05 (41) / 2023

CZASOPISMO RYNKU SECURITY

a&S POLSKA

www.aspolska.pl

Raport: Przemysł (w) przyszłości

20 zł
(w tym 8% VAT)

ISSN 2451-5175

Infiltracja, sabotaż, terroryzm

Przemysł musi być na nie gotowy. W walce z przeciwnikiem nie pozostajemy bezsilni, ale broń musimy znać lepiej niż on.

Widzieć nawet w ciemności

Kamery termowizyjne pracują praktycznie w każdych warunkach. Jak w pełni wykorzystać ich możliwości?

Drony i ciemna strona mocy

Czy polskie firmy są przygotowane na atak bezzałogowych statków powietrznych?

Zeskanuj kod
i dowiedz się więcej

Inteligentny elektroniczny dostęp bez klucza 24 godziny na dobę, 7 dni w tygodniu zapewniający bezpieczeństwo i sprawne zarzadzanie.

Unikaj drogiego okablowania dzięki bezprzewodowej technologii zabezpieczającej dowolne przejścia i punkty dostępu.

Wyeliminuj klucze mechaniczne, uprość operacje za pomocą precyzyjnego, zautomatyzowanego przyznawania dostępu pracownikom.

Zwiększ kontrolę dzięki całodobowemu monitorowaniu obiektu przemysłowego w czasie rzeczywistym

Zrównoważ bezpieczeństwo i wygodę, zarządzaj dostępem do wielu jednostek produkcyjnych na jednej, elastycznej platformie.

XS4 Original
Zamek elektroniczny

SALTO Neo Cylinder
Wkładka elektroniczna

Gantner NET.Lock
Zamki szafkowe dla pracowników

SALTO Neoxx Padlock
Kłódka elektroniczna

Pozostańmy w kontakcie @SaltoSystems - www.saltosystems.com

SALTO
inspiredaccess

Przemysł (w) przyszłości

Jak ma się polski przemysł? To zależy. Pesymiści twierdzą, że jest źle. Optymiści mówią, że przecież mogłoby być gorzej. Bez wątpienia rzeczywistość nas wszystkich ostatnio nie rozpieszcza, czasy są po prostu trudne. Prawdziwy ogląd sytuacji, w jakiej znajdują się polskie przedsiębiorstwa produkcyjne, zdecydowanie utrudnia fakt, że media i specjalistyczne serwisy powołują się na różne, czasami sprzeczne dane. W co i komu wierzyć? Pewne światło na to, jak faktycznie jest, rzuca przygotowany przez nas raport pod znamiennym tytułem *Pikuje czy zwyżkuje?* (str. 16).

Pandemia, wojna, inflacja, problemy z dostępem do surowców energetycznych – to tylko niektóre wyzwania, z jakimi zmagają się polskie firmy. Zakłady produkcyjne są na nie jednak szczególnie wrażliwe. Dodajmy do tego nieco niestabilne otoczenie prawne, brak rąk do pracy i zjawisko „cichych odejść", a zyskamy nieco pełniejszy obraz pozwalający na wysnucie wniosku, że prowadzenie biznesu w naszym kraju do łatwych nie należy.

A przecież sytuacja ekonomiczna polskich firm produkcyjnych bezpośrednio przekłada się na branżę security. Jej powodzenie i finansowy sukces wprost zależy od tego, jak będą się miewać odbiorcy oferty. To typowy przykład zestawu naczyń połączonych. Efekt rygla, czyli zjawisko ekonomiczne typowe dla gospodarstw domowych, polegające na tym, że pomimo spadku poziomu dochodu gospodarstwa domowego nie zmniejsza się wielkość jego konsumpcji, firm nie dotyczy. Przedsiębiorcy nie czekają, najpierw tną koszty, najczęściej tzw. ludzkie, ograniczając zatrudnienie, a potem minimalizują inwestycje. Również te w zabezpieczenia. Temu problemowi poświęcony jest ekspercki komentarz do naszego raportu *Mogłoby być lepiej* (str. 22).

Skoro środki na inwestycje w najnowsze zabezpieczenia, takie jak choćby systemy antydronowe (o których piszemy na str. 52 w artykule *Atak dronów)* czy bardziej tradycyjne, np. kamery termowizyjne (przegląd tych urządzeń na str. 58) są raczej mniejsze niż większe, to jak do tematu powinny podejść zarządy lub menedżerowie ds. bezpieczeństwa? Próbę zmierzenia się z tymi pytaniami przedstawiamy w *Głosie branży* (str. 46).

Niezależnie jednak od tego, jak trudne byłoby otoczenie makroekonomiczne, nasi rodacy nie tracą na przedsiębiorczości, o czym mowa w tekście *Nowa Ziemia Obiecana – przemysł w rękach firm rodzinnych* (str. 26). Czytając ten artykuł, nie sposób nie wspomnieć o słynnym fragmencie z Reymontowskiej „Ziemi obiecanej", który brzmi: *Ja nie mam nic, ty nie masz nic, on nie ma nic (…). To razem właśnie mamy tyle, w sam raz tyle, żeby założyć wielką fabrykę.*

Nasi rodacy nie boją się zakładać fabryk. Sęk w tym, że jeszcze muszą je ochronić. Skutecznie. I naszej branży w tym głowa.

Redakcja

ZŁOTY PARTNER A&S POLSKA

AXIS COMMUNICATIONS BCS Linc Polska Sp. z o.o. nedap SCHRACK SECONET smart-i

SREBRNY PARTNER A&S POLSKA

HIKVISION

CZASOPISMO RYNKU SECURITY

a&S POLSKA

05 (41) / 2023

SPIS TREŚCI

Raport: Przemysł (w) przyszłości

REDAKCJA

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

info@aspolska.pl
www.aspolska.pl

PREZES ZARZĄDU
Mariusz Kucharski

REDAKTOR NACZELNA
Marta Dynakowska

Z-CA RED. NACZELNEGO
Jan T. Grusznic

REDAKCJA
Monika Żuber-Mamakis
Adela Prochyra

DZIAŁ REKLAMY
Iwona Krawiec

DZIAŁ PROJEKTÓW SPECJALNYCH
Jolanta A. Kucharska
Aleksandra Czapska

CENTRUM KOMPETENCJI
Jacek Grzechowiak

KOREKTA
Jolanta Kucharska

PROJEKT GRAFICZNY I SKŁAD
Bogusław Kalwala

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

www.sensgroup.pl

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

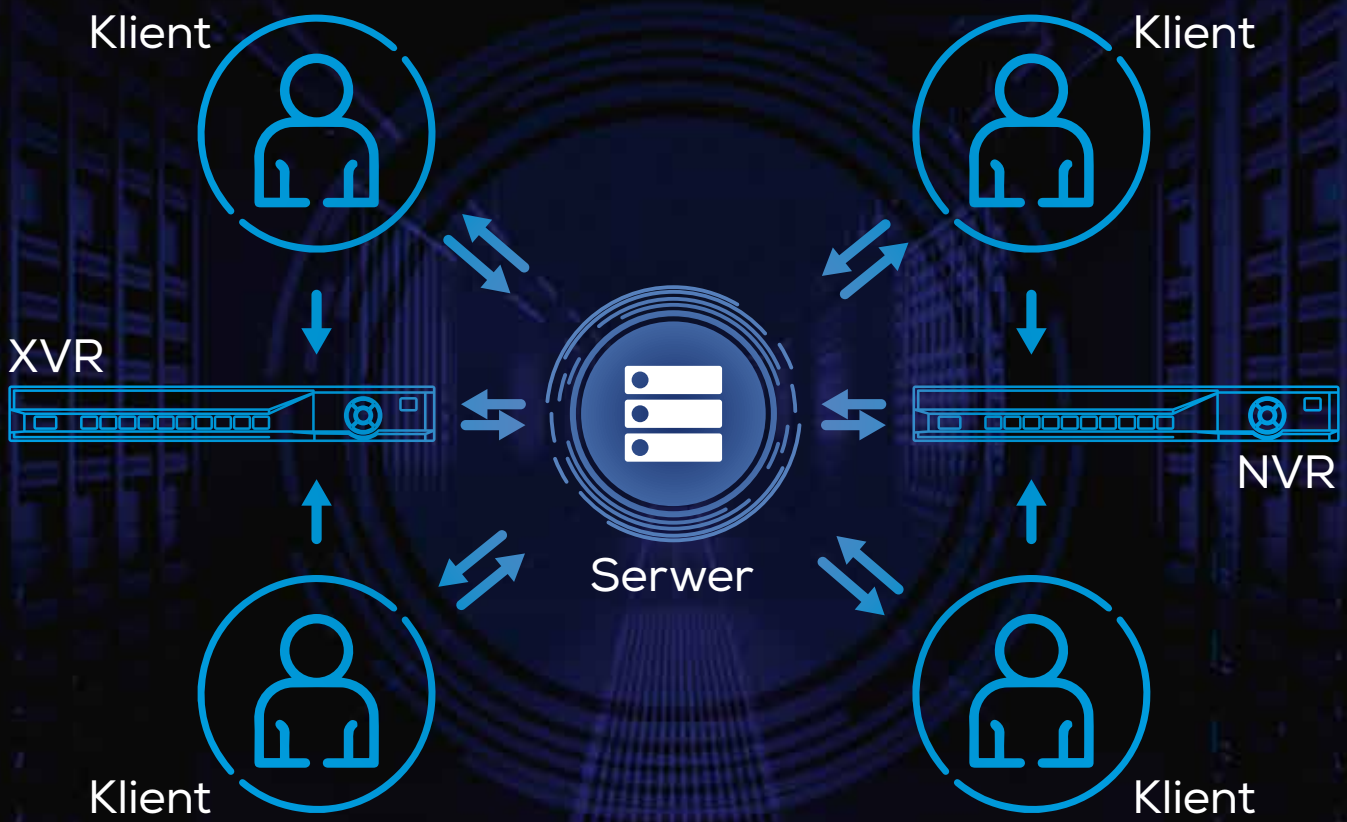
Opinie autorów nie muszą być tożsame z poglądami Redakcji.

Za treść reklam i artykułów partnerów Redakcja nie odpowiada.

Przedruki tekstów bez zgody Wydawcy są niedozwolone.

© Copyright by a&s Polska

Wydajne i wygodne zarządzanie rozproszonymi systemami CCTV



BCS MANAGER SERVER

Zastosowanie aplikacji BCS Manager w wersji klient-serwer do zarządzania rozległymi systemami CCTV wymiernie przekłada się na zmniejszenie kosztów zarządzania obiektami oraz użytkownikami. Przejrzysty system zakupu oprogramowania pozwala na korzystanie ze wszystkich funkcji aplikacji oraz rozbudowę systemu o kolejne urządzenia bez ponoszenia dodatkowych opłat licencyjnych.

» Więcej przeczytasz na stronie 8

POLSKA MARKA BCS

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

BCS®

CZASOPISMO RYNKU SECURITY

a&S POLSKA

05 (41) / 2023

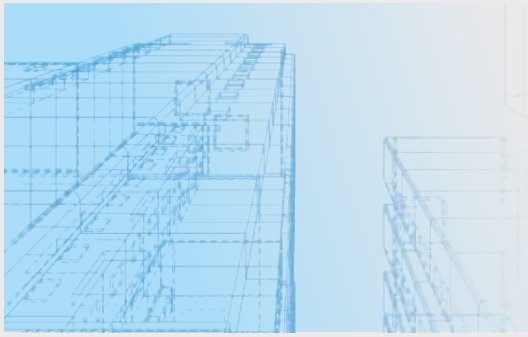
SPIS TREŚCI

RACS 5 v2 Polska platforma kontroli dostępu, bezpieczeństwa i automatyki klasy *Enterprise*

roger
Intelligence for Building

- Obsługa systemów rozproszonych terytorialnie
- Integracja z systemami SSP, SSWiN, CCTV
- Zarządzanie systemami bezpieczeństwa w module VISO SMS
- Integracje z platformami BMS, VMS, SMS, PSIM i aplikacjami do zarządzania biurowcem
- Integracja z usługą Active Directory
- Integracja z serwerowymi systemami windowymi firm KONE, Schindler i innych






Prezentujemy najnowsze urządzenia z oferty firm:

Axis Communications, BCS (NSS), D+H Polska, EVVA, GDE Polska, Hikvision, Linc Polska, Nedap Security Management, Schrack Seconet Polska, TP-Link, ZKTeco

AXIS COMMUNICATIONS

Nowe kamery panoramiczne z wybitną jakością obrazu

AXIS wprowadza na rynek dwie nowe kamery panoramiczne z techniką głębokiego uczenia.

AXIS M4317-PLVE (6 Mpix) oraz AXIS M4318-PLVE (14 Mpix) to doskonale radzące sobie w każdym oświetleniu i dyskretne urządzenia typu mini dome, od razu gotowe do montażu zewnętrznego. Obie kamery mają obiektyw stereograficzny i funkcję Sharpdome 360, która zapewnia wysoką ostrość obrazu na krawędziach, co pozwala na dokładniejszą analizę obrazu. Funkcja dzień/noc oraz wbudowane oświetlenie IR z indywidualnym sterowaniem diodami LED zapewniają wyraźny obraz bez odblasków i znakomitą jakość nawet w słabym oświetleniu lub całkowitej ciemności.

Kamery charakteryzują się fabrycznie wyregulowaną ostrością, a cyfrowa regulacja ustawienia umożliwia zdalne ukierunkowanie na żądany obszar obserwacji. Model AXIS M4318-PLVE oferuje dodatkowo cyfrowe ustawienia PTZ oraz możliwość wybrania widoków: panoramicznego, poczwórnego, narożnego i korytarzowego.

Urządzenia są wyposażone w jednostkę przetwarzania głębokiego uczenia (DLPU), która otwiera nowe możliwości w dziedzinie analityki. Aplikacja AXIS Object Analytics umożliwia detekcję i klasyfikację osób oraz pojazdów w sposób dostosowany do potrzeb klienta. W połączeniu z możliwościami dozoru w zakresie 360° jedna kamera obejmuje obserwacją spory teren, powiadamiając o wykrytych zdarzeniach. Dodatkowo kamery mini dome z układem ARTPEC-8 mają wbudowane zabezpieczenia przed dostępem osób niepowołanych i próbami ataków na system.

Więcej na: www.axis.com/pl-pl

BCS

BCS Manager wersja klient-serwer

Wraz z rozwojem technologii wzrastają wymagania klientów. Wychodząc naprzeciw ich oczekiwaniom, powstała aplikacja BCS Manager w wersji klient-serwer. Taką architekturę systemu wymuszają rozproszone lokalizacje rejestratorów użytkowników.

Za pomocą BCS Manager klient-serwer można uzyskać elastyczne rozwiązanie idealnie dopasowane do rozproszonej struktury dużych organizacji lub obiektów przemysłowych, w których jest wielu operatorów.

Aplikacja skupia w sobie wszystkie standardowe funkcje BCS Managera, a przy tym nie ma ograniczeń w dodawaniu urządzeń i użytkowników do serwera. Zarządzanie systemem można prowadzić z dowolnego miejsca przy użyciu konta z uprawnieniami administratora.

Serwer umożliwia zbieranie sygnałów alarmowych z dowolnych urządzeń podłączonych do systemu (obiektów). Wraz z możliwością konfiguracji obiektów można decydować, jakie alarmy będą przyjmowane, oraz zintegrować BCS Managera z systemem alarmowym obiektu.

Kolejnym udogodnieniem jest możliwość tworzenia zdalnych obchodów, które pozwalają w określony sposób sprawdzić i zapisać stan obiektu, tworząc odpowiednią dokumentację zdjęciową. Wszystkie funkcje aplikacji sprawiają, że BCS Manager idealnie sprawdzi się jako rozwiązanie zarówno do dużych stacji monitorowania z wieloma operatorami, jak i do małych, gdzie jest jedno stanowisko podglądu.

Więcej na: www.bcs.pl

NOVUS MANAGEMENT SYSTEM AC

POLSKI PRODUKT

EFEKTYWNE ZARZĄDZANIE SYSTEMAMI ROZPOSZONYMI

NOWA WERSJA!

NOVUS MANAGEMENT SYSTEM AC V.5

Zbuduj system bezpieczeństwa w oparciu o wiele rozproszonych serwerów. Zarządzaj w sposób scentralizowany z jednego lub wielu centr nadzorczych. Idealne rozwiązanie dla sieci handlowych, bankowych czy obiektów o zasięgu ogólnokrajowym lub globalnym.

JAK TO DZIAŁA?

NMSAC.AAT.PL

NMS AC to profesjonalne polskie oprogramowanie zarządzające systemami bezpieczeństwa w obiektach.

Do nabycia u najlepszych instalatorów!

AAT SYSTEMY BEZPIECZEŃSTWA

PRODUCENT I DOSTAWCA ELEKTRONICZNYCH SYSTEMÓW ZABEZPIECZENIA MIENIA

www.aat.pl

D+H POLSKA

Napęd drzwiowy do zadań specjalnych

Napowietrzanie za pomocą stolarki jest nieodłącznym elementem grawitacyjnych systemów oddymiania. Skrzydła drzwiowe mogą być otwierane automatycznie za pomocą siłownika DDS 54/500. Pozwala on na otwarcie rozwiernych drzwi do kąta 90˚, zapewniając bezpieczną drogę ewakuacyjną i wydajne napowietrzanie.

Napęd DDS 54/500 jest przeznaczony do drzwi jedno- lub dwuskrzydłowych i może być montowany na ościeżnicy lub bezpośrednio nad nią. Minimalna szerokość skrzydła wynosi 400 mm. Napęd jest sterowany za pomocą dedykowanego interfejsu D+H – indywidualnie lub w konfiguracji z innymi elementami systemu. Można go także połączyć z ryglem elektromagnetycznym.

DDS wyróżnia się solidną, kompaktową konstrukcją i możliwością kolorystycznego dopasowania do stolarki drzwiowej. Produkt ma świadectwo dopuszczenia CNBOP oraz Krajowy Certyfikat Stałości Właściwości Użytkowych.

Napęd DDS może być stosowany w obiektach, w których stolarka drzwiowa jest zintegrowana z systemami kontroli dostępu.

Więcej na: www.dhpolska.pl

EVVA

EVVA 4KS – klucz do bezpieczeństwa

EVVA 4KS to rewolucyjny system zamknięć, który łączy w sobie niezrównane bezpieczeństwo z innowacyjną technologią. To idealne rozwiązanie dla tych, którzy cenią sobie spokój i komfort w swoim otoczeniu, gdyż 4KS jest elastyczny, skalowalny i można go w łatwy sposób dostosować do poziomu zabezpieczeń zarówno w firmach, jak i w domu.

System jest rezultatem rozwoju sprawdzonego rozwiązania EVVA bazującego na unikatowej konstrukcji opartej na wyfrezowanych krzywych. 4KS oferuje znakomite możliwości kombinatoryki pozycji zamykających, co jest niezbędne do realizacji złożonych systemów master key, a dzięki wysokiemu poziomowi odporności i wytrzymałości sprawdza się nawet w najtrudniejszych warunkach.

4KS to technologia bezsprężynowa i w odróżnieniu od tradycyjnych systemów zamknięć elementy blokujące we wkładce są przesuwane przez wyfrezowane na kluczu krzywe. Łącznie 12 niesprężynujących, masywnych elementów blokujących jest ustawianych w określonych pozycjach.

Wymuszone sterowanie sześcioma krzywymi na kluczu jest weryfikowane za pomocą dwóch listew bocznych. Dzięki krzyżującym się krzywym manipulacja wkładki jest praktycznie niemożliwa.

Ochrona patentowa oraz zabezpieczenie przed rozwierceniem oznacza osiągnięcie przez 4KS najwyższej klasy bezpieczeństwa wg EN-1303:2015.

Więcej na: www.evva.pl

GDE POLSKA

VKH-1I-VNWT – uniwersalny wideodomofon firmy MAZi

VKH-1I-VNWT to kompletny jednoabonentowy zestaw wideomofonowy składający się ze stacji bramowej pozwalającej na montaż natynkowy, karty Mifare, monitora 7”, switcha z 4 portami PoE i 2 portami uplink, puszki natynkowej oraz karty SD 16GB. Zestaw jest jednym z elementów wideodomofonów MAZi, gdzie dostępne są także wideodomofony modularne oraz dwuprzewodowe.

Zestaw bazuje na technologii IP, pozwala na stosowanie mieszanych połączeń LAN oraz Wi-Fi, jest zasilany ze switcha PoE lub zasilacza 12 V DC. Możliwe jest połączenie stacji bramowej z monitorem za pomocą Wi-Fi – przydatne wtedy, gdy brakuje połączenia przewodowego.

Stacja ma dwa wyjścia przekaźnikowe do sterowanie bramą i furtką, 4 wejścia alarmowe, Wi-Fi, czytnik Mifare, kamerę 2-Mpix. Możliwe jest dodanie kolejnych monitorów i stacji bramowych, a czytnik Mifare pozwala na wygodne otwieranie furtki lub bramy brelokiem lub kartą. System jest kompatybilny z aplikacją smartfonową CTR-MAZi stosowaną w systemach monitoringu MAZi.

Systemy wideodomofonowe MAZi pozwalają na integrację z systemami CCTV, SSWiN oraz KD. Ciekawymi funkcjami są podgląd kamer IP oraz funkcja centralki alarmowej korzystająca z 8 wejść alarmowych w monitorze. Dodatkowym atutem są wyjścia przekaźnikowe w monitorze, których zastosowanie ogranicza tylko inwencja użytkownika. Istnieje możliwość rejestracji obrazu ze stacji bramowej na rejestratorze.

Wyłącznym dystrybutorem firmy MAZi jest GDE Polska.

Więcej na: www.gde.pl

DESIGNA SMART PARKING. ROZWIĄZANIA BEZBILETOWE

Zoptymalizuj jakość parkowania w swoim obiekcie dzięki nowoczesnym rozwiązaniom bezbiletowym DESIGNA.
Dzięki najnowocześniejszej technologii LPR, płynnemu procesowi wyjazdu i wyjazdu oraz zmniejszonemu zużyciu papieru, rozwiązania parkingowe DESIGNA umożliwiają wydajne i wygodne parkowanie dla klientów, jednocześnie upraszczając procedury dla operatorów.

Skontaktuj się już teraz z naszym nowym oddziałem DESIGNA Poland pod adresem info@designa.com, aby poznać inteligentny system zarządzania parkingami.

designa.com

DESIGNA

HIKVISION

Szeroka oferta kamer termowizyjnych

Oferta kamer termowizyjnych firmy Hikvision podzielona jest na dwie grupy: kamery dystrybucyjne oraz kamery projektowe.

Kamery dystrybucyjne są przeznaczone do montażu w różnego rodzaju obiektach - od domów jednorodzinnych po hale magazynowe i fabryki. Przykładem takiej kamery jest model DS-2TD2628-3/QA, który cechuje się wysoką rozdzielczością obiektywu termowizyjnego (256x192 pikseli), szerokim kątem widzenia (50° dla termowizji) oraz stałoogniskowym obiektywem o rozdzielczości 4 Mpix z oświetlaczem podczerwieni do 30 m.

Przykładem kamery projektowej jest model DS-2TD95C8-300ZK-2FL/W, który znakomicie sprawdzi się m.in. w ochronie granic oraz w systemach monitoringu miejskiego. Model ten cechuje się przede wszystkim bardzo wysoką rozdzielczością obiektywu termowizyjnego (aż 1280x1024 pikseli), zmiennoogniskowym obiektywem termowizyjnym z 10-krotnym zoomem optycznym (o kącie widzenia od 28,7° do 2,9°) oraz zmiennoogniskowym obiektywem o rozdzielczości 2 Mpix z 100-krotnym zoomem optycznym oraz z laserowym oświetlaczem podczerwieni o zasięgu aż 3 km. Kamera ta umożliwia również detekcję pożaru już w rozmiarze 1x1 m z odległości ponad 12 km.

W obu przypadkach kamery wyposażono w zaawansowane algorytmy sztucznej inteligencji, które pozwalają na detekcję pożaru, realizację ochrony perymetrycznej (obwodowej) oraz pomiar temperatury w skonfigurowanych punktach, liniach oraz obszarach. Dodatkowe obiektywy światła widzialnego pozwolą na wideoweryfikację alarmów oraz rejestrację szczegółów, co jest niezwykle ważne w przypadku ochrony perymetrycznej oraz detekcji pożarów.

Więcej na: www.hikvision.com/pl

LINC POLSKA

Czytelny obraz z analizą zdarzeń nawet w nocy!

Najnowsze kamery Honeywell serii 35 to odpowiedź na rosnące wymagania rynku. Zapewniają wyjątkowo dobry obraz nawet w warunkach słabego oświetlenia, a zastosowany oświetlacz podczerwieni pozwala na skuteczną obserwację zarówno w dzień, jak i w nocy.

Seria Honeywell 35 obejmuje modele stałe i obrotowe (PTZ) z szeroką gamą obudów i opcji montażu. Kamery są wyposażone w stałe obiektywy i motozoom oraz oferują rozdzielczość od 2 do 8 Mpix. Inteligentna analiza obrazu wspierana AI skutecznie rozróżnia ludzi i pojazdy, ograniczając nieuzasadnione alarmy, co stanowi kolejny atut wymienionych kamer. Dodatkowe funkcje, takie jak WDR 120 dB, redukcja szumów 2D/3D czy smart IR zapewniają wyraźny obraz zarówno w dzień, jak i w nocy.

Seria 35 została tak zaprojektowana, aby umożliwić elastyczną integrację kamer z rozwiązaniami już pracującymi w obiekcie poprzez ONVIF Profile S, G czy T, dzięki czemu jest w stanie sprostać najróżniejszym wymaganiom klientów. Połączenie z innymi systemami umożliwiają też dodatkowe wejścia i wyjścia audio.

Kamery serii 35 firmy Honeywell są w pełni zgodne z NDAA – amerykańską ustawą definiującą politykę bezpieczeństwa USA.

Seria 35 to przystępne cenowo kamery, które idealnie sprawdzą się w małych i średnich obiektach, gdzie stosunek ceny do jakości jest kluczowym aspektem przy wyborze rozwiązania do ochrony.

Więcej na: www.linc.pl

&

NEDAP SECURITY MANAGEMENT

System kontroli dostępu AEOS zintegrowany z bezprzewodowymi zamkami iLOQ

iLOQ to wiodący w branży innowator opatentowanej technologii bezbateryjnych zamków bezprzewodowych. Firma oferuje samodzielnie zasilane zamki oraz rozwiązania przeznaczone do zarządzania mobilnym dostępem za pomocą technologii NFC.

iLOQ oferuje elektroniczne zamki niewymagające używania baterii, co pozwala na zastosowanie tych urządzeń w miejscach, gdzie dostęp do stałego źródła zasilania nie jest możliwy.

Integracja między AEOS i iLOQ pozwala użytkownikom końcowym kontrolować np. klucze mobilne z iLOQ w AEOS. W systemie AEOS można wykonać wszystkie czynności związane z autoryzacją, np. wysyłanie klucza mobilnego, edytowanie praw dostępu, dostosowywanie czasu lub zwracanie kluczy.

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

ECHODYNE

EchoShield®

WIELOZADANIOWY RADAR 3D

Radar średniego zasięgu z wyróżniającymi się parametrami wykrywania, klasyfikacji i śledzenia dronów.

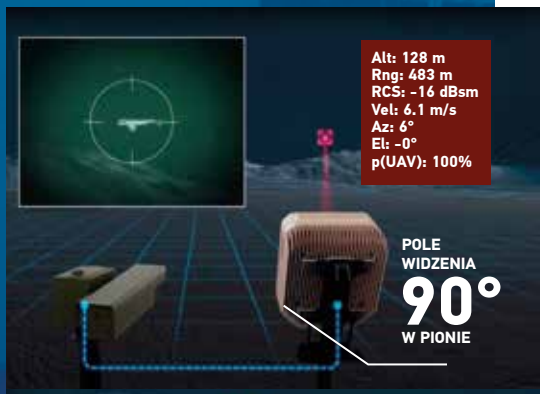
EchoGuard®

RADAR DOZOROWANIA 3D

Lider na rynku krótkiego zasięgu pod względem mobilności i wydajności.

RADARY ECHODYNE W AKCJI

- Pole widzenia 130° azymut x 90° wysokość
- Dokładność śledzenia: < 0.5° azymut x < 0.5° wysokość
- Skuteczność identyfikacji dronów do 100%
- Mikroskanowanie
- Drive & scan
- Identyfikacja i śledzenie do 40 obiektów o wysokim oraz do 1 000 obiektów o niskim priorytecie
- Radary Echodyne używane są już we wszystkich agencjach federalnych USA, jak i w wielu innych obiektach
- Standard MESA® – opatentowana przez Echodyne matryca elektronicznie skanowanych metamateriałów



Linc Polska Sp. z o.o.

Oficjalny partner:

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

SCHRACK SECONET POLSKA

Visocall Mobile – elastyczna komunikacja, mniej stresu

Visocall Mobile jest aplikacją dostępną na telefony typu smartphone. Produkt jest nowoczesnym rozwiązaniem komunikacyjnym pozwalającym na łatwą poprawę jakości procesu opieki każdej placówki medycznej.

Głównym celem tej aplikacji jest ułatwienie pracy wszystkim osobom zaangażowanym w opiekę nad pacjentem. Realizowane jest to poprzez szereg praktycznych funkcji, takich jak:
Powiadomienia push – niezależnie od lokalizacji każdy użytkownik systemu jest informowany o wszystkich zdarzeniach, które wystąpiły w systemie, wraz ze szczegółowym opisem miejsca ich wystąpienia.
Bezpośrednia komunikacja głosowa – personel może odpowiedzieć na odebrane zdarzenie przez połączenie głosowe z osobą, która wygenerowała alarm, lub zdalnie zaakceptować przywołanie, zapalając odpowiednią lampkę nad drzwiami danego pomieszczenia.

Dodatkowo aplikacja umożliwia nawiązania połączenia głosowego z dowolnym urządzeniem w systemie.
Lista pomieszczeń – z opisami i ikoną obecności personelu. Z poziomu tej listy można zmienić priorytet łóżka pacjenta lub nawiązać bezpośrednią komunikację głosową z dowolnym łóżkiem/pomieszczeniem.
Lista przywołań i usterek – w tym alarmów z systemów zintegrowanych, np. z SSP. Ponadto aplikacja ma dedykowaną zakładkę usterek systemu.
Kompatybilność z urządzeniami mobilnymi iOS i Android.

Aplikacja Visocall Mobile jest doskonałym uzupełnieniem systemu Visocall IP.

Więcej na: www.schrack-seconet.com/pl

TP-LINK

TP-Link VIGI C250 – kopułkowa kamera IP, IK10 i IP67

VIGI C250 to kamera sieciowa, która generuje obraz w rozdzielczości 5 Mpix. Wbudowane diody LED zapewniają kolorowy obraz także w całkowitej ciemności. Urządzenie zostało wyposażone w wodoodporną i pyłoszczelną obudowę o stopniu ochrony IP67, dzięki czemu jest odporne na warunki atmosferyczne. Stopień wytrzymałości mechanicznej IK10 chroni kamerę przed aktami wandalizmu, zapewniając nieprzerwany monitoring w dowolnym miejscu.

Funkcja detekcji smart wykrywa osoby oraz pojazdy, ruch, przekroczenie linii, wtargnięcie na obszar, zabrania lub porzucenia obiektu czy sabotaż kamery. Do skorzystania z tej funkcji nie jest wymagany rejestrator VIGI. Urządzenie wykorzystuje kompresję H.265+, co zmniejsza obciążenie sieci i obniża koszty monitoringu bez utraty jakości obrazu.

VIGI C250 może być zasilana za pomocą zasilacza 12 V lub – dla łatwiejszego montażu – również kablem Ethernet (PoE). Kamera o rozdzielczości 5 Mpix występuje w dwóch wariantach: z obiektywem o ogniskowej 4 lub 2,8 mm.

Dzięki aplikacji VIGI na urządzenia przenośne z systemem iOS lub Android kamerami z tej serii można w prosty sposób zarządzać

z poziomu smartfona. Systemem do monitoringu VIGI można też zarządzać z poziomu dedykowanego oprogramowania na komputer oraz rejestrator NVR.

Wszystkie urządzenia z serii TP-Link VIGI są zgodne ze standardem ONVIF, dzięki czemu współpracują z kamerami i rejestratorami różnych producentów i umożliwiają stworzenie kompleksowego systemu monitoringu. Kamera VIGI C250 została objęta 3-letnią gwarancją producenta.

Więcej na: www.tp-link.com/pl

ZKTECO

Terminale SpeedFace-V3L firmy ZKTeco

Firma ZKTeco wprowadziła na rynek kolejną serię terminali kontroli dostępu i rejestracji czasu pracy. Oparte na systemie Linux hybrydowo-biometryczne autonomiczne terminale serii SpeedFace-V3L to rozwiązania integrujące szereg metod uwierzytelniania.

Wszystkie terminale wyposażono w funkcję rozpoznawania twarzy w świetle widzialnym z regulowaną czułością, a każdy z serii w inne dodatkowe czytniki:

- **SpeedFace-V3L w czytnik rozpoznawania twarzy i linii papilarnych,**
- **SpeedFace-V3L [RFID] w czytnik rozpoznawania twarzy i czytnik RFID,**
- **SpeedFace-V3L [QR] w czytnik rozpoznawania twarzy i czytnik kodów QR.**

Seria ta jest również wyposażona w zaawansowany algorytm uodporniający terminale na fałszowanie obrazu podczas rozpoznawania twarzy, w tym przez podstawianie zdjęć czy filmów. Wszystkie terminale są zamknięte w szczelnej, odpornej na kurz i wodę obudowie (IP65) i wyposażone w dotykowy wielofunkcyjny wyświetlacz o przekątnej 2,4". Mają wbudowany serwer internetowy do konfiguracji systemu i pojemną pamięć umożliwiającą przechowywanie 500 wzorców twarzy, 3000 wzorców linii papilarnych, 3000 kart RFID oraz 200 tys. rekordów zdarzeń.

Szereg podstawowych funkcji kontroli dostępu uzupełniono o takie funkcje, jak AntiPassback i Multiple AntiPassback, tworzenie grup i poziomów dostępu, wpisywanie świąt itp. Seria SpeedFace-V3L jest kompatybilna z oprogramowaniem ZKBio Access oraz aplikacją mobilną.

Więcej na: https://zkteco.eu/

POLON-ALFA

dobrze zaprojektowane BEZPIECZEŃSTWO

KOMPLEKSOWE SYSTEMY SYGNALIZACJI POŻAROWEJ

• PRODUKCJA • SERWIS • SZKOLENIA
• WSPARCIE TECHNICZNE I PROJEKTOWE

AUTOMATYKA POŻAROWA

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

Pikuje czy zwyżkuje?

Raport o stanie polskiego przemysłu

Komunikaty na temat przemysłu w naszym kraju są niespójne. W tym samym tygodniu można się dowiedzieć, że sytuacja ekonomiczna jest znakomita, jak też że gospodarkę trawi poważny kryzys. Media i specjalistyczne serwisy powołują się na różne dane, które potwierdzają jedną lub drugą tezę. W co i komu wierzyć oraz jak jest faktycznie w polskim przemyśle? O tym traktuje poniższy raport.

Adela Prochyra

Obraz sytuacji jest o tyle nieostry, że wskaźniki i prognozy, na które powołują się ekonomiści, nieraz nie znajdują odbicia w sytuacji poszczególnych branż, gałęzi przemysłu i firm. Ta bywa nieraz lepsza, niż można się spodziewać przy galopującej inflacji i szybujących cenach energii elektrycznej lub, przeciwnie, gorsza mimo niezłych rokowań ogólnych. Jedną z przyczyn tego rozdźwięku jest fakt, że ekonomia jest nauką społeczną, a nie ścisłą, a prognozy mogą być przydatne w czasach spokojnych, ale zwykle okazują się niewiele warte wobec tak szokowych zdarzeń, jak pandemia czy wybuch wojny. Mówimy o prognozach, nastrojach przedsiębiorców, zagrożeniach i ogólnych trendach. Skąd jednak wiadomo, jak sytuacja polskiego przemysłu wygląda naprawdę? Owszem, inflacja jest wysoka. Na potwierdzenie tego faktu wszyscy odnotowują podwyżkę cen niemal wszystkiego. Ogólna drożyzna dotyczy zarówno indywidualnych konsumentów, jak i przedsiębiorstw, skąd możemy wnioskować, że także one znajdują się w niełatwej sytuacji. Jednocześnie nie słyszy się o upadkach banków, spektakularnych bankructwach firm czy nawet państw, jak, nie szukając daleko, w czasie kryzysu 2008 r. Przyjrzyjmy się więc danym i spróbujmy złożyć obraz polskiego przemysłu w roku 2023.

Ostre hamowanie

Polska gospodarka zwalnia. Po latach prosperity, którego zdawały się nie imać przetaczające się przez kontynent i cały glob procesy ekonomiczne ani polityczne, występuje gwałtowne hamowanie. Przyczyn tego procesu jest kilka, ale najważniejszą z nich okazał się kryzys energetyczny, który uderzył w samo jądro krajowej ekonomii. Przemysł odpowiada za 17% PKB Polski i właściwie bez względu na branżę jest w dużym stopniu uzależniony od cen energii. Te, jak wiadomo, w ciągu ostatnich kilkunastu miesięcy zwiększyły się nawet kilkukrotnie, co nie mogło pozostać bez wpływu na sektor wytwórczy.

Aż 7 na 10 średnich i dużych polskich przedsiębiorstw produkcyjnych badanych w raporcie *ABB Energy Insight Survey 2023* przyznało, że wzrost cen energii ma wpływ na ich działalność. Bez znaczenia okazał się on dla zaledwie 30%. Z raportu wynika także, że z każdego 1000 zł wydawanego na utrzymanie ponad 200 zł firmy przemysłowe przeznaczają obecnie na energię elektryczną. Jak przekłada się to na rynek? Firmy nie tylko mniej sprzedają, ale też, właśnie z powodu wyższych cen energii, obniżają swoją marżę. Tak odpowiedziało 40% przedsiębiorstw biorących udział w badaniu, ale jest to symptomatyczne dla całego polskiego rynku, który od początku tego roku odnotowuje znaczne spadki.

W tegorocznych raportach sygnalnych GUS w kolejnych miesiącach ogłasza obniżki produkcji sprzedanej przemysłu*. W marcu 2023 r.– o 2,9% w stosunku do analogicznego okresu w 2022 r. W kwietniu – o 6,4%, w maju – o 3,2%, w czerwcu – o 1,4%. Dla dopełnienia obrazu dodajmy, że we wszystkich wymienionych okresach w 2022 r. wartości te były o kilkanaście procent wyższe w porównaniu z rokiem 2021. Mówimy więc o spadkach po dość długiej fali wzrostowej. W pierwszym półroczu tego roku produkcja sprzedana przemysłu była o 1,7% niższa w porównaniu z pierwszym półroczem 2022 roku. Wtedy odnotowano wzrost o 13,6% w stosunku do porównywalnego okresu poprzedniego roku. O 0,6% spadło też zatrudnienie w przemyśle w ujęciu rok do roku (do 2 751 000 osób).

Wyniki okazały się niższe od oczekiwań rynkowych oraz prognoz Krajowej Izby Gospodarczej, które zakładały dodatnią dynamikę produkcji w ujęciu rocznym. Ta spadła w 19 spośród 34 działów przemysłu, m.in. w produkcji metali (o 23,8%), produkcji chemikaliów i wyrobów chemicznych (o 20,2%), produkcji wyrobów z drewna, korka, słomy i wikliny (o 15,2%), produkcji wyrobów z pozostałych mineralnych surowców niemetalicznych (o 11,8%), produkcji papieru i wyrobów z papieru (o 11,7%), produkcji mebli (o 8,5%), produkcji komputerów, wyrobów elektronicznych i optycznych (o 8,4%) czy też w wytwarzaniu i zaopatrywaniu w energię elektryczną, gaz, parę wodną i gorącą wodę (o 4,7%). Wzrost w ujęciu rocznym odnotowano z kolei w 13 działach, np. w produkcji urządzeń elektrycznych (o 24,5%), produkcji pojazdów samochodowych, przyczep i naczep (o 15,0%), produkcji maszyn i urządzeń (o 11,1%), w naprawie, konserwacji i instalowaniu maszyn i urządzeń (o 7,3%) czy produkcji artykułów spożywczych (o 3,0%).

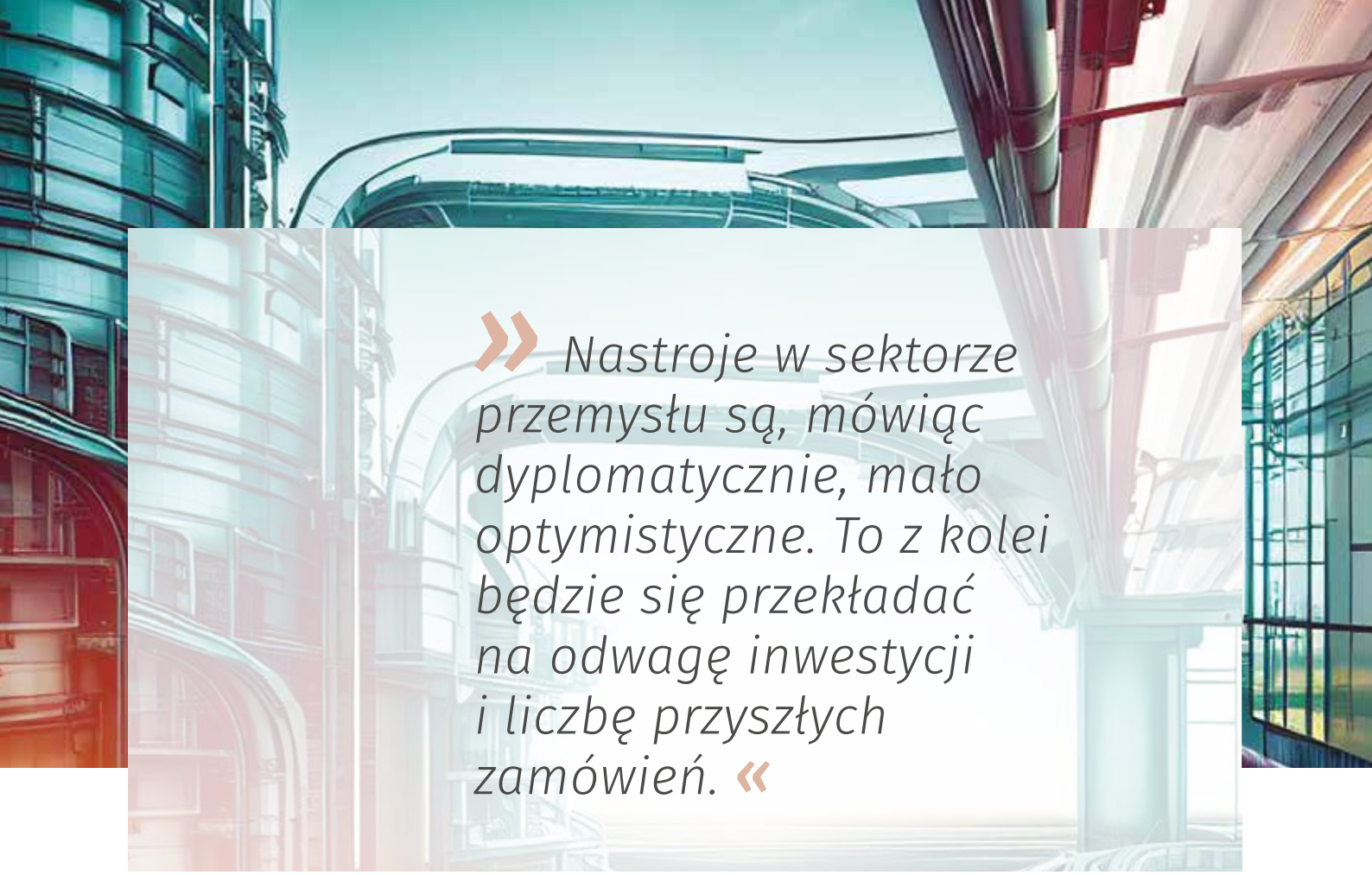
Do kogo płynie prąd?

W sytuacji spadku obrotów i powszechnie obniżanych marż gospodarka traci na konkurencyjności. Z pomocą miał przyjść rządowy program rekompensat pn. „Pomoc dla sektorów energochłonnych związana z nagłymi wzrostami cen gazu ziemnego i energii elektrycznej w 2022 r.", na który wygospodarowano 5 mld zł. Program, jak czytamy na stronie Serwis Rzeczypospolitej Polskiej, powołano w obawie przed całościowym lub pełnym wstrzymaniem produkcji, niedoborami surowców i półproduktów oraz w trosce o bezpieczeństwo pracy tysięcy pracowników zatrudnionych w sektorach energochłonnego przemysłu. Sęk w tym, że ze wsparcia skorzystać mogą przede wszystkim duże i średnie przedsiębiorstwa – takie, które zużywają rocznie ponad 20 TWh energii elektrycznej. Ustawodawca przewidział ten pomost finansowy dla takich branż jak hutnictwo, ceramika, produkcja cementu czy nawozów. Skorzysta z niego ok. 1000 firm. Pozostałe 7116 (łączna liczba przedsiębiorstw w przemyśle w IV kwartale 2022 r. wynosiła 8116 – na podstawie danych GUS) będą musiały polegać na własnej pomysłowości w zarządzaniu. Mówi się o nadchodzącym renesansie tzw. szczupłego zarządzania, które w dużym uproszczeniu opiera się na poprawie efektywności przez wyeliminowanie wszelkiego marnotrawstwa w organizacji. Inne możliwe rozwiązania dla sektora to automatyzacja, cyfryzacja i wykorzystanie szeroko pojętej sztucznej inteligencji. Małe i średnie przedsiębiorstwa mogły także skorzystać z opcji zamrożenia cen prądu na poziomie z 2022 r. – do 785 zł za 1000 kWh. Od 1 października 2023 r. maksymalna stawka za energię elektryczną ma zostać jeszcze obniżona – do 693 zł za 1000 kWh – dla jednostek samorządu terytorialnego, podmiotów wrażliwych i MŚP.

Wskaźnik wskaźnikowi nierówny

Jeśli wziąć pod uwagę poszczególne wskaźniki, np. liczbę rozpoczętych inwestycji w przemyśle, może się okazać, że sytuacja rysuje się wręcz optymistycznie. W roku 2022 była ona porównywalna z latami 2018–19, które były jednymi z najlepszych od dekady (patrz: tabela 1).

* Produkcja sprzedana przemysłu to wartość wyrażona w bieżących cenach bazowych, tj. bez podatku od towarów i usług (VAT), podatku akcyzowego, a łącznie z wartością otrzymanych dotacji przedmiotowych, tj. dotacji do produktów (wyrobów i usług). Źródło: stat.gov.pl (dostęp: 4.08.2023)



> *Nastroje w sektorze przemysłu są, mówiąc dyplomatycznie, mało optymistyczne. To z kolei będzie się przekładać na odwagę inwestycji i liczbę przyszłych zamówień.*

TABELA 1. Inwestycje rozpoczęte – przemysł

2018	Q1-Q2	91 393
	Q1-Q3	14 0430
	Q1-Q4	18 5872
2019	Q1-Q2	98 105
	Q1-Q3	152 431
	Q1-Q4	212 434
2020	Q1-Q2	109 392
	Q1-Q3	157 194
	Q1-Q4	218 925
2021	Q1-Q2	117 419
	Q1-Q3	188 363
	Q1-Q4	256 482
2022	Q1-Q2	90 907
	Q1-Q3	137 584
	Q1-Q4	185 680

Źródło: Główny Urząd Statystyczny, *Biuletyn Statystyczny* nr 3/2023 (data publikacji: 26.04.2023)

Gdy przyjrzeć się wynikom finansowym w przemyśle, także trudno o powody do paniki. Przychody netto z roku na rok sukcesywnie się zwiększają, podobnie zysk netto i wyniki finansowe netto. Wiele branż i firm faktycznie ma się stosunkowo nieźle, podczas gdy różne wskaźniki ekonomiczne zniżkują. Paradoks polega na tym, że w generalnie złej sytuacji poszczególne podmioty mogą prosperować zupełnie dobrze, i na odwrót. Nie dziwi to, biorąc pod uwagę dużą złożoność sytuacji. Przykładowo – w czasie rozwoju gospodarczego rozkwit przeżywają takie branże jak budownictwo. Duży popyt nie idzie jednak w parze z brakiem pracowników i gwałtownym wzrostem cen materiałów. W praktyce wiele firm budowlanych musi wywiązać się ze sztywnych zapisów w kontraktach, dotrzymując terminów i operując w ramach budżetu, który z dnia na dzień okazuje się dalece niewystarczający.

Właśnie dlatego pojedyncze wskaźniki są niemiarodajne, ponieważ pokazują jedynie wybrane, wąskie fragmenty rzeczywistości. Pełniejszy obraz daje kompilacja wielu danych, czyli wskaźnik koniunktury gospodarczej, który mówi, czy klimat koniunktury jest dobry (wskaźnik powyżej zera), czy zły (wskaźnik poniżej zera). Jest to wskaźnik złożony, który odzwierciedla stan gospodarki, obliczany jako średnia arytmetyczna sald odpowiedzi na pytania z ankiety miesięcznej dotyczące bieżącej i przewidywanej sytuacji gospodarczej przedsiębiorstwa. Od początku 2022 r. generalny wskaźnik koniunktury dla przemysłu jest na minusie i są to wartości dwucyfrowe (patrz: tabela 2). Nie broni się hipoteza o wciąż nieodrobionych pandemicznych latach. Po gwałtownym tąpnięciu w kwietniu 2020 r. (-46,7) wskaźnik powoli zbliżał się do zera, osiągając wartość nawet -2,9. Od półtora roku jest znacznie obniżony i waha się od -18,4 do -10,8. Właściwie nie ma znaczenia, który aspekt weźmiemy pod uwagę – od miesięcy na kilkunastoprocentowym minusie jest zarówno wskaźnik ogólnego klimatu koniunktury, jak i diagnoza ogólnej sytuacji gospodarczej, diagnoza produkcji i prognoza produkcji.

Wskaźnik ten jest jednocześnie opisem bieżącej sytuacji i swego rodzaju prognostykiem. Z jego niskich wartości wynika m.in. to, że nastroje w sektorze przemysłu są, mówiąc dyplomatycznie, mało optymistyczne. To z kolei będzie się przekładać na odwagę inwestycji i liczbę przyszłych zamówień.

Sprawozdanie niefinansowe

Dodatkowym wymogiem, który powoli staje się rzeczywistością większych polskich firm, jest raportowanie ESG *(Environmental, Social and Corporate Governance)*. 5 stycznia 2023 r. weszła w życie unijna dyrektywa *Corporate Sustainability Reporting Directive,* zgodnie z którą firmy w całej Unii Europejskiej, w tym w Polsce – w pierwszej kolejności największe spółki giełdowe, w dalszej kolejności też duże spółki, czyli zatrudniające ponad 250 osób lub/i posiadających 40 mln euro obrotu lub/i posiadających ogółem 20 mln euro aktywów – zobowiązane są raportować swoje działania w zakresie zrównoważonego rozwoju. Od roku 2027 obowiązkiem raportowania z zakresu ESG zostaną też objęte małe i średnie przedsiębiorstwa zatrudniające więcej niż 10 pracowników. Wówczas będą musiały złożyć raport niefinansowy za 2026 r. Dla wielu firm, zwłaszcza mniejszych, obowiązek raportowania będzie skokiem na głęboką wodę, ponieważ będzie oznaczał konieczność zebrania dużej ilości danych. Do tego może okazać się niezbędne zatrudnienie osoby, która będzie mieć nad tym pieczę, lub wynajęcie zewnętrznego eksperta.

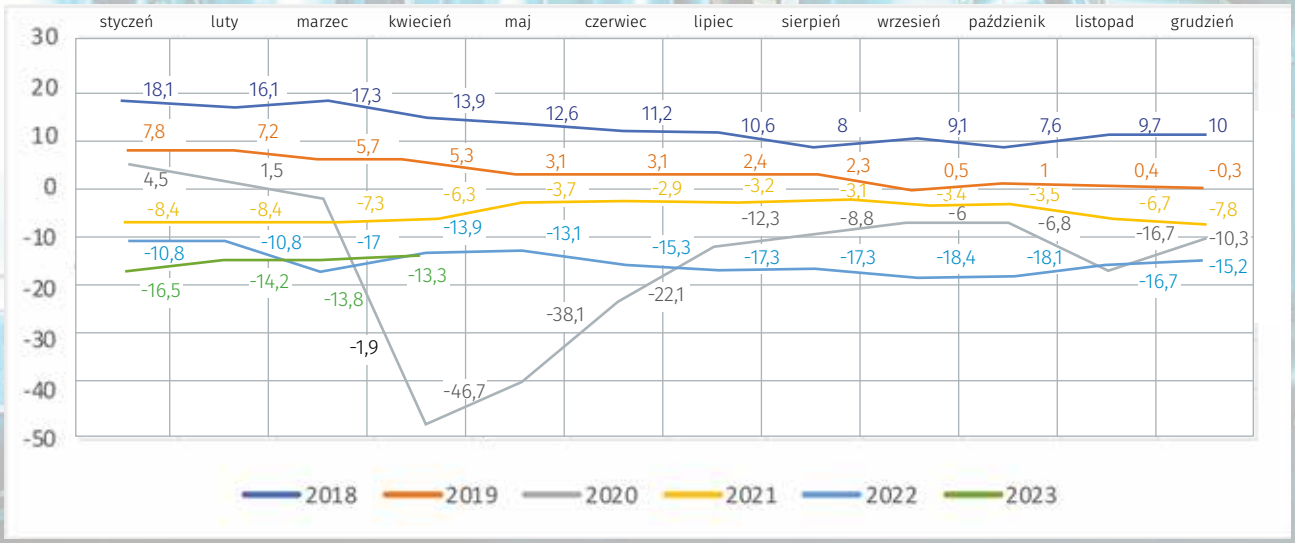
Rewolucja polega na tym, że – w przeciwieństwie do chociażby pokrewnego CSR – dane zawarte w raporcie mają być mierzalne. Sposób raportowania kwestii zrównoważonego rozwoju zostanie wystandaryzowany, a więc będzie można zweryfikować firmy pod tym względem i porównać je, co dotąd było niemożliwe wobec braku jednorodnych wytycznych co do sporządzania sprawozdań niefinansowych. W raporcie ESG będzie aż 1200 wskaźników, w tym 300 obligatoryjnych dla wszystkich podmiotów objętych nowym obowiązkiem. Będą to m.in. informacje o emisji bezpośredniej i pośredniej (wynikającej z zakupu energii) gazów cieplarnianych, łańcuchu dostaw, transporcie, inwestycjach, utylizacji odpadów. Firmy, tworząc taki raport, będą więc musiały ujawnić cały łańcuch swoich powiązań z innymi firmami i podmiotami.

Będzie to miało różnorakie konsekwencje, niektóre nieoczywiste, jak chociażby trudniej dostępne kredyty na inwestycje zakładające wykorzystanie np. nieodnawialnych źródeł energii. Już dziś kwestie ESG wpływają na wycenę spółek na polskim rynku, choć na razie, jak przyznają inwestorzy, są to zwykle zagadnienia drugorzędne. W przyszłości instytucje finansowe będą musiały uwzględniać pozafinansowe szanse i ryzyka w swoich procesach inwestycyjnych i finansowych. To celowe działanie Unii Europejskiej, która poprzez regulacje prawne i rynkowe chce doprowadzić do transformacji gospodarek i firm. Dyrektywa SFDR (UE) 2019/2088, która weszła w życie 10 marca br., zobowiązuje inwestorów finansowych do uwzględniania aspektów związanych ze środowiskiem i społeczeństwem oraz z zarządzaniem (ESG) w ocenie ryzyka oraz włączenia kwestii ESG do swoich strategii inwestycyjnych.

Nie tylko inwestorzy, lecz również klienci będą śledzić, w jaki sposób przedsiębiorstwa uwzględniają kwestie związane z klimatem, ochroną środowiska, społeczną odpowiedzialnością oraz sprawiedliwymi standardami zarządzania korporacyjnego w swoich celach strategicznych i operacyjnych. Firmy, które nie dostosują się do tych wymagań i nie będą w stanie udokumentować tych działań w obszarach ESG, obniżą swoje perspektywy na zdobycie kapitału w perspektywie długoterminowej oraz będą narażone na obniżoną wycenę, a także na trudności w utrzymaniu relacji z partnerami w ramach łańcucha dostaw. ●

TABELA 2. Wskaźniki koniunktury gospodarczej wyrównane sezonowo – przetwórstwo przemysłowe

	styczeń	luty	marzec	kwiecień	maj	czerwiec	lipiec	sierpień	wrzesień	październik	listopad	grudzień
2018	18,1	16,1	17,3	13,9	12,6	11,2	10,6	8	9,1	7,6	9,7	10
2019	7,8	7,2	5,7	5,3	3,1	3,1	2,4	2,3	0,5	1	0,4	-0,3
2020	4,5	1,5	-1,9	-46,7	-38,1	-22,1	-12,3	-8,8	-6	-6,8	-16,7	-10,3
2021	-8,4	-8,4	-7,3	-6,3	-3,7	-2,9	-3,2	-3,1	-3,4	-3,5	-6,7	-7,8
2022	-10,8	-10,8	-17	-13,9	-13,1	-15,3	-17,3	-17,3	-18,4	-18,1	-16,7	-15,2
2023	-16,5	-14,2	-13,8	-13,3								



Źródło: Główny Urząd Statystyczny, *Biuletyn Statystyczny* nr 3/2023 (data publikacji: 26.04.2023)

Mogłoby być lepiej

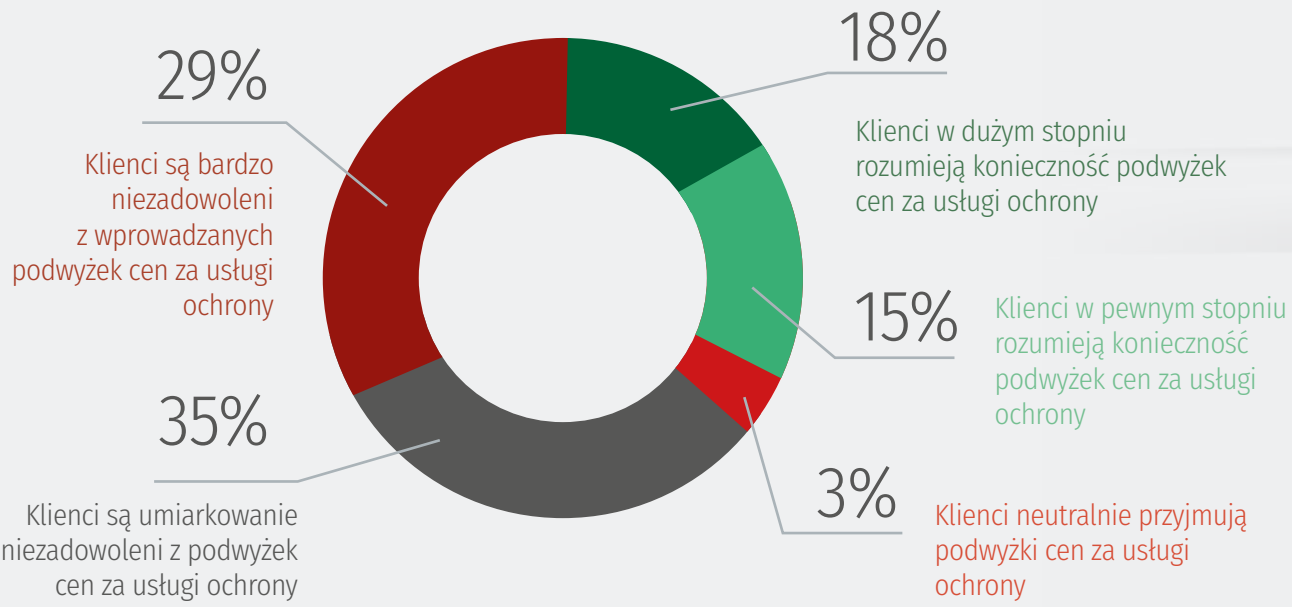
Analiza najnowszego raportu *Branża bezpieczeństwa w Polsce. Szanse, zagrożenia, kierunki rozwoju* przygotowanego przez PZP Ochrona może sugerować, że branża ochrony jest w nie najlepszej kondycji. W ten sposób ocenia ją aż 83% respondentów. A przecież widocznie zauważalny jest wzrost obrotów firm zajmujących się profesjonalnymi usługami security, które stan swoich finansów oceniają pozytywnie.

Jan T. Grusznic

Firmy z branży security chętnie zatrudniają, choć menedżerowie skarżą się na trudności z pozyskaniem wykwalifikowanych pracowników. Dostawcy elektronicznych systemów zabezpieczeń pałają większym optymizmem. Zerwane łańcuchy dostaw i wynikające z nich problemy z realizacją zamówień w większości mają już za sobą. Wzrost płacy minimalnej może przełożyć się na większe inwestycje klientów w zabezpieczenia techniczne, co dla branży może stanowić okazję do wzrostu. Nic zatem dziwnego, że przedstawiciele producentów intensywnie zabiegają o zwiększenie swojego udziału w rynku. Muszą jednak pamiętać, że coraz częściej na decyzje zakupowe klientów wpływ ma nie tylko ostateczna cena, ale także aspekt ekologiczny związany z konkretnym rozwiązaniem, TCO *(Total Cost of Ownership)* oraz cyberbezpieczeństwo. To ostatnie wynika z bliskiego wejścia w życie dyrektywy NIS2.

Mimo tych stosunkowo dobrych wiadomości nie da się ukryć, że branża ochrony odczuwa pewne trudności: zawirowania związane z pandemią i konfliktem za naszą wschodnią granicą, do tego wysoka inflacja (14,4% w 2022 r. i 10,1% w sierpniu 2023 r.) oraz utrzymujące się niskie bezrobocie (3% w 2022 r. i 5% w czerwcu 2023 r.) znacząco wpłynęły na działania firm security. Konieczność podniesienia cen za usługi wynikająca ze wzrostu płacy minimalnej nie najlepiej wpłynęła na nastroje klientów. Trzeba jednak pamiętać, że był to krok nieunikniony. Wynagrodzenia pracowników to nadal ok. 80% wszystkich kosztów sektora usług, co zawsze przekłada się na znaczące podwyżki cen usług (ostatnio o ok. 20% r/r). Ponadto spadająca dynamika produkcji sprzedanej przemysłu (w okresie styczeń–lipiec br. produkcja sprzedana przemysłu była wg GUS o 1,9% niższa w porównaniu z analogicznym okresem 2022 r.) i utrzymujący

Czy podwyżki cen za usługi ochrony, związane z zaplanowaniem na 2023 rok wysokich podwyżek strawek minimalnego wynagrodzenia za pracę, mają dostrzegalny wpływ na nastroje państwa klientów?



Źródło: Raport 2022-2023 *Branża bezpieczeństwa w Polsce. Szanse, zagrożenia, kierunki rozwoju*, PZP Ochrona (https://pzpochrona.pl/)

się ujemny wskaźnik koniunktury gospodarczej spowodowały spadek zamówień oraz zamrożenie inwestycji. Brak akceptacji dużych podwyżek cen usług zmusił przedstawicieli firm branży ochrony do elastycznego podejścia z jednej strony do potrzeb klientów, z drugiej – ich finansowej możliwości. Zwiększyła się zatem liczba rozwiązań technicznych wspierających lub zastępujących ochronę fizyczną. W kolejnych latach wzrośnie rola monitoringu wizyjnego przy jednoczesnym zwiększaniu nakładów na rozwiązania techniczne i ograniczaniu roli ochrony fizycznej stałej. Niewątpliwie wpłyną na to kolejne zmiany w prawie. Do uzgodnień międzyresortowych i konsultacji publicznych trafił właśnie projekt rozporządzenia Rady Ministrów w sprawie wysokości minimalnego wynagrodzenia za pracę oraz wysokości minimalnej stawki godzinowej w 2024 r., zwiększający je o 19,4% r/r.

Software as a Service zyska na znaczeniu

Mniejsze budżety na bezpieczeństwo ograniczają możliwość użycia najnowszych osiągnięć technicznych, zmuszając firmy do wykorzystania posiadanych zasobów. W sukurs przychodzą im rozwiązania chmurowe opłacane w modelu *Software as a Service* (SaaS). Oferują one niższy koszt początkowy, mniejszy koszt wdrożenia i przewidywalność wydatków bieżących w zamian za szeroki wachlarz funkcjonalności, począwszy od usług analizy obrazu, przez rozproszone systemy kontroli dostępu, skończywszy na zintegrowanych platformach zarządzających bezpieczeństwem oraz usługach monitoringu w chmurze. Coraz większa dostępność usług SaaS powoduje, że stają się one atrakcyjną alternatywą dla rozwiązań on premises (oprogramowanie jest instalowane lokalnie na urządzeniach klienta).
Liczba wdrożeń typu SaaS jest jednak niewielka. Branża wciąż nie darzy zaufaniem tych rozwiązań, ponieważ przetwarzanie danych powierzonych przez podmiot zewnętrzny odbywa się na maszynach dostawcy usługi. Nadal pokutuje przeświadczenie, że nad systemami lokalnie instalowanymi łatwiej o nadzór. Warto mieć na względzie to, że elektroniczne systemy zabezpieczeń wdrażane są z innymi priorytetami niż jest to w świecie SaaS, gdzie obowiązują poufność, zachowanie integralności danych, a dopiero potem ich dostępność. Elektroniczne systemy zabezpieczeń, aby działać skutecznie, wymagają najpierw możliwości kontroli w czasie rzeczywistym i funkcjonalności, dostępności, integralności, a dopiero na końcu pojawia się konieczność zachowania poufności. Przy czym części składowe systemów ochrony nie zawsze uwzględniają podstawowe wymagania z zakresu bezpieczeństwa IT, w zamian oferują osiągnięcie celów funkcjonalnych. Jednak rosnąca dostępność rozwiązań typu SaaS oraz atrakcyjny model finansowania dobrze rokują na przyszłość.

W cieniu NIS2

Problem ochrony elektronicznych systemów zabezpieczeń jest znamienny. Rozwiązania te kontrolują i monitorują procesy przemysłowe, infrastrukturę krytyczną i inne urządzenia fizyczne. Niekiedy mają kluczowe znaczenie dla prawidłowego funkcjonowania różnych branż, takich jak produkcja, wytwarzanie energii czy transport. Tymczasem wiele z nich nadal pracuje na starszym sprzęcie, wykorzystując oprogramowanie, które nie zostało zaprojektowane z myślą o zaawansowanym cyberbezpieczeństwie. Stosowane są w nich niewystarczające, z obecnej perspektywy, mechanizmy uwierzytelniania i taka kontrola dostępu, która może dać nieautoryzowanym użytkownikom uzyskanie wglądu do danych wrażliwych. Nagminne stosowanie protokołów komunikacyjnych pozbawionych szyfrowania czyni je podatnymi na podsłuchiwanie i manipulowanie danymi. Brak aktualizacji tworzy luki w zabezpieczeniach, które atakujący mogą wykorzystać. Jednocześnie rosnąca konwergencja rozwiązań IT z elektronicznymi systemami zabezpieczeń może wprowadzać nowe podatności, ponieważ luki w jednej sieci mogą być potencjalnie użyte do naruszenia bezpieczeństwa drugiej.
W 2016 r. Unia Europejska wydała Dyrektywę NIS w celu zwalczania wszechobecnych i wyrafinowanych cyberataków na infrastrukturę krytyczną (IK). Dyrektywa ta miała na celu nakłonienie państw do opracowania krajowych oraz transgranicznych norm i przepisów dotyczących cyberbezpieczeństwa. Zgodnie z nią operatorzy usług kluczowych (m.in. banki, podmioty świadczące opiekę zdrowotną, dostawcy wody pitnej i energii) oraz dostawcy usług cyfrowych (w tym usług w chmurze i e-commerce) są zobowiązani do poprawy swojego bezpieczeństwa cyfrowego i zgłaszania incydentów cybernetycznych.
W 2020 r. Komisja Europejska dokonała nowelizacji dyrektywy. NIS2 wejdzie w życie w 2024 r., nakładając rygorystyczne wymagania dotyczące cyberbezpieczeństwa na większą liczbę podmiotów. Dyrektywa NIS2 ma istotne znaczenie dla branży ochrony, ponieważ wpływa także na podwykonawców i usługodawców mających dostęp do IK. Na przykład w sektorze energetycznym środki ostrożności nie będą dotyczyć wyłącznie dostawców surowców, producentów i dystrybutorów energii elektrycznej, ale wszystkich podwykonawców, co oznacza także firmy z branży ochrony fizycznej. To zaś może stanowić kolejny powód do zmartwień dla branży, która już teraz ma niełatwo. ●

fot: shutterstock (3)

Przemysł 5.0?

Ledwo branża produkcyjna oswoiła się z pojęciem 4. rewolucji przemysłowej, a tymczasem zaczęły powstawać wizje kolejnego etapu zmian nazywane przemysłem 5.0.

Damian Kwiek

W 2017 roku tego terminu użył Esben H. Østergaard, CEO w REInvest Robotics. Dwa lata później o p5.0 mówił Aroop Zutshi, prezes Frost & Sullivan. Natomiast w 2021 roku powstała pierwsza kompleksowa wizja 5. rewolucji przemysłowej w postaci raportu Komisji Europejskiej pt. *Industry 5.0*. W dokumencie podano, że produkcja oznaczona numerem 5 będzie miała trzy filary:

- zorientowanie na człowieka *(human-centric)*,
- zrównoważony rozwój *(sustainable)*,
- odporność *(resilient)*.

Autorzy raportu, definiując nowe pojęcie, tłumaczą, że podejście zorientowane na człowieka oznacza usytuowanie ludzkich potrzeb i interesów w sercu procesu produkcji. *Zamiast pytać, co możemy zrobić dla technologii, pytamy, co technologia może zrobić dla nas* – piszą Maija Breque, Lars De Nul i Athanasios Petridis. W odniesieniu do rozwoju filaru zrównoważonego rozwoju eksperci powtarzają znane założenia dotyczące gospodarki obiegu zamkniętego, ekologii, zielonej energii, realizowania potrzeb ludzi bez narażania na szwank tych samych potrzeb przyszłych generacji oraz podkreślają potencjał SI w optymalizowaniu zużycia dóbr. W kwestii odporności dokument nawiązuje do zmian geopolitycznych, kryzysów w rodzaju pandemii COVID-19 i wyzwań wynikających z delikatności zglobalizowanej produkcji.

Przemysł 5.0 liczy na SI

W branżowych publikacjach próbujących definiować przemysł 5.0 jako oś nowego terminu pojawia się też np. podniesienie na wyższy poziom komunikacji ludzi z maszynami *(Tweeting Factory)*. O tym i o doskonalszej optymalizacji produkcji przy użyciu AI pisał dr Maciej Zięba z DSR. Z kolei zdaniem Artura Komolki z Sumitomo Bordnetze, p5.0 będzie związany z bardziej zaawansowaną analityką korzystającą z machine learningu, (znów) sztucznej inteligencji oraz z nowymi systemami i blockchainem. Również dr Zbigniew Piątek w serwisie AutomatykaB2B argumentował, że przemysł 5.0 można próbować ewentualnie łączyć z potencjałem SI i pogłębieniem interakcji między ludźmi a maszynami z użyciem machine learningu. Wspólnym mianownikiem wszystkich tych dywagacji są więc nadzieje dotyczące skokowego rozwoju AI wpływającego zarówno na analizę danych, jak i komunikację pracowników i urządzeń (we wszystkich konfiguracjach).

Trzy dokumenty unijne i Industry 5.0 Award

Wracając do działań unijnych, Komisja Europejska prowadzi konkurs The Industry 5.0 Award. 1 kwietnia zakończyła przyjmowanie zgłoszeń, a zwycięzcy zostali ogłoszeni podczas Research & Innovation Days w czerwcu 2022 r. Projekty dotyczyły rozwiązań z zakresu trzech filarów p5.0 zdefiniowanych we wspomnianym wyżej raporcie KE. Warunkiem było też to, aby przedsięwzięcia były finansowane z programów Horyzont 2020, Horyzont Europa lub Europejskiego Instytutu Innowacji i Technologii. Cezura czasowa wyznaczona przez organizatorów to start inicjatywy po 1 września 2018 r. Osadzenie konkursu w ten sposób, w finansowaniu unijnym jeszcze sprzed 2020 r., dowodzi, że idea przemysłu 5.0 była opracowywana wcześniej i świadomie zakotwiczana w innych obszarach (nie tylko teoretycznych dokumentach). Zresztą we wrześniu 2020 r. Komisja Europejska opublikowała dokument autorstwa Juliana Müllera zatytułowany *Enabling Technologies for Industry 5.0. Results of a workshop with Europe's technology leaders*. Opracowanie zawiera wczesną propozycję koncepcji p5.0, opisuje technologie istotne dla tego etapu oraz wskazuje społeczne, rządowe, polityczne i ekonomiczne wyzwania. Z kolei po raporcie *Industry 5.0* ze stycznia 2021 r. KE opublikowała równo rok później jeszcze studium *Industry 5.0, a transformative vision for Europe. Governing Systemic Transformations towards a Sustainable Industry*. Dokument opracowany przez 15 specjalistów pod przewodnictwem Sandrine Dixson-Decleve jest krokiem pomiędzy kompleksową definicją z Industry 5.0 a opracowaniem planu działania dla realizacji tej koncepcji.

Rewolucja czy upgrade?

Główną wartością działania Komisji Europejskiej w tym obszarze jest fakt wypracowania pierwszej kompleksowej koncepcji przemysłu 5.0. Inne znane mi wypowiedzi na ten temat były albo skrótowymi wtrąceniami rozważającymi, czym mógłby on być, albo opracowaniami, które jednak nie aspirowały do pełnego zdefiniowania pojęcia. Wizja 5. rewolucji przemysłowej stanowiła też temat dyskusji panelowych i roboczych. Zatem tutaj „rząd" Unii Europejskiej, również z racji instytucjonalnego charakteru pozwalającego wpływać na rzeczywistość, wykonuje ważny ruch. Docenić też należy apel, aby przemysł przyszłości nie stawiał na pierwszym miejscu zysku, efektywności, konkurencyjności gospodarki z dopasowaną do tego celu rolą pracownika, ale aby podstawową wartością stało się dobro człowieka *(human-centric).* Inne istotne cele mają być podporządkowane ludzkiemu *wellbeing* (trochę nieszczęśliwie tłumaczonemu w Polsce jako „dobrostan").

Kłopot w tym, że każdy z trzech filarów tak ujętego przemysłu 5.0 jest generalnie obecny od dekady w przemyśle 4.0. Akcentowanie roli człowieka, zadbanie o sytuację pracownika to jedna z podstawowych narracji 4. rewolucji przemysłowej. „Organizacja skupiona na człowieku" stanowi piąty obszar transformacji w ramach ADvanced MAnufacturing. Zrównoważony rozwój z kolei autorzy metodyki wyraźnie zaznaczyli w trzecim obszarze, czyli „Ekologicznej fabryce". I ostatni z filarów Industry 5.0, czyli odporność. Ślady myślenia w podobnych kategoriach można odnaleźć w prawie każdym obszarze Admy, bo cała koncepcja p4.0 zasadza się na konkurencyjności firm w szybko zmieniających się warunkach rynkowych i dostosowywaniu produkcji do równie szybko ewoluujących potrzeb klientów. Dodatkowo w orbicie przemysłu 4.0 funkcjonuje strategiczna koncepcja zarządzania VUCA zakładająca, że cechami współczesności, które należy traktować jako zwyczajny element krajobrazu, są: zmienność, niepewność, złożoność i niejednoznaczność.

Redefinicja przemysłu 4.0

Interesująco koncepcję przemysłu 5.0 komentuje serwis I-scoop założony przez J.P. De Clercka. W artykule Industry 5.0 – the essence and reasons why it gets more attention czytamy: Przemysłu 5.0 nie należy łączyć z kolejną rewolucją przemysłową, to byłoby całkowicie błędne. Dalej autor przypomina, że np. w Stanach Zjednoczonych zamiast p4.0 często używa się terminu IIoT w rozumieniu przemysłowego Internetu, z kolei w Japonii występuje pojęcie społeczeństwa 5.0. Dodam, że w nauce funkcjonuje koncepcja dzieląca „nasz" przemysł 1.0 na dwie rewolucje, w czego konsekwencji uznawany szeroko przemysł 4.0 u Carloty Perez jest p5.0. I z powrotem w tekście na I-scoop mamy obserwację: *Wszystko jest względne, a rewolucje przemysłowe dzisiaj są kwestią wizji. Innymi słowy przemysł 4.0 bywa odbierany jako coś, powiedzmy, „chłodnego". I stąd chęć nadania mu bardziej „ludzkiego" oblicza.*

Choć teza, że p4.0 skupia się przede wszystkim na technologiach, jest tylko dość popularnym mitem. W rzeczywistości sensem 4. rewolucji przemysłowej są zmiany daleko głębsze niż technologiczne, czyli obejmujące doskonalenie organizacji, wprowadzanie nowych modeli biznesowych i dbające o mądre usytuowanie w tym wszystkim pracownika. Niemniej trzeba koncepcji Komisji Europejskiej oddać, że świeże jest zaproponowanie, aby to od pozycji i dobra człowieka rozpoczynało się myślenie o zmianie. W przemyśle 4.0, tak jak go rozumiem, pracownik raczej miał w naturalny sposób skorzystać na tym, że firma będzie lepiej zorganizowana i w ogóle przetrwa, „uciekając do przodu", dzięki poprawie konkurencyjności. Propozycja zawarta w dokumencie *Industry 5.0* jest cenna z wielu powodów, jednak to nie rewolucja, a raczej nowe spojrzenie na przemysł 4.0. ●

Artykuł ukazał się pierwotnie na portalu Platforma Przemysłu Przyszłości: https://przemyslprzyszlosci.gov.pl/

Nowa Ziemia Obiecana
– przemysł w rękach firm rodzinnych

W latach 80. XX wieku Polaków nazywano współczesnymi Fenicjanami. Wynikało to z niezwykłej energii naszych rodaków handlujących dosłownie wszystkim i wszędzie – od Budapesztu, bazarów Stambułu, przez Berlin Zachodni i Wiedeń, po Hongkong i Tajlandię. Z wielu tych pionierskich i często zuchwałych wypraw wyrosły dzisiejsze firmy rodzinne. Tak jak część znaczących dziś firm produkcyjnych, szczególnie w branżach okiennej i meblowej, zaczynało w przydomowych warsztatach rzemieślniczych.

Jacek Tyburek

Według danych GUS-u na koniec lipca 2023 r. w Polsce było zarejestrowanych ponad 4,5 mln podmiotów gospodarczych, w tym 830 tys. firm rodzinnych. Z kolei z zestawienia 100 największych (pod względem kapitału) polskich firm prywatnych około 40 stanowią przedsiębiorstwa produkcyjne lub zajmujące się produkcją własnych wyrobów i ich sprzedażą. Podążając za tą myślą, 22 firmy produkcyjne z tego zestawienia to firmy klasycznie rodzinne, często nadal pozostające w rękach założycieli. Warto zaznaczyć, że w zdecydowanej większości są to firmy ambitne, z szeroko i strategicznie zarysowanymi planami. W ostatnim czasie polski biznes rodzinny potrafił doskonale wykorzystać inflację. Zdecydowana większość, bo aż 88% jego przedstawicieli, którzy wzięli udział w badaniu PwC, pochwaliła się zwiększeniem przychodów ze sprzedaży w 2022 r., przy czym 68% osiągnęło aż dwucyfrowy wzrost – wynika z polskiej edycji globalnego Badania Firm Rodzinnych *Family Business Survey 2023*. Dane te pokazują, jak dobrze polskie firmy rodzinne opanowały zdolność radzenia sobie z kryzysem.

– *Pandemia COVID-19, zakłócenia w łańcuchach dostaw, wojna w Ukrainie czy wysoka inflacja pokazały, w jak trudnym, zmiennym i wymagającym otoczeniu funkcjonujemy, a nasze badanie wskazuje, że firmy rodzinne bardzo często radzą sobie z wyzwaniami lepiej niż pozostałe segmenty gospodarki* – zaznacza

» W kilku branżach polskie produkcyjne firmy rodzinne stanowią znaczącą siłę na rynkach międzynarodowych. Wyróżniają się szczególnie wytwórcy stolarki okiennej i drzwiowej, mebli, jachtów, kosmetyków czy wózków dziecięcych. «

Krzysztof Sieczkowski, partner PwC Polska, lider Praktyki Polskich Firm Prywatnych. Rodzinne biznesy nad Wisłą radziły sobie w zeszłym roku nawet lepiej niż w 2021 r. Wtedy o wzroście sprzedaży mówiło 70%, a o spadku co dziesiąty z polskich uczestników badania.

Prymusi, najwięksi producenci i prawdziwi liderzy swoich branż

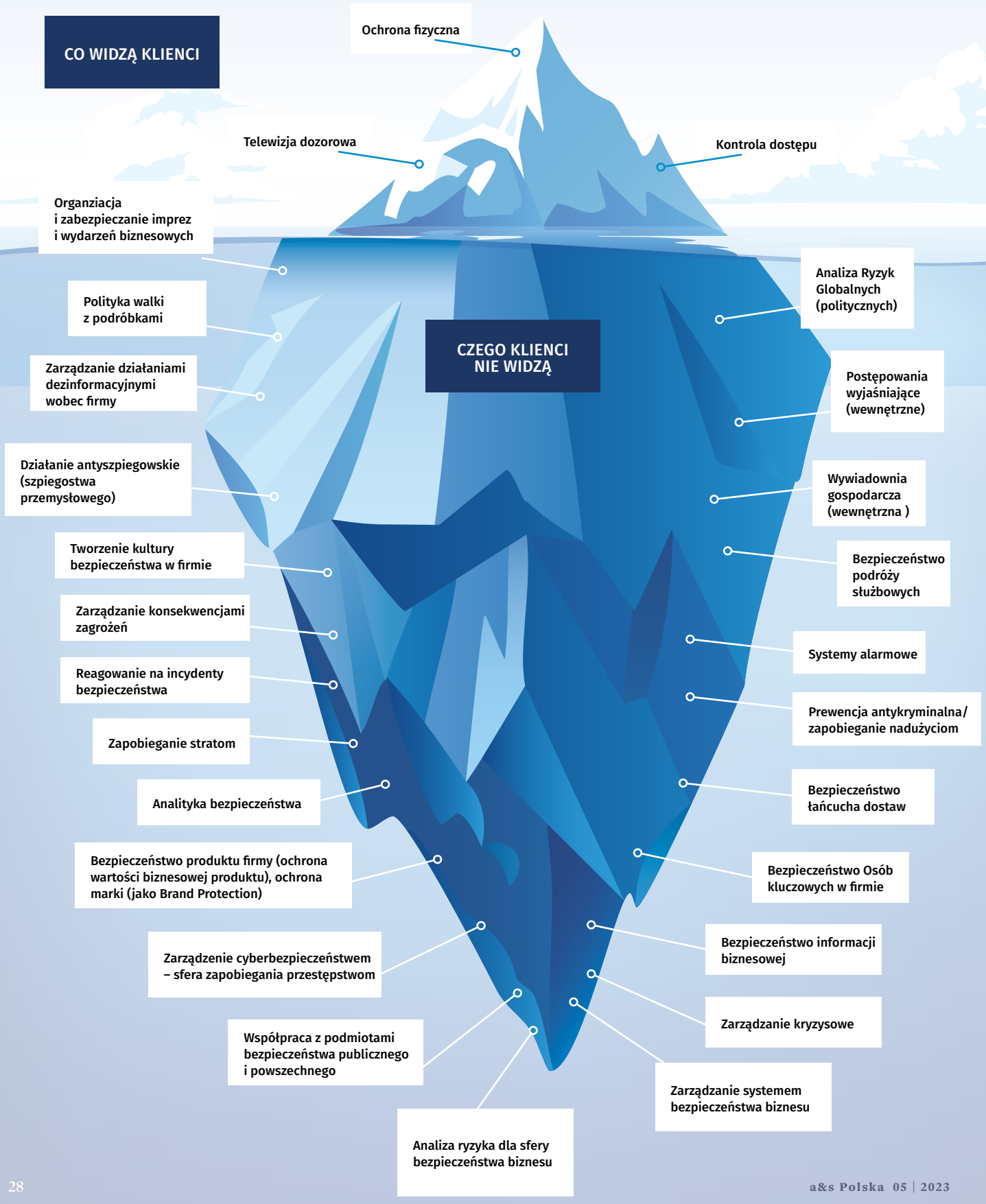
W kilku branżach polskie produkcyjne firmy rodzinne stanowią znaczącą siłę na rynkach międzynarodowych. Wyróżniają się szczególnie wytwórcy stolarki okiennej i drzwiowej (w tym również okien i systemów okiennych z przeznaczeniem dla okrętów), mebli, jachtów, kosmetyków czy wózków dziecięcych. Należy wymienić firmy takie jak Drutex, Fakro, Oknoplast, Eko okna, Dako, Bohamet w branży okien, Kler, Grupa Nowy Styl czy Malow w branży meblowej. Polscy producenci jachtów to Delphia Yachts oraz Balt Yacht, a przemysł kosmetyczny reprezentują Ziaja, Dr Irena Eris, Bielenda, Inglot. Nie można nie wspomnieć również o niewątpliwym sukcesie firmy Solaris, która została założona przez Krzysztofa i Solange Olszewskich. W podpoznańskim Bolechowie powstała najpierw montownia autobusów Neoplan, a potem na tej bazie powstawały autobusy Solaris, które obecne są w wielu miastach na całym świecie. Solaris dziś już nie jest firmą polską ani rodzinną, ale jako taka powstała i rozwinęła się do poziomu dostawcy rozpoznawalnego i dostarczającego wysokiej jakości autobusy i trolejbusy do co najmniej kilku krajów.

Celowo koncentrujemy się na dużych firmach rodzinnych wchodzących bez kompleksów na rynki międzynarodowe. Ich brawurowy rozwój wymagał bowiem pogłębionej analizy ryzyka oraz bezpiecznej ekspansji, by grać w tej samej lidze co konkurencja międzynarodowa, nierzadko mocno już ugruntowana.

Krzysztof Domarecki, przewodniczący Rady Nadzorczej Selena FM SA, która zaczynała w 1992 r. od dwóch rodzinnych spółek w Polsce, a dziś grupa działa w 17 krajach na czterech kontynentach i jest w pierwszej trójce największych światowych producentów piany poliuretanowej, wskazuje na kilka kluczowych czynników powodzenia ekspansji. Jeden z podstawowych to dostęp do wiarygodnej informacji oraz ochrona własnych zasobów informacyjnych. Informacja musi być w znacznym stopniu profilowana. Nadmiarowe i sprzeczne często dane stanowią poważny problem w wyborze. Kluczową kompetencją jest więc ich selekcja i dobór tych, które są istotne z punktu widzenia prowadzonego biznesu. Po 20 latach międzynarodowej ekspansji Seleny K. Domarecki podkreśla, że z punktu widzenia firm rodzinnych przed podjęciem decyzji o wyjściu za granicę ogromne znaczenie ma analiza relacji między skalą swoich obecnych zasobów a możliwościami

GÓRA LODOWA CORPORATE SECURITY KARSTENA

Nie można się oprzeć wrażeniu, że poniższy graf autorstwa Karstena Griesshammera, Senior Directora, Head of Global Security&Protection w BioNtech SE, doskonale oddaje postrzeganie bezpieczeństwa biznesu w wielu przedsiębiorstwach, w tym także w firmach rodzinnych.



skutecznego działania po ekspansji. Ta spowoduje bowiem wzrost złożoności organizacyjnej prowadzenia biznesu. A to może stanowić wyzwanie dla pewnego i bezpiecznego rozwoju. Analiza jest podstawą, żeby się zorientować, jak daleko można się posunąć w planach podbijania kolejnych rynków.

Przekładając to na rzeczywistość zarządzania bezpieczeństwem w firmach rodzinnych, nie sposób odnieść wrażenia, że zarządzanie bezpieczeństwem to dziedzina, której potrzeba jest dopiero uświadamiana. Specjaliści czy menedżerowie lub działy bezpieczeństwa występują najczęściej w rodzinnych firmach branży retail i handlu. Zarządzanie bezpieczeństwem niejako wymuszone poprzez standard TAPA występuje w tych firmach, które tenże standard posiadają.

Zapóźnienie szansą, brzmi jak u Orwella...

Polskie produkcyjne przedsiębiorstwa rodzinne z oczywistych względów nie miały kontynuacji w PRL-u na skalę, na jaką zasługiwały. Toteż ich historia jest znacznie krótsza niż ich zagranicznych konkurentów. Wynika z tego jednak poważny benefit! Według opinii Jana Kolańskiego, prezesa zarządu firmy rodzinnej Colian Holding SA, znanego na świecie producenta słodyczy, przypraw, bakalii i napojów, właściciela takich marek jak Grześki, Jutrzenka czy Hellena, który eksportuje swoje produkty do ponad 60 krajów, wyrasta on z handicapu, jakim była sytuacja „późnego startu".

Kraje zachodniej Europy inwestowały w rozwój przemysłu przez kilkadziesiąt lat. Dziś te inwestycje są już przestarzałe. Są jeszcze funkcjonujące czteropiętrowe fabryki, gdzie towar wozi się windami, a logistyka jest bardzo droga… My, Polacy, nie mieliśmy nic i budowaliśmy wszystko od zera. Z pomocą Unii Europejskiej postawiliśmy nowe zakłady, w których działa bardzo nowoczesny park maszynowy, a przy tym nadal możemy konkurować ceną siły roboczej.

Wymienione wcześniej firmy z TOP 100 największych polskich firm rodzinnych to czołówka, najwięksi z największych. Opowieść o polskim sektorze firm rodzinnych to historia fascynująca, ale też nie pozbawiona wstrząsów i konfliktów.

Sukcesja, ekspansja, konflikt, cybergroza

Słowem kluczowym jest tutaj sukcesja. I nie chodzi oczywiście o jeden z najlepszych seriali w ostatnich latach, ale o zmianę pokoleniową na szczytach władzy firm rodzinnych. Łatwo obliczyć, że ich założyciele, szczególnie dużych przedsiębiorstw produkcyjnych, którzy startowali w latach 80. ubiegłego stulecia, to obecnie ludzie w zaawansowanym wieku. Rzadko przechodzą na emeryturę, gdyż wciąż prowadzą swój biznes.

Niestety, czasami dochodzi do konfliktów przeradzających się w głębokie rodzinne wojny. Można tu przywołać choćby głośną sprawę sprzed kilku lat. Założyciel producenta okien Drutex, Leszek Gierszewski, oskarżył członków rodziny o nielegalną próbę przejęcia firmy. Ci z kolei zarzucają mu działanie na szkodę przedsiębiorstwa. W obronie firmy przed wrogim przejęciem pomogła Gierszewskiemu znana firma detektywistyczno-ochronna należąca do medialnego detektywa. Doszło tu do ostrej walki o władzę nad spółką, która jest gigantem w skali europejskiej na rynku producentów okien. Ogromny biznes, ogromne emocje i bezpardonowa walka o władzę w firmie.

To jedna z najbardziej dramatycznych sytuacji, która obrazuje, jak istotne w fazie przekazywania zarządzania nad dużym przedsiębiorstwem produkcyjnym są bezpieczeństwo, spójność i odporność (lepiej oddawane przez określenie z języka angielskiego *resilience*). Do tego dochodzi odważne wchodzenie na rynki zagraniczne i pozbawiona kompleksów walka o mocną na nich pozycję.

Premia za digitalizację

Z polskiej edycji globalnego badania Firm Rodzinnych *Family Business Survey 2023* przeprowadzonego przez PwC wynika, że tylko 35% respondentów jest zdania, że ich organizacja ma solidne kompetencje cyfrowe. Jest to wynik poniżej średniej globalnej, która wynosi 42%. Aż 65% firm twierdzi, że ma dostęp do wiarygodnych i aktualnych informacji/danych, które są wykorzystywane w procesie podejmowania decyzji (w porównaniu z 64% na świecie).

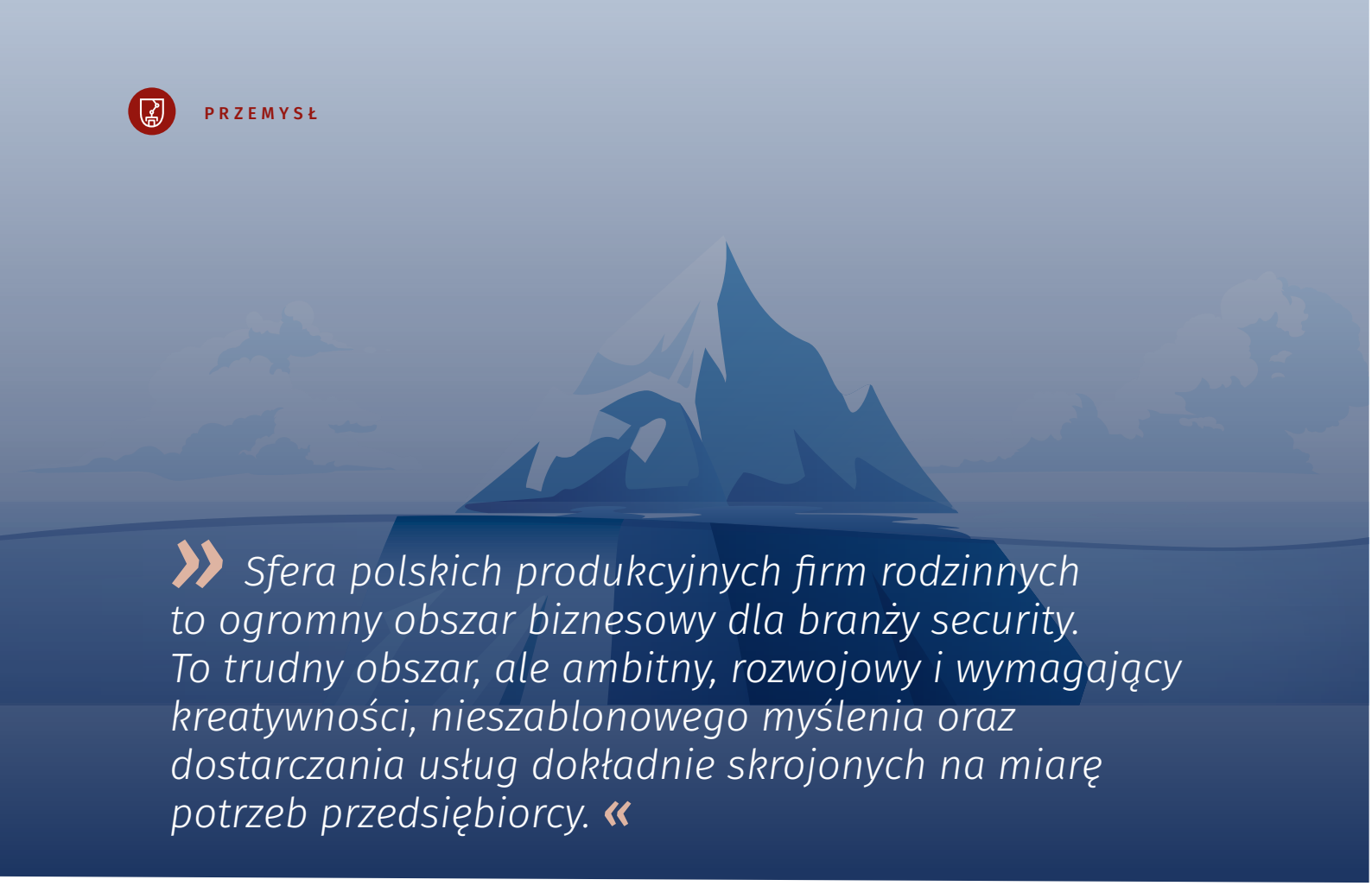
> *» 35% respondentów jest zdania, że ich organizacja ma solidne kompetencje cyfrowe. Jest to wynik poniżej średniej globalnej, która wynosi 42% «*

To bardzo istotna informacja dla branży security, bo jest niemal pewne, że firmy rodzinne są na etapie cyfryzacji i muszą korzystać z wiarygodnych danych zewnętrznych oraz zdobyć umiejętność ich selekcjonowania. Nie zapominajmy przy tym, że przedsiębiorstwa rodzinne, w związku z rozwojem ich parku maszynowego, generują również dane związane z procesem produkcji, a następnie także te pochodzące z systemów bezpieczeństwa i z łańcucha dostaw. Na styku IT, bezpieczeństwa i utrzymania ruchu oraz zarządzania logistyką w formule Control Tower wytwarza się ogromną ilość *big data*. Dane te powinny być w pełni wykorzystywane do analizy w procesie rozwoju biznesu, ale przede wszystkim muszą być odpowiednio chronione.

W miarę jak coraz więcej firm rodzinnych przenosi swoje działania związane z zarządzaniem do świata cyfrowego, obawy dotyczące bezpieczeństwa stają się bardziej powszechne. W jaki sposób organizacje mogą analizować swój stan bezpieczeństwa, opracowywać ramy kontroli i łączyć działania proaktywne i reaktywne potrzebne do skutecznego zarządzania bezpieczeństwem? Wszystko przy zachowaniu kontroli nad budżetem i dalszym prowadzeniu działalności biznesowej.

Wdrażanie zabezpieczeń i ochrony wiąże się z wieloma wyzwaniami. Po pierwsze, większość firm rodzinnych ma często bardzo mały zespół odpowiedzialny za technologie informacyjne i zazwyczaj nie posiada dużej wiedzy na temat bezpieczeństwa wewnętrznego. Po drugie, scentralizowany system informatyczny wśród zarządu, akcjonariusza i wszystkich powiązań rodzinny to rzadkość.

→



» Sfera polskich produkcyjnych firm rodzinnych to ogromny obszar biznesowy dla branży security. To trudny obszar, ale ambitny, rozwojowy i wymagający kreatywności, nieszablonowego myślenia oraz dostarczania usług dokładnie skrojonych na miarę potrzeb przedsiębiorcy. «

Wielu członków rodziny będzie używać osobistych adresów e-mail i własnych urządzeń, a utrzymanie centralnej strategii bezpieczeństwa i technologii jest trudne, jeśli nie niemożliwe.

Chmura już zostanie, a jej wykorzystanie w życiu osobistym stopniowo przekształciło się w życie biznesowe, zwłaszcza gdy ludzie znajdują się w sytuacjach kryzysowych i nieoczekiwanie muszą korzystać z technologii jak nigdy dotąd. Nie mając czasu na opracowanie odpowiednich korporacyjnych zasad i strategii bezpieczeństwa, wiele osób po prostu korzysta z osobistych wiadomości e-mail i popularnych rozwiązań do przechowywania danych w chmurze, aby udostępniać członkom rodziny poufną komunikację firmową. To zjawisko szczególnie powszechne w firmach rodzinnych, gdzie wielu członków rodziny faktycznie nie pracuje bezpośrednio dla firmy. W tym scenariuszu zwykle stosuje się raczej reaktywne, oparte na incydentach, niż proaktywne, planowane podejście do bezpieczeństwa.

Praktyczne wskazówki dotyczące ustalania priorytetów i organizacji bezpieczeństwa obejmują cztery kluczowe obszary: politykę, odpowiedzialność, ryzyko i edukację.

W tym kontekście należy jasno zdefiniować strategie i przełożyć je na politykę. Polityka oznacza ustalenie szczegółów podstawowych działań dla organizacji i jej interesariuszy oraz zadawanie odpowiednich pytań. Środki bezpieczeństwa powinny mieć charakter praktyczny, zaczynając od uzasadnienia biznesowego polegającego na upewnieniu się, że dane pozostają w zasięgu osób, które powinny mieć do nich dostęp.

Odpowiedzialność to upewnienie się, że jest ktoś odpowiedzialny za kierowanie działaniami w zakresie bezpieczeństwa, zarządzanie zespołem ds. bezpieczeństwa i pełnienie funkcji bezpieczeństwa. Bezpieczeństwo jest celem stale się zmieniającym i ugrzęźnięcie w definiowaniu celów w perspektywie krótkoterminowej może prowadzić do niezauważenia tego, co się zmienia. Jednakże po utworzeniu zespołu i uruchomieniu ogólnych procesów funkcjonalnych bezpieczeństwa cele długoterminowe mogą odegrać większą rolę.

Przydatne jest utworzenie, prowadzenie i regularne przeglądanie rejestru ryzyka, który powinien być opracowywany we współpracy z zainteresowanymi stronami i przy ustalaniu priorytetów działań związanych z bezpieczeństwem uwzględniać wpływ, prawdopodobieństwo i ramy czasowe.

Edukacja opiera się na fakcie, że bezpieczeństwo jest tak mocne, jak najsłabsze ogniwo. Plan edukacyjny niekoniecznie musi być formalnym programem szkoleniowym, ale może obejmować otwartą dyskusję, ćwiczenia symulacyjne lub zasady wdrażania i opuszczania firmy, mające na celu uwzględnienie uważności wśród pracowników i członków rodziny. Edukację można rozpocząć od pracowników zatrudnionych na wrażliwych stanowiskach i kontynuować, upewniając się, że wszyscy są świadomi swoich ról i obowiązków oraz środków stosowanych w celu ochrony i zabezpieczania informacji firmy. Tylko w ten sposób organizacja jako całość może być silna.

Firmy rodzinne z ambicjami graczy globalnych stoją przed nie lada wyzwaniem. Z jednej strony to organizacje bardzo elastyczne, z ośrodkiem decyzyjnym niezwykle blisko zadania i dostępu do budżetu oraz decyzji. Z drugiej – żeby grać w podobnej lidze co najwięksi, muszą, a co najmniej powinny stosować wiele zasad wypracowanych przez korporacje. Nie można jednak nie dostrzegać, że stoją też przed niepowtarzalną szasną skoku w przyszłość,

jaki dla wielkich organizacji będzie bolesny, długotrwały i nie wiadomo czy nie zabójczy. Dla organizacji rodzinnych AI może być ogromną szansą korzystania z zasobów, o których jeszcze kilka lat temu nie mogły nawet marzyć. Właściciel, założyciel lub jego sukcesor z wizją ma szansę dokonać rozwoju, o jakim nikomu się nie śniło.

Bezpieczeństwo i odporność poprzez ludzi i technologie również w tej podróży może i powinno być kluczem do sukcesu.

Poszukaj Złotego Graala Security

Niestety, praktyka podpowiada, że firmy rodzinne oprócz ogromnej liczby zalet mają też często ograniczenia i tzw. hamulcowych. Ze względu na to, że jest to dzieło życia i źródło ekonomicznej i statusowej potęgi rodzin, dość często z nowymi ideami i rozwiązaniami trzeba się przebić przez mur nieufności, konserwatyzmu oraz sieci podskórnych gier i zależności oplatających przedsiębiorstwa rodzinne. Nie jest to specyfika tylko polska. To mechanizm psychologiczny występujący na całym świecie. Z tą tylko różnicą, że wielkie międzynarodowe brandy produkcyjne, których nazwy już nie przywodzą na myśl nazwisk ich założycieli, ale nimi de facto są (plejada np. niemieckiego, amerykańskiego i japońskiego przemysłu samochodowego) mają już ten etap za sobą.

Znam sytuacje, gdy produkcyjne firmy rodzinne w wyniku zmian na rynkach i w obliczu konieczności przebranżowienia stanęły przed ogromnym wyzwaniem. Produkt niby ten sam, ale odbiorca inny, bo instytucjonalny i wymagający. Bez udokumentowanych certyfikatów z zakresu bezpieczeństwa informacji czy cyberbezpieczeństwa przedsiębiorstwo staje przed murem nie do przebycia. Otrzymuje więc jednoznaczny komunikat: nie jesteś bezpieczny w rozumieniu bezpieczeństwa informacji, cyberbezpieczeństwa, zarządzania incydentami, panowania nad spójnością infrastruktury zakładów produkcyjnych i łańcuchów dostaw, nie pracujemy z tobą.

Reasumując, sfera polskich produkcyjnych firm rodzinnych to ogromny obszar biznesowy dla branży security. To trudny obszar, ale ambitny, rozwojowy i wymagający kreatywności, nieszablonowego myślenia oraz dostarczania usług dokładnie skrojonych na miarę potrzeb przedsiębiorcy. I to zarówno tych z widocznej części góry lodowej Karstena Griesshammera, jak i całej podwodnej części. Tego właśnie potrzebuje klient pod nazwą: polskie firmy rodzinne z branży przemysłowej. Dostawca, który z takim Złotym Graalem Security skutecznie pojawi się na rynku, wykona mnóstwo pożytecznej pracy dla gospodarki narodowej, a także zapewni dobrych i wiernych klientów sobie i swojej organizacji. ●

Jacek Tyburek

Menedżer bezpieczeństwa organizacji. Doświadczenie zdobywał w różnych obszarach bezpieczeństwa: od przemysłu i logistyki, przez BPO, po bezpieczeństwo w rzeczywistości wirtualnej. Promotor pojęcia *Organisational Resilience*. Obecnie związany z Black Onion Resilience Community.

REKLAMA

ARITECH

Advisor Advanced

Przenieś cyberbezpieczeństwo na wyższy poziom

Innowacyjny

Skuteczny

Idealny dla klienta

Aritech jest globalną marką firmy Carrier reprezentującą rozwiązania zabezpieczeń dla klientów prywatnych, komercyjnych i korporacyjnych. Oferujemy zintegrowaną platformę bezpieczeństwa w obszarze systemów alarmowych, kontroli dostępu, wideo i wykrywania pożaru. Aritech cieszy się zaufaniem klientów od ponad 40 lat.

Odwiedź: **pl.firesecurityproducts.com**

Carrier

Infiltracja, sabotaż i akty terrorystyczne – nie tylko przemysł obronny musi być na to gotowy

Zakłady przemysłowe, jako obiekty, które łączą liczne procesy, niekiedy realizowane w wielu lokalizacjach, zarówno własnych, jak i wynajmowanych bądź będących własnością kooperantów, narażone są na szerokie spektrum zagrożeń. Mowa tu o takich, które mają źródła nie tylko w operacjach własnych, ale także kooperantów, a nawet ich klientów czy dostawców. W ten sposób obiekty te ogniskują konsekwencje tych zagrożeń, co może mieć dużo bardziej negatywny wpływ na bezpieczeństwo organizacji, niż wynikałoby to z analizy własnych operacji i zasobów. Nic więc dziwnego, że właśnie w tych obiektach nasycenie systemów bezpieczeństwa rozwiązaniami technicznymi jest tak duże.

Jacek Grzechowiak

Koncentracja wyłącznie na zasobach materialnych i związanych z nimi procesach, postrzeganych przez zarządzających zakładami produkcyjnymi jako zasoby główne, byłaby jednak dość poważnym błędem, o czym mogą przekonać nas m.in. doniesienia prasowe z ostatnich miesięcy.

Truizmem będzie teza, że zakłady przemysłowe są częścią gospodarki, ale w dobie globalizacji należy zadać sobie pytanie, o jakiej gospodarce mówimy, bo coraz częściej trudno już przypisać daną fabrykę tylko do jednego kraju. Stan ten ma szczególne znaczenie w kontekście wojny w Ukrainie – coraz więcej zakładów produkcyjnych bowiem tam kieruje swoje produkty. W ten sposób znajdują się więc w centrum zainteresowania rosyjskich służb specjalnych. Do dotychczasowych zagrożeń kryminalnych doszedł więc zestaw innych ściśle związanych z wojną, poczynając od infiltracji, kończąc na sabotażu i aktach terrorystycznych. Istniały one także wcześniej, jednak obecnie dociera do nas znacznie więcej informacji o symptomach ich możliwego wystąpienia.

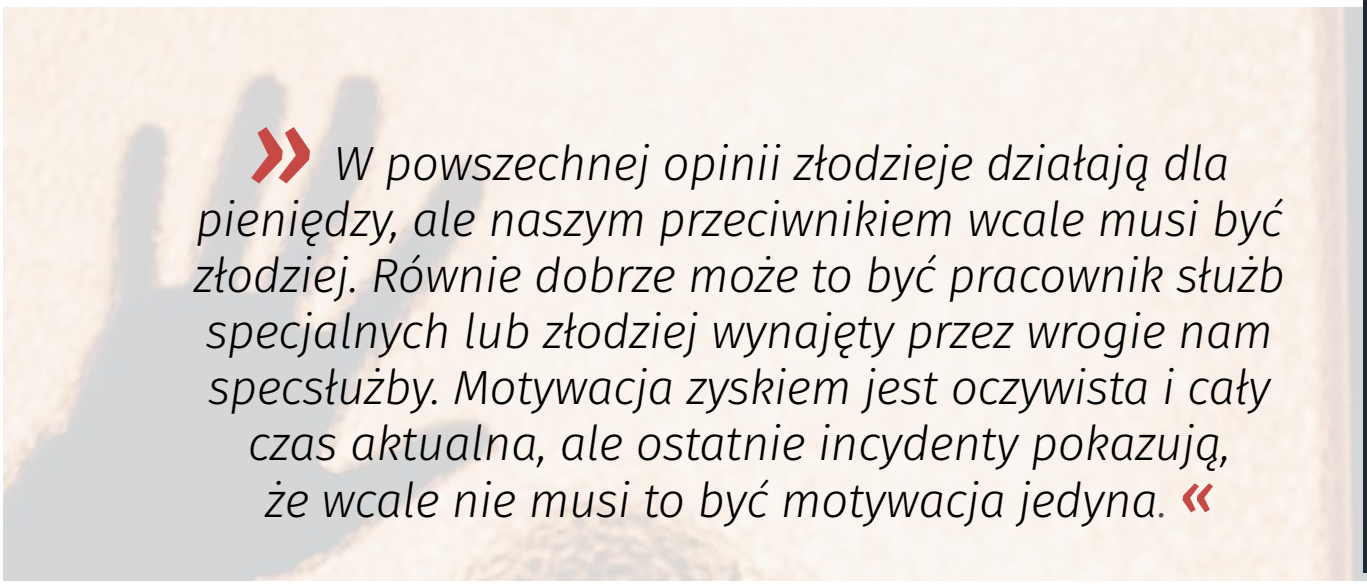
Kiedy w roku 2001 media doniosły o postawieniu zarzutów szpiegostwa pracownikowi ochrony wykonującemu obowiązki w londyńskiej siedzibie znanej firmy zbrojeniowej, wielu zapewne pomyślało „no tak, przemysł zbrojeniowy był, jest i będzie na celowniku". I oczywiście jest w tym wiele racji, choć warto zwrócić uwagę, że szpiegiem był nie konstruktor czy inżynier, ale pracownik ochrony, który do szczegółowych informacji na temat technologii obronnych nie powinien mieć dostępu. Ktoś zapyta: „Gdzie była zasada wiedzy koniecznej i zasada czystego biurka?". I to jest bardzo dobre pytanie, które z pewnością zostało wtedy postawione. Ktoś inny zapyta: „Czy CCTV/VSS może zapobiec szpiegostwu? Czyżby potrafił zajrzeć do mózgu?". Do roli systemów zabezpieczenia technicznego jeszcze wrócę, ale tu ważniejsze jest to, że pracownik ochrony był w stanie dotrzeć do informacji opatrzonych natowskimi klauzulami niejawności.

Warto zauważyć, że istnieją przykłady pokazujące, że zakład przemysłowy wcale nie musi należeć do sektora obronnego (w dosłownym tego słowa znaczeniu, bo przecież w dzisiejszych czasach raczej nie ma już produktów nieistotnych z wojskowego i wojennego punktu widzenia), aby doświadczyć tego typu działań. Choćby sprawa kontraktora pracującego dla znanych szwedzkich firm motoryzacyjnych, który został aresztowany w 2021 r. i skazany za szpiegostwo. Jak wynika z doniesień medialnych, przekazał on rosyjskiemu dyplomacie wrażliwe materiały na temat pojazdów autonomicznych, w tym kod programowania, który posiadał na nośnikach zewnętrznych. Dane te nie były tajemnicami wojskowymi, a jednak przedstawiciele szwedzkiego kontrwywiadu Säpo uznali i publicznie oświadczyli, że materiały te mogą zostać wykorzystane militarnie i wzmocnić potencjał wojskowy. Jak więc widać, przemysł teoretycznie nieobronny ma jak najbardziej obronne znaczenie.

Kolejną ważną informacją, która dotarła do nas niedawno, są kolejne dane dotyczące działań podejmowanych przez członków siatki szpiegowskiej, ujmowanych sukcesywnie przez nasze służby specjalne. Jak wynika z doniesień „The Washington Post", zwerbowani agenci otrzymali zadania rozpoznania w portach morskich, lokowania kamer wzdłuż linii kolejowych i umieszczania w ładunkach wojskowych urządzeń śledzących. Amerykańskie służby specjalne ostrzegały już w lutym tego roku (a zapewne także i wcześniej), że Rosja może podejmować próby sabotowania obiektów logistycznych na terytorium NATO, czyli także w Polsce (a może biorąc pod uwagę znaczenie naszego terenu i infrastruktury, przede wszystkim u nas). Tak poważne sygnały nie mogą być lekceważone, i choć informacje prasowe koncentrują się na infrastrukturze krytycznej oraz logistyce, to powinniśmy pamiętać, że całkiem spora grupa zakładów przemysłowych kwalifikuje się do obiektów kategorii IK. Jednocześnie to przeciwnik decyduje, jakie obiekty uzna za krytyczne, co w praktyce oznacza, że nawet jeśli jakiś zakład przemysłowy zgodnie z naszymi przepisami nie należy do tej kategorii, to i tak może za taki zostać uznany przez wroga. Wreszcie, przywołane za mediami amerykańskimi „umieszczanie urządzeń śledzących w ładunkach wojskowych", powinniśmy postrzegać także przez pryzmat możliwości dokonywania tego typu działań właśnie w zakładzie produkcyjnym, gdzie przecież istnieją do tego potencjalnie bardzo dobre warunki.

Jak można się chronić?

Oczywiste stają się tu kwestie świadomości pracowników, zwłaszcza ich wyszkolenie, i co istotne przyjęcie praktyki, że każdy



» W powszechnej opinii złodzieje działają dla pieniędzy, ale naszym przeciwnikiem wcale musi być złodziej. Równie dobrze może to być pracownik służb specjalnych lub złodziej wynajęty przez wrogie nam specsłużby. Motywacja zyskiem jest oczywista i cały czas aktualna, ale ostatnie incydenty pokazują, że wcale nie musi to być motywacja jedyna. «

(z mocnym naciskiem na to słowo) pracownik partnera zewnętrznego musi mieć ten sam poziom świadomości co pracownik zakładu przemysłowego i jednocześnie podlegać tym samym regułom wewnątrz zakładu przemysłowego. Drugim oczywistym elementem jest efektywne stosowanie systemów zabezpieczenia technicznego i to zdecydowanie nie w modelu reaktywnym, ale co najmniej proaktywnym, a najlepiej predyktywnym.

Zamek, kłódka, drzwi, klucz, karta KD...

Dobre zabezpieczenia, które w takich obiektach ze wszech miar są uzasadnione, powinny działać zarówno zewnętrznie, jak i wewnętrznie. W obiektach przemysłowych najczęściej mamy do czynienia z bardzo dużym nasyceniem systemem CCTV/VSS, ale kluczowe staje się zapewnienie zamknięcia pomieszczeń i stref. Patrolujący pracownik ochrony z londyńskiego przedsiębiorstwa nie dotarłby do wrażliwych dokumentów, gdyby były one zamknięte.

W tym miejscu warto zwrócić uwagę, że o ile w biurach projektowych i technologicznych z reguły przywiązuje się dużą wagę do zabezpieczenia tych informacji, zwłaszcza że są one najczęściej przetwarzane w systemach IT, rzadko występując w formie papierowej, to jednak moje doświadczenia z przeglądów pojemników na śmieci w takich pomieszczeniach pokazują wprost, że tamtędy wciąż wyciekają informacje. Drugi, znacznie poważniejszy kanał ulotu informacji znajduje się w halach produkcyjnych i magazynach, gdzie dokumenty z wrażliwymi informacjami niekiedy leżą bezpośrednio na produkowanych wyrobach, a blokowanie komputerów sterujących obrabiarkami jest wciąż sporym problemem. Dlatego właśnie tak ważne jest stosowanie efektywnej kontroli wejścia, zwłaszcza do pomieszczeń, w których pracownik może przebywać sam, mając jakieś dodatkowe czynniki „komfortu", np. brak okien.

Efektywna kontrola dostępu w kontekście zamków to w dużej mierze procedura zarządzania kluczami, które muszą być nie tylko zabezpieczone przed dorobieniem, poczynając od zakazu ich wynoszenia na zewnątrz, ale także powinny być w pełni rozliczalne, a każdy przypadek zagubienia – choćby czasowego – należy wyjaśnić i wiązać się z wymianą zamka czy wkładki, a być może całej sekcji, jeśli zagubienie dotyczy klucza strefowego czy – czego nikomu nie życzę – klucza generalnego. Czasowa utrata klucza wprowadza bowiem stan niepewności, w praktyce oznaczający możliwość posiadania klucza przez osobę nieupoważnioną.

Rozwiązaniem tego problemu są klucze elektroniczne wyposażone w mikroprocesor z danymi umożliwiającymi dostęp. Co więcej, klucze elektroniczne mogą być wykorzystywane także jako typowy element systemu kontroli dostępu. Jak widać, efekt synergii jest bezsprzeczny, a inteligentny system dostępowy pozwala nie tylko wzmocnić system bezpieczeństwa zarówno w warstwie bezpośredniego zamknięcia poprzez konieczność zadziałania w tym samym czasie komponentów mechanicznego i elektronicznego, jak i minimalizowania negatywnych wpływów czynnika ludzkiego, które mogą osłabiać ten element, np. poprzez zagubienie klucza, a co gorsza, ukrycie faktu zagubienia – bardzo często obserwowane przeze mnie podczas wykonywanych audytów bezpieczeństwa.

Jest tu oczywiście kilka warunków. Przede wszystkim komunikacja pomiędzy identyfikatorami a komponentami drzwiowymi musi odbywać się w sposób szyfrowany. Dobrej klasy drzwi i taki zamek to także jasny sygnał dla złodzieja czy sabotażysty, że nie będzie mu

→

> *Zanim przyjrzymy się kamerom, spójrzmy na ogrodzenie obiektu, bo to pierwsza linia obrony. Ten wciąż niedoceniany element zabezpieczenia ma sens, ale aby był on rzeczywisty, a nie urojony, ogrodzenie musi być kompletne.*

łatwo, a przede wszystkim, że nie pozostanie anonimowy. W przypadku kluczy z komponentem elektronicznym to także możliwość nie tylko weryfikacji osób wchodzących, ale także detekcji zagrożeń już na etapie symptomów, gdzie pracownik usiłujący wejść do strefy dla niego nieprzeznaczonej lub poza godzinami nadanych uprawnień niejako sam sygnalizuje nam potencjał ryzyka. To oczywiście nie musi być ryzyko krytyczne, ale to właśnie ten moment, kiedy podjęte działania wyjaśniające i szkoleniowe mogą zapobiec eskalacji zagrożenia.

Kamery, czyli to co zakłady produkcyjne lubią najbardziej

Kamery wykorzystujemy w celu detekcji nieuprawnionego wejścia czy różnego rodzaju zdarzeń, które mogą prowadzić do przerwania pracy bądź kradzieży mienia, a w konsekwencji do zagrożenia ciągłości operacji. Zanim jednak przyjrzymy się kamerom, spójrzmy na ogrodzenie obiektu, bo to pierwsza linia obrony. Ten wciąż niedoceniany element zabezpieczenia ma sens, ale aby był on rzeczywisty, a nie urojony, ogrodzenie musi być kompletne, i nawet jeśli nie zbudujemy 2-metrowego ogrodzenia, zwieńczonego drutem żyletkowym, wyposażonego w system wykrywania wibracji mechanicznych powodowanych np. próbami jego forsowania poprzez wspinanie się, przecinanie czy odchylanie lub podnoszenie, to warto zadbać, aby ogrodzenie było trwale związane z fundamentem. W końcu dużo wygodniej jest przechodzić pod ogrodzeniem niż nad nim.

Współczesne kamery, bardzo często pracujące w połączeniu z funkcjami analitycznymi, są w praktyce zaawansowanymi czujnikami i pozwalają na całkiem precyzyjną detekcję, a nade wszystko zapewniają świadomość sytuacyjną, a to istotna przewaga. Kamery mogą także budować wirtualne ogrodzenia, sygnalizować ich naruszenie lub inne incydenty (np. niewłaściwy kierunek ruchu, przebywanie osób w strefie zabronionej, zbyt duża

liczba osób w strefie z ograniczeniem, upadek czy choćby brak środków ochrony osobistej). Mamy już pozytywne doświadczenia w tym zakresie, a systemy CCTV/VSS prawdopodobnie przeszły już wszystkie tzw. choroby wieku dziecięcego. Przy założeniu, że zespół ochronny ma wysokie kwalifikacje, pojawia się więc mnóstwo możliwości operacyjnych, takich jak monitoring strefy załadunku, detekcja uszkodzeń, niewłaściwa kompletacja i pakowanie, które można wykorzystać w ramach synergii w relacji logistyka–ochrona. Właściwie każda z tych korzyści jest odpowiedzią także na zagrożenia będące przedmiotem naszej szczególnej troski w związku ze statusem naszego kraju opisanym we wstępie. Umiejscowienie lokalizatora ładunku najpewniej odbędzie się podczas kompletacji przesyłki, więc prewencja w tym zakresie jest jak najbardziej wskazana. Aby to jednak miało szansę być rzeczywistą przewagą, niezbędne są efektywne procedury, gdyż właśnie tam znajdą się algorytmy czy scenariusze postępowania, a więc to, co na poziomie wykonawczym decyduje o powodzeniu działań ochronnych.

Rozważając kwestie CCTV/VSS, nie sposób pominąć tematu oświetlenia, które równie łatwo może wspierać i utrudniać ochronę. Paradoksalnie niekiedy problemem jest za mocne oświetlenie, które powoduje, że kamera „nie radzi sobie" z efektem olśnienia. Dzieje się tak najczęściej przy kamerach o niskiej dynamice. Faza projektowa jest więc niezwykle ważna.

Czy system sygnalizacja włamania i napadu to przeżytek?

Dość często słyszę, że SSWiN przechodzi do lamusa. Tezę tę promują producenci CCTV/VSS, gdyż faktem jest, że funkcje oferowane przez ich systemy pozwalają obecnie na detekcję ruchu, tworzenie wirtualnych ogrodzeń i tym podobne funkcje, które wchodzą na pole SSWiN, ale wciąż jest wiele miejsc zastosowania SSWiN, jak choćby monitoring wejścia na dach czy też monitoring strefy sufitu, dzięki czemu można zapobiec włamaniom dokonywanym przez dach. Inną ciekawą możliwością jest tworzenie ad hoc stref typu wirtualny magazyn, bazujących na wirtualnej ścianie. Wszystko to ma także zastosowanie do zabezpieczenia przed zagrożeniami, o których wspomniałem na początku.

Co ważniejsze, tu właśnie występuje typowy efekt synergiczny, gdyż czujki ruchu, zwłaszcza bazujące na technologii laserowej, są z reguły bardziej efektywne w warunkach dużej zmienności oświetlenia, a nawet niezależnie od oświetlenia. I choć technologia LiDAR, na której są oparte czujki laserowe, ma już 60 lat, to wciąż dobrze służy naszemu bezpieczeństwu. Dobrej jakości czujki pozwalają na detekcję naruszenia strefy przez obiekty o wymiarach nawet 2–3 cm – i to przy próbie zarówno kradzieży tak niewielkich przedmiotów, jak i np. wrzucenia ich w strefę wrażliwą. Tego typu rozwiązanie w minimalizowaniu zagrożenia sabotażowego także ma wiele do zaoferowania.

Zarządzanie, czyli systemy integrujące

Nie sposób nie poruszyć kwestii systemów integrujących. Ich znaczenie jest naprawdę niemałe, zwłaszcza że widać wyraźnie, jak dużą ilość danych będą zbierały wszystkie systemu opisane powyżej. W związku z tym poważnym problemem będzie efektywne ich przetwarzanie, a zarazem ryzykiem może być *data overload*, czyli przeciążenie informacyjne. W konsekwencji efektywność procesu zarządzania bezpieczeństwem zostanie poważnie obniżona.

Najważniejszą kwestią w tym zakresie jest możliwość integracji wszystkich systemów, która pozwala uzyskać funkcjonalności, jakich żaden z podsystemów nie oferuje oddzielnie. Stosując więc PSIM (*Physical Security Information Management*), możemy osiągnąć liczne efekty synergii – od zmniejszenia liczby stanowisk monitorowania, a więc i kosztów związanych z użytkowaniem systemu zabezpieczeń technicznych, po większą wydajność systemów zintegrowanych. Ta synergia jest warta wysiłku wkładanego na etapie implementacji. Modelowym rozwiązaniem jest ujęcie tych potrzeb w planie ochrony. Pozwala to na obniżenie kosztów personelu dzięki lepszemu wykorzystaniu czasu pracy (większa ilość działań wykonywanych w tle). W efekcie stworzony system nie tylko będzie odpowiadał na nowe zagrożenia, ale także umożliwi lepsze ich przewidywanie, co w dzisiejszych zmiennych czasach jest niezwykle potrzebne.

Jak widać, w walce z przeciwnikiem nie pozostajemy bezbronni, ale broń musi być nam znana lepiej niż przeciwnikowi. ●

Jacek Grzechowiak

Menedżer ryzyka i bezpieczeństwa. Absolwent WAT, studiów podyplomowych w SGH i Akademii L. Koźmińskiego. Gościnnie wykłada na uczelniach wyższych. W przeszłości związany z grupami Securitas, Avon i Celsa, w których zarządzał bezpieczeństwem i ryzykiem. Obecnie pełni funkcję konsultanta Zarządu ds. Ryzyka i Bezpieczeństwa w TAURUS OCHRONA. Dyrektor Centrum Kompetencji „a&s Polska".

Nowe możliwości systemów zabezpieczeń

W erze Przemysłu 4.0 transformacja cyfrowa rewolucjonizuje sposoby, w jakie przedsiębiorstwa prowadzą produkcję, zarządzają zasobami oraz zabezpieczają swój majątek. Systemy zabezpieczeń nie są już oddzielnymi systemami, stały się integralną częścią technologicznego ekosystemu przedsiębiorstwa. Ich zadania znacznie wykraczają poza zabezpieczenie przed niepowołanym dostępem.

Tomasz Olejniczak

W środowisku Przemysłu 4.0, gdzie technologie cyfrowe i Internet rzeczy (IoT) odgrywają kluczową rolę, elektroniczne urządzenia zabezpieczające mienie pełnią istotną funkcję w zapewnianiu ciągłości działalności oraz minimalizowaniu ryzyka strat. Systemy Hikvision stały się nieodłącznym elementem tej ewolucji, zapewniając skuteczną ochronę w każdych warunkach. Firma koncentruje się na czterech najważniejszych aspektach Przemysłu 4.0:

1) dostarcza gotowe rozwiązania sprzętowe do instalacji w różnych warunkach środowiskowych, technologicznych oraz funkcjonalnych,
2) wspiera dostarczanie i analizowanie danych w czasie rzeczywistym dzięki AIoT (*Artificial Intelligence of Things*), zwiększając znacząco świadomość sytuacyjną osób zarządzających bezpieczeństwem przedsiębiorstwa,
3) dostarcza interfejsy integracji (HEOP, OpenAPI, SDK itp.) z systemami zarządzania przedsiębiorstwem (MES, ERP),
4) promuje działania na rzecz cyberbezpieczeństwa, wspierając metody innowacyjne, takie jak Zero Trust, BOM (*bill of materials*).

Przejście do Przemysłu 4.0 niesie nowe wyzwania. Wzrost liczby połączonych urządzeń oznacza większe pole do działania cyberprzestępcom. Na bezpieczeństwo negatywnie wpływa też skomplikowana infrastruktura technologiczna. Oba czynniki mogą prowadzić do trudności w identyfikacji i zrozumieniu zagrożeń, co z kolei stwarza potrzebę doskonalenia procedur reagowania na incydenty.

Dbając o wysoki poziom bezpieczeństwa, urządzenia Hikvision są projektowane i wykonywane zgodnie z metodą Zero Trust. To podstawowy element tworzenia inteligentnych rozwiązań AIoT. Pozwala

Kamera bispektralna DS-2TD2637-35QY

na przejrzyste i wizualne zarządzanie całą topologią połączeń sieciowych, od serwerów agregujących dane (rejestratory, macierze, serwery), przez przełączniki sieciowe pracujące w topologii gwiazdy, ringu lub drzewa, aż po urządzenia zbierające dane (kamery, domofony, bramki, tripody, kontrolery, detektory, skanery podwozia).

Hikvision rozwija zaawansowane urządzenia sieciowe w celu poprawy bezpieczeństwa i odporności systemu na cyberataki. Do tych urządzeń należą przełączniki Smart Managed, które zasilają urządzenia ze standardem PoE, oraz przełączniki agregujące warstwy 3. pozwalające na stworzenie środowiska sieciowego na potrzeby systemu dozoru wizyjnego. Zwizualizowanie całej topologii umożliwia przejrzyste monitorowanie wszystkich urządzeń sieciowych i administrowanie nimi. Do zarządzania całą siecią stosuje się przełączniki rdzeniowe. Hikvision ma w ofercie szeroki wachlarz tych urządzeń, jednym z nich jest DS-3E37806. Przełącznik ten jest zbudowany z modułów: LPU (zapewnia potrzebną liczbę i typy portów), MPU (zarządza siecią i monitoruje ruch sieciowy) oraz zasilaczy. Jednostki MPU oraz zasilacze mogą pracować w trybie redundancji, a samo urządzenie może działać w trybie wirtualizacji, co zwiększa bezpieczeństwo.

Urządzeniami wspierającymi ochronę obwodową są np. kamery bispektralne, które zapewniają bardzo dobrą jakość obrazu w paśmie widzialnym oraz obrazowanie w paśmie podczerwonym.

Termowizja zapewnia wysoką skuteczność w wykrywaniu osób i pojazdów nawet w trudnych warunkach atmosferycznych. Wszystkie

kamery oferują zaawansowaną analizę obrazu, która klasyfikuje obiekty (człowiek/pojazd) oraz pozwala na wyznaczenie wirtualnych linii – po ich przekroczeniu osoba lub pojazd wyzwoli zdarzenie alarmowe.

Seria kamer termowizyjnych zawiera również modele wyspecjalizowane do termografii. Urządzenia te od wielu lat znajdują zastosowanie w prewencji pożaru i detekcji wzrostu temperatury w różnych miejscach (serwerownie, stacje energetyczne, urządzenia elektryczne, miejsca składowania odpadów). Kamery termograficzne mogą monitorować temperaturę w zakresie od -20°C do 550°C z dokładnością pomiaru ±2°C.

Dla zapewnienia bezpieczeństwa na wejściach do obiektów Hikvision dostarcza kompletne systemy kontroli dostępu z wykorzystaniem takich urządzeń, jak bramki obrotowe (DS-K3G501X), bramki uchylne – DS-K3B530X, bramki rozsuwane – DS-K3Y501SX.

Wszystkie bramki są wyposażone w sterownik i czytniki kontroli dostępu, zapewniając różne typy uwierzytelnienia jedno- lub wieloskładnikowe. Czytniki mogą wykorzystywać karty oraz dodatkowo biometrię, kody QR (dla gości lub osób bez karty), smartfon.

Zaawansowane funkcje uprawnień i autoryzacji pozwalają na dostosowanie urządzeń do kontroli przejścia do stref o zróżnicowanym poziomie bezpieczeństwa. Wyjątkowość rozwiązań Hikvision AIoT polega na zautomatyzowaniu procesu uwierzytelnienia z zastosowaniem warunków koniecznych do autoryzacji. Jako przykład może posłużyć weryfikacja, czy pracownicy posiadają uprawnienia dostępu (karta, kod, QR) oraz czy mają założone środki ochrony osobistej (kask, okulary ochronne, kamizelka odblaskowa). Dopiero spełnienie obu warunków pozwala na autoryzację i wejście do kontrolowanej strefy. Kolejnym zastosowaniem rozwiązań Hikvision z podwójną weryfikacją jest sprawdzenie, czy osoby wchodzące do stref EPA (ESDPA – *Electrostatic Discharge Protected Area*) są wyposażone w odpowiednią odzież antyelektrostatyczną. W tym celu kontrola dostępu wsparta jest przez kamery z funkcją HEOP (*Hikvision Embedded Open Platform 2.0*). Funkcja ta pozwala na łatwą implementację algorytmów opartych na sieciach neuronowych głębokiego uczenia. Do każdej kamery z funkcją (HEOP) można zaimplementować dowolny algorytm przygotowany przez AI Training Server (DS-IN1001-A3U).

Rozwiązania AIoT umożliwiają weryfikację liczby osób przebywających wewnątrz zakładu, wykorzystując kontrolę dostępu, kamery z analityką HEOP oraz system Digital Signage do pokazywania w czasie rzeczywistym osób w każdej strefie. W przypadku zagrożenia informacja ta pozwala na weryfikacją liczby osób wymagających ewakuacji. Urządzenia rejestrujące i serwery zarządzające zostały zaprojektowane z interfejsami SDK i API do integracji z systemami typu ERP/MES w obiekcie. Udostępniają pełne informacje z rejestracji czasu pracy oraz zasoby do weryfikacji zarejestrowanych danych. Funkcja porównująca liczbę wejść na tripodzie z analizą obrazu z kamery pozwala na wykrycie zarówno nieautoryzowanego wejścia, jak i odbicia dwóch kart przez jedną osobę.

Miejsca szczególnie narażone na szkodliwe warunki środowiskowe czy miejsca o wysokim ryzyku powstania wybuchu powinny być stale monitorowane. Hikvision dostarcza rozwiązania w postaci urządzeń w wykonaniu antykorozyjnym, iskrobezpiecznym oraz odpornym na wybuchy, spełniających standardy i normy technologiczne.

Przykładem urządzenia do pracy w bardzo trudnych warunkach jest kamera PTZ DS-2DY7432IXG-X. Spełnia ona wymagania dyrektywy ATEx, wykonano ją ze stali SUS 316L odpornej na korozję, ponadto jej powierzchnia została pokryta środkiem antykorozyjnym. Jest

Kamera PTZ DS-2DY7432IXG-X do pracy w bardzo trudnych warunkach

wyposażona w duży przetwornik 1/1,8 cala. Zapewnia obserwację w kolorze przy bardzo niskim poziomie oświetlenia, co sprawia, że doskonale działa przy słabym sztucznym oświetleniu (czułość przetwornika w kolorze 0,005 luksa). Na szczegółową weryfikację miejsc obserwacji przez operatora pozwala obiektyw o zmiennej ogniskowej w zakresie 5,9~188,8 mm z motorzoomem oraz dodatkowo 16-krotny zoom cyfrowy. Oprogramowanie kamery wykorzystuje zaawansowane algorytmy analizy obrazu opartej na sieciach neuronowych głębokiego uczenia. Pozwala to na automatyczne powiadamianie o wejściu osób do strefy chronionej, wykrycie wyjścia ze strefy, pojawienie się lub zniknięcie obiektu, detekcję twarzy aż do 10 osób jednocześnie. Wykorzystanie tej analizy w połączeniu z funkcją automatycznego śledzenia obiektów znacząco wspomaga pracę operatora systemu dozoru wizyjnego.

Innym istotnym elementem ekosystemu Hikvision jest dostarczanie API i SDK do integracji z systemami MES i ERP. Systemy umożliwiają sprawne wykrycie zagrożeń, identyfikację miejsc szybkiej poprawy bezpieczeństwa, pozwalając, by odpowiednie jednostki organizacyjne przedsiębiorstwa opracowały na ich podstawie rozwiązania proceduralne i techniczne zmniejszające poziom ryzyka dla pracowników. ●

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

Bramki rozsuwane DS-K3G501X

Architektura Edge w systemie telewizji dozorowej – efektywna ochrona terenów rozległych

W dzisiejszej rzeczywistości bezpieczeństwo i nadzór stały się integralną częścią codziennego życia. Sztuczna inteligencja (AI) zastosowana w systemach telewizji dozorowej CCTV zrewolucjonizowała sposób, w jaki monitorujemy i zabezpieczamy swoje otoczenie. Pojawia się jednak pytanie: gdzie powinno się odbywać przetwarzanie AI w systemach CCTV? Odpowiedź kryje się w sile architektury Edge.

Zanim przejdziemy do uzasadnienia, dlaczego przetwarzanie AI w architekturze Edge jest najlepsze w systemach CCTV, zdefiniujmy, czym ono jest. Przetwarzanie Edge, znane także jako obliczenia na brzegu sieci, oznacza praktykę wykonywania przetwarzania i analizy danych lokalnie na urządzeniu lub sensorze zamiast na scentralizowanym serwerze w chmurze. W kontekście systemów monitoringu wizyjnego oznacza to, że algorytmy AI odpowiedzialne za analizę wideo i rozpoznawanie zdarzeń są wykonywane na pobliskim serwerze Edge w sieci lokalnej. Brakuje przesyłania wszystkich danych do zdalnego serwera w chmurze w celu analizy.

Zalety architektury Edge

Przetwarzanie na brzegu sieci dzięki swoim zaletom jest najlepszą opcją do zastosowania w systemach telewizji dozorowej. Wśród największych zalet należy wskazać:

Niskie opóźnienia

Jedną z największych zalet przetwarzania na Edge w systemach CCTV jest niska latencja. Kiedy algorytmy AI analizują strumienie wizyjne na brzegu sieci, wyniki są generowane w czasie rzeczywistym lub z minimalnym opóźnieniem. Małe opóźnienie jest kluczowe w sytuacjach, w których jest wymagana natychmiastowa reakcja, np. w przypadku naruszenia strefy bezpieczeństwa czy reagowaniu na sytuacje awaryjne. Kiedy nieupoważniona osoba wchodzi do chronionego obszaru, przetwarzanie na brzegu sieci spowoduje natychmiastowe uruchomienie alertu, pozwalając pracownikom ochrony na szybkie działanie.

Efektywność przepustowości

Przesyłanie strumieni wizyjnych o wysokiej rozdzielczości do zdalnego serwera w chmurze w celu analizy może obciążać przepustowość sieci, prowadząc do opóźnień i potencjalnych wąskich gardeł. Przetwarzanie na brzegu redukuje ilość danych, które trzeba przesłać przez sieć, ponieważ przekazywane są tylko istotne zdarzenia lub metadane. Efektywność przepustowości nie tylko oszczędza koszty, ale także zapewnia płynniejszy i bardziej reaktywny system dozoru.

Prywatność i bezpieczeństwo

Architektura Edge zwiększa prywatność i bezpieczeństwo systemów telewizji dozorowej. Dzięki lokalnemu przetwarzaniu danych wrażliwe informacje pozostają na miejscu, co zmniejsza ryzyko naruszeń danych czy możliwość nieuprawnionego dostępu. Jest to szczególnie istotne w przypadku środowisk o wysokim stopniu poufności, takich jak instytucje rządowe czy infrastruktura krytyczna.

Podsumowując, przesunięcie przetwarzania AI bliżej źródła zbierania danych pozwala stworzyć inteligentniejsze, reaktywniejsze i bezpieczniejsze systemy dozorowe, które są lepiej przystosowane do ochrony osób i mienia. W miarę rozwoju technologii architektura Edge staje się przyszłością systemów CCTV z wykorzystaniem AI.

Studium przypadku

Architekturę Egde wykorzystano w zabezpieczeniu średniej wielkości farmy fotowoltaicznej jednego z największych państwowych koncernów energetycznych. Zadanie stojące przed dostawcą technologii AI, czyli amerykańską firmą Scylla AI oraz polską firmą Global Security Partner, która zaprojektowała rozwiązanie i je dostarczyła, polegało na:

- zaprojektowaniu i dostarczeniu kompletnego i autonomicznego systemu ochrony perymetrycznej terenu farmy fotowoltaicznej o mocy 13 MW,
- integracji z systemem SSWiN,
- integracji z głośnikami IP,
- integracji 90 kamer IP wybranych wcześniej przez inwestora,
- wdrożeniu oprogramowania integrującego i zarządzającego,
- wykorzystaniu kamer pozbawionych zaawansowanej analityki do detekcji intruza.

Rozwiązanie oparte na platformie Scylla VMS i serwerze analityki Edge Scylla Asteria pozwoliło na:

- zredukowanie do minimum fałszywych alarmów (ok. 3 fałszywe alarmy na dobę ze wszystkich kamer, mimo dużej liczby pająków pojawiających się w ich kadrze),
- uproszczenie obsługi systemu poprzez integrację z systemem SSWiN – obsługa za pomocą manipulatora,
- wczesną detekcję intruza wraz z sygnałami ostrzegania bez udziału operatora,
- integrację sygnałów ze wszystkich systemów, ustawienie zależności detekcji od stanu uzbrojeń/rozbrojeń stref, przydział odpowiednich komunikatów z poziomu Scylla VMS,
- zredukowanie liczby kamer potrzebnych do monitorowania terenu (zasięgi detekcji były imponujące nawet z kamer 2 Mpix), a wraz z tym liczby potrzebnych urządzeń sieciowych, przewodów oraz zmniejszenie nakładów pracy, a także liczby kanałów w oprogramowaniu VMS,
- brak konieczności stosowania specjalnych, drogich kamer projektowych.

Głównymi wyzwaniami, które stanęły przed instalatorami, były konfiguracja zdalna przy ograniczonym dostępie Internetu LTE oraz brak zasilania sieciowego i konieczność używania generatorów (we wczesnej fazie wdrażania). Mimo wszystko projekt został zakończony sukcesem, a inwestor planuje kolejne inwestycje.

Ta realizacja niewątpliwie udowodniła, że z punktu widzenia biznesowego i technicznego zastosowanie sztucznej inteligencji w rozległych systemach zabezpieczeń w postaci analityki wideo znacznie usprawniło pracę operatorów (reakcja na rzeczywiste zdarzenia). Skutecznie odstraszało też potencjalnych intruzów poprzez automatyczne i autonomiczne oraz skuteczne działania systemów odstraszająco-zabezpieczających.

Wszystkie systemy zostały połączone za pomocą systemu zarządzającego Scylla VMS, który umożliwiał zapis wideo, oznaczanie nagrań alarmów z analityki Scylla, kreację logiki zdarzeń, integrację systemu alarmowego, głośników IP i Scylla Asteria.

Dostawcy technologii

Global Security Partner, jako Value Partner wielu światowych producentów systemów zabezpieczeń, posiada kompetencje do projektowania, doradztwa oraz dostarczania zintegrowanych rozwiązań bezpieczeństwa z wykorzystaniem najnowszych technologii dostępnych na rynku. Zapewnia niezawodność i pewność działania osiąganą dotychczas w systemach klasy militarnej.

Scylla AI, amerykański dostawca technologii analityk wideo opartych na algorytmach sztucznej inteligencji, oferuje szereg rozwiązań, które nie zostały wykorzystane przy tym projekcie. W portfolio firmy znajdują się m.in.:

- detekcja broni, z klasyfikacją jej rodzaju;
- grupa analityk behawioralnych
  – rozpoznawanie anomalnych zachowań, np.
    - wykrywanie podejrzanych zachowań w sklepie – wsparcie detekcji kradzieży,
    - detekcja upadku i poślizgnięcia,
    - detekcja aktów wandalizmu i bójek;
- analityki środowiskowe:
    - detekcja dymu i ognia (z obrazu kamery wizyjnej);
- inne analityki rozpoznające:
    - twarz (standard i *auto-enrolment),*
    - tablice rejestracyjne,
    - kamizelkę ochronną i kask,
    - pozostawione obiekty;
- analityki dotyczące *business intelligence:*
    - analiza przepływu ruchu (mapy ciepła, zliczanie ludzi, łącznie z kategoryzacją płci, wieku, przeszukiwanie wg atrybutów itp.).

Wszystkie analityki zostały przetestowane i sprawdzone w praktyce. Największym atutem rozwiązań jest możliwość zastosowania analityk na funkcjonujących już systemach bez konieczności kosztownych modernizacji. W ekstremalnych przypadkach analitykę można wdrożyć nawet w systemach analogowych, jednakże nie należy zapominać o tym, iż ich skuteczność może być ograniczona ze względu na słabą jakość obrazu. ●

Global Security Partner
ul. Lęborska 3b, 80-286 Gdańsk
www.gspartner.pl
kontakt@gspartner.pl

Systemy Yard Management: nowa era bezpieczeństwa w obiektach przemysłowych

Współczesny przemysł dynamicznie ewoluuje, wdrażając nowoczesne technologie, aby zwiększyć efektywność i bezpieczeństwo operacji. Jednym z kluczowych elementów tej ewolucji są systemy zarządzania przestrzenią wewnętrzną i zewnętrzną, zwane systemami Yard Management.

Krzysztof Bereza

Systemy Yard Management (YMS) nie tylko pomagają w optymalizacji procesów logistycznych, ale także stanowią znakomite narzędzie w zapewnieniu bezpieczeństwa w obiektach przemysłowych.

Rola Systemów Yard Management

YMS wspierają bezpieczeństwo zakładu produkcyjnego, pozwalając na lepszą kontrolę i monitorowanie obszarów zewnętrznych obiektu. Dzięki nim można skutecznie kontrolować dostęp do terenu przemysłowego poprzez koordynację procesu identyfikacji i autoryzacji kierowców oraz wjeżdżających pojazdów. Eliminuje to ryzyko nieautoryzowanego dostępu i potencjalnych zagrożeń, które wynikają z wtargnięcia nieuprawnionych osób na chroniony teren.

Kolejną kluczową funkcją systemów klasy YMS jest ciągłe monitorowanie ruchu pojazdów na terenie obiektu. W przypadku wystąpienia awarii lub niebezpiecznej sytuacji można szybko zareagować, zminimalizować ryzyko wypadków i zwiększyć bezpieczeństwo ludzi, a przede wszystkim sprawnie zarządzać ewakuacją.

Wdrożenie systemu pomaga w efektywnym planowaniu i alokacji przestrzeni na danym terenie oraz wspiera zarządzanie parkingami buforowymi. Jest to istotne, ponieważ unika się zatłoczenia, które może prowadzić do kolizji lub innych niebezpiecznych sytuacji.

Automatyzacja procesów z wykorzystaniem YMS pozwala na zmniejszenie ryzyka wystąpienia błędów ludzkich, które mogą prowadzić do np. błędnego skierowania do nieodpowiedniego doku lub obsługę w niewłaściwym czasie. Systemy mogą automatycznie kierować pojazdy do odpowiednich stref na terenie obiektu i informować o konieczności wykonania określonych czynności. YMS obsługuje automatycznie procesy kontrolne, np. ważenie lub sprawdzanie próbek. W systemie można zdefiniować tzw. bibliotekę szablonów wizyt, co upraszcza kontrolę procesów. Jeśli np. odbiór odpadów jest realizowany z określoną częstotliwością, a wizyta na terenie obiektu nie może być dłuższa niż 30 minut, to po przekroczeniu tego czasu pracownicy ochrony otrzymują komunikat o nieprawidłowości w zaplanowanej wizycie i pojazd jest kierowany do szczegółowej kontroli. Automatyzację procesów wspierają samoobsługowe kioski awizacyjne lub terminale wjazdowe, które stają się coraz bardziej popularnym narzędziem pomagającym w efektywnym zarządzaniu bezpieczeństwem w obiektach przemysłowych.

Wspomniane kioski awizacyjne to interaktywne urządzenia umieszczone w strategicznych miejscach na terenie obiektu. Pozwalają one pracownikom oraz dostawcom zgłosić swoją obecność i zarejestrować się, pomagając tym samym w przestrzeganiu procedur bezpieczeństwa. Urządzenia umożliwiają potwierdzanie tożsamości przed wejściem na teren obiektu. Kioski pozwalają także na zgłaszanie awarii i incydentów oraz mogą dostarczać informacji na temat procedur bezpieczeństwa oraz zapewniać dostęp do materiałów szkoleniowych, co pomaga w podnoszeniu świadomości i umiejętności pracowników.

Zastosowanie kiosków stanowiących uzupełnienie systemów klasy Yard Management niesie liczne korzyści. Przede wszystkim przyspiesza proces rejestracji i awizacji, co pomaga redukować kolejki, oraz oszczędza czas zarówno pracowników, jak i dostawców. Automatyczne rejestrowanie obecności i zgłaszanie incydentów eliminują ryzyko błędów, co przyczynia się do lepszej jakości danych i raportów. Kioski umożliwiają bieżącą komunikację z pracownikami i dostawcami, co jest szczególnie przydatne w zarządzaniu kolejnością obsługi oraz stanowi wsparcie w sytuacjach kryzysowych.

Systemy Yard Management można łatwo zintegrować z innymi systemami bezpieczeństwa, takimi jak telewizja dozorowa, sygnalizacja pożaru czy system alarmowy. Dzięki temu możliwa jest szybka reakcja na potencjalne zagrożenia.

Praktyczne zastosowania Systemów Yard Management

Systemy YMS pomagają w zapewnieniu, że pojazdy na terenie obiektu przemysłowego poruszają się w sposób bezpieczny i zgodny z przepisami. Można kontrolować ich prędkość, kierunek ruchu, a także monitorować zachowanie kierowców. System pozwala na identyfikację i oznaczenie na terenie obiektu stref niebezpiecznych, by w razie potrzeby automatycznie zablokować do nich dostęp. Funkcje systemu pozwalają na natychmiastową reakcję na awarie lub incydenty. Dzięki precyzyjnej kontroli nad ruchem można szybko ewakuować obszary zagrożone. W przypadku obiektów przemysłowych, w których przechowywane są materiały niebezpieczne, YMS może ułatwić zapewnienie szczególnej ochrony oraz kontrolować wyposażenie w środki ochrony osobistej poprzez wykorzystanie dostępnych funkcji analitycznych z wykorzystaniem algorytmów sztucznej inteligencji.

Systemy Yard Management stanowią nieocenioną pomoc w zapewnieniu bezpieczeństwa w obiektach przemysłowych. Dzięki kontroli dostępu, monitorowaniu ruchu, planowaniu przestrzeni oraz integracji z systemami bezpieczeństwa YMS pomagają minimalizować ryzyko wypadków i niepożądanych zdarzeń. Rola Yard Management w przemyśle będzie rosła wraz z postępem technologicznym i dalszym dążeniem do zapewnienia bezpieczeństwa w miejscach pracy.

Dla przedsiębiorstw, które priorytetowo traktują bezpieczeństwo pracowników i mienia, inwestycja w systemy Yard Management może przynieść liczne korzyści. To krok w kierunku nie tylko bardziej efektywnego zarządzania, ale także znacznie bezpieczniejszej przyszłości przemysłu. ●

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

Elektroniczna kontrola dostępu blueSmart w obiektach przemysłowych

Zdjęcia wykonano w Centrum Szkoleniowym Nord Napędy w Zakrzowie

Inteligentny system kontroli dostępu Winkhaus blueSmart jest przeznaczony do obiektów różnego typu i wielkości. Sprawdza się także w rozbudowanych kompleksach infrastruktury przemysłowej, składających się z wielu budynków, a nawet lokalizacji.

Komponenty i zalety systemu blueSmart

System blueSmart łączy zalety systemów offline i online. Nośnikiem informacji jest tu elektroniczny klucz z chipem, który jest aktywowany w czytniku na podstawie uprawnień dostępowych nadanych przez administratora. Uprawnienia te mogą być czasowe lub bezterminowe, ich zakres ogranicza tylko struktura pomieszczeń. Zagubiony klucz można łatwo i bezkosztowo wyeliminować z systemu bez konieczności wymiany wkładek. Wkładka elektroniczna zapisuje historię 2000 ostatnich zdarzeń, co umożliwia odtworzenie obecności osób w danym pomieszczeniu, a także prób użycia nieautoryzowanego klucza. Wkładki elektroniczne Winkhaus mają najwyższą 6 klasę bezpieczeństwa, potwierdzoną certyfikatem Instytutu Mechaniki Precyzyjnej w Warszawie.

Co wyróżnia system blueSmart?

Wyróżniającą cechą systemu Winkhaus jest bezprzewodowa komunikacja z komponentami. Dzięki temu system kontroli dostępu może być zainstalowany na dowolnym etapie inwestycji. Instalacja odbywa się bezinwazyjnie: tradycyjne wkładki patentowe zostają zastąpione przez odpowiedniki elektroniczne.

Funkcje dodatkowe

System blueSmart nie tylko elastycznie dopasowuje się do specyfiki danego obiektu, administrując wejścia do pomieszczeń, ale także może pełnić dodatkowe funkcje takie jak rejestracja czasu pracy, dostęp do miejsc parkingowych, sterowanie drzwiami automatycznymi, windami i urządzeniami biurowymi. Może obejmować zasięgiem także budynki peryferyjne i oddziały usytuowane często w różnych lokalizacjach.

Jeden system, trzy lokalizacje

Firma NORD Napędy w Polsce jest zlokalizowana w trzech odległych miejscach: Nowej Soli, Zakrzowie i Wiechlicach. Wszystkie te obiekty działają w ramach jednego systemu blueSmart. W przypadku rozproszonych lokalizacji ma zastosowanie rozbudowana struktura organizacji dostępu: klucze i wkładki tworzą grupy. Zarządzanie systemem odbywa się za pośrednictwem oprogramowania blueControl Professional. Klucz blueSmart nie tylko obsługuje dostęp do pomieszczeń, lecz także służy jako identyfikator dla autonomicznych systemów rejestracji czasu pracy oraz kontroli dostępu do stref chronionych.

Centralne sterowanie – pełna kontrola

System elektronicznej kontroli dostępu blueSmart we wszystkich obiektach NORD Napędy w Polsce jest obsługiwany z centralnego komputera. Administrator za pomocą oprogramowania blueControl Professional przydziela prawa dostępowe oraz nadzoruje wejścia i wyjścia z jednego miejsca.

System blueSmart zintegrowano także z zewnętrznymi systemami działającymi w NORD Napędy dzięki wyposażeniu kluczy w dodatkowy transponder. Niezależnie od podstawowej funkcji, jaką jest otwieranie elektronicznych wkładek, dwusystemowe klucze Winkhaus zapewniają bezprzewodową identyfikację użytkownika również w innych, zainstalowanych w NORD, systemach RFID.

W portfolio obiektów referencyjnych dla systemu blueSmart są przedsiębiorstwa różnych branż i wielkości.

Więcej na: blueSmart.winkhaus.com. ●

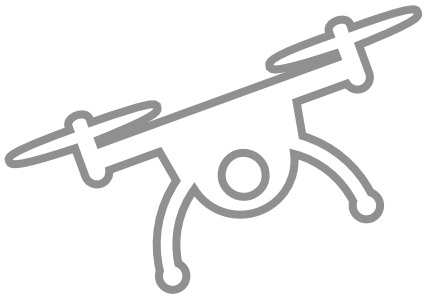
Winkhaus Polska Beteiligungs
ul. Przemysłowa 1
64-130 Rydzyna
bluesmart@winkhaus.pl

ALNET SYSTEMS

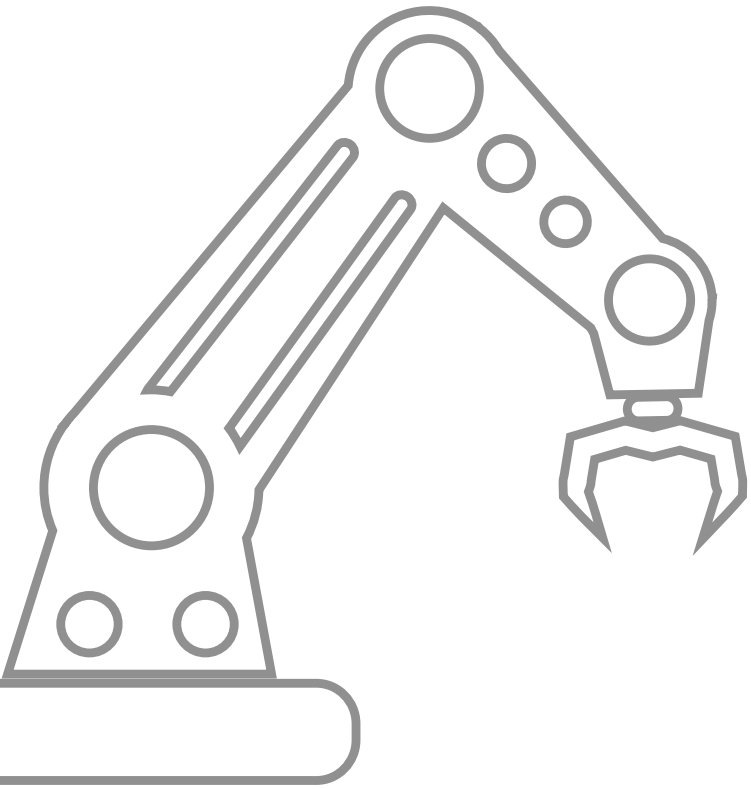
Polskie profesjonalne zintegrowane rozwiązania VMS
Ponad 200 000 instalacji na całym świecie
Jesteśmy z Wami od 2003 roku

www.alnetsystems.com

głos branży



Zdania na temat kondycji polskiego przemysłu są podzielone. Jedni twierdzą, że sytuacja ekonomiczna naszego kraju jest znakomita, drudzy, że gospodarkę trawi poważny kryzys. Jak w tej sytuacji znaleźć środki na inwestycje w najnowsze systemy zabezpieczeń, które zapewnią skuteczną ochronę obiektów przemysłowych? Co radzą doświadczeni eksperci?



dr inż. Artur Pollak
APA GROUP

Bezpieczne środowisko przemysłowe

Bezpieczeństwo w obiektach przemysłowych to niezwykle złożona, ale kluczowa dziedzina, która musi być zarządzana w sposób zintegrowany, aby zapewnić ochronę zarówno ludzi, jak i zasobów. Współczesne metody identyfikacji towarów, maszyn i urządzeń, takie jak systemy lokalizacji w czasie rzeczywistym (RTLS), odgrywają tu kluczową rolę. Dzięki RTLS można nie tylko efektywnie zarządzać zasobami, ale także monitorować potencjalne zagrożenia, takie jak punkty styku pomiędzy pojazdami a pracownikami, co znacząco podnosi poziom bezpieczeństwa.

Jednocześnie zyskują na znaczeniu funkcje *traceability*, czyli śledzenia w czasie rzeczywistym. Informacje z różnych podsystemów umożliwiają błyskawiczne reagowanie na wszelkie nieprawidłowości, co jest niezwykle ważne w kontekście bezpieczeństwa. Na przykład awaria jednej z maszyn może zostać natychmiast zasygnalizowana, co pozwoli na szybkie działania zaradcze.

Technologie zarządzania budynkami, takie jak platformy BMS, zapewniają zintegrowane zarządzanie wszystkimi systemami obiektu, od klimatyzacji po systemy przeciwpożarowe. W tym kontekście zaawansowane BMS mogą działać w symbiozie z systemami zarządzania procesami przemysłowymi, umożliwiając kompleksowe zarządzanie zarówno ludźmi, jak i maszynami.

Nie można też zapominać o nowoczesnym monitoringu CCTV z AI i analitycznym przetwarzaniem obrazu. Dzięki zaawansowanym algorytmom sztucznej inteligencji te systemy są w stanie wychwycić zagrożenia, które mogą umknąć ludzkiemu oku, i generować natychmiastowe alarmy.

Powstaje całkiem nowa sensoryka oparta na nowoczesnych urządzeniach z przetwarzaniem brzegowym. Zaawansowane czujniki wyposażone w dedykowane algorytmy mogą np. monitorować poziom hałasu czy temperaturę, a nawet wcześnie wykrywać sytuację zagrożenia, takie jak upadek pracownika lub inne zdarzenia odbiegające od normy.

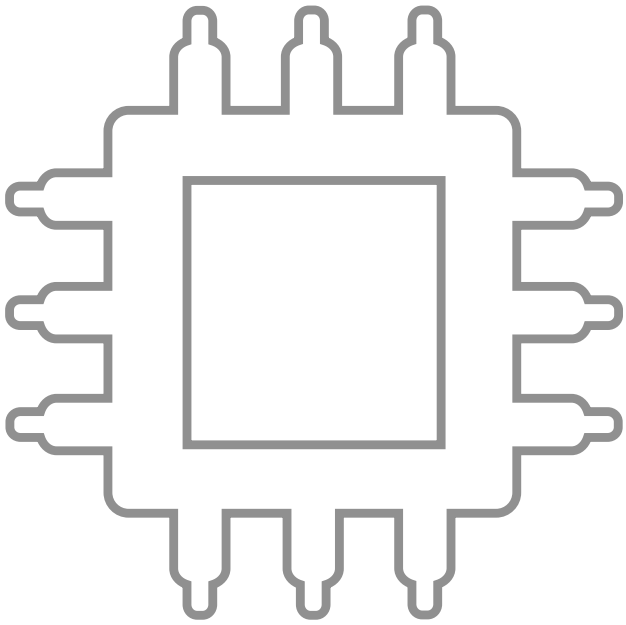
Warto też wspomnieć o cyberbezpieczeństwie, co jest niezwykle istotne w dobie Przemysłu 4.0 i urządzeń funkcjonujących w ramach IIoT. Platformy będące zaawansowanymi środowiskami programistyczno-sprzętowymi działają na podstawie modelu ISO OSI, który zapewnia ochronę na różnych warstwach systemu, od lokalnych centrów danych po urządzenia Internetu rzeczy. Skupiają się na zapewnieniu ciągłości i bezpieczeństwa w różnorodnych środowiskach IT. Poprzez zintegrowany harmonogram i rotację danych taki system zapewnia spójność i dostępność danych, nawet w przypadku awarii. Użycie odseparowanych i zabezpieczonych podsieci VLAN oraz rozbudowane reguły firewalla sprzętowego minimalizują ryzyko przeniknięcia do sieci. Działa też jako dodatkowa warstwa ochrony dla usług publicznych, zabezpieczając infrastrukturę przed nieautoryzowanym dostępem. Funkcjonalności wychwytywania nietypowych zdarzeń i dynamicznych list zablokowanych IP pomagają w identyfikacji i prewencji ataków sieciowych.

Wszystkie te elementy, od RTLS po cyberbezpieczeństwo, są częścią jednego ekosystemu zarządzania, co pozwala na ich efektywną integrację i stworzenie naprawdę zabezpieczonego środowiska przemysłowego.

Jarosław Sapko
AXIS COMMUNICATIONS

Wieloaspektowa koncepcja ochrony

Segment obiektów przemysłowych oraz infrastruktury krytycznej często wiąże się z odległymi lokalizacjami i rozległymi terenami. Tworząc koncepcję ochrony tego typu miejsc, należy uwzględnić wiele aspektów, innych rozwiązań potrzebujemy do ochrony perymetrycznej, inne rozwiązanie będzie potrzebne, by zabezpieczyć teren wewnątrz oraz budynki.



Dużym wyzwaniem jest ochrona tego typu miejsc przed intruzami, gdyż z jednej strony mamy do czynienia z bardzo długą linią ogrodzeń, z drugiej – są to miejsca niezwykle istotne dla właściwego funkcjonowania gospodarki. Podstawowymi celami systemów bezpieczeństwa w tych instytucjach są ochrona przed wtargnięciem osoby nieuprawnionej na ich teren oraz zapewnienie ciągłości świadczonych usług. Z tego też względu w celu ochrony obiektów przemysłowych są wykorzystywane coraz bardziej zaawansowane technologie łączące różne sposoby detekcji i analizy zachowań.

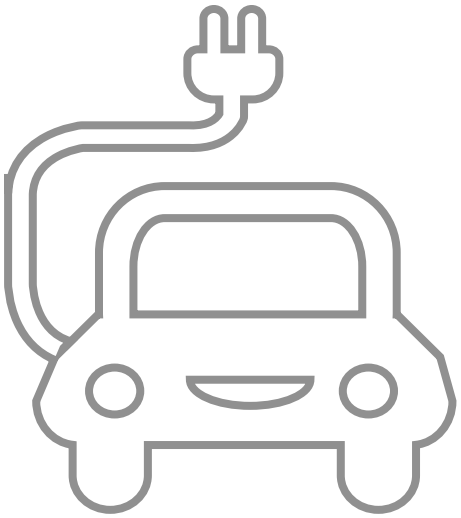
Nadrzędnym celem jest ochrona obwodowa, która ma za zadanie powstrzymać i zapobiec przedostaniu się „nieproszonych gości" na teren obiektu. Pomocne w tym może być zintegrowane rozwiązanie łączące kamerę z radarem o wąskim polu widzenia. Dzięki temu możemy skutecznie chronić długie linie ogrodzeń w każdych warunkach atmosferycznych, gdzie radar wykrywa, a kamera identyfikuje zagrożenie. Innym rozwiązaniem mogą być kamery termowizyjne z analityką.

Kolejną linią ochrony jest teren pomiędzy ogrodzeniem a obiektem wewnątrz. W tym zakresie z pomocą mogą przyjść również radary, ale połączone z kamerami wieloprzetwornikowymi i kamerami PTZ. Dzięki temu mamy możliwość śledzenia intruza i skutecznej interwencji ochrony.

Natomiast wewnątrz budynków obiektu przemysłowego sprawdzą się kamery wieloprzetwornikowe, które gwarantują doskonały ogląd sytuacji z wykorzystaniem niewielkiej liczby urządzeń.

Dodatkowym elementem w systemie bezpieczeństwa coraz częściej jest nagłośnienie, które umożliwia odstraszanie intruzów, zanim przekroczą ogrodzenie, dzięki komunikatom nagranym lub nadawanym „na żywo". Nagłośnienie może być wykorzystywane również jako skuteczne narzędzie do komunikacji z pracownikami.

→



Marcin Walczuk
BCS

Skuteczne bezpieczeństwo = kompleksowe podejście

Specyfiką obiektów przemysłowych czy rozproszonych jest to, że najczęściej zajmują duże powierzchnie, składają się z wielu budynków i elementów infrastruktury (często w różnych lokalizacjach). Zabezpieczanie przed zagrożeniami zewnętrznymi i wewnętrznymi takich obiektów, jak elektrownie, rafinerie, fabryki, magazyny, farmy wiatrowe, sieci energetyczne czy gazociągi jest nie lada wyzwaniem dla ich właścicieli i zarządców. Zagrożenia te mogą mieć negatywny wpływ na bezpieczeństwo pracowników, procesy przemysłowe, jakość produktów, środowisko naturalne i ciągłość działania organizacji.

Aby zapewnić skuteczne bezpieczeństwo tego typu obiektów, należy zastosować kompleksowe podejście oparte na trzech elementach kluczowych: kosztach, celach i zarządzaniu ryzykiem. Koszty oznaczają dostosowanie środków bezpieczeństwa w inwestycji do przewidywanych korzyści i strat. Cele oznaczają precyzyjne określenie funkcji systemu bezpieczeństwa, który nie powinien spełniać tylko funkcji chroniącej przed nieuprawnionym dostępem, ale także zapewniać utrzymanie ciągłości działania organizacji. Zarządzanie ryzykiem oznacza identyfikowanie zagrożeń, ocenianie ich prawdopodobieństwa i wpływu na procesy oraz ustalanie i wdrażanie standardów bezpieczeństwa.

System bezpieczeństwa obiektów przemysłowych i rozproszonych powinien być zintegrowany i obejmować różne aspekty: fizyczny (np. ogrodzenia, zamki, bariery), techniczny (np. kamery, czujniki, alarmy), organizacyjny (np. procedury, szkolenia, komunikacja) i cybernetyczny (np. szyfrowanie, firewall, backup). Najlepiej, aby taki system był możliwie jak najbardziej elastyczny i mógł dostosowywać się do zmieniających się warunków i potrzeb, a jego monitorowanie oraz kontrola powierzona odpowiednio wykwalifikowanemu personelowi.

Bezpieczeństwo takich obiektów jest bardzo ważnym zagadnieniem dla sektora zarówno prywatnego, jak i publicznego. W dobie globalizacji, cyfryzacji i niestabilności politycznej jest to również zagadnienie strategiczne dla bezpieczeństwa narodowego i międzynarodowego. Dlatego warto inwestować w nowoczesne rozwiązania i najlepsze praktyki w tym obszarze.

Tomasz Guzikowski
CIECH GROUP

Kluczem jest wiedza i zrozumienie

Bezpieczeństwo obiektów przemysłowych jest pojęciem bardzo szerokim i obejmującym swoim zakresem obszary, które na pierwszy rzut oka mogą się wydawać ze sobą niepowiązane. Oczywiście bardzo dużo zależy od charakteru zakładu produkcyjnego, jego wielkości i skomplikowania procesów technologicznych, ale również występujących w nim zagrożeń, stosowanych substancji niebezpiecznych i ich ilości oraz wielu innych czynników.

Security Manager musi się wykazać przede wszystkim bardzo dobrą znajomością nie tylko samej infrastruktury zakładu produkcyjnego, zagrożeń wynikających z uwarunkowań fizycznych i technicznych w zakresie bezpieczeństwa osób i mienia, ale również procesów technologicznych, powiązań pomiędzy poszczególnymi instalacjami i ich współzależnością. Musi znać również na tyle dobrze organizację i posiadać takie kompetencje, aby w sposób płynny poruszać się pomiędzy bardzo często sprzecznymi interesami, jakimi czasami są poziom produkcji vs. jej bezpieczeństwo.

Musi umieć wykazać zależność, która w sposób jasny i poparty konkretnymi wyliczeniami wskazuje na bezpośredni wpływ wzrostu poziomu bezpieczeństwa na wyniki finansowe zakładu produkcyjnego. A to nie zawsze wydaje się takie oczywiste. Często trudno jest przekonać osoby decyzyjne, iż inwestycja w poprawę bezpieczeństwa w perspektywie czasu przełoży się na zmniejszenie liczby awarii, obniżenie przestojów i zaniżeń produkcyjnych, wydłużenie okresu pomiędzy postojami czy chociażby na wizerunek u dostawców i odbiorców. Nie wspominając już o tak oczywistej obecnie rzeczy, jak możliwość optymalizacji samej ochrony fizycznej, której koszty z roku na rok są coraz wyższe, za pomocą najnowszych rozwiązań techniki, tym bardziej iż obecne rozwiązania dają wiele możliwości analitycznych, począwszy od analizy obrazu, poprzez odczyt temperatury, drgań, a na integracji wielu systemów bezpieczeństwa skończywszy.

Kluczem jest to, aby umieć wykorzystać tę wiedzę do stworzenia systemu optymalnego, w którym poniesione koszty będą adekwatne do osiągniętych korzyści.

Tomasz Olejniczak
HIKVISION POLAND

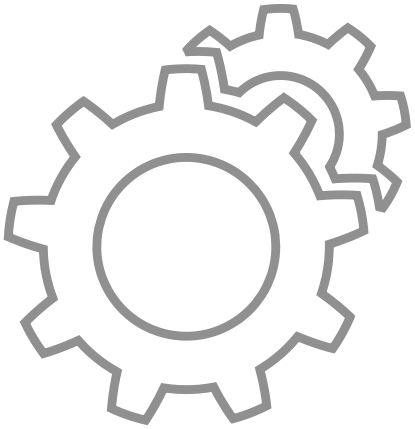
Bezpieczne ekosystemy

W *Opowieści o dwóch miastach* Karol Dickens napisał: *Była to najlepsza i najgorsza z epok, wiek rozumu i wiek szaleństwa, czas wiary i czas zwątpienia, okres światła i okres mroków, wiosna pięknych nadziei i zima rozpaczy.*

Czas, w jakim żyjemy, może stać się „(…) wiosną pięknych nadziei (…)" dla biznesu. Aby tak się stało, biznes powinien być bezpieczny. W celu zabezpieczenia zmieniającego się środowiska pracy firma Hikvision korzysta w swoich urządzeniach z analizy obrazu opartej na sieciach neuronowych głębokiego uczenia (AIoT). Analityka pozwala powiadamiać o potencjalnie niebezpiecznych sytuacjach wewnątrz (wypadki, zasłabnięcia, brak środków ochrony osobistej, wycieki niebezpiecznych substancji, wzrost temperatury urządzeń elektrycznych itp.) oraz chronić zakład na zewnątrz przed niepowołanym wtargnięciem. Rozwiązania AIoT wdrażają także zabezpieczenia przed atakami sieciowymi (*ZeroTrust,* BOM), poprawiając bezpieczeństwo całej sieci wewnątrzzakładowej.

Podniesienie poziomu bezpieczeństwa to dziś konieczność. Można to osiągnąć przede wszystkim przez zmianę podejścia. Systemy SDK,VSS, I&HAS, SSP powinny uzupełniać się i wymieniać dane, zwiększając świadomość operatorów o stanie obiektu. W systemach zabezpieczeń przeniesienie przetwarzania dużej ilości danych na poziom urządzeń (AI) oraz korzystanie z oprogramowania DSS (System Wspomagania Decyzji) pozwala na prewencję i wspieranie podejmowania decyzji w sytuacji zagrożenia.

Do zabezpieczenia materiału wideo warto stosować najnowsze rozwiązania, nnp. jednocześnie funkcję ANR (automatyczna synchronizacja nagrań zapisanych na karcie SD w kamerze z rejestratorem po przywróceniu połączenia), funkcja failover, dostępna w profesjonalnych urządzeniach i pozwalająca na zastosowanie nadmiarowego urządzenia, które przejmie nagrywanie wszystkich kamer z dowolnego uszkodzonego rejestratora, oraz RAID (*Redundant Array of Independent Disks* – macierz dysków tworząca jedną przestrzeń pamięci masowej odporną na uszkodzenie jednego lub wielu dysków). Dla zapewnienie dynamicznego skalowania zasobów i nieprzerwanego dostępu do systemu dla operatorów oprogramowanie zarządzające powinno umożliwiać pracę w środowisku IaaS Microsoft Azure, Amazon AWS lub na maszynach wirtualnych, np. Vmware, Hyper-V. Projektowanie systemów zabezpieczeń zgodnie z obowiązującymi normami zapewnia optymalny dobór rozwiązań, jednocześnie podnosząc bezpieczeństwo.



Wincenty Ignatowski
CEMEX

Wyzwania Security Managera

Obecnie bardziej niż kiedykolwiek bezpieczeństwo stało się ważnym aspektem naszego życia prywatnego i zawodowego. Szczególnego znaczenia nabiera zapewnienie bezpieczeństwa w zakładzie przemysłowym. Zatem priorytetem dla każdego Security Managera powinno być nieustanne przekonanie, że sprawne działanie systemu zabezpieczeń leży w interesie całej społeczności każdego przedsiębiorstwa.

Przed Security Managerem stoi dziś wiele wyzwań. Jednym z najważniejszych z całą pewnością jest dbałość o cyberbezpieczeństwo. Wiedza o cyberzagrożeniach jest niewątpliwie specjalistyczna, ale nie oznacza to, że należy ją pozostawić w gestii informatyków. Wręcz przeciwnie, wymagania dotyczące cyberbezpieczeństwa, a dokładnie rzecz ujmując, zarządzanie nim powinno być powierzone osobie odpowiadającej za całość bezpieczeństwa w przedsiębiorstwie. W definicji cyberbezpieczeństwa mieści się nie tylko technologia, lecz także cały proces, który kontroluje i ochrania sieć, programy oraz urządzenia. Najważniejszym celem zapewnienia bezpieczeństwa w sieci jest zmniejszenie ryzyka ataków cybernetycznych oraz skuteczna ochrona przed nieuprawnionym wykorzystaniem danych i programów.

Jest wiele składowych cyberbezpieczeństwa, o które powinien zadbać Security Manager. Jedną z ważniejszych jest opracowaniu programu bezpiecznego miejsca pracy. Dzięki niemu można ograniczyć i złagodzić ryzyko związane z wyciekiem informacji, kradzieżą danych i szpiegostwem korporacyjnym, zapewnić ochronę informacji i know-how firmy, własności intelektualnej i danych poufnych, osobowych oraz zapobiec celowym i niezamierzonym naruszeniom.

Podczas tworzenia programu bezpiecznego miejsca pracy Security Manager powinien skoncentrować się na siedmiu podstawowych obszarach:

1. Inżynierii społecznej.
2. Polityce „czystego biurka".

→

3. Dokumentach pozostawionych bez nadzoru.
4. Zachowaniu prywatności w miejscach publicznych.
5. Dbałości o świadome i bezpieczne korzystanie z urządzeń zewnętrznych podłączanych za pośrednictwem portów USB.
6. Kontroli dostępu do biur i tzw. pomieszczeń wrażliwych (serwerownie, archiwa, sterownie produkcyjne itp.).
7. Zachowaniu poufności dokumentów i ich klasyfikowaniu oraz właściwym oznakowaniu.

Wprowadzając program bezpiecznego miejsca pracy, Security Manager powinien posłużyć się metodologią polegającą m.in. na:

- budowaniu świadomości wszystkich pracowników przedsiębiorstwa w zakresie inżynierii społecznej poprzez m.in. szkolenia,
- utrzymaniu zgodności z zasadami czystego biurka poprzez kampanie komunikacyjne,
- unikaniu podłączania urządzeń zewnętrznych (USB, ładowarek bezprzewodowych itp.) do laptopów i komputerów stacjonarnych,
- udzielaniu wskazówek dotyczących ochrony danych podczas podróży służbowych,
- wdrożeniu systemów kontroli dostępu w biurach i zakładach produkcyjnych (punkty dostępu lub wejścia do biur, pomieszczeń kontrolnych, serwerów itp.).

Jeżeli któryś z ww. obszarów zostanie zaniedbany, może się to skończyć dużymi stratami dla zakładu przemysłowego. Boleśnie przekonał się o tym jeden z czołowych na świecie producentów materiałów budowlanych, który pod koniec maja br. padł ofiarą cyberataku. Wpłynęło to negatywnie na działalność firmy, a skutki odczuło kilka krajów w Europie. Potwierdzono, że operacje biznesowe zostały zakłócone w części zarówno produkcyjnej, jak i sprzedażowej.

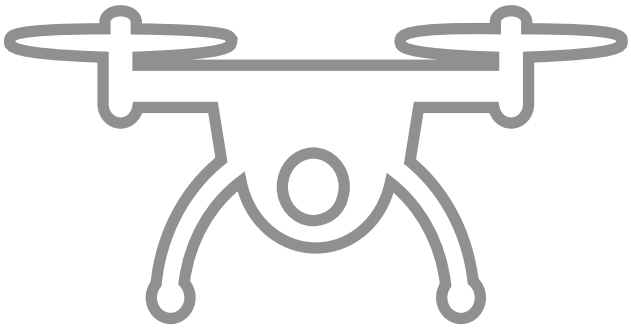
Dlatego intencją wprowadzenia programu bezpiecznego miejsca pracy, w którego procesie Security Manager powinien odgrywać rolę lidera, jest zwiększenie odporności przedsiębiorstwa i wspieranie celów strategicznych firmy.

Artur Nowakowski
LINC POLSKA

Sojusznik czy intruz?

Chyba nie ma osoby, która nie wiedziałaby, czym jest dron. UAV to bezzałogowy statek powietrzny, który jest częścią UAS, bezzałogowego systemu powietrznego, składającego się zarówno z drona, jak i operatora wraz z narzędziami i oprogramowaniem używanym do jego obsługi.

Od powszechnie dostępniej zabawki drony przeistoczyły się w narzędzia wykorzystywane do najróżniejszych celów – również strategicznych. Najbardziej popularną branżą, która nie może obyć się już bez z tych urządzeń, jest branża filmowa. Ale poza rozrywką istnieje cała gama rozwiązań, w których są stosowane bezzałogowe statki powietrzne. Już w 2014 r. w Słowińskim Parku Narodowym



używano dronów do liczenia dzikiej zwierzyny, a dzięki wykorzystaniu termowizji możliwe było skuteczne wykrywanie jeleni w trudno dostępnych miejscach, np. na bagnach. Obrazowanie termowizyjne jest wykorzystywane również w sektorze przemysłowym do nadzorowania i ochrony napowietrznych linii elektrycznych, farm fotowoltaicznych czy trakcji kolejowych. Kolejnym przykładem wykorzystania dronów są działania ratownicze czy mające na celu monitorowanie granic – wykrywanie ludzi w lasach oraz innych trudno dostępnych miejscach.

Bezzałogowe statki powietrzne są bardzo pomocne w wykrywaniu nieprawidłowości i nadużyć, np. straż miejska wyposażona w takie urządzania skutecznie odnajduje źródła generujące zanieczyszczenia, a policja wychwytuje piratów drogowych. Znane są też rozwiązania, w których UAV wykorzystuje się do transportu krwi czy leków pilnie potrzebnych przy operacjach ratujących życie.

Te małe latające platformy niosą wiele korzyści, jeżeli jednak trafią w niepowołane ręce z przydatnych i użytecznych przekształcają się w niebezpieczne i zagrażające porządkowi publicznemu.

W ostatnim czasie było kilka przypadków, kiedy drony pojawiły się w bliskiej okolicy lotnisk, w zamkniętej dla nich przestrzeni powietrznej, stając się tym samym poważnym zagrożeniem dla samolotów i pasażerów. Dron przeznaczony do transportu towarów z powodzeniem może zostać użyty do przenoszenia ładunków wybuchowych, co niejednokrotnie miało już miejsce podczas wojny w Ukrainie.

Tak więc z całą odpowiedzialnością można powiedzieć, że zagrożenie ze strony bezzałogowych statków powietrznych jest realne, a konsekwencje zdarzeń z dronami mogą być bardzo poważne. Dlatego istotne jest, aby kluczowe obiekty państwowe oraz infrastruktura krytyczna były odpowiednio zabezpieczone. Pierwszym elementem takiego systemu jest wczesne wykrywanie i identyfikowanie dronów. Do tego celu stosuje się systemy radarowe 3D wspomagane kamerami zarówno światła widzialnego, jak i termowizyjnymi. Umożliwiają nie tylko wczesne wykrycie UAV, ale również jego śledzenie oraz obserwację. Dzięki technologii Microdoppler można je szczegółowo identyfikować i bardzo precyzyjnie lokalizować.

Dzięki tego typu danym pracownicy ochrony mają informacje, aby podejmować dalsze czynności związane z unieszkodliwieniem drona. Ale trzeba pamiętać, że do tego celu poza możliwościami technicznymi potrzebna jest znajomość odpowiednich regulacji prawnych. Obecnie zagłuszacze (*jammer*) czy inne rozwiązania przechwytujące są w zasadzie niedostępne dla odbiorcy komercyjnego. Należy zatem zastanowić się nad stworzeniem właściwych przepisów, które umożliwią skuteczną obronę przed dronami. ●

MOTOROLA SOLUTIONS NEXUS iPRO megavision technology

Megavision Technology ogłasza premierę na polskim rynku nowej linii produktowej profesjonalnych kamer wysokich rozdzielczości NEXUS iPRO

Kamery produkowane są w Korei Południowej zgodnie z wymogami NDAA oraz TAA zapewniając tym samym najwyższy poziom bezpieczeństwa dla użytowników

venompsim.pl

Atak dronów

Nie ma wątpliwości, że drony znacząco ułatwiają ochronę obwodową, szczególnie w przypadku obiektów o infrastrukturze rozproszonej. A co się stanie, kiedy drony zostaną wykorzystane przez ciemną stronę mocy? Czy polskie firmy są na taki scenariusz przygotowane? Jak się bronić przed atakiem dronów?

Monika Żuber-Mamakis

Dron dronowi nierówny. Jedne to niewinne, w zasadzie dziecięce zabawki, inne z sukcesem są wykorzystywane jako groźna broń. Mówiąc „dron", najczęściej mamy na myśli bezzałogowy statek powietrzny. Nie zapominajmy jednak, że istnieje też kategoria dronów, które doskonale sobie radzą pod wodą. W obu przypadkach mogą zarówno służyć do ochrony obiektów przemysłowych, jak i stać się skutecznym narzędziem atakującym lub szpiegującym. Jak temu zapobiec?

Nim przejdziemy do współczesnych zastosowań dronów, czyli bezzałogowych statków powietrznych *(Unmanned Aerial Vehicle – UAV)*, a przede wszystkim temu, jak radzić sobie z zagrożeniami, jakie mogą im towarzyszyć, przyda się kilka słów o samych dronach. Przy okazji małe wyjaśnienie: w polskiej nomenklaturze występuje też akronim BSP, my jednak pozostaniemy przy lepiej rozpoznawalnym UAV, skoro nawet twórcy Prawa lotniczego się nim posługują.

Skąd się wzięły trutnie

Termin „dron" pojawił się naszym języku stosunkowo niedawno. Przed dwunastoma laty na pytanie, jak odmieniać „dron czy drona", odpowiedzi udzielił, w ramach Poradni językowej PWN, prof. Mirosław Bańko: *Jak się przekonałem, w mediach przeważa forma męska, ściślej – męskozwierzęca, czytamy bowiem np. „USA straciły kolejnego drona" (jak kolejnego trutnia), a nie „USA straciły kolejny dron"*. Już z tego można wnioskować, że drony są w naszej rzeczywistości zjawiskiem stosunkowo młodym.

Profesor M. Bańko zapewne nie bez powodu przytoczył przykład z trutniem. Otóż *drone* w języku angielskim oznacza „truteń". Tej nazwy użyli już w roku 1935 konstruktorzy z brytyjskiej wytwórni lotniczej de Havilland. Kiedy w 1931 r. brytyjskie Ministerstwo Lotnictwa *(Air Ministry)* złożyło zamówienie na samolot sterowany radiem, który miał służyć jako cel podczas szkoleń artylerzystów brytyjskiej armii oraz królewskiej marynarki, siłą rzeczy musiał być to samolot bezzałogowy. W ten oto sposób w roku 1935 na bazie samolotu de Havilland DH-60T „Tiger Moth" powstał model bezzałogowy DH.82 „Queen Bee", czule nazywany przez twórców trutniem, czyli… dronem.

→

Mniej więcej w tym samym czasie statkami bezzałogowymi zajął się inny Brytyjczyk, Reginald Denny. Zajmował się on sprzedażą zabawek, a dokładnie sterowanych radiowo modeli samolotów. R. Denny wpadł na pomysł, by zabawkowe samoloty zdecydowanie powiększyć, by mogły stać się celem ćwiczebnym dla wojsk przeciwlotniczych. W roku 1935 firma Reginald Denny Industries zaprezentowała prototyp drona – RP-1, czyli Radioplane One. Denny był o tyle skutecznym sprzedawcą, że choć jego samolot nie do końca poradził sobie podczas prezentacji dla amerykańskiej armii, wojsko podpisało umowę na kolejne trzy prototypy.

Jednak Brytyjczycy wcale nie byli pierwsi. Tak naprawdę palmę pierwszeństwa należałoby wręczyć genialnemu Nikoli Tesli. To właśnie on we wrześniu 1898 r. zaprezentował na pierwszej Wystawie Elektrycznej w Madison Square Garden nowy wynalazek, który nazwał teleautomatonem. Było to pierwsze w historii urządzenie sterowane radiowo. Teleautomaton został zamontowany w niewielkiej łodzi zasilanej przez akumulatory umieszczone w kadłubie. Odbiornik radiowy zamontowany w modelu był połączony ze śrubą napędową, sterem kierunkowym i zanurzenia. Teleautomaton nie zrobił furory. Pech Tesli polegał na tym, że jak zawsze wyprzedził swoje czasy. W tym przypadku miał choć tyle szczęścia, że udało mu się wynalazek opatentować (nr patentu: US613,809). To tyle historii, a jak wygląda „bezzałogowa" teraźniejszość?

Po jasnej stronie mocy

Drony, pierwotnie przeznaczone do zastosowań wojskowych, z czasem weszły do użytku cywilnego. Są więc drony transportowe, rolnicze, meteorologiczne oraz wykorzystywane przez służby ratunkowe i leśne. Niektóre mapują teren, wspomagając geodetów, inne nadzorują uprawy i oczywiście stanowią doskonałe uzupełnienie ochrony perymetrycznej obiektów przemysłowych. Wraz z coraz szerszym wachlarzem zastosowań rośnie gama modeli dronów konsumenckich. Po niebie pomykają więc trikoptery, quadkoptery, heksakoptery lub oktokoptery z odpowiednio: 3, 4, 6 lub 8 wirnikami. Ich cena zależy od różnych cech urządzenia, takich jak jego rozmiar, liczba czujników i rodzaj wyposażenia, a także od zastosowanych baterii i trybu lotu. Jednak eksperci wskazują, że urządzenia te tanieją ze względu na niższe koszty produkcji i malejące ceny materiałów. Oczywiście z zastrzeżeniem, że ten trend nie dotyczy dronów wojskowych.

Rosnąca popularność dronów powoduje, że wg raportu firmy MarketsandMarkets dla globalnego rynku produkcji dronów prognozowany wzrost CAGR (skumulowany wskaźnik wzrostu roczny) wyniesie ok. 13% w okresie prognozy 2019–24. Z kolei analitycy z Emergen Research skupili się na wartości globalnego rynku dronów wykorzystywanych do inspekcji i monitoringu. Uważają, że w latach 2021–30 zwiększy się ona z 10 do 36 mld USD, co przełoży się na średni coroczny wzrost na poziomie 16%.

O ocenę wartości polskiego rynku dronów pokusiło się w 2019 r. Ministerstwo Infrastruktury, które wraz z Polskim Instytutem Ekonomicznym opracowało *Białą księgę rynku bezzałogowych statków powietrznych.* Pracujący nad publikacją eksperci szacują, że wartość polskiego rynku dronów wyniesie do 2026 r. 3,26 mld zł, ale efekt dla całej gospodarki może sięgać nawet 576 mld zł wg scenariusza umiarkowanego. PIE zwraca także uwagę na tendencje rozwojowe lotnictwa bezzałogowego, które podlega szybkiej automatyzacji, kreując nowy wymiar Internetu rzeczy w przestrzeni powietrznej, tzw. U-space.

To oczywiste, że drony znakomicie sprawdzają się w ochronie obwodowej. Zapewniają lepszy zasięg i szybszy czas reakcji. Korzystanie z nich zmniejsza koszty związane z ochroną fizyczną obiektu. Mówiąc wprost, pozwala na zmniejszenie liczby osób patrolujących teren. Co jednak się stanie, kiedy wrogie drony naruszą granicę obiektu? Co zrobić, by do tego nie dopuścić?

Mroczne widmo

Rozwój technologii udoskonalających funkcjonowanie bezzałogowych statków powietrznych to dla wielu gałęzi gospodarki dobrodziejstwo. Niestety, to tylko jedna strona medalu. Drugą jest zastosowanie dronów do szpiegowania, przemytu, transportu broni i innych niecnych zadań.

Nie każdy przykład użycia UAV musi mieć wojnę w tle. I tak 15 września 2013 r. podczas wiecu wyborczego w Dreźnie mały kwadrokopter przeleciał niedaleko kanclerz Niemiec Angeli Merkel i ministra obrony Thomasa de Maiziere'a, zawisając przez chwilę przed obojgiem, by po chwili spaść u stóp Merkel. Nie był to atak. W ten sposób Niemiecka Partia Piratów próbowała zwrócić uwagę na fakt, że bez odpowiednich regulacji łatwo doprowadzić do sytuacji, gdy drony z jednej strony będą ingerować w życie prywatnych ludzi, z drugiej – mogą prowadzić do ograniczenia swobód obywateli.

Niespełna pięć lat później, 4 sierpnia 2018 r. dwa drony zdetonowały materiały wybuchowe w pobliżu Avenida Bolívar w Caracas, gdzie prezydent Wenezueli Nicolás Maduro przemawiał do Boliwariańskiej Gwardii Narodowej przed Centro Simón Bolívar Towers i Palacio de Justicia de Caracas. To chyba jeden z najbardziej spektakularnych przykładów zastosowania dronów nie bezpośrednio na polu walki, choć przeciwko politycznemu antagoniście. Prezydent Maduro z tego ataku wyszedł cało.

Drony są coraz częściej wykorzystywane przez gangi i organizacje terrorystyczne. Przestępcy używają ich do przemytu nielegalnych substancji, organizacje terrorystyczne, takie jak ISIS, również zaopatrzyły się drony, tyle że uzbrojone. W USA problemem jest

Dron, jaki jest, każdy widzi

- Bezzałogowy statek powietrzny, BSP *(Unmanned Aerial Vehicle* – UAV) lub bezzałogowy system powietrzny *(Unmanned Aerial System* – UAS), zwany też dronem, to statek powietrzny, który nie wymaga do lotu załogi obecnej na pokładzie oraz nie ma możliwości zabierania pasażerów, pilotowany zdalnie lub wykonujący lot autonomicznie.
- Polskie prawo nie definiuje, czym jest dron, ale bezzałogowy statek powietrzny pojawił się w znowelizowanej w 2011 r. ustawie Prawo lotnicze. W myśl art. 126 tejże ustawy „w polskiej przestrzeni powietrznej mogą być wykonywane loty bezzałogowych statków powietrznych", a „bezzałogowy statek powietrzny (UAV) musi być wyposażony w takie same urządzenia umożliwiające lot, nawigację i łączność jak załogowy statek powietrzny wykonujący lot z widocznością (VFR) lub według wskazań przyrządów (IFR) w określonej klasie przestrzeni powietrznej. Odstępstwa mające zastosowanie w tym zakresie dla załogowych statków powietrznych stosuje się jednakowo do bezzałogowych statków powietrznych (UAV)".

kontrabanda przenoszona drogą powietrzną. Władze tego kraju od ok. 2013 r. walczą z nielegalnymi dostawami do więzień dokonywanych drogą powietrzną, i nadal z problemem się nie uporały. Podobne przypadki miały miejsce również we Włoszech i Francji. Oprócz przenoszenia ładunków lub monitorowania wrażliwych miejsc drony mogą być również wykorzystywane jako punkty wyjścia dla ataków przeciwko cyberbezpieczeństwu, stanowiąc tym samym zagrożenie bezpieczeństwa fizycznego, wywiadowczego i cyfrowego, co stwarza złożony dylemat bezpieczeństwa.

Akcja wywołuje reakcję

Ataki dronów mogą stanowić zagrożenie dla wielu branż i przedsiębiorstw, tych o znaczeniu zarówno krytycznym, jak i nie. Zresztą, jak zauważa Jacek Grzechowiak w tekście *Infiltracja, sabotaż i akty terrorystyczne – nie tylko przemysł obronny musi być na to gotowy na str. 32*, to w istocie przestępcy decydują o tym, jaki obiekt ma znaczenie krytyczne. Drony mogą nie tylko szpiegować to, co dzieje się na terenie infrastruktury krytycznej, ale także infiltrować tereny przygraniczne, wywoływać niepokoje podczas dużych wydarzeń, służyć do przemytu.

Zwiększenie sprzedaży dronów na całym świecie przekłada się na wzrost ryzyka naruszenia prywatności, zagraża szczelności granic państwowych, wpływa na bezpieczeństwo lotnisk i ułatwia nielegalne filmowanie obiektów IK. Skutkiem jest wzrastający popyt na systemy antydronowe. To zaś powoduje, że tak jak rośnie wartość rynku produkcji dronów, tak też rośnie wartość rynku systemów antydronowych. Według analiz MarketsandMarkets globalny rynek systemów C-UAV osiągnie w roku 2027 wartość ok. 3,8 mld USD, co zważywszy na fakt, że w roku 2023 wartość ta oceniana jest na 1,47 mld USD, daje CAGR wynoszący 27,7%.

Nowa nadzieja, czyli systemy antydronowe

Aby przeciwdziałać zagrożeniom, potrzebny jest dobry system antydronowy, skutecznie wykrywający bezzałogowe statki powietrzne. Powinien on przede wszystkim błyskawiczne reagować na UAV próbujące naruszyć chroniony obszar i albo zakłócić ich działanie, albo je zneutralizować. Celem jest uniemożliwienie dronowi wypełnienia jego misji, niezależnie od tego, czy jest nią obserwacja, gromadzenie danych wywiadowczych, czy przeprowadzenie ataku. Wielowarstwowy mechanizm obronny, na który składają się wykrywanie, weryfikacja, śledzenie i neutralizacja wrogiego UAV, ma kluczowe znaczenie, niezależnie od tego, czy chodzi o zagrożenia dalekiego, czy krótkiego zasięgu, stacjonarne czy mobilne.

Należy jednak pamiętać, że w Polsce neutralizacja zagrożenia ze strony UAV obwarowana jest kilkoma warunkami przewidzianymi w art. 126a Prawa lotniczego. Trzeba przyznać, że jest to artykuł →

» Eksperci PIE szacują, że wartość polskiego rynku dronów wyniesie do 2026 r. 3,26 mld zł, ale efekt dla całej gospodarki może sięgać nawet 576 mld zł wg scenariusza umiarkowanego. «

stosunkowo pojemny i dający spore pole manewru co do zwalczania wrogich urządzeń. Wystarczy, by dron np. stwarzał zagrożenie dla chronionych obiektów, urządzeń lub obszarów, zakłócał przebieg imprezy masowej albo zagrażał bezpieczeństwu jej uczestników bądź wywoływał uzasadnione podejrzenie, że może zostać użyty jako środek ataku terrorystycznego.

Ważniejsze jest jednak to, że nie każdy, komu nie podoba się dron latający nad posesją, może próbować go uziemić. Ustawa mówi wprost, że uprawnieni są do tego, w zależności od rodzaju zagrożenia, funkcjonariusze policji, Straży Granicznej, Służby Ochrony Państwa, ABW, Agencji Wywiadu, CBA, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego, Służby Celno-Skarbowej i Służby Więziennej, Straży Marszałkowskiej, żołnierze Żandarmerii Wojskowej i Sił Zbrojnych RP oraz pracownicy specjalistycznych uzbrojonych formacji ochronnych. Przeciętny Kowalski do czegoś, co bzyczy mu nad głową, strzelać nie może. Nawet z procy.

A z jakich urządzeń mogą korzystać uprawnione podmioty? Otóż same urządzenia można podzielić na dwa główne rodzaje: sprzęt do monitorowania dronów może być bowiem pasywny (np. tylko nasłuch) lub aktywny (wysyłanie sygnału i analizowanie danych zwrotnych). Może oferować kilka funkcji, choć niekoniecznie wszystkie jednocześnie:

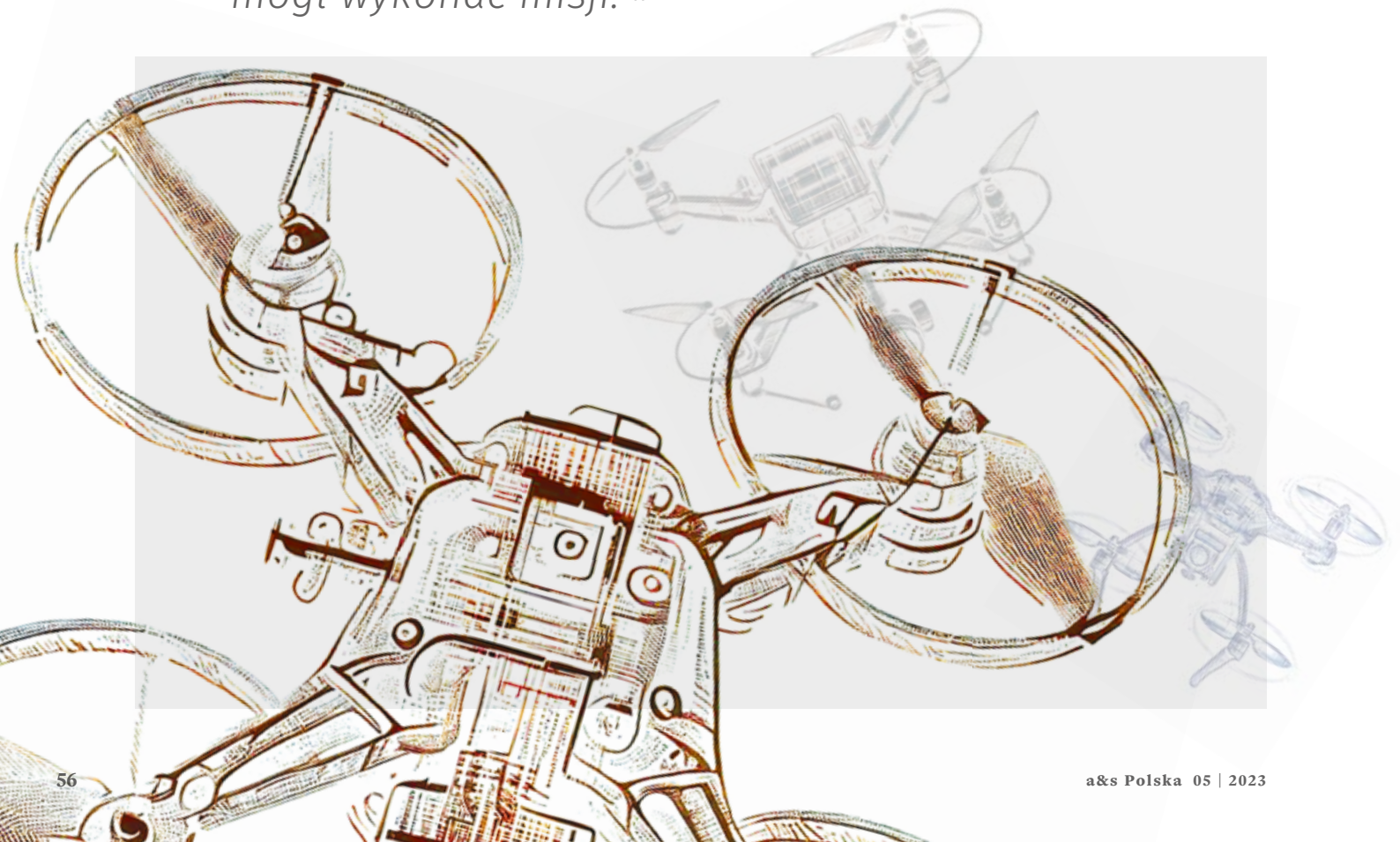
1. wykrywanie intruza,
2. rozpoznanie rodzaju UAV,
3. zlokalizowanie i śledzenie,
4. powiadamianie o zagrożeniu.

Samo wykrycie zagrożenia to zwykle za mało. Przydatna jest też klasyfikacja wykrytego obiektu. Technologia, która klasyfikuje drony, zwykle będzie w stanie oddzielić drony od innych typów obiektów, np. ptaków czy samolotów. Identyfikacja pozwala poznać konkretny model urządzenia, w niektórych przypadkach nawet adres MAC. Już otrzymanie powiadomienia, że nad chronionym obiektem pojawił się dron-intruz, jest przydatne. Ale znacznie lepsze jest, jeśli system antydronowy poda dokładną lokalizację statku powietrznego i jego operatora.

Występują cztery główne rodzaje urządzeń monitorujących przestrzeń i wykrywających bezzałogowe statki powietrzne:

- **Analizatory częstotliwości radiowej (radionamierniki, RF)** – składają się z jednej lub więcej anten odbierających fale radiowe i procesora analizującego widmo RF. Są one używane do wykrywania komunikacji radiowej między dronem a jego operatorem. Niektóre systemy są w stanie rozpoznawać marki i modele dronów, a niektóre zidentyfikować adresy MAC drona i operatora (jeśli komunikacja przebiega przez Wi-Fi). Niektóre wysokiej klasy systemy mogą za pomocą triangulacji określić położenie oraz szybkość i kierunek lotu urządzenia.
- **Czujniki akustyczne (mikrofony)** – mikrofon lub układ

» Wykryty dron powinien zostać zneutralizowany, co nie oznacza, że zniszczony (choć polskie prawo na to pozwala), lecz doprowadzony do tego, by nie mógł wykonać misji. «



mikrofonów odbiera dźwięk wydawany przez lecący dron i na podstawie natężenia tego dźwięku wylicza kierunek lotu.

- **Wizualny system detekcji (kamery)** – w momencie wykrycia intruza automatycznie skierowują obiektyw w jego stronę. Współczesne kamery o dużej mocy przetwarzania, wyposażone w oprogramowanie bazujące na algorytmach AI mogą zbierać światło widzialne o różnej długości fal, w tym podczerwone, a także promieniowanie termiczne. Obraz z kamery pozwala obsłudze zorientować się, czy np. intruz nie oznacza dodatkowego zagrożenia, choćby w postaci niesionego ładunku wybuchowego.
- **Radary do wykrywania UAV można podzielić ze względu na zasięg** – radary o zasięgu 4D, radary dopplerowskie są przeznaczone do wykrywania bezzałogowych statków powietrznych na dużych odległościach; radary dookólne 3D to urządzenia średniego zasięgu przeznaczone do wykrywania i śledzenia dronów elektronicznie skanowaną wiązką (zasięg wykrywania do kilkunastu kilometrów); radary sektorowe 3D (małego zasięgu) pozwalają na zabezpieczenie obszarów infrastruktury krytycznej, wykrywanie i śledzenia niepożądanych UAV (zasięg działania to najczęściej kilka kilometrów).

Wykryty dron powinien zostać zneutralizowany, co nie oznacza, że zniszczony (choć polskie prawo na to pozwala), lecz doprowadzony do tego, by nie mógł wykonać misji. Inną opcją jest przejęcie kontroli nad dronem, który może dostarczyć ciekawych informacji.

Jest kilka sposobów na neutralizację dronów. Należą do nich:

- **Zagłuszanie (zakłócanie) fal radiowych za pomocą tzw. jammera (zagłuszacza lub zakłócacza)** – w celu zablokowania komunikacji pomiędzy urządzeniem a operatorem *jammer* RF przesyła sygnały o bardzo dużej mocy, na tej samej częstotliwości, na które prowadzona jest komunikacja z dronem. Z tej metody korzystają różnego rodzaju neutralizatory ręczne.
- ***Spoofing* (fałszowanie) danych GPS** to próba oszukania odbiornika GPS zamontowanego w dronie poprzez wyemitowanie fałszywego sygnału GPS. Dron traci orientację w terenie. Dynamicznie zmieniając współrzędne GPS w czasie rzeczywistym, „spoofer" może kontrolować pozycję UAV. Po przejęciu kontroli możne skierować pojazd do „bezpiecznej strefy".
- **Wysyłanie fal elektromagnetycznych dużej mocy *(High Power Microwave)*.** Urządzenia mikrofalowe dużej mocy (HPM) generują impuls elektromagnetyczny (EMP) zdolny do zakłócania pracy urządzeń elektronicznych. EMP zakłóca łącza radiowe lub niszczy obwody elektroniczne w dronach (oraz wszelkich innych urządzeniach elektronicznych w zasięgu). Urządzenia emitujące HPM mogą zawierać antenę skupiającą impuls w określonym kierunku, zmniejszając potencjalne skutki uboczne.
- **Chwytanie w sieć** – fizyczne pochwycenie UAV w sieć wystrzeloną ze specjalnego karabinu lub działka bądź własnego drona wyposażonego w działko z siecią.
- **Strzał z lasera** wysokoenergetycznego wytwarzającego niezwykle skupioną wiązkę światła.
- **Cyberprzejęcie *(cyber takedown)*** – stosunkowo nowe rozwiązanie polegające na wykryciu transmisji radiowej w oparciu o protokół lub częstotliwość, na której działa dron. Następnie, za pomocą funkcji sztucznej inteligencji pracującej m.in. na danych z bazy zawierającej znane cechy dronów, są rozpoznawane numer seryjny modelu i pozycja operatora. Jeśli operator C-UAS uzna urządzenie za potencjalnie groźne, może wysłać sygnał, który hakuje funkcję dowodzenia i kontroli, zmuszając UAV do lądowania.

Systemy antydronowe to bardzo często kombinacja kilku metod. Producenci np. wprowadzają systemy wieloczujnikowe z algorytmami fuzji danych, rakietami czy sieciami, aby zapewnić kompleksowe zintegrowane rozwiązanie do zwalczania dronów. W Polsce, jeśli chodzi o C-UAS, powstały systemy, które sprawdzają się w boju. Serwis Defence24 cytuje słowa ukraińskiego żołnierza: „To najlepszy system, który ja i inne jednostki widzieliśmy i wykorzystywaliśmy. Może śledzić wszystkie trzy klasy BSP i neutralizować je w sposób niekinetyczny. Jego zasięg odpowiada specyfikacji, a nawet jest lepszy, w zależności od wysokości lotu BSP".

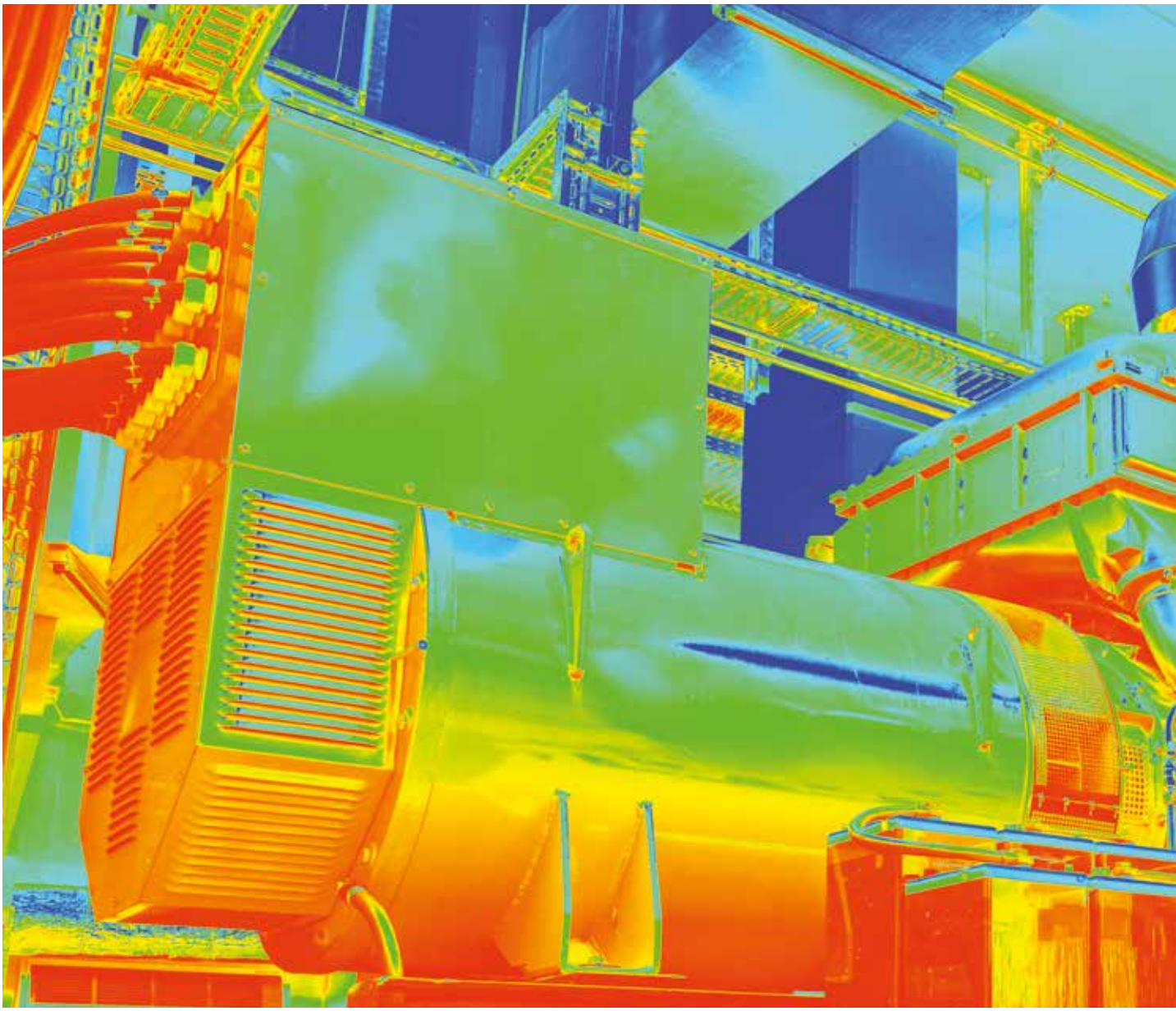
Jak wygląda pod tym względem wyposażenie np. polskiej armii? Temat podjęła „Polska Zbrojna". W lutym bieżącego roku opublikowała artykuł, w którym czytamy:

Jak zaznaczają Agencja Uzbrojenia i Sztab Generalny WP, informacje na temat posiadanych czy planowanych do pozyskania przez siły zbrojne zdolności, związanych z ochroną i obroną wojsk, w tym infrastruktury krytycznej, są niejawne. Płk Łukasz Andrzejewski-Popow z SGWP przyznaje tylko, że do wyposażenia SZRP wprowadzane są obecnie systemy radarowe umożliwiające wykrywanie, śledzenie i klasyfikację dronów. Cytowany dalej płk Andrzejewski-Popow powiedział, że armia poszukuje kompleksowych rozwiązań w tym zakresie, systemów zarówno kinetycznych, jak i niekinetycznych.

Według autorów artykułu systemy antydronowe pozostają w obszarze zainteresowania resortu obrony. Środki na zakup tego rodzaju technologii przewidziano także w „Planie modernizacji technicznej sił zbrojnych na lata 2021–35".

Skoro tak ma się rzecz w polskiej armii, to jak wygląda kwestia ochrony obiektów cywilnych, szczególnie z kategorii IK? Z wywiadu „Jak chronić infrastrukturę krytyczną przed dronem" przeprowadzonego przez „Rzeczpospolitą" w listopadzie 2022 r. z dr. Jędrzejem Łukasiewiczem, wiceprezesem Polskiego Towarzystwa Bezpieczeństwa Narodowego, można wywnioskować, że mogłoby być lepiej. J. Łukasiewicz zwrócił uwagę na bardzo ważny aspekt związany z ochroną antydronową: państwo powinno stworzyć ramy prawne, które pozwolą operatorom IK na użycie systemów neutralizujących bezzałogowe statki powietrzne.

W przepisach prawa muszą się zatem znaleźć choćby zapisy o odpowiedzialności za ich zestrzelenie. Porusza też kwestię odpowiedzialności, dostrzegając, że podmioty odpowiedzialne za IK nie zawsze mają kompetencje do oceny skuteczności systemów oferowanych przez firmy komercyjne. Zawsze jednak powinny ocenić ryzyko ataku i na miarę własnych możliwości i kompetencji postarać się o stosowną ochronę przeciw potencjalnym atakom dronów. Być może sięgając po załącznik nr 1 do *Narodowego programu ochrony infrastruktury krytycznej* (2023 r.), gdzie zapobieganiu, reagowaniu i ograniczaniu skutków zagrożeń ze strony systemów bezzałogowych poświęcono kilkanaście stron. ●



Kamery termowizyjne – o czym warto wiedzieć

Kamery termowizyjne stosowane w dozorze wizyjnym charakteryzuje praca praktycznie w każdych warunkach, nawet w absolutnej ciemności i przy ekstremalnie złej pogodzie. Na co zwrócić uwagę, by w pełni wykorzystać możliwości tych urządzeń?

Jan T. Grusznic, a&s Polska

Zrozumienie zasad działania urządzeń wpływa na ich efektywniejsze wykorzystanie. Nie inaczej jest z kamerami termowizyjnymi, chętnie stosowanymi w systemach ochrony obwodowej, ale też do kontrolowania temperatury procesów przemysłowych. Kamera termowizyjna tworzy obraz, wykorzystując promieniowanie podczerwone. Podczerwień to promieniowanie elektromagnetyczne o długości fali od 780 µm do 1 mm. To zakres fal leżący pomiędzy światłem widzialnym a promieniowaniem mikrofalowym.

Wyróżniamy cztery podstawowe pasma:

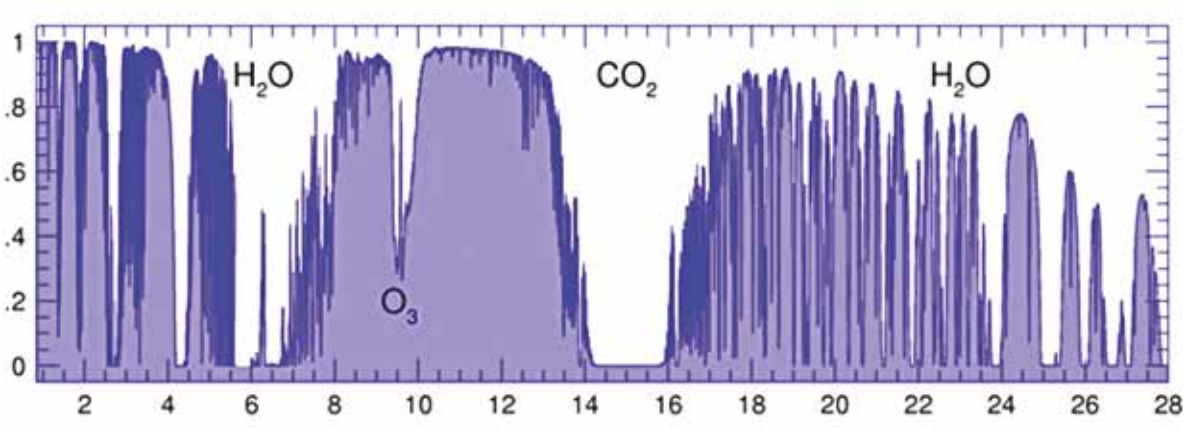
- bliska podczerwień *(near infrared, NIR)* 0,8–1,1 µm
- krótka podczerwień *(short wave infrared, SWIR)* – zakres 0,9–2,5 µm,
- średnia podczerwień *(mid wave infrared, MWIR)* – zakres 3–5 µm,
- daleka podczerwień *(long wave infrared, LWIR)* – zakres 7–14 µm.

Znaczna część tego spektrum nie jest jednak rejestrowana przez kamery termowizyjne, wiele długości fal jest bowiem pochłanianych przez gazy znajdujące się w atmosferze ziemskiej *(rys. 1)*. Istotne dla funkcjonowania kamer są tzw. okna widmowe lub okna transmisji atmosferycznej. Określają pasma, które mogą zostać wykorzystane. Każdy obiekt, którego temperatura jest wyższa od zera bezwzględnego, tj. -273,15°C emituje energię. Jej ilość zależy od temperatury obiektu, wielkości jego powierzchni oraz poziomu emisyjności. Tworzenie obrazu polega na rejestracji przez kamerę promieniowania emitowanego przez obiekt, a następnie przetworzeniu go na obraz widoczny dla ludzkiego oka. Kamery termowizyjne są w stanie dostarczyć czytelny obraz zarówno za dnia, jak i nocą, nawet mimo mgły, deszczu czy opadów śniegu, choć duże zamglenie lub opady ograniczą obszar efektywnego działania urządzenia. Najważniejsze jest to, że kamery termowizyjne nie potrzebują do tego żadnego źródła światła.

Chłód się ceni

Obecne na rynku kamery termowizyjne można podzielić na dwa typy: z przetwornikiem niechłodzonym i chłodzonym. Te pierwsze są przystosowane do pracy w oknie widmowym LWIR, te drugie

Rys. 1. Przepuszczalność promieniowania podczerwonego warstwy atmosfery ziemskiej w funkcji długości



Źródło: *Uncooled Infrared Imaging Market : Commercial & Military applications,* Sample report, Yole Développement, 2011

– MWIR. Oba typy różnią się, co oczywiste, nie tylko sposobem działania i budową detektorów, lecz także ceną. Kamery z przetwornikiem niechłodzonym są wielokrotnie tańsze od tych dla fal MWIR.

Typowe kamery termowizyjne stosowane w dozorze wizyjnym mają matrycę detektorów niechłodzonych o rozdzielczości od 160 x 120 pikseli nawet do 1280 x 1024 pikseli. Wykonywane są z materiałów typowych dla detektorów termicznych, takich jak tlenek wanadu (VOx – największy udział w rynku) lub krzem amorficzny (a-Si – popularny z uwagi na fakt, że jego produkcja jest łatwiejsza, a co za tym idzie tańsza).

Zasięg detekcyjny

Jakość niechłodzonych przetworników jest tak wysoka, że mogą one wykrywać obiekty odległe nawet o 8 km. To oczywiście rzadko wykorzystywana możliwość. Zazwyczaj objęte dozorem odcinki mierzą od 100 do 500 m. Zasięg detekcyjny zależy od ogniskowej użytego obiektywu, ale również od warunków pogodowych. W sytuacji, gdy w atmosferze unoszą się różnego rodzaju cząstki, np. wody (z mgły) lub dymu, to ogólnie rzecz biorąc, transmisja fal o długości LWIR będzie lepsza, niż ma to miejsce w przypadku transmisji fal widzialnych w zakresie 0,38–0,78 µm. W większości przypadków są one bowiem pochłaniane i rozpraszane przez cząstki w większym stopniu niż ma to miejsce w przypadku LWIR. Zmniejsza to skuteczność działania kamer wizyjnych w porównaniu z kamerami termowizyjnymi. Nie oznacza to jednak, że kamery termowizyjne będą idealnie działać w każdych warunkach. Należy bowiem pamiętać o takim aspekcie, jakim jest wpływ środowiska na tłumienie fali, tzw. tłumienność.

Załóżmy, że kamera do pracy wymaga różnicy temperatur wynoszącej 2°C między obiektem docelowym a tłem. Mgła, deszcz lub śnieg będą negatywnie wpływać na obraz termowizyjny, pochłaniając i rozpraszając fale promieniowania i niwelując różnicę temperatury. Dzieje się tak, ponieważ wzrost tłumienności zwiększa się wraz z ilością cząsteczek pochłaniających promieniowanie oraz z wydłużeniem się drogi transmisji promieniowania, co wpływa to na zmniejszenie mocy promieniowania docierającego do obiektywu kamery, i ostatecznie do detektora *(tab. 1)*.

Tabela 1. Zakres detekcji kamer wizyjnych i termowizyjnych LWIR w zależności od klasy mgły

Klasa mgły	Kamery wizyjne (promieniowanie widzialne)	Kamery termowizyjne (typ LWIR)
I	1220 m	5,9–10,1 km
II	610 m	2,4 km
IIIa	305 m	293 m
IIIb	92 m	87 m

W przypadku mgły klasy I i II zakres LWIR jest znacznie większy niż zakres wizyjny. Jednak w przypadku mgły klasy III nawet fale LWIR są pochłaniane i rozpraszane. W takich warunkach nie ma prawie żadnej różnicy w zasięgu między kamerami wizualnymi a termowizyjnymi.

Na przykład kamera termowizyjna z obiektywem 60 mm będzie miała zasięg detekcyjny ok. 600 m. W mglisty dzień tłumienie będzie wynosić 10 dB/km lub 1 dB/100 m, co daje całkowite tłumienie na poziomie 3 dB. Zatem tylko 50% energii emitowanej przez obiekt dotrze do detektora, co spowoduje niższy sygnał wejściowy. Niższy sygnał wejściowy da bardziej zaszumiony obraz, ponieważ zmniejsza się stosunek sygnału do szumu. Do pewnego stopnia zostanie to zrekompensowane przez przetwarzanie obrazu, ale nie zmienia to faktu, że będzie on zawierać mniej informacji, będzie bardziej „szary" i mniej kontrastowy, co utrudni odróżnienie szczegółów. Tłumienie sygnału negatywnie wpłynie na wydajność kamery i utrudni pracę aplikacji do analizy wideo. Dlatego należy unikać instalacji, w których kamera pracuje na granicy maksymalnej deklarowanej wydajności detekcyjnej.

Czułość

Czułość termiczna to poprawność wizualizacji przez kamerę przy zwiększeniu kontrastu obrazu. Czułość termiczna zależy od temperatury obiektu. Gdy temperatura obiektu rośnie, generowany przez kamerę sygnał również wzrasta. Oznacza to, że stosunek sygnału (wzrost) do szumu (wartość stała) zwiększa się, gdy obserwacja dotyczy cieplejszych obiektów. Najczęściej czułość kamery termowizyjnej przedstawiana jest jako wartość NETD *(Noise Equvialent Temperature Difference* – różnica temperatury równoważna szumowi) wyrażana w milikelwinach (mK) i jest najchętniej stosowanym parametrem w praktyce termograficznej, gdyż ma odniesienie do rzeczywistych warunków pracy kamery. NETD jest pomiarem ilościowym ukazującym różnice temperaturowe w scenie równe szumowi detektora lub całego systemu pomiarowego. Wartości NETD podawane są na ogół dla temperatury od 20 do 25°C. Przy niższych temperaturach otoczenia wartość NETD maleje, co przekłada się na wzrost czułości kamery termowizyjnej. Dlatego kamera termowizyjna może wydawać się czulsza o poranku, gdy różnica między chłodnym tłem a emitującym energię obiektem jest większa, niż ma to miejsce w południe. Zdecydowane zwiększenie czułości zauważymy zimą, a zmniejszenie latem. Im niższa wartość, tym wyższa czułość urządzenia, ponieważ oznacza to, że kamera jest w stanie rozróżnić mniejsze zakresy temperatur i uzyskać bardziej szczegółowy obraz. Wiele sprzedawanych obecnie kamer termowizyjnych oferuje czułość na poziomie >50 mK, przy czym modele wyższej jakości osiągają czułość >40 mK, a urządzenia z najwyższej półki nawet >35 mK.

Urządzenia o wyższej czułości termicznej mają ogromną przewagę podczas pracy w niekorzystnych warunkach otoczenia, takich jak mgła, dym i kurz.

Bardzo duży wpływ na czułość termiczną mają zastosowane obiektywy. Standardowo w kamerach termowizyjnych wykorzystuje się obiektywy o apreturze F1.0 (ogniskowa jest równa średnicy soczewki). Jednak ciągła walka cenowa oraz dążenie do zmniejszenia wielkości soczewek, co z kolei pozwala zmniejszyć całe urządzenie, powodują, że coraz częściej stosowane są obiektywy o mniejszej aperturze. Na przykład soczewki F1.4 wywołują dwukrotne zmniejszenie czułości termicznej, a F2.0 – czterokrotne. Dlatego kamerze o czułości 50mK (0,05°C) w momencie użycia obiektywu F1.4 zmieni się czułość termiczna do 100mK (0,1°C). Warto mieć to na uwadze, porównując parametry kamer.

DOBRE PRAKTYKI

1. Tło o równomiernie rozłożonej temepraturze, w porównaniu ze scenami o dużej rozpiętości temperaturowej, umożliwia szybszą i skuteczniejszą detekcję obiektów. Zadbaj o to, aby kamera obserwowała w miarę jednolity pod względem temperatury teren (np. murawę, kostkę brukową, asfalt itp.). W kadrze nie powinny znajdować się elementy przysłaniające obraz, takie jak drzewa, flagi itp.

2. Nim dobierzesz zakres ogniskowych, sprawdź ukształtowanie terenu. Duże różnice wysokości terenu i jego silne pofałdowanie negatywnie wpłyną na jakość detekcji. Pomocne jest narzędzie Głównego Urzędu Geodezji i Kartografii dostępne na stronie https://mapy.geoportal.gov.pl/imap/Imgp_2.html

3. Silne mgły poważnie ograniczają zasięg detekcyjny. Dobierając urządzenie, warto wcześniej sprawdzić, jakie jest prawdopodobieństwo powstawania mgieł w danym regionie. Można to zrobić np. korzystając ze strony Państwowego Instytutu Badawczego Instytutu Meteorologii i Gospodarki Wodnej dostępnego pod adresem: https://imgw.isok.gov.pl/mapy-klimatologiczne/mgla.html

4. Staraj się unikać kadrów zawierających znaczną liczbę obiektów silnie nagrzanych i zacienionych (np. elementy architektury, drzewa, skład złomu, słupy energetyczne itp.)

5. Zastosowanie kamery z długą ogniskową zapewnia obserwację na długich odcinkach. Aby zminimalizować ryzyko drgań obrazu, co bezpośrednio wpływa na skuteczność detekcji, zadbaj o instalację na trwałych elementach (np. mur, słup betonowy, ściana budynku itp.). W przypadku wykorzystywania słupów oświetleniowych zadbaj o to, by kamera wyposażona była w cyfrową stabilizację obrazu i zapewnij krótki, dostosowany do modelu kamery wysięgnik

6. Każda kamera posiada tzw. martwą strefę, czyli obszar, który nie jest widoczny dla kamery lub taki, w którym analiza zawartości obrazu nie jest stanie poprawnie wykryć obiektu. Dla ogniskowych 60 mm strefa ta może sięgać ponad 70 m od punktu zamontowania kamery. Zadbaj, by martwa strefa była dozorowana przez kamerę poprzedzającą

7. Zasięg detekcyjny dla kamer termowizyjnych wg kryteriów Johnsona nie powinien być przenoszony 1:1 dla zasięgów wynikających z zastosowanych algorytmów analizy obrazu, które potrzebują często wyższej szczegółowości obiektu (reprezentacji przez większą liczbę pikseli)

8. Choć pojedyncza kamera termowizyjna jest kilkukrotnie droższa od kamery wizyjnej, warto pamiętać, że do efektywnego pokrycia tego samego odcinka potrzeba mniej kamer termowizyjnych niż kamer wizyjnych. Co więcej, moc obliczeniowa tych urządzeń wzrosła na tyle, że umożliwiają one przeprowadzanie zaawansowanych analiz na coraz mniejszej grupie pikseli, co efektywnie zwiększa zasięg detekcyjny. Kamery termowizyjne należą również do produktów o najdłuższym czasie życia. Średni czas "życia" (tj. obecności na rynku i supportu) kamery termowizyjnej jest ponad 3x dłuższy w porównaniu do kamery wizyjnej

9. Kamery termowizyjne mogą być użyte do obserwacji części terenów przyległych do obiektu, spełniając wymagania dotyczące utrzymania prywatności. Kamery termowizyjne bowiem nie dostarczają obrazów umożliwiających wiarygodną identyfikację osób

Obraz nie całkiem monochromatyczny

Obraz uzyskiwany z kamery termograficznej jest monochromatyczny, ponieważ takie urządzenie zawiera przetwornik wrażliwy tylko na jeden zakres długości fal promieniowania podczerwonego. Zazwyczaj kamery monochromatyczne wyświetlają obraz, wykorzystując do tego 256 odcieni jednego koloru, by w ten sposób odwzorować zmianę intensywności sygnału. Jest to użyteczne, gdyż mimo że oko ludzkie ma większą rozpiętość dynamiki dla jasności niż koloru, to możliwość dostrzegania subtelnych różnic na obszarach o wysokiej jasności jest u ludzi mocno ograniczona. Najczęściej wykorzystywaną paletą jest *white hot* (gorący biały) lub *black hot* (gorący czarny). Głównie wynika to z wykorzystania analizy zawartości obrazu, która najlepiej wykrywa zmiany w kontrastowym obrazie *(rys. 2)*.

W zależności od typu kamery i producenta zastosowana paleta odcieni będzie mieć różne nazwy, a przede wszystkim rozkład tonalny. Choć najczęściej używanymi trybami pracy są *black hot* i *white hot,* to dostawcy nie szczędzą wysiłków, aby dostosowywać odcienie stosowanych kolorów do wymagań użytkowników. Przykładem może być wprowadzenie palety *ice and fire*, gdzie najcieplejsze miejsca są czerwone, a najzimniejsze mają barwę niebieską. Paleta *ice and fire* powstała na bazie palety white hot.

Rys. 2. Przykładowy obraz z kamery termowizyjnej. U góry *black hot*, u dołu *white hot*. Źródło: www.oemcameras.com, www.x20.org

Instalacja

Właściwa instalacja jest kluczowa dla wykorzystania pełnego potencjału termowizji. Umiejscowienie kamery ma znaczący wpływ na jej skuteczność. Montaż powinien zapewniać jak najpełniejszy obraz obserwowanego obszaru. Natomiast temperatura tła monitorowanej sceny powinna być jak najbardziej równomierna i niższa lub wyższa od temperatury typowej osoby, która może pojawić się w scenie. W ten sposób obiekt będzie odróżniać się od tła. (Informacja, co zrobić, by w miarę możliwości spełnić ten warunek, znajduje się w ramce na poprzedniej stronie).

Należy też zapewnić swobodną linię widoku z kamery bez żadnego elementu zakłócającego lub blokującego. Najlepiej, by obserwowany obszar pozbawiony był takich elementów jak gałęzie drzew czy flagi, czyli takie obiekty, które podczas wietrznej pogody będą chaotycznie poruszać się w kadrze. W zasięgu obserwowanej sceny powinien znajdować się jeden lub kilka łatwo rozpoznawalnych obiektów, np. komin na tle nieba lub budynek. Ułatwi to użytkownikom szybszą identyfikację obserwowanego miejsca.
Kamera powinna być zamontowana tak stabilnie, jak to tylko możliwe. W przypadku instalacji na słupie jego ruch lub drżenie może być interpretowane jako ruch w scenie, mimo że nic się nie poruszyło. Przydatne staje się wykorzystanie elektronicznej stabilizacji obrazu, zwłaszcza dla kamer z dużymi ogniskowymi do dalekiej obserwacji.

Stabilizacja obrazu

Elektroniczna stabilizacja obrazu, znana również jako cyfrowa stabilizacja obrazu, została opracowana przede wszystkim dla kamer wideo. Wykorzystuje różne algorytmy modelowania ruchu kamery, które są następnie używane do korygowania obrazu. Zarejestrowane piksele są stosowane jako bufor dla ruchu, a informacje o nich można następnie wykorzystać do przesunięcia obrazu elektronicznego z klatki na klatkę, by zrównoważyć ruch i stworzyć stabilny strumień wideo.

Pojawienie się niedrogich żyroskopów wraz z bardziej wydajnymi algorytmami modelowania ruchu umożliwia tworzenie systemów hybrydowych wykorzystujących pomiary żyroskopowe do cyfrowego przetwarzania obrazów, zapewniając szeroki zakres częstotliwości. Nawet w warunkach słabego kontrastu stabilizacja obrazu spełnia swoje zadanie, ponieważ do obliczeń są stosowane informacje żyroskopowe, a nie zawartość strumienia wideo. Z tego powodu urządzenie wyposażone w elektroniczną stabilizację obrazu jest odporne na ewentualne drżenia i wibracje wywołane np. przez podmuchy wiatru.

Maksymalny potencjał kamer termowizyjnych zostanie wykorzystany tylko wtedy, gdy proces instalacji zostanie poprzedzony analizą sytuacyjną i warunkami, w jakich będzie pracować kamera lub cały ich zestaw. Bez tego nawet najbardziej wyrafinowana kamera nie spełni swojego zadania – ochrony mienia powierzonego jej czujnemu oku.

Część kamer termowizyjnych jest wyposażona w funkcję alarmowania związanego z temperaturą do zdalnego monitorowania np. stanu wygrzania urządzeń. Istnieją dwa podstawowe typy alarmów temperatury. Jeden jest wyzwalany, gdy temperatura wzrasta powyżej lub poniżej ustawionego limitu temperatury, ale także wtedy, gdy temperatura zmienia się zbyt szybko. Drugi to punktowy alarm temperatury, w którym kamera mierzy temperaturę określonego obszaru na obrazie. •

Axis Communications

Więcej na: www.axis.com/pl-pl

Kamera termowizyjna Q1951-E	
Typ przetwornika termowizyjnego	Niechłodzona matryca mikrobolometryczna
Rozdzielczość przetwornika termowizyjnego [piksele]	384x288 (skalowalne do 768 x 576)
Czułość termiczna (NETD) [mK]	40
Zakres widmowy modułu termowizyjnego [µm]	8-14
Częstotliwość odświeżania obrazu modułu termowizyjnego	8.3 kl./s lub 30 kl./s (zależnie od wersji)
Ogniskowa obiektywu modułu termowizyjnego [mm]	7, 13, 19 lub 35 (zależnie od wersji)
Deklarowany maks. dystans detekcji człowieka / pojazdu [m]	70, 130, 190 lub 350 (zależnie od wybranej ogniskowej)
Tryby pracy	White-hot, Black-hot, Axis, Rainbow, Planck, Atlantis, Nightvision, Ice-and-fire
Cyfrowa stabilizacja obrazu	TAK
Pomiar temperatury	NIE
Obsługa zapisu lokalnego zapisu na kartach pamięci	TAK
PoE [klasa] / zasilacz zewnętrzny [VAC, VDC]	PoE, IEEE802.3af / IEEE 802.3at klasa 3
Pobór mocy [W] Max / nominalny	Maks: 12.95 W, nominalnie: 4,92 W
Zakres temperaturowy pracy [°C]	-20 ... +60 °C
Wymiary [mm]/Masa [kg]	Średnica 132 x 272 / 1,4
Okres gwarancji	60 miesięcy

Dahua Technology Poland

Więcej na: www.dahuasecurity.com

Kamera termowizyjna TPC-PT8441MA-T	
Typ przetwornika termowizyjnego	Niechłodzona matryca mikrobolometryczna
Rozdzielczość przetwornika termowizyjnego	400x300
Czułość termiczna (NETD) [mK]	< 35
Zakres widmowy modułu termowizyjnego [µm]	8-14
Częstotliwość odświeżania obrazu modułu termowizyjnego	25 kl./s
Ogniskowa obiektywu modułu termowizyjnego [mm]	7,5; 13; 25; 50
Deklarowany maks. dystans detekcji człowieka / pojazdu [m]	1470 / 4525
Tryby pracy	18 (white hot/black hot/fusion/rainbow/ golden autumn/midday/iron red/amber/ jade/sunset/icefire/painting/pomegran- ate/emerald /spring/summer/autumn/ winter)
Cyfrowa stabilizacja obrazu	NIE
Pomiar temperatury	TAK
Obsługa zapisu lokalnego zapisu na kartach pamięci	TAK
PoE [klasa] / zasilacz zewnętrzny [VAC, VDC]	Zasilacz zewnętrzny 10-36 VDC
Pobór mocy [W] Max / nominalny	Maks: 43
Zakres temperaturowy pracy [°C]	-40 ... 70 °C
Wymiary [mm]/Masa [kg]	231,3 × 389,7 × 276,9 / 9
Okres gwarancji	60 miesięcy

TIANDY (w ofercie Genway)

Więcej na: www.genway.pl

Kamera bispektralna TC-C35LP Spec: I5W/E/Y/T/6mm/V4.2	
Typ przetwornika termowizyjnego	Niechłodzona matryca mikrobolometryczna Vox
Rozdzielczość przetwornika termowizyjnego [piksele]	256 x 192
Rozdzielczość przetwornika modułu wizyjnego [piksele]	2880 x 1620
Czułość termiczna (NETD) [mK]	< 55
Zakres widmowy modułu termowizyjnego [µm]	8-14
Częstotliwość odświeżania obrazu modułu termowizyjnego	25 kl./s
Ogniskowa obiektywu modułu termowizyjnego [mm]	6,8
Ogniskowa obiektywu modułu wizyjnego [mm]	6
Deklarowany maks. dystans detekcji człowieka / pojazdu[m]	290 /890
Tryby pracy	white-hot, black-hot, red-hot, rainbow, iron-oxide, shimmer, aurora, jungle, medical
Cyfrowa stabilizacja obrazu	TAK
Pomiar temperatury	TAK
Obsługa zapisu lokalnego na kartach pamięci	TAK
PoE [klasa] / zasilacz zewnętrzny [VAC, VDC]	IEEE802.3af, 12 VDC
Pobór mocy [W] Max / nominalny	Maks: 9, nominalnie: 7,6
Zakres temperaturowy pracy [°C]	-35 ... 65 °C
Klasa szczelności obudowy	IP 67
Współpraca modułu wizyjnego z termowizyjnym	Wyświetlanie pomiarów temperatury na obu kanałach wizyjnych
Wymiary [mm]/Masa [kg]	330 x 114 x 107 / 1,5
Okres gwarancji	36 miesięcy

HIKVISION

Więcej na: www.hikvision.com/pl/

Kamera bispektralna DS-2TD6267-100C4L/W	
Typ przetwornika termowizyjnego	Niechłodzona matryca mikrobolometryczna VOx
Rozdzielczość przetwornika termowizyjnego [piksele]	640 × 512
Rozdzielczość przetwornika modułu wizyjnego [piksele]	2688 × 1520
Czułość termiczna (NETD) [mK]	< 35
Zakres widmowy modułu termowizyjnego [µm]	8 do 14
Częstotliwość odświeżania obrazu modułu termowizyjnego	50 kl./s
Ogniskowa obiektywu modułu termowizyjnego [mm]	100
Ogniskowa obiektywu modułu wizyjnego [mm]	6-336
Deklarowany maks. dystans detekcji człowieka / pojazdu[m]	2941 / 9020
Tryby pracy (white-hot, black-hot, inne)	white-hot, black-hot, rainbow, ice-and-fire, fusion 1, fusion 2, ironbow 1, ironbow 2, speia, color 1, color 2, rain, red hot, green hot, dark blue
Cyfrowa stabilizacja obrazu	TAK
Pomiar temperatury	TAK
Obsługa zapisu lokalnego zapisu na kartach pamięci	TAK
PoE [klasa] / zasilacz zewnętrzny [VAC, VDC]	36 VDC, 48 VDC
Pobór mocy [W] Maks. / nominalny	Maks: 120 W
Zakres temperaturowy pracy [°C]	-40 ... 65 °C
Klasa szczelności obudowy	IP 67
Współpraca moduły wizyjnego z termowizyjnym	Wyniki analizy obrazu nanoszone na obraz termowizyjny, łączenie obrazów (tzw. fusion) w celu podniesienia szczegółów w obrazie termowizyjnym
Wymiary [mm]/Masa [kg]	486,1 × 337,6 × 450,3 / 20
Okres gwarancji	36 miesięcy

FLIR (w ofercie Linc Polska)

ELARA™ FC-SERIES AI
Kamera termowizyjna z analityką

Typ przetwornika termowizyjnego	Niechłodzony mikrobolometr Vox o długiej żywotności
Rozdzielczość przetwornika termowizyjnego [piksele]	640x512
Czułość termiczna (NETD) [mK]	<30 @ 25°C dla F# 1.0
Zakres widmowy modułu termowizyjnego [µm]	7.5 do 13.5
Częstotliwość odświeżania obrazu modułu termowizyjnego	30 kl./s
Ogniskowa obiektywu modułu termowizyjnego [mm]	7.5/9/13/19/25/35/60/ 75
Deklarowany maks. dystans detekcji człowieka / pojazdu [m]	60-700 (detekcja człowieka w zależności od obiektywu)
Tryby pracy	white-hot, black-hot, rainbow+invert, contrast+invert, IronBlow2+invert, Arcitc+invert, Icefire+invert
Cyfrowa stabilizacja obrazu	Nie
Pomiar temperatury	Nie
Obsługa zapisu lokalnego zapisu na kartach pamięci	Tak
PoE [klasa] / zasilacz zewnętrzny [VAC, VDC]	POE+ (802.3 at), 12 VDC, 24 VDC, 24 VAC
Pobór mocy [W] Max / nominalny	25 z grzałką, 15 standard
Zakres temperaturowy pracy [°C]	-50 ... 70°C (ciągła praca) -40 ... 70°C (zimny start)
Wymiary [mm]/Masa [kg]	Bez osłony: 259 × 114 × 106 mm, z osłoną: 282 × 129 × 115 mm 7,5-35 mm - 2,2 kg, 60 mm - 2.4 kg, 75 mm - 2,5 kg
Okres gwarancji	Kamera: 3 lata Przetwornik: 10 lat

Więcej na: www.linc.pl

REKLAMA

Bi-spektralna kamera termowizyjna z AI

TNM–C4960TD/4950TD/4940TD

Dokładne wykrywanie obiektów na podstawie algorytmów Deep-Learning

www.hanwhavision.eu

Ochrona podstacji elektrycznych za pomocą technologii termowizyjnej

Podstacje elektryczne są narażone na zagrożenia pochodzące z wielu źródeł. Należą do nich zarówno wandale i intruzi, jak i niebezpieczne warunki pogodowe oraz okresy wysokiego zapotrzebowania na energię. Do tego dochodzą trudności związane z tym, że podstacje są bezzałogowe i często zlokalizowane w oddalonych miejscach. Utrudnia to ich ochronę przed włamaniami, kradzieżami i sabotażem. Są wrażliwymi punktami w sieci elektrycznej, a zatem mają krytyczne znaczenie dla dostaw energii. To sprawia, że jeszcze ważniejsza jest możliwość zachowania kontroli nad nimi.

Zarządzający podstacjami coraz bardziej koncentrują się na rozwiązywaniu tych kwestii, aby zapewnić nieprzerwane dostawy energii mieszkańcom miast i wsi, firmom oraz zakładom przemysłowym. Wymaga to monitorowania ostrzeżeń o potencjalnym naruszeniu, a także oznak awarii urządzeń.

Monitorowanie nadal w dużej mierze jest oparte na obserwacji przez pracowników w Centrum Monitoringu, ale coraz więcej firm energetycznych szuka sposobów, aby robić to bardziej wydajnie, z możliwością szybkiego podejmowania odpowiednich działań. Obrazowanie termowizyjne można wykorzystać do wsparcia tych wysiłków i zapewnienia ciągłego, dokładnego monitorowania podstacji, aby nie tylko poprawić bezpieczeństwo, ale także wspierać wydajność operacyjną i ciągłość działania.

Kamery termowizyjne a kamery wizyjne

Obrazowanie termiczne nie wymaga światła. W ogóle. Kamery termowizyjne umożliwiają widzenie w całkowitej ciemności i są równie skuteczne w godzinach dziennych. To odróżnia je od kamer wizyjnych, które wymagają padającego światła, aby przetwornik mógł wygenerować obraz. Obrazowanie termiczne jest oparte na wykrywaniu różnicy temperatur w energii cieplnej emitowanej przez obiekt, a następnie przełożeniu tego na szczegóły obrazu. Jest tak samo dokładne w ciemności, mgle, kamuflażu i w słoneczny dzień.

Nowe przetworniki obrazu, materiały i ulepszona kalibracja sprawiają, że kamery termowizyjne są bardziej niezawodne, a przystępność cenowa sprawia, że zyskują na popularności. Są stosowane głównie do celów dozorowych, wykrywając takie obiekty, jak ludzie i pojazdy. Istnieją też inne możliwe obszary ich zastosowań. Kamera termowizyjna może monitorować pracę urządzeń i procesy produkcyjne. Umożliwia skalibrowanie wyświetlacza ciepła z danymi liczbowymi, innymi słowy z temperaturą. Wysyła alerty, gdy temperatura wykracza poza ustawiony zakres, co umożliwia szybką reakcję. Jest to szczególnie przydatne do poprawy wydajności operacyjnej w przypadku krytycznych zasobów i urządzeń.

Termowizja poprawia wydajność operacyjną

Ręczne kamery termowizyjne są wykorzystywane w podstacjach do pomiaru temperatury i dostarczania termograficznego odczytu emitowanej energii. Kontrole te są przeprowadzane w odstępach od trzech do sześciu miesięcy. Pomiary ręczne wymagają fizycznych wizyt na miejscu, natomiast kamera termowizyjna zamontowana na stałe wprowadza alternatywę dla kontroli osobistych, monitorując odpowiedni sprzęt w dzień i w nocy przez cały rok.

Kamery termowizyjne mogą zarówno generować alarmy o wzroście temperatury, jak i rutynowo przeprowadzać kontrole krytycznych obszarów, co zapewnia lepsze zrozumienie sytuacji. Całodobowe monitorowanie obiektu za pomocą termowizji pomaga wychwycić potencjalny problem, zanim stanie się on poważniejszy i bardziej kosztowny. Wczesna interwencja może zatem pozytywnie wpłynąć na zwrot z inwestycji.

Kamery termowizyjne staną się niezbędnym elementem wyposażenia, za pomocą których będzie można analizować trendy i wydajność operacyjną, a także ciągle monitorować obszar w celu utrzymania ciągłości pracy podstacji.

Wykrywanie różnych zagrożeń

Ze względu na kluczową rolę, jaką odgrywają podstacje, są one narażone na różne zagrożenia, w tym ataki cybernetyczne. Kamery z wbudowanymi funkcjami cyberbezpieczeństwa pomagają zapobiegać infiltracji sieci przez hakerów i zakłóceniom ciągłości działania. Na każdym etapie cyklu życia urządzenia sieciowego – od produkcji po wycofanie z eksploatacji – istnieje ryzyko związane z cyberzagrożeniami. Jeśli jakiś element tego ryzyka zostanie przeoczony, może to doprowadzić do zakłócenia funkcjonowania oraz utraty poufności, integralności i dostępności danych. Dlatego tak ważne jest to, aby wszystkie związane z produktem podmioty – od dostawcy po klienta – dbały o zarządzanie ryzykiem.

Axis wspiera cyberbezpieczeństwo w swoich urządzeniach, ograniczając ryzyko w całym cyklu istnienia dzięki sprzętowej platformie Axis Edge Vault, która obsługuje funkcje chroniące tożsamość i integralność urządzenia przed nieuprawnionym dostępem. Firma stosuje system operacyjny AXIS OS z Axis Security Development Model (ASDM) – modelem rozwoju zabezpieczeń w celu obniżenia ryzyka wydania produktów z lukami w zabezpieczeniach oprogramowania.

Czasami inne zagrożenia przybierają jednak fizyczną formę, np. włamania, kradzieże czy sabotaż. W porównaniu do kamer wizyjnych wykorzystanie kamer termowizyjnych do wykrywania potencjalnych intruzów zapewnia bardziej niezawodne wskazywanie i rozpoznawanie kształtów. Jest to możliwe dzięki połączeniu wysokiego kontrastu obrazu z detekcją ruchu. W rezultacie wskaźnik fałszywych alarmów może być niższy przy mniejszej liczbie niepotrzebnych reakcji i działań ze strony personelu.

Kamery termowizyjne mogą pomóc w wykrywaniu aktywności na granicach terenu i tuż poza nimi zarówno w dzień, jak i w nocy. Wsparcie w zakresie ochrony obwodowej może odgrywać ważną rolę w zabezpieczaniu linii ogrodzenia. Rozwiązanie to może składać się z kamery termowizyjnej z funkcją analityczną wykrywającą potencjalnego intruza, która uruchamia kamerę PTZ, aby przyjrzeć się nieproszonemu gościowi, dostarczyć jego dobry obraz, a także śledzić go w pobliżu. Do tego rozwiązania można również dodać dźwiękowe i świetlne środki odstraszające, takie jak głośniki czy lampy stroboskopowe, które mogą zniechęcić intruza.

Korzystając z wykrywania dźwięku, urządzenia mogą ostrzegać o potencjalnym ataku na obiekt, co umożliwi pracownikom ochrony sprawdzenie miejsca zdarzenia. Na przykład, jeśli zaatakowano transformator i uszkodzono go, ostrzeżenie umożliwi wczesne jego naprawienie.

Kolejnym rosnącym zagrożeniem są drony coraz częściej wykorzystywane przez intruzów do monitorowania podstacji i powodowania jej awarii poprzez zrzucenie ładunków. Wykrywanie dronów odbywa się za pomocą urządzeń i oprogramowania partnerskiego. Podobnie jak w przypadku kamery wizyjnej kamera termowizyjna może udostępnić obraz drona.

Bezpieczeństwo w podstacji

Większy nacisk na utrzymanie pracy podstacji oznacza również częstsze monitorowanie terenu. Przegrzanie zwiększa ryzyko zarówno pożaru, jak i wybuchu, a kamery termowizyjne i termometryczne mogą monitorować urządzenia. Poprawia to bezpieczeństwo inżynierów, zapewniając podgląd stanu maszyn przed wysłaniem ich na miejsce.

Obrazowanie termowizyjne umożliwia wykrywania intruzów i uruchamianie innych urządzeń w systemach zabezpieczeń w celu odstraszenia niepożądanych osób za pomocą dźwięku i świateł. Poza bezpieczeństwem obiektu i znajdujących się w nim cennych aktywów odstraszanie służy również ochronie przypadkowych osób, takich jak dzieci lub nastolatki, które wchodzą do podstacji z ciekawości lub dla zabawy. Przebywanie wśród urządzeń wysokiego napięcia grozi śmiercią lub poważnymi obrażeniami.

Budowanie odporności

Awaria wielu podstacji na jednym obszarze spowodowałaby wiele społecznych i biznesowych problemów operacyjnych. W związku z tym niezwykle ważne jest wyposażenie podstacji w dodatkowe warstwy zabezpieczeń, aby zwiększyć odporność na potencjalne zagrożenia. To właśnie tutaj termowizja może wnieść największą wartość dodaną.

Obrazowanie termowizyjne ma kluczowe znaczenie dla poprawy bezpieczeństwa podstacji poprzez monitorowanie terenu obiektu i wokół niego 24 godziny na dobę, 7 dni w tygodniu. Celem jest powstrzymanie potencjalnych intruzów i wykrycie anomalii w funkcjonowaniu urządzeń na jak najwcześniejszym etapie, aby uniknąć nieoczekiwanych wyłączeń lub zdarzeń kaskadowych. Kamery termowizyjne mogą pełnić funkcję pierwszego reagującego urządzenia. ●

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

Upraszczamy codzienną pracę menedżerów ds. bezpieczeństwa, pracowników i liderów biznesu

Eksperci Nedap intensywnie pracują, aby wprowadzać na rynek zabezpieczeń kolejne innowacje. W ostatnich latach zespół R&D współdziałał z wieloma kluczowymi klientami i decydentami, aby poznać największe wyzwania, którym muszą sprostać w codziennych obowiązkach. Zebrane informacje zostały wykorzystane do stworzenia kompletnie nowego rozwiązania, jakim jest PACE.

Jednym z największych wyzwań dla dużych organizacji (np. przemysłowych, rządowych, edukacyjnych) jest zarządzanie dostępem dużej liczby pracowników w wielu budynkach i lokalizacjach. Chociaż istniejące systemy kontroli dostępu oferują doskonałą technologię do zarządzania dostępem, większość z nich nie nadaje się do tego na poziomie organizacyjnym uwzględniającym dynamikę przepływu ludzi.

Wiele lokalizacji wiąże się z licznymi wyzwaniami

Organizacje zatrudniające dużą liczbę pracowników często mają do czynienia z rosnącą dynamiką zmian posiadaczy kart (np. pracownicy zmieniający funkcję lub zawód, goście odwiedzający lokal). Dysponowanie wieloma lokalizacjami z różnymi systemami kontroli dostępu oprócz większych kosztów oznacza również konieczność sprostania wyzwaniom związanym ze zgodnością z przepisami, aby upewnić się, że wszystkie lokalizacje i wszystkie systemy kontroli dostępu są zgodne z polityką bezpieczeństwa.

Przykładowo, jeśli ktoś opuszcza organizację, to zgodnie z polityką bezpieczeństwa należy zablokować tej osobie dostęp do wszystkich lokalizacji biznesowych. Ale czy tak w istocie jest? I skąd menedżer ds. bezpieczeństwa może to wiedzieć?

Wraz z wyzwaniami przychodzą możliwości: rozwiązania PIAM

Rozwiązanie do zarządzania tożsamością i dostępem (PIAM – *Physical Identity and Access Management*) zostało zaprojektowane w celu zapewnienia prostszych, bardziej intuicyjnych sposobów zarządzania fizyczną tożsamością i zmianami dostępu. W końcu zmiana jest dziś normą, ponieważ wszyscy poruszamy się w ciągle zmieniającym się świecie. Wdrażanie i zwalnianie części pracowników, wewnętrzne ruchy i transfery oraz doraźne żądania dostępu pojawiają się każdego dnia. Chociaż wszyscy staramy się zaakceptować zmiany, specjaliści ds. bezpieczeństwa szukają sposobów, aby mieć czas na skupienie się na tym, co najważniejsze, czyli bezpieczeństwie. I tutaj pojawia się rozwiązanie PIAM.

Odpowiednie rozwiązanie PIAM powinno nie tylko pomóc w zmniejszeniu obciążenia operacyjnego, o którym mowa wcześniej, ale także poprawić produktywność biznesową i poprawić doświadczenia pracowników, przy jednoczesnym zachowaniu bezpieczeństwa i zgodności z politykami organizacyjnymi. Pracując nad rozwiązaniem PIAM, zespół Nedap wchodził w „różne buty": menedżerów bezpieczeństwa, pracowników i liderów biznesowych, poznając specyfikę ich pracy.

PIAM ma na celu usunięcie ciężaru operacyjnego związanego z zarządzaniem dostępem i umożliwienie menedżerom bezpieczeństwa wygodnego delegowania uprawnień do zarządzania dostępem w każdej lokalizacji biznesowej. Delegując obowiązki, osoby decyzyjne w każdym obszarze mogą szybciej i dokładniej obsługiwać żądania dostępu. Rozwiązanie sprawia, że zarządzanie dostępem jest łatwe w obsłudze i przyjazne dla użytkownika. Odbywa się poprzez automatyzację zadań i uczynienie ich bardziej intuicyjnymi.

Oferta PIAM opiera się na technologii cyfrowych bliźniaków

Misją Nedap jest opracowywanie inteligentnych technologii, które pomagają organizacjom bez problemu zarządzać tożsamością i dostępem niezależnie od tego, jakiego systemu kontroli dostępu używają na miejscu. Systemy bezpieczeństwa muszą pracować dla nas, a nie na odwrót: to nie my powinniśmy pracować na rzecz naszego systemu bezpieczeństwa.

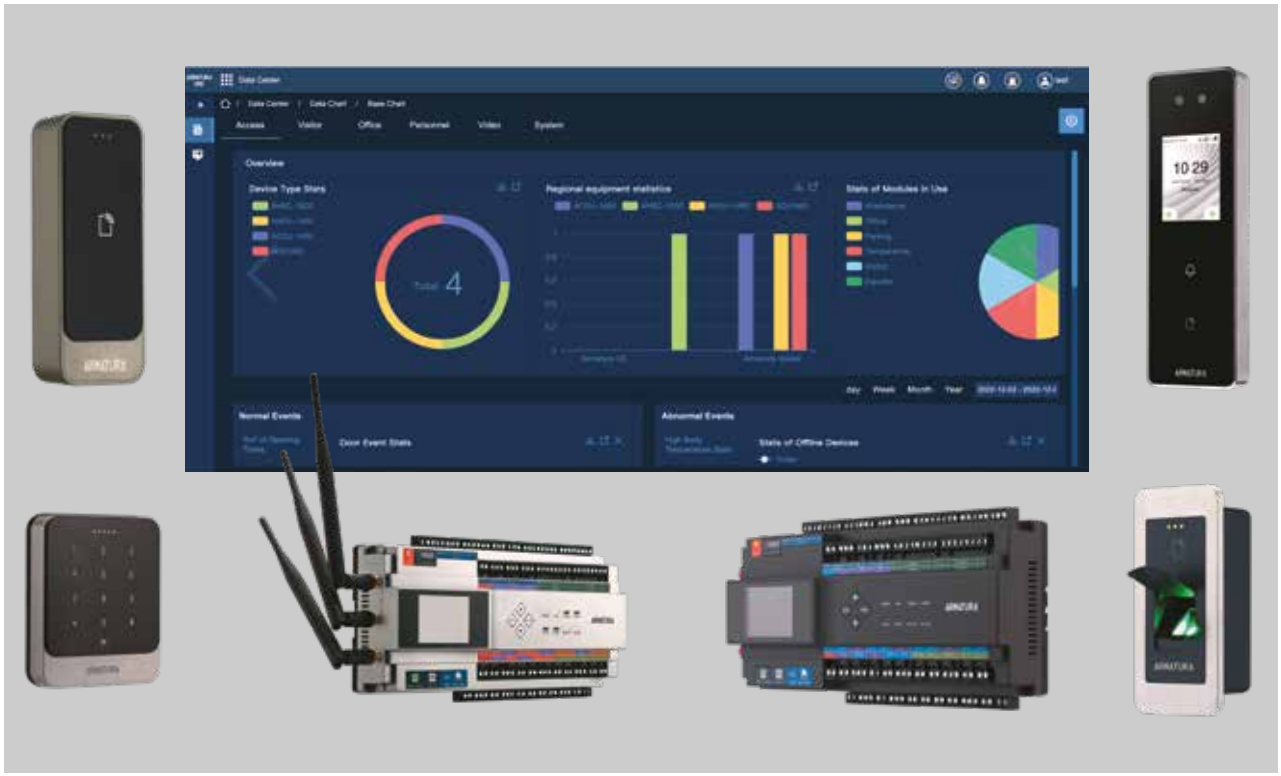
PIAM opiera się na unikatowej technologii cyfrowego bliźniaka. Polega ona na stworzeniu cyfrowej kopii rzeczywistego układu obiektu i systemów zabezpieczeń – cyfrowej wersji rzeczywistości. Cyfrowy bliźniak może pomóc w planowaniu, przewidywaniu, zarządzaniu i podejmowaniu decyzji dotyczących bezpieczeństwa i przepływu osób. To prawie tak, jak mapy Google'a wspierają w nawigacji, wyszukiwaniu i ulepszaniu podróży.

Nic bardziej nie frustruje pracowników niż czekanie przy zamkniętych drzwiach po dotarciu do miejsca pracy. Wyobraźmy sobie, jak bardzo poprawi się ich samopoczucie, jeśli wyeliminujemy opóźnienia i zawiłości w uzyskaniu odpowiedniego dostępu! Nie wspominając już o doświadczeniach gości i kontrahentów. Badania wykazały, że pozytywne doświadczenia w pracy zwiększają produktywność, a swobodne i bezpieczne poruszanie się ma tu kluczowe znaczenie.

Czy dołączysz do nas?

Jesteśmy na początku drogi w kierunku dostarczania niesamowitych i inteligentnych usług, które mogą zrewolucjonizować zarządzanie dostępem. Wraz z pierwszym wdrożeniem platformy PIAM czekamy niecierpliwie na nowości, które dodamy do naszej technologii w nadchodzących latach. ●

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



Platforma Armatura One do systemów kontroli dostępu

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

Marek Piotrowski

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

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

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

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

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

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

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

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

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

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

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

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

ARMATURA

MADE IN THAILAND

ZAPROJEKTOWANO W USA ARMATURA

High-tech Biometrics and Security Solution Provider

ARMATURA ONE

Kompatybilny z

Line · Whatsapp · Amazon SNS · Google Map · Super Map

WSZECHSTRONNA WEB-OWA PLATFORMA BEZPIECZEŃSTWA

AES 256 ENCRYPTION · TLS · BACnet · OPC · Modbus

Armatura One to najlepsza internetowa platforma bezpieczeństwa typu wszystko w jednym; opracowana dla ZKTeco przez firmę Armatura. Zawiera wiele zintegrowanych modułów takich jak: personel, kontrola dostępu, rejestracja czasu pracy, dostęp do wind, obsługa gości, zarządzanie parkingiem, zarządzanie systemem wideo, biuro, alarm przeciwpożarowy, kontrola przejść, kiosk z rozpoznawaniem twarzy, pomiar temperatury, zarządzanie ochroną, monitorowanie danych, automatyka budynkowa.

Peresonel	Dostęp	RCP	Windy	Goście	Parking	Wideo	Biuro
Alarm ppoż	Przejścia kontrolowane	FaceKiosk	Pomiar temperatury	Ochrona	Monitor danych	Automatyka budynkowa	Włamanie

ZKTeco

Authorized Worldwide Exclusive Distributor

www.zkteco.eu/armatura

BAS IP: Innowacje w świecie interkomów

Systemy interkomowe odgrywają kluczową rolę w dzisiejszych budynkach mieszkalnych i komercyjnych, zapewniając bezpieczeństwo oraz komunikację między mieszkańcami i gośćmi. Rozwijająca się technologia zmienia jednak sposób, w jaki patrzymy na te systemy. Jedną z firm wiodących w tej rewolucji jest BAS IP.

Radosław Suchodoła

BAS IP to firma z Wielkiej Brytanii, która od 2008 r. dostarcza innowacyjne rozwiązania w dziedzinie systemów interkomowych. Obecnie urządzenia BAS IP są dostępne w ponad 64 krajach, a główne biura handlowe znajdują się w Londynie, Hongkongu, Pradze i Kijowie. Jednym z kamieni milowych w historii firmy był rok 2010, kiedy to wprowadziła na rynek pierwszy interkom wideo oparty na technologii IP.

Głównym atutem BAS IP jest wykorzystanie technologii IP do komunikacji. W przeciwieństwie do tradycyjnych systemów interkomowych, które opierają się na analogowej transmisji sygnałów, produkty BAS IP korzystają z cyfrowego przesyłania danych przez sieć IP. Zapewnia to najwyższą jakość dźwięku i obrazu oraz umożliwia integrację z innymi systemami, takimi jak CCTV czy KD poprzez OpenAPI. Dodatkowym atutem jest prostota konfiguracji. Wystarczy nadać urządzeniom logiczne adresy i system będzie działać. Nie ma potrzeby przeprowadzania żmudnego procesu dodawania urządzeń do panelu głównego lub serwera. Przyspiesza to cały proces uruchomienia systemu. Adresy IP urządzeń mogą być nadane z DHCP i w dowolnym momencie zmienione.

Produkty i rozwiązania BAS IP

Jednym z kluczowych produktów firmy są wideodomofony IP, które umożliwiają użytkownikom komunikację z gośćmi i kontrolę dostępu za pomocą smartfonów lub tabletów. Z poziomu aplikacji na telefonie można również przydzielić kod dostępu lub QR dla gościa lub kuriera, który umożliwia wejście do wyznaczonych części obiektu przez określony czas. To rozwiązanie pozwala mieszkańcom na zarządzanie i kontrolę nad tym, kto przychodzi do budynku, nawet wtedy, gdy są poza nim.

W ofercie znalazły się również panele wewnętrzne z wbudowaną kamerą, które umożliwiają dwustronną komunikację audio-wideo nie tylko z użytkownikami, ale również z panelem zewnętrznym wyposażonym w 10-calowy ekran LCD. W przypadku obiektów biurowych lub użyteczności publicznej zdecydowanie poprawia to doświadczenia gościa, który rozmawia twarzą w twarz z obsługą obiektu lub pracownikiem firmy.

BAS IP dostarcza również rozwiązania kontroli dostępu do budynków komercyjnych oparte na technologii biometrycznej. Dzięki temu przedsiębiorstwa mogą zwiększyć poziom bezpieczeństwa, eliminując potrzebę korzystania z tradycyjnych kart dostępu na rzecz rozpoznawania twarzy, QR kodów, NFC lub UKEY, czyli wirtualnego klucza wgrywanego do telefonu, który pozwala na bezdotykowe otwieranie drzwi wejściowych do budynku.

Integracja i automatyzacja

Do unikatowych możliwości należy integracja z systemami windowymi. Użytkownik ma możliwość „wezwania" do 3 różnych wind w budynku za pomocą swojego panelu użytkownika lub smartfona. Jest to przydatne zwłaszcza w przypadkach, gdy obsługa windy wymaga użycia karty dostępu.

Ponadto produkty BAS IP są często wyposażone w funkcje automatyzacji, które pozwalają na oszczędność energii i zwiększenie komfortu mieszkańców. Przykładem jest zdalne sterowanie oświetleniem czy ogrzewaniem za pomocą smartfona lub tabletu z poziomu jednej aplikacji.

Wpływ na branżę

Dzięki innowacjom i nowoczesnym technologiom BAS IP rewolucjonizuje branżę systemów interkomowych. Jego produkty nie tylko poprawiają bezpieczeństwo i komfort użytkowników, ale także wpływają na całą branżę, inspirując inne firmy do inwestowania w rozwój i dostarczanie coraz lepszych rozwiązań. Dzięki wykorzystaniu technologii IP, integracji z innymi systemami oraz stałemu dążeniu do innowacji BAS IP zdobywa coraz większe uznanie na rynku interkomów.

Dystrybutorem produktów BAS IP w Polsce jest firma Global Security Partner. ●

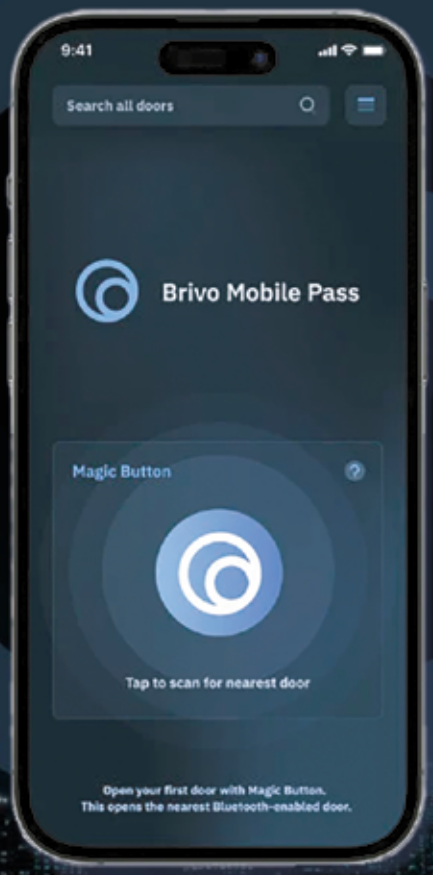
Global Security Partner
ul. Lęborska 3b, 80-286 Gdańsk
www.gspartner.pl
kontakt@gspartner.pl

brivo

smart-i

DOSTĘP JEST PRZYSZŁOŚCIĄ INTELIGENTNYCH BIUR

ZOPTYMALIZUJ SWOJE NIERUCHOMOŚCI DZIĘKI KONTROLI DOSTĘPU BRIVO



Technologia zabezpieczeń klasy korporacyjnej dla każdego rodzaju obiektu

60+

KRAJÓW NA CAŁYM ŚWIECIE

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

90+

TYSIĄCE WDROŻEŃ

Możliwości integracji, aby połączyć istniejące inwestycje technologiczne

450Mkw

NIERUCHOMOŚCI W ZARZĄDZANIU

brivo

866.692.7486 | brivo.com

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

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

PARTNER:

smart-i

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

www.smart-i.pl

„Wystarczy porozmawiać” – komunikacja w placówkach medycznych

Opieka nad pacjentem wymaga wymiany dużej ilości informacji, często pomiędzy różnymi grupami personelu. Liczba możliwych konwersacji i dróg do wymiany danych dla każdego oddziału zależy ściśle od liczby osób zaangażowanych w proces opieki. Zasadniczo są to trzy grupy: pacjenci, lekarze i pielęgniarki, co daje trzy podstawowe tory komunikacji. Wystarczy jednak rozszerzyć bieżący personel np. o laboratorium lub wyspecjalizowanych lekarzy, m.in. anestezjologów, by dla niektórych oddziałów mieć już 10 możliwych torów komunikacyjnych. To pokazuje, że nawet niewielkie zespoły medyczne mogą generować duże zapotrzebowanie na efektywne sposoby wymiany informacji.

Mateusz Bachański

Systemy przyzywowe w nowoczesnych placówkach medycznych są projektowane jako systemy alarmowe i komunikacji, a więc nie tylko chronią, ale też pomagają i ułatwiają pracę wszystkim osobom zaangażowanym w proces opieki nad pacjentem. Wyobraźmy sobie sytuację, gdy pacjent potrzebujący pomocy aktywuje przycisk alarmu na manipulatorze przy łóżku. Spowoduje to wygenerowanie przywołania w systemie przyzywowym i wysłanie odpowiedniej informacji do personelu w dyżurce oraz pracowników znajdujących się w salach chorych, a także w pokojach socjalnych. Łatwo zauważyć, że już tak banalna czynność jest w istocie prostą wymianą informacji pomiędzy pacjentem a pielęgniarką. Idąc dalej, możemy rozszerzyć ten scenariusz o cały oddział, różnych pacjentów, różne grupy personelu i różne alarmy, dzięki temu zobaczymy, jak duże wyzwanie stoi przed systemem przyzywowym.

Najprostszym rozwiązaniem jest oczywiście implementacja komunikacji głosowej, która pozwala w łatwy sposób rozszerzyć możliwości bezpieczeństwa i przesyłu danych w ramach obiektu medycznego. Funkcja komunikacji głosowej umożliwia personelowi zminimalizowanie zadań, które wymagają ich fizycznej obecności. Przekłada się to na zmniejszenie drogi przebytej przez personel w obiekcie w ciągu dnia. Dzięki temu zarówno pielęgniarki, jak i lekarze mają więcej czasu na to, co jest najważniejsze, czyli pomoc choremu w powrocie do zdrowia.

Bezpośrednia komunikacja głosowa pomiędzy pacjentem a personelem ponadto pozwala na zwiększenie satysfakcji pacjenta z opieki medycznej, a także usprawnia sam proces opieki. Pielęgniarka poprzez rozmowę z pacjentem jest w stanie wstępnie mu pomóc, udzielić szczegółowych informacji medycznych lub zaplanować dalsze działania. Należy przy tym pamiętać o przestrzeganiu zasad RODO i zapewnieniu komunikacji dyskretnej na linii pacjent – personel, np. przez słuchawki przy łóżkach, aby osoby postronne, np. znajomy innych chorych przebywających w sali, nie mieli dostępu do danych wrażliwych.

Rosnące zapotrzebowanie sektora medycznego na inteligentne rozwiązania sprawia, że generowanie i odbieranie przywołań różnego typu oraz komunikacja są dzisiaj standardem, jakiego oczekuje się od systemów przyzywowych. Nietrudno więc zrozumieć, że zarówno użytkownik docelowy, jak i klient biznesowy próbują znaleźć najbardziej użyteczne i praktyczne rozwiązanie.

System przyzywowy Visocall IP firmy Schrack Seconet oferuje wiele różnych opcji komunikacji, w tym komunikacji głosowej. Konstruktorzy

położyli duży nacisk na bezpieczeństwo i skalowalność rozwiązania. Podstawowa funkcjonalność systemów przyzywowych – generowanie alarmów – często może negatywnie wpływać na pracę placówki medycznej. Mowa tu o alarmach nieukierunkowanych. Statystycznie typowy oddział 20-łóżkowy potrafi generować dziennie nawet do 1000 różnych alarmów w ciągu doby, co przekłada się na mniej więcej 1 alarm co 90 s. Widać więc, że już liczba i częstotliwość mogą przytłoczyć nawet najbardziej efektywny zespół medyczny, powodując zmęczenie oraz spadek wydajności. W dłuższej perspektywie taki stan może powodować pogorszenie się jakości opieki, wydłużony czas powrotu do zdrowia, a w skrajnych przypadkach nawet możliwość wystąpienia sytuacji zagrażającej życiu i zdrowiu pacjenta.

System Visocall IP radzi sobie z tym zagadnieniem na wielu płaszczyznach.

- **Szczegółowa identyfikacja zdarzenia** – szereg urządzeń generuje różnego typu alarmy w zależności od zapotrzebowania (terminale pacjenta, przyciski przyzywowe moduły we/wy, gniazda diagnostyczne itp.).
- **Filtracja danych** – każdemu zdarzeniu alarmowemu przypisuje się odpowiedni priorytet i typ personelu lub indywidualny albo grupowy numer telefonu, do którego powinno trafić.
- **Odpowiednia wizualizacja** – wiele urządzeń umożliwia wizualizację: terminale z wyświetlaczem, komunikacyjne, oddziałowe, stanowiska wizualizacji, wyświetlacze korytarzowe, urządzenia mobilne. Ponadto wszystkie zdarzenia trafiają bezpośrednio do tych, które zostały przypisane do danej grupy opieki.

Te trzy proste zasady powiązane z komunikacją głosową pozwoliły na wyeliminowanie fałszywych alarmów oraz zoptymalizowanie procesu opieki w zakresie przesyłania informacji.

Funkcja komunikacji głosowej zapewnia też szereg bardzo użytecznych możliwości zarówno pacjentowi, jak i personelowi. Pielęgniarka, korzystając z terminalu oddziałowego, stanowiska wizualizacji lub urządzenia mobilnego, ma możliwość nawiązania połączenia głosowego z dowolnym pacjentem lub inną osobą z personelu. Podczas takiego połączenia może dokonać wstępnego wywiadu medycznego, udzielić prostych informacji lub poprosić pacjenta na badanie. Kiedy potrzebna jest komunikacja z większą grupą osób jednocześnie, personel ma do dyspozycji funkcję zapowiedzi, która może być kierowana do wszystkich na oddziale lub wybranych grup personelu.

Chory, mając przyłóżkowy terminal pacjenta, może rozmawiać z personelem w sposób dyskretny lub głośnomówiący. Dzięki temu terminale spełniają zapisy Rozporządzenia o Ochronie Danych Osobowych (RODO) i ustawy z 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta. Terminale mają dodatkowo wyjście słuchawkowe umożliwiające podłączenie zewnętrznych pętli indukcyjnych, aby umożliwić kontakt osobom niedosłyszącym.

Pacjent, korzystając ze znajdującego się przy łóżku terminala w kształcie słuchawki, ma możliwość komunikacji z personelem z wielu różnych oddziałów, np. kobieta na oddziale ginekologicznym może przywołać do siebie pielęgniarkę z oddziału ginekologicznego, a do noworodka pielęgniarkę z oddziału noworodkowego. Personel medyczny może używać urządzeń komunikacyjnych systemu Visocall IP do rozmów i konsultacji w ramach danego oddziału lub pomiędzy oddziałami.

Nowoczesne placówki medyczne mają dzisiaj wiele potrzeb i oczekują dużej elastyczności. Dlatego niezwykle istotna jest możliwość integracji z różnymi systemami jako rozwiązanie zmniejszające koszty indywidualnych instalacji oraz rozszerzające możliwości samego systemu. Na rynku często spotyka się rozwiązania zamknięte, gdzie jeden producent dostarcza wszystko, począwszy od hardware'u, skończywszy na oprogramowaniu i sterownikach. Daje to wiele niezależnych rozwiązań i systemów, które często działają autonomicznie. Firma Schrack Seconet natomiast projektuje systemy jako platformy otwarte z możliwością integracji jak największej liczby systemów w ramach jednego rozwiązania. Tak jest w przypadku systemu Visocall IP. Wykorzystanie interfejsu IP oraz otwartych protokołów w integracjach z systemami

zewnętrznymi jest najlepszym wyborem. Pozwala to na uzyskanie wysokiej kompatybilności z jak największą liczbą producentów. Klient nie jest skazany na jednego producenta, ma możliwość wyboru odpowiedniego dla niego rozwiązania.

Dla nas, jako producenta, integracja jest niezwykle istotna, dlatego staramy się wdrożyć ją na każdym etapie naszego systemu przyzywowego, aby rozbudować jego możliwości i funkcjonalność.

Zgodnie z rozporządzeniem MSWiA z 7 czerwca 2010 r. w sprawie ochrony przeciwpożarowej budynków, innych obiektów budowlanych i terenów dźwiękowy system ostrzegawczy projektuje się z wyłączeniem pomieszczeń intensywnej opieki medycznej, sal operacyjnych oraz sal z chorymi. Z tego powodu najlepszym sposobem na usprawnienie procedur związanych z ewakuacją pacjentów jest bezpośrednia integracja z systemem przyzywowym do optycznej i akustycznej sygnalizacji alarmów pożarowych.

Kolejnym elementem, który może rozbudować podstawową funkcjonalność systemu przyzywowego, jest integracja z centralą alarmową. Dzięki otwartym protokołom ESPA 4.4.4 i ESPA-X możliwe jest przesyłanie informacji o typach alarmów (w tym alarmów pożarowych lub z innych zintegrowanych systemów) i ich lokalizacji do urządzeń mobilnych w formie wiadomości tekstowych.

Funkcja komunikacji głosowej może również być w łatwy sposób rozbudowana, np. poprzez integrację z centralą telefoniczną IP. Integracja w ramach systemu Visocall IP może zostać zrealizowana na dwa sposoby. Pierwszy, poprzez zalogowanie poszczególnych przyłóżkowych terminali pacjentów i terminali pielęgniarskich jako indywidualnych użytkowników SIP w centrali telefonicznej (protokół SIP lub H.232). Pozwala to na przypisanie każdemu terminalowi konkretnego numeru w ramach systemu telefonicznego obiektu oraz korzystanie z nich jak z telefonów stacjonarnych. Dzięki temu pacjenci (na oddziałach zamkniętych, geriatrycznych, w DPS-ach itp.) mogą komunikować się między sobą lub z bliskimi.

Drugi sposób to integracja poprzez wykorzystanie protokołu SIP-TRUNK. To rozwiązanie pozwala personelowi medycznemu odbierać na telefonach przenośnych DECT/VoIP i smartfonach wszystkie przywołania z systemu przyzywowego ze szczegółowym opisem każdego zdarzenia (w tym alarmów pożarowych lub z innych zintegrowanych systemów) oraz lokalizacji jego wystąpienia wraz z możliwością prowadzenia rozmów, zdalnego ich zakończenia, a także potwierdzenia przyjęcia alarmu. Ponadto każdy terminal IP (zarówno komunikacyjne personelu, jak i przyłóżkowe pacjentów) może mieć przypisany numer w systemie przyzywowym, na który można później zadzwonić i połączyć się z danym urządzeniem Visocall IP z dowolnego telefonu stacjonarnego lub mobilnego, który jest zarejestrowany w centrali telefonicznej.

W tym roku rozszerzamy portfolio o własne rozwiązanie z zakresu urządzeń mobilnych, które nadal będzie rozwiązaniem w duchu zachowującym koncepcję platformy otwartej. Mowa tu o aplikacji Visocall Mobile. To aplikacja mobilna dostępna na dowolne urządzenie typu smartfon z systemem operacyjnym Android lub IOS. Aplikacja ta pozwala na korzystanie ze wszystkich funkcji terminala pielęgniarskiego: odbieranie wszystkich przywołań z funkcją komunikacji głosowej, generowanie bezpośrednich połączeń z każdym terminalem komunikacyjnym i pacjenta, a także odbieranie przywołań z systemów zintegrowanych, w tym z SSP. Dzięki powiadomieniom push użytkownik zalogowany do systemu dostanie powiadomienia o alarmach w każdym miejscu z dostępem do Internetu. Rozwiązanie to nie tylko zwiększa elastyczność pracy personelu, lecz także optymalizuje proces opieki i zmniejsza koszty dodatkowych instalacji. ●

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

Dedykowany system integracji dla obiektów infrastruktury krytycznej

Światowa nowość na polskim rynku klasy PSIM - CSIM

Venom

PSIM PLATFORM

POLSKIE ROZWIĄZANIE

ŚWIATOWEJ KLASY

Dowiedz się więcej

venompsim.pl

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

Po raz kolejny przedstawiamy mapę inwestycji, które są w trakcie realizacji lub dopiero się rozpoczną. Wybraliśmy te, których termin ukończenia nie upływa przed II kwartałem 2024 r., z jednym wyjątkiem. Są to przede wszystkim duże inwestycje prowadzone przez renomowane firmy, w których widzimy szansę na współpracę dla podmiotów sektora security. Jednocześnie polecamy uwadze poprzednie numery „a&s Polska", w których umieściliśmy zestawienie innych przedsięwzięć o długim czasie realizacji i interesującym zakresie działań. W tym numerze dużą część planowanych inwestycji stanowią te o charakterze energetycznym i wojskowym.

Adela Prochyra, a&s Polska

Mapa inwestycji

ATREM SA

Co: WYBUDOWANIE STACJI ELEKTROENERGETYCZNEJ 110KV RS SIEDLISKA UMOŻLIWIAJĄCEJ POŁĄCZENIE SIECI INSTALACJI PODSTACJI TRAKCYJNEJ SIEDLISKA PKP ENERGETYKA SA.

Gdzie: Białystok

Kiedy: 12 miesięcy od dnia zawarcia umowy (24 lipca 2023)

1

CONSTRUCTO SP. Z O.O.

Co: DOKOŃCZENIE ROBÓT BUDOWLANYCH W RAMACH ZADANIA INWESTYCYJNEGO POD NAZWĄ „PRZEBUDOWA, ROZBUDOWA I REMONT ZAKŁADU OPIEKUŃCZO-LECZNICZEGO I REHABILITACJI MEDYCZNEJ PRZY UL. MOGILEŃSKIEJ 42 W POZNANIU O DODATKOWĄ SKRZYDŁO WRAZ Z WBUDOWANYM WYPOSAŻENIEM".

Gdzie: Poznań

Kiedy: 280 dni od dnia podpisania umowy (30.08.2023)

2

ELEKTROTIM SA

Co: WYMIANA OGRODZENIA WEWNĘTRZNEGO I ZEWNĘTRZNEGO OBWODNICY WRAZ Z BRAMAMI I FURTKAMI W KOMPLEKSIE WOJSKOWYM NR K-0596 GOŁAWICE

Gdzie: Goławice

Kiedy: 540 dni od dnia podpisania umowy (7.08.2023)

3

Co: ROZBUDOWA SYSTEMU ALARMOWEGO W MAGAZYNACH ŚRODKÓW BOJOWYCH ORAZ NA OBWODNICY KOMPLEKSU WRAZ Z WYMIANĄ OŚWIETLENIA W KOMPLEKSIE WOJSKOWYM GOŁAWICE.

Gdzie: Goławice

Kiedy: Inwestor został wybrany, ale umowa nie została jeszcze podpisana

4

ENERGOAPARATURA SA

Co: WYKONYWANIE W LATACH 2023–26 PRAC ZWIĄZANYCH Z PRZEGLĄDAMI ORAZ REMONTAMI INFRASTRUKTURY ELEKTROENERGETYCZNEJ RAFINERII GDAŃSKIEJ W GDAŃSKU WEDŁUG ZLECEŃ ZAMAWIAJĄCEGO (UMOWA RAMOWA)

Gdzie: Gdańsk

Kiedy: 2023–26

5

Co: MODERNIZACJA STACJI ELEKTROENERGETYCZNEJ 110/15 KV LEŻAJSK SIEDLANKA

Gdzie: Leżajsk

Kiedy: 24 miesiące od dnia podpisania umowy (19.05.2023)

6

Co: WYKONYWANIE W LATACH 2023, 2024 I 2025 ROBÓT INWESTYCYJNYCH Z BRANŻY AUTOMATYKI NA INSTALACJACH I OBIEKTACH RAFINERII GDAŃSKIEJ WEDŁUG ZLECEŃ ZAMAWIAJĄCEGO (UMOWA RAMOWA)

Gdzie: Gdańsk

Kiedy: 2023–25

7

ERBUD

Co: BUDOWA TYMCZASOWYCH OBOZOWISK KONTENEROWYCH

Gdzie: woj. podlaskie

Kiedy: listopad 2023

8

Co: POROZUMIENIE O WSPÓŁPRACY Z DAEWOO ENGINEERING & CONSTRUCTION

Gdzie: Polska

Kiedy: najbliższe pięć lat

9

ENERGOINSTAL SA

Co: WYKONANIE MODUŁU PROTOTYPOWEGO DO MAŁYCH REAKTORÓW MODUŁOWYCH (ANG. SMR – SMALL MODULAR REACTOR)

Gdzie: Legnicka Specjalna Strefa Ekonomiczna

Kiedy: 22.08.2023 podpisano list intencyjny z Last Energy Polska sp. z o.o.

10

MDI ENERGIA SA

Co: BUDOWA ELEKTROCIEPŁOWNI NA BIOGAZ ROLNICZY

Gdzie: Bagdad w gminie Wyrzysk

Kiedy: 14 miesięcy od dnia podpisania umowy (29.08.2023)

11

Co: BUDOWA ELEKTROCIEPŁOWNI NA BIOGAZ ROLNICZY

Gdzie: Kaplonosy, gm. Wyryki

Kiedy: 17 miesięcy od dnia podpisania umowy (31.03.2023)

12

UNIBEP

Co: BUDOWA MIEJSKIEGO ŻŁOBKA W TECHNOLOGII MODUŁOWEJ WRAZ Z ZAGOSPODAROWANIEM TERENU PRZY UL. PRYMASA TYSIĄCLECIA W CIECHANOWIE

Gdzie: Ciechanów

Kiedy: 650 dni od dnia podpisania umowy (30.08.2023)

13

Co: BUDOWA CENTRUM INNOWACJI I CYBERBEZPIECZEŃSTWA WYDZIAŁU CYBERNETYKI

Gdzie: Wojskowa Akademia Techniki, Warszawa

Kiedy: Oferta uznana za najkorzystniejszą, ale umowa nie została jeszcze podpisana; 48 miesięcy od dnia podpisania umowy

14

Cyberbezpieczeństwo w Polsce
Raport ABW

Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV, działający pod kierownictwem szefa Agencji Bezpieczeństwa Wewnętrznego, co roku przygotowuje raport dotyczący bezpieczeństwa cyberprzestrzeni. Tegoroczny *Raport o stanie bezpieczeństwa cyberprzestrzeni w roku 2022* przedstawia zagrożenia i aktywności w sieci, które wpływają na ważne systemy państwowe, infrastrukturę krytyczną i kluczowe usługi.

Adela Prochyra, a&s Polska

Raport powstał na podstawie analizy zgłaszanych oraz rozpoznawanych przez CSIRT GOV incydentów bezpieczeństwa teleinformatycznego, danych z systemów autonomicznego wykrywania zagrożeń (zwłaszcza systemu wczesnego ostrzegania ARAKIS GOV), a także informacji zebranych przez zespół.

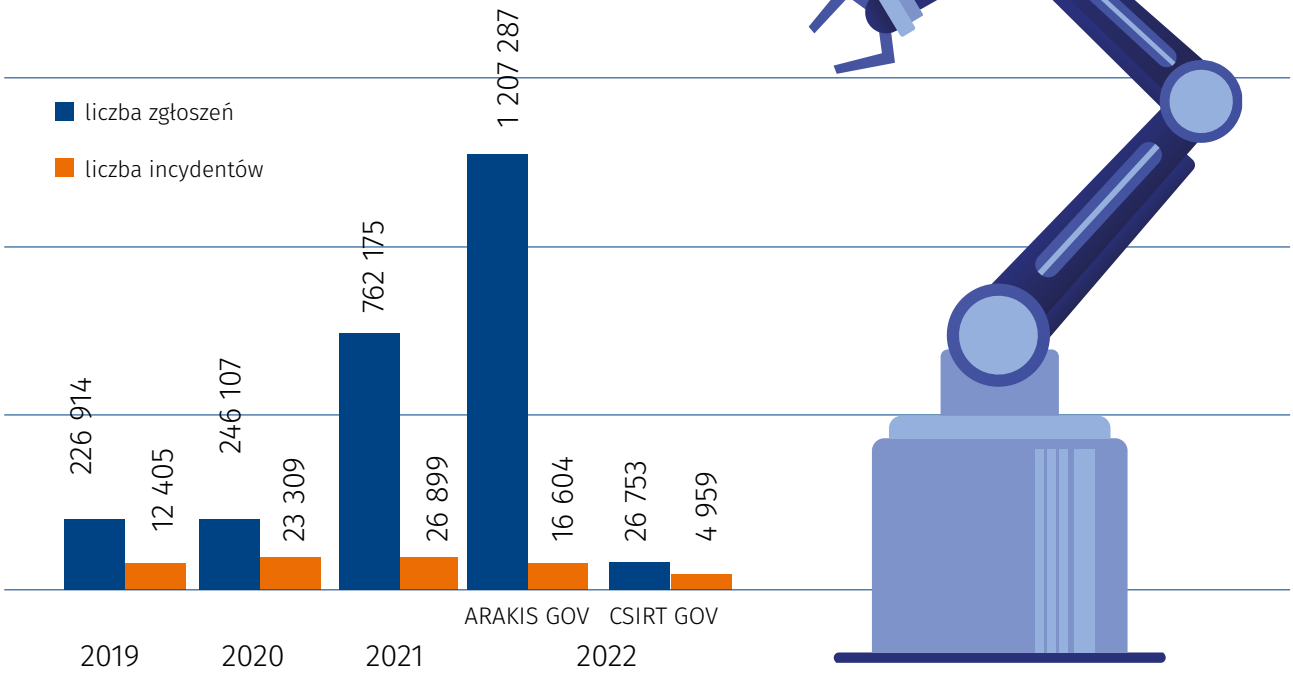
Niepokojące statystyki

Liczba odnotowywanych kampanii socjotechnicznych, a także wolumen ataków DDoS *(Distributed Denial of Service)*, wymierzonych w usługi publiczne świadczone z wykorzystaniem Internetu, wciąż rośnie.

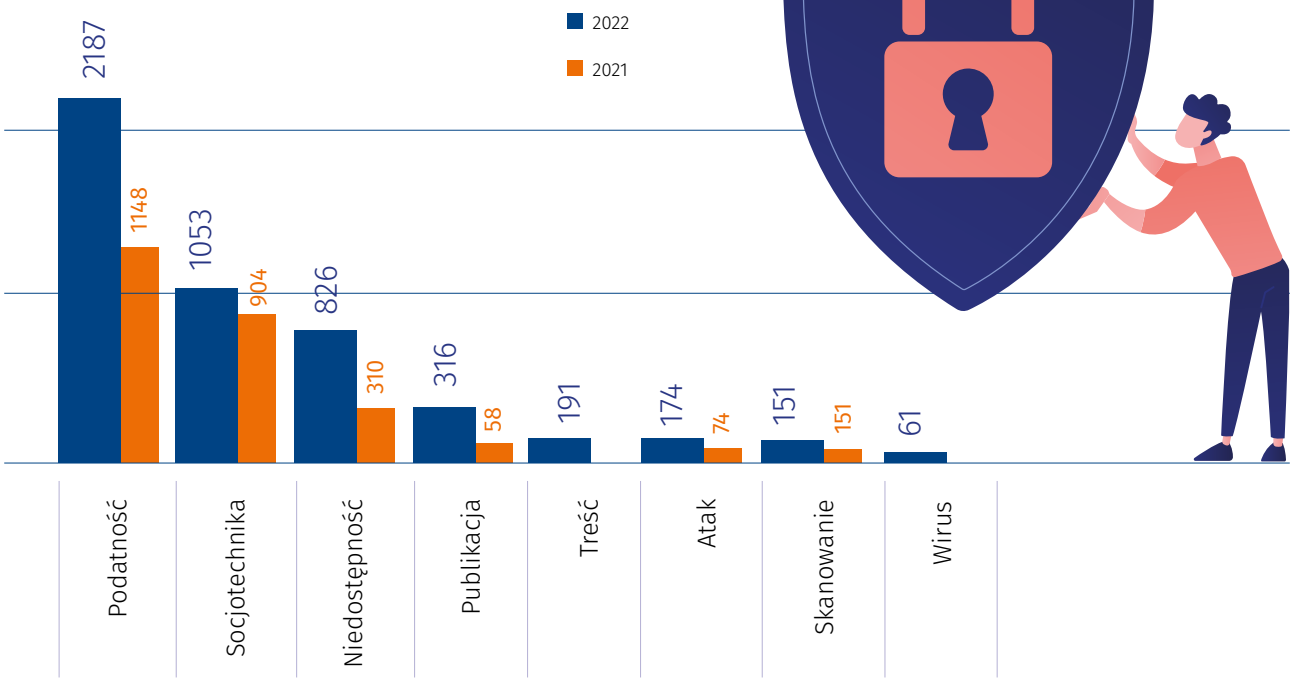
W roku 2022 odnotowano łącznie 1 234 040 zgłoszeń, w tym 21 563 zdarzenia, zdecydowanie więcej niż w 2021 r. z 762 175 zgłoszeniami, z czego zanotowano 26 899 zdarzeń.

Najwięcej zgłoszeń odnotowano w I i II kwartale 2022 r. (odpowiednio: 8937 i 8232), co wiązało się z wprowadzeniem w kraju stopni alarmowych: ALFA-CRP w styczniu i CHARLIE-CRP w lutym.

Liczba zarejestrowanych zgłoszeń i zdarzeń oraz incydentów w poszczególnych latach



Statystyka incydentów zgłoszonych przez podmioty krajowego systemu cyberbezpieczeństwa w 2022 r. i 2021 r.



Rodzaje incydentów

Najwięcej incydentów odnotowano w trzech kategoriach: podatność, socjotechnika, niedostępność.

PODATNOŚĆ: szczególnie problemy związane z wykrywaniem słabych punktów w systemach teleinformatycznych, błędów konfiguracyjnych i brakiem odpowiedniej polityki bezpieczeństwa w zakresie stałej aktualizacji oraz weryfikacji wdrożonych rozwiązań.

SOCJOTECHNIKA: kampanie phishingowe, podszycia oraz ataki z wykorzystaniem inżynierii społecznej, które miały na celu wyłudzenie informacji poufnych, zainfekowanie stacji roboczych bądź nakłonienie użytkownika do działań niezgodnych z zasadami bezpieczeństwa pracy w systemach teleinformatycznych. W statystyce ujęto głównie ukierunkowane ataki, wymierzone w infrastrukturę podmiotów oraz instytucji pozostających w zakresie właściwości CSIRT GOV.

NIEDOSTĘPNOŚĆ: incydenty polegające na niedostępności witryn internetowych, wynikających zarówno z ataków DDoS, jak i awarii czy wykonywanych prac technicznych. Od momentu wprowadzenia stopnia alarmowego CHARLIE-CRP na terenie kraju (luty 2022) odnotowano zwiększony wolumen kampanii DDoS realizowanych przez grupy haktywistyczne, m.in. NoName057(16), Killnet, CyberArmia Ludowa.

PUBLIKACJA: „wyciek" danych, nieuprawniona modyfikacja treści bądź kampania dezinformacyjna.

TREŚĆ: różne treści naruszające szeroko pojęte dobro publiczne.

ATAK: wszelkiego rodzaju ataki na systemy teleinformatyczne, w szczególności próby przełamania zabezpieczeń.

SKANOWANIE: wzmożony rekonesans infrastruktury teleinformatycznej administracji publicznej oraz podmiotów infrastruktury krytycznej w celu identyfikacji podatności systemów i usług.

WIRUS: infekcje stacji roboczych, serwerów, a także urządzeń sieciowych.

Infrastruktura krytyczna na celowniku

Najwięcej zgłoszeń dotyczyło zagrożeń dla systemów i sieci telekomunikacyjnych wykorzystywanych przez operatorów infrastruktury krytycznej.

Najbardziej narażona na ataki wycelowane w sieci i systemy teleinformatyczne jest infrastruktura krytyczna RP, w tym sektory energii i transportu, w szczególności lotniczego oraz kolejowego, ale także strony internetowe Narodowego Banku Polskiego, policji, administracji podatkowej operatorów sieci komórkowych.

Najistotniejszą kategorię zagrożeń stanowią dla niej incydenty z kategorii Wirus – zarówno w 2022 r., jak i w poprzednich. Największe niebezpieczeństwa to:

- brak aktualizacji systemów,
- brak odpowiedniej polityki bezpieczeństwa,
- brak monitorowania prób ataków,
- brak adekwatnego reagowania na incydenty.

Najbardziej zaawansowane zagrożenie dla cyberbezpieczeństwa infrastruktury teleinformatycznej organów administracji publicznej oraz stanowiącej element infrastruktury krytycznej stanowi działalność grup APT *(Advanced Persistent Threat)*. Identyfikacja ataków oraz ich powstrzymywanie to jedno z kluczowych wyzwań stojących przed zespołami CSIRT. ●

Pełny raport jest dostępny na stronie https://csirt.gov.pl.

DESIGNA

Inteligentne rozwiązania parkingowe

DESIGNA jest światowym liderem na rynku w pełni zautomatyzowanych systemów parkingowych, mającym 70-letnie doświadczenie w tworzeniu i dostawie nowoczesnych oraz nowatorskich rozwiązań. Już od ponad 10 lat dostarcza usługi typu *cloud services.*

Firma łączy klasyczne rozwiązania z najnowszymi technologiami, a dzięki adaptowalnym funkcjom cyfrowym tworzy najbardziej elastyczne systemy na rynku.

Rozwiązania DESIGNA na nowo definiują technologię zarządzania parkingami. Ponad 500 pracowników w 60 krajach dokłada wszelkich starań, aby spełniać złożone wymagania klientów. Każdy system jest starannie dostosowywany do rzeczywistych potrzeb odbiorców – lotnisk, hoteli, centrów handlowych, uniwersytetów, szpitali, a nawet całych miast. Wszystkie elementy systemów są precyzyjnie dopasowane do konkretnego zastosowania i opracowane z myślą o płynności funkcjonowania.

Duże, indywidualne systemy parkingowe DESIGNA zarządzają dziesiątkami tysięcy miejsc parkingowych lub stanowią inteligentną część całej sieci miejskiej. Firma opracowała i zainstalowała nowoczesne systemy zarządzania parkingami dla ponad 200 lotnisk na całym świecie, w tym w Nowym Jorku, New Jersey, we Frankfurcie czy na lotnisku Chopina w Warszawie – zawierające nieraz ponad 500 urządzeń. Najnowocześniejsze rozwiązania parkingowe działają też w szpitalach, np. w kilku obiektach sieci Main Line Health z Pensylwanii.

Inżynierowie firmy współpracują z wieloma agencjami rządowymi w celu opracowania unikalnych rozwiązań parkingowych dla miast i społeczności. Wszystko od DESIGNA, od rozwoju aż po produkcję, pochodzi z jednego źródła w Niemczech. ●

REKLAMA

NEDAP SECURITY MANAGEMENT

Nedap Security Day

4. edycja Nedap Security Day w 2023 r. odbyła się w Sierpcu. 13 września kilkadziesiąt osób spotkało się w hotelu Skansen na zaproszenie Nedap Security Management. Partnerami technologicznymi wydarzenia byli: HID Global, CBC Poland, iLOQ oraz Ela-compil. Uczestnicy dyskutowali o zmieniającym się środowisku pracy w branży security, cyberbezpieczeństwie, nowych rozwiązaniach security i chmurze, która staje się nieodzownym elementem systemów bezpieczeństwa.

Spotkanie otworzył Artur Kurasiński, inwestor i bloger technologiczny. Mówił o tym, jak chmura jest implementowana w biznesie. Czy obawy związane z jej stosowaniem są uzasadnione oraz jak rozmawiać z użytkownikami systemów zabezpieczeń, by strach nie odebrał im szansy na bezpieczne wejście w ten standard.

– *Chmury nie należy się bać. Chciałem uświadomić zgromadzonym słuchaczom, że to rozwiązanie bezpieczne, gdy pamiętają o kwestiach właścicielskich* – mówił A. Kurasiński.

Po spotkaniu Lidia Fałtyn z mBanku skomentowała: *Bardzo cenne i praktyczne wystąpienia ekspertów. Myślę, że były to skondensowane informacje, dzięki którym łatwiej poznać nowości na rynku.*

– *W naszej działalności korzystamy już z systemu Nedap. Moim celem było poznanie nowości w kontroli dostępu, które można by było implementować. Szczególnie że jako firma farmaceutyczna nie możemy korzystać ze wszystkiego, mamy ograniczenia prawne* – powiedział Przemysław Prajsner z Polpharma Biologics.

Z kolei Paweł Starszuk z Naftoportu zwrócił uwagę na wiele nowości i ciekawostek oraz możliwości integracji rozwiązań Nedap z produktami partnerów technologicznych firmy.

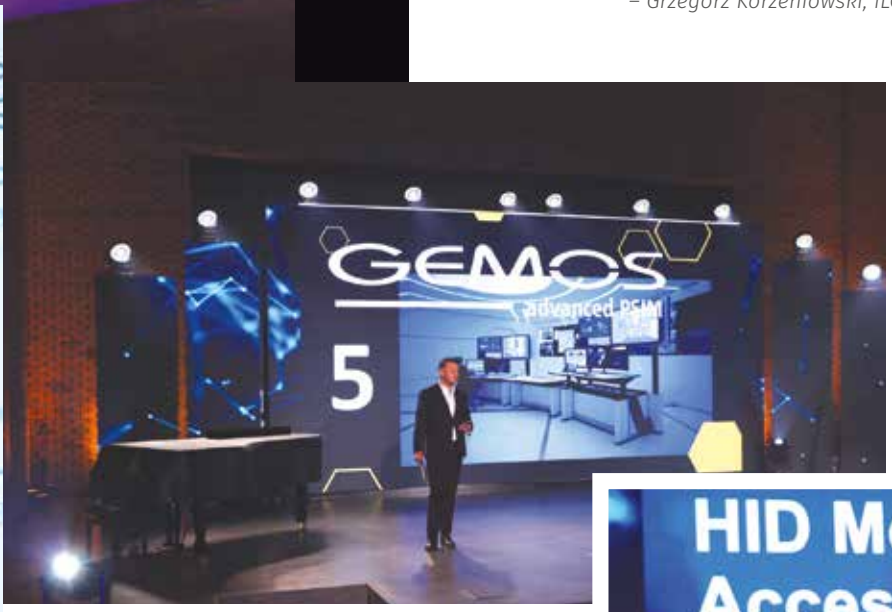
– *Dużą część tych rozwiązań moglibyśmy wykorzystać w naszych obiektach* – stwierdził P. Straszuk.

Kolejne jubileuszowe spotkanie w ramach Nedap Security Day w 2024 roku. ●

– *Nas, jako organizatorów, najbardziej cieszy frekwencja. Oprócz networkingu i możliwości spotkania w jednym miejscu integratorów, partnerów technologicznych oraz klientów końcowych mogliśmy zaprezentować naszą nowość Access At Work – system kontroli dostępu nowej generacji w chmurze, oferowany w modelu SaaS. Zaprezentowaliśmy także nowy system PACE – rozwiązanie do zarządzania tożsamością i i dostępem (PIAM – Physical Identity and Access Management) oraz intergrację naszego rozwiązania z Apple Wallet* – powiedziała Anna Twardowska, Nedap Security Management.

Połączenie naszych systemów przetestowaliśmy w praktyce – także mogliśmy pokazać istniejące, działające rozwiązanie. Zawsze ciekawsze jest zaprezentowanie na wydarzeniu wdrożenia, a nie samych produktów. To szczególnie ważne, bo pełną synergię pomiędzy AEOS a Ganz VMS Cortrol utworzyliśmy w stosunkowo krótkim czasie – Przemysław Szamocki, CBC Poland

Tematyka wydarzenia była bardzo nowoczesna i innowacyjna. Z naszej strony wpasowaliśmy się naturalnie z produktem, dzięki któremu można dostać się do obiektu za pomocą telefonu, a wkładki do bezprzewodowych zamków nie potrzebują dodatkowego źródła zasilania. Wydarzenie pełne nowości i trendów, mogliśmy zauważyć w którą stronę zmierza branża security – Grzegorz Korzeniowski, iLOQ



Prezentowaliśmy systemy integrujące Nedap z naszym PSIM Gemos. Mają one wiele zastosowań, pokazaliśmy klientom szereg wdrożeń w Polsce – od infrastruktury krytycznej, przez obiekty komercyjne aż po duże obiekty przemysłowe. Takie spotkania to wymiana doświadczeń i wiele ciekawych dyskusji, bardzo łączą one branżę – Łukasz Głowiński, ela-Compil.

Mieliśmy okazję zaprezentować integrację naszego rozwiązania dostępu mobilnego z platformą AEOS. Daje ona możliwość generowania poświadczeń mobilnych na smartfonach czy smartwatchach – z systemem iOS i Android. Myślę, że eventy, które skupiają się na konkretnych rozwiązaniach i dla konkretnych segmentów rynku są strzałem w dziesiątki zarówno dla nas, jak i dla klientów – Kamil Targalski, HID Global

AAT SYSTEMY BEZPIECZEŃSTWA

Teraz zobaczysz więcej

Kamery IP dualne (termowizyjne/wizyjne) NVIP-5H-6711/TA/3 oraz NVIP-5VE-6711/TA/3 marki NOVUS.

Charakterystyczną cechą kamer marki NOVUS jest THERMO DUAL VISION, rozwiązanie umożliwiające nałożenie obrazu termowizyjnego na obraz klasyczny. Funkcja ta jest przydatna np. w monitorowaniu instalacji przemysłowych – detekcja nadmiernie nagrzanych elementów może wskazywać na występowanie nieprawidłowości.

Funkcja detekcji ognia pozwala na zaalarmowanie użytkownika w razie wykrycia ognia w polu widzenia kamery – poprzez wysterowanie wyjścia alarmowego, alarm świetlny, alarm dźwiękowy, wiadomość e-mail lub wysłanie zdarzenia do rejestratora.

Kamery wyposażone są też w aktywne odstraszanie pozwalające na reagowanie na wykryte obiekty w celu odstraszenia potencjalnych intruzów. W momencie wykrycia obiektu kamera może świecić światłem ciągłym lub migającym, nadawać dźwięki ostrzegawcze lub komunikaty głosowe (liczba i dobór funkcji odstraszania różni się w zależności od modelu kamery). Funkcja ta ma na celu ochronę monitorowanego miejsca, zniechęcenie intruza do dalszych działań i odstraszenie go bez potrzeby interwencji ochrony.

Kamery wyposażono również w funkcje INGENIUS PLUS – m.in. klasyfikację typu obiektu, zliczanie obiektów, naruszenie strefy, przekroczenie linii. ●

LINC POLSKA

Teledyne FLIR – najnowsze kamery z serii FH

Bi-spektralne kamery marki Teledyne FLIR to wytrzymałe urządzenia stałopozycyjne, które łączą obrazowanie termowizyjne z obrazowaniem widzialnym 4K. Połączenie tych cech zapewnia niezawodność w wykrywaniu intruzów, a tym samym bezpieczeństwo w strefie ochrony obwodowej bez względu na warunki atmosferyczne.

Wbudowane funkcje analityczne oparte na konwolucyjnej sieci neuronowej (CNN) z dużą dokładnością wykrywają i jednocześnie klasyfikują zagrożenia (osoby, pojazdy). Wychwytują obiekty poruszające się zarówno z dużą, jak i małą prędkością, minimalizując przy tym fałszywe alarmy.

Dzięki połączeniu komplementarnych technologii kamery Teledyne FLIR umożliwiają nieszablonowe podejście do projektowania systemów zabezpieczeń – zapewniając skuteczną ochronę obiektów, niezależnie od pory dnia i pogody. Nie tylko warunki atmosferyczne mają wpływ na pogorszenie widoczności, ale dym czy rozpylony gaz równie skutecznie uniemożliwia pracę kamer z obrazowaniem widzialnym – wtedy nieoceniona okazuje się technologia termowizyjna.

Tak właśnie działają nowe kamery Teledyne FLIR z serii FH. ●

ROGER

Integracja systemu RACS 5 z systemem rezerwacji biurowych URVE Smart Office

System kontroli dostępu klasy Enterprise o nazwie RACS 5 firmy Roger zyskał w ostatnich 5 latach sprzedaży renomę atrakcyjnego, sprawdzonego rozwiązania na rynku projektowym.

Przekłada się to zarówno na kolejne realizacje, jak i zainteresowanie innych dostawców rozwiązań na tym rynku. Kolejną firmą, która zdecydowała się na integrację swoich rozwiązań z systemem RACS 5, jest Eveo — uznany dostawca rozwiązań z zakresu smart office.

Integracja systemu URVE Smart Office z systemem RACS 5 została zrealizowana za pośrednictwem tzw. usługi Serwera Integracji. Oprogramowanie URVE Smart Office pozwala na wygodne zarządzanie pomieszczeniami konferencyjnymi, biurkami, miejscami parkingowymi, szafkami i innymi dowolnymi zasobami w biurze. Użytkownicy mogą korzystać ze Smart Office za pomocą aplikacji instalowanej na telefonie komórkowym lub za pośrednictwem interaktywnego panelu. Umożliwia rezerwację pokoi spotkań, sprawdzanie i współtworzenie harmonogramów dostępności przestrzeni biurowej. Na podstawie rezerwacji system Eveo tworzy użytkownika w systemie RACS 5 i nadaje mu czasowe uprawnienia dostępu do przejść i pomieszczeń. Rozpoznawane i rejestrowane jest też skorzystanie użytkownika z zarezerwowanego pomieszczenia.

Rozwiązanie znajduje zastosowanie przede wszystkim w biurowcach, ale można je z powodzeniem wykorzystać wszędzie tam, gdzie trzeba dynamicznie i sprawnie zarządzać przestrzenią biurową. ●

EUROPEAN SECURITY TRADING POLSKA

Wsparcie operacji a bezpieczeństwo

19 września w Kinogramie w Fabryce Norblina odbyły się warsztaty „Wsparcie operacji a bezpieczeństwo" dla specjalistów z branży transport i logistyka prowadzone przez European Security Trading Polska i firmę Genetec.

Warsztaty są przeznaczone dla przedstawicieli firm, którzy w swoich organizacjach zajmują się bezpieczeństwem: menedżerów security and safety, loss prevention, zarządzania kryzysowego czy zarządzania ryzykiem. Na to wydanie zaproszono specjalistów z branży transportu i logistyki.

W trakcie spotkania uczestnicy dyskutowali o tym, jak powinna wyglądać integracja systemów w obszarze monitoringu wizyjnego, jak poprawić efektywność analityki wideo w logistyce i jak zoptymalizować architekturę systemu, by wspierać łańcuch dostaw. ●

HANWHA VISION

Kamera SolidEDGE – urządzenie brzegowe z aplikacją VMS

Wprowadzona na rynek przez Hanwha Vision kamera SolidEDGE jest pierwszą na rynku kamerą opartą na dyskach półprzewodnikowych (SSD) klasy przemysłowej z wbudowanym serwerem Wisenet WAVE VMS.

W ofercie znajdują się dwa modele – PNV-A6081R-E1T (1 TB pamięci masowej) i PNV-A6081R-E2T (2 TB). Żaden z nich nie wymaga serwera zewnętrznego ani subskrypcji w chmurze do przechowywania materiałów czy szybkiej łączności, pozostawiając kontrolę nad danymi przechowywanymi lokalnie na miejscu.

Kamera SolidEDGE jest wyposażona w funkcję zarządzania wideo w chmurze za pomocą Wisenet WAVE Sync. Dzięki nowoczesnym roziwązaniom urzadzenie jest szczególnie atrakcyjne dla zdalnych instalacji, w których nie ma miejsca na serwer lub NVR, np. wokół bankomatów, farm fotowoltaicznych, podstacji elektrycznych, przejazdów kolejowych, dworców autobusowych czy małych niezależnych sklepów. ●

ZKTECO

Bramki uchylne SBTL 8000

Firma ZKTeco wprowadziła na rynek kolejną serię szybkich bramek uchylnych do zastosowań wewnętrznych, charakteryzujących się modułowością konstrukcji panelu czytnika. Modularyzacja ta nie tylko przynosi korzyści użytkownikom (łatwa aktualizacja czytnika), ale także pomaga odciążyć magazyny dystrybutorów (umożliwia szybkie dostawy produktu dopasowanego do potrzeb klientów). Wybór modeli jest szeroki: od czytników kart RFID, po czytniki biometryczne (np. linii papilarnych czy rozpoznające twarz).

Montaż lub wymiana czytnika jest prosta i nie wymaga ani obróbki mechanicznej, ani wiercenia. Poprawiono też efektywność i wygodę użytkowania bramek – zastosowano nowy typ serwomotoru, który sprawia, że mają one większą od poprzednich modeli prędkość otwierania i niższy poziom hałasu. Wyniki testu pokazują, że prędkość otwierania tej bramki zmniejsza się do 0,8 s. Dla większej precyzji liczbę czujników podczerwieni zwiększono do 10 par.

Obudowa bramki wykonana jest w większości ze stali nierdzewnej SUS304 wysokiej jakości, zapewniającej wyjątkową trwałość urządzenia. Panele wykonane są z akrylu o wysokiej odporności na starzenie i uszkodzenia mechaniczne.

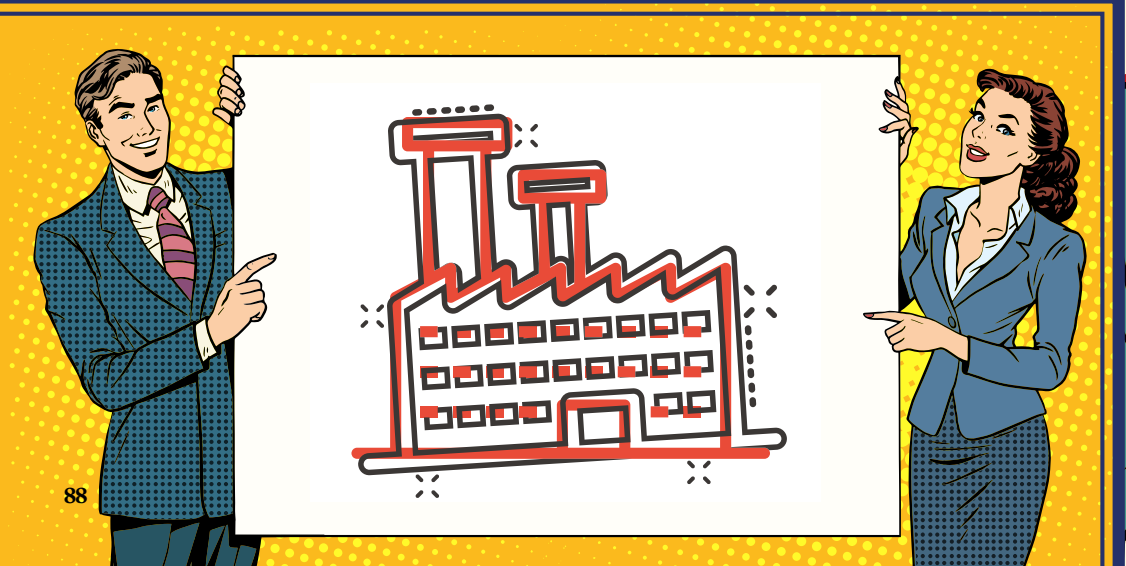
Inne cechy bramek SBTL 8000: nowoczesny wygląd, dwukierunkowa kontrola działania, wskaźnik przejścia LED w obu kierunkach, tryb awaryjny umożliwiający swobodny dostęp w razie awarii zasilania lub sytuacji wyjątkowej. Bramki mają przepustowość 40 osób/min, szerokość przejścia 66 cm, a wymiary zewnętrzne (dł. x szer. x wys.) 160 x 104 x 102 [cm]. Firma oferuje też bramki tej serii w wersji z poszerzonym do 92 cm przejściem i podwyższoną barierą do 150 cm. ●

Od tygodni nie padało

Marianna była osobą bystrą i wścibską. Miała tego świadomość. Mawiała o sobie, że ma wzrok jak słoń, a pamięć jak jastrząb. Albo na odwrót. Zawsze się jej myliło. Na studia z ochrony środowiska wybrała się z premedytacją. Miała tropić firmy uprawiające *greenwashing*, znajdować źródła wszelkich zanieczyszczeń i walczyć z każdym, kto zagraża naturze.

Plany były ambitne, ale na razie utknęła na stażu w małej hucie, w której, co tu dużo kryć, roboty dla niej było niewiele. Diabli nadali, że trafił jej się zakład, w którym wszyscy przestrzegali przepisów BHP, a zarząd stawał na głowie, by firma dostała certyfikat The Cooper Mark. Na razie było do tego jeszcze daleko, ale Marianna miała okazję się przekonać, że dział odpowiedzialny za ochronę środowiska naprawdę robi, co może, by huta jak najmniej szkodziła otoczeniu.

Nic więc dziwnego, że zamiast śledzić uchybienia przeciwko przepisom, młoda stażystka każdego ranka najpierw sprawdzała wraz z szefem, czy wszystkie parametry pracy huty są zgodne z wyśrubowanymi normami środowiskowymi, a potem wędrowała „po obiekcie". Tego dnia chciała zajrzeć do walcowni, ale gdy tylko przekroczyła jej próg, groźny wąsaty majster obszotrcował ją haniebnie, że „dziewuszysko włóczy się po próżnicy i jeszcze z tego jakieś nieszczęście będzie". Nie pozostało jej nic innego, jak powędrować do pokoju socjalnego na zasłużone późne śniadanie.



Kto po nocach nie śpi?

Stała właśnie z głową w lodówce, gapiąc się jak sroka w gnat w puste miejsce po serku wiejskim, którego na pewno nie zjadła, kiedy drzwi do „socjalnego" otworzyły się z hukiem i do pomieszczenia wkroczyli Adam Jagodziński, główny technolog huty, oraz odpowiedzialny za zaopatrzenie w surowce Robert Mucha, zwany Bzykiem.

– …i problem jest! – Jagodziński prawie krzyczał.

Marianna zastrzygła uszami. Problemy. W końcu coś się dzieje.

– Adasiu, ty się tak nie unoś. – Bzyk ewidentnie próbował łagodzić ton dyskusji.

– No jak nie unoś, jak nie unoś, jak tu problem jest! – Główny technolog aż poczerwieniał ze złości. – Co chwila coś się dzieje. Przecież ja pieca nie wygaszę, ot tak! Ty wiesz, jakie to pieniądze?! – Jagodziński rozlał kawę, którą zamaszyście nalał z ekspresu przelewowego. Wycierając podłogę, klął pod nosem szpetnie i mamrotał: „Panie Jagodziński, Adasiu, nie denerwuj się, będzie dobrze. A cholera, kto potem po nocach spać nie może? Ja!".

Marianna zrozumiała, że kroi się jakaś grubsza afera, choć zupełnie nie z jej branży. Wprawdzie przez ostatnie miesiące tego i owego o działaniu huty się dowiedziała, ale miała świadomość, że to tylko wierzchołek góry lodowej. „A może raczej wulkanu? Tak, wulkan bardziej pasuje do huty", ustaliła w myślach.

– Adamie, przecież wiem, jakie to pieniądze. – Bzyk próbował zachować spokój. – Wiem, że coś tu jest nie tak. Ale dopóki nie znajdę źródła kłopotów, to nic nie poradzę. Przecież nie będę ręcznie przerzucał całego złomu, który do nas przyjeżdża. Wszystko mamy zautomaty…

– Automatyzacja-sracja! – Jagodziński poderwał się znad podłogi, rozlał resztę kawy, tym razem stawiając gwałtownie kubek na kuchennym blacie. – Jak tu chłopaki sami rozładowywali, to nie było takich sytuacji! Wszystko chodziło jak w zegarku. A teraz?! Teraz mnie się parametry surówki nie zgadzają. Ty wiesz, ile ja muszę dodatków stopowych dorzucać!? Za darmo nie są! Na drzewach nie rosną! – To mówiąc, Jagodziński walnął mop w kąt i gwałtownie usiadł na krześle, które niepokojąco jęknęło. – Jakbym tam wody dolewał, cholera, tak to wygląda.

– Główny technolog dodał głosem już trochę spokojniejszym.

– Wiesz, czytałem o pewnym procederze i – tu Bzyk się chwilę zasępił – nie jest to niemożliwe. Na razie jednak nikogo za rękę nie złapałem. Kontrolujemy wyrywkowo, wszystkich nie jesteśmy w stanie. Sam wiesz, że trzeba było zautomatyzować. Inaczej się nie da. Dostawców mamy sprawdzonych. Widzisz zresztą – Robert wskazał za okno – ile tego do nas zjeżdża.

Obaj panowie, Marianna również, spojrzeli odruchowo na plac.

– A tam co znowu? – jęknął Bzyk. – Za czym kolejka ta stoi? Znaczy się – poprawił się szybko Robert Mucha – dlaczego stoi?

Faktycznie, za główną bramą wjazdową do huty ustawiła się kolejka ciężarówek załadowanych złomem. „Jak w PRL-u za papierem toaletowym", pomyślała Marianna, a potem szybko się poprawiła: „Po papier, bo za papierem to rusycyzm". O tym, jak wyglądał PRL, opowiadali Mariannie rodzice.

– To może ja pójdę sprawdzić? – Marianna zapytała cichutkim głosikiem. – Bo i tak do sklepu idę. Tego za bramą. Po serek i colę, sami panowie wiecie, siła nałogu. Dziesięć minut i wrócę.

– A idź, dziecko, idź – Bzyk był od Marianny starszy raptem lat dziewięć, ale jakoś tak się utarło, że Robert Mucha jest starszy od wszystkich, łącznie z główną księgową, której tylko trzy miesiące do emerytury zostało. Może z tej prostej przyczyny, że zawsze miał zbolały wyraz twarzy i poruszał się niespiesznie.

Straszna susza

Marianna ruszyła żwawym krokiem przez plac. Dotarła do bramy, gdzie władzę o tej porze trzymał niewzruszony jak skała pracownik wartowni Piotr Kamieniak.

– Cóż to się stało, panie Piotrze? – zapytała Marianna, która choć w hucie była od niedawna, wszystkich już doskonale znała. O Kamieniaku wiedziała, że ma żonę, trzy ukochane wnuczki, jazgotliwego jamnika i złote serce. Ryby łowił, ale przestał, bo mu się z wiekiem porobiło tak, że ich mu szkoda. Za to nabył akwarium. Wiedziałaby wiele więcej, ale ostatecznie widywali się może minutę każdego dnia.

Piotr Kamieniak z rezygnacją machnął ręką.

– Się nam tu jedna ciężarówka rozkraczyła, jak sam raz na wadze. Dopóki nie zjedzie, to stoi reszta. Drugiej wagi nie ma, a bez wagi na plac nie wpuszczę.

– Jasna sprawa. – Marianna pokiwała głową ze zrozumieniem. Nagle dostrzegła coś kątem oka i zapytała z głupia frant: – Panie Piotrze, a w nocy to padało?

– Padało? Jakie padało? – Kamieniak nie krył zdumienia. – Sucho jak pieprz, pomidory muszę podlewać, trawa schnie. Od tygodni ani kropli.

Marianna, idąc w stronę jednej z ciężarówek, z której dziwnym trafem

kapała jakby woda czy błoto, nie słuchała już narzekania Kamieniaka na brak opadów i mszyce. Pewna myśl zaświtała jej w głowie.

Triumf dedukcji

Gdy wróciła z serkiem (o coli oczywiście zapomniała), dwaj panowie czekali z niecierpliwością na wieści „za czym kolejka ta stoi". Chwilę później do pomieszczenia wkroczył szef ochrony.

– *Panowie, zechcecie, proszę, spojrzeć za okno?* – zaczęła Marianna. – *Na trzecią w kolejce ciężarówkę.*

Panowie zechcieli. A potem jak jeden mąż ze zdziwieniem spojrzeli na Mariannę.

– I…? – Jagodziński uniósł pytająco brwi.

– I odpowiedzcie mi na pytanie: kiedy ostatnio padał deszcz? – Marianna poczuła się jak skrzyżowanie panny Marple z porucznikiem Borewiczem. Żaden z nich nie mógł sobie przypomnieć.

– No właśnie! Nie padało od tygodni. Co panowie na to? – Marianna triumfalnie podniosła palec.

Opracowała Monika Mamakis na bazie scenariusza Jacka Grzechowiaka

- **Co takiego zwróciło uwagę młodej stażystki, kiedy wychodziła za bramę huty, i jaki związek może to mieć z kłopotami głównego technologa?**

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

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

Paweł Wawryła, Volvo Polska

Dzisiejsze szkolenie było bardzo aktywne. Ta ciekawa forma angażowała uczestników, nie byliśmy tylko biernymi słuchaczami, ale mogliśmy faktycznie wymienić się doświadczeniami z najlepszymi ekspertami w branży. Myślę, że to była ciekawa lekcja dla nas i wszystkim to szkolenie polecam. Dziękuję organizatorom za możliwość uczestnictwa.

Piotr Kozak, DB Schenker

Szkolenie było bardzo praktyczne. Świetnie przedstawiony i z dużym zaangażowaniem ciekawy case, który zwrócił nam uwagę na wiele rzeczy, których na co dzień sobie nie uświadamiamy. Myślę, że wszystkim nam to uzmysłowiło, jak szeroką wiedzę muszą mieć ludzie z tej branży i jak głęboko trzeba wejść w szczegóły działalności zakładu, aby móc zapobiegać stratom i zapewnić bezpieczeństwo.

Jacek Baran, 3M

Forma szkolenia bardzo pozytywnie mnie zaskoczyła. Było to ciekawe omówienie konkretnego zdarzenia, a zagadką było, co się następnie wydarzy. Na tym przykładzie można było zdobyć wiedzę o specyfice prowadzenia śledztw i mogących wystąpić pułapkach. Szkolenie dało mi dużo do myślenia i z pewnością wykorzystam tę wiedzę w swojej pracy, gdyż teraz lepiej rozumiem niuanse występujące w takich przypadkach.


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

BCS®

dla profesjonalistów

Szeroka perspektywa obrazu

Termowizja z obiektywem o ogniskowej 2 mm i taka sama ogniskowa na przetworniku wizyjnym zapewniają bardzo szeroki kąt obserwacji. To w połączeniu z funkcjami ochrony obwodowej doskonale zabezpieczy Twoje mienie w każdych warunkach.

POLSKA MARKA BCS

www.bcs.pl

www.facebook.com/bcspl