02 (56) / 2026

CZASOPISMO RYNKU SECURITY

a&S POLSKA

BATERIA NIE MOŻE ZAWIEŚĆ

Zasilanie awaryjne nie jest jedynie dodatkiem do systemu bezpieczeństwa. Jak sprawić, by baterie naprawdę chroniły? Odpowiedź tkwi w technologii, normach i twardych liczbach.

GRANICA SIĘ PRZESUWA

Inteligentne systemy ochrony obwodowej zmieniają zasady gry. Perymetr przestaje być statyczną linią, a staje się inteligentnym, zintegrowanym ekosystemem.

INFRASTRUKTURA KRYTYCZNA

Przykłady ataków na cele pozornie nieistotne pokazują, że sprawcy kierują się własnymi kryteriami wyboru celów. Nie znamy planów przeciwnika, ale możemy je rozpoznać.

www.aspolska.pl

20 zł
(w tym 8% VAT)

ISSN 2451-5175 05
9 772451 517703

20/04/2026 • Renaissance Warsaw Airport Hotel

INFRASTRUKTURA KRYTYCZNA ENERGETYKA I OZE

Strategiczna platforma dla liderów bezpieczeństwa i odporności organizacji

Szczegóły na:
SECURITYFORUM.PL

ORGANIZATOR

a&S POLSKA

PATRONAT HONOROWY

RCB Rządowe Centrum Bezpieczeństwa

Polskie Stowarzyszenie Fotowoltaiki i Magazynowania Energii

STOWARZYSZENIE BRANŻY FOTOWOLTAICZNEJ I MAGAZYNOWANIA ENERGII

PTBN Polskie Towarzystwo Bezpieczeństwa Narodowego

WSPÓŁORGANIZATOR

TAURUS OCHRONA

PARTNERZY TECHNOLOGICZNI

CIAS

Hanwha Vision

MEGAVISION TECHNOLOGY

roger ASSA ABLOY

Bezpieczeństwo bez kompromisów

W realiach działań hybrydowych granica między zagrożeniami fizycznymi a cyfrowymi coraz częściej zanika. Infrastruktura krytyczna – od energetyki po transport i łączność – działa dziś jako jeden, silnie powiązany ekosystem technologii, danych i ludzi. Dlatego skuteczne bezpieczeństwo nie polega już na wyborze między światem analogowym a cyfrowym, lecz na ich pełnej integracji.

Najnowsze wydanie „a&s Polska" poświęcamy właśnie temu obszarowi styku, łącząc analizę kluczowych ryzyk z praktycznymi wskazówkami dla zarządzających bezpieczeństwem.

Już w tekście *Bateria nie może zawieść. Prawda o zasilaniu awaryjnym w systemach zabezpieczeń* (str. 12) obalamy popularne, lecz kosztowne w skutkach przekonanie, że zasilanie awaryjne jest jedynie dodatkiem do systemu bezpieczeństwa. Pokazujemy, dlaczego to właśnie ono decyduje o realnej ciągłości działania oraz jak nowoczesne podejście zmienia sposób projektowania i eksploatacji instalacji.

Strategiczne spojrzenie na bezpieczeństwo prezentuje tekst *Infrastruktura krytyczna – sabotaż, chaos i dane* (str. 40), osadzony w realiach świata VUCA i BANI. Autor zachęca do spojrzenia na systemy ochrony z perspektywy przeciwnika oraz do refleksji nad tym, że „krytyczność" infrastruktury nie zawsze wynika wyłącznie z definicji prawnych, lecz z realnych scenariuszy operacyjnych i zależności systemowych.

Zmieniające się podejście do ochrony fizycznej najlepiej widać na granicach chronionych obiektów. W artykule *Granica się przesuwa. Jak inteligentne systemy ochrony obwodowej zmieniają zasady gry* (str. 34) pokazujemy, jak perymetr przestaje być statyczną linią, a staje się inteligentnym, zintegrowanym ekosystemem, w którym kluczową rolę odgrywają projektowanie, integracja i cyberodporność.

Z kolei transformację architektury monitoringu wizyjnego opisujemy w materiale *Kamera w chmurze. Rewolucja VSaaS zmienia zasady gry w ochronie obiektów* (str. 22), gdzie rozwiązania chmurowe i sztuczna inteligencja redefiniują sposób zarządzania dozorem. Chmura przestaje być alternatywą – staje się naturalnym środowiskiem skalowania systemów, analizowania danych i optymalizacji kosztów.

Temat standardów i odpowiedzialności projektowych rozwijamy w artykule *Kto i dla kogo opracował normę PN–EN 62676. Systemy dozoru wizyjnego. Planowanie – rola inwestora/użytkownika końcowego* (str. 18). Analiza najnowszej wersji normy VSS jasno pokazuje przesunięcie akcentów: od technologii w stronę roli inwestora i użytkownika końcowego oraz świadomego podejmowania decyzji już na etapie planowania systemu.

Numer zamyka niezwykle istotny materiał *Odpowiedzialność kierownictwa w świetle krajowych regulacji implementujących Dyrektywy CER i NIS2* (str. 58). Nowe przepisy nie pozostawiają wątpliwości – bezpieczeństwo przestaje być zagadnieniem technicznym delegowanym do działów operacyjnych, a staje się jednoznaczną odpowiedzialnością zarządu.

To wydanie „a&s Polska" nie jest jedynie zbiorem artykułów. To mapa drogowa dla wszystkich, którzy odpowiadają za bezpieczeństwo w świecie rosnącej niepewności, presji regulacyjnej i zacierających się granic między domenami zagrożeń. Jeśli chcesz zrozumieć, dokąd zmierza branża i jak przygotować się na nadchodzące wyzwania – ta lektura jest punktem obowiązkowym. •

Redakcja

A&S POLSKA WYDANIE ONLINE: aspolska.pl

CZASOPISMO RYNKU SECURITY

a&s POLSKA

02 (56) / 2026

Spis treści

PRODUKTY NUMERU

RYNEK SECURITY

REDAKCJA

ADRES REDAKCJI
a&s Polska
ul. Złoczowska 25
03-972 Warszawa
info@aspolska.pl
www.aspolska.pl

PREZES ZARZĄDU
Mariusz Kucharski

REDAKTOR NACZELNA
Marta Dynakowska

Z-CA RED. NACZELNEGO
Jan T. Grusznic

REDAKCJA
Monika Żuber-Mamakis
Adela Prochyra

DZIAŁ REKLAMY
Iwona Krawiec

DZIAŁ PROJEKTÓW SPECJALNYCH
Jolanta A. Kucharska
Aleksandra Czapska

CENTRUM KOMPETENCJI
Jacek Grzechowiak

KOREKTA
Jolanta Kucharska

PROJEKT GRAFICZNY I SKŁAD
Marta Kołodziejak

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

SZEROKIE SPOJRZENIE NA **BEZPIECZEŃSTWO**

BCS-P-PEIP2X4FCR3L3-Ai1

BCS

Kamera panoramiczna 8 Mpix zapewnia pełną kontrolę dzięki kątowi widzenia 180° – jedna kamera może zastąpić kilka urządzeń. NightColor 2.0 gwarantuje kolorowy obraz nawet w nocy, a inteligentna analiza obrazu ogranicza fałszywe alarmy. Wbudowany mikrofon i głośnik umożliwiają dwukierunkową komunikację, a promiennik IR i światła białego skutecznie doświetlają scenę po zmroku. Odporna konstrukcja i zasilanie PoE sprawiają, że to idealne rozwiązanie profesjonalnego monitoringu.

POLSKA MARKA

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

>> WIĘCEJ PRZECZYTASZ NA STRONIE 8

CZASOPISMO RYNKU SECURITY

a&S POLSKA

02 (56) / 2026

Spis treści

INFRASTRUKTURA KRYTYCZNA

CYBERBEZPIECZEŃSTWO

SERWIS INFORMACYJNY

camect

INTELIGENTNY HUB
efektywna i skuteczna detekcja zagrożenia

SZTUCZNA INTELIGENCJA
wbudowana, zaawansowana sztuczna inteligencja

ROZRÓŻNIA PONAD 30 TYPÓW OBIEKTÓW
ludzi, pojazdy, zwierzęta

WSPÓŁDZIAŁANIE
z różnymi kamerami IP

KOMPATYBILNOŚĆ
z SAFESTAR

OFICJALNY DYSTRYBUTOR:

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

www.linc.pl

WIĘCEJ O NAS:

Linc Polska Sp. z o.o.

Prezentujemy najnowsze urządzenia z oferty firm

BCS, HIKVISION, TP-LINK, VCS, WINKHAUS





BCS

BCS-P-PEIP2X4FCR3L3--Ai1 – szerokie spojrzenie na bezpieczeństwo

BCS-P-PEIP2X4FCR3L3-Ai1 jest nowoczesną kamerą dwuobiektywową zaprojektowaną z myślą o skutecznym monitoringu rozległych przestrzeni. Dzięki zastosowaniu dwóch przetworników 4 Mpix generuje obraz o łącznej rozdzielczości 8 Mpix, oferując jednocześnie szeroki kąt obserwacji – aż 180° w poziomie oraz 65° w pionie. Co istotne, mimo podwójnej optyki model ten zajmuje tylko jeden kanał w rejestratorze, tak jak standardowa kamera.

Bardzo jasny obiektyw o aperturze F1.0 i wysoka czułość na poziomie 0,002 lx przekładają się na doskonałą jakość kolorowego obrazu nawet w trudnych warunkach oświetleniowych. Podwójny system doświetlenia – podczerwień (IR) umieszczony po bokach oraz światło białe umieszczone centralnie zapewniają oświetlenie pełnego kadru aż do 30 m. Skuteczność ochrony zwiększają umieszczone centralnie światła aktywnego odstraszania, które podczas alarmu emitują intensywne czerwono-niebieskie światło, wyraźnie sygnalizując zdarzenie w chronionym obszarze. Model ma również wbudowany mikrofon i głośnik, a także dodatkowe wejście i wyjście audio, co umożliwia prowadzenie dwukierunkowej komunikacji z poziomu systemu monitoringu czy aplikacji.

Działanie kamery uzupełniają inteligentne funkcje analizy obrazu, takie jak ochrona perymetryczna oraz ultra detekcja ruchu, które pozwalają na szybkie wykrywanie potencjalnych zagrożeń. Opcja filtrowania obiektów pozwala na ograniczenie liczby fałszywych alarmów i skuteczne zarządzanie nimi. Kamera zapewnia szerokie pole widzenia, wysoką jakość obrazu i zaawansowane procedury bezpieczeństwa, sprawdzając się szczególnie w monitoringu otwartych przestrzeni, parkingów czy obiektów przemysłowych. •

Więcej na: www.bcs.pl

HIKVISION

Skuteczna ochrona perymetryczna

Hikvision HM-TX3840-25-G1-T3 to zaawansowana kamera bispektralna, zaprojektowana do skutecznej ochrony perymetrycznej w każdych warunkach środowiskowych.

Urządzenie łączy moduł termowizyjny o rozdzielczości 384 × 288 pikseli z 4-Mpix kamerą pasma widzialnego oraz szybkoobrotową kamerą PTZ z 40-krotnym zoomem optycznym. Takie zestawienie pozwala na swobodną detekcję, weryfikację i identyfikację obiektów.

Przetwornik termowizyjny typu VOx o wysokiej czułości (<25 mK) pozwala na wykrywanie minimalnych różnic temperatury, co przekłada się na skuteczne działanie w nocy, we mgle, w dymie oraz przy małych różnicach kontrastu termicznego.

Kamera oferuje zaawansowaną analitykę obrazu w paśmie zarówno widzialnym, jak i termowizyjnym, w tym detekcję wtargnięcia, przekroczenie linii oraz wczesne wykrywanie pożaru. Kluczowym elementem jest technologia TandemVu, zapewniająca współpracę wszystkich modułów. Po wykryciu zdarzenia przez termowizję kamera PTZ automatycznie jest kierowana w miejsce incydentu. Operator otrzymuje jednocześnie widok ogólny i szczegółowy w obu obszarach widma, co znacząco poprawia dokładność obserwacji i skraca czas reakcji.

HM-TX3840-25-G1-T3 sprawdza się w ochronie infrastruktury krytycznej, obiektów przemysłowych czy logistyki. Integracja kilku technologii w jednej platformie pozwala znakomicie zwiększyć skuteczność systemu bezpieczeństwa, poprawić reakcje operatora, a jednocześnie ograniczyć liczbę fałszywych alarmów. •

Więcej na: www.hikvision.com/pl/

RACS 5

roger
ASSA ABLOY

Nowoczesna transformacja bez rewolucji

Nowy system, ta sama instalacja.
Wykorzystaj istniejącą infrastrukturę i zyskaj nowe możliwości.

Maksymalne bezpieczeństwo. Minimalny wysiłek.
Protokół OSDP, szyfrowana komunikacja, Grade 4 – najwyższy poziom w standardzie.

Nowoczesność w praktyce: efektywność, komfort, elastyczność.
Wydajna baza SQL, bezpieczna identyfikacja mobilna i wielostanowiskowa architektura.

Jeden system. Pełna kontrola.
Zarządzaj dostępem, monitoruj i wizualizuj zintegrowane systemy bezpieczeństwa – wszystko z jednego miejsca.

Technologia, która myśli jak Ty.
Nowoczesny interfejs, intuicyjna obsługa, pełna kontrola.

Zainwestuj w przyszłość – dziś.
RACS 5 to długoterminowe wsparcie i rozwój.

Experience a safer
and more open world

TP-LINK

Omada ER701-5G-Outdoor dla biznesu bez przerw

W dynamicznym środowisku biznesowym stabilny dostęp do Internetu jest kluczowy dla ciągłości operacyjnej – niezależnie od lokalizacji. TP-link Omada ER701-5G-Outdoor to zewnętrzna brama sieciowa 5G zaprojektowana z myślą o firmach działających w miejscach bez dostępu do infrastruktury kablowej lub wymagających niezawodnego łącza zapasowego.

Urządzenie wykorzystuje technologię Omada Ultra5G opartą na standardzie 3GPP Release 16, paśmie Sub-6 GHz oraz konfiguracji 4×4 MIMO. W połączeniu z dziewięcioma antenami komórkowymi o wysokim zysku zapewnia stabilną i wydajną transmisję danych, umożliwiając płynną pracę systemów sprzedażowych, monitoringu wizyjnego czy pracy zdalnej. Obsługa sieci 5G NR o prędkości do 7,01 Gb/s pozwala wykorzystać rozwiązanie zarówno jako główne, jak i zapasowe łącze WAN.

Omada ER701-5G-Outdoor integruje łączność 5G/LTE z przewodową infrastrukturą sieciową oraz platformą Omada SDN, umożliwiając centralne zarządzanie rozproszoną siecią z poziomu chmury, aplikacji lub przeglądarki. Port 2,5G Ethernet z obsługą zasilania PoE pozwala na jednoczesne zasilanie urządzenia i transmisję danych jednym przewodem, co upraszcza i przyspiesza instalację. Dwa sloty Nano SIM zapewniają automatyczne przełączanie awaryjne, zwiększając ciągłość działania.

Konstrukcja przystosowana do pracy na zewnątrz, obudowa IP66 oraz odporność na temperaturę od -30°C do 60°C umożliwiają całoroczną, bezobsługową pracę urządzenia w wymagających warunkach.

Omada ER701-5G-Outdoor objęta jest pięcioletnią gwarancją TP-Link. •

Więcej na: www.tp-link.com/pl/

VCS

Mini iTower – bezprzewodowa, szybko wdrażalna ochrona mobilna

Mini iTower to mobilna jednostka alarmowa szybkiego wdrażania, zaprojektowana zgodnie z zasadą trzech kroków: „POSTAW – WŁĄCZ – CHROŃ". Wyróżnia ją łatwość obsługi oraz swoboda wyboru lokalizacji, a także zaawansowana funkcja wykonywania zdjęć – zarówno na żądanie użytkownika, jak i automatycznie przy każdym wywołaniu alarmu. System zapewnia nie tylko skuteczną ochronę, lecz także natychmiastowy wgląd w bieżącą sytuację.

Zalety:

- **Pełna autonomiczność energetyczna –** niezależne zasilanie solarne umożliwia nieograniczony czas pracy przy dostępie do światła słonecznego (bez słońca od ok. 14 dni do 3 miesięcy, zależnie od wersji).
- **Ochrona 360° i wizualna weryfikacja zagrożeń –** cztery czujki MotionCam zapewniają pełne pokrycie chronionego terenu, a seria zdjęć sytuacyjnych wykonanych i przesyłanych po wykryciu intruza umożliwia błyskawiczną ocenę zdarzenia oraz redukcję kosztów związanych z fałszywymi alarmami.
- **Lekka, kompaktowa i modułowa konstrukcja –** transport oraz rozstawienie systemu przez jednego operatora zajmuje zaledwie kilka minut.
- **Gotowość do działania od razu po uruchomieniu –** wieża jest skonfigurowana i przygotowana do natychmiastowej pracy.

Ponadto wyjątkową łatwość obsługi zapewnia możliwość zarządzania wszystkimi urządzeniami w ramach jednej wieży, jak również wieloma wieżami jednocześnie, za pomocą jednego intuicyjnego interfejsu. Zastosowane aplikacje są dostosowane do wszystkich platform – od komputera, przez tablet i telefon, aż po centrum zarządzania ze zintegrowanym systemem obsługi zdarzeń. •

Więcej na: www.vcs.pl

WINKHAUS

blueEvo – bezprzewodowy system kontroli dostępu do nowoczesnych obiektów

blueEvo to nowoczesny system elektronicznej kontroli dostępu, który łączy wysoki poziom bezpieczeństwa z elastycznością oraz wygodą zarządzania uprawnieniami.

Oferuje szeroką gamę komponentów, w tym elektroniczne wkładki różnych typów, klamki wewnętrzne i zewnętrzne, czytniki online i offline, zamki meblowe oraz identyfikatory, odpowiadające na zróżnicowane potrzeby użytkowników. Skutecznie eliminuje dostęp do pomieszczeń osobom nieuprawnionym, a także ogranicza możliwość wejścia poza godzinami pracy dzięki zastosowaniu profili czasowych oraz regularnej aktualizacji uprawnień dostępu.

blueEvo opiera się na tzw. sieci wirtualnej, w której identyfikatory użytkowników przenoszą dane pomiędzy oprogramowaniem a czytnikami oraz wkładkami lub klamkami elektronicznymi zamontowanymi w drzwiach. Taki sposób komunikacji, niewymagający okablowania, sprawia, że system jest szybki i wygodny w montażu.

Rozwiązanie to eliminuje również ryzyko zgubienia lub kradzieży kluczy. Po upływie zaprogramowanego czasu dostępu identyfikator staje się bezużyteczny, a administrator może go zablokować w kilku kliknięciach za pomocą oprogramowania. Istotną zaletą systemu jest także jego niezależność od zewnętrznych źródeł energii – komponenty montowane w drzwiach są zasilane bateryjnie, dzięki czemu pozostają odporne na przerwy w dostawie prądu.

System blueEvo, w 100% produkowany w Niemczech, znakomicie sprawdza się w różnorodnych obiektach – od zakładów przemysłowych i biurowców po placówki medyczne oraz infrastrukturę krytyczną. •

Więcej na: www.winkhaus.pl

VCS

MINI TOWER®

360°
zakres detekcji 360°

autonomiczność energetyczna

alarm + zdjęcia

gotowość do działania

BEZPRZEWODOWA SZYBKOWDRAŻALNA MOBILNA OCHRONA

Powered by: AJAX

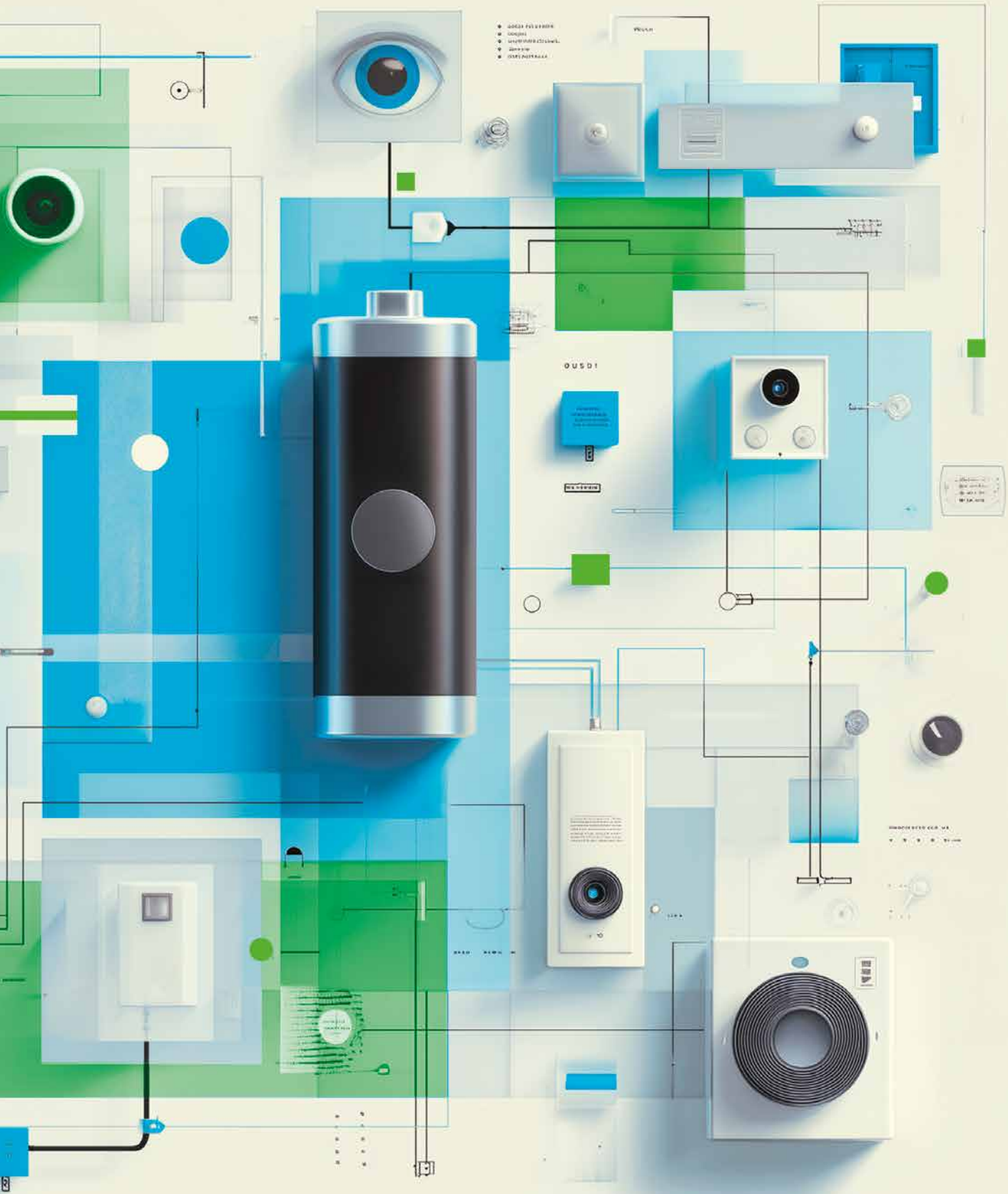
WWW.VCS.PL

Bateria nie może zawieść

Prawda o zasilaniu awaryjnym w systemach zabezpieczeń

Zanik prądu w newralgicznym momencie to najgorsza rzecz, jaka może przydarzyć się systemowi zabezpieczeń. Wyłączone kamery, głucha centrala alarmowa, zablokowane drzwi – albo przeciwnie, drzwi, których nie można zamknąć. Jak sprawić, by baterie naprawdę chroniły, a nie tylko stwarzały pozory ochrony? Odpowiedź tkwi w technologii, normach i twardych liczbach.

Jan T. Grusznic



Rynek rośnie szybciej niż chcielibyśmy myśleć

Rynek zasilaczy dedykowanych systemom bezpieczeństwa przestał być niszą. Według prognoz analityków jego globalna wartość wyniesie ponad 11,5 mld USD w 2025 r. – i do roku 2030 urośnie do niemal 20 mld USD. Średniorocznastopa wzrostu na poziomie ponad 11% stawia ten segment w gronie najdynamiczniej rozwijających się gałęzi branży security.

Za tym wzrostem stoją dwa czynniki: coraz bardziej wymagające przepisy dotyczące ochrony obiektów oraz postępująca cyfryzacja infrastruktury, która oznacza więcej urządzeń IP – a każde z nich potrzebuje ciągłego zasilania. Na czele stawki plasują się Eaton z udziałem blisko 27%, XP Power z ponad 20% i Emerson/Artesyn przekraczający 17% globalnego rynku.

Rok	Wartość rynkowa (mld USD)	Dynamika r/r
2025	11,48	—
2026	12,76	+11,1%
2028	15,79	+10,9%
2030	19,56	+10,5%

Prognozowana wartość globalnego rynku Security Power Supply. Źródło: opracowanie własne na podstawie danych rynkowych

LiFePO4 kontra AGM – pojedynek, który już się rozstrzygnął

Jeszcze kilka lat temu kwasowe akumulatory AGM były oczywistym wyborem w systemach alarmowych i kontroli dostępu. Niski koszt zakupu, powszechna dostępność i prosta obsługa przekonywały instalatorów. Tyle że rachunek ekonomiczny zaczyna wyglądać zupełnie inaczej, gdy spojrzymy na całkowity koszt posiadania.

Weźmy dwa praktyczne scenariusze z codziennej pracy instalatora. Punkt kamerowy pobierający 15 W i wymagający 12 godzin autonomii potrzebuje akumulatora AGM o pojemności ok. 35-40 Ah przy 12 V. Przyjmując wymianę co 4 lata i 10-letni cykl eksploatacji, oznacza to dwie wymiany — łącznie trzy zestawy plus koszty obsługi serwisowej. Akumulator LiFePO4 o pojemności 20-25 Ah (dzięki pełnemu DoD – ang. Depth of Discharge, czyli głębokość rozładowania) wystarczy na całe 10 lat bez żadnej wymiany, przy koszcie zakupu porównywalnym lub niższym i zerowych kosztach eksploatacji.

Bardziej wyrazisty jest przypadek wieży CCTV pobierającej 180 W, zaprojektowanej na 60 godzin autonomii. Wymagana pojemność instalowana przy akumulatorach AGM (DoD 50%) wynosi ok. 2 100–2 200 Ah. Przy wymianie co 4 lata i 10-letnim cyklu eksploatacji niezbędne są trzy zestawy bateryjne (dwie wymiany). Łączny koszt całkowity: zakup, dwie wymiany i serwis zamknie się w przedziale 25–40 tys. PLN. System LiFePO4 potrzebuje o połowę mniejszej pojemności instalowanej (ok. 1 200 Ah), nie wymaga wymiany przez cały cykl i kosztuje ok. 15–25 tys. PLN. Różnica niemal dwa razy na korzyść litu rośnie wprost proporcjonalnie do mocy i wymaganego czasu podtrzymania.

Kluczowy argument techniczny to krzywa rozładowania. Bateria LiFePO4 utrzymuje napięcie bliskie 12,8 V niemal do całkowitego wyczerpania. Elektronika w systemach zabezpieczeń po prostu na tym zyskuje – stabilne zasilanie to stabilna praca czujników, central i kamer. AGM tymczasem już w połowie swojej pojemności oddaje napięcie wyraźnie obniżone, co może oznaczać nieoczekiwane resetowanie urządzeń.

Dobra wiadomość dla tych, którzy wahają się przy cenie zakupu: zestawy bateryjne Li-ion tanieją systematycznie. W 2024 roku średnia cena rynkowa wyniosła ok. 450 PLN/kWh – o 20% mniej niż rok wcześniej. Prognozy na 2030 rok zakładają poziom 350–380 PLN/kWh. Punkt zwrotny opłacalności przesunął się na korzyść litu definitywnie.

Normy mówią wprost: ile godzin, to ile

Branżowy żargon potrafi zniechęcić, ale wymogi normowe w zakresie zasilania rezerwowego są zaskakująco konkretne. Polska norma PN-EN 50131-6 dla systemów SSWiN dzieli instalacje na cztery stopnie zabezpieczenia (Grade 1–4) i dla każdego z nich precyzuje minimalny czas podtrzymania zasilania.

Dla obiektów podwyższonego ryzyka (Grade 3 i 4) standardem są 60 godziny pracy bateryjnej – a w wariancie B aż 120 godzin. Wyjątek od tej reguły istnieje tylko wtedy, gdy system automatycznie raportuje zanik zasilania do stacji monitorowania z zagwarantowanym czasem przyjazdu serwisu. Wtedy minimalny próg spada do 4 godzin.

Norma PN-EN 60839-11-1 dla systemów kontroli dostępu jest nieco łaskawsza: wymaga co najmniej 2 godzin pracy pod pełnym obciążeniem. W obiektach infrastruktury krytycznej (Grade 4) dochodzi jeszcze

Parametr	AGM (VRLA)	LiFePO4
Gęstość energii	30–50 Wh/kg	150–200 Wh/kg
Żywotność (cykle)	300–500	2000–6000
Sprawność ładowania	~85%	95–98%
Dopuszczalne rozładowanie (DoD)	50%	do 100%
Samorozładowanie	średnie	bardzo niskie

Porównanie kluczowych parametrów technicznych akumulatorów AGM i LiFePO4

Stopień (Grade)	Poziom ryzyka	Typ A (godz.)	Typ B (godz.)
Grade 1	Bardzo niskie	12	24
Grade 2	Małe	12	24
Grade 3	Wysokie	60	120
Grade 4	Bardzo wysokie	60	120

Wymagania czasowe podtrzymania zasilania wg PN-EN 50131-6

wymóg stałego monitorowania zasilania i automatycznego raportowania usterek.

Osobną kategorię stanowią instalacje przeciwpożarowe. Zasilacze do central SAP i DSO muszą mieć certyfikaty CNBOP-PIB. Wg normy PN-EN 54-4 dla dźwiękowego systemu ostrzegawczego (DSO) standardem jest 30 godzin gotowości i co najmniej 30 minut pracy alarmowej przy pełnej mocy wzmacniaczy. Monitoring wizyjny na składowiskach odpadów rządzi się własną regułą: polskie prawo (Dz.U. 2019 poz. 1755) wymaga minimum 2 godzin podtrzymania.

Jak liczyć pojemność, żeby nie liczyć strat

Dobór akumulatora „na oko" to przepis na kłopoty. Precyzyjne obliczenia bilansowe powinny uwzględniać cztery kluczowe zmienne: całkowity pobór prądu systemu (w trybie czuwania i alarmu), wymagany czas autonomii, współczynnik starzenia baterii oraz, często zapominany przez instalatorów, temperaturowy współczynnik pojemności.

Ten ostatni potrafi zaskoczyć. W temperaturze 0°C sprawność ogniwa kwasowego spada do zaledwie 71% pojemności nominalnej. Oznacza to, że akumulator dobrany pod laboratoryjne 20°C może nie sprostać wymogom normy podczas mroźnej nocy. Praktyczna zasada brzmi: przy instalacjach narażonych na niskie temperatury zwiększ obliczoną pojemność o co najmniej 40%.

Sprawność ładowania to kolejna zmienna, którą łatwo zbagatelizować. Przy akumulatorach kwasowych wynosi ona ok. 85% – co oznacza, że 15% energii z sieci przepada bezpowrotnie jako ciepło. Ogniwa LiFePO4 osiągają sprawność 95–98%, co przy dużych instalacjach przekłada się na zauważalne oszczędności na rachunku za prąd.

Monitoring zdalny – serwis, który sam do nas dzwoni

Nowoczesne zasilacze potrafią znacznie więcej niż trzymać baterię pod napięciem. Urządzenia klasy APS-30-BO wykonują automatyczny pomiar rezystancji wewnętrznej akumulatora i porównują wynik z wartością wzorcową nowej baterii. Wzrost tego parametru o 100% to jednoznaczny sygnał: czas wymiany. Bez pomiaru na żywo tego nie widać dopóki bateria nie zawiedzie w najgorszym momencie.

Zasilacze wyposażone w interfejsy MQTT lub SNMP wpisują się w logikę Przemysłu 4.0: przekazują dane diagnostyczne do centralnych systemów zarządzania budynkiem lub platform monitorujących. Oprogramowanie pozwala na zdalny podgląd prądów wyjściowych i inicjowanie testów dynamicznych bez wychodzenia z biura.

Zdalna diagnostyka to nie tylko wygoda, ale konkretna oszczędność. Szacuje się, że inteligentny monitoring redukuje koszty serwisu o około 30%, eliminując niepotrzebne przejazdy do obiektów, które „powinny" wymagać uwagi, a faktycznie działają bez zarzutu.

Wieże mobilne – zabezpieczenia tam, gdzie nie ma prądu

Coraz większym segmentem rynku stają się autonomiczne mobilne wieże monitorujące – rozwiązanie dla placów budowy, terenów otwartych i infrastruktury liniowej, gdzie podłączenie do sieci energetycznej jest niemożliwe lub nieopłacalne. Globalny rynek tych urządzeń wyceniany jest na ok. 1,36 mld USD w 2025 roku; do 2030 roku ma urosnąć do 2,18 mld USD. Typowa wieża klasy „Pro" to maszt teleskopowy osiągający od 5,5 do 7,2 m, bank akumulatorów LiFePO4 lub AGM o pojemności

Cecha	Wieża lekka	Wieża ciężka	Mobilny punkt na latarni
Akumulator	100–200 Ah (LiFePO4)	400–900 Ah (AGM/GEL)	18–40 Ah (LFP)
Moc PV	300–600 W	1,3–2,0 kW	15–50 W
Autonomia (zima)	2–4 dni	7–20 dni	12–24 godz.
Łączność	4G / 5G / Starlink	4G / 5G / P2P Radio	4G / LTE

Porównanie parametrów zasilania mobilnych systemów monitorujących

200–900 Ah oraz panele fotowoltaiczne o mocy 1–2 kW, niekiedy wsparte turbinką wiatrową lub ogniwami paliwowymi. Autonomia takiego systemu w polskich warunkach zimowych wynosi 7–10 dni przy obciążeniu rzędu 25–40 W.

Wyzwaniem ostatnich lat jest integracja AI bezpośrednio w kamerach *(edge processing)*. Aktywna analityka wideo jak detekcja osób, pojazdów, analiza zachowań wpływa na zwiększenie poboru energii w zależności od zastosowanego rozwiązania.

Polski rynek: duży gracz w globalnej grze

Polska branża security należy do największych w Europie Środkowo-Wschodniej. Całkowita wartość rynku rozwiązań bezpieczeństwa i ICT w Polsce szacowana jest na 74 mld PLN w 2025 r. Krajowi producenci i instalatorzy aktywnie wdrażają nowe technologie zarówno pod presją rosnących wymogów ustawowych, jak i z powodów czysto ekonomicznych.

Polska pozostaje też istotnym uczestnikiem łańcucha dostaw ogniw litowych

Bateria to nie akcesorium, to element systemu. Wybór technologii powinien być poprzedzony pełną analizą TCO, a nie tylko porównaniem cen katalogowych.

w skali europejskiej, choć wartość eksportu ogniw Li-ion wyniosła 3,2 mld EUR w pierwszej połowie 2024 r., nieco poniżej rekordowych poziomów sprzed roku. Zmieniający się globalny rynek surowców i przyspieszona lokalizacja produkcji w Europie stawiają krajowych graczy w dobrej pozycji na kolejne lata.

Trzy wnioski, które zmienią sposób myślenia o zasilaniu

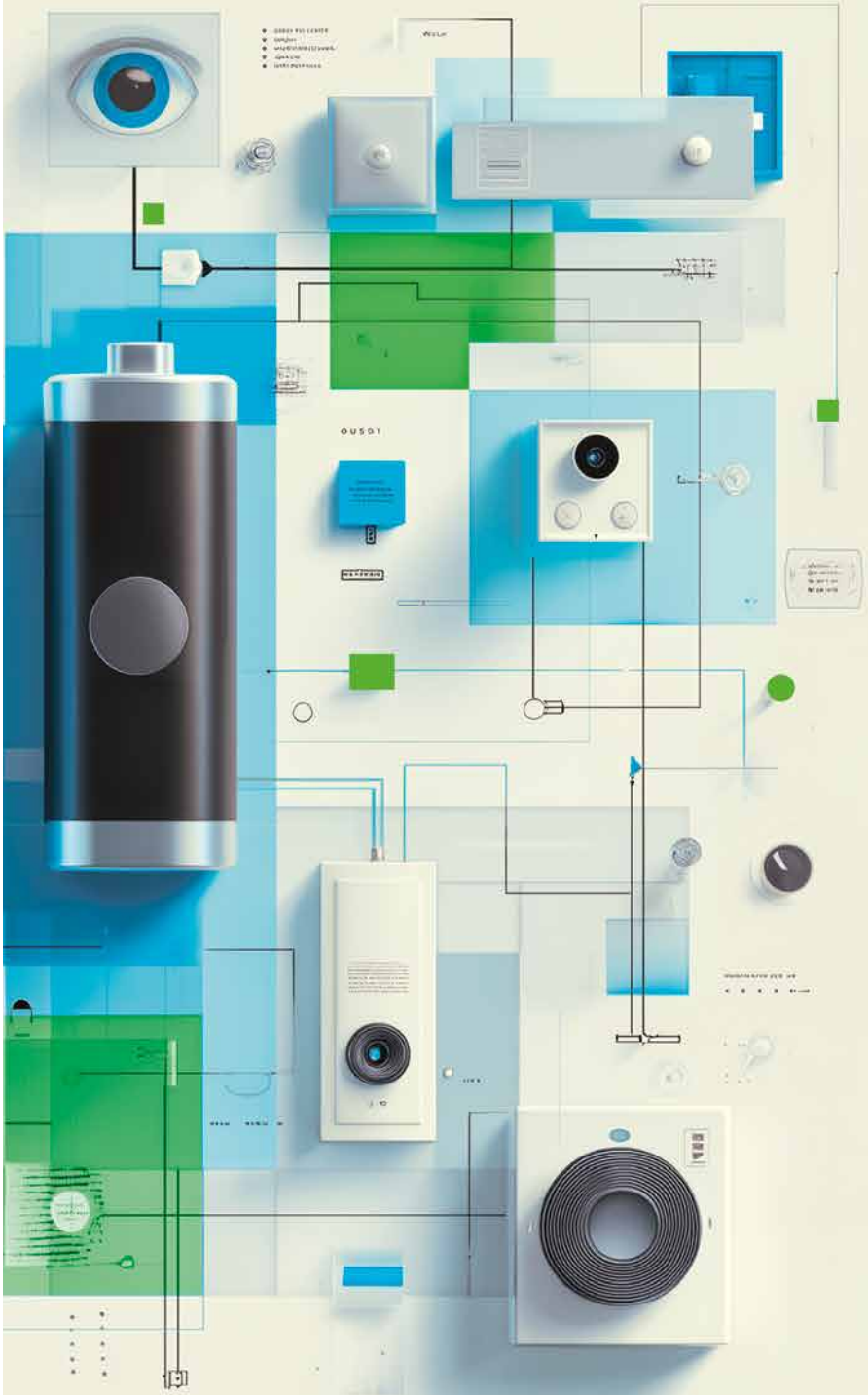
Po pierwsze: bateria to nie akcesorium, to element systemu. Wybór technologii powinien być poprzedzony pełną analizą TCO, a nie tylko porównaniem cen katalogowych. Przy obecnych trendach cenowych decyzja o przejściu na LiFePO4 w systemach off-grid uzasadnia się sama: całkowity koszt posiadania jest o ok. 60% niższy w horyzoncie 8 lat.

Po drugie: normy to minimalny punkt wyjścia, nie cel sam w sobie. Zwłaszcza dla obiektów Grade 3 i 4 warto rozważyć przekroczenie wymogów normatywnych szczególnie gdy mamy do czynienia z instalacjami w trudnym terenie lub obiektami, gdzie reakcja serwisu może trwać wiele godzin.

Po trzecie: zdalna diagnostyka to inwestycja, która zwraca się szybciej niż myślimy. Systemy z monitoringiem SNMP/MQTT redukują koszty obsługi serwisowej o nawet 30% – i co ważniejsze, pozwalają reagować na problemy zanim staną się awariami. •

Jan T. Grusznic
Redaktor „a&s Polska”

Artykuł przygotowany na podstawie danych rynkowych MarketsandMarkets, danych branżowych oraz obowiązujących norm PN-EN 50131-6 i PN-EN 60839-11-1.



Ilustracje: Marta Kołodziejak / A&S AI Studio

Kto i dla kogo opracował normę PN-EN 62676 Systemy dozoru wizyjnego

Planowanie – rola inwestora, użytkownika końcowego

Jak wskazano we wprowadzeniu do drugiego wydania normy, anuluje ono i zastępuje pierwsze (ang. *cancels and replaces*) oraz stanowi rewizję techniczną (*constitutes a technical revision*). Już samo użycie tych określeń jest odstępstwem od reguł języka norm. Zgodnie z nimi kolejne wydanie zastępuje (*supersedes*) poprzednie, które staje się tym samym wycofane (*withdrawn*). I rzeczywiście – zmiany są radykalne, i to nie tylko w odniesieniu do planowania.

Co nowego w PN-EN 62676-4:2026-01E?

W informacji prasowej przygotowanej przez kierownika grupy projektowej, która opracowała normę IEC 62676-4:2025, wskazano cztery grupy zagadnień zawierających nowe zapisy:

1. nowe gęstości pikselowe,
2. koncepcję zabezpieczeń,
3. obsługę,
4. stopniowanie zabezpieczeń i wymagania infrastruktury krytycznej.

Nowe gęstości pikselowe – koniec epoki DORI/MDORII

Sądząc po wypowiedziach, które pojawiły się po wprowadzeniu nowego wydania normy, najbardziej „ekscytujące" dla branży są zmiany dotyczące określenia celów prowadzenia dozoru wizyjnego (zadań operatora). Zdefiniowano je na nowo, nadając im nowe nazwy i przypisując odmienne wymagania jakościowe obrazu (tzw. gęstości pikselowe).

Zerwano nie tylko z nazewnictwem stosowanym od czasu, gdy – na bazie dokumentów brytyjskiej policji – opracowano pierwszą normę dotyczącą CCTV w zastosowaniach związanych z zabezpieczeniami (1996 r.). Redefiniując gęstości pikselowe, zerwano również z dotychczasową bazą odniesienia dla wyższych jakości obrazu (HDTV i UHDTV), którą była jakość obrazu telewizji standardowej rozdzielczości (SDTV, potocznie nazywanej telewizją analogową).

Wprowadzono dwa nowe obrazy testowe, zastępujące jeden poprzednio

Wieloczęściową normę PN-EN 62676 opracowaliśmy sami dla siebie – producenci, projektanci i użytkownicy systemów dozoru wizyjnego dla producentów, projektantów i użytkowników systemów dozoru wizyjnego. W październiku 2025 r. – po 11 latach od pierwszego – wprowadziliśmy do zbioru norm drugie wydanie części IEC 62676-4, a w nim m.in. nowe zapisy dotyczące udziału inwestora/użytkownika końcowego w procesie planowania zabezpieczeń.

Waldemar Więckowski

używany. Zmiany te określono jako modernizację dotychczasowego systemu MDORII, obejmującego sześć gęstości pikselowych, do nowego systemu O2DCPVS, z siedmioma gęstościami pikselowymi, różniącymi się od poprzednio stosowanych i podzielonymi na dwie grupy.

Słowem: koniec epoki MDORII – początek epoki O2DCPVS

O tej zmianie definicji celów prowadzenia dozoru wizyjnego wspominałem już w części I niniejszego artykułu (nr 04/2025). Zagadnienie to samo w sobie wymaga jednak odrębnego omówienia oraz właściwego wprowadzenia. Niektóre wypowiedzi zdają się bowiem świadczyć o tym, że ich autorzy nie pamiętają, nie wiedzą lub nie rozumieją pojęć wcześniej zdefiniowanych w normie jako MDORII, a obecnie jako O2DCPVS.

Dlatego w pierwszej kolejności warto odnieść się do zapisów normy dotyczących planowania oraz koncepcji zabezpieczeń (por. pkt 2 wykazu nowych zagadnień). Jest to zresztą logiczna kolejność etapów w procesie implementacji systemów dozoru wizyjnego. Najpierw powinna zostać opracowana koncepcja zabezpieczeń (plan ochrony), a dopiero później wymagania użytkowe, w których określa się zadania operatora, czyli cele prowadzenia dozoru wizyjnego. Te ostatnie opisano w normie skrótem O2DCPVS (a nie OODCPVS, pojawiającym się w wielu informacjach o normie).

Uwaga: druga edycja normy PN–EN 62676-4:2026-01E jest obecnie dostępna w PKN w języku angielskim. Przywołane w niniejszym artykule fragmenty są tłumaczeniem własnym autora i mogą nie być zgodne z polskojęzyczną wersją normy, gdy ta zostanie opracowana i wprowadzona do zbioru Polskich Norm.

Kto powinien planować VSS

W drugim wydaniu normy stwierdza się, że VSS powinien być planowany, instalowany, rozbudowywany, modyfikowany oraz utrzymywany w ruchu wyłącznie (!) przez kompetentnego inżyniera systemowego VSS.

Jest to specjalista, który nie występował w pierwszym wydaniu normy. Jednak uważna analiza jego normatywnie zdefiniowanych kompetencji oraz odniesienie do norm pokrewnych pozwalają zauważyć,

że analogiczna rola została opisana w normie PN–EN 50726-1:2024-08E *Systemy sytuacji awaryjnych i niebezpiecznych – Część 1: Systemy reagowania na sytuacje awaryjne i niebezpieczne (EDRS)*. Występuje tam osoba wykwalifikowana w dziedzinie elektrotechniki (*electrically skilled person*).

W normie PN–EN 50726-1 zdefiniowano również osobę przeszkoloną (*instructed person*). Jej odpowiednikiem w drugim wydaniu normy VSS jest osoba kompetentna w dziedzinie VSS (*competent person VSS*), przeszkolona przez kompetentnego inżyniera systemowego VSS w zakresie przydzielonych zadań kontrolnych w lokalizacji oraz możliwych zagrożeń i konsekwencji niewłaściwego postępowania.

Norma PN–EN 62676-4:2026-01E definiuje ponadto trzecią kategorię – osobę przeszkoloną (*instructed person*), czyli osobę przeszkoloną przez kompetentnego inżyniera systemowego VSS w zakresie zadań wymaganych do obsługi VSS i zdolną do samodzielnej obsługi systemu. Innymi słowy – operatora systemu.

Obsługa VSS – trzy poziomy kwalifikacji

Obsługę VSS określono w sposób porównywalny z obsługą innych systemów zabezpieczeń. Zapewnia to, że z punktu widzenia norm procedury obsługowe są względnie podobne we wszystkich instalowanych systemach zabezpieczeń.

Zdefiniowano trzy poziomy kwalifikacji, przypisane do różnych faz: planowania, instalacji, uruchomienia i eksploatacji VSS. Eksploatację podzielono na konserwację (zapobiegawczą, korygującą oraz ulepszeniową) oraz kontrole wizualne w obiekcie. Określono obszerne listy kontrolne dotyczące kontroli wizualnych, kontroli funkcjonalnych oraz przeglądów serwisowych.

Kompetentny inżynier systemowy VSS

Jest to najwyższy poziom kwalifikacji wymagany do obsługi VSS. Zgodnie z definicją normatywną jest to osoba, która – na podstawie profesjonalnego wykształcenia technicznego, wiedzy i doświadczenia, a także znajomości odpowiednich norm, przepisów i dyrektyw – jest w stanie ocenić prace, które mają być wykonane, oraz rozpoznać możliwe zagrożenia.

W normie opisano kwalifikacje inżyniera systemowego VSS oraz sposób ich potwierdzania. Określono również, że może on być zatrudniony w firmie instalacyjnej lub integrującej systemy, w firmie projektowej albo u właściciela bądź użytkownika VSS.

Koncepcja zabezpieczeń

Jak napisano we wprowadzeniu do drugiego wydania normy, uwzględniono w nim żądanie określenia koncepcji zabezpieczeń zamiast jedynie analizy ryzyka (*request for define a security concept instead of just a risk analysis*).

Zgodnie z definicją normatywną koncepcja zabezpieczeń stanowi całość zidentyfikowanych ryzyk i zagrożeń w połączeniu z określonymi środkami organizacyjnymi, kadrowymi, technicznymi i strukturalnymi, mającymi na celu zabezpieczenie obiektu oraz zapobieganie zagrożeniom.

Pomocny w wyjaśnieniu tej różnicy jest schemat zamieszczony w normie, przedstawiający strukturę czynności wykonywanych w ramach opracowywania koncepcji zabezpieczeń.

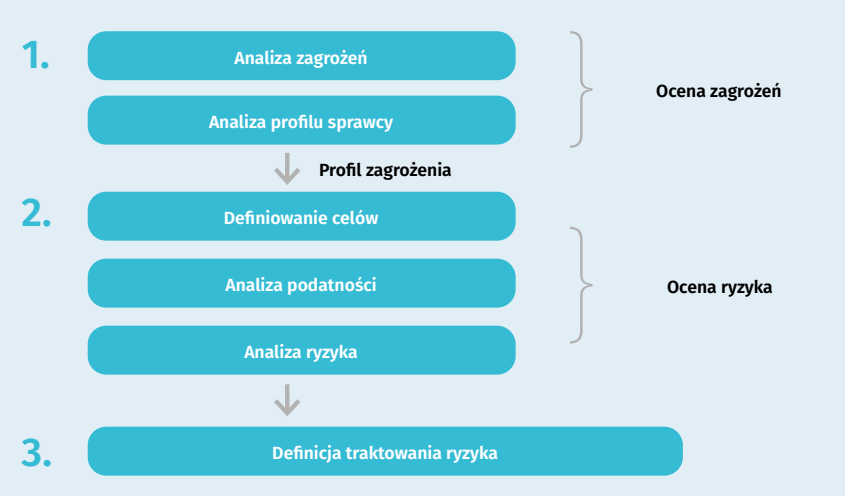
Przed rysunkiem w normie znajduje się również akapit określający VSS jako element „trójczłonowej strategii zabezpieczeń", na którą składają się środki:

- konstrukcyjno-mechaniczne, zapewniające odpowiedni czas odporności,
- elektroniczne, w tym VSS,
- organizacyjne, wspierające bezpieczną i wolną od fałszywych alarmów eksploatację oraz umożliwiające właściwą reakcję na alarmy i awarie, a także zastępujące inne środki w przypadku ich wyłączenia.

Koncepcja zabezpieczeń powinna opisywać wzajemne oddziaływanie tych trzech komponentów w odniesieniu do konkretnych uwarunkowań obiektu.

Kto opracowuje koncepcję zabezpieczeń

Zgodnie z normą podstawą planowania VSS jest koncepcja zabezpieczeń, która powinna mieć postać formalnego dokumentu, a jej aktualizacje powinny stanowić część dokumentacji systemu. Za jej opracowanie

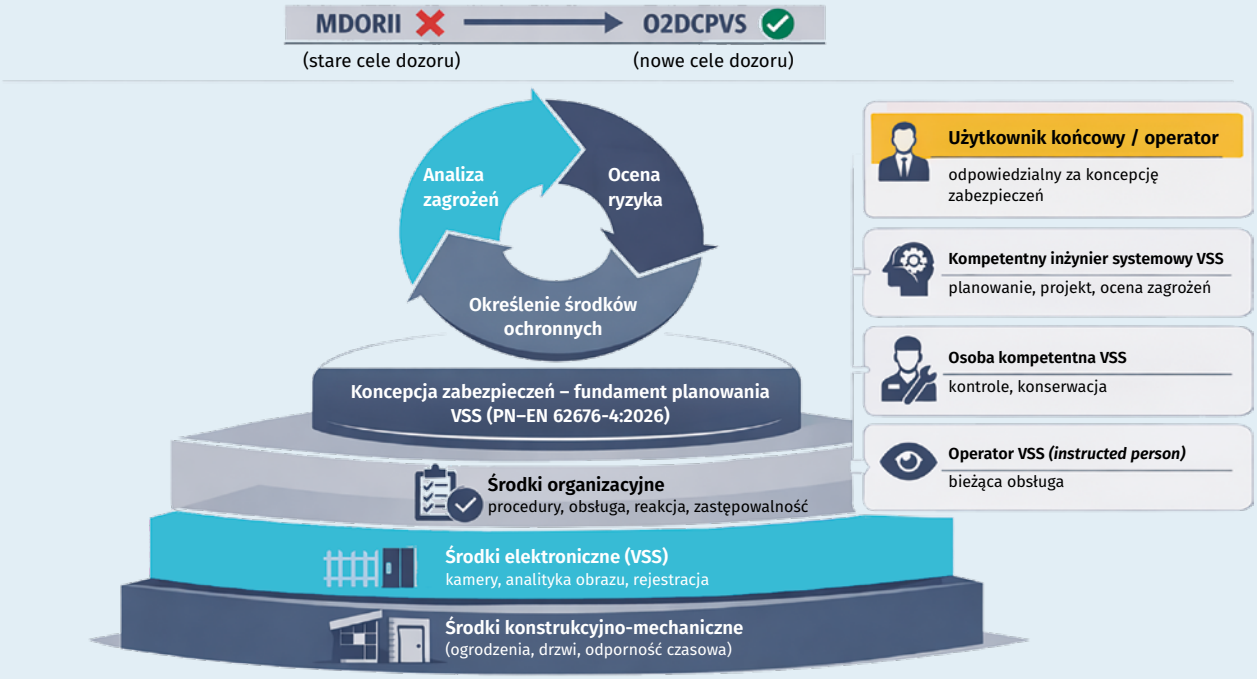


Warto zauważyć, że w pierwszym wydaniu normy ujęta została ocena ryzyka, a nie jedynie „analiza ryzyka". Różnica sprowadza się zatem do wprowadzenia dodatkowej czynności określanej jako „definicja traktowania ryzyka" (*definition of risk treatment*). W praktyce czytelniejsze wydaje się sformułowanie „określenie środków ochronnych" (*definition of protective measures*), użyte w analogicznym schemacie zawartym w dokumencie VdS 3143:2012-09, omówionym w dalszej części artykułu.

odpowiada użytkownik końcowy lub operator. W przypadku rezygnacji z opracowania koncepcji zabezpieczeń użytkownik końcowy powinien złożyć pisemną deklarację projektantowi lub kompetentnemu inżynierowi systemowemu VSS.

Można mieć nadzieję, że to normatywne wymaganie przyczyni się do eliminacji sytuacji, w których inwestor, zamawiając projekt systemu dozoru wizyjnego, całą swoją koncepcję zabezpieczeń sprowadza do sformułowania: „system wideomonitoringu – sztuk jeden".

OD ANALIZY RYZYKA DO KONCEPCJI ZABEZPIECZEŃ – NOWA ROLA INWESTORA W PN–EN 62676



Użytkownik końcowy lub operator określa środki zabezpieczeń wspólnie z podmiotami odpowiedzialnymi oraz innymi uczestnikami projektu (planistami, władzami, ubezpieczycielami, kompetentnymi inżynierami systemowymi VSS itp.). Warunkiem wstępnym opracowania koncepcji zabezpieczeń jest przeprowadzenie analizy zagrożeń i określenie celów ochrony, wykonane przez użytkownika końcowego/operatora lub upoważniony podmiot, np. wyspecjalizowanych planistów lub ekspertów.

Norma wyraźnie zaleca użytkownikowi końcowemu/operatorowi powierzanie oceny ryzyka specjalistom, wskazując normy ISO 31000 oraz IEC 31010 jako źródła szczegółowych informacji dotyczących zarządzania ryzykiem. VSS powinien być zaprojektowany w sposób minimalizujący ocenione ryzyko, a sam proces projektowania powinien być zgodny z normą PN–EN 62676-4.

Dokument VdS 3143:2012-09 Sicherungsleitfaden Perimeter

O koncepcji zabezpieczeń w drugim wydaniu normy napisano niewiele ponad przedstawione powyżej informacje. Może to zaskakiwać, biorąc pod uwagę fakt, że jej wprowadzenie zostało określone jako istotna zmiana techniczna. W rzeczywistości nowością jest samo formalne wprowadzenie koncepcji do normy, a nie jej treść.

Szczegółowe omówienie „holistycznej koncepcji zabezpieczeń" można znaleźć w dokumencie VdS 3143:2012-09, starszym o 13 lat od drugiego wydania normy. Zawarto w nim schemat identyczny strukturalnie z tym zamieszczonym w normie, opisany jako usystematyzowany proces określania środków ochronnych, oparty na logice normy ISO 31000.

Na szczególną uwagę zasługuje zalecenie zaangażowania kierownictwa organizacji w proces decyzyjny związany z opracowywaniem koncepcji zabezpieczeń. Ułatwia to późniejsze podejmowanie decyzji oraz świadome priorytetyzowanie zabezpieczeń, zwłaszcza w warunkach ograniczonego budżetu.

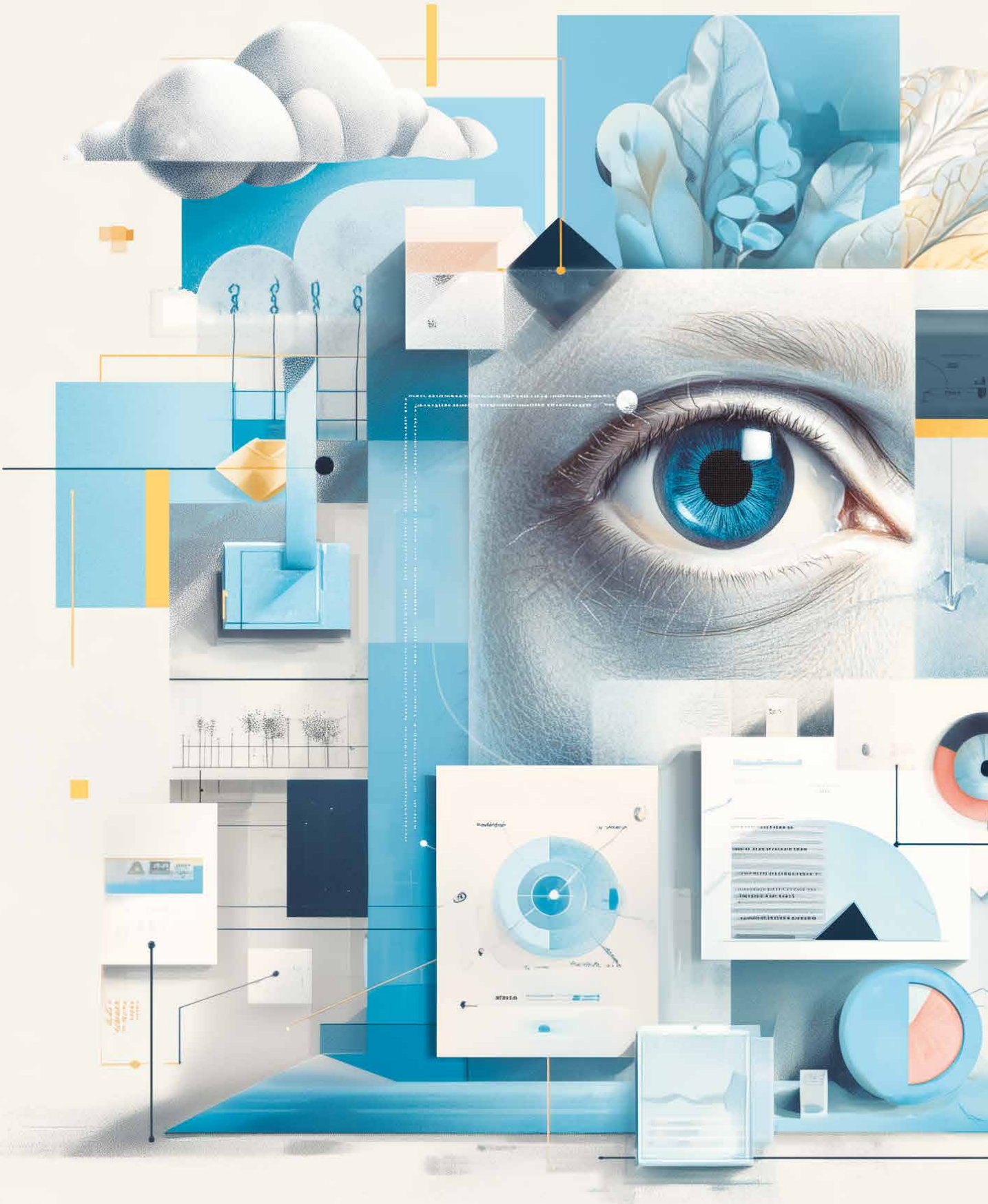
Dokument VdS szerzej omawia również trójczłonową strategię zabezpieczeń oraz podaje przykłady koncepcji dla zewnętrznych perymetrycznych systemów zabezpieczeń. Może on stanowić cenne uzupełnienie Specyfikacji Technicznej PKN-CLC/TS 50661-1:2024-10E, w której po raz pierwszy przedstawiono warstwową koncepcję detekcji intruza.

W przeciwieństwie do specyfikacji, dokument VdS uwzględnia wykorzystanie VSS nie tylko do wizualnej weryfikacji alarmów, lecz również jako sensor wykrywający intruza. •

(Dokument VdS 3143 nie został wymieniony w bibliografii normy. Jest jednak dostępny w Internecie, również w wersji anglojęzycznej.)

Waldemar Więckowski
Członek Komitetu Technicznego nr 52 ds. Systemów Alarmowych Włamania i Napadu przy PKN. Wykładowca na kursach Ośrodka Szkoleniowego Polskiej Izby Systemów Alarmowych

Ilustracje: Marta Kołodziejak / A&S AI Studio



Kamera w chmurze

Rewolucja VSaaS zmienia zasady gry w ochronie obiektów

Rynek dozoru wizyjnego przeżywa największy przewrót od czasu odejścia od analogu. Systemy oparte na chmurze rosną w tempie 18% rocznie, a sztuczna inteligencja przestaje być produktem premium – staje się standardem. Co to oznacza dla instalatorów, dystrybutorów i menedżerów bezpieczeństwa?

Do 2029 r. wartość globalnego rynku VSaaS – systemów dozoru wizyjnego dostarczanych jako usługa chmurowa – ma przekroczyć 10 mld dolarów. Dziś wynosi niespełna 5 mld. Ten skok nie jest przypadkowy: za VSaaS stoi rzeczywista zmiana w sposobie myślenia o bezpieczeństwie fizycznym.

Epoka szaf serwerowych wypełnionych rejestratorami, macierzami dyskowymi i serwerami powoli dobiega końca. W jej miejsce wchodzi model, w którym „mózg" systemu ochrony mieszka w centrum danych dostawcy, a użytkownik zarządza setkami kamer z poziomu przeglądarki internetowej – z dowolnego miejsca na świecie.

Koniec lokalnej serwerowni?

Tradycyjny system dozoru wizyjnego opiera się na fizycznej infrastrukturze: rejestrator NVR lub DVR, serwer z oprogramowaniem VMS, macierze dyskowe, system podtrzymania zasilania i system chłodzenia. Wszystko to wymaga stałego utrzymania, regularnych aktualizacji oraz wykwalifikowanego personelu serwisowego.

VSaaS wywraca ten model do góry nogami. Kamery IP lub urządzenia brzegowe przesyłają strumień obrazu bezpośrednio

do chmury. Całe przetwarzanie, zarządzanie i przechowywanie nagrań odbywa się po stronie dostawcy usługi. Klient dostaje dostęp przez aplikację lub przeglądarkę i przestaje martwić się o to, jaki jest stan macierzy albo czy serwer wymaga restartu.

Kluczową konsekwencją tej zmiany jest skalowalność. W systemach tradycyjnych dodanie kamer często oznacza zakup nowego rejestratora (o określonej liczbie kanałów: 8, 16, 32). W modelu chmurowym można dołączyć w dowolnym momencie jedną kamerę lub dwieście, płacąc wyłącznie za faktycznie wykorzystane zasoby. To szczególnie ważne dla firm, które szybko rosną albo zarządzają wieloma rozproszonymi lokalizacjami.

Trzy warianty, jeden kierunek

Rynek VSaaS nie jest jednolity. Wyróżnia się trzy główne modele wdrożenia, które odpowiadają na różne potrzeby operacyjne i budżetowe.

- ***Hosted VSaaS*** – obraz trafia bezpośrednio do chmury, bez lokalnych rejestratorów. Rozwiązanie typowe dla małych firm i obiektów o rozproszonej strukturze.
- ***Managed VSaaS*** – nagrania mogą być przechowywane lokalnie (np. karta SD w kamerze), ale zarządzanie i dostęp do systemu odbywa się przez chmurę. Kompromis między kontrolą nad danymi a wygodą.
- ***Hybrid VSaaS*** – model, który zyskuje najwięcej zwolenników w sektorze korporacyjnym. Łączy zapis lokalny (wysoka niezawodność, niezależność od łącza) z chmurową analityką i centralnym zarządzaniem.

Model hybrydowy jest szczególnie istotny tam, gdzie liczą się ciągłość nagrywania 24/7 i pełna suwerenność nad materiałem wideo, m.in. w infrastrukturze krytycznej, zakładach przemysłowych i szkołach. Organizacje mogą przy tym zachować istniejące kamery i okablowanie, dodając jedynie inteligentne bramy lub rejestratory hybrydowe, które „upgrade'ują" stare systemy i wzbogacają je o analitykę AI.

AI przestała być dodatkiem

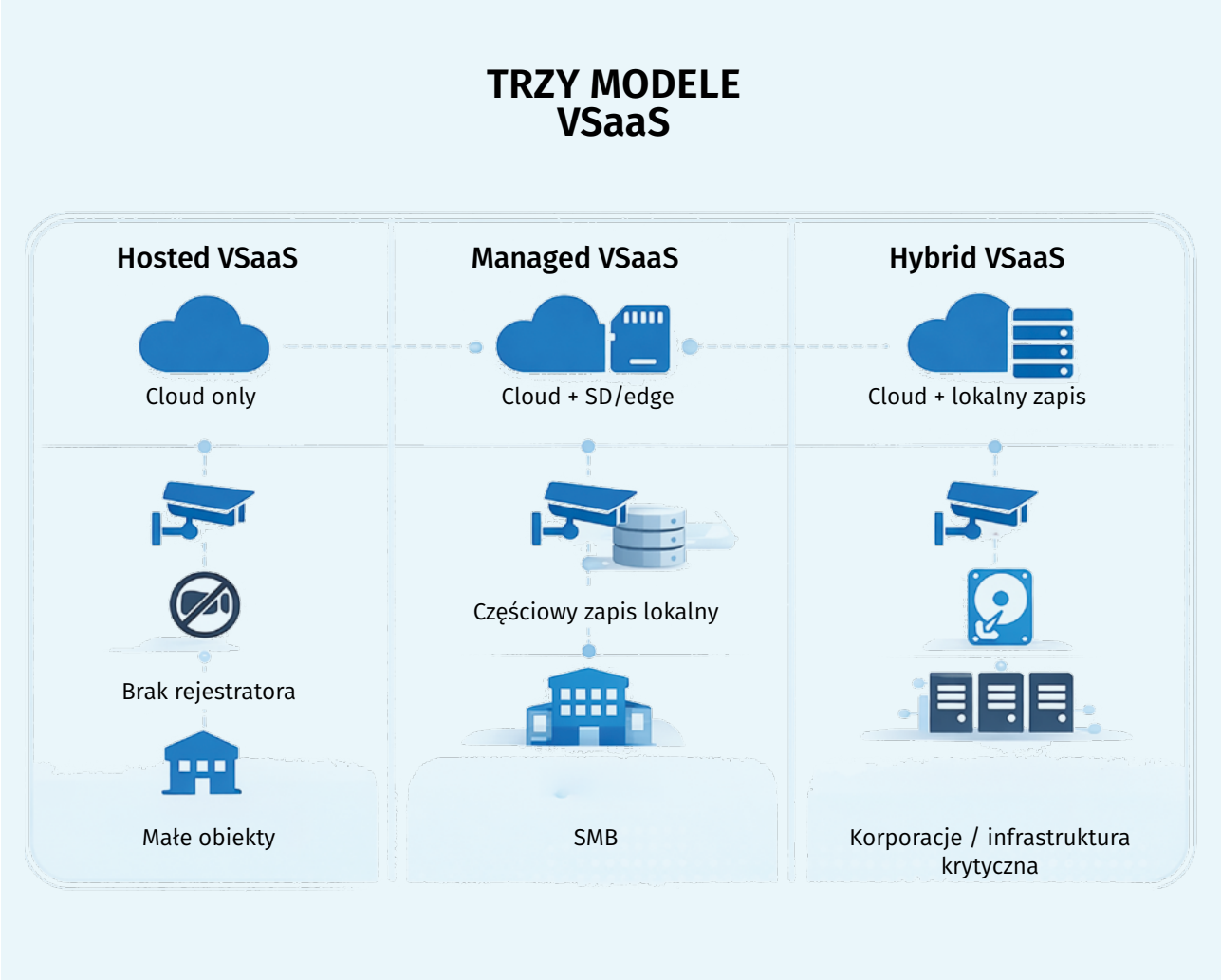
Jeszcze kilka lat temu analityka wideo była traktowana jako kosztowny luksus. Dziś subskrypcje oparte na sztucznej inteligencji rosną w tempie ponad 17% rocznie, co wyraźnie pokazuje zmianę priorytetów: użytkownicy przestają płacić za samo nagrywanie, a zaczynają inwestować w systemy, które rozumieją to, co widzą.

Chmura umożliwia uruchamianie algorytmów, które byłyby niemożliwe do zaimplementowania na typowym rejestratorze lokalnym. Nowoczesne systemy VSaaS nie tylko wykrywają ruch, ale także rozróżniają osoby, identyfikują pojazdy, wykrywają dym i ogień, analizują zachowania tłumu. To drastycznie redukuje liczbę fałszywych alarmów, które od lat pozostają jedną z głównych bolączek branży.

Najnowszy trend to tzw. Agentic AI, autonomiczne agenty programowe zdolne do planowania i wykonywania wieloetapowych zadań. Przykłady zastosowań? Automatyczne kontrole zgodności z procedurami BHP, weryfikacja dostępności produktów na półkach sklepowych czy automatyczne generowanie raportów z incydentów.

Równie przełomowe jest wprowadzenie modeli językowych (LLM/VLM) do interfejsów systemów wizyjnych. Dzięki nim operator może wpisywać polecenia językiem naturalnym, np. „znajdź mężczyznę w niebieskiej koszuli z plecakiem", a system przeszuka setki godzin materiału z wielu kamer jednocześnie. Rola operatora zmienia się tym samym z obserwatora ekranów w analityka podejmującego decyzje na podstawie przetworzonych danych.

VSaaS – zarządzanie dozorem wizyjnym
z dowolnego miejsca, bez lokalnej infrastruktury



Cyberbezpieczeństwo: nowe ryzyka, nowe wymagania

Przeniesienie strumieni wideo do chmury publicznej rodzi pytania, których nie można lekceważyć. W modelu VSaaS obowiązuje tzw. *Shared Responsibility Model:* dostawca infrastruktury chmurowej (AWS, MS Azure, Google Cloud) odpowiada za bezpieczeństwo samej platformy, ale konfiguracja aplikacji, zarządzanie tożsamością i ochrona danych leżą po stronie klienta i dostawcy usługi VSaaS.

Najczęstsze wektory ataku to błędy konfiguracji (np. źle ustawione uprawnienia do kontenerów danych), słabe zarządzanie hasłami i tożsamością (kradzież kont administratorów przez phishing) oraz podatności interfejsów API. Poważnym zagrożeniem pozostają również tzw. *insider threats*, czyli nadużycia przez uprawnionych pracowników po stronie zarówno dostawcy, jak i klienta.

Dojrzali dostawcy VSaaS odpowiadają na te ryzyka wielowarstwową ochroną: szyfrowaniem danych w czasie wymiany (TLS 1.3) i w spoczynku (AES-256), kluczami przechowywanymi w sprzętowych modułach HSM oraz podejściem Zero Trust, gdzie każda próba dostępu do systemu musi zostać uwierzytelniona i autoryzowana w czasie rzeczywistym, niezależnie od tego, skąd pochodzi.

RODO, CLOUD Act i suwerenne chmury

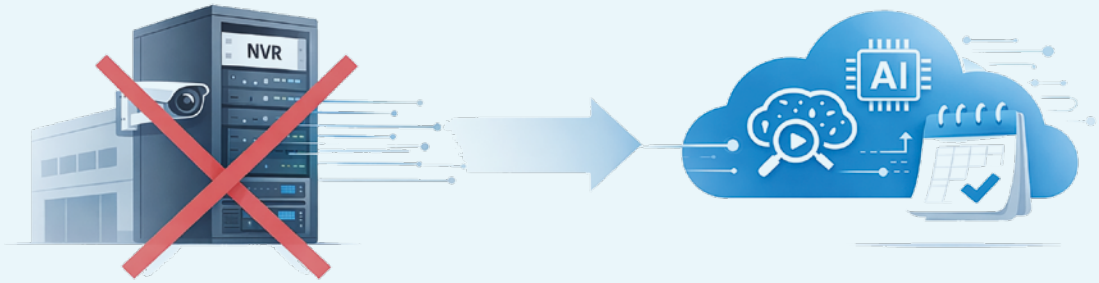
Dla polskich i europejskich użytkowników VSaaS niezwykle istotna jest kwestia rezydencji danych. Przepisy RODO wymagają przechowywania wizerunków osób w regionach geograficznych zgodnych z unijnymi standardami. Dostawcy muszą zapewnić, że dane trafiają np. do regionów Azure we Frankfurcie lub AWS w Warszawie, a nie do serwerów poza UE.

Dodatkową komplikacją jest kolizja prawna między RODO a amerykańskim CLOUD Act, który teoretycznie pozwala organom ścigania USA żądać dostępu do danych przechowywanych przez amerykańskie spółki, nawet jeśli serwery stoją w Europie. Odpowiedzią na ten dylemat są tzw. *Sovereign Clouds* (suwerenne chmury) lub mechanizm HYOK *(Hold Your Own Key)*, gdzie dostawca usługi nie ma dostępu do klucza deszyfrującego, co uniemożliwia mu udostępnienie czytelnych danych jakiemukolwiek organowi.

Nowy układ sił w kanałach dystrybucji

VSaaS nie zmienia tylko technologii, zmienia również biznes. Tradycyjny łańcuch: Producent → Dystrybutor → Instalator → Klient końcowy jest dziś pod poważną presją. Producenci platform coraz częściej nawiązują bezpośrednią relację

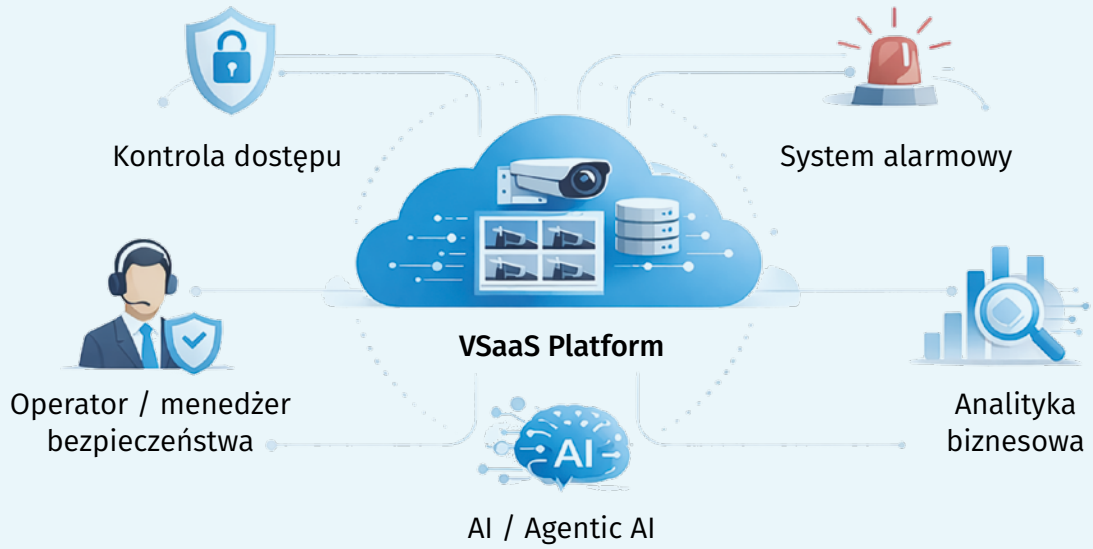
OD SERWEROWNI DO SUBSKRYPCJI



CAPEX, serwis, aktualizacje, ograniczona skala

OPEX, skalowalność, AI w standardzie

NOWY EKOSYSTEM BEZPIECZEŃSTWA



Wideo jako aktywne źródło danych, nie pasywny zapis

z instalatorami lub klientami końcowymi przez portale chmurowe. Kamery „direct-to-cloud" nie wymagają zakupu rejestratora, spada więc wartość sprzętu w projekcie i marża tradycyjnych dystrybutorów.

Dodatkową siłą napędową dezintermediacji są operatorzy telekomunikacyjni, którzy mając infrastrukturę sieciową i relację bilingową z klientem, zaczynają oferować dozór wizyjny jako usługę dodaną. Dla tradycyjnych integratorów to bezpośrednia konkurencja.

Jednak VSaaS otwiera również nowe możliwości. Instalatorzy, którzy przestawią się na model subskrypcyjny, zyskują źródło stałego, miesięcznego dochodu *(Recurring Monthly Revenu* – RMR). Zamiast jednorazowego zysku ze sprzedaży sprzętu budują portfel klientów abonamentowych. Dystrybutorzy z kolei mają szansę przekształcić się w Cloud Service Providerów, agregując subskrypcje wielu dostawców i oferując instalatorom jedno, zunifikowane miejsce zarządzania.

Polska na ścieżce chmurowej

Krajowy rynek systemów bezpieczeństwa podąża śladem globalnych trendów. Wartość polskiego rynku IT/ICT przekroczyła w 2025 roku 31 mld USD, a segment bezpieczeństwa wizyjnego należy do najszybciej rosnących obszarów. Impuls regulacyjny jest wyraźny – nowelizacja ustawy o Krajowym Systemie Cyberbezpieczeństwa wdraża dyrektywy NIS2 i CER, co wymusza inwestycje w odporność infrastruktury u tysięcy podmiotów.

Ilustracje: Marta Kołodziejak / A&S AI Studio

Firmy w Polsce deklarują zwiększone inwestycje w AI, ale jednocześnie wskazują na braki kompetencyjne w zarządzaniu złożoną technologią. To sprawia, że model „as-a-service" jest tu szczególnie atrakcyjny: zdejmuje z użytkownika ciężar utrzymania i aktualizacji systemu, dostarczając zaawansowaną analitykę w ramach miesięcznego abonamentu.

Co z tego wynika? Wnioski dla branży

VSaaS przestaje być nowinką technologiczną dla entuzjastów. Staje się strategiczną koniecznością dla organizacji szukających odporności operacyjnej. Najważniejsze konsekwencje tej zmiany:

1. **AI się demokratyzuje.** Zaawansowana analityka, dostępna kiedyś tylko dla służb i wielkich korporacji, trafia dziś do małych i średnich firm w ramach przystępnych abonamentów.
2. **Granice między IT a fizycznym bezpieczeństwem zacierają się.** Systemy wideo przestają być samotnym silosem, integrują się z kontrolą dostępu, systemami alarmowymi i analityką biznesową w jeden, spójny ekosystem.
3. **Cyberbezpieczeństwo staje się najważniejszym kryterium wyboru dostawcy.** Certyfikacje ISO 27001, zgodność z RODO i transparentność polityki rezydencji danych to dziś przepustka do kolejnych wdrożeń.
4. **Instalatorzy i dystrybutorzy,** którzy nie zaadaptują modelu subskrypcyjnego, ryzykują wyparcie przez zwinnych dostawców cloud-native i operatorów telekomunikacyjnych.

Zwycięzcami tej transformacji będą ci, którzy wideo przestaną postrzegać jako „pasywny zapis na wypadek zdarzenia", a zaczną traktować je jako „aktywne źródło inteligencji biznesowej". Rolą nowoczesnego menedżera bezpieczeństwa jest dziś nie zarządzanie serwerownią, lecz architektura informacji wizyjnej, która chroni aktywa, optymalizuje procesy i reaguje na zagrożenia, zanim się zmaterializują. •

Opracowanie na podstawie: *Research and Markets, Video Surveillance as a Service (VSaaS) Market Report 2026*; openeye.net; banyannetworks.com

Redakcja „a&s Polska"

Sztuczna inteligencja to wsparcie, a nie zastępstwo

W dobie dynamicznego rozwoju sztucznej inteligencji pojawia się pytanie o jej rolę w szeroko rozumianym obszarze bezpieczeństwa. Jak dziś wygląda współpraca człowieka i AI? Które kompetencje zyskują na znaczeniu? I czy algorytmom można zaufać przy odpowiedzialnych decyzjach operacyjnych? Na te pytania odpowiada **Marek Skowronek**, Chief Commercial & Solutions Officer oraz Member of the Board Securitas Polska, dzieląc się perspektywą rynku i przedstawiając przykłady współpracy z AI.

Na początek nakreślmy punkt wyjścia. Jak dziś wykorzystywana jest AI w obszarze security i w których aspektach przewyższa możliwości człowieka?

AI może działać bardzo skutecznie, ale jej efektywność zawsze zależy od kontekstu. Sama automatyzacja nie wystarcza, szczególnie w środowiskach podwyższonego ryzyka. Sztuczna inteligencja sprawdza się przy analizie dużych zbiorów danych, szybkim przetwarzaniu informacji i identyfikacji powtarzalnych wzorców. Człowiek natomiast pozostaje niezastąpiony tam, gdzie kluczowe są ocena sytuacji, odpowiedzialność i zrozumienie szerszego kontekstu.

Skoro AI daje przewagę w analizie, a ma ograniczenia w rozumieniu kontekstu, gdzie kończy się jej autonomia, a zaczyna rola człowieka?

AI działa z natury retrospektywnie – opiera się na danych historycznych i znanych wzorcach. Dobrze radzi sobie z tym, co już zostało zdefiniowane, ale ma trudności z nowymi, nieprzewidywalnymi sytuacjami i intencjami ludzi. Przy podwyższonym ryzyku, ograniczonej dostępności informacji i szybko zmieniających się warunkach nadal kluczowe pozostaje doświadczenie, umiejętność właściwej oceny sytuacji i odpowiedzialność człowieka.

Jaka jest rola operatora stacji monitorowania w świecie wspieranym przez AI?

Rola operatora zmieniła się diametralnie. Nie jest już jedynie obserwatorem polegającym na własnej spostrzegawczości – świadomie korzysta ze wsparcia AI, ale to on ostatecznie podejmuje decyzje. Operatorzy nigdy nie powinni bezkrytycznie przyjmować interpretacji generowanych przez AI – zawsze analizują je w kontekście rzeczywistości i obowiązujących procedur.

Intuicja i doświadczenie operatora pozostaną zawsze niezastąpione. AI nie rozpozna subtelnych, potencjalnie niebezpiecznych zachowań ani nie zinterpretuje w pełni kontekstu sytuacyjnego. Może też generować błędne wnioski („halucynacje"), a decyzje oparte na takich wskazaniach mogą mieć poważne konsekwencje. Dlatego krytyczna analiza i świadoma interwencja są kluczowe.

Biorąc pod uwagę, że AI może popełniać błędy, jak przygotować operatorów do odpowiedzialnego korzystania z tych narzędzi?

Podstawą jest jasne określenie ról: AI wspiera decyzje, człowiek jest decydentem. Systemy wykrywają ruch, sylwetki czy nietypowe zachowania oraz integrują dane z różnych źródeł, ale nie interpretują pełnego kontekstu zdarzeń. Przykładem jest sytuacja, gdzie system zarejestrował osobę trzymającą przedmiot o wysokiej temperaturze, ale nie powiązał tego z pożarem w pobliżu. Dopiero analiza operatora pozwoliła połączyć informacje w spójną całość i podjąć właściwą decyzję o powiadomieniu odpowiednich służb.

Szkoląc operatorów, podkreślamy, że AI nie może być traktowana bezkrytycznie. Systemy mogą generować fałszywe alarmy, nie wykrywać realnych zagrożeń lub błędnie je interpretować. Operator wie, że pozostaje ostatnim ogniwem bezpieczeństwa i ponosi pełną odpowiedzialność. To człowiek decyduje o wysłaniu patrolu, nadaniu komunikatu czy wezwaniu policji – technologia jest wsparciem, a nie zastępstwem.

Patrząc na współpracę człowieka i technologii, jak będzie wyglądać rola operatora w przyszłości?

Rozwój technologii i kompetencji operatorów musi postępować równolegle. Część zadań, szczególnie opartych na prostych analizach danych, ulega automatyzacji, ale pojawią się nowe obowiązki i wymagania kompetencyjne. Operator przyszłości będzie wysoko wykwalifikowanym specjalistą, przygotowanym do szybkiego podejmowania decyzji, których skutki mają realne konsekwencje dla ludzi. Ostatecznie to człowiek pozostaje niezbędnym ogniwem, nadającym sens i kontekst pracy technologii. •

Securitas Polska
Postępu 6
02-676 Warszawa
securitas@securitas.pl

ALNET SYSTEMS

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

www.alnetsystems.com

Mifare DUOX – nowy wymiar zabezpieczeń

Rodzina rozwiązań opartych na technologii kart Mifare została rozszerzona o nowy format **Mifare DUOX,** opracowany przez firmę NXP. Dołączył on do wcześniej rozwijanych przez NXP standardów, takich jak Mifare Plus, Mifare DESFire czy Mifare Ultralight.

Nowy standard kart Mifare DUOX jest wyjątkowo innowacyjny, ponieważ jako pierwszy łączy kryptografię asymetryczną i symetryczną w jednym układzie mikroprocesorowym. Rozszerzenie mechanizmów szyfrowania, przy jednoczesnym uproszczeniu zarządzania i dystrybucji kluczy oraz obsługi certyfikatów, a także zapewnienie ulepszonych funkcji bezpieczeństwa potwierdzonych certyfikatem CC EAL6+ sprawia, że Mifare DUOX oferuje wysoką wydajność i bezpieczeństwo przy relatywnie niskich kosztach.

Nowa technologia została opracowana z myślą o zabezpieczaniu dostępu do samochodów oraz aplikacji służących do ładowania pojazdów elektrycznych. Ciekawostką jest fakt, że początkowo rozwiązania z systemów kontroli dostępu migrowały do zabezpieczeń samochodowych, natomiast obecnie technologie rozwijane dla branży motoryzacyjnej – po dalszym udoskonaleniu – wracają do systemów kontroli dostępu.

Standard kart Mifare DUOX jest stosunkowo nowym rozwiązaniem. W listopadzie 2024 r. firma NXP udostępniła wstępne informacje na jego temat, a już w lipcu 2025 r. opublikowano obszerną dokumentację techniczną. Od tego czasu wielu producentów rozpoczęło wdrażanie nowego standardu. Do ich grona należy również firma IFTER, która rozszerzyła swoją ofertę o nową rodzinę czytników EQU-R500. Głównym celem podczas opracowywania tych czytników było zapewnienie wysokiego poziomu

bezpieczeństwa, niezawodności, wytrzymałości i funkcjonalności.

Czytniki standardowo są wyposażone w nowoczesny, dwukierunkowy i szyfrowany protokół komunikacji OSDP 2.2, zapewniający bezpieczną i niezawodną transmisję danych z kontrolerem przez interfejs RS 485. Czytniki z dodatkową obsługą niezabezpieczonego Wieganda są dostarczane tylko na wyraźne życzenie klienta, ale ten standard nie jest rekomendowany, ponieważ nie spełnia oczekiwanego poziomu bezpieczeństwa. Każdy czytnik ma unikalny identyfikator na magistrali RS485 oraz MAC adres weryfikowany podczas inicjacji połączenia. Podczas tej operacji wgrywane są również klucze szyfrowania indywidualne dla danego obiektu. Przy próbie użycia czytnika bez rejestracji takiej operacji na kontrolerze zostanie wywołany alarm, a czytnik nie będzie odczytywał kart. Dane wrażliwe, m.in. identyfikator kart, są szyfrowane zgodnie z metodą szyfrowania OSDP-SC.

Zabezpieczenie danych

Same dane są zabezpieczone szyfrowaniem AES-128 z kluczami ustanowionymi dla danego obiektu. Część klucza szyfrowania AES-128 po uzgodnieniu połączenia między kontrolerem a czytnikiem jest zmieniana po każdej sesji szyfrowania. Stanowi to zabezpieczenie przed podsłuchaniem i ponownym użyciem przez obce urządzenie. Należy podkreślić, że firma IFTER nie przechowuje żadnych kluczy szyfrowania swoich klientów. Każdy klient sam generuje swoje klucze szyfrowania i zapamiętuje je we własnym zakresie. Dzięki czemu nie może dojść do „przypadkowego" wycieku tak newralgicznych danych.

Konstrukcja czytnika

Konstrukcja czytnika rodziny EQU-R500 (jak również EQU-R400) umożliwia pracę w ekstremalnych warunkach. Zapewnia to brak jakichkolwiek elementów mechanicznych – przycisków, DIP switchy, pinów do zwierania czy też złącza śrubowego. Zabezpieczenie elektroniki wytrzymałą żywicą epoksydową oraz zastosowanie optycznego czujnika sabotażu pozwala bez obaw zastosować czytnik w bardzo mokrych środowiskach (IP65) i w zakresie temperatury od -40°C do +70°C.

Czytnik wyposażono w solidną obudowę umożliwiającą montaż na standardowej ścianie, w puszce elektroinstalacyjnej lub z wykorzystaniem dystansu zwiększającego przestrzeń na przewody i ułatwiającego montaż na betonie lub stali. Obudowa jest wykonana z kompozytu składającego się z kopoliestru PET-G domieszkowanego włóknami węglowymi charakteryzującą się wysoką odpornością na udary, zarysowania, wodę oraz promieniowanie UV. Dzięki temu uzyskano ponad 10 mm wielowarstwowej twardej konstrukcji.

Jeżeli czytnik jest w wersji z klawiaturą, to wykorzystywana jest klawiatura pojemnościowa umożliwiająca pracę w pełnym zakresie temperatury, niezależnie, czy osoba wprowadza kod PIN bezpośrednio palcami, czy też w grubej rękawicy. Przyciski są podświetlane, aby ułatwić wprowadzanie kodu. Czytniki mogą pracować w trybie: tylko karta, karta i PIN, karta lub PIN.

Standardowo czytnik jest w kolorze czarnym, ale może być dostępny w dowolnej kolorystyce. Na uwagę zwraca również szeroki zakres zasilania od 10 do 30 VDC oraz niski pobór prądu: 40 mA podczas standardowej transmisji danych i 80 mA podczas odczytu karty przy wykorzystaniu pełnego szyfrowania i zabezpieczeń.

Dostępne modele

W ramach rodziny czytników EQU-R500 są dostępne modele: EQU-R500, EQU--R502, EQU-R503, EQU-R505, EQU-R520, EQU-WE530.

Czytnik EQU-R500 z interfejsem USB do podłączania do komputera. Służy do programowania kart Mifare DUOX oraz odczytywania już zaprogramowanych kart, np. do weryfikacji lub przypisania innej osobie. Czytnik może być stosowany w metodzie podwójnej weryfikacji dostępu do aplikacji zarządzającej systemem. Programowanie kart polega na wpisaniu wszelkich zabezpieczeń i nadaniu unikalnego szyfrowanego identyfikatora. Jest wyposażony w kolorową diodę LED do sygnalizowania stanu połączenia i odczytu karty.

Czytnik EQU-R502 z szyfrowanym protokołem OSDP2.2. Wykonany w wytrzymałej stylowej obudowie odpornej na zarysowania gwarantującej jego długowieczność. Występuje w wersji zarówno z klawiaturą, jak i bez. Jest wyposażony w trzy kolorowe diody LED do sygnalizacji bieżącego stanu buzer oraz czujnik sabotażu.

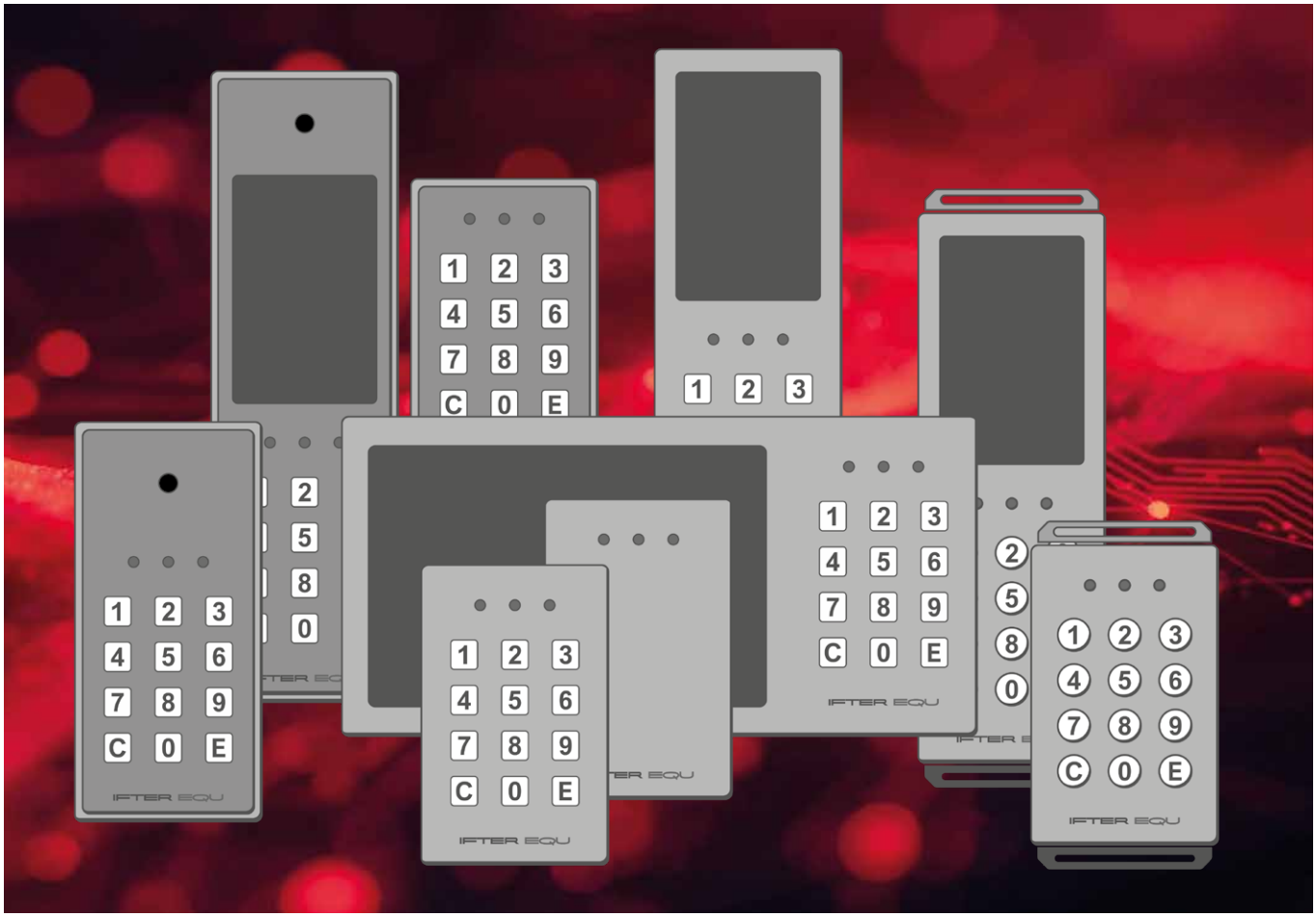
Czytnik EQU-R503 jest bliźniaczym rozwiązaniem czytnika EQU-R502 mającym szklany front o wysokiej jakości wykończenia, który można w pełni dostosować do indywidualnych potrzeb klienta. Od umieszczenia logo firmy, nazw pomieszczeń i numerów stref po wybór kolorystyki, wzorów oraz efektów graficznych. Zastosowane w nim grube wytrzymałe szkło, którego krawędzie są dodatkowo chronione przez kompozytową obudowę. Pozwala to na uzyskanie wysokiego poziomu wytrzymałości mechanicznej.

Czytnik EQU-R505 o bardzo rozbudowanych możliwościach. Może występować z wyświetlaczem 4,3", klawiaturą i kamerą. Wyświetlacz charakteryzuje się bardzo wysoką jakością pozwalającą na poprawne odczytanie informacji nawet w miejscach w pełnym słońcu. Jednocześnie jest bardzo energooszczędny. Na wyświetlaczu mogą być prezentowane informacje o przyznanym dostępie, odmowie dostępu ze względu na brak uprawnień, zbyt dużej liczbie osób w pomieszczeniu, zablokowaniu w ramach anti-passback. Dodatkowe mogą być wyświetlane takie informacje, jak przypomnienie o kończących się uprawnieniach, np. do świadczenia pracy, z pokazaniem aktualnej daty i czasu.

Interesującą opcją jest zastosowanie kamery w tej samej obudowie. Tego typu rozwiązanie pozwala na weryfikację, czy posiadacz karty jest jej właścicielem. Znacznie upraszcza to weryfikację, ponieważ osoba zbliżająca kartę do czytnika i próbująca otworzyć drzwi musi spojrzeć na wprost na czytnik. Jest to znacznie lepsze rozwiązanie niż montaż kamery na ścianie, ponieważ osoba przechodząca przez przejście nie musi być zwrócona w stronę kamery oraz kąt, pod jakim znajduje się kamera, może nie ułatwiać identyfikacji. Kamera znajduje się w czytniku za grubym szkłem. Jest typową kamerą kolorową wysokiej jakości o rozdzielczości 4 Mpix, zasilanie 12 VDC lub PoE.

Czytnik ma również złączkę do wpięcia przewodu RJ45 w celu podłączenia kamery do rejestratora. Jeżeli rejestrator wideo jest zintegrowany w naszym systemie i ma analityczne funkcje rozpoznawania twarzy, to kamera może stanowić kolejny element weryfikacji tożsamości. Korelacja funkcji czytnika, kamery i wyświetlacza w jednym urządzeniu pozwala na uzyskanie nowych możliwości w systemach zarządzania bezpieczeństwem. Co więcej, aby sprostać nawet najbardziej ambitnym oczekiwaniom, funkcjonalność czytnika można rozszerzyć o innowacyjne rozwiązania ograniczone jedynie możliwościami wyświetlacza i kamery.

Czytniki mobilne **EQU-MR520** pozwalają na weryfikację osób i sterowanie przejazdami



bezprzewodowo. W ramach serii rozróżniamy trzy modele:

- EQU-MR520 – moduł antenowy,
- EQU-MR521 – czytnik mobilny z klawiaturą,
- EQU-MR522 – czytnik mobilny z klawiaturą i wyświetlaczem 4,3".

Do transmisji danych między modułem antenowym a czytnikami mobilnymi zastosowano technologię radiową LoRa (*Long Range*), która wykorzystuje częstotliwość od 863 do 873 MHz i pozwala na transmisję do 10 km. Mając na uwadze oszczędność energii w urządzeniach mobilnych oraz dbając o wysoką jakość transmisji danych, zdecydowaliśmy się ograniczyć maksymalną odległość urządzenia mobilnego od modułu antenowego do 200 m w terenie otwartym, przy czym użytkownik we własnym zakresie może skonfigurować zasięg w zakresie od 10 do 200 m. Zasięg definiuje się przez aplikację.

Moduł EQU-MR520 obsługuje interfejs RS485 z protokołem OSDP2.2 do komunikacji z kontrolerem oraz moduł radiowy, który komunikuje się z czytnikiem, wykorzystując szyfrowanie AES-128. Obudowa modułu pozwala na montaż na zewnątrz, co poprawia zasięg i poprawność transmisji danych. Czytniki mobilne EQU-MR521 i EQU-MR522 pozwalają sterować do 99 różnych przejść. Osoba odbijająca się na czytniku może dokonać sterowania domyślnego lub wybrać konkretne sterowanie z klawiatury. Na wyświetlaczu w sposób czytelny prezentowane są informacje, czy osoba ma uprawnienia do wejścia/przejazdu, oraz jej dane pozwalające na weryfikację. Dodatkowo są prezentowane data i czas rejestracji zdarzenia oraz informacja o liczbie osób przebywających na terenie firmy.

Czytnik EQU-WR530 z klawiaturą i kolorowym wyświetlaczem dotykowym 4,3", oraz czytnik **EQU-WR532** z klawiaturą i kolorowym wyświetlaczem dotykowym 7". Oprócz eleganckiego wyglądu czytniki obsługują system RCP z wyborem typu przejścia (wejście/wyjście do pracy, wyjazd służbowy, prywatny i inne definiowane przez użytkownika). Dodatkowo prezentowane są aktualne data i czas.

Firma IFTER z najwyższą starannością przygotowała się do obsługi nowego standardu identyfikacji Mifare DUOX, dostarczając użytkownikom kompletny zestaw rozwiązań podnoszących poziom bezpieczeństwa chronionych obiektów. Nasze kompleksowe podejście, połączone z elastycznością w dostosowywaniu produktów do indywidualnych potrzeb, sprawia, że klienci korzystają z systemu z pełnym komfortem i satysfakcją. Dążenie do doskonałości jest dla nas naturalną konsekwencją szacunku, jakim darzymy tych, którzy obdarzyli nas swoim zaufaniem. •

IFTER Jerzy Taczalski
Wola Niemiecka 78c
21-025 Niemce
www.ifter.com.pl

POLON-ALFA

CNBOP-PIB

PIERWSZY W POLSCE **CERTYFIKOWANY**

PANEL OBSŁUGI DLA STRAŻY POŻARNEJ

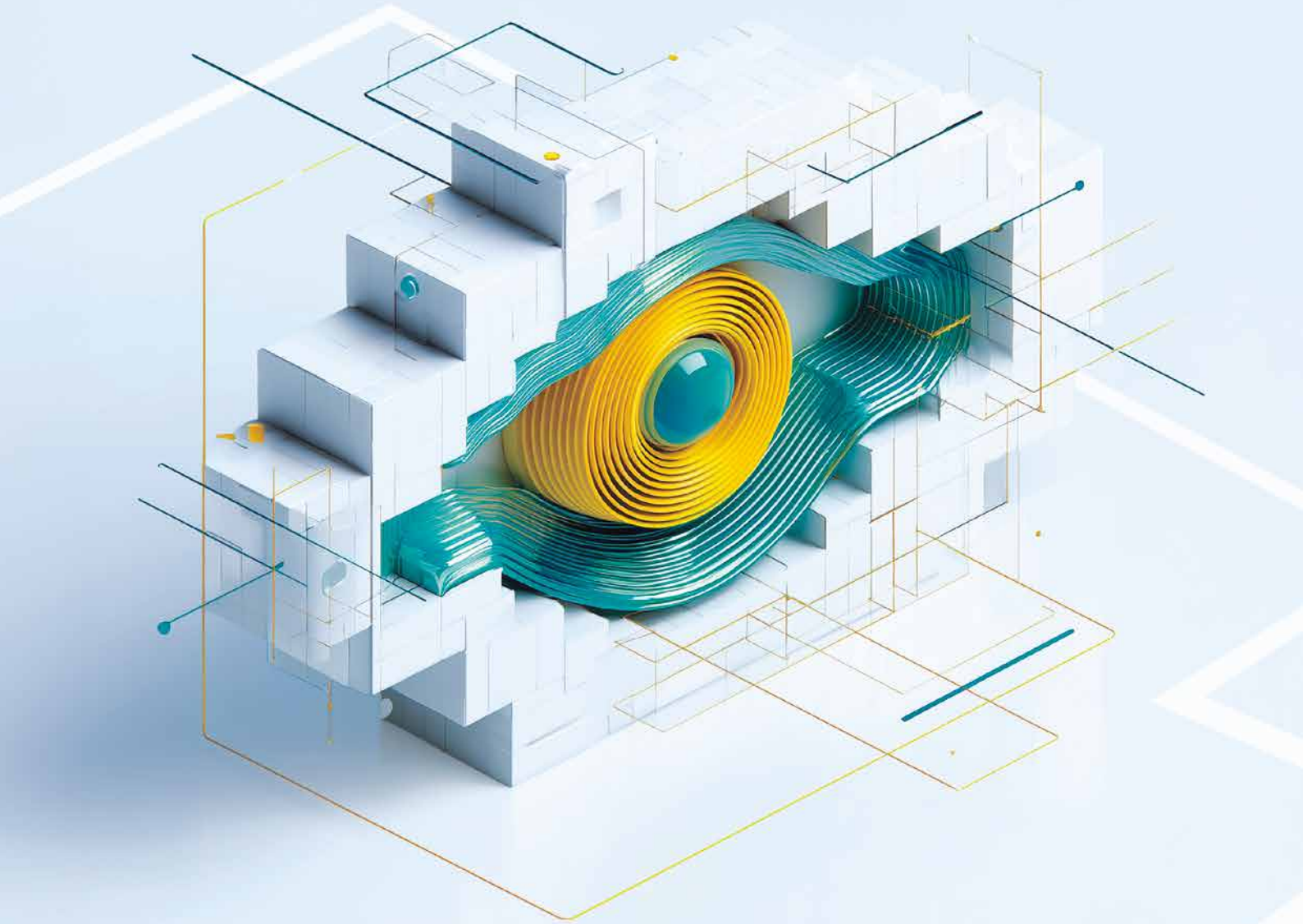
POSP 6000

- **PEŁNA INTEGRACJA Z SYSTEMEM SYGNALIZACJI POŻAROWEJ**
  Panel współpracuje bezpośrednio z centralą – wszystkie dane są przesyłane w czasie rzeczywistym, zapewniając aktualny obraz sytuacji.
- **NATYCHMIASTOWY DOSTĘP DO KLUCZOWYCH INFORMACJI**
  Panel instalowany w odległości maks. 5 m od wejścia głównego umożliwia szybkie podjęcie działań już od pierwszych sekund akcji ratowniczej.
- **WSPARCIE DLA WSZYSTKICH SŁUŻB RATOWNICZYCH**
  Intuicyjna obsługa i przejrzystość informacji wspierają działania zarówno straży pożarnej, jak i operatorów technicznych czy personelu ochrony.

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

Granica się przesuwa

Jak inteligentne systemy ochrony obwodowej zmieniają zasady gry



Rynek zabezpieczeń perymetrycznych rozwija się w tempie nienotowanym od lat, wchodząc w fazę fundamentalnych zmian. Same ogrodzenia i monitoring wizyjny przestają spełniać swoją funkcję – współczesne systemy ochrony ewoluują w kierunku spójnych platform, gdzie sztuczna inteligencja, cyberochrona i bezpieczeństwo fizyczne funkcjonują jako jeden, zintegrowany system. AI, zaawansowana integracja oraz konwergencja świata cyfrowego i fizycznego redefiniują reguły gry, wpływając zarówno na producentów, instalatorów, jak i integratorów.

Jan T. Grusznic

Dane nie pozostawiają wątpliwości. Globalny rynek ochrony obwodowej w 2025 r. osiągnął wartość szacowaną na 88–95 mld dolarów, a według prognoz do 2031 r. przekroczy poziom 141 mld. To skala wzrostu, obok której trudno przejść obojętnie – zwłaszcza że bezpośrednio przekłada się ona na rosnącą liczbę zapytań trafiających do zespołów sprzedażowych firm integratorskich. Jednak dynamika rynku to tylko część obrazu. Równie ważna jest zmiana charakteru oczekiwań inwestorów i operatorów obiektów. Tradycyjnie rozumiana ochrona obwodowa oparta na ogrodzeniach, kamerach czy barierach podczerwieni i mikrofalowych stopniowo traci na znaczeniu. Zastępuje ją znacznie bardziej zaawansowane podejście: kompleksowy, wielopoziomowy ekosystem, w którym urządzenia, oprogramowanie i analityka tworzą spójną całość.

Perymetr to coś więcej niż linia ogrodzenia

Każdy incydent zaczyna się na granicy obiektu. Zbyt często jednak ochrona perymetryczna jest traktowana jako zbiór urządzeń: kabel sensoryczny, bariera IR, kamera. Tymczasem nowoczesny system ochrony obwodowej to spójny system alarmowy, którego zadaniem nie jest „zadziałać", lecz wiarygodnie wykryć, poprawnie zinterpretować i umożliwić reakcję, zanim intruz znajdzie się wewnątrz chronionej strefy.

Specyfikacja techniczna PKN-CLC/TS 50661-1 porządkuje to podejście, przesuwając akcent:

z urządzeń → na system,
z detekcji → na skuteczność i weryfikowalność,
z instalacji → na pełny cykl życia rozwiązania

Wielu inwestorów zaczyna rozmowę od pytania: „Jaki czujnik na ogrodzenie?". Norma odwraca to pytanie: „Jaki system ma wykrywać naruszenie granicy i co ma się wydarzyć dalej?".

Specyfikacja techniczna jednoznacznie wskazuje, że dobór technologii perymetrycznej nie może być dziełem przypadku. Zastosowane rozwiązanie powinno wynikać z charakteru chronionego obiektu (krytyczny, przemysłowy, logistyczny, administracyjny), profilu zagrożeń (wandalizm, kradzież, sabotaż, zorganizowane wtargnięcie), warunków środowiskowych (teren otwarty, zalesiony, przemysłowy) oraz potencjalnych konsekwencji wystąpienia incydentu.

Dla dyrektora bezpieczeństwa oznacza to konieczność postrzegania perymetru jako integralnego elementu strategii ochrony, a nie jedynie „ogrodzenia z czujnikiem". Zewnętrzny system perymetryczny nie powinien funkcjonować w oderwaniu od pozostałych rozwiązań i musi być projektowany z myślą o integracji z systemami alarmowymi (SSWiN), dozoru wizyjnego (weryfikacja wideo), kontroli dostępu oraz systemami zarządzania bezpieczeństwem (PSIM / SMS / VMS+).

Co więcej, zgodnie z wymaganiami funkcjonalnymi określonymi w dokumencie system powinien wykrywać naruszenia zgodnie z przyjętymi scenariuszami zagrożeń, ograniczać liczbę alarmów niepożądanych (powodowanych m.in. przez zwierzęta, roślinność czy warunki atmosferyczne), umożliwiać precyzyjną lokalizację zdarzeń (odcinek, strefa) oraz zapewniać stabilne parametry pracy w długim okresie. Dla instalatora przekłada się to na konieczność właściwej konfiguracji czułości, dostosowania systemu do warunków terenowych oraz przeprowadzenia testów w warunkach rzeczywistych.

System ma warstwy

Jeżeli inwestor zgłasza się z prośbą o montaż pojedynczej kamery na ogrodzeniu, warto uświadomić mu, że jedna technologia detekcji z natury rzeczy pozostaje podatna na obejście. Trend, który jest zauważalny w 2026 r., jednoznacznie wskazuje, że skuteczna ochrona obwodowa opiera się na architekturze wielowarstwowej i to właśnie takie podejście powinno być standardem rekomendowanym przez integratorów stawiających na jakość i niezawodność wdrożeń.

Koncepcja warstwowa polega na budowie stref detekcji, które wzajemnie

się uzupełniają i potwierdzają wykryte zdarzenia.

- **Pierwszą warstwę** stanowią zazwyczaj czujniki inercyjne montowane na ogrodzeniu lub kablowe systemy detekcji, reagujące na fizyczny kontakt z barierą.
- **Drugą warstwą** jest analiza obrazu monitorująca przestrzeń przed ogrodzeniem.
- **Trzecia warstwa** może obejmować radary krótkiego zasięgu, skuteczne również w warunkach ograniczonej widoczności.
- **Czwartą warstwę** stanowi termowizja – niezastąpiona nocą oraz przy trudnych warunkach atmosferycznych.

Każda z tych warstw kompensuje ograniczenia pozostałych. Radar wykryje obiekt w gęstej mgle, gdy kamera wizyjna przestaje dostarczać użyteczny obraz. Termowizja zapewni skuteczną detekcję po zmroku. Czujnik obecności zadziała natomiast w sytuacji, gdy intruz zdecyduje się pozostać poza zasięgiem radaru lub systemu wizyjnego.

Architektura wielowarstwowa wymaga jednak starannie zaprojektowanych stref detekcji oraz przemyślanej logiki alarmowej. W przeciwnym razie zamiast ograniczenia liczby fałszywych alarmów można doprowadzić do ich eskalacji.

Na rynku zabezpieczeń technicznych dostępnych jest obecnie wiele różnorodnych rozwiązań przeznaczonych do ochrony perymetrycznej, reprezentujących odmienne podejścia do tego zagadnienia. Kluczowe jest jednak to, że żadne z nich, stosowane pojedynczo, nie jest w stanie w pełni zabezpieczyć perymetru obiektu.

– Dlatego w Hikvision stawiamy na integrację systemów działających w różnych obszarach widma elektromagnetycznego. W naszej ofercie znajdują się kamery bispektralne, łączące obserwację w paśmie widzialnym i termowizyjnym. Wspieramy je radarami mikrofalowymi o zasięgu wielu setek metrów, które umożliwiają jednoczesne śledzenie kilkudziesięciu obiektów.

Uzupełnieniem jest światłowodowy, sensoryczny system detekcji napłotowej, obejmujący nawet kilka kilometrów ogrodzenia. Całości dopełniają kamery PTZ z funkcją automatycznego śledzenia oraz tor audio – głośniki tubowe, mikrofony wbudowane w kamery i system detekcji dźwięku. Nieodzownym elementem jest także sztuczna inteligencja wraz z kompleksową platformą zarządzającą.

Każdy z wymienionych elementów stanowiących warstwy systemu ochrony perymetrycznej jest w pełni zintegrowany w naszym autorskim środowisku VMS. Zapewnia to operatorom znacząco zwiększoną świadomość sytuacyjną i operacyjną, a całemu systemowi najwyższą możliwą skuteczność w praktycznie każdych warunkach – podkreśla Piotr Rogalewski, Technical Manager w Hikvision Poland.

Sztuczna inteligencja w kamerach – nudna, ale skuteczna

Przez lata kamery systemów dozoru wizyjnego stanowiły jeden podstawowy problem: generowały nadmiar danych. W 2015 r. IPVM przeprowadził ankietę wśród 120 integratorów, która wykazała, że przeglądanych jest mniej niż 1% wszystkich nagrań z monitoringu1. Systemy oparte na AI odwróciły tę logikę. Zamiast rejestrować wszystko i analizować po fakcie, algorytmy pracują na materiale bieżącym, klasyfikując obiekty, oceniając zachowania i podnosząc alarm tylko wtedy, gdy rzeczywiście dzieje się coś, co wymaga powiadomienia operatora.

Kluczową zmianą jest tu ograniczenie liczby tzw. fałszywych alarmów. Nowoczesne algorytmy potrafią w czasie rzeczywistym odróżnić lisa przebiegającego przez strefę detekcji od człowieka, który zatrzymał się przy ogrodzeniu i analizuje teren. To rozróżnienie ma fundamentalne znaczenie operacyjne: redukuje liczbę fałszywych alarmów i przywraca zaufanie operatorów do systemu.

Wsparcie algorytmami głębokiego uczenia umożliwia też coś, czego wcześniej po prostu nie było – analizę predykcyjną. Systemy mogą uczyć się wzorców aktywności na danym obiekcie i potrafią oznaczać sytuacje, które są odchyleniem od normy. To przejście od ochrony reaktywnej do proaktywnej, o którym branża mówiła od lat, dzisiaj staje się rzeczywistością operacyjną.

– Nad ograniczeniem liczby fałszywych alarmów firma Hikvision pracuje od wielu lat. Na polskim rynku byliśmy jednym z pierwszych producentów, którzy udostępnili filtrowanie fałszywych alarmów w oparciu o modele AI. Technologii AcuSense nie trzeba dziś nikomu przedstawiać – tysiące zrealizowanych instalacji i zadowolonych klientów są tego najlepszym dowodem.

Obecnie wprowadzamy na rynek kolejną generację urządzeń opartych na wielkoskalowych modelach AI o nazwie Guanlan. Technologia ta pozwala osiągnąć niespotykaną dotąd skuteczność filtrowania fałszywych alarmów, a jednocześnie minimalizuje liczbę niewykrytych zdarzeń – komentuje Piotr Rogalewski.

Dron to nowy intruz

Jeszcze do niedawna ochrona przestrzeni powietrznej była domeną wojska i lotnisk.

Dziś jest problemem operatora centrum logistycznego, zarządcy zakładu karnego czy dyrektora fabryki farmaceutycznej.

Drony komercyjne stały się narzędziem przemytu, rozpoznania i inwigilacji dostępnym dosłownie dla każdego. Odpowiedzią branży security są systemy C-UAS (*Counter-Unmanned Aircraft Systems*, czyli systemy przeciwdziałania bezzałogowym statkom powietrznym), łączące radary 3D zdolne do śledzenia małych obiektów latających z technologiami analizującymi sygnały sterowania i telemetryczne, kamerami wizyjnymi lub termowizyjnymi czy czujnikami akustycznymi.

Często w kontekście C-UAS wspomina się o neutralizacji dronów metodą *soft-kill,* polegającą na zakłócaniu częstotliwości radiowych wymuszającym lądowanie lub powrót do punktu startu lub *hard-kill*, polegającą na zestrzeleniu obiektu. Warto jednak pamiętać, że w Polsce i większości krajów UE stosowanie aktywnych środków przeciwdronowych wymaga odpowiednich zezwoleń. Integrator oferujący kompleksowe systemy C-UAS musi operować w ścisłej współpracy z prawnikiem i odpowiednimi organami regulacyjnymi. Sprzedaż samego radaru detekcyjnego (pasywna obserwacja) jest znacznie mniej skomplikowana regulacyjnie i może stanowić dobry punkt wejścia na ten rynek.

Pisząc o dronach, nie sposób nie wspomnieć o nowelizacji ustawy o ochronie osób i mienia (Dz.U. 1997 nr 114 poz. 740), przyznającej kwalifikowanym pracownikom ochrony uprawnień do neutralizacji dronów naruszających przestrzeń powietrzną nad obiektami chronionymi. Zmiany z 24 marca 2025 r. wprowadza nowelizacja art. 36. Pracownicy ochrony, pełniąc swoje obowiązki, mogą teraz stosować konkretne środki z ustawy o środkach przymusu bezpośredniego – także te przeznaczone do unieruchamiania lub przejmowania kontroli nad dronem.

Oznacza to w praktyce, że w jasno określonych przypadkach (m.in. gdy dron zagraża ludziom i mieniu, zakłóca imprezę masową, stwarza ryzyko ataku terrorystycznego lub występuje wbrew zakazowi), na terenie chronionych obiektów i obszarów, pracownik ochrony w ramach Specjalistycznej Uzbrojonej Formacji Ochronnej może użyć siatek obezwładniających lub pocisków niepenetracyjnych. Użycie środków przymusu bezpośredniego (ŚPB) wobec bezzałogowych statków powietrznych (BSP) MUSI być przewidziane w planie ochrony z uwzględnieniem art. 156 Ustawy o prawie lotniczym Dz.U. 2025 poz. 1431, kto podejmuje decyzję, określeniem, jakie środki (np. siatka) i współdziałaniem z Policją lub wojskiem.

Rozwój technologii perymetrycznych – w kontekście dronów i systemów Counter UAS

Rewolucja dronowa dzieje się na naszych oczach. Bezzałogowe systemy znajdują kolejne zastosowania i coraz pewniej wkraczają w nowe sektory. Już dziś z powodzeniem realizujemy projekty, gdzie dron staje się narzędziem do wideoweryfikacji i reakcji na incydent zagrożenia bezpieczeństwa.

Jednocześnie rośnie liczba zdarzeń z udziałem bezzałogowych statków powietrznych. Ze względu na brak narzędzi wielu zarządzających obiektami infrastruktury krytycznej nie jest świadomych i nie posiada wiedzy o zakresie prowadzonej inwigilacji. Doświadczenia pokazują, że takie sytuacje nie są odosobnione. Z tego

UPRAWNIENIA SPECJALISTYCZNEJ UZBROJONEJ FORMACJI OCHRONNEJ – INFRASTRUKTURA KRYTYCZNA

Obszar / środek	SUFO – CZY MOŻE?	Warunki / komentarz
Detekcja drona (radar, EO/IR, RF pasywne)	TAK	Dozwolone bez ograniczeń – brak ingerencji w lot lub łączność
Obserwacja / śledzenie / identyfikacja	TAK	Element ochrony obiektu i wczesnego ostrzegania
Alarmowanie / eskalacja do policji / wojska	TAK	Obowiązek przy zagrożeniu IK
Zabezpieczenie terenu/ ewakuacja / strefy bezpieczeństwa	TAK	Standardowe czynności ochrony
Ujęcie operatora drona (jeśli zidentyfikowany)	TAK	Na zasadach ogólnych (jak wobec osoby)
Siatka obezwładniająca (ŚPB art. 12 ust. 1 pkt 5)	TAK	Wyłącznie zgodnie z art. 156ze Prawa lotniczego i planem ochrony
Pociski niepenetracyjne (ŚPB art. 12 ust. 1 pkt 11)	WARUNKOWO	Teoretycznie dopuszczalne w reżimie 156ze, praktycznie bardzo wysokie ryzyko prawne
Broń palna – amunicja ostra / penetracyjna	NIE	Brak podstawy prawnej wobec BSP
Jammery RF / GPS / spoofing	NIE	Zakazane w środowisku cywilnym
„Prewencyjne" strącanie drona bez przesłanek	NIE	Muszą wystąpić przesłanki z art. 156ze
Działania poza planem ochrony IK	NIE	Nawet legalny środek = nielegalny bez ujęcia w planie
Samodzielna „obrona powietrzna" obiektu	NIE	SUFO działa w trybie ochrony, nie obrony przeciwlotniczej

też względu ochrona antydronowa zyskuje na znaczeniu, a wręcz jest nieodzowna.

– *Rozwiązania techniczne służące do detekcji, identyfikacji, śledzenia oraz neutralizacji bezzałogowych statków powietrznych, tzw. C-UAS, stają się obowiązkową warstwą systemów zabezpieczeń, niezbędną dla zapewnienia ciągłości działania ochranianych podmiotów. W wykrywaniu dronów doskonale sprawdzają się systemy pasywne, np. ODIN R2, i aktywne w postaci radarów, np. Echoshield, a ich producenci stale udoskonalają technologie detekcyjne. W zmieniających się realiach systemy antydronowe muszą być aktualizowane na bieżąco, aby spełnić swą funkcję. Naglące są także zmiany w regulacjach prawnych, które obecnie znacząco ograniczają możliwości operatorów infrastruktury krytycznej* – podkreśla Artur Nowakowski, Senior Solution Architect, Linc Polska.

Thermal Radar – nowa generacja ochrony obwodowej 360°

W projektowaniu systemów perymetrycznych coraz częściej pojawiają się dwie technologie radarowego dozoru obszarowego: *thermal radar* oparty na kamerach termowizyjnych skanujących otoczenie w 360° oraz radar MFCW (*Multi-Frequency Continuous Wave*) – aktywny sensor radiowy krótkiego zasięgu. Obie pełnią podobną funkcję: wczesne wykrycie intruza i przekazanie jego lokalizacji do centrum operacyjnego. Różnią się jednak fundamentalnie zasadą działania, co przekłada się na konkretne różnice operacyjne.

Thermal radar to sensor pasywny – wykrywa promieniowanie podczerwone emitowane przez obiekty. Rejestruje różnicę temperatur między obiektem a tłem i na tej podstawie buduje obraz otoczenia. Nie emituje żadnego sygnału, jest więc niewykrywalny dla potencjalnego intruza.

Radar MFCW to sensor aktywny – emituje sygnały radiowe na kilku częstotliwościach jednocześnie i analizuje ich odbicia. Analiza różnic fazowych i dopplerowskich pozwala precyzyjnie określić odległość, prędkość i kierunek ruchu obiektu – w tym obiektów poruszających się bardzo wolno lub chwilowo stojących, co jest ograniczeniem klasycznych radarów CW.

Thermal radar dostarcza obraz, a operator lub algorytm analizy obrazu „widzi", co się dzieje, i może klasyfikować obiekt jako człowieka, pojazd lub zwierzę. To istotne w obiektach z dużą presją fauny lub złożonym otoczeniem, gdzie sama informacja o ruchu jest niewystarczająca do podjęcia decyzji.

Radar MFCW nie dostarcza obrazu, ale jest odporny na warunki, które ograniczają termowizję – przede wszystkim intensywne opady deszczu i śniegu. Wykrywa obiekty na podstawie ich sygnatury ruchowej, co sprawia, że fałszywe alarmy od roślinności czy drobnych zwierząt są naturalnie filtrowane przez specyfikę fizyczną technologii.

Kiedy ogrodzenie ma adres IP – cyberbezpieczeństwo jako część ochrony obwodowej

Ekspansja urządzeń zabezpieczających opartych na protokole IP przyniosła nieoczekiwany paradoks: im bardziej zaawansowany technologicznie system bezpieczeństwa fizycznego, tym większa jego powierzchnia ataku dla cyberprzestępców. Kamera IP z niezmienionym domyślnym hasłem jest łatwiejszym celem niż niejeden serwer firmowy.

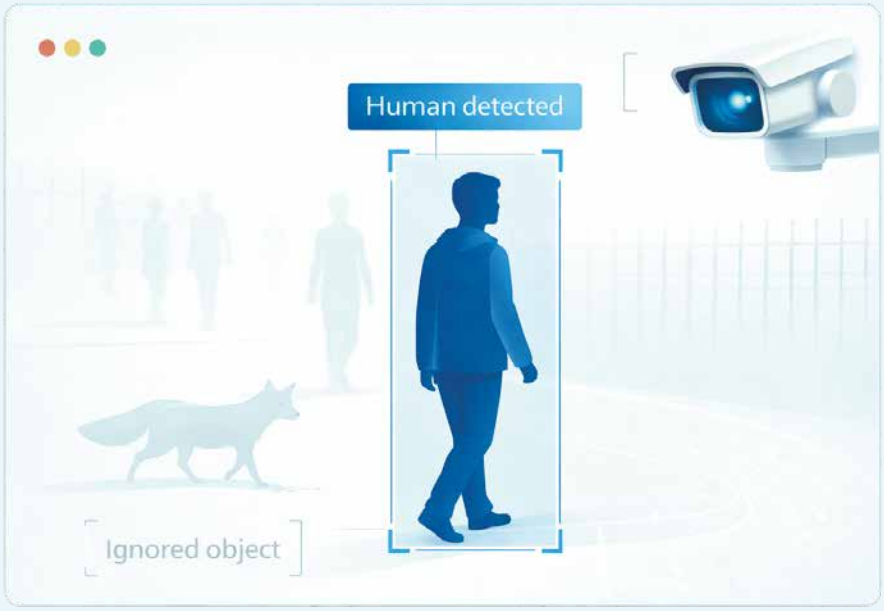
Podejście Zero Trust, zakładające, że żadne urządzenie w sieci nie jest domyślnie zaufane, nawet jeśli znajduje się wewnątrz obwodu, staje się standardem w projektach dla klientów świadomych cyberzagrożeń. Dla integratorów oznacza to konieczność rozmowy z działem IT klienta już na etapie projektu, segmentację sieci dla urządzeń bezpieczeństwa i właściwe zarządzanie dostępami i certyfikatami.

Ignorowanie tej warstwy to nie tylko ryzyko dla klienta – to również ryzyko reputacyjne dla firmy integratorskiej. Instalacja, która stała się wektorem ataku ransomware, wraca do wykonawcy niezależnie od zapisów w umowie.

O funkcjach urządzeń i oprogramowania można opowiadać długo, ale bez właściwego ujęcia ich w cały ekosystem pozostaną tylko ciekawymi funkcjami. Prawdziwą wartość daje dobrze wykonany i zrealizowany projekt i zdefiniowanie dobrych założeń, które legły u jego podstaw. Zgodnie z obowiązującymi normami, standardami i dobrymi praktykami, zarówno z zakresu ochrony technicznej, jak i IT. Sprzęt i oprogramowanie będą wówczas spójnym elementem takiego projektu, a ich funkcje – jego doskonałym uzupełnieniem.

I tak na przykład solidna obudowa kamery, z możliwością ukrycia i zabezpieczenia okablowania, pomaga chronić system przed ingerencją fizyczną. Brak

CZŁOWIEK VS AI
(DETEKCJA I KLASYFIKACJA)



domyślnych haseł oraz wymuszanie ich wysokiej złożoności zwiększają odporność na ataki na etapie logowania.

Moduł szyfrujący TPM umożliwia stworzenie bezpiecznego środowiska uruchomieniowego i zapewnia odporność na próby „wstrzyknięcia" obcego kodu czy zakłócenia procesu ładowania oprogramowania do pamięci. Filtrowanie adresów wspiera ochronę przed nieautoryzowanymi próbami połączenia, natomiast szyfrowanie na etapie uwierzytelniania i transmisji zabezpiecza strumienie wideo przed podsłuchem oraz ewentualną manipulacją.

Szczegółowe dzienniki zdarzeń pozwalają monitorować próby infiltracji i ułatwiają prowadzenie dokładnej analizy incydentów. Do tego należy dodać sprawny, skuteczny i szybki system zarządzania podatnościami, dzięki któremu klient otrzymuje na czas aktualizacje oprogramowania, a poprawki są niezwłocznie wdrażane w urządzeniach.

– *Jako producent dbamy o wszystkie te obszary i dzielimy się wiedzą z zakresu cyberbezpieczeństwa podczas konferencji, prezentacji, szkoleń oraz w mediach społecznościowych. Bezpieczeństwo to nasze wspólne dobro, dlatego zachęcamy wszystkich producentów do podejmowania podobnych działań* – podkreśla Piotr Rogalewski.

Pułapki nowoczesności

Transformacja technologiczna nie eliminuje klasycznych błędów wdrożeniowych. Wręcz przeciwnie, zwiększa ich konsekwencje. Syndrom „zainstaluj i zapomnij" jest wciąż nagminny. System, który nie jest regularnie audytowany, aktualizowany i testowany, nieuchronnie staje się systemem dziurawym. Polityki bezpieczeństwa napisane przy wdrożeniu i nigdy nieaktualizowane przestają odzwierciedlać rzeczywistość obiektu.

Zmęczenie alarmami to kolejna pułapka, szczególnie dotkliwa przy źle skalibrowanych systemach AI. Jeśli system generuje kilkaset alertów dziennie, z których znaczący procent to fałszywe alarmy, personel po prostu przestaje reagować. Właściwa kalibracja i regularna weryfikacja skuteczności detekcji to element serwisu, nie luksus.

Nie można też pomijać zagrożeń low-tech. Zaawansowany system kontroli dostępu przy bramie głównej traci sens, jeśli brama techniczna jest zabezpieczona zasuwką ze sklepu budowlanego, a ekipy remontowe poruszają się po obiekcie bez eskorty i rejestracji. Ocena ryzyka musi obejmować cały obwód, nie tylko jego technologiczne elementy.

Wreszcie: fragmentacja systemów. Kamery, które nie „rozmawiają" z kontrolą dostępu, alarmy, które nie integrują się z platformą zarządzania, to klasyczny przepis na opóźnioną reakcję w momencie rzeczywistego zdarzenia. Przy projektowaniu nalegajmy na wspólne platformy zarządzania lub otwarte API umożliwiające integrację.

Granica obiektu przestała być linią na mapie. Stała się dynamicznym, wielowarstwowym ekosystemem, w którym AI, fizyczne bariery, systemy cyberbezpieczeństwa i zarządzanie tożsamością działają wspólnie w czasie rzeczywistym. Dla dyrektorów bezpieczeństwa i specjalistów ds. ciągłości działania oznacza to konieczność myślenia o ochronie obwodowej nie jako o osobnym projekcie infrastrukturalnym, lecz jako o integralnej części strategii zarządzania ryzykiem organizacji. Technologia jest dziś dostępna i coraz bardziej przystępna cenowo. Pytanie nie brzmi już „czy nas na to stać?", ale „czy możemy sobie pozwolić na brak tego podejścia?".

Dla integratorów i instalatorów oznacza to jedno: klient kupuje dziś nie produkty, ale kompetencje. Wygra ten, kto potrafi zaprojektować architekturę, wdrożyć ją poprawnie i utrzymać w sprawności przez lata, a nie ten, kto zaoferuje najtańszą kamerę.

Granica bezpieczeństwa stała się inteligentna. Czas, by inteligentni stali się też jej budowniczowie. •

Jan T. Grusznic
redaktor „a&s Polska"

Ilustracje: Marta Kołodziejak / A&S AI Studio

Przedsiębiorstwa funkcjonują dziś w rzeczywistości, w której zmienność, nieprzewidywalność oraz rosnąca złożoność otoczenia stają się jednymi z kluczowych wyzwań zarządczych. Zjawiska te, opisywane modelami VUCA i BANI, coraz silniej wpływają na ciągłość operacji, odporność organizacyjną oraz bezpieczeństwo procesów biznesowych – i to nie tylko w miejscach prowadzenia działalności gospodarczej.

Jacek Grzechowiak

Infrastruktura krytyczna – SABOTAŻ, CHAOS I DANE

W obliczu napięć geopolitycznych, presji gospodarczej oraz nowych (?) form oddziaływania na infrastrukturę przedsiębiorstw szczególnego znaczenia nabiera zdolność identyfikowania zagrożeń, które jeszcze niedawno wydawały się marginalne. Sabotaż, działania destabilizujące czy celowe naruszenia bezpieczeństwa stają się realnym elementem ryzyka, wymagającym strategicznego podejścia i świadomych decyzji na poziomie zarządczym.

Hybrydowa natura współczesnych konfliktów, w której granice między stanem wojny a pokojem ulegają zatarciu, wymusza na menedżerach bezpieczeństwa przyjęcie bardziej elastycznego i wyprzedzającego podejścia. Oznacza to konieczność inwestowania w zaawansowaną analitykę danych oraz technologie predykcyjne – mogące wspierać identyfikację zagrożeń, zanim się zmaterializują – a także ich integrację z wysoko wykwalifikowanym personelem ochrony.

Przykłady ataków na cele pozornie nieistotne, takie jak małe firmy logistyczne czy wiejskie sklepy, pokazują, że sprawcy kierują się własnymi, często nieprzewidywalnymi kryteriami wyboru celów.

Przykłady ataków na cele pozornie nieistotne, takie jak małe firmy logistyczne czy wiejskie sklepy, pokazują, że sprawcy kierują się własnymi, często nieprzewidywalnymi kryteriami wyboru celów.

Przykłady ataków na cele pozornie nieistotne, takie jak małe firmy logistyczne (Wielka Brytania) czy wiejskie sklepy (Estonia), pokazują, że sprawcy kierują się własnymi, często nieprzewidywalnymi kryteriami wyboru celów.

Zrozumienie tej dynamiki jest kluczowe dla skutecznego zarządzania bezpieczeństwem w świecie złożonych zagrożeń. Przykład ostrzeżenia National Counterintelligence and Security Center (NCSC) do

amerykańskich firm w Europie pokazuje, że zagrożenia mogą przybierać różne formy i nie ograniczają się jedynie do fizycznych ataków na obiekty IK. Dziś firmy muszą być przygotowane na szeroką gamę ryzyk. Poglądy takie wyrażają także takie europejskie instytucje, jak: NPSA (Wielka Brytania) czy SÄPO (Szwecja). Również z Rządowego Centrum Bezpieczeństwa płynie szereg komunikatów ostrzegawczych, wskazujących na rosnącą skalę i różnorodność zagrożeń.

Kolej na kolej... ale czy tylko?

Obecnie w sposób naturalny koncentrujemy uwagę na infrastrukturze krytycznej. Tymczasem w ostatnim okresie pożary wybuchały zarówno w dużych centrach handlowych, jak i w mniejszych sklepach, a najbardziej medialna próba podpalenia zakładu przemysłowego dotyczyła fabryki farb. Już te przykłady pokazują, że spektrum potencjalnych celów jest znacznie szersze, niż mogłoby się wydawać.

Pod koniec ubiegłego roku doszło jednak do zdarzenia, które szczególnie silnie skierowało uwagę opinii publicznej na zagrożenia w transporcie publicznym. Chodzi o incydent z 16 listopada 2025 r. na linii kolejowej Dęblin-Warszawa, w okolicach stacji PKP Mika (Życzyn). Zdarzenie to stanowi kolejny przykład ingerencji w infrastrukturę mającej bezpośredni wpływ na życie i zdrowie społeczeństwa.

Nie dziwi więc wprowadzenie stopnia alarmowego CHARLIE dla obszarów kolejowych. Co istotne, podobne incydenty odnotowano również w innych krajach europejskich, np. Francji, Niemczech czy Szwecji. Skłania to do głębszej refleksji – zwłaszcza że infrastruktura kolejowa stanowi kręgosłup transportowy zarówno dla wsparcia Ukrainy, jak i dla funkcjonowania gospodarki europejskiej.

Znak zapytania umieszczony przy „nowych formach oddziaływania" w pierwszym akapicie artykułu jest w pełni zamierzony. Odnosi się do poglądu, z którym nie sposób się zgodzić. W istocie nie mamy do czynienia z jakościowo nowymi formami oddziaływania – zmieniły się jedynie narzędzia. Tam, gdzie kiedyś wykorzystywano proce, dziś używa się dronów. Narzędzie jest inne, ale cel pozostaje ten sam, a efekt bywa bardzo zbliżony.

Co więcej, niektóre metody nie tylko nie zniknęły, ale wręcz powróciły. Wysadzanie torów kolejowych było powszechną praktyką w czasie II wojny światowej. Nie trzeba jednak sięgać aż tak daleko – zanim używano materiałów wybuchowych, sabotażyści po prostu rozkręcali tory.

Dobrym przykładem jest incydent z 20 marca 2020 r. na linii KDP Frankfurt-Kolonia. Maszynista zwrócił uwagę na nietypowe zachowanie pociągu podczas przejazdu przez most Theisstal. Dochodzenie wykazało, że na 80-metrowym odcinku trasy poluzowano aż 254 śruby mocujące szyny. Skala ingerencji była tak duża, że jeden z kolejnych pociągów mógłby się wykoleić.

Do tego dochodzi przypadek odłączenia wagonu kolejowego w Katowicach w październiku 2025 r. Zestawienie tych zdarzeń prowadzi do oczywistego wniosku: nie są to przykłady historyczne, lecz element naszej codzienności. Pytanie, czy jest to jeszcze codzienność „przedwojenna", czy już „wojenna", pozostaje otwarte.

Woda – czy tylko jej źródło?

Kolejnym obszarem są wodociągi rozumiane szeroko jako system obejmujący również oczyszczalnie ścieków. Choć dla części odbiorców może to być nieintuicyjne, „produktem" oczyszczalni jest czysta woda trafiająca do środowiska naturalnego, a następnie – po pewnym czasie – do systemów zaopatrzenia w wodę, czyli wodociągów.

Obiekty te już obecnie podlegają zagrożeniom o charakterze sabotażowym, dywersyjnym i szpiegowskim. Potwierdzają to ustalenia Najwyższej Izby Kontroli, zawarte m.in. w raporcie *Bezpieczeństwo zakładów, obiektów i urządzeń o istotnym znaczeniu dla funkcjonowania aglomeracji miejskich w województwie lubelskim* LLU.430.3.2024[1].

Z materiałów tych wynika, że nieautoryzowane wejścia na teren obiektów oraz próby dotarcia do wrażliwych instalacji i urządzeń stają się coraz poważniejszym problemem. Wymaga to odejścia od podejścia reaktywnego na rzecz działań proaktywnych.

Przykłady

Na terenie spółki należącej do Miasta **nr** 4 w połowie 2022 r. doszło do niegroźnego incydentu – na teren spółki wtargnęło dwóch młodych mężczyzn, którzy weszli na dach zbiornika wody, a po interwencji pracownika spółki opuścili teren zakładu. Oględziny miejsca zdarzenia nie wykazały żadnych strat ani naruszeń zabezpieczeń zbiorników i instalacji wodociągowej. O powyższym zdarzeniu powiadomiono Policję.

W spółce należącej do Miasta **nr 6** odnotowano wystąpienie zdarzenia o charakterze szpiegowskim dokonanym przez nieznane osoby obcego obywatelstwa, o której zawiadomione zostały służby Policji i Agencji Bezpieczeństwa Wewnętrznego. Po tym incydencie spółka wdrożyła procedury zwiększające ochronę obiektów, dokonano analiz ryzyk wystąpienia nieuprawnionej ingerencji w stosunku do obiektów i urządzeń spółki oraz podjęto konkretne działania wobec zidentyfikowanych zagrożeń.

Prąd jest ważny, ale czy tylko jego produkcja?

Kolejnym ważnym elementem IK jest energetyka. Jednym z najbardziej znanych przykładów ataków ostatniego okresu był cyberatak z 29 grudnia 2025 r., który objął co najmniej 30 farm wiatrowych i fotowoltaicznych, prywatną spółkę z sektora produkcyjnego oraz dużą elektrociepłownię, która zaopatruje prawie pół miliona odbiorców w Polsce. I choć – jak twierdzi CERT[2] – ataki, które można było porównać do podpaleń w świecie fizycznym, spowodowały zerwanie komunikacji z operatorami sieci, to jednak nie wpłynęły na produkcję energii elektrycznej. Atak na elektrociepłownię również nie spowodował przerw w dostawie ciepła do odbiorców. A więc CERT mówi: obroniliśmy się!

Na pierwszy rzut oka można więc uznać, że system zadziałał prawidłowo. Warto jednak spojrzeć na tę sytuację w szerszym kontekście. W dniu rozpoczęcia rosyjskiej agresji na Ukrainę doszło do ataku, którego skutkiem była utrata kontroli nad blisko 6 tys. turbin wiatrowych w całej Europie, o łącznej mocy 11 GW.

Trudno uznać tę zbieżność za przypadkową. Warto w tym kontekście przypomnieć doktrynę Gierasimowa, określaną niekiedy mianem teorii chaosu. Nie należy jej jednak demonizować – wykorzystanie pozamilitarnych metod wspierania lub inicjowania konfliktów jest znane od starożytności, o czym świadczy choćby „Sztuka wojny" Sun Tzu. Należy jednak pamiętać, że w tej doktrynie to właśnie działania pozamilitarne odgrywają rolę dominującą. Z tej perspektywy sektor energetyczny jawi się jako naturalny cel oddziaływania.

Na ten temat powstało już bardzo wiele publikacji, dlatego nie zamierzam konkurować z ich autorami. Chciałbym natomiast zwrócić uwagę na proces obecny w każdej organizacji, niezależnie od jej profilu działalności. Mowa o usuwaniu awarii, często określanym jako DR&BC. Proces ten najczęściej koncentruje się na systemach IT, rzadziej – choć coraz częściej – obejmuje również systemy OT. Warto jednak podkreślić, że jego znaczenie dla bezpieczeństwa fizycznego jest znacznie większe, niż powszechnie się przyjmuje.

Przykładem będzie incydent ze Szwecji, z branży bardzo bliskiej energetyce, jaką jest telekomunikacja. W ubiegłym roku w jednej z takich firm w tym samym czasie doszło do licznych awarii sprzętu technicznego. I pewnie można by uznać, że nie ma tu nic niezwykłego, gdyby nie fakt, że awarie dotyczyły określonego – i niezbyt dużego – obszaru. I choć ataki nie doprowadziły do większych zakłóceń, to i firma, i szwedzkie służby potraktowały je poważnie. Osoby zarządzające bezpieczeństwem przyjęły założenie, że część incydentów ma związek z pozyskiwaniem informacji wywiadowczych i sabotażem, mającym na celu sprawdzenie możliwości i obserwację działań realizowanych w sytuacjach kryzowych.

To bardzo ważna kwestia, bo najczęściej koncentrujemy uwagę na samym zakłóceniu działania i na metodach, jakie do niego doprowadziły. Jeśli jednak przyjmiemy założenie, że celem ataku nie jest już samo zakłócenie działania, to prowadzi nas to do co najmniej 2 wniosków (i z uwagi na publiczny charakter tego artykułu muszę i chcę ograniczyć się tylko do nich):

1. Najprawdopodobniej potencjalne metody doprowadzenia do incydentu i jego skutki są już wystarczająco dobrze znane adwersarzowi i po prostu JUŻ go nie interesują.
2. Teraz adwersarz poszukuje informacji, dającej mu przewagę operacyjną w postaci rozpoznania algorytmów i procedur odtwarzania uszkodzonej infrastruktury oraz przywracania funkcjonowania usług krytycznych, co w praktyce umożliwi – w jego przeświadczeniu – uderzenie w działania naprawcze, ergo adwersarz przygotowuje się do wywołania awarii niemożliwej lub skrajnie utrudnionej do usunięcia, a więc rozległej i długotrwałej.

Adwersarz poszukuje informacji dającej mu przewagę operacyjną w postaci rozpoznania algorytmów i procedur odtwarzania uszkodzonej infrastruktury oraz przywracania funkcjonowania usług krytycznych.

Last but not least

Pytanie: „Czy mój obiekt jest infrastrukturą krytyczną?" należy uznać za błędnie postawione. Mimo to słyszę je wyjątkowo często. Zdecydowanie zbyt często. Infrastruktura krytyczna jest bez wątpienia miejscem mającym bezpośredni wpływ na życie całego społeczeństwa, co znajduje odzwierciedlenie w naszym prawie, ale czy aby na pewno powinniśmy patrzeć na to tylko przez pryzmat ustawowy? Przywołane na początku pożary w sklepach wielkopowierzchniowych pokazują, że patrzenie na IK przez pryzmat definicji ustawowej znacznie zawęża pole widzenia. A to błąd. Część obiektów w rozumieniu naszego przeciwnika jest infrastrukturą krytyczną, mimo iż nie są takimi z ustawowego punktu widzenia. A w analizie ryzyka ważniejsza jest perspektywa adwersarza, bo to on decyduje, na kogo, gdzie, kiedy i jak uderza.

Jak może więc wyglądać obiekt, który nie jest infrastrukturą krytyczną w naszym rozumieniu, a jest w rozumieniu adwersarza. Sklepy wielkopowierzchniowe już omówiliśmy. A zakłady przemysłowe? Całkiem niedawno na stronie **Eurojust**[3] (European Union Agency for Criminal Justice Cooperation) został opublikowany komunikat, informujący o skazaniu sprawców podpaleń, dokonywanych na zlecenie służb specjalnych Rosji. Komunikat zawiera kilka ciekawych informacji, przydatnych w bieżącej pracy operacyjnej zarówno w zakresie zarządzania bezpieczeństwem (klienci), jak i w zakresie świadczenia usług ochrony osób i mienia (agencje ochrony). Podejrzani wzięli na cel fabrykę produkującą materiały dla Sił Zbrojnych Ukrainy i ją podpalili. Próbę podejmowali dwukrotnie. Za pierwszym razem zrezygnowali, gdyż obok przechodzili przechodnie. Druga próba zakończyła się sukcesem, choć nie spowodowała żadnych szkód, ponieważ użyto niewystarczającej ilości materiałów łatwopalnych. Już na tym etapie widać, że zarządzanie bezpieczeństwem zawiodło. A to dopiero początek...

Fotografie pochodzą z komunikatu Eurojust: *Terrorist group responsible for arson attacks across Europe taken to court* z 27 stycznia 2026.

Analiza zdarzenia wskazuje na kilka podstawowych błędów:

1. Składowanie sprzętu na zewnątrz, które prawdopodobnie jest wynikiem deficytu powierzchni magazynowej, wynikającego z nadmiernego i nieprzewidywanego wzrostu wolumenu produkcyjnego;
2. Ogrodzenie wykonane z typowych paneli ogrodzeniowych 3D, w praktyce spełniające bardziej funkcję wydzielenia terenu niż jego zabezpieczenia przed nieautoryzowanym wejściem;
3. Rozmieszczenie wyrobów gotowych w miejscu podatnym na bezpośrednią ingerencję.

Każdy z tych elementów ma bezpośredni związek z zarządzaniem bezpieczeństwem. W praktyce jednak – zarówno w tym przypadku, jak i w wielu obiektach, które miałem okazję obserwować (niekiedy zupełnie przypadkowo) – funkcjonują one w oderwaniu od tego obszaru. Często przybierają wręcz formę silosową: magazyn rzadko konsultuje z działem bezpieczeństwa kwestie lokalizacji wyrobów gotowych. W efekcie trafiają one w miejsca tak blisko ogrodzenia, że ich dewastacja staje się banalnie prosta.

Dlatego tego typu przypadki warto analizować wspólnie z osobą odpowiedzialną za zarządzanie bezpieczeństwem oraz przedstawicielem podmiotu świadczącego usługi ochrony. Takie podejście, oparte na realnej współpracy, pozwala uruchomić trzeci, kluczowy element: SYNERGIĘ. Jeśli dodatkowo do procesu zostanie włączony doświadczony analityk ryzyka, grający rolę „adwokata diabła", efekty mogą być jeszcze lepsze.

Praktycznym potwierdzeniem skuteczności takiego podejścia są warsztaty operacyjne, m.in. te, które prowadziłem podczas Bootcampu. Uczestnicy mieli w ich trakcie możliwość wejścia w rolę insidera, co wyraźnie pokazało, jak wiele można zyskać dzięki wspólnej analizie i symulacji

Profil zawodowy potencjalnego szpiega czy dywersanta nie ma kluczowego znaczenia, ważniejsza jest jego determinacja.

zagrożeń. Tego typu warsztaty stają się dziś niezbędnym elementem działań na poziomie operacyjnym.

Procesy operacyjne i zagrożenia wewnętrzne

Analiza przypadku „litewskiego" skłania do kilku wniosków natury operacyjnej, ale także do refleksji na temat motywów działania sprawców, a przede wszystkim metod pozyskiwania ich przez obce służby specjalne. Coraz częściej docierają do nas informacje, iż wśród sprawców mamy także obywateli naszego kraju. Najnowszym takim przypadkiem jest akt oskarżenia przeciwko obywatelowi RP Wiktorowi Ź., jaki został skierowany 12 lutego 2026 r. do Sądu Okręgowego w Bydgoszczy. Jak wynika z komunikatu ABW, oskarżony prowadził działalność szpiegowską na rzecz wywiadu Rosji na terenie woj. kujawsko-pomorskiego, przekazując informacje nt. zabezpieczeń technicznych Portu Lotniczego Bydgoszcz S.A., Wojskowych Zakładów Lotniczych Nr 2 S.A. w Bydgoszczy, Zakładów Chemicznych NITRO-CHEM S.A. w Bydgoszczy. Z doniesień medialnych wynika, że Wiktor Ź. jest muzykiem i lingwistą, co mówi nam, że oficjalny profil zawodowy potencjalnego szpiega czy dywersanta nie ma kluczowego znaczenia, a ważniejsza jest jego determinacja i umiejętność pozyskiwania informacji z wnętrza chronionych obiektów. To powinno skutkować szkoleniami pracowników ochrony oraz kadry non-security w zakresie zagrożeń wewnętrznych, określanych terminem „insider".

Podsumowanie

Infrastruktura krytyczna pozostaje najważniejszym zasobem wymagającym ochrony, dlatego nie dziwi fakt, że znaczna jej część znajduje się pod nadzorem zarówno służb państwowych, jak i prywatnych agencji ochrony. Kluczowe jest jednak przyjęcie znacznie szerszej perspektywy – to, co ustawowo uznajemy za infrastrukturę krytyczną, stanowi jedynie fragment tego, co jako krytyczne postrzega nasz adwersarz.

Nie znamy celów przeciwnika, ale możemy je rozpoznać, jeśli nauczymy się patrzeć na rzeczywistość jego oczami. Każdy z nas w dowolnej chwili może znaleźć się w miejscu, które zostanie przez niego uznane za krytyczne – nawet nie zdając sobie z tego sprawy. Dopiero przyjęcie jego perspektywy pozwala dostrzec takie miejsca. •

Jacek Grzechowiak
Menedżer ryzyka i bezpieczeństwa. Absolwent WAT, studiów podyplomowych w SGH i Akademii L. Koźmińskiego. Gościnnie wykłada na uczelniach wyższych. Właściciel firmy RISKRESPONSE. Dyrektor Centrum Kompetencji „a&s Polska".

1) Za: www.nik.gov.pl
2) Za: https://cert.pl/posts/2026/01/raport-incydent-sektor-energii-2025/
3) Za: https://www.eurojust.europa.eu/news/terrorist-group-responsible-arson-attacks-across-europe-taken-court

Ilustracje: Marta Kołodziejak / A&S AI Studio

Jak chronić **infrastrukturę krytyczną** w czasach niepewności?

O wpływie sytuacji geopolitycznej i szybkim rozwoju technologii na ochronę infrastruktury krytycznej, roli sztucznej inteligencji, ryzykach związanych z pochodzeniem technologii oraz największych wyzwaniach dla sektora IK mówi **Kamil Barański,** CEO Megavision Technology.

Jak dziś chronić infrastrukturę krytyczną w kontekście napięć geopolitycznych? Od czego należy zacząć?

Przede wszystkim od edukacji i budowania świadomości. Osoby odpowiedzialne za bezpieczeństwo powinny nie tylko same rozumieć jego znaczenie, ale także aktywnie kształtować tę świadomość w swoim otoczeniu.

Bezpieczeństwo to wartość, którą należy pielęgnować w każdym obszarze funkcjonowania organizacji. Jeśli nie podejdziemy do tego systemowo i nie nauczymy się działać w sposób świadomy i konsekwentny, w niedalekiej przyszłości możemy stanąć przed poważnymi problemami.

To wszystko zaczyna się od nas – od zmiany podejścia, wypracowania odpowiednich nawyków i wykorzystania dostępnych narzędzi.

W takim razie jaką rolę odgrywa sztuczna inteligencja?

Trzeba jasno powiedzieć – sztuczna inteligencja to teraźniejszość. Stanowi jeden z kluczowych elementów nowoczesnych systemów bezpieczeństwa. W praktyce oznacza to, że systemy pozbawione wsparcia AI mogą wkrótce okazać się niewystarczające lub mówiąc wprost, nieprzydatne. AI rozszerza nasze możliwości – w zakresie zarówno analizy danych, jak i percepcji zdarzeń.

Przykłady z wojny w Ukrainie pokazują, że AI umożliwia nie tylko reagowanie, ale przede wszystkim działanie proaktywne – przewidywanie zagrożeń i zapobieganie im.

Współpracujecie z sektorem wojskowym. Jakie potrzeby są dziś dla niego kluczowe?

Jednym z wyróżników obiektów wojskowych jest szerokie wykorzystanie kamer termowizyjnych – to standard w ich ochronie. W sektorze publicznym i komercyjnym ta technologia dopiero zaczyna się upowszechniać, choć jej potencjał jest ogromny. Podobnie wygląda sytuacja z ochroną perymetryczną – coraz więcej obiektów zaczyna wdrażać takie rozwiązania na dużą skalę.

A czy pochodzenie technologii ma dziś znaczenie?

Zdecydowanie tak. W przypadku infrastruktury krytycznej i obiektów wojskowych ogromne znaczenie ma kraj pochodzenia technologii.

W Polsce wykorzystuje się rozwiązania m.in. z Korei, Szwecji czy USA, czyli krajów należących do NATO lub bliskich sojuszników. Jednocześnie świadomie unika się technologii pochodzących z Chin, szczególnie w kontekście cyberbezpieczeństwa i systemów opartych na AI.

Problem polega na tym, że rynek chiński rozwija się bardzo dynamicznie i oferuje często wysoko zaawansowane rozwiązania. To stawia Europę i Zachód przed koniecznością przyspieszenia rozwoju własnych technologii.

Jakie jest największe wyzwanie dla bezpieczeństwa infrastruktury krytycznej w Polsce?

Według mnie największym wyzwaniem pozostaje dziś czas. a właściwie jego niedobór. Procesy inwestycyjne oraz zamówienia publiczne trwają miesiącami, a niekiedy nawet latami, podczas gdy zagrożenia rozwijają się dynamicznie i wymagają szybkiej reakcji. Niesprawne procedury utrudniają wdrażanie nowoczesnych rozwiązań i ograniczają możliwość działania w sposób proaktywny.

Istotnym obszarem ryzyka pozostaje również cyberbezpieczeństwo, szczególnie w kontekście systemów monitoringu wizyjnego. Kamery stanowią dziś podstawowe źródło informacji, ale jednocześnie mogą być potencjalnym punktem ataku. Doświadczenia z konfliktów międzynarodowych pokazują, że tego typu systemy mogą być wykorzystywane do działań wywiadowczych. Ewentualne błędy w tym zakresie mogą prowadzić do poważnych konsekwencji – zarówno operacyjnych, jak i wizerunkowych.

Na koniec: czy w erze AI człowiek nadal pozostaje najważniejszy?

Tak – i jeszcze długo tak będzie. Sztuczna inteligencja może wspierać analizę i wskazywać potencjalne zagrożenia, ale ostateczna decyzja powinna należeć do człowieka. Warunkiem jest jednak odpowiednie przygotowanie – inwestycja w kompetencje, szkolenia i rozwój operatorów systemów bezpieczeństwa. To właśnie człowiek, wspierany przez technologię, pozostaje dziś najważniejszym elementem całego systemu. •

MEGAVISION TECHNOLOGY
ul. Heliotropów 1
04-796 Warszawa
www.megavision.pl

Karta to nie tożsamość

Dlaczego kontrola dostępu w infrastrukturze krytycznej (IK) wymaga zmiany podejścia

W wielu obiektach IK kontrola dostępu nadal opiera się na prostym mechanizmie identyfikatora fizycznego – karty, breloka czy opaski RFID. Czytnik odczytuje numer identyfikatora, system sprawdza go w bazie uprawnień i – jeśli wszystko się zgadza – drzwi zostają otwarte.

Technicznie taki model działa poprawnie, jednak jego ograniczenia są dobrze znane. Fizyczny identyfikator nie jest tożsamością użytkownika – jest jedynie przedmiotem, który można zgubić, przekazać lub pozostawić poza kontrolą organizacji. System weryfikuje więc poprawność karty, ale nie ma pewności, kto faktycznie z niej korzysta.

W wielu środowiskach nie stanowi to dużego problemu. W przypadku IK sytuacja wygląda jednak inaczej. Dostęp do stref technologicznych, pomieszczeń sterowniczych czy infrastruktury operacyjnej oznacza realny wpływ na bezpieczeństwo ludzi oraz ciągłość procesów biznesowych.

W takich miejscach znaczenie ma nie tylko to, czy identyfikator jest ważny, ale przede wszystkim to, kto próbuje uzyskać dostęp oraz w jakim kontekście operacyjnym się to dzieje.

Tożsamość w smartfonie

Jednym z elementów takiego podejścia jest rozwiązanie SECORUN MobileID, które przenosi poświadczenie dostępu do środowiska mobilnego użytkownika.

Rozwiązanie jest oparte na technologii HID MobileID, a uprawnienie jest zapisywane w Apple Wallet lub Google Wallet i przechowywane w Secure Element telefonu – sprzętowym module bezpieczeństwa wykorzystywanym również do płatności mobilnych.

Aktywacja dostępu wymaga uwierzytelnienia użytkownika, np. przy użyciu rozpoznawania twarzy lub odcisku palca. System nie opiera się już wyłącznie na przedmiocie, który może zmienić właściciela, lecz na potwierdzonej tożsamości osoby korzystającej z identyfikatora.

Od zarządzania kartami do zarządzania tożsamością i kontekstem

Coraz więcej organizacji zaczyna postrzegać kontrolę dostępu nie jako logistykę zarządzania kartami, lecz jako element zarządzania tożsamością oraz ryzykiem operacyjnym.

Nowoczesne systemy nie ograniczają się już do sprawdzenia identyfikatora. Coraz częściej analizują również kontekst próby wejścia, np. powiązanie użytkownika z aktualnym zadaniem, zleceniem serwisowym czy awizacją wizyty.

Takie podejście pozwala powiązać system kontroli dostępu z rzeczywistymi procesami biznesowymi organizacji. Oznacza to integrację z systemami zarządzania pracami, logistyką wizyt czy obsługą podwykonawców – tak jak w module zarządzania awizacjami SECORUN AWZ.

Dzięki temu system może oceniać nie tylko „czy ktoś ma kartę", ale także to, czy konkretna osoba powinna znajdować się w danym miejscu i czasie w ramach realizowanego procesu operacyjnego lub kontekstu.

Element większego ekosystemu bezpieczeństwa

Zarówno SECORUN MobileID, jak i SECORUN AWZ nie są rozwiązaniami funkcjonującymi w izolacji. Stanowią część szerszego ekosystemu platformy SECORUN, obejmującej m.in.:

- SECORUN KD – system kontroli dostępu,
- SECORUN BPL – bezpieczeństwo procesów logistycznych,
- SECORUN MA – zarządzanie alarmami na mapach obiektów,
- SECORUN EWK – wsparcie procesów ewakuacyjnych,
- SECORUN BI – przekrojowe analizy danych (również w zakresie KPI dotyczących bezpieczeństwa).

W tym modelu kontrola dostępu przestaje być jedynie infrastrukturą obsługującą czytniki i przejścia. Staje się elementem systemu zarządzania bezpieczeństwem operacyjnym, łączącym weryfikację tożsamości z analizą kontekstu działania użytkownika oraz z procesami biznesowymi organizacji. •

Vemco Sp. z o.o.
ul. Biała 1
80-435 Gdańsk
secorun.pl

Mniej ryzyka, więcej kontroli: uporządkowany dostęp w infrastrukturze krytycznej

Kiedy stawką jest ciągłość dostaw energii, przepływ węzłów transportowych, dostępność zasobów w data center czy bezpieczeństwo obiektów gospodarki wodnej, kontrola dostępu przestaje być „systemem do drzwi". Staje się narzędziem, które porządkuje ruch osób, ogranicza ryzyko nadużyć i dostarcza twarde dane do audytu dokładnie wtedy, gdy liczy się każda minuta.

W obiektach infrastruktury krytycznej powtarzają się podobne scenariusze.

Po pierwsze: kontraktorzy i goście

Serwisy, dostawy i prace okresowe wymagają nadawania uprawnień na czas i w konkretnym zakresie oraz rozliczalności dostępu: identyfikacji osoby, miejsca i czasu zdarzenia.

Po drugie: rozproszenie

Wiele lokalizacji i stref bezpieczeństwa trzeba prowadzić jedną, spójną polityką, a dostęp odebrać natychmiast, gdy sytuacja się zmienia.

Po trzecie: audyt i zgodność

Potrzebny jest wiarygodny ślad zdarzeń i raporty, zarówno do rutynowych kontroli, jak i po incydencie.

Dlatego nowoczesny system kontroli dostępu powinien działać jak element odporności organizacji: wspierać strefowanie i zasadę dostępu tylko wtedy, gdy jest to niezbędne, pozwalać na logiczny podział instalacji (partycje), a w skali całego obiektu uruchamiać

mechanizmy globalne, takie jak anti-passback czy strefy obwodowe. W praktyce liczy się też reakcja: monitoring przejść, alarmy, alerty i działania uruchamiane zdarzeniem skracają czas od wykrycia naruszenia do decyzji operatora.

Właśnie w takiej roli sprawdzają się platformy klasy Enterprise, takie jak RACS 5. System jest projektowany z myślą o środowiskach wymagających (w tym o infrastrukturze krytycznej), daje możliwość podziału na partycje oraz szerokie opcje integracji i dostępne API, dzięki czemu może stać się centralnym „kręgosłupem" polityki dostępu w organizacji. Kluczowe jest również bezpieczeństwo transmisji i identyfikacji: RACS 5 spełnia wymagania normy EN 60839-11-1 na poziomie Grade IV i wspiera OSDP z kanałem Secure Channel.

Od strony operacyjnej zyskujemy jedno miejsce zarządzania i wglądu w zdarzenia: oprogramowanie VISO współpracuje z centralną bazą danych Microsoft SQL Server i umożliwia pracę wielostanowiskową, a komunikacja z kontrolerami jest szyfrowana (AES-128). Dodatkowo VISO SMS wspiera monitoring i wizualizację systemów bezpieczeństwa, automatyczne wykrywanie sytuacji alarmowych oraz działania operatora w podjęciu właściwych działań zgodnie z polityką bezpieczeństwa obiektu. Efekt? Mniej chaosu w dostępie kontraktorów, szybsze zmiany uprawnień w wielu lokalizacjach, lepsza rozliczalność i większa przewidywalność działania, gdy ryzyko rośnie.

Poglądowo widać to także w różnych sektorach:

- energetyka stawia na wielowarstwową ochronę obszarów krytycznych,
- transport – na kontrolę stref zastrzeżonych przy dużym przepływie,
- data center – na ścisłą segmentację w modelu multitenant,
- gospodarka wodna – na rozliczalność i ograniczanie ryzyka w rozproszonych, zdalnych obiektach.

W każdym z tych przypadków dobrze zaprojektowana kontrola dostępu realnie wspiera ciągłość usług. W infrastrukturze krytycznej ma to szerszy wymiar, bo mówimy o obiektach i usługach kluczowych dla bezpieczeństwa państwa i obywateli oraz sprawnego funkcjonowania instytucji i przedsiębiorców. Dlatego zabezpieczenia na poziomie dostępu należy traktować jako element ochrony infrastruktury, czyli działań ukierunkowanych na utrzymanie jej funkcjonalności, ciągłości działania i integralności – a nie wyłącznie jako system otwierania przejść. •

Roger sp. z o.o. sp. k.
Gościszewo 59, 82-400 Sztum
roger@roger.pl
www.roger.pl

Głos branży

Infrastruktura krytyczna pod presją zagrożeń hybrydowych

ŁUKASZ WOLNY
BCS

Największym błędem w myśleniu o bezpieczeństwie infrastruktury krytycznej jest dziś traktowanie cyberzagrożeń i zagrożeń fizycznych jako dwóch odrębnych światów. W praktyce coraz częściej mamy do czynienia z zagrożeniami hybrydowymi – od socjotechniki, kradzieży poświadczeń i ransomware po sabotaż, wtargnięcia do stref technicznych oraz działania wymierzone w ciągłość usług. Dyrektywa NIS2 wzmacnia wymagania dotyczące zarządzania ryzykiem cyberbezpieczeństwa, natomiast dyrektywa CER podkreśla odporność podmiotów krytycznych również na zagrożenia fizyczne oraz celowe działania człowieka.

W obiektach infrastruktury krytycznej najpoważniejsze ryzyka koncentrują się dziś w kilku obszarach: przejęciu dostępu wskutek słabych haseł lub phishingu, zakłóceniach pracy systemów IT i OT, zależnościach od dostawców i zdalnego serwisu, a także utracie kontroli nad obiektem w wyniku awarii zasilania, łączności lub działań sabotażowych. Europejskie instytucje bezpieczeństwa od kilku lat konsekwentnie wskazują, że ochrona takich obiektów musi uwzględniać zarówno incydenty cybernetyczne, jak i presję wynikającą z napięć geopolitycznych oraz działań hybrydowych.

Odpowiedzią na te wyzwania nie może być pojedyncze urządzenie, lecz architektura warstwowa. Obejmuje ona m.in. segmentację sieci IT i OT, silne uwierzytelnianie, zasadę minimalnych uprawnień, szyfrowanie, rejestrowanie zdarzeń, procedury reagowania, testy ciągłości działania oraz fizyczną ochronę stref krytycznych. W tym modelu kontrola dostępu nie pełni już wyłącznie funkcji „czytnik–karta–drzwi", lecz staje się narzędziem egzekwowania polityki bezpieczeństwa: ogranicza dostęp do obszarów o podwyższonym ryzyku, wspiera rozliczalność działań i umożliwia szybsze wykrywanie nieprawidłowości. To właśnie takie podejście najlepiej odpowiada wymaganiom NIS2 oraz koncepcji odporności operacyjnej.

Kluczowa jest także integracja systemów. Sam wpis w dzienniku zdarzeń nie daje jeszcze pełnego obrazu incydentu – dopiero połączenie kontroli dostępu z monitoringiem wizyjnym, analityką obrazu, alarmami oraz systemem nadrzędnym pozwala właściwie interpretować zdarzenia i szybko podejmować decyzje. W tej roli BCS Line CMS Pro może pełnić funkcję centralnej platformy zarządzającej, integrującej obraz z kamer, zdarzenia z kontroli dostępu oraz wybrane sygnały z systemów zewnętrznych, co ma szczególne znaczenie w obiektach wielostrefowych i rozproszonych. Dziś najwyższy poziom bezpieczeństwa zapewnia nie pojedynczy produkt, lecz spójny, odporny i stale nadzorowany ekosystem zabezpieczeń. •

Bezpieczeństwo obiektów infrastruktury krytycznej to dziś jedno z kluczowych wyzwań zarządczych. Menedżerowie security mierzą się z dynamicznie zmieniającym się krajobrazem zagrożeń, rosnącą presją regulacyjną oraz koniecznością łączenia bezpieczeństwa fizycznego i cyfrowego. Skuteczna ochrona wymaga nie tylko zaawansowanych technologii, ale także dojrzałego zarządzania ryzykiem i szybkiego podejmowania decyzji. Wypowiedzi ekspertów pokazują, z jakimi problemami liderzy bezpieczeństwa spotykają się najczęściej i jak odpowiadają na te wyzwania w praktyce.

Bezpieczeństwo IK w praktyce

PIOTR SITKO
POLSKA WYTWÓRNIA PAPIERÓW WARTOŚCIOWYCH S.A.

W niepewnej sytuacji geopolitycznej i w czasie nasilonych działań hybrydowych menedżerowie ds. bezpieczeństwa obiektów strategicznych zachowują szczególną czujność. Priorytetami są działania prowadzące do modernizacji systemów bezpieczeństwa, wdrożenie AI i skuteczna edukacja pracowników.

W obszarze security kluczowymi elementami są stała kontrola i czujność. Oznacza to całodobową pracę zespołów bezpieczeństwa, modernizację sprzętu, eliminowanie luk w zabezpieczeniach oraz ciągły rozwój organizacji poprzez szkolenia.

W Polskiej Wytwórni Papierów Wartościowych S.A. obowiązują szczegółowo określone zasady bezpieczeństwa, które są rygorystycznie przestrzegane. Praca zaczyna się od podstawowych, codziennych, absolutnie wymaganych czynności. Przede wszystkim należy zwracać uwagę na każdy szczegół i niestandardowe sytuacje, np. czy ktoś nie przymocował czegoś do ogrodzenia, nie pozostawił podejrzanej paczki, czy nie pojawia się zbyt często w pobliżu obiektu, nie wykonuje zdjęć lub nagrań, nie wnosi nietypowych przedmiotów. Równie ważna jest kontrola dostępu do organizacji. Oznacza to m.in. dokładne sprawdzanie tożsamości i bagażu gości, firm realizujących inwestycje na terenie obiektu oraz kontrolę pojazdów wjeżdżających na teren zakładu i niego wyjeżdżających.

Kolejną bardzo ważną kwestią jest ciągłe testowanie systemów bezpieczeństwa oraz planów ciągłości działania. Z jednej strony testy fizyczne, sprawdzające, czy pracownicy służby ochrony właściwie reagują na alarmy, czy są czujni i gotowi do interwencji. Z drugiej strony testy związane z ciągłością działania, czyli weryfikacja, czy organizacja poradzi sobie w sytuacjach kryzysowych, takich jak przerwy w dostawach energii, problemy z dostępem do zasobów czy zakłócenia w łańcuchu dostaw.

Priorytetem dla security managera powinna być także uważna obserwacja zmieniającego się otoczenia. Ważne jest śledzenie rozwoju nowych technologii, takich jak systemy antydronowe, rozwiązania związane z ochroną perymetryczną, wdrażania AI. Należy jednak pamiętać, że technologie powinny wspierać, a nie zastępować ludzi. W PWPW S.A. regularnie prowadzimy szkolenia, m.in. z zakresu phishingu i symulowanych ataków, aby uwrażliwić pracowników i zwiększyć ich świadomość. Dzięki temu dobrze radzimy sobie z tego typu zagrożeniami.

Nie ma dziś bezpieczeństwa bez inwestycji zarówno w rozwój kompetencji pracowników, jak i w nowoczesne rozwiązania technologiczne. Kluczowe jest korzystanie z aktualnych, wspieranych przez producentów systemów oraz bieżące reagowanie na zmiany.

Współczesne systemy zabezpieczeń, takie jak systemy alarmowe, monitoring wizyjny czy kontrola dostępu, powinny być uzupełniane o rozwiązania pozwalające analizować zdarzenia i wykrywać anomalie. Należy jak najszybciej wdrażać rozwiązania oparte na sztucznej inteligencji, które wspierają identyfikację nietypowych zachowań i zagrożeń.

Najważniejsze jest szybkie reagowanie na zmiany i podejmowanie decyzji. Nie zawsze będą one idealne, ale brak decyzji w obszarze bezpieczeństwa może mieć bardzo poważne konsekwencje, włącznie z utratą danych i znacznymi stratami finansowymi.

Mamy to szczęście, że Zarząd PWPW S.A. doskonale rozumie znaczenie bezpieczeństwa. Jest ono fundamentem naszej działalności, zarówno w kontekście produktów, jak i warunków ich wytwarzania. Nieustannie podkreślam, że bez inwestycji i otwartej rozmowy o bezpieczeństwie nie da się zapewnić jego odpowiedniego poziomu ani budować stabilnej organizacji. •

Podejmowanie właściwych strategicznych decyzji

JANUSZ SYRÓWKA
eon

Przez ostatnie kilka lat w branży bezpieczeństwa obserwujemy zjawisko nieustannego wzrostu poziomu zagrożeń. Jest to sytuacja wyjątkowo trudna, w której wszystkie dotychczasowe rozwiązania zabezpieczające są brutalnie weryfikowane przez rzeczywistość. Próbie „ognia" poddawane są zarówno poszczególne elementy systemów ochrony, jak i – co najważniejsze – całe strategie bezpieczeństwa. To moment krytyczny, w którym należy podejmować decyzje strategiczne: po co i w jaki sposób budować bezpieczeństwo na nadchodzące, trudne i niespokojne lata.

Firmy mające infrastrukturę krytyczną stają dziś pod bezprecedensową presją. Niezależnie od scenariusza zagrożeń, społeczeństwo musi mieć zapewniony dostęp do prądu, wody, żywności czy ciepła w okresie zimowym. To oczywisty i niezwykle istotny aspekt społeczny. Istnieje jednak jeszcze jedna kwestia, która – moim zdaniem – ginie w debacie publicznej: obronność państwa. Jesteśmy zasypywani informacjami o liczbie zakupionych lub zamówionych czołgów, samolotów, rakiet czy okrętów. To bez wątpienia ważne, jednak czym będzie ten sprzęt bez dostępu do energii elektrycznej oraz sprawnie działającego transportu drogowego, kolejowego i lotniczego? Odporni operatorzy infrastruktury krytycznej są dla obronności równie niezbędni jak armia.

Mam wrażenie, że wymagania obecnej sytuacji zaczynają wykraczać poza możliwości pojedynczych przedsiębiorstw. Oczywiście firmy dysponują szerokim polem działania w zakresie zabezpieczania własnej infrastruktury, należy jednak pamiętać, że stanowią one jedynie element państwowego systemu bezpieczeństwa, który składa się z wielu warstw. Dobrym przykładem są rozwiązania antydronowe. Wielu dostawców oferuje różnorodne systemy operatorom infrastruktury krytycznej – pojawia się jednak pytanie: w jakim celu? Brakuje bowiem regulacji prawnych i systemowych rozwiązań umożliwiających stworzenie wielowarstwowego systemu obrony przeciwlotniczej w kraju. Jeśli przedsiębiorstwa infrastruktury krytycznej mają odgrywać w nim określoną rolę, musi ona zostać jasno zdefiniowana.

Wracając do decyzji strategicznych – wszystkie działania powinny być ukierunkowane na odbudowę infrastruktury krytycznej, tak aby możliwie jak najszybciej przywracać świadczenie usług. W obszarze bezpieczeństwa oznacza to wzmacnianie zdolności wykrywania zagrożeń i incydentów, rozwój komunikacji kryzysowej oraz doskonalenie systemów ciągłości działania. Nie można przy tym pominąć kwestii wykraczającej poza same służby bezpieczeństwa – konieczne jest przemodelowanie polityk magazynowania części zamiennych i materiałów niezbędnych do odbudowy.

W dobie powszechnej dyskusji na temat sztucznej inteligencji chciałbym wskazać jeden istotny kierunek, który może stanowić element strategii bezpieczeństwa. Rozwiązania oparte na sztucznej inteligencji to bez wątpienia nowa jakość, niosąca ze sobą niespotykany dotąd potencjał w tej dziedzinie. Pytanie jednak, czy jesteśmy w stanie ten potencjał realnie wykorzystać. Dobrym punktem wyjścia jest analiza przepustowości posiadanych sieci teleinformatycznych. Nową jakość musimy bowiem budować od podstaw – także tych mniej atrakcyjnych i kosztownych. •

Priorytety menedżera bezpieczeństwa

RAFAŁ BATKOWSKI
ekspert ds. bezpieczeństwa

Żyjemy w wyjątkowo skomplikowanym czasie, naznaczonym dwoma konfliktami, które w istotny sposób wpływają na infrastrukturę krytyczną, w tym sektor energii w naszym kraju. Obiekty te są szczególnie narażone na zagrożenia asymetryczne, hybrydowe, z jakimi mierzy się dziś świat. To infrastruktura kluczowa do obrony w przypadku kryzysu militarnego.

Moim zdaniem świadomość i kompetencje naszych menedżerów bezpieczeństwa są obecnie na bardzo wysokim poziomie. Miałem okazję obserwować sytuację w innych krajach, dlatego z pełnym przekonaniem mogę powiedzieć, że w Polsce rozumienie tego, jak powinniśmy chronić infrastrukturę, jest bardzo pogłębione. Przekłada się to na konkretne działania, które pozwalają na stosowanie skutecznych praktyk ochronnych.

W rzeczywistości bezpieczeństwo przenika wszystkie procesy biznesowe. Dlatego jednym z najważniejszych wyzwań stojących dziś przed menedżerami jest całościowe podejście do zarządzania bezpieczeństwem oraz skuteczne kontrolowanie i prowadzenie tych procesów – począwszy od weryfikacji kontrahentów aż po analizę łańcuchów dostaw. Dzisiaj takie idee, jak *security by design* (wdrażanie standardów bezpieczeństwa już od fazy koncepcyjnej, projektowej) oraz *predictive security* (wykorzystanie zaawansowanych modeli matematycznych i AI do przewidywania zagrożeń/zdarzeń), mają kluczowe znaczenie.

Istotnym elementem jest także bezpieczeństwo gospodarcze, obejmujące procesy mniej widoczne, takie jak zakupy czy inwestycje. Ich opóźnianie lub nieuprawniona ingerencja mogą prowadzić do strat, opóźnień, a w konsekwencji do braku realizacji kluczowych inicjatyw wspierających funkcjonowanie infrastruktury krytycznej.

Najpoważniejsze wyzwania, w mojej ocenie, stanowią dziś zagrożenia cybernetyczne, które przenikają niemal wszystkie obszary zarządzania bezpieczeństwem. Każde działanie – także sprawców – jest dziś w pewnym stopniu powiązane z przestrzenią cyfrową: Internetem, komunikacją i zdalnym przesyłem danych. Wszyscy pozostawiamy ślady w tej przestrzeni. Z jednej strony umożliwia to identyfikację sprawców, z drugiej jednak pokazuje, że niemal wszystkie procesy są dziś cyfrowo przetwarzane, od danych po obrazy z systemów monitoringu i sensorów. Cyberprzestrzeń staje się więc kluczowym polem działań.

Jeśli chodzi o priorytety dla zarządzających bezpieczeństwem, należy wskazać przede wszystkim zagrożenia hybrydowe, których obecnie doświadczamy. Tworzą one złożony system oddziaływań, w którym trudno o jednoznaczne schematy działania. Dlatego kluczowe znaczenie ma zdolność do całościowego spojrzenia na zagrożenia oraz ujęcia ich w spójną politykę i strategię bezpieczeństwa, ukierunkowaną na budowanie odporności organizacji. •

Ochrona obiektów IK

DAWID KARCZEWSKI
Grupa LipCo Foods

Obiekty infrastruktury krytycznej (IK) stanowią kluczowe elementy funkcjonowania państwa i fundament bezpieczeństwa obywateli. Obejmują one takie sektory jak: energetyka, transport, łączność i sieci teleinformatyczne, zaopatrzenie w wodę, finanse, ratownictwo i ochrona zdrowia, żywność, chemia i promieniotwórczość oraz administracja publiczna.

Z tego względu ochrona obiektów IK jest dla menedżerów ds. bezpieczeństwa obszarem priorytetowym – wymagającym szerokiego spojrzenia i umiejętności identyfikacji różnorodnych typów zagrożeń, na jakie obiekty te mogą być narażone.

W dziedzinie bezpieczeństwa IK można wyróżnić następujące obszary wymagające szczególnej uwagi:

- **Bezpieczeństwo fizyczne –** ochrona obiektów przed nieautoryzowanym dostępem, kradzieżą i aktami wandalizmu.
- **Zagrożenia hybrydowe –** sabotaż i dywersja.
- **Cyberbezpieczeństwo –** ochrona przed cyberatakami, których obiekty IK są częstym celem.
- **Szkolenia –** systematyczna edukacja pracowników w zakresie procedur bezpieczeństwa i potencjalnych zagrożeń.
- **Systemy zarządzania kryzysowego –** opracowane i aktualizowane plany reagowania na sytuacje kryzysowe oraz plany ciągłości działania.
- **Integracja systemów –** połączenie bezpieczeństwa fizycznego z cyberbezpieczeństwem jako skuteczniejsza i spójna forma ochrony.
- **Monitorowanie i analiza –** bieżąca obserwacja infrastruktury, analiza zagrożeń oraz ciągłe doskonalenie procedur, wspierane wewnętrznymi audytami bezpieczeństwa.

Ochrona obiektów IK wymaga zatem bardzo szerokiego i wielowymiarowego podejścia do tematyki bezpieczeństwa. Spektrum potencjalnych zagrożeń jest rozległe, co oznacza konieczność ich sprawnej identyfikacji i systematycznego zarządzania ryzykiem. Wymaga to nieustannego doskonalenia systemów ochrony – zarówno w zakresie zabezpieczeń technicznych, ochrony fizycznej, jak i bezpieczeństwa sieci IT. W warunkach rosnących kosztów pracy niezbędna staje się inwestycja w nowoczesne systemy i programy szkoleniowe, które podnoszą kwalifikacje pracowników sektora bezpieczeństwa i zwiększają efektywność ich działania. Ciągłe doskonalenie jest bezwzględnym warunkiem utrzymania odpowiedniego poziomu ochrony obiektów IK w obliczu tak złożonego i dynamicznie zmieniającego się środowiska zagrożeń. •

Wyzwania dla menedżerów IK

IRENEUSZ RUPIK
TAURON NOWE TECHNOLOGIE

W obecnej dynamicznie zmieniającej się sytuacji geopolitycznej bezpieczeństwo infrastruktury krytycznej staje się jednym z kluczowych obszarów odpowiedzialności organizacji. Rosnąca liczba incydentów, zarówno cybernetycznych, jak i fizycznych, pokazuje, że zagrożenia stają się bardziej złożone i coraz częściej mają charakter hybrydowy.

Menedżerowie odpowiedzialni za bezpieczeństwo obiektów IK muszą więc koncentrować się na budowaniu realnej odporności oraz na wczesnym wykrywaniu symptomów potencjalnych ataków, które mogą zakłócić ciągłość działania lub doprowadzić do poważnych strat operacyjnych.

Kluczowe znaczenie ma dziś modernizacja systemów bezpieczeństwa, szczególnie w obszarach monitoringu, detekcji anomalii oraz integracji różnych warstw zabezpieczeń. Technologie oparte na sztucznej inteligencji przynoszą wymierne korzyści – pozwalają szybciej analizować dane, skuteczniej identyfikować nietypowe zachowania i poprawiają jakość reakcji na zagrożenia. W środowiskach przemysłowych, gdzie każda przerwa w działaniu może mieć szerokie konsekwencje, nowoczesne narzędzia zwiększają odporność operacyjną i wspierają bardziej świadome decyzje.

Jednocześnie należy pamiętać, że nawet najbardziej zaawansowane technologie nie zastąpią dobrze przygotowanych pracowników. Regularne szkolenia, podnoszenie świadomości zagrożeń oraz praktyczne ćwiczenia obejmujące także scenariusze międzysektorowe pozostają fundamentem skutecznego bezpieczeństwa. W równym stopniu istotne jest utrzymywanie aktualnych procedur, przetestowanych planów ciągłości działania oraz sprawnej komunikacji wewnętrznej.

W obliczu obecnych wyzwań priorytetem staje się więc połączenie modernizacji technicznej, wzmacniania kompetencji personelu oraz wdrażania podejścia opartego na ciągłym doskonaleniu. Tylko takie działania pozwalają budować odporność infrastruktury krytycznej na zagrożenia, które dziś zmieniają się szybciej niż kiedykolwiek wcześniej. •

Wodociągi pod specjalnym nadzorem

KRZYSZTOF NOWACKI
Przedsiębiorstwo Wodociągów i Kanalizacji w Obornikach

Dziś bezpieczeństwo w branży wodociągowo-kanalizacyjnej trzeba rozumieć znacznie szerzej niż jeszcze kilka lat temu. To już nie tylko ochrona fizyczna obiektów, ogrodzenia czy monitoring, choć nadal pozostają one ważnym elementem systemu. Coraz większym i bardzo realnym zagrożeniem są cyberataki, które dotykają nie tylko dużych przedsiębiorstw, ale również mniejszych wodociągów.

Kluczowe jest więc budowanie świadomości wśród kadry zarządzającej oraz przeprowadzenie rzetelnej inwentaryzacji zasobów, zarówno infrastruktury technicznej, jak i systemów IT/OT. Dopiero pełna wiedza o tym, co posiadamy i gdzie mogą występować słabe punkty, pozwala skutecznie zarządzać ryzykiem i ograniczać potencjalne wektory ataku.

Warto również patrzeć na zagrożenia w sposób zintegrowany. Przykłady z ostatnich tygodni, m.in. z Iranu, pokazują, że ataki mogą mieć charakter hybrydowy, jednocześnie atak cyber oraz fizyczny. Dlatego plany ciągłości działania i plany bezpieczeństwa powinny obejmować wszystkie elementy systemu: od ujęć wody, przez oczyszczalnie, aż po instalacje pomocnicze, takie jak fotowoltaika, APN-y czy systemy zdalnego sterowania.

Nie można też zapominać o czynniku ludzkim. Nawet najlepsze zabezpieczenia techniczne nie zastąpią świadomego i przeszkolonego pracownika. Dziś to właśnie brak wiedzy i czujności personelu jest jednym z najsłabszych ogniw w systemie bezpieczeństwa.

W obecnej sytuacji trudno wskazać jeden uniwersalny priorytet, bo bezpieczeństwo w branży wodociągowo-kanalizacyjnej to system naczyń połączonych. Punktem wyjścia powinna być jednak świadomość, realne zrozumienie zagrożeń oraz uczciwa diagnoza własnej organizacji. Kluczowe jest zdefiniowanie słabych obszarów i sprawdzenie, co jesteśmy w stanie zrobić własnymi siłami, a gdzie potrzebne będzie wsparcie zewnętrzne.

Dobrym krokiem jest powołanie zespołu roboczego, który krok po kroku będzie budował odporność organizacji. Na początku warto przeanalizować obowiązujące procedury, wiele z nich bowiem istnieje tylko „na papierze" lub są nieaktualne. Równolegle należy zadbać o bezpieczeństwo codziennej pracy: zarówno w wymiarze fizycznym (kontrola dostępu, zamykanie obiektów, obserwacja ujęć wody), jak i wymiarze cyberbezpieczeństwa, czyli tzw. higienę cyfrową.

Nie można pomijać inwentaryzacji zasobów, od infrastruktury po systemy IT i OT. Dopiero mając pełny obraz, można świadomie wdrażać nowe rozwiązania, w tym narzędzia oparte na AI, np. w monitoringu wizyjnym czy analizie danych.

Najważniejsze są jednak trzy elementy: świadomość, dobry plan i konsekwencja. Cyberodporność nie kończy się na spisaniu procedur czy wdrożeniu jednego systemu, to proces, który dopiero się wtedy zaczyna i wymaga ciągłego doskonalenia. •

Zagrożenia ze strony powietrznych statków bezzałogowych

ARTUR NOWAKOWSKI
Linc Polska

Incydent związany z odnalezieniem bezzałogowego statku powietrznego na terenie kopalni węgla brunatnego w Wielkopolsce jest kolejnym sygnałem wskazującym na zmiany w środowisku bezpieczeństwa obiektów przemysłowych i infrastruktury krytycznej. Obiekt został znaleziony przez pracownika zakładu, a służby potwierdziły, że nie był uzbrojony. Według nieoficjalnych informacji odnaleziony dron mógł przypominać bezzałogowce, które wcześniej wtargnęły do polskiej przestrzeni powietrznej ze wschodu. Choć w tym przypadku nie doszło do zniszczeń i nikt nie ucierpiał, zdarzenie stanowi wyraźne ostrzeżenie.

Drony stały się powszechnie dostępne, relatywnie tanie i łatwe w użyciu. Mogą być wykorzystywane zarówno do szpiegostwa przemysłowego, jak i do działań sabotażowych. Instytucje bezpieczeństwa zwracają uwagę, że bezzałogowce coraz częściej pojawiają się w pobliżu infrastruktury krytycznej.

Nowoczesne zakłady przemysłowe, takie jak kopalnie, elektrownie, rafinerie, magazyny paliw, centra logistyczne czy zakłady produkcyjne, od lat inwestują w fizyczne systemy zabezpieczeń: ogrodzenia, kontrolę dostępu, monitoring wizyjny oraz ochronę fizyczną. Współczesne systemy bezpieczeństwa powinny jednak uwzględniać także zagrożenia z powietrza, w szczególności wynikające z dynamicznego rozwoju technologii statków bezzałogowych.

W tym kontekście kluczowe znaczenie ma wczesne wykrywanie, identyfikacja oraz śledzenie obiektów latających w pobliżu chronionego terenu. Połączenie systemów radarowych oraz systemów detekcji sygnałów radiowych (RF) przynosi obecnie najlepsze rezultaty. Radary krótkiego zasięgu umożliwiają wykrywanie niewielkich obiektów powietrznych w odległości kilku kilometrów, natomiast systemy RF analizują emisję radiową pomiędzy dronem a jego operatorem, pozwalając na identyfikację typu urządzenia, kierunku lotu, a w wielu przypadkach także lokalizację operatora. Kooperacja tych technologii tworzy podstawową warstwę świadomości sytuacyjnej w przestrzeni powietrznej nad chronionym obiektem.

Wykrycie intruza uruchamia kolejne elementy systemu bezpieczeństwa – od alarmowania służb, poprzez analizę zagrożenia, aż po zastosowanie środków neutralizacji. Brak warstwy detekcyjnej sprawia, że system zabezpieczeń pozostaje „ślepy” na zagrożenia z powietrza.

Incydenty takie jak ten w wielkopolskiej kopalni pokazują, że przestrzeń powietrzna nad obiektami przemysłowymi i infrastrukturą krytyczną staje się nowym obszarem ryzyka. W dobie powszechnej dostępności dronów bezpieczeństwo tych obiektów musi być chronione w sposób kompleksowy. •

Ilustracje: Marta Kołodziejak / A&S AI Studio

Hikvision wyznacza nowe standardy cyberbezpieczeństwa i zaufania cyfrowego

Hikvision po raz kolejny potwierdza swoje zaangażowanie w przejrzystość oraz najwyższe standardy bezpieczeństwa cyfrowego, uzyskując prestiżowe certyfikaty ISO/IEC 29147:2018 oraz ISO/IEC 30111:2019 przyznane przez renomowaną organizację BSI Group.

Jarosław Grzybowski

Międzynarodowe normy tej rangi stanowią punkt odniesienia dla firm technologicznych na całym świecie i potwierdzają, że procesy zarządzania podatnościami stosowane przez firmę należą do najbardziej zaawansowanych i dojrzałych w branży.

Uzyskane certyfikacje potwierdzają konsekwentne wdrażanie filozofii *Secure by Design*, traktowanej jako fundament całego cyklu życia produktu – od etapu koncepcji, przez projektowanie i produkcję, aż po wdrożenie i eksploatację przez użytkownika końcowego. Oznacza to, że bezpieczeństwo nie jest dodatkiem, lecz integralną częścią każdego rozwiązania, a decyzje projektowe uwzględniają potencjalne zagrożenia już na najwcześniejszym etapie.

Transparentność i skuteczne zarządzanie podatnościami

Certyfikaty ISO/IEC 29147:2018 oraz ISO/IEC 30111:2019 podkreślają dwa kluczowe obszary działalności firmy: przejrzyste ujawnianie podatności oraz ich systematyczne usuwanie.

Zgodność z normą ISO/IEC 29147:2018 oznacza stosowanie globalnych wytycznych dotyczących raportowania potencjalnych zagrożeń oraz zapewnienie otwartej i odpowiedzialnej komunikacji ze społecznością ekspertów ds. cyberbezpieczeństwa.

Z kolei ISO/IEC 30111:2019 definiuje rygorystyczne procedury wewnętrzne związane z analizą i eliminacją podatności. Każda wykryta luka bezpieczeństwa jest analizowana w sposób ustandaryzowany i usuwana zgodnie z jasno określonymi procesami. Takie podejście minimalizuje ryzyko, zwiększa zaufanie użytkowników oraz skraca czas reakcji na potencjalne zagrożenia.

W ramach rozwiniętego systemu zarządzania bezpieczeństwem funkcjonuje dedykowane centrum reagowania na incydenty bezpieczeństwa (HSRC – *Hikvision Security Response Center)*, które odpowiada za przyjmowanie zgłoszeń, analizę oraz koordynację publikacji informacji o podatnościach.

Firma stosuje również uznane globalne standardy klasyfikacji i raportowania podatności, takie jak CVE *(Common Vulnerabilities and Exposures)* oraz CVSS, co umożliwia jednoznaczne określenie poziomu ryzyka i ułatwia współpracę z międzynarodową społecznością ekspertów.

Istotnym elementem jest także jasno zdefiniowany czas reakcji – podatności o wysokim i krytycznym poziomie ryzyka usuwane są nawet w ciągu 24 godzin, co znacząco ogranicza potencjalne zagrożenia dla użytkowników.

Certyfikaty te uzupełniają szerokie portfolio międzynarodowych standardów, które firma już spełnia, w tym:

- ISO/IEC 27001 i 27701 – zarządzanie bezpieczeństwem informacji i prywatnością
- ISO/IEC 29151 – ochrona danych osobowych (PII)
- ETSI EN 303 645 – cyberbezpieczeństwo urządzeń IoT
- Common Criteria (EAL3+) – certyfikacja bezpieczeństwa produktów IT
- CSA STAR oraz Singapore CLS – standardy bezpieczeństwa usług chmurowych
- CMMI Level 5 – najwyższy poziom dojrzałości procesów wytwarzania oprogramowania

Tak szeroki zakres certyfikacji potwierdza wielowarstwowe podejście do bezpieczeństwa, obejmujące zarówno infrastrukturę technologiczną, jak i procesy organizacyjne, zarządzanie ryzykiem oraz kulturę bezpieczeństwa w całej organizacji.

Od bezpiecznego projektu do bezpiecznej eksploatacji

Budowanie zaufania cyfrowego nie kończy się na etapie projektowania produktów. Bezpieczeństwo traktowane jest jako proces ciągły, który musi być utrzymywany przez cały cykl życia systemu. Obejmuje to regularne aktualizacje oprogramowania, monitorowanie zagrożeń oraz szybkie reagowanie na nowe podatności.

Firma prowadzi także publiczne komunikaty bezpieczeństwa (*security advisories*), w których na bieżąco informuje użytkowników o wykrytych zagrożeniach oraz dostępnych aktualizacjach oprogramowania.

W ramach kompleksowego podejścia wdrażane są m.in.:

- bezpieczny cykl życia rozwoju oprogramowania (SSDLC)
- zarządzanie podatnościami i ich priorytetyzacja
- testy penetracyjne oraz audyty bezpieczeństwa realizowane przez podmioty zewnętrzne
- mechanizmy aktualizacji firmware i zarządzania poprawkami
- systemy wykrywania i reagowania na incydenty bezpieczeństwa

Dodatkowo stosowany jest model tzw. skoordynowanego ujawniania podatności (*coordinated vulnerability disclosure*), który zakłada współpracę z badaczami bezpieczeństwa i publikację informacji dopiero po przygotowaniu odpowiednich poprawek.

Takie działania pozwalają nie tylko reagować na zagrożenia, ale również je przewidywać i ograniczać ich wpływ jeszcze przed wystąpieniem incydentu.

Prywatność i suwerenność danych

Ochrona prywatności użytkowników stanowi jeden z filarów strategii firmy. Właścicielem danych pozostaje zawsze użytkownik końcowy, który zachowuje pełną kontrolę nad ich przechowywaniem i przetwarzaniem.

Rozwiązania projektowane są z myślą o różnych scenariuszach wdrożeniowych – zarówno lokalnych (*on-premises*), chmurowych, jak i hybrydowych. Podejście to wpisuje się w rosnące znaczenie suwerenności danych, czyli możliwości zarządzania informacjami zgodnie z lokalnymi regulacjami oraz wymaganiami organizacyjnymi.

Cyberbezpieczeństwo jako wspólna odpowiedzialność

Cyberbezpieczeństwo postrzegane jest jako wspólna odpowiedzialność wszystkich uczestników ekosystemu – producentów, integratorów systemów, instalatorów oraz użytkowników końcowych.

Firma aktywnie zachęca również badaczy bezpieczeństwa do zgłaszania potencjalnych podatności poprzez dedykowane kanały komunikacji, co wspiera rozwój bezpiecznego ekosystemu technologicznego oraz umożliwia szybsze wykrywanie zagrożeń.

Ostateczny poziom bezpieczeństwa zależy jednak również od sposobu wdrożenia, konfiguracji oraz codziennego użytkowania systemów, dlatego duży nacisk kładziony jest na edukację i dobre praktyki.

Wsparcie i edukacja użytkowników

W celu wsparcia partnerów i klientów realizowany jest szeroko zakrojony program edukacyjny obejmujący:

- webinary prowadzone przez ekspertów
- kursy online dotyczące konfiguracji i zabezpieczeń
- dokumentację techniczną oraz poradniki wdrożeniowe
- materiały wideo i artykuły eksperckie

Celem tych działań jest budowanie systemów odpornych na cyberzagrożenia oraz promowanie tzw. „cyfrowej higieny", czyli codziennych praktyk ograniczających ryzyko incydentów.

Istotnym elementem jest również zapewnienie użytkownikom dostępu do aktualizacji oraz poprawek bezpieczeństwa, które są publikowane wraz z zaleceniami wdrożeniowymi, co umożliwia szybkie zabezpieczenie systemów przed znanymi zagrożeniami.

Aby uzyskać więcej informacji na temat inicjatyw Hikvision w zakresie cyberbezpieczeństwa i dostępu do materiałów edukacyjnych, odwiedź stronę: https://www.hikvision.com/pl/support/cybersecurity/. •

O FIRMIE HIKVISION

Firma Hikvision została założona w 2001 r. i koncentruje się na zintegrowanych systemach bezpieczeństwa oraz cyfryzacji opartej na scenariuszach zastosowań. Wykorzystując technologie sztucznej inteligencji oraz Internetu Rzeczy (AIoT), dostarcza zaawansowane rozwiązania dla wielu sektorów gospodarki.

Działalność firmy rozwija się dzięki technologiom głęboko zakorzenionym w innowacji oraz stale poszerzanej ofercie produktów i rozwiązań AIoT. Dzięki otwartemu ekosystemowi Hikvision aktywnie wspiera rozwój branży oraz współpracuje z partnerami na całym świecie.

Kierując się wartościami profesjonalizmu, rzetelności i uczciwości, firma rozwija innowacyjne technologie percepcji maszynowej, wspierając podejmowanie trafnych decyzji oraz przyczyniając się do zwiększenia bezpieczeństwa i zrównoważonego rozwoju.

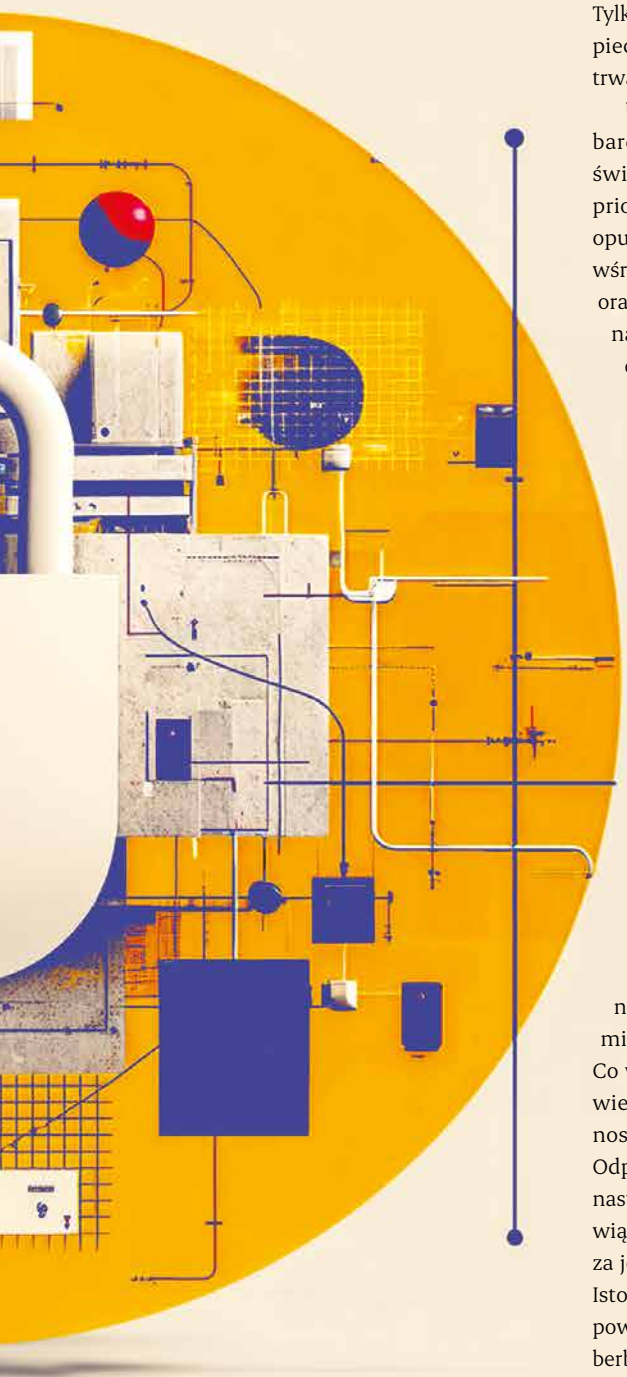
Obecnie organizacja posiada 11 centrów badawczo-rozwojowych oraz 7 baz produkcyjnych na całym świecie, a jej produkty i usługi są dostępne w ponad 180 krajach i regionach. W 2024 r. przychody firmy wyniosły 92,50 mld RMB (około 12,87 mld USD), co potwierdza jej silną pozycję na globalnym rynku technologii bezpieczeństwa.

Hikvision Poland
ul. Żwirki i Wigury 16B
02-092 Warszawa
www.hikvision.com/europe/
info.pl@hikvision.com

Odpowiedzialność kierownictwa w świetle krajowych regulacji implementujących Dyrektywy CER i NIS2

Dynamiczny wzrost zagrożeń w cyberprzestrzeni oraz rosnące znaczenie infrastruktury krytycznej spowodowały istotną zmianę podejścia do kwestii cyberbezpieczeństwa. W obliczu poważnych zagrożeń przyspieszający rozwój cyfrowego świata wymaga wspólnych i odpowiedzialnych działań, które powinny być kluczowym elementem budowania cyberbezpieczeństwa w każdej organizacji.

Dorota Duda



Dbanie o cyberbezpieczeństwo obejmuje nie tylko implementację odpowiednich narzędzi i technologii, ale także rozwój kultury bezpieczeństwa, regularne szkolenia pracowników oraz tworzenie i utrzymywanie planów reagowania na incydenty. Tylko kompleksowe podejście do cyberbezpieczeństwa może zapewnić organizacji trwałą ochronę.

Unia Europejska (UE) w ramach coraz bardziej zglobalizowanego i cyfrowego świata uznaje cyberbezpieczeństwo za priorytetową kwestię. 27 grudnia 2022 r. opublikowała pakiet regulacji prawnych, wśród których znalazły się dyrektywy CER oraz NIS2. Pierwsza z nich koncentruje się na wzmocnieniu cyberbezpieczeństwa, druga zaś skupia się na odporności podmiotów krytycznych. W obu dyrektywach podkreślone jest znaczenie ról i odpowiedzialności za realizację działań w zakresie odporności organizacji.

Dyrektywa NIS2 kładzie szczególny nacisk na **odpowiedzialność kierownictwa poszczególnych podmiotów w zakresie zapewnienia cyberbezpieczeństwa.** W polskim porządku prawnym zmiany te znajdują odzwierciedlenie w znowelizowanej ustawie o krajowym systemie cyberbezpieczeństwa z 2026 r. Wprowadza ona do polskiego porządku prawnego nową, istotną rolę: **kierownika podmiotu kluczowego lub podmiotu ważnego.** Ponosi on odpowiedzialność za wykonywanie obowiązków podmiotu w zakresie cyberbezpieczeństwa. Co ważne, jeżeli kierownikiem jest organ wieloosobowy, to odpowiedzialność ponoszą wszyscy członkowie tego organu. Odpowiedzialność kierownika podmiotu następuje także wtedy, gdy niektóre z obowiązków zostały powierzone innej osobie za jej zgodą. Jaki jest cel tych rozwiązań? Istotne jest, aby kierownictwo podmiotu poważnie podchodziło do zapewnienia cyberbezpieczeństwa podmiotu. Obecnie bez bezpiecznych systemów informacyjnych nie jest możliwe sprawne świadczenie usług innym podmiotom i konsumentom. **A więc cyberbezpieczeństwo przestaje być jedynie domeną działów IT, a staje się priorytetowym zadaniem kadry zarządzającej.**

Jakie są najistotniejsze zadania kierownika podmiotu kluczowego lub podmiotu ważnego?

- Podejmowanie decyzji w zakresie przygotowania, wdrażania, stosowania i przeglądu systemu zarządzania bezpieczeństwem informacji (SZBI) w podmiocie. Kierownik odpowiada za SZBI i jego rozwój zgodnie z cyklem Deminga.
- Planowanie adekwatnych środków finansowych na realizację obowiązków z zakresu cyberbezpieczeństwa, które wymagają nakładów (nie powinny one być pomijane w budżetach podmiotów kluczowych lub ważnych).
- Przydzielanie zadań z zakresu cyberbezpieczeństwa w podmiocie i nadzorowanie ich wykonania.
- Zapewnienie, że personel podmiotu jest świadomy obowiązków z zakresu cyberbezpieczeństwa i zna przepisy prawa oraz wewnętrzne regulacje w tym zakresie. SZBI wymaga, aby każdy pracownik organizacji miał przypisaną rolę i zadania do wykonania celem zachowania bezpieczeństwa informacji.
- Zapewnienie zgodności działania podmiotu z przepisami prawa oraz z wewnętrznymi regulacjami podmiotu.

Mając na względzie, jak ważną rolę odgrywa w każdej organizacji kształtowanie kultury bezpieczeństwa, osoby kierujące podmiotami kluczowymi lub ważnymi muszą **raz na rok przejść szkolenie z zakresu cyberbezpieczeństwa, którego realizacja musi być udokumentowana.**

Powyższe gwarantuje, że osoby te będą posiadać świadomość i aktualną wiedzę na temat zagrożeń, obszarów ich występowania i wzajemnych powiązań oraz możliwości podejmowania działań prewencyjnych, które pozwalają na budowanie bezpieczeństwa organizacji.

Ważną gwarancją prawidłowego wykonywania zadań z zakresu cyberbezpieczeństwa jest potwierdzenie, że zadań tych nie mogą wykonywać osoby skazane za przestępstwa przeciwko ochronie informacji. Daje to odpowiednią gwarancję, że zadania te będą wykonywały osoby dające rękojmię ich prawidłowej realizacji. Zaświadczenia w tym zakresie będą weryfikowane przez ich pracodawców. Weryfikacja personelu przed przydzieleniem zadań z zakresu cyberbezpieczeństwa jest przewidywana przez normy techniczne, np. normę ISO 27001.

W kontekście odpowiedzialności kierownictwa kluczowe znaczenie mają przepisy nakładające obowiązek:

- wdrożenia systemu zarządzania bezpieczeństwem informacji;
- przeprowadzania analizy ryzyka;
- zapewnienia ciągłości działania oraz bezpieczeństwa łańcucha dostaw produktów, usług i procesów;
- raportowania incydentów.

Co więcej, istotne znaczenie ma również edukacja z zakresu cyberbezpieczeństwa dla personelu podmiotu kluczowego lub ważnego oraz stosowanie podstawowych zasad cyberhigieny.

Z kolei dyrektywa CER koncentruje się na odporności podmiotów krytycznych wobec różnorodnych zagrożeń, nie tylko cybernetycznych. W polskim porządku prawnym zmiany te znajdują odzwierciedlenie w nowelizowanej ustawie o zarządzaniu kryzysowym.

Projektowane rozwiązania mają na celu m.in. wzmocnienie ochrony infrastruktury krytycznej, w szczególności niezbędnej do świadczenia tzw. usług kluczowych przez podmioty krytyczne czy też wdrożenie rozwiązań umożliwiających wzmocnienie ochrony najważniejszych dla państwa obszarów, obiektów i urządzeń, w szczególności infrastruktury morskiej. Obowiązki podmiotów krytycznych dotyczą m.in. przeprowadzania oceny ryzyka oraz wdrożenie adekwatnie do jej wyników odpowiednich rozwiązań organizacyjno-technicznych, zapewnienie: bezpieczeństwa osobowego dotyczącego pracowników i dostawców zewnętrznych, bezpieczeństwa prawnego świadczenia usługi kluczowej, ciągłości działania i odtwarzania usługi kluczowej czy też przeprowadzania szkoleń i ćwiczeń personelu celem przygotowania na różnego rodzaju zagrożenia i incydenty.

Przepisy nowelizowanej ustawy wprowadzają rolę **pełnomocnika bezpieczeństwa usługi kluczowej oraz jego zastępcę,** który wyznaczany jest przez podmiot krytyczny. Jego obowiązki dotyczą efektywnej realizacji zadań związanych z bezpieczeństwem świadczenia usługi kluczowej. Posiada on wiedzę, umiejętności i doświadczenie w zakresie zarządzania bezpieczeństwem, z uwzględnieniem przedmiotu działalności podmiotu świadczącego usługę kluczową. Co ważne, nie był skazany prawomocnym wyrokiem za umyślne przestępstwo lub umyślne przestępstwo skarbowe oraz spełnia wymagania bezpieczeństwa osobowego w zakresie dostępu do informacji niejawnych o klauzuli „poufne". Pełnomocnik bezpieczeństwa usługi kluczowej podlega bezpośrednio organowi zarządzającemu podmiotu krytycznego.

Z kolei operator infrastruktury krytycznej (IK) wyznacza **koordynatora ochrony infrastruktury krytycznej oraz jego zastępcę.** Zgodnie z projektowanymi regulacjami może nim być osoba, która m.in. korzysta z pełni praw publicznych, posiada wiedzę, umiejętności i doświadczenie w zakresie zarządzania bezpieczeństwem, z uwzględnieniem przedmiotu działalności operatora infrastruktury krytycznej, nie była skazana prawomocnym wyrokiem za umyślne przestępstwo lub umyślne przestępstwo skarbowe oraz spełnia wymagania bezpieczeństwa osobowego w zakresie dostępu do informacji niejawnych. Aby skutecznie realizować powierzone obowiązki, koordynator ochrony infrastruktury krytycznej podlega bezpośrednio organowi zarządzającemu operatora IK.

Implementacja dyrektyw NIS2 oraz CER na gruncie prawa krajowego stanowi istotny krok w kierunku wzmocnienia bezpieczeństwa państwa i gospodarki. To istotne zwiększenie odpowiedzialności zarządów podmiotów objętych regulacjami, dla których istotna stała się konieczność integracji systemów zarządzania ryzykiem, unikania silosowego podejścia, jak również budowania kultury bezpieczeństwa w całej organizacji.

Kierownictwo nie może już ograniczać się do roli biernego nadzorcy. Konieczne jest aktywne zaangażowanie w procesy zarządzania ryzykiem, budowanie odporności organizacyjnej oraz zapewnienie zgodności z przepisami. •

Dorota Duda
główny specjalista
Wydział Ochrony Infrastruktury Krytycznej
Rządowe Centrum Bezpieczeństwa

Ilustracje: Marta Kołodziejak / A&S AI Studio

Hikvision

Hikvision Master Workshops 2026 – technologia, której możesz dotknąć

Wiosną 2026 r. Hikvision zaprasza Partnerów i Instalatorów na wyjątkowe wydarzenie edukacyjne – Hikvision Master Workshops. To już trzecia edycja cyklu warsztatów, które łączą wiedzę ekspercką z praktycznym doświadczeniem pracy na realnym sprzęcie. Jest to wydarzenie zaprojektowane z myślą o maksymalnej efektywności nauki. Zamiast klasycznych prezentacji uczestnicy otrzymują dostęp do:

- pracy z najnowszymi urządzeniami i rozwiązaniami AIoT,
- interaktywnych warsztatów prowadzonych przez ekspertów,
- godzinnych sesji szkoleniowych w małych grupach,
- praktycznych scenariuszy wdrożeń.

Kolejny raz Hikvision stawia na hasło: minimum slajdów, maksimum sprzętu, dzięki czemu zdobyta wiedza może być wykorzystana od razu w codziennej pracy. W tym roku program wydarzenia obejmuje trzy główne bloki tematyczne, które odpowiadają kluczowym obszarom nowoczesnych systemów bezpieczeństwa:

1. „Zobacz więcej" – monitoring i AI w praktyce

Nowe kamery i funkcje analityki obrazu, rozwój ochrony perymetrycznej opartej na AI, zastosowanie termowizji w bezpieczeństwie i ppoż.

2. „Kontroluj, dzwoń, rozmawiaj" – kontrola dostępu i komunikacja

Zaawansowane systemy kontroli dostępu, rozwiązania wideodomofonowe nowej generacji, integracja systemów dla zwiększenia świadomości sytuacyjnej.

3. „Projektuj, zarządzaj, łącz" – infrastruktura i zarządzanie

Nowoczesne rozwiązania sieciowe, systemy zasilania awaryjnego, narzędzia do zarządzania i konfiguracji instalacji.

Cykl spotkań odbędzie się w Rzeszowie, Krakowie, Wrocławiu, Łodzi, Gdańsku i Białystoku.

Rejestracja na Hikvision Master Workshops 2026 odbywa się za pośrednictwem aplikacji **Hik-Partner Pro – zakładka Szkolenia** oraz platformy eLearning. Liczba miejsc jest ograniczona, dlatego warto zapisać się z wyprzedzeniem.•

VCS

iTower Observa

iTower Observa to najnowszy model w rodzinie wież do monitoringu marki VCS. Została zaprojektowana w odpowiedzi na potrzeby klientów poszukujących kompaktowych rozwiązań, które nie rezygnują z pełnej funkcjonalności technologicznej. iTower Observa łączy niewielkie rozmiary z zaawansowanymi możliwościami systemowymi. Sprawdzi się w różnorodnych zastosowaniach, m.in. w tymczasowej kontroli prędkości, w zabezpieczeniu peronów, przejść dla pieszych, parków, hal garażowych, czy nielegalnych składowisk odpadów.

Zalety:

- kompaktowa konstrukcja ułatwiająca transport i szybką instalację przez jedną osobę,
- wysokość masztu do 4,4 m,
- stabilność przy podmuchach wiatru do 85 km/h (4 wysuwane podpory),
- gotowy uchwyt pozwalający na szybki montaż popularnych urządzeń, np. kamer PTZ (360°),

- bezpieczeństwo – okablowanie wewnątrz teleskopowej konstrukcji ograniczające ryzyko uszkodzeń w wyniku np. aktów wandalizmu,
- przestronna szafa elektryczna wyposażona w centralę komunikacyjną,
- łatwość przemieszczania wieży – 2 uchwyty do podnoszenia (możliwość transportu przy użyciu wózka widłowego lub paletowego),
- autonomiczność – 2 demontowalne panele słoneczne (2 x 200 Wp), system zasilania awaryjnego (akumulator/UPS), ogniwo paliwowe na metanol.

Portfolio VCS obejmuje szeroką gamę rozwiązań mobilnych, w tym wiele modeli wież o różnej wielkości i różnym przeznaczeniu, począwszy od wież oświetleniowych po wieże do detekcji dronów. •

Genetec rozwija Security Center SaaS o nowe funkcje kontroli dostępu

Genetec ogłosił rozszerzenie funkcji kontroli dostępu w platformie Security Center SaaS. Nowe rozwiązania łączą zarządzanie wizytami i dostępem w jednym systemie oraz pozwalają przenosić istniejącą infrastrukturę do chmury bez jej wymiany.

Zmiany wpisują się w rosnący trend migracji systemów bezpieczeństwa technicznego do modelu SaaS. W wielu organizacjach wciąż działają jednak rozproszone, starsze systemy, które utrudniają zarządzanie dostępem i obsługę gości.

Recepcja jako słaby punkt bezpieczeństwa

W wielu firmach recepcja jest ważnym elementem systemu bezpieczeństwa, ale obsługa gości i kontrola dostępu często działają w oddzielnych systemach. Security Center SaaS łączy te procesy w jednym rozwiązaniu chmurowym.

Recepcja może z jednego miejsca obsługiwać zarówno zaplanowane wizyty, jak i gości bez zapowiedzi, a system automatycznie nadaje odpowiednie uprawnienia dostępu.

Genetec

Platforma umożliwia także weryfikację gości w czasie rzeczywistym, np. w zewnętrznych bazach danych. W przypadku wykrycia ryzyka czy niezgodności system może automatycznie powiadomić ochronę lub uruchomić inne procedury.

Rozwiązanie jest kierowane m.in. do szkół, placówek medycznych i biur, gdzie kluczowe jest połączenie bezpieczeństwa z płynną obsługą gości.

W chmurę bez wymiany sprzętu

Jedną z głównych barier migracji do chmury w obszarze bezpieczeństwa jest konieczność wymiany istniejącej infrastruktury.

Genetec stawia na inne podejście. Dzięki otwartej architekturze i urządzeniom Cloudlink firmy mogą podłączyć obecne systemy kontroli dostępu i alarmy do chmury bez ich wymiany i we własnym tempie.

Platforma obsługuje także coraz szerszy zakres urządzeń. Nowe integracje obejmują systemy alarmowe Radionix (dawniej Bosch) i Honeywell, a wsparcie dla DMP ma pojawić się w czerwcu 2026 r.

Dodatkowo firma zapowiedziała integrację z rozwiązaniem SAFR SCAN, które umożliwia biometryczną identyfikację twarzy. Ma to ograniczyć wykorzystanie fizycznych identyfikatorów, takich jak karty dostępu. •

Nowa seria wzmocnionych kamer PTZ od Hanwha Vision

Zabezpieczenie infrastruktury krytycznej, węzłów komunikacyjnych czy obszarów przemysłowych to wyzwanie, w którym standardowe systemy wizyjne często zawodzą. Zmienne warunki pogodowe, wibracje i skrajne temperatury wymagają sprzętu o bezkompromisowej budowie. Odpowiadając na te potrzeby, Hanwha Vision wprowadza na rynek trzy nowe, wzmocnione modele kamer PTZ (TNP-A6550RW, TNP-A7430RW oraz TNP-A9430RW), w których fizyczna wytrzymałość spotyka się z zaawansowaną analityką opartą na sztucznej inteligencji i autorskim chipsecie Wisenet 9.

Projektowanie systemów dozoru dla trudnych środowisk wymaga uwzględnienia czynników, które mogą trwale uszkodzić elektronikę lub uniemożliwić precyzyjną obserwację. Nowe modele Hanwha Vision zostały zaprojektowane tak, aby gwarantować ciągłość pracy w najtrudniejszych scenariuszach:

- **Skrajne temperatury robocze:** Urządzenia bez problemu funkcjonują w zakresie **od -50°C do +60°C,** co pozwala na ich wdrażanie zarówno w mroźnych strefach klimatycznych, jak i w zakładach o wysokiej emisji ciepła.
- **Odporność na huragany:** Konstrukcja przeszła rygorystyczne testy przy wiatrach o prędkości **do 257 km/h** (odpowiednik huraganu 5. kategorii).
- **Aktywne zapobieganie oblodzeniu:** Wbudowane grzałki mechanizmów obrotowych oraz system odszraniania szyby obiektywu zapewniają pełną mobilność PTZ i czysty obraz podczas mrozów.
- **Stabilizacja w warunkach wibracji:** Zaawansowana optyczna stabilizacja obrazu (OIS) oraz cyfrowa stabilizacja obrazu (DIS) skutecznie niwelują drgania wynikające z silnego wiatru lub ruchu ciężkich pojazdów.
- **Militarne standardy wytrzymałości:** Kamery posiadają certyfikaty IP68 (wodo- i pyłoszczelność), IK10 (odporność na uderzenia) oraz spełniają rygorystyczną normę wojskową MIL-STD-810H, co czyni je odpornymi m.in. na mgłę solną w portach morskich czy piasek w strefach przemysłowych. •

12 czerwca 2026

WARSAW SECURITY SUMMIT

Szczegóły na: **warsawsecuritysummit.online**

a&S POLSKA

Zestaw
wideodomofonowy
BCS-P-VIS01

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

POLSKA MARKA