ryzyko nieautoryzowanego dostępu do urządzeń.

Rosnąca popularność i coraz szersze możliwości sprawiają, że nie da się zakazać w firmach posiadania urządzeń ubieralnych, ale też nie można ignorować faktu, że pracownicy z nich korzystają. Kluczem jest znalezienie równowagi między wygodą użytkowania a bezpieczeństwem firmowych danych. Świadome podejście do zagrożeń, jasne zasady i systematyczne działania prewencyjne pozwolą czerpać korzyści z technologii ubieralnych przy jednoczesnym zachowaniu wysokich standardów cyberbezpieczeństwa. W końcu *wearables*, jak każde narzędzie, mogą być zarówno użyteczne, jak i potencjalnie niebezpieczne – wszystko zależy od tego, jak nimi zarządzamy. •

Monika Żuber-Mamakis
redaktorka „a&s Polska"

Ilustracje: freepik, shutterstock

Światłowód FFT gwarantem bezpieczeństwa

Linc Polska

Infrastruktura krytyczna, jaką niewątpliwie są lotniska, wymaga specjalnych systemów zabezpieczeń pozwalających na działanie na dużym obszarze. Jednym z takich rozwiązań jest oferowany przez Future Fibre Technologies (FFT) system wykrywania i lokalizacji wtargnięć oparty na światłowodach. Rozwiązania wykorzystujące tę technologię pozwalają na ochronę perymetryczną obiektów zarówno na ogrodzeniu, jak i w ziemi. Pod względem zasięgu są to jedne z najbardziej efektywnych rozwiązań na rynku pozwalające na zabezpieczenie rozległych obszarów, w tym obiektów infrastruktury krytycznej.

Najnowsza generacja sterowników marki FFT Aura Ai-X, wspierana przez algorytmy sztucznej inteligencji, pozwala na dokładniejsze określenie i wykrycie zdefiniowanych zachowań. Oferuje skuteczniejszą detekcję, m.in. wspinania się na ogrodzenie, jego przecięcia lub unoszenia, a w przypadku instalacji w ziemi przejścia, przebiegania lub podkopywania. Z zasięgiem działania nawet do 110 km Aura Ai-X pozwala na wykrycie, wskazanie i zaraportowanie zaburzeń w wiązce lasera z dokładnością do ±2 m.

Sterownik Aura Ai-X wysyła światło lasera przewodem światłowodowym przez dwa kanały detekcyjne. Włókna detekcyjne są umieszczone w przewodzie zamontowanym na ogrodzeniu lub zakopanym w ziemi. Ruchy ogrodzenia lub drgania podłoża powodują drgania włókien i zmiany w odbiciu światła lasera. Sterownik automatycznie analizuje światło odbite w celu wykrycia i lokalizacji wtargnięcia. Dzięki przetwarzaniu sygnałów przez wbudowane algorytmy oraz wykorzystaniu sztucznej inteligencji z łatwością ustala, co jest wtargnięciem, niechcianym alarmem lub innym zdarzeniem.

Oprogramowanie obsługujące Aura Ai-X inteligentnie analizuje pomiary światła lasera i ustawienia sterownika, aby zoptymalizować czułość i zredukować niechciane alarmy oraz zwiększyć prawdopodobieństwo wykrycia zagrożenia.

Nawet w przypadku przecięcia lub zniszczenia przewodu, jeżeli włókna podłączone są do obu kanałów w konfiguracji redundantnej pętli, Aura Ai-X działa, kontynuując detekcję do miejsca przecięcia.

Wykorzystanie algorytmu sztucznej inteligencji w sterowniku Aura Ai-X oraz zaawansowana i skuteczna weryfikacja sygnałów zapobiega uciążliwym, niechcianym alarmom przy zachowaniu maksymalnej czułości na włamania, co sprawia, że to rozwiązanie jest odpowiednie dla obiektów infrastruktury krytycznej, lotnisk, granic czy terenów wojskowych. •

Integracja systemu kontroli dostępu RACS 5 z platformą PSIM VENOM

Roger

System kontroli dostępu RACS 5 firmy Roger zaprojektowany z myślą o elastycznym i niezawodnym zarządzaniu dostępem umożliwia integrację z platformą PSIM VENOM. Dzięki integracji rozwiązań użytkownicy zyskują dostęp do nowych zaawansowanych operacji, które wspierają szybkie reagowanie na potencjalne zagrożenia oraz optymalizację procesów bezpieczeństwa. Integracja ta pozwala uzyskać szereg dwukierunkowych funkcji, takich jak:

- pobieranie zdarzeń,
- kontrola stanów przejść i kontrolerów,
- sterowanie przejściami,
- synchronizacja użytkowników.

Dzięki integracji RACS 5 z PSIM VENOM użytkownicy mogą sprawniej, szybciej i efektywniej zarządzać bezpieczeństwem w obiektach o różnej skali i specyfice. Integracja ta szczególnie sprawdza się w przemyśle, biurowcach, centrach logistycznych i obiektach infrastruktury krytycznej.

Integracja RACS 5 z platformą PSIM VENOM umożliwia kompleksowe zarządzanie bezpieczeństwem. Rozbudowanie systemu kontroli dostępu RACS 5 o funkcje automatyzacji i centralizacji zarządzania nie tylko zwiększa świadomość sytuacyjną i przyspiesza reakcję w sytuacjach zagrożenia, ale także umożliwia użytkownikom optymalizację kosztów i zasobów. Dzięki kolejnym integracjom platforma RACS 5 staje się jeszcze bardziej elastycznym narzędziem, które doskonale odpowiada na wyzwania współczesnych obiektów, zapewniając im bezpieczeństwo i efektywność operacyjną na najwyższym poziomie. •


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 ULTRA

KOREA MADE IN

NDAA COMPLIANT

- Urządzenia pochodzące z nowej linii produktowej zgodnej z Amerykańską dyrektywą NDAA.
- Wtargnięcie w obszar, przekroczenie linii • Rozpoznawanie obiektów osoba/pojazd
- Inteligentna wykrywanie zagubionych/pozostawionych obiektów
- Wykrywanie twarzy

Tworzymy obraz

zgodnie ze sztuką

www.bcs.pl

www.facebook.com/bcspl

POLSKA MARKA BCS