CZASOPISMO RYNKU SECURITY

a&S POLSKA

№ 05
2019 (17)
wrzesień /październik

przemysł 4.0

www.aspolska.pl

15 zł
(w tym 8% VAT)

ISSN 2451-5175
05
9 772451 517703

HIKVISION

KOLOROWY OBRAZ, NAWET W CIEMNOŚCI

Poznaj produkty:
DS-2CE72DFT-F(3.6mm)
DS-2CE10DFT-F(3.6mm)
DS-2CD2347G1-L(4mm)
DS-2CD2T47G1-L(4mm)

Ciesz się żywym, kolorowym obrazem przez całą dobę, dzięki technologii ColorVu

– Jasny obiektyw
Przez obiektyw F 1.0 do przetwornika dociera więcej światła, przez co uzyskasz jaśniejszy obraz

– Wysoka czułość
Dużo lepsze wykorzystanie docierającego światła, dzięki zaawansowanym przetwornikom

– Przyjazne oświetlenie
W pełnej ciemności ciepłe oświetlenie zagwarantuje kolorowy obraz

Dołącz do Programu Partnerskiego Hikvision i uzyskaj dostęp do najnowszych promocji oraz pełnego wsparcia Hikvision!
Wejdź na: **https://partner.hikvision.com/eu/**

Hikvision Poland Sp. z o.o.
ul. Krakowiaków 50
02-255 Warszawa
T +48 22 4600150
info.pl@hikvision.com

@HikvisionPoland @HikvisionEurope HIKVISION Poland www.hikvision.com/pl/

HIKVISION

WIELKA URODZINOWA LOTERIA HIKVISION

1. DOŁĄCZ DO PROGRAMU PARTNERSKIEGO HIKVISION.
2. KUPUJ PRODUKTY HIKVISION I WEŹ FAKTURĘ, NA KTÓREJ BĘDĄ WYŁĄCZNIE PRODUKTY TEJ MARKI. ZA KAŻDY WYDANY 1000 PLN NETTO OTRZYMASZ 1 SZANSĘ NA WYGRANĄ. ZACHOWAJ DOWODY ZAKUPÓW
3. REJESTRUJ SWOJE ZAKUPY NA **LOTERIAHIKVISION.PL**
4. WEŹ UDZIAŁ W LOSOWANIU

5 FIATÓW FIORINO

CZAS TRWANIA LOTERII: **01.06.19 – 15.11.19**
SZCZEGÓŁY I REGULAMIN NA STRONIE ORAGNIZATORA WWW.SMOLAR.PL I WWW.LOTERIAHIKVISION.PL

EDYTORIAL

Drodzy Czytelnicy

Jedyne, czego możemy być pewni, to zmiana. Maksyma ta znajduje potwierdzenie w każdej dziedzinie życia. **W aspekcie bezpieczeństwa zmiana otoczenia czy funkcjonowania obiektu jest przesłanką do zmodyfikowania koncepcji zabezpieczenia. Zmiana warunków gospodarczych może z kolei skłonić do przejścia od ochrony fizycznej do technicznej.** Zdarza się, że zabezpieczenia techniczne – zamiast podnosić – obniżają poziom bezpieczeństwa. O paradoksie stosowania systemów kontroli dostępu bez odpowiednich procedur i szkoleń piszemy na s. 24.
Zmiana sposobu funkcjonowania i postępująca globalizacja powodują potrzebę coraz większej integracji urządzeń i systemów security. Już w pojedynczym obiekcie przynosi to wymierne korzyści w postaci poprawy poziomu bezpieczeństwa, jeszcze większe znaczenie ma to w lokalizacjach rozproszonych. Tak jest w opisywanym przez nas przypadku rozproszonej infrastruktury zarządzanej przez Służbę Więzienną (s. 32).

Zmiana świata na cyfrowy to efekt postępującej digitalizacji. Dzięki temu branża security może wspierać się algorytmami sztucznej inteligencji. **Dlaczego jednak, nawet przy zaawansowanych algorytmach analizy wizyjnej, efekt działania systemów wizyjnych jest czasem niezadowalający? Czy to kwestia nieprawidłowej implementacji, czy błędów w konfiguracji, projektowaniu, a może doborze sprzętu?** Odpowiedź tkwi w jakości obrazu, jaki dostarczamy na wejściu danego algorytmu – polecamy obszerny artykuł na ten temat (s. 40). Prezentujemy także ofertę rynkową kamer do tego typu zastosowań (s. 46).

Dynamiczny rozwój robotyzacji polski przemysł ma dopiero przed sobą, jednak już dziś wiele firm zdaje sobie sprawę, że bez wdrożenia odpowiednich procesów pozostaną w tyle za zachodnimi konkurentami (s. 49). **Roboty coraz częściej są wykorzystywane w przemyśle, i ta tendencja będzie rosnąć. Aby zapewnić akceptowalne bezpieczeństwo współpracy człowieka z robotem, pojawił się robot współpracujący – cobot.** Szukamy odpowiedzi na pytania o przyszłość i współpracę człowieka z maszyną (s. 50). Zadajemy także 10 pytań o bezpieczeństwo przemysłowych systemów sterowania, na które odpowiedzi powinna znać każda firma z branży produkcyjnej (s. 56)
Polecamy także artykuł o bezpieczeństwie przemysłowym w obliczu nadchodzących zmian (s. 66) oraz o bezpieczeństwie rozproszonych obiektów przemysłowych (s. 70). Na naszych łamach nie mogło też zabraknąć głosu branży licznie reprezentowanej zarówno przez specjalistów oferujących systemy zabezpieczeń, jak i doświadczonych szefów bezpieczeństwa z firm przemysłowych (s. 77).

W dziale Bezpieczeństwo biznesu przedstawiamy osiem rad, jak wykryć i powstrzymać kradzież z firmowego magazynu (s. 92). To istotne, szczególnie że coraz chętniej stosowana automatyzacja likwiduje część problemów, jednak osobom nieuczciwym tworzy nowe możliwości kradzieży.

W tym wydaniu rozpoczynamy cykl rozmów z ważnymi dla branży ludźmi, które będą zamykały każdy kolejny numer a&s Polska. Cykl inaugurujemy wywiadem z Grzegorzem Ćwiekiem, prezesem Schrack Seconet Polska, który zdradza swoje plany na przyszłość i ogłasza zmianę w fotelu prezesa firmy! (s. 106)

Wszystkim Czytelnikom życzymy samych pozytywnych zmian!

Marta Dynakowska
REDAKTOR NACZELNA

Jan T. Grusznic
Z-CA REDAKTORA NACZELNEGO

Mariusz Kucharski
DYREKTOR ZARZĄDZAJĄCY

a&S POLSKA

www.aspolska.pl

Wydawca
A&S Polska Sp. z o.o.
ul. Rondo ONZ 1
00-124 Warszawa

Dyrektor zarządzający
Mariusz Kucharski

Redaktor naczelna
Marta Dynakowska

Z-ca redaktora naczelnego
Jan T. Grusznic

Stały felietonista
Andrzej Popielski

Dział marketingu i reklamy
Iwona Krawiec

Dział eventów i konferencji
Jolanta A. Kucharska
Aleksandra Czapska

Projekt graficzny i skład
Bogusław Kalwala

Redakcja
ul. A. Branickiego 15
Wilanów Office Park, bud. 1
02-972 Warszawa
e-mail: info@aspolska.pl
www.aspolska.pl

Kolegium redakcyjne
Norbert Bartkowiak
Sebastian Błażkiewicz
Marek Domański
Jacek Grzechowiak
Rafał Łupkowski
Przemysław Pierzchała
Janusz Sawicki
Stefan Jerzy Siudalski
Jerzy Sobstel
Jacek Tyburek
Paweł Wittich
Waldemar Wnęk
Aleksander M. Woronow

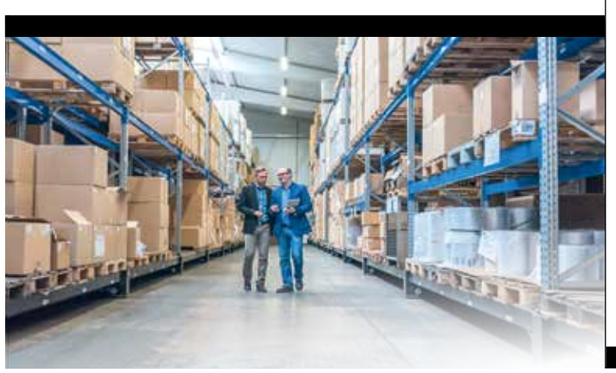
Korekta
Jolanta Kucharska

Prenumerata
www.aspolska.pl/prenumerata

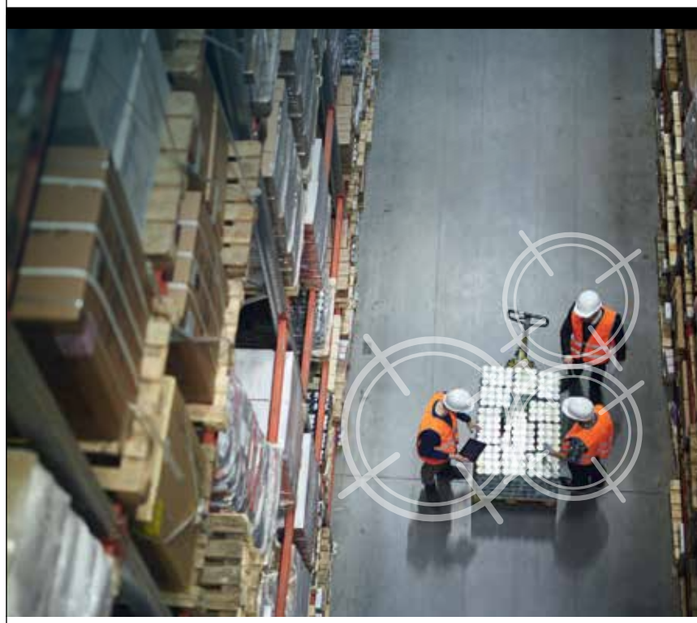
SPIS TREŚCI

№ 05
2019 (17)
wrzesień/październik
a&S POLSKA

BEZPIECZEŃSTWO POŻAROWE



BEZPIECZEŃSTWO BIZNESU



SERWIS INFORMACYJNY

WYWIAD

FELIETON O BEZPIECZEŃSTWIE

ATTE www.atte.pl

xPoE-3 Miniaturowy switch i extender PoE

xPoE-3-11 to chyba najmniejszy 3-portowy (1xPoE IN 802.3at/af + 2xPoE OUT) profesjonalny switch i extender PoE dostępny na rynku. Powstał przy ścisłej współpracy z instalatorami CCTV, której celem było zaprojektowanie mniejszego odpowiednika znanego na rynku extendera xPoE-4-11-HS. Miniaturowe rozmiary i kierunek złącz RJ-45 umożliwiają montaż urządzenia bezpośrednio w podstawie kamery, bez konieczności prowadzenia dodatkowego okablowania i puszek instalacyjnych.

Najważniejsze cechy:
- zasilany bezpośrednio z PoE 802.3at/af lub PoE Passive
- przenosi zasilanie PoE na wyjścia (sumaryczna moc do 50 W)
- rozdziela i „przedłuża" LAN o kolejne 100 m
- zwarta, miniaturowa zintegrowana obudowa z poliwęglanu
- szeroki zakres temperatury pracy
- bardzo niski pobór mocy (<1 W)

xPoE-3-11 został zaprojektowany jako extender *(repeater)* sieci LAN oraz zasilania PoE. Regeneruje sygnał sieciowy i przenosi zasilanie PoE na wybrane wyjścia. Najczęściej stosowany jako „wzmacniacz" do przedłużania sieci na odcinkach dłuższych niż 100 m. Ponadto idealnie sprawdza się jako „aktywny rozdzielacz" w sytuacjach, gdy na jednym kablu trzeba uruchomić kilka odbiorników PoE (np. kilka kamer IP), lub gdy jest potrzebne dodatkowe odgałęzienie sieciowe.

Urządzenie występuje w dwóch wersjach: xPoE-3-10 i xPoE-3-11. Bardziej uniwersalny xPoE-3-11 może być zasilany z dowolnego switcha 802.3at/af lub PoE PASSIVE, natomiast mniejszy xPoE-3-10 wyłącznie ze switcha lub adaptera PoE PASSIVE.

AXIS COMMUNICATIONS www.axis.com/pl

AXIS Q6215-LE sieciowa kamera PTZ

Wzmocniona kamera PTZ z funkcją OptimizedIR
- ➔ HDTV 1080p i 30-krotny zoom optyczny
- ➔ Optymalizowane oświetlenie w zakresie podczerwieni OptimizedIR (zasięg 400 m)

- ➔ Przetwornik obrazu 1/2", szeroki zakres dynamiki
- ➔ Zgodność z MIL-STD-810G i NEMA TS-2
- ➔ Klasa ochrony obudowy IP66/IP68, odporność mechaniczna IK10
- ➔ Łatwy montaż w dowolnym miejscu

AXIS Q6215-LE to niezawodna, wytrzymała kamera sieciowa przeznaczona do monitorowania na dużą odległość. Udostępnia precyzyjne funkcje PTZ i oświetlacz IR o dużym zasięgu. Rozpoznaje i identyfikuje cele na rozległych otwartych obszarach nawet przy słabym oświetleniu lub w całkowitej ciemności – porty i lotniska, autostrady. Spełnia wymagania normy MIL-STD-810G, zapewniając niezawodne działanie w ekstremalnych warunkach pogodowych i przy wietrze o prędkości do 245 km/h (152 mph). Szczelna obudowa o klasie ochrony IP66/68 i odporności mechanicznej IK10 oznacza, że kamera jest odporna na działanie warunków atmosferycznych (opady) i akty wandalizmu. Może być montowana z obiektywem skierowanym w górę lub w dół, w zależności od potrzeb (w zestawie płytka montażowa z suwakami). Dzięki wbudowanej wycieraczce obrazy mają dobrą jakość nawet podczas opadów.

BCS www.bcscctv.pl

Nowa seria kamer BCS-Ai

Tej jesieni swoją premierę ma nowa seria kamer IP BCS Line wyposażona w algorytmy sztucznej inteligencji. Seria ta składa się z pięciu modeli kamer dostępnych w rozdzielczościach 2 i 5 Mpix: dwa modele kamer tubowych i dwa kamer kopułowych, w wersjach z regulowanym bądź stałym obiektywem, oraz dobrze wszystkim znana wersja box umożliwiająca dobór konkretnego obiektywu.

Co odróżnia tę serię kamer od spotykanych dotychczas, już oferujących różnego typu mniej lub bardziej zaawansowaną analizę obrazu? Otóż dostajemy teraz wzbogaconą o zbieranie metadanych detekcję twarzy, funkcję liczenia osób wchodzących czy osób pozostających dłużej w strefie – dla obu funkcji można określić 4 obszary detekcji.

Decydując się na dodatkowe filtrowanie obiektów wyzwalających alarm, można zmniejszyć liczbę fałszywych alarmów, a jednocześnie ukierunkować system na wykrywanie konkretnego typu zdarzeń.

Jednak najszybciej będzie można zaadaptować i wykorzystać w wizyjnym systemie monitoringu funkcje wspierające ochronę obwodową. Można skorzystać z dobrze już znanych funkcji przekroczenia linii czy wtargnięcia w strefę, dodatkowo określając, jakiego typu obiekt taką linię czy strefę naruszy.

Dzięki umiejętności klasyfikacji obiektów, kamery dokładniej kontrolują obserwowany teren. Monitorując miejsca parkingowe, mogą wykrywać obiekty pozostające w strefie zbyt długo, a także takie niestandardowe zachowania, jak tzw. wałęsanie czy gromadzenie się tłumu.

DAHUA TECHNOLOGY POLAND www.dahuasecurity.com/pl

ASR2201 Czytnik z modułem Bluetooth

Firma Dahua Technology wprowadziła do oferty czytnik umożliwiający identyfikację użytkownika poprzez aplikację zainstalowaną na urządzeniu mobilnym. Przesłanie informacji z urządzenia mobilnego jest realizowane z wykorzystaniem protokołu Bluetooth. Użytkownik, który chciałby korzystać z identyfikatora mobilnego, powinien zgłosić się do administratora systemu kontroli dostępu w celu otrzymania kodu QR powiązanego ze swoim kontem w programie **SmartPSS lub DSS Express**. Kod QR należy dodać do aplikacji **Easy4Key,** którą można pobrać ze sklepu Google. Jest to aplikacja firmy Dahua Technology przeznaczona do obsługi tego modelu czytnika. W celu identyfikacji w czytniku należy nacisnąć przycisk Door w aplikacji lub potrząsnąć urządzeniem mobilnym.
Terminal oferuje ponadto weryfikację użytkownika w sposób tradycyjny, tj. za pomocą identyfikatora **RFID formatu Unique 125 kHz** (**model ASR2201D-BD**), **Mifare Classic 13,56 MHz (model ASR2201D)** lub kodu PIN (dotyczy obu modeli). Komunikacja czytnika z kontrolerem odbywa się za pomocą protokołu RS485 lub Wiegand 34. Producent posiada w swojej ofercie również firmware z protokołem **Wiegand 26 bitów**. Obudowa czytnika ma stopień ochrony **IP65.**

GDE www.gde.pl

Rejestrator IMVR-08QPOE z nowej serii Q

Firma MAZi wprowadziła do oferty nową serię rejestratorów IP. Mniej wprawnych użytkowników zainteresuje metoda *plug-and-play* – wystarczy podłączyć kamery MAZi do portów PoE i po chwili połączenie z kamerami oraz nagrywanie skonfiguruje się automatycznie. Rejestratory IMVR idealnie nadają się do małych systemów dozoru wizyjnego wyposażonych w najbardziej popularne kamery o rozdzielczości **2 i 4 Mpix** z kodekami **H.265+/H.265/H.264+/H.264.** Zapewniona jest pełna współpraca z kamerami wyposażonymi w analitykę obrazu (dotyczy kamer z kompatybilnymi funkcjami **VCA**), m.in. detekcję przekroczenia linii. Rejestrator może być zarządzany przez smartfon, przeglądarkę, a także zaawansowane oprogramowanie na Windows, pozwalające na zarządzanie ponad **200 urządzeniami** liczącymi łącznie ponad **1000 kanałów**. Dzięki pracy w chmurze jest możliwość łatwego połączenia z rejestratorem, gdy dostęp do Internetu zapewnia połączenie przez 3G/LTE. Konto gościa pozwala na szybkie skonfigurowanie połączenia przez chmurę po zeskanowaniu z menu rejestratora kodu QR.
Seria Q składa się z ekonomicznych **IMVR (IMVR-04Q/08Q/ /04QPOE/08QPOE)** oraz większych rejestratorów **INVR (INVR--04/08/16Q/04/08/16QPOE)**. INVR-xx to rejestratory w obudowie metalowej, wyposażone w 1 lub 2 dyski, obsługujące kamery o rozdzielczości **8 Mpix** oraz mające wyjście **HDMI 4K**.
Wyłącznym przedstawicielem firmy MAZi Security Systems jest GDE Polska.

HIKVISION www.hikvision.com/pl

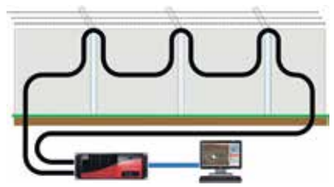
Kamery i rejestratory serii AcuSense z algorytmami deep learning

Firma Hikvision wprowadziła urządzenia AcuSense (Accurate Sense), które wykorzystując algorytmy głębokiego uczenia *(deep learning)*, dostarczają rozwiązania przeznaczone do ochrony perymetrycznej. Technologia Hikvision AcuSense klasyfikuje obiekty do trzech kategorii – człowiek, pojazd i inne, co pozwala zredukować fałszywe alarmy do minimum.
System w zależności od zaprogramowanego scenariusza alarmuje tylko w przypadku wtargnięcia intruza (wykrycie osoby), zapisując pozostałe niepożądane alarmy w pamięci rejestratora. Szybkie wyszukiwanie celu pod kątem obecności osób lub pojazdów pozwala dokładnie przeszukać zarejestrowany materiał szybko i wygodnie. **Wszystkie kamery serii AcuSense są wspierane technologią Power by DarkFighter, która zapewnia wysokiej jakości obraz,** nawet przy bardzo słabym oświetleniu.
Najnowszy model sieciowy AcuSense DS-2CD-2T46G1-4I/SL, oprócz funkcji analizy obrazu (detekcja intruza, przekroczenie linii, wejście w obszar) i klasyfikacji alarmów, ma wbudowane oświetlenie stroboskopowe oraz emituje komunikaty głosowe, uruchamiane po wykryciu potencjalnego intruza, o natężeniu dostosowanym do warunków otoczenia. Ma to na celu ostrzeżenie intruza przed próbą wtargnięcia, a zwrócenie uwagi mrugającym światłem ułatwia zarejestrowanie twarzy.
AcuSense jest dostępny w urządzeniach sieciowych serii Easy IP 4.0 oraz cyfrowych rejestratorach DVR Turbo HD 5.0. Rejestratory AcuSense można stosować w już istniejących instalacjach, wprowadzając analizę *deep learning* do starszych systemów.

LINC POLSKA www.linc.pl

FFT – światłowodowy system detekcji

Future Fibre Technologies (FFT) jest producentem światłowodowych systemów detekcji do ochrony perymetrycznej (obwodowej) obiektów infrastruktury krytycznej, rurociągów lub sieci przesyłowych. Portfolio tego producenta obejmuje kilka rozwiązań, które odpowiadają różnym potrzebom i wymaganiom, oferując detekcję m.in. takich zachowań, jak wspinanie się na ogrodzenie, jego cięcie lub unoszenie.



FFT AURA Ai-2 to światłowodowy system detekcji wtargnięć umożliwiający skuteczną ochronę obwodową. Został zaprojektowany do ochrony obwodowej dużych obiektów, terenów ogrodzonych lub otwartych. Obejmuje sterownik oraz przewód sensoryczny instalowany na ogrodzeniu lub zakopywany w ziemi. Sterownik ma zasięg działania do 80 lub nawet 110 km i zaraportuje zaburzenia w przewodzie z dokładnością od 1 do 4 m. Umożliwia wydzielenie dwóch przewodów detekcyjnych (każdy o długości do 40 lub 55 km). Pozwala na ciągłą detekcję, nawet po przecięciu kabla do miejsca jego przecięcia.
FFT Secure Fence umożliwia detekcję o dokładności od 10 do 25 m oraz stworzenie dowolnej liczby stref w dedykowanym oprogramowaniu CAMS zainstalowanym na serwerze.
FFT Secure Point – dla tego sterownika można określić 2 strefy o długości do 1,6 km każda, z dokładnością detekcji co do strefy.

Sztuczna inteligencja zastosowana w rozwiązaniach marki FFT połączona z zaawansowaną dyskryminacją sygnałów zapobiega uciążliwym, fałszywym alarmom przy zachowaniu maksymalnej czułości na włamania.

ROPAM www.ropam.com.pl

NeoGSM-IP-64 – alarm i automatyka

Nowa centrala alarmowa łącząca bezpieczeństwo i funkcjonalność została zaprojektowana tak, aby jej obsługa i sterowanie było maksymalnie wygodne. Dzięki budowie hybrydowej system można z łatwością dopasować do potrzeb użytkownika. W standardzie wbudowana komunikacja GSM oraz Wi-Fi, dzięki czemu aplikacja mobilna działa szybko i niezawodnie, a ponadto, w przypadku połączenia przez Wi-Fi, bez kosztów obsługi transmisji GSM. Interfejs obsługi systemu jest w pełni graficzny, intuicyjny, i co najważniejsze, może zostać łatwo dostosowany do konkretnych wymogów klienta. Edycja wyglądu ekranów jest możliwa zarówno w lokalnych panelach, jak i w aplikacji mobilnej.

Podstawowe właściwości:
- 4 niezależne strefy,
- do 64 wejść programowalnych,
- do 40 wyjść programowalnych,
- do 32 modułów roletowych,
- do 32 użytkowników (kodów).

Obsługa czujników temperatury, wbudowane osiem termostatów pokojowych. Jedno wejście analogowe do obsługi dowolnych czujników z **wyjściami 0-10 V lub 4-20 mA**. Programowane sceny – 4 makra (sekwencja) do wywołania z paneli dotykowych lub aplikacji. Obsługa systemu **IQPLC (SmartPLC)** – sterowanie po sieci zasilania **230 VAC**. Tworzenie własnej logiki w graficznym i przyjaznym edytorze blokowym – DiagramEditor, podobnie jak schematy blokowe.
Szybka integracja z agencjami ochrony dzięki wbudowanemu protokołowi transmisji SIA-IP TCP/IP.

ROPAM www.ropam.com.pl

Aplikacja mobilna RopamNeo do systemu NeoGSM-IP/NeoGSM-IP-64

Właściwości:
- aplikacja na systemy Android i iOS,
- połączenie z systemem jest realizowane przez Internet: Wi-Fi/ LAN lub GPRS,
- bezkosztowe połączenie przez Internet domowy i automatyczne przełączanie na GPRS,
- obsługa powiadomień PUSH ze zdarzeniami z centrali (wymagany dostęp do RopamBridge),
- sterowanie za pomocą widżetów na ekranie głównym Android,
- sterowanie głosem – wsparcie Asystenta Google,
- możliwość modyfikacji i tworzenia własnego układu ekranów aplikacji wg wymagań systemu lub użytkownika,
- kilka ekranów aplikacji o siatce ikon: 3x4, 2x3, 4x6,
- tworzenie własnych funkcji makro – jeden przycisk wykonuje w sekwencji kilka funkcji,
- tryb tabletowy z dopasowaniem wielkości ikon oraz możliwością obrotu okna aplikacji,
- prosta konfiguracja polegająca na zeskanowaniu kodu QR.

Po połączeniu z centralą NeoGSM-IP/-64 można wykonywać następujące operacje:
- podgląd stanu centrali,
- podgląd stanu stref,
- podgląd stanu wejść,
- podgląd stanu wyjść,
- sterowanie wyjściami (zdalne załączanie światła, otwieranie bram, sterowanie roletami itp.),
- uzbrajanie stref,
- rozbrajanie stref,
- sterowanie temperaturą za pomocą termostatu (profile temperatury, kalendarz),
- podgląd aktualnych awarii w systemie,
- podgląd zdarzeń systemowych,
- zmiana kodu użytkownika,
- obsługa kodów USSD, np. kontrola kart *pre-paid*.

SCHRACK SECONET POLSKA www.schrack-seconet.pl

Czujki marki Spectrex

Czujki marki Spectrex oferują szeroki wachlarz rozwiązań w zakresie wczesnej i niezawodnej detekcji płomienia. Najbardziej zaawansowane funkcje i parametry techniczne mają urządzenia **serii 40/40**. Stosuje się je w najbardziej wymagających obiektach, m.in. w strefach zagrożonych wybuchem. W ramach serii dostępnych jest 10 modeli czujek z czujnikami **IR, 3IR, UV i UV/IR** – dzięki takiej różnorodności łatwo dobrać odpowiednią do danej aplikacji.

Każda czujka serii 40/40 ma:

- układ ogrzewania wizjera w celu wyeliminowania zjawiska kondensacji pary wodnej i oblodzenia,
- szerokie pole widzenia (100° poziomo/95° pionowo);
- obudowę ze stali nierdzewnej lub aluminium (opcja), IP 66/67;
- temperaturę pracy od -55°C do 75°C,
- wszechstronną komunikację: analogowa, protokół HART7, przekaźniki, RS485 – ModBUS,
- certyfikaty EN54-10, Shell TAMAP, FM3260, ATEX, FN/FMC, CSA.

Do każdej czujki 40/40 dostępne są akcesoria: dedykowane uchwyty montażowe, symulatory pola widzenia, kurtyny powietrzne czy urządzenia testujące wspierające proces implementacji rozwiązań Spectrex – instalację, konserwację i codzienną eksploatację. Czujka 40/40I wykrywa pożary węglowodorowych paliw i gazów, zapewniając najwyższą odporność na fałszywe alarmy dzięki detekcji w trzech pasmach podczerwieni. Urządzenie jest niewrażliwe na negatywne zjawiska środowiskowe, np. olśnienie słoneczne czy promieniowanie nagrzanych powierzchni. Znajduje zastosowanie w obiektach przemysłowych przy zabezpieczaniu procesów technologicznych czy dużych magazynach materiałów łatwopalnych.

TP-LINK www.tp-link.com.pl

TP-Link ułatwia migrację do 10G: przełącznik T1700G-28TQ

Nawet w mniejszych firmach przyszłością są sieci szybsze niż gigabitowe. Dlatego infrastrukturę warto rozbudować o rozwiązania, które ułatwią migrację do sieci 10G, zapewniając jednocześnie stabilność i bezpieczeństwo połączeń. Ze względu na coraz większą liczbę przesyłanych danych, rozwój wirtualizacji, usług chmurowych oraz streamingu wideo w **rozdzielczości HD** nawet średniej wielkości przedsiębiorstwom przestają wystarczać sieci gigabitowe. Dotyczy to np. działów przesyłających ogromne ilości danych albo komunikacji pomiędzy jednostkami firmy. Wówczas do transferu danych wykorzystuje się łącza SFP+, a komputery w poszczególnych działach są połączone gigabitowym portem RJ45.

Administratorzy, modernizując infrastrukturę firmową, powinni wybrać rozwiązania, które w razie potrzeby umożliwiają łatwe zwiększenie przepustowości do 10G i rozbudowę sieci, zapewniając jednocześnie stabilność i bezpieczeństwo połączeń. Do tego celu nadaje się model T1700G-28TQ z serii Smart, przeznaczony do sieci firmowych. Został wyposażony w 24 porty Gigabit Ethernet oraz cztery sloty **SFP+**. W stos można połączyć do sześciu takich urządzeń (funkcja stackowania), co zapewnia dwukierunkową przepustowość na poziomie **40 Gb/s.** Zestawienie sześciu jednostek daje łącznie 144-gigabitowe porty **Ethernet, 12 slotów SFP+ 10G** oraz przepustowość **768 Gb/s. T1700G-28TQ** ma funkcje zwiększające bezpieczeństwo i wydajność sieci, np. **802.1Q VLAN,** agregacja połączeń **(LACP),** funkcje wykrywania pętli oraz **QoS**. Ponadto oferuje funkcjonalność warstwy **L2+** dzięki obsłudze statycznego routingu.

WAGNER POLAND www.wagnerpoland.pl

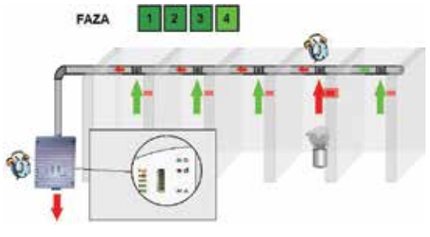
TITANUS® MICRO SENS - zasysająca czujka wczesnej detekcji dymu z funkcją ROOM-IDENT

ROOM-IDENT umożliwia dokładne ustalenie miejsca pożaru przy kontroli maks. **5 oddzielnych pomieszczeń** obsługiwanych przez **jedną zasysającą czujkę dymu.** Lokalizacja miejsca pożaru składa się z 4 etapów:

Etap 1. Normalny tryb pracy: powietrze z chronionych pomieszczeń jest zasysane i transportowane do jednostki detekcyjnej, gdzie kontrolowane jest pod kątem obecności cząstek dymu.

Etap 2. Wczesna detekcja dymu: z chwilą wykrycia cząstek dymu czujka sygnalizuje alarm pożarowy.

Etap 3. Wydmuchiwanie: następuje wydmuchanie powietrza z rurociągu zasysającego.



Etap 4. Lokalizacja miejsca pożaru: następuje zassanie powietrza i na podstawie tzw. czasu transportu cząstek dymu do komory detekcyjnej identyfikuje się źródło dymu.

Lokalizacja pomieszczenia, w którym rozwija się pożar, jest sygnalizowana na panelu czujki zasysającej – jedna z pięciu diod LED świeci czerwonym światłem. Informacja o miejscu pożaru jest też przesyłana do centrali systemu sygnalizacji pożaru. Do czujki zasysającej można podłączyć wskaźniki zadziałania zainstalowane przy kontrolowanych pomieszczeniach.

W praktyce **ROOM-IDENT** może mieć zastosowanie do lokalizacji pożaru w sąsiadujących ze sobą: **komorach trafo, małych rozdzielniach elektrycznych, kontenerach telekomunikacyjnych, małych serwerowniach itp.**

Statystyki

Najnowsze dane branżowe i analizy rynku security

TEKST
a&s International

Sprzedaż sztucznej inteligencji w przemyśle będzie rosnąć w tempie 24 proc. rocznie

Sztuczna inteligencja zyskuje na popularności w sektorze przemysłowym, który do 2025 r. zamierza inwestować rocznie 13,2 mld USD w oprogramowanie, sprzęt i usługi AI. Przełoży się to na średnią roczną stopę wzrostu (CAGR) wynoszącą 24,3 proc. (wartość sprzedaży w 2018 r. to 2,9 mld USD).

Na sumę 13,2 mld USD będą się składać usługi AI – obejmujące instalację, szkolenie, dostosowywanie, integrację aplikacji, wsparcie, utrzymanie itp. – warte 6,5 mld USD, urządzenia – 4,0 mld USD oraz oprogramowanie – 2,7 mld USD.

W ujęciu geograficznym największą część przychodów będą generowały rynki Azji i Pacyfiku, na co wpływ ma tamtejsza wielkość produkcji. Firma analityczna Tractica przewiduje, że do 2025 r. przychody w tamtym regionie osiągną 4,9 mld USD. Następna będzie Ameryka Płn. (3,9 mld USD), a trzecia Europa (3,0 mld USD).

Głównymi czynnikami napędzającymi inwestycje w AI dla przemysłu są potrzeby monitorowania jakości, poprawy wydajności, predykcyjnego utrzymania, zarządzania zużyciem energii i in. Wykorzystanie AI prowadzi do zwiększenia wydajności operacyjnej, a w konsekwencji do obniżenia kosztów procesów produkcyjnych.

W sektorze produkcyjnym mają być wdrażane mechanizmy predykcyjne uruchamiane przy użyciu technik uczenia maszynowego (*machine learning*) oraz głębokiego uczenia (*deep learning*). Systemy sztucznej inteligencji korzystają również z innych technik, takich jak zautomatyzowane systemy komputerowe i wizyjne (*computer and machine vision*), przetwarzanie języka naturalnego oraz różne techniki klasyfikacji informacji. W połączeniu z *machine* i *deep learning* oraz wykorzystaniem mocy istniejących procesorów mają one na celu takie przetwarzanie danych wyjściowych, które zapewni informacje dające się interpretować i kształtować za pomocą zautomatyzowanych algorytmów, odróżniając ludzi od analizowania niezliczonych punktów danych.

Globalne przychody z usług AI do 2025 r. (mld USD)

Źródło: Tractica

Rynek inteligentnych termostatów będzie rósł w latach 2019–2025 w tempie 9 proc.

Jak przewidują analitycy z Global Market Insights, światowy rynek inteligentnych termostatów zwiększy swoją wartość z 3 mld USD w 2018 r. do 6 mld USD w 2025 r. Wartość rynku termostatów przeznaczonych do montażu w pomieszczeniach przekroczyła w 2018 r. 1,5 mld USD. Według prognoz ten segment ma w latach 2019-2025 osiągać dwucyfrowe roczne tempo wzrostu. Z kolei przychody na rynku termostatów dla mediów użytkowych mają do 2025 przekroczyć 500 mln USD. Popyt powinny zwiększać różne programy oferujące zniżki i inne zachęty do instalowania tego rodzaju urządzeń. Także różne opcje w kanale dystrybucji energii, których celem jest zmniejszenie obciążenia sieci, mogą przynieść klientom kolejne oszczędności. Coraz więcej klientów dowiaduje się o istnieniu doskonalszych rozwiązań do monitorowania zużycia energii. Rosnąca świadomość w połączeniu ze zwiększającą penetracją urządzeń inteligentnego domu będą wpływać na szybszy rozwój w tej branży.

Źródło: Global Market Insights

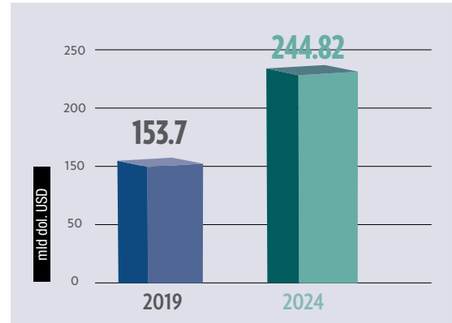
Rynek Smart Factory osiągnie w 2024 r. wartość 244,82 mld USD, przy średnim rocznym tempie wzrostu wynoszącym do tego czasu 9 proc.

Według MarketsandMarkets przychody na rynku Smart Factory magą w 2019 r. osiągnąć 153,7 mld USD, a w 2024 r. – 244,82 mld USD. Średnie roczne tempo wzrostu w latach 2019–2024 wyniesie 9,76 proc. Zdaniem analityków znaczący udział w rynku inteligentnych fabryk będzie miała produkcja elementów dla konkretnych odbiorców, a branżę w prognozowanym okresie zdominują systemy MES (*Manufactoring Execution System* – system realizacji produkcji).

Czynnikami napędzającymi wzrost rynku są ewolucja Internetu Rzeczy (IoT), coraz powszechniejsze wykorzystanie technologii wspomagających produkcję, rosnące zastosowanie robotów przemysłowych w sektorze produkcyjnym (zwłaszcza robotów współpracujących), wdrażanie wizji *Connected Enterprise*, wreszcie masowa produkcja w celu zaspokojenia zwiększającej się populacji. Z kolei główne czynniki hamujące wzrost rynku są związane z koniecznością poczynienia dużych inwestycji kapitałowych oraz ryzykiem zagrożeń dla systemów cyfrowych i fizycznych.

Prognozuje się, że roboty przemysłowe będą miały największy udział w światowym rynku Smart Factory. Wdrożenie robotyki przemysłowej w inteligentnych procesach produkcyjnych może poprawić wydajność, ograniczyć błędy ludzkie oraz zwiększyć wielkość produkcji.

Smart Factory market Value



Źródło: MarketsandMarkets

Państwo	Liczba robotów przypadających na 10 tys. pracowników	
Polska	32	> 0,4%
Czechy	128	> 1,3 %
Słowacja	135	> 1,4 %

Raport Międzynarodowej Federacji Robotyki (IFR)

System bezprzewodowy ABAX 2

Do realizacji zadań z zakresu SSWiN coraz częściej stosowane są urządzenia wykorzystujące łączność radiową. Przykładem nowoczesnego rozwiązania, zapewniającego skuteczność i niezawodność działania na poziomie niemal identycznym jak w przypadku instalacji przewodowych, jest ABAX 2.

ABAX 2 to nowa odsłona bezprzewodowego systemu ABAX, oferowanego przez SATEL od 2005 r. Podobnie jak w przypadku poprzednika, komunikacja między urządzeniami bezprzewodowymi jest dwukierunkowa. Nowością jest natomiast tzw. dywersyfikacja kanałów transmisji. Układ radiowy stale analizuje poziom zakłóceń w każdym z czterech kanałów wydzielonych w pasmie częstotliwości 868 MHz, aby do transmisji wybrać ten, w którym interferencje z innymi sygnałami są najmniejsze. Bezpieczeństwo przesyłanych danych zapewnia szyfrowanie AES-128.

Większy zasięg, dłuższy czas pracy

ABAX 2 cechuje się doskonałym zasięgiem – odległość między kontrolerem systemu bezprzewodowego a współpracującymi urządzeniami może wynieść do 2 km w otwartej przestrzeni, a przy zastosowaniu retransmitera ARU-200 nawet dwukrotnie więcej. Imponujący jest także maksymalny czas pracy urządzeń zasilanych bateryjnie – do 8 lat, zależnie od produktu i jego konfiguracji (tryb ECO).

Serce systemu

Dostępne są dwa kontrolery: ACU-220 oraz kompaktowy ACU-280. Oba mogą pełnić funkcję ekspanderów urządzeń bezprzewodowych w systemach alarmowych bazujących na centralach INTEGRA, INTEGRA Plus i rodziny VERSA. Połączenie z nimi jest realizowane za pośrednictwem magistrali komunikacyjnej. ACU-220 może też pracować autonomicznie, z dowolną centralą alarmową lub sterownikiem automatyki – wówczas wykorzystywane są programowalne wejścia i wyjścia kontrolera.

Skuteczna detekcja oraz sygnalizacja

ABAX 2 obejmuje szeroki asortyment czujek bezprzewodowych. Są wśród nich urządzenia wykrywające ruch – czujki PIR: APD-200 i APD-200 Pet oraz dualne: APMD-250, AOD-210 i kurtynowa AOCD-260. Dwie ostatnie mogą pracować na zewnątrz pomieszczeń. Dostępne są też czujki zbicia szyby AGD-200, czujki dymu ASD-250 oraz dymu i ciepła ASD-200. Nowością jest AXD-200 – uniwersalne urządzenie, które może pracować w jednym z wybranych trybów, jako czujka:

- magnetyczna 1- lub 2-kanałowa,
- magnetyczna z wejściem roletowym,
- wstrząsowa i magnetyczna,
- przemieszczenia,
- temperatury,
- zalania.

Gama produktów systemu ABAX 2 będzie wkrótce rozszerzona m.in. o czujkę zmierzchu i przycisk napadowy.

Z kontrolerami ABAX 2 współpracują sygnalizatory akustyczno-optyczne: zewnętrzny ASP-200 i wewnętrzny ASP-215. Podobnie jak czujki ruchu, czujka uniwersalna i kontrolery spełniają wymagania normy EN 50131 Grade 2.

Automatyka i sterowanie

Funkcje automatyki budynkowej mogą być realizowane sterownikami 230 V AC: dopuszkowymi ASW-200 oraz podłączanymi do gniazd sieciowych ASW-210. System można rozszerzyć o urządzenia przewodowe za pomocą ekspanderów: miniaturowego ACX-210 oraz z wyjściami przekaźnikowymi ACX-220. Do zdalnego sterowania służą dwukierunkowe piloty APT-200.

Programowanie i diagnostyka

Przy współpracy z centralami SATEL programowanie systemu odbywa się z poziomu komputera z zainstalowanym programem DLOADX lub z manipulatora. Gdy ACU-220 działa autonomicznie lub z inną centralą, do konfiguracji służy oprogramowanie ABAX 2 Soft. Ma ono dodatkowo funkcje diagnostyczne pozwalające na weryfikację jakości sygnału radiowego oraz stanu poszczególnych elementów systemu. Aby zbadać warunki komunikacji radiowej w obiekcie i określić optymalne miejsca montażu urządzeń, należy użyć testera ARF-200.

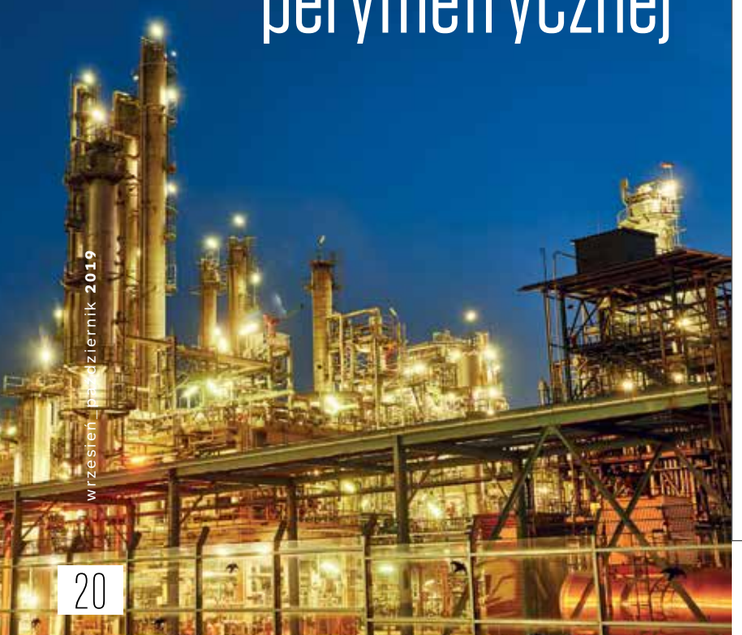
Warto zaznaczyć, że SATEL zadbał o kompatybilność wsteczną – urządzenia ABAX 2 współpracują z kontrolerami ABAX. □

SATEL

ul. Budowlanych 66
80-298 Gdańsk
www.satel.pl

Daj sobie więcej czasu na reakcję

Zaawansowane detektory jako elementy systemów ochrony perymetrycznej



Laserowa czujka skanująca RLS-2020

Projektując systemy zabezpieczeń obiektów, szczególny nacisk powinno się kłaść na zapewnienie ich wysokiego stopnia ochrony w strefie obwodowej. Takie podejście zapewnia możliwość najwcześniejszego wykrycia zagrożenia i pozostawia czas na interwencję, co sprawia, że możemy ograniczyć straty materialne związane z kradzieżą czy wandalizmem. Rozwój technologii w ostatnich latach w znacznym stopniu zwiększył skuteczność (prawdopodobieństwo wykrycia) i precyzję urządzeń zewnętrznych. Jednak wciąż brak jest wytycznych pozwalających na objęcie czujek instalowanych na zewnętrz budynków normą EN 50131-1.
Wysoka jakość produktów firmy OPTEX i stosowane w nich różne technologie pozwalają na coraz skuteczniejsze zapewnienie odpowiedniej ochrony dostosowanej do wymagań konkretnej aplikacji. Do ochrony obwodowej najczęściej wykorzystuje się: aktywne bariery podczerwieni, czujki PIR dalekiego zasięgu, laserowe czujki skanujące oraz światłowodowe systemy napłotowe. W przypadku obiektów infrastruktury krytycznej warto rozważyć zastosowanie kilku systemów opartych na różnych technologiach. Zapewni to wyższą niezawodność rozwiązania.

Popularnymi detektorami wykorzystywanymi w systemach ochrony obwodowej są **aktywne bariery podczerwieni.** Urządzenia te są stosunkowo łatwe w obsłudze, mechanizm ich działania nie jest skomplikowany, mają przystępną cenę, więc zyskały uznanie wielu instalatorów i użytkowników. Zastosowanie urządzenia dobrej jakości oraz precyzyjne dostrojenie pozwala uniknąć problemów związanych z czynnikami środowiskowymi (deszcz, śnieg, mgła). Istotne jest również zapewnienie stabilnego zamontowania do podłoża (przy kolumnach o wysokości 3 m należy zastosować dodatkowe wsporniki montażowe, a w szczególnych przypadkach także odciągi stabilizacyjne). Kolumny nadajnika i odbiornika można instalować samodzielnie lub w dedykowanych obudowach kolumnowych, które utrudniają identyfikację rzeczywistego obszaru działania wiązki podczerwieni. Z takiego rozwiązania korzysta m.in. jedno z największych na świecie przedsiębiorstw handlowych do ochrony obwodowej swojego magazynu w Czechach. Firma wybrała czterowiązkowe bariery podczernieni OPTEX SL- 350QFR zasilane bateryjnie, wyposażone w system komunikacji wewnętrznej firmy INOVONICS. Wybór takiego rozwiązania był podyktowany koniecznością pilnej instalacji systemu bez prowadzenia okablowania.

W projektowanym systemie ochrony obwodowej można również wykorzystać **czujki PIR dalekiego zasięgu. Detektory OPTEX SIP** wyposażono w inteligentny system detekcji, automatycznie dostosowujący czułość do zmian środowiskowych, takich jak temperatura otoczenia czy natężenie oświetlenia. Z kolei urządzenia serii REDWALL-V są idealnym rozwiązaniem do sterowania kamerami zewnętrznymi w systemach, od których oczekuje się wysokiej efektywności. Rozwiązanie to znalazło zastosowanie np. w zabezpieczeniu jednego z zakładów penitencjarnych na terenie Polski. Na słupkach oświetleniowych znajdujących się na granicy obszaru zamontowano czujki SIP-XXX/5. Na każdym zainstalowano dwie czujki. Jedna z nich jest wyposażona w detektor strefy podejścia, który zabezpiecza martwą strefę w miejscu montażu czujek. Tam, gdzie obszar chroniony był bardzo wąski, zastosowano dodatkowo bariery podczerwieni oraz czujki kurtynowe. W niektórych projektach zorganizowanie odpowiedniej ochrony obwodowej wymaga zastosowania czujek o różnej charakterystyce pokrycia.

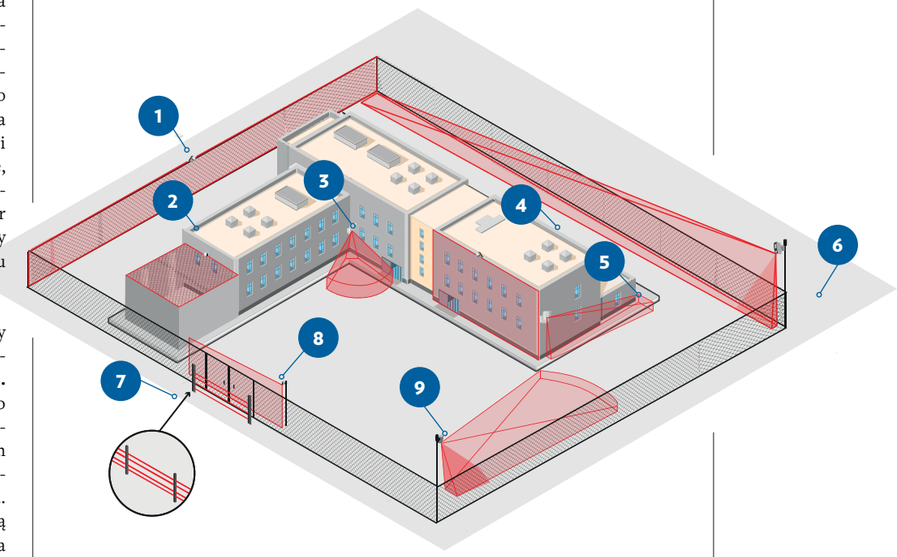
W zabezpieczaniu strefy obwodowej obiektów zastosowanie znalazły **laserowe czujki skanujące.** W ofercie produktów OPTEX są dostępne dwa modele **z serii REDSCAN**, różniące się kształtem i wielkością strefy detekcji: RLS-2020 oraz RLS-3060. Technologia użyta w czujkach skanujących może zapewnić efektywną ochronę w miejscach wymagających wysokiego poziomu zabezpieczenia. Dostępność dwóch różnych charakterystyk detekcji – poziomej lub pionowej, ułatwia projektowanie systemu i pozwala na optymalizację kosztów jego wdrożenia. Czujki RLS-3060 zastosowano w ochronie obwodowej jednej z największych elektrowni w Polsce. Wspomagają w niej pracę systemu telewizji dozorowej CCTV. Z kolei RLS-2020 została w kilku projektach użyta do ochrony bramy. Często stanowi też uzupełnienie ochrony obwodowej wykorzystujące czujki RLS 3060 na krótszych odcinkach.

W przypadku rozległego obszaru do jego ochrony obwodowej doskonale nadają się **napłotowe systemy światłowodowe.** W ich elemencie detekcyjnym nie ma możliwości wystąpienia wyładowania elektrycznego, więc można go zastosować nawet w strefie zagrożenia wybuchem. W odróżnieniu od rozwiązań opartych na detektorach elektrycznych, światłowód jest odporny na działanie czynników środowiskowych, takich jak promieniowanie UV, promieniowanie elektromagnetyczne, wilgoć, sól czy wyładowania atmosferyczne. System pracuje stabilnie we mgle, w warunkach zapylenia czy ciemności.

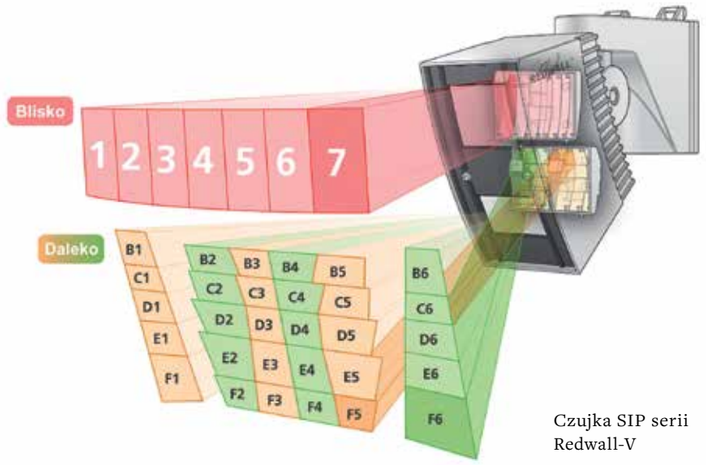
AKTYWNE BARIERY PODCZERWIENI

Aktywne bariery podczerwieni, składające się z nadajnika i odbiornika, tworzą linię detekcji podobną do linii granicznej w analizie wizyjnej lub wirtualnego muru oraz dodatkowo „trzeci wymiar" – wysokość. Nadajnik przesyła wiązkę podczerwieni do odbiornika, a w przypadku przerwania wiązki przez intruza uruchamia alarm. Bariery podczerwieni są również dostępne w wersji sieciowej IP.

PROPOZYCJA ZASTOSOWANIA PRODUKTÓW FIRMY OPTEX DO OCHRONY OBWODOWEJ



1. **RLS-3060** – laserowa czujka skanująca
2. **RLS-2020S** – laserowa czujka skanująca?
3. **HX-40AM/DAM** – czujka PIR
4. **RLS-3060** – laserowa czujka skanująca?
5. **HX-80NAM** – czujka PIR
6. **SIP-100** – czujka PIR dalekiego zasięgu
7. **SL 200QDP** – aktywna bariera podczerwieni
8. **RLS-2020S** – laserowa czujka skanująca
9. **SIP-3020/5** – czujka PIR dalekiego zasięgu



Czujka SIP serii Redwall-V

Parametry techniczne i niezawodność rozwiązania potwierdza certyfikat najwyższej klasy ochrony armii USA, zezwalający na instalację w obiektach, w których są przechowywane materiały nuklearne. System jest również rekomendowany przez brytyjskie urząd ochrony infrastruktur krytycznej (CPNI). Światłowodowy system napłotowy OPTEX został wykorzystany m.in. na jednym z większych polskich lotnisk.

Ważnym elementem podczas projektowania zabezpieczeń elektronicznych, na który firma OPTEX zwraca szczególna uwagę, jest zapewnienie integracji poszczególnych elementów systemu. Czujki RL-3060, RLS-2020, Redwall SIP oraz bariery z serii SL można podłączyć do sieci komputerowej (bezpośrednio do oprogramowania VMS). Komunikują się one wówczas w oparciu o protokół komunikacyjny wykorzystujący ciąg tekstowy ASCII, a zasilane są poprzez technologię Power-over-Ethernet (PoE). Protokół ten jest kompatybilny z systemami VMS i PSIM wiodących producentów, takich jak Milestone, Genetec, Exacq, ElaSoft, Axxon. Dzięki temu można z łatwością prowadzić wideoweryfikację alarmów czy ich wizualizację na planie obiektu.

Strefa ochrony obwodowej jest często kluczową, a w wielu przypadkach jedyną strefą w planie zabezpieczenia całego obiektu. Niezwykle ważne jest, aby do przygotowania strategii ochrony każdego obiektu podchodzić indywidualnie, starannie rozpatrując wszystkie potencjalne zagrożenia. OPTEX może się pochwalić najszerszą na rynku ofertą rozwiązań do ochrony zewnętrznej.

Dostępność technologii na rynku jest na tyle duża, że można dopasować system odpowiedni zarówno pod względem funkcjonalności, jaki i kosztów ponoszonych na jego zbudowanie i utrzymanie. □

NAPŁOTOWY SYSTEM ŚWIATŁOWODOWY

Koncepcja napłotowego systemu światłowodowego jest oparta na aktywnym światłowodzie mocowanym do istniejącego ogrodzenia. Drgania ogrodzenia wywołane ingerencją intruza (wspinanie, cięcie, podnoszenie) są analizowane w procesorze, który wysyła sygnał alarmowy. W zależności od modelu jeden procesor może obsługiwać nawet 25 stref detekcji; strefy mogą mieć maks. długość 2,3 km. Dopasowanie do wymogów instalacji ułatwia zastosowanie dodatkowego kabla nieaktywnego, pozwalającego na zamontowanie procesora sterującego w odległości do 20 km od ochranianego fragmentu ogrodzenia. Strojenie systemu odbywa się z wykorzystaniem dedykowanych aplikacji komputerowych.

REDWALL-V

Seria pasywnych czujek podczerwieni wyposażonych w oddzielne zestawy detektorów dla strefy bliższej i dalszej oraz detektor strefy podejścia (w modelach SIP-xxx/5). Czujki serii SIP mają charakterystykę przestrzenną lub kurtynową oraz zasięgi od 30 do 100 m. Za kształtowanie pól detekcji odpowiadają lustra skupiające. Elementy aktywne są pokryte filtrem eliminującym zakłócenia elektromagnetyczne i światło widzialne. Analiza sygnałów przebiega w dedykowanych mikroprocesorach z zaawansowanym algorytmem detekcji. Rozdzielenie torów obróbki sygnału poszczególnych kanałów umożliwia ustawienie różnych parametrów dla każdej strefy: czułość detekcji, praca w trybie AND lub OR, albo wyłączenie strefy dalekiej. Użyteczna jest możliwość zablokowania wyjścia alarmowego na określony czas po pierwszym wykryciu intruza. Zapobiega to kolejnym aktywacjom czujki, spowodowanym tą samą przyczyną i daje czas operatorowi na weryfikację zdarzenia. Zasadą detekcji na dużym obszarze jest dwukrotne wykrycie intruza przez ten sam detektor przed wysłaniem sygnału alarmowego (tryb AND). Wpływa to na zmniejszenie liczby niepotrzebnych aktywacji.

OPTEX Security

ul. Bitwy Warszawskiej 1920r 7b
02-366 Warszawa
www.optex-europe.com/pl

KONTROLA DOSTĘPU – technika i organizacja

CORAZ WIĘCEJ ORGANIZACJI MA PROBLEM Z KONTROLOWANIEM DOSTĘPU DO DANYCH SZCZEGÓLNIE CHRONIONYCH, NIEZALEŻNIE CZY JEST TO KNOW HOW, CZY DANE OSOBOWE. SPORA CZĘŚĆ ORGANIZACJI STARA SIĘ ZABEZPIECZAĆ POSZCZEGÓLNE OBIEKTY LUB POMIESZCZENIA. DUŻA ICH CZĘŚĆ WDRAŻA ZABEZPIECZENIA TECHNICZNE, Z POMINIĘCIEM ROZWIĄZAŃ ORGANIZACYJNYCH. KILKANAŚCIE LAT PRAKTYKI POZWALA MI NA DOŚĆ ŚMIAŁĄ TEZĘ: ZABEZPIECZENIA TECHNICZNE BEZ ODPOWIEDNICH PROCEDUR I SZKOLEŃ OBNIŻAJĄ POZIOM BEZPIECZEŃSTWA!

TEKST
Przemysław Bańko

Czy techniczna kontrola dostępu podnosi poziom bezpieczeństwa?

Ileż to razy w trakcie audytów widziałem personel wchodzący do danej strefy z wykorzystaniem karty dostępu jednego z pracowników. Ilu z nas spotkało się z niedbale wbijanym kodem PIN do systemu. Jak często widzimy drzwi wejściowe przystawione popielniczką lub kubłem z wodą. Jak często widujemy pomieszczenia bez obsługi z zalogowanymi komputerami. Przykłady można by mnożyć. Statystyki naruszeń, i to nie tylko w zakresie ochrony danych osobowych, wskazują, iż do naruszeń w przeważającej mierze dochodzi z winy personelu. Bagatelizowanie ryzyka, omijanie procedur – jeżeli istnieją – i przeświadczenie, że przecież nigdy nic się nie stało, bywa zgubne.

Zawsze na pytanie „dlaczego tak funkcjonuje to konkretne zabezpieczanie" otrzymuję odpowiedzi typu „to dziś tak zupełnie przypadkiem", „na co dzień drzwi są zamknięte", „po raz pierwszy zapomniałem swojej karty dostępu". Każdy, kto brał udział w audycie, dodałby jeszcze kilkanaście zwyczajowych kłamstw. Tylko w jakim celu – zadaję sobie pytanie – inwestujemy w zabezpieczenia? Dla wydawania pieniędzy? Dla prestiżu? Dla poprawy wizerunku? Jeden z moich pierwszych szefów zwykł mawiać „system nałożony na bałagan, daje jeszcze większy bałagan". Ostatnich dwadzieścia lat uświadamia mi prawie na co dzień, iż miał rację. Zdaję sobie sprawę, że dostawcom rozwiązań zależy na szybkiej dostawie, sprzedaży rozwiązania, podpisaniu umowy serwisowej. To naturalne, z tego przecież się utrzymują. Rozmawiam często w branży i słyszę, że „klient tak chciał, więc tak wykonaliśmy". Czy nie lepiej dla wszystkich byłoby wyedukować klienta, iż każdy system, nawet najdroższy, bez odpowiednich zapisów w organizacji może być dla niego ryzykowny?

Dla zobrazowania opiszę konkretną sytuację w jednym z sądów apelacyjnych. Przez lata obowiązywała w nim procedura, iż przed rozprawami dla szczególnie niebezpiecznych przestępców, tzw. eNek, policja sprawdza cały budynek w celu wykrycia niebezpieczeństw. Po analizie sprawdzeń kierownictwo sądu zadecydowało o odcięciu parteru i kilku pomieszczeń pierwszego piętra od pozostałej części budynku solidnym systemem kontroli dostępu. Natychmiast po wdrożeniu systemu starą procedurę zmieniono. Od momentu wdrożenia policja sprawdzała jedynie parter i część ogólnodostępnego pierwszego piętra, „bo przecież dalej było już bezpiecznie".

Siedziałem pewnego razu, czekając na spotkanie z kierownictwem sądu, tuż przy wejściu do strefy chronionej obiektu. I jakież było moje zdziwienie, gdy raz za razem wchodzący do strefy bezpiecznej wprowadzali jeden i ten sam kod 1 – 2 – 3 – 4 #. Nie wierzyłem własnym oczom. Natychmiast po rozpoczęciu spotkania poinformowałem w dość żartobliwym tonie rozmówców o swoim odkryciu. Ot, taka przyjacielska pogadanka w stylu „bardzo fajny system wdrożyliście, ale dobrze byłoby, aby pracownicy bardziej zakrywali kod, którym się posługują. Może warto z nimi porozmawiać". Miny moich rozmówców nie były radosne, miałem wręcz wrażenie, że wyrażały wściekłość i zdziwienie. Puenta: w sądzie nadal funkcjonuje system kontroli dostępu, a policja, jak przed jego wdrożeniem, sprawdza cały budynek.

Myślę, że taką lub inną sytuację zaobserwował każdy z nas. Otwarta serwerownia. Otwarty korytarz i wszystkie biura w ciągu, bo tak przecież łatwiej i szybciej się sprząta. Włączony komputer w ogólnodostępnym sekretariacie. Papierzyska walające się na stołach i parapetach. Można wymienić setki przykładów.

> Statystyki naruszeń, nie tylko w zakresie ochrony danych osobowych, wskazują, iż do naruszeń w przeważającej mierze dochodzi z winy personelu

Zaplanuj, zaprojektuj, opisz w procedurach, przeszkól personel. Tylko tyle i aż tyle

Planując system zabezpieczeń, nie musimy wyważać otwartych drzwi. Możemy sięgnąć po normy, po wiedzę konsultanta lub stworzyć własny interdyscyplinarny zespół, który odpowie na pytania, w jakim celu chcemy wdrożyć zabezpieczenia techniczne, w jaki sposób wpłyną na obniżenie ryzyka wystąpienia incydentu lub naruszenia, co zrobić, aby system był wykorzystywany zgodnie ze swoim przeznaczeniem, w jaki sposób monitorować zabezpieczenie.

Przykładem norm pomocnych przy wdrożeniu każdego z zabezpieczeń technicznych jest rodzina norm ISO 27000. Warto przy inwestycji w zabezpieczenia techniczne wysupłać kilkaset złotych i zakupić w Polskim Komitecie Normalizacyjnym normy:

- PN-EN ISO/IEC 27005 – Technika informatyczna. Techniki bezpieczeństwa. Zarządzanie ryzykiem w bezpieczeństwie informacji
- PN-EN ISO/IEC 27001 – Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Wymagania
- PN-EN ISO/IEC 27002 – Technika informatyczna. Techniki bezpieczeństwa. Praktyczne aspekty zabezpieczania informacji

Zawierają one wiele przydatnych informacji pozwalających na zaplanowanie zabezpieczeń, ich dobór, opracowanie niezbędnych procedur i instrukcji.

Do czego będą przydatne normy?

Przede wszystkim do określenia, jaki obszar i jakie dane chcemy chronić. Analiza ryzyka zagrożeń – bo od niej właśnie zawsze zaczynamy – pozwala na dokładne określenie granic bezpieczeństwa, stref bezpieczeństwa i pomieszczeń bezpieczeństwa. Wiemy w końcu, gdzie incydent będzie dla nas najbardziej bolesny. Analiza umożliwi zinwentaryzowanie przetwarzanej informacji, systemów, aplikacji, baz danych. Pozwoli ponadto wskazać główne podatności i zagrożenia, a także oszacować ewentualne straty, gdyby do niechcianego naruszenia bądź incydentu doszło. Znając miejsce i wartość informacji, wiemy z grubsza, ile powinniśmy

wydać na jej zabezpieczenie. Wtedy trudniej powiedzieć zarządzającym organizacją, że „nie stać nas na zabezpieczenie”.
Po analizie ryzyka warto zaplanować, które konkretne zabezpieczenia odpowiadają w jak największym stopniu za minimalizację zinwentaryzowanych zagrożeń. Czy konieczne jest wytyczenie stref bezpieczeństwa. Czy niezbędna jest inwestycja w system monitoringu wizyjnego, system kontroli dostępu, czy inne systemy zabezpieczenia. Wtedy będziemy w stanie wskazać projektującym nasze instalacje, które obszary są dla nas kluczowe. Po prawidłowej analizie ryzyka zagrożeń stajemy się dla projektujących i wdrażających systemy bezpieczeństwa partnerem. Jednocześnie wewnętrzne struktury firmy już na tym etapie powinny przemyśleć, jak zorganizujemy dostęp do poszczególnych miejsc organizacji lub systemów. W jaki sposób nadamy i będziemy odbierali uprawnienia do poszczególnych miejsc, ról i systemów. Jak będziemy weryfikowali, kontrolowali, monitorowali i audytowali poprawność korzystania z nadanych uprawnień.
Warto spojrzeć na rozdziały dziewiąte norm ISO 27001 i 27002. W pierwszej z nich znajdziemy dobre praktyki zabezpieczeń, w drugiej szczegółowy opis, jak wdrażać zabezpieczenia techniczne, proceduralne i organizacyjne. Idąc krok po kroku, będziemy w stanie wyznaczyć:

- fizyczne granice obszaru bezpiecznego (od płotu po zamek w drzwiach),
- fizyczne zabezpieczenia wejścia i modele nadawania uprawnień do wejścia na teren chroniony,
- sposoby dostawania się do pomieszczeń pracowników zewnętrznych, np. serwisu technicznego lub sprzątającego,
- kontrole miejsc przebywania personelu,
- standardy zabezpieczania systemów, usług i informacji – znana i nadal niepraktykowana zasada czystego biurka i czystego ekranu,
- standardy dostępu do systemów z urządzeń mobilnych,
- minimalny zakres przeszkolenia pracowników.

Warto spojrzeć na rozdziały dziewiąte norm ISO 27001 i 27002. W pierwszej znajdziemy dobre praktyki zabezpieczeń, w drugiej szczegółowy opis, jak wdrażać zabezpieczenia techniczne, proceduralne i organizacyjne

Pamiętajmy, że dobrze zaprojektowany system kontroli dostępu do miejsc i informacji pozwoli na realną próbę ograniczenia skutków incydentów i naruszeń. Same zabezpieczenia są połową sukcesu, ale bywają wręcz preludium do porażki. Gdy nałożymy system zabezpieczeń technicznych na uporządkowany, zaplanowany, zaprojektowany i prawidłowo wdrożony system techniczny, bez wątpienia zmniejszymy różne rodzaje ryzyka w obszarze bezpieczeństwa fizycznego oraz teleinformatycznego.
Warto również pomyśleć o testach zabezpieczeń. Przydatne może być podejście socjotechniczne – rzucony w kąt pendrive lub odłożona karta do systemu kontroli dostępu. Bo pomimo opracowanych polityk i procedur, instrukcji i szkoleń jesteśmy tylko ludźmi, najsłabszymi elementami systemu bezpieczeństwa. □

BIO

Przemysław Bańko

Dyrektor ds. bezpieczeństwa spółki specjalizującej się w nowoczesnych technologiach informatycznych, trener, wdrożeniowiec i audytor specjalizujący się w tematyce zarządzania: ryzykiem (ISO 31000), bezpieczeństwem informacji (ISO 27001), jakością (ISO 9001) oraz compliance (Dyrektywa NIS, Rozporządzenie RODO).

System kontroli dostępu Hikvision

Systemy kontroli dostępu firmy Hikvision obejmują szeroką gamę urządzeń pozwalających na realizację różnorodnych scenariuszy, identyfikację użytkowników na wiele sposobów oraz zaawansowane możliwości obsługi dostępu do stref i pomieszczeń.

System KD spełnia swoje zadanie, działając autonomicznie, jednak wiele nowych możliwości pojawia się, gdy współpracuje z innymi urządzeniami Hikvision: wideodomofonami czy telewizji dozorowej zarządzanymi z jednej platformy programowej iVMS4200. Takie podejście pozwala tworzyć rozwiązania, w których ta sama baza danych użytkowników jest wykorzystywana przez wszystkie systemy, użytkownik jest przypisany do wybranych przejść, a kamery szybko weryfikują, czy kartą posługuje się uprawniona osoba.
„Zmysłami” systemu KD, które odczytują dane uwierzytelniające użytkowników, są czytniki. W ofercie Hikvision są dostępne tradycyjne czytniki kart lub dodatkowo z klawiaturą umożliwiającą podwójną weryfikację lub wejście przy użyciu samego kodu, jeśli użytkownicy nie używają kart. Duża różnorodność oferty pozwoli dobrać czytnik do wystroju pomieszczeń, a model DS-K1104 zapewni odporność na akty wandalizmu (obudowa klasy IK10).

Coraz więcej systemów opiera uwierzytelnianie użytkowników na danych biometrycznych, co wyklucza przekazanie transpondera lub kodu osobie niepowołanej. Czytniki skanujące linie papilarne jednoznacznie identyfikują osoby, a zaletą jest też brak konieczności noszenia kart czy breloków. Wśród rozwiązań Hikvision na uwagę zasługują czytniki linii papilarnych oraz kart zbliżeniowych serii DS-K1201, które można podłączyć do kontrolerów serii DS-K2600 za pomocą dwukierunkowego interfejsu komunikacyjnego RS-485. Kontrolery w wersjach na 1, 2 lub 4 przejścia umożliwiają korzystanie z czytników z interfejsem RS-485 lub Wiegand, obsługując przejścia dwu- lub jednostronne. Zastosowanie kontrolerów serii DS-K2600 pozwala na realizację złożonych scenariuszy kontroli dostępu, łączenie przejść w śluzy, funkcje *antipassback* pomiędzy kontrolerami i otwieranie lub uwierzytelnianie przejścia za pomocą pierwszej karty. Przejścia są bezpieczne, gdyż tylko czytnik znajduje się poza chronioną strefą, natomiast część decyzyjna z przekaźnikiem sterującym przejściem jest zlokalizowana wewnątrz niej.

Kolejną grupą urządzeń są terminale, czyli kompletne zestawy sterujące dostępem zamknięte w jednej obudowie: czytnik, część decyzyjna oraz przekaźnik. Znajdują się w nich, zależnie od wersji wyposażenia, klawiatury oraz czytniki kart EM 125 kHz i Mifare 13,56 MHz, linii papilarnych i rozpoznawania twarzy. Tryb uwierzytelniania można skonfigurować, wybierając wśród technologii dostępnych w terminalu. W przypadku bardziej zaawansowanych urządzeń zapewnia to bardzo wysoki poziom poprawności uwierzytelniania, wymagający od użytkownika weryfikacji twarzy, identyfikacji za pomocą linii papilarnych oraz zbliżenia karty. Przykładem jest terminal rozpoznający twarze DS-K1T607MFW wyposażony w duży ekran ułatwiający korzystanie z urządzenia. Rozpoznawanie twarzy zostało oparte na znanej z kamer Hikvision technologii *deep learning*, zapewniającej pewne i szybkie rozpoznanie osoby w czasie krótszym niż 1 s. Z kolei zastosowanie w terminalu dwóch kamer pozwala zweryfikować, czy uwierzytelnia się żywa osoba, a nie jest to próba oszukania za pomocą np. fotografii.

Terminal ma wbudowany przekaźnik, należy więc zastosować moduł bezpieczeństwa DS-K2M060, który jest elementem wykonawczym komunikującym się z terminalem poprzez protokół RS-485. W takiej konfiguracji nawet w przypadku prób manipulacji czy zniszczenia urządzenia przekaźnik znajdujący się w strefie chronionej pozostanie zamknięty.

Uniwersalność urządzeń Hikvision pozwala na skonfigurowanie terminala DS-K1T607MFW jako czytnika i podłączenie go do kontrolera DS-K2600, co zwiększy poziom bezpieczeństwa i funkcjonalność. Ofertę uzupełniają karty, przyciski, zamki, a nawet bramki, co pozwala na budowanie kompletnego przejścia z zastosowaniem urządzeń jednego producenta. □

Hikvision Poland

ul. Żwirki i Wigury 16B,
02-092 Warszawa
tel. 22 460 01 50
faks 22 464 32 11
e-mail:
info.pl@hikvision.com

EQU ACC System kontroli dostępu w stopniu 3.

Część menedżerów zakładów przemysłowych, zwłaszcza infrastruktury krytycznej, nie zdaje sobie sprawy z konieczności posiadania systemu kontroli dostępu w stopniu 3. zabezpieczenia – zgodnie z PN-EN 60839-11-1. Mimo że norma obowiązuje od 2013 r., wiedza o niej jest znikoma.

Na ograniczenie dostępności do tej wiedzy może wpływać fakt, że Polski Komitet Normalizacyjny nie przetłumaczył jeszcze tego dokumentu, co w świetle obowiązującego prawa nie jest wytłumaczeniem. Stopień 3. powyższej normy jest wymagany dla obiektów przemysłowych, administracji i instytucji finansowych, których destabilizacja może negatywnie wpłynąć na działanie nie tylko tych obiektów, ale również zagrażać społeczeństwu.

Zakłada się, że atakujący jest biegły w zakresie systemów kontroli dostępu, posiada szeroki zestaw profesjonalnych narzędzi i przenośnej aparatury elektronicznej pozwalającej na kopiowanie kart, dokonywanie podsłuchu transmisji danych między czytnikiem a kontrolerem (zwłaszcza gdy w obiekcie jest wykorzystywany interfejs Wiegand) i innych rozwiązań umożliwiających przejęcie kontroli nad obiektem. System KD w takim przypadku ma za zadanie powstrzymać, spowolnić, wykryć i pomóc w identyfikacji.

W odpowiedzi na zapotrzebowanie powstało wiele rozwiązań spełniających stopień 3. Jednym z nich jest polski produkt EQU ACC firmy IFTER. Charakteryzuje się on przede wszystkim modułową konstrukcją – każdy kontroler zawiera port Ethernet pozwalający na komunikację z dwoma serwerami danych.

Na każdym etapie transmisji dane są zabezpieczone na najwyższym poziomie (do szyfrowania wykorzystano najnowsze mechanizmy do autentykacji oraz szyfrowanie AES z mechanizmem zmiany klucza szyfrującego po przesłaniu każdego pakietu). W serii 160 EQU ACC zastosowano obsługę kart Mifare Plus i Mifare DESFire, zapewniających najwyższy poziom zabezpieczeń. Każdy użytkownik sam ustawia klucze obiektowe i szyfrowania, dzięki czemu nawet producent nie ma możliwości uzyskania dostępu.

W EQU ACC w ramach kontrolera (autonomiczny lub globalny) można wykorzystywać *anti-passback* globalny, obejmujący wszystkie kontrolery w sieci (np. jeżeli ktoś nie potwierdził wyjścia z obiektu w Krakowie, nie może wejść do obiektu w Warszawie). Na podobnej zasadzie działa mechanizm śluzowania, często wykorzystywany przy wjazdach do zakładów lub w więziennictwie.

W ramach jednej sieci komputerowej system obsługuje do 65 tys. kontrolerów. Każdy z nich pamięta uprawnienia 64 tys. kart (jedna osoba może mieć więcej niż jedną kartę) oraz 48 tys. zdarzeń. Jeżeli jest potrzebny system dla większej liczby użytkowników, to nie ma problemu, ponieważ EQU ACC jest w stanie rozróżnić do 4 mld unikalnych identyfikatorów (niepotrzebne w obiekcie uprawnienia będą przechowywane w bazie danych na serwerze).

Elastyczność systemu w dostosowywaniu do potrzeb obiektu zwiększa zastosowanie modułowych obudów zapinanych na szynę DIN35 dla kontrolerów i modułów wejść/wyjść, których funkcjonalność swobodnie definiuje instalator. Dla zwiększenia bezpieczeństwa kontroler obsługuje dodatkowe moduły i czytniki po szyfrowanej magistrali RS485 o długości do 300 m.

Oprócz zakresu zasilania 10-28 VDC wszystkie oferowane urządzenia charakteryzują się też niewielkim poborem energii, co pozwala na zastosowanie mniejszych akumulatorów oraz zasilanie urządzeń w przypadku 24 VDC również na znacznych odległościach.

Użytkownik może zarządzać systemem KD poprzez rozbudowane oprogramowanie. W ramach pakietu IFTER EQU zyskuje możliwość swobodnej wizualizacji i integracji z pozostałymi instalacjami w obiekcie, takimi jak systemy: sygnalizacji pożarowej, sygnalizacji włamania, telewizji dozorowej czy automatyki budynkowej z rozbudowanymi układami pomiarowymi.

IFTER Jerzy Taczalski

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

Dahua Technology wkracza z ofertą systemów kontroli dostępu

Firma Dahua Technology ma w swojej ofercie bogate portfolio urządzeń kontroli dostępu i rejestracji czasu pracy. Dostępna oferta pozwala budować systemy sterujące zarówno pojedynczymi przejściami, jak i dużymi, rozproszonymi instalacjami. Aktualną ofertę można podzielić na 6 grup produktowych.

TEKST
Grzegorz Michalski
Dahua Technology

Autonomiczne kontrolery dedykowane do rejestracji czasu pracy (ASA)

Umożliwiają ewidencjonowanie czasu pracy pracowników. Użytkownik może samodzielnie wybrać jeden z typów zdarzeń: wejście, wyjście, początek i koniec przerwy, początek i koniec nadgodzin. Użytkownik jest identyfikowany za pomocą PIN-u/identyfikatora RFID/wzorca biometrycznego lub ich kombinacji. Dane do programu służącego do przygotowania raportów pobierane są poprzez port USB lub moduł TCP/IP. Kontrolery mogą obsłużyć do 30 tys. użytkowników, 3 tys. wzorców biometrycznych i 150 tys. zdarzeń.

Autonomiczne kontrolery obsługujące pojedyncze przejścia (ASI)

Są to urządzenia, które zawierają zintegrowany zarówno czytnik, jak i kontroler. Programowanie może być wykonywane z poziomu wbudowanej klawiatury i wyświetlacza lub aplikacji, np. Smart PSS lub DSS. Kontrolery umożliwiają zabezpieczenie przejść jedno- lub dwustronnie kontrolowanych, wyposażonych w czujnik stanu drzwi, przycisk wyjścia, z obsługą do 30 tys. użytkowników i 3 tys. wzorów linii papilarnych.

Czytniki (ASR)

Pozwalają identyfikować użytkownika za pomocą kodu PIN, identyfikatora RFID lub wzorca biometrycznego. Do komunikacji czytnika z kontrolerem jest stosowany protokół Wiegand lub RS485. Ze względu na to, że czytnik jest jednym z niewielu elementów systemu kontroli dostępu, który jest widoczny dla użytkowników, firma Dahua Technology cały czas rozbudowuje ofertę czytników, by sprostać wymaganiom zarówno technicznym, jak i estetycznym.

Sieciowe kontrolery (ASC)

Spełniają oczekiwania najbardziej wymagających instalacji. W tej grupie można znaleźć zarówno podstawowe, jak i zaawansowane kontrolery serii Caesar. Pojedynczy kontroler serii basic może obsłużyć od 2 do 8 przejść, 100 tys. użytkowników i zebrać 150 tys. zdarzeń. Seria Caesar, oprócz większej pamięci, tj. 200 tys. użytkowników, pozwala na utworzenie globalnych sprzętowych (bez udziału serwera) zależności między 68 przejściami. Warto tutaj wyróżnić globalny *antipassback*, funkcję śluzy, zależności między wejściami a wyjściami alarmowymi.

Kontrolery są dostępne w wersji do montażu na szynę DIN lub w postaci płyty PCB zabudowanej w metalowej obudowie wyposażonej w dedykowany zasilacz i miejsce na akumulator.

Oprogramowanie

Pozwala nadzorować nie tylko system kontroli dostępu, ale również integrować go z innymi grupami produktowymi z oferty Dahua Technology, np. CCTV, wideodomofonami, systemem alarmowym. Aktualnie do obsługi najczęściej jest wykorzystywana bezpłatna aplikacja Smart PSS, która docelowo zostanie zastąpiona przez serwerową aplikację DSS Express w wersji FREE, Plus lub PRO. Wersja FREE, niewymagająca zakupu licencji, umożliwi utworzenie systemu obsługującego maks. 64 drzwi, 128 modułów VDP, 2 kamery rozpoznające twarz i 2 kamery LPR. Wersja PLUS pozwoli zbudować system z obsługą maks. 1024 drzwi, 1024 modułów VDP, 32 kamer rozpoznających twarz i 32 kamer LPR.

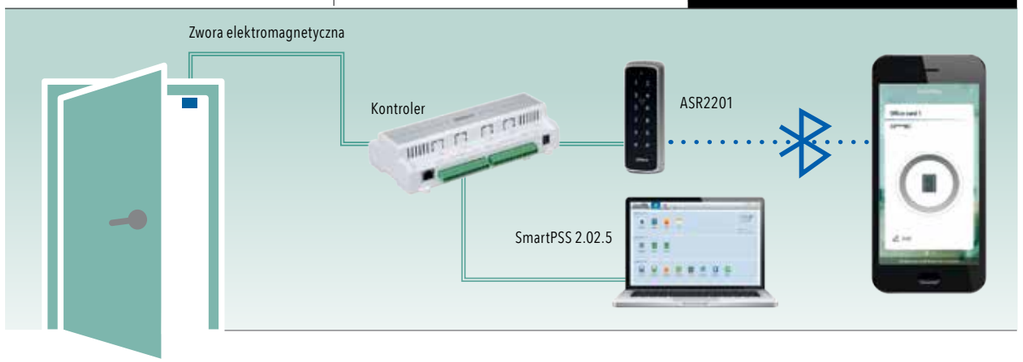
Akcesoria

W tej grupie produktowej znajdują się przyciski wyjścia, przycisk awaryjnego wyjścia, elementy ryglujące, takie jak zwory elektromagnetyczne, elektrozaczepy, elektrorygle, czytniki administracyjne, identyfikatory.

Pełna oferta firmy Dahua Technology jest dostępna pod adresem: https://www.dahuasecurity.com/.

Dahua Technology Poland

ul. Salsy 2, 02-823 Warszawa
www.dahuasecurity.com/pl



Skuteczne zarządzanie uprawnieniami w AEOS

Kontrola dostępu skupiona na ludziach – ponieważ to ludzie, a nie karty potrzebują dostępu

Nadawanie uprawnień ludziom, a nie identyfikatorom

Tradycyjnie systemy zabezpieczeń przydzielają prawa dostępu identyfikatorom, takim jak karty, odciski palców lub kody PIN. Takie podejście jednak różni się od rzeczywistych doświadczeń większości ludzi w przypadku kontroli dostępu. Dostępu wymaga osoba lub pojazd, a nie karta. Dlatego AEOS stosuje wyjątkowy model autoryzacji, który przydziela prawa dostępu osobom i pojazdom, a nie ich identyfikatorom.

Szybciej i bezpieczniej

Ten elastyczny model autoryzacji ułatwia zarządzanie i wyklucza błędy. Nadawanie uprawnień ludziom umożliwia obsługę wielu identyfikatorów przez jedną osobę i ułatwia ich wymianę.
Teraz nie ma już znaczenia, z którego identyfikatora lub z ilu identyfikatorów korzysta dana osoba i czy jest to karta, wydrukowany kod kreskowy, paszport, odcisk palca, głos, a nawet wszystkie jednocześnie. Wszystkie identyfikatory są bowiem powiązane z tymi samymi prawami dostępu danej osoby, dzięki czemu nadanie dodatkowych uprawnień jest bardzo proste.

Działanie modelu autoryzacji

W systemie AEOS ludzi i pojazdy nazywamy nośnikami lub użytkownikami. Użytkownik może mieć jeden lub kilka identyfikatorów, takich jak karta lub odcisk palca.

Użytkownicy mogą mieć prawo do korzystania z jednego albo kilku wejść lub ich grup w określonym przedziale czasowym, jest to ich harmonogram dzienny/godzinowy.
Identyfikatory, dozwolone wejścia i harmonogramy dzienne/godzinowe dla każdego typu użytkownika (np. pracownik, gość lub wykonawca) system łączy w łatwe do utrzymania szablony użytkowników/nośników. Szablony te można następnie przypisać do pojedynczego użytkownika/nośnika lub do grupy. Do jednego użytkownika/nośnika można przypisać wiele szablonów, takich jak pracownik działu B&R czy pracownik zespołu kryzysowego.
W przypadku autoryzacji dotyczących tylko jednego użytkownika można skorzystać z profilu użytkownika w celu unieważnienia określonych autoryzacji w jego szablonie.

Automatyzacja wprowadzania danych autoryzacji za pomocą tzw. silnika reguł

Silnik reguł w systemie AEOS może w znacznym stopniu ułatwić życie administratorom. Może automatycznie i w czasie rzeczywistym łączyć prawa dostępu z atrybutami z bazy danych pracowników w dziale HR, np. dział, budynek lub data nawiązania stosunku pracy.

„Czy trzeba ręcznie wprowadzać do systemu kontroli dostępu dane już wpisane do firmowej bazy danych?"

Następnie wystarczy jedno kliknięcie, aby nadać uprawnienia pojedynczym osobom lub całym grupom – lokalnie lub globalnie. Uprawnienia dostępu pracowników odchodzących z firmy można automatycznie zablokować, a uprawnienia pracowników przeniesionych do innego biura – natychmiast zmienić na odpowiednie prawa dostępu obowiązujące w nowej lokalizacji. Dzięki *Rule Engine* zmiany, które dotychczas zawsze wprowadzano ręcznie, można teraz zautomatyzować i wykonywać bezbłędnie. Dzięki temu autoryzacje są stale aktualne, a ryzyko związane z bezpieczeństwem – ograniczone.

„W razie pożaru można w ciągu kilku sekund zablokować dostęp do budynku wszystkim oprócz pracownikom zespołu kryzysowego"

Możliwość błyskawicznej zmiany scenariuszy bezpieczeństwa dzięki poziomom bezpieczeństwa

Poważne naruszenie bezpieczeństwa może wymagać natychmiastowego podjęcia zdecydowanych działań. Poziomy bezpieczeństwa systemu AEOS umożliwiają wstępne zdefiniowanie dowolnej liczby scenariuszy bezpieczeństwa, które można uruchomić w kilka sekund.
Można np. wstępnie określić uprawnienia i grupy użytkowników, które zostaną zastosowane w przypadku strajku, alarmu pożarowego, dnia otwartego lub zorganizowanego zwiedzania budynku. Użytkownik może przejść do odpowiedniego scenariusza, a następnie przywrócić standardowy scenariusz autoryzacji, gdy sytuacja się wyjaśni.

Poziomy bezpieczeństwa doskonale sprawdzają się w:
- dużych firmach działających w różnych lokalizacjach, regionach lub krajach,
- organizacjach o intensywnym i skomplikowanym ruchu pracowników i odwiedzających,
- firmach wymagających dodatkowego zabezpieczenia ze względu na obsługę niebezpiecznych lub wartościowych towarów.

Zarządzanie rozproszoną infrastrukturą krytyczną

na przykładzie obiektów Służby Więziennej

TRUDNO SOBIE WYOBRAZIĆ WSPÓŁCZESNĄ OCHRONĘ BEZ ELEKTRONICZNYCH SYSTEMÓW ZABEZPIECZEŃ. A PRZECIEŻ NIE SĄ TO JEDYNE URZĄDZENIA I SYSTEMY ELEKTRONICZNE W OBIEKCIE. KIEDY ICH LICZBA PRZEKRACZA SETKI I TYSIĄCE, ZARZĄDZANIE NIMI STAJE SIĘ CORAZ TRUDNIEJSZE NIE TYLKO W KWESTII FUNKCJONALNEJ I EKSPLOATACYJNEJ, ALE TAKŻE W ZARZĄDZANIU MIENIEM.

TEKST
Cezary Mecwaldowski

Infrastruktura krytyczna należy do szczególnej kategorii obiektów. Różnią się one zarówno architekturą, jak i funkcją, podlegają kompetencyjnie różnym podmiotom i operatorom infrastruktury krytycznej. Mimo różnic obiekty te mają też pewne cechy wspólne, np. obiekty służby więziennej są rozmieszczone na dużym obszarze (często całego kraju) i zarządzane przez nadrzędną komórkę organizacyjną, operatora. Nie wszystkie posiadają na swoim terenie służby ochrony, ale są objęte obowiązkową ochroną za pomocą systemów elektronicznych i mechanicznych. Co do samej zasady przedstawione w artykule zarządzanie systemami może być zastosowane do każdej grupy obiektów.

Modernizacje, odrębne wymagania w zakresie kancelarii tajnych, archiwów, magazynów broni oraz innych związanych z podmiotem, któremu podlegają obiekty, powodowały, że przez lata wzrastała liczba systemów zabezpieczeń elektronicznych i urządzeń związanych z bezpieczeństwem. Często były rozbudowywane do rozmiarów powodujących poważne trudności w ich obsłudze i eksploatacji. W rezultacie niezintegrowane systemy zamiast podnosić rzeczywiste bezpieczeństwo obiektu, obniżały je. Przykłady systemów i urządzeń funkcjonujących w chronionych obiektach służby więziennej infrastruktury krytycznej:

- zabezpieczenia elektroniczne (systemy alarmowe, urządzenia ochrony obwodowej, systemy telewizji dozorowej, kontroli dostępu, sygnalizacji pożarowej itp.);
- systemy i urządzenia do kontroli osób, pojazdów, bagażu (skanery X-Ray, bramkowe wykrywacze metali, detektory telefonów komórkowych itp.);
- systemy automatyki budynkowej;
- systemy wentylacji/klimatyzacji;
- systemy automatyki pożarowej, ewakuacyjne, gaszenia, oddymiania;
- systemy rozliczania mediów: energii, gazu, wody, ciepła;
- systemy zasilania gwarantowanego (agregaty prądotwórcze, zasilacze buforowe i UPS, zasilanie solarne);
- systemy nadzoru patroli;
- systemy radarowe, lokalizacyjne obiektów, funkcjonariuszy, osadzonych, dronów itp.;
- systemy zarządzania infrastrukturą IT/ICT, serwerownią – protokół SNMP;
- systemy LPR;
- systemy RCP;
- depozytory kluczy, radiotelefonów, broni itp.;
- systemy łączności przewodowej i bezprzewodowej;
- sterowanie i monitorowanie wind;
- systemy nagłośnienia PA i DSO;
- systemy multimedialne;
- systemy oświetlenia.

Zintegrowanie urządzeń i systemów już w pojedynczym obiekcie przynosi wymierne korzyści w postaci poprawy poziomu bezpieczeństwa. Znacznie większe znaczenie ma zintegrowanie systemów w wielu rozproszonych lokalizacjach, i nie ma tu znaczenia fakt występujących między nimi różnic architektonicznych i funkcjonalnych. Pozwala przede wszystkim zwiększyć bezpieczeństwo obiektów poprzez:

- efektywniejszą obsługę wielu systemów i urządzeń (wizualizacja, jednorodna obsługa różnych systemów, podpowiedzi i automatyka systemu – priorytety wyświetlania, logika, raporty, wizualizacja patroli, dronów itp.);
- niezależny od poszczególnych systemów nadzór nad ich funkcjonowaniem (rejestrowanie i raportowanie usterek, alarmów ułatwia diagnozę, utrzymanie wszystkich systemów w sprawności, rozliczanie z prac eksploatacyjnych i napraw itp.);
- powiązanie różnych sygnałów z sytuacją występującą w obiekcie, np. zapis zdarzenia w powiązaniu (tagi) z pojedynczymi klatkami z systemu dozoru wizyjnego ułatwia wyszukiwanie i identyfikowanie zdarzeń (co bez integracji wymagałoby wiele czasu, zaangażowania większych sił i środków);
- nadawanie uprawnień w systemie w dowolnym zakresie zależnie od potrzeb;
- synchronizację czasu wszystkich zdarzeń i operacji w systemach (utrzymuje czas systemowy niezależnie od zintegrowanych systemów i urządzeń, gdy nie zawsze jest możliwa automatyczna synchronizacja);
- rejestrowanie wykonywanych zadań przez operatora;
- uproszczenie szkoleń stanowiskowych, specjalistycznych i doskonalących.

Najsłabszym ogniwem prawidłowo wykonanych systemów jest człowiek ze swoją naturą i predyspozycjami psychofizycznymi. Profesjonalny system integrujący wspiera użytkowników, i niejako ich „prowadzi". Zapobiega skłonnościom operatora do unikania obowiązków, pomijania procedur. Przypomina o czasowym wyłączeniu systemów lub urządzeń, np. w związku z pracami remontowymi i innymi.

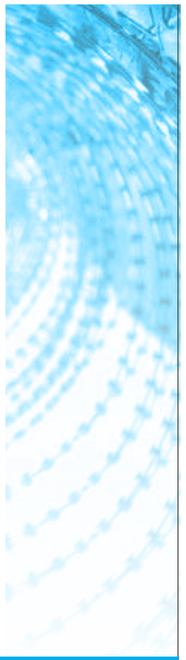
Integrację systemów zabezpieczeń elektronicznych można wykonać za pomocą różnych rozwiązań dostępnych na rynku:

- oprogramowanie do zdalnego zarządzania i konfiguracji systemów zabezpieczeń elektronicznych;
- IB – *Intelligent Building;*
- BMS – *Building Management System*;
- SMS – *Security Management System*;

Zintegrowanie urządzeń i systemów w wielu rozproszonych lokalizacjach, a nawet w pojedynczym obiekcie przynosi wymierne korzyści w postaci poprawy poziomu bezpieczeństwa

- VMS – *Video Management Software*;
- BMCS – *Building Management and Control System*;
- PSIM – *Physical Security Information Management*.

Podana kolejność ma znaczenie. Kolejne rozwiązania nie są tożsame i posiadają coraz większe funkcjonalności. Systemy klasy PSIM są rzeczywistymi integratorami umożliwiającymi hierarchiczne zarządzanie bezpieczeństwem. Skalowalność systemu PSIM umożliwia zarówno rozbudowę, jak i ograniczanie poszczególnych podrzędnych systemów w całej strukturze organizacji. Do uruchomienia systemu PSIM zarządzającego obiektami rozproszonymi potrzebna jest łączność pomiędzy nimi. Obecnie wykorzystuje się technologie IP VPN MPLS do stworzenia infrastruktury WAN z łączami światłowodowymi, satelitarnymi lub LTE. Wprowadzona modernizacja systemu łączności bezprzewodowej w służbie więziennej pozwala na zintegrowanie tego systemu z PSIM. Operatorzy wszystkich jednostek w Polsce mogą komunikować się między sobą za pomocą stacji bazowej poprzez routery sieciowe i strukturę WAN.
Systemy PSIM pozawalają połączyć ochronę obiektu z cyberbezpieczeństwem, nadzorem systemowym infrastruktury IT – system niejako sam siebie nadzoruje. Przykładowo serwerownia w zakresie kompleksowym: pomiar temperatury, wilgotności, zasilania, systemów alarmowych, nadzoru i sterowania klimatyzacji, ale także poprzez protokół SNMP nadzór nad obciążeniem procesorów (także tych wirtualnych), pamięci, dysków w serwerach i macierzach, urządzeń aktywnych sieci i innych.
System PSIM pozwala zarządzać infrastrukturą nie tylko na poziomie gromadzenia danych, wizualizacji, priorytetyzacji, automatyki i podpowiedzi, ale także w zakresie eksploatacji urządzeń, optymalnej gospodarki zasobami, np. kliknięcie na symbol czujki, która sygnalizuje usterkę, pozwala wyświetlić kartę techniczną z informacją nt. urządzenia, napraw i konserwacji, a także historią zdarzeń z tego urządzania.



RYS. 1. SŁUŻBA WIĘZIENNA – JAKO PRZYKŁAD OBIEKTÓW ROZPROSZONEJ INFRASTRUKTURY KRYTYCZNEJ

Źródło: aktualizacja na podstawie Biura Informacji i Statystyki CZSW, grudzień 2018 r.

Koncepcja zarządzania systemami zabezpieczeń elektronicznych w obiektach Służby Więziennej

Polska Służba Więzienna (na koniec 2018 r.) organizacyjnie przedstawia się następująco:

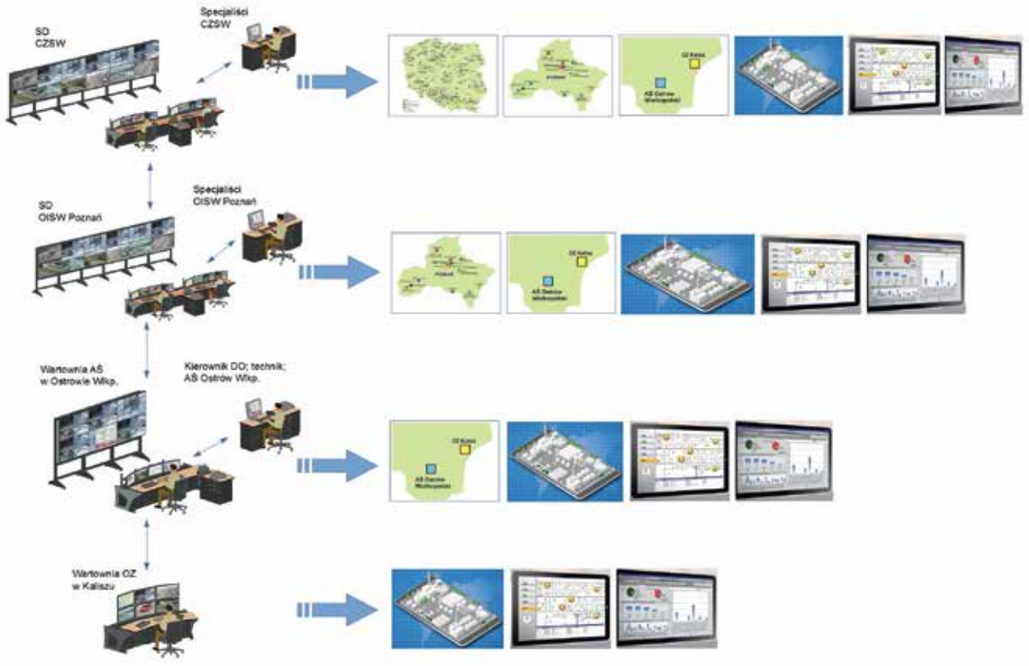
- Centralny Zarząd Służby Więziennej w Warszawie (CZSW);
- Centralny Ośrodek Szkolenia Służby Więziennej w Kaliszu (COSSW);
- 3 ośrodki szkolenia Służby Więziennej z 3 oddziałami (OSSW);
- 15 okręgowych inspektoratów Służby Więziennej (OISW);
- 81 zakładów karnych (ZK);
- 39 aresztów śledczych (AŚ);
- 52 oddziałów zewnętrznych zakładów karnych i aresztów śledczych (OZ);
- 4 oddziały tymczasowego zakwaterowania (OTZ).

Łącznie liczy 199 obiektów rozlokowanych na całym terytorium Polski (rys. 1). W obiektach tych zainstalowano kilkaset systemów zabezpieczeń elektronicznych z kilkuset tysiącami urządzeń, kilkaset agregatów prądotwórczych, kilkaset urządzeń do kontroli, tysiące radiotelefonów itp. Gospodarowanie taką liczbą urządzeń i ich eksploatacja staje się coraz trudniejsza już na poziomie jednostek podstawowych, a co dopiero w skali całego kraju.
Pomimo zmniejszenia liczby jednostek trwały modernizacje i rozbudowy systemów, więc liczba urządzeń się zwiększyła. Widać to szczególnie we wzroście liczby kamer, których w 2012 r. było ponad 13 tys., w 2015 r. – 14,5 tys., a w grudniu 2018 r. – 19,5 tys. Każdy wymieniony powyżej system czy urządzenie może zostać zintegrowane w systemie klasy PSIM – lokalnie w danej jednostce organizacyjnej Służby Więziennej, a następnie włączony w globalny hierarchiczny system zarządzania bezpieczeństwem obiektów całej SW (przykład na *rys. 1 i 4*). Jeżeli w jed-

TABELA 1. KONCEPCJA UPRAWNIEŃ OPERATORÓW W OBIEKTACH SW W ZAKRESIE ZARZĄDZANIA SYSTEMAMI BEZPIECZEŃSTWA

Jednostka organizacyjna SW	Dział	Operator PSIM	Zakres uprawnień systemowych
Centralny Zarząd Służby Więziennej	Ochrona	Stanowisko dowodzenia CZSW	Nadzór nad systemami we wszystkich jednostkach SW (w ograniczonym zakresie poprzez OISW lub bezpośrednio w pełnym zakresie); Zarządzanie systemami i urządzeniami we wszystkich jednostkach SW (w ograniczonym zakresie poprzez OISW lub bezpośrednio w pełnym zakresie); Nadzór nad pracą operatorów OISW, OSSW, ZK/AŚ, OZ; Raportowanie i statystki funkcjonowania systemów bezpieczeństwa w jednostkach
		Specjalista biura ochrony i spraw obronnych BOiSO	Raportowanie ze stanu i funkcjonowania systemów i urządzeń w podziale na OISW; Analiza zdarzeń, alarmów, usterek; Powiązanie zdarzeń z zapisem sygnału wizyjnego; Nadzór nad rozmowami telefonicznymi osadzonych
	Kwatermistrze	Specjalista Biura Kwatermistrzowskiego BKW	Raportowanie ze stanu urządzeń w podziale na OISW; Raportowanie z zużycia mediów w podziale na OISW i poszczególne jednostki; Raportowanie z usterek zasilania i pracy agregatów prądotwórczych, UPS-ów itp.
	Informatyka i łączność	Specjalista Biura Informatyki i Łączności BIŁ	Raportowanie ze stanu urządzeń w podziale na OISW; Nadzór nad systemami łączności, serwerowni, obciążeniem procesorów, pamięci, dysków itp.; Raportowanie z usterek zasilania i klimatyzacji, UPS-ów, systemów gaszenia itp.
Okręgowy Inspektorat Służby Więziennej	Ochrona	Stanowisko dowodzenia OISW	Nadzór nad systemami we wszystkich podległych OISW jednostkach (w ograniczonym zakresie lub bezpośrednio w pełnym zakresie); Zarządzanie systemami i urządzeniami we wszystkich podległych OISW jednostkach (w ograniczonym zakresie lub bezpośrednio w pełnym zakresie); Nadzór nad pracą operatorów ZK/AŚ, OZ; Raportowanie i statystki funkcjonowania systemów bezpieczeństwa podległych ZK/AŚ, OZ
		Specjalista	Raportowanie ze stanu i funkcjonowania systemów i urządzeń jednostek podległych OISW; Analiza zdarzeń, alarmów, usterek; Powiązanie zdarzeń z zapisem sygnału wizyjnego; Nadzór nad rozmowami telefonicznymi osadzonych
	Kwatermistrze	Specjalista	Raportowanie ze stanu urządzeń jednostek podległych OISW; Raportowanie z zużycia mediów; Raportowanie z usterek zasilania i pracy agregatów prądotwórczych, UPS-ów itp.
	Informatyka i Łączność	Specjalista	Raportowanie ze stanu urządzeń jednostek podległych OISW; Nadzór nad systemami łączności, serwerowni, obciążeniem procesorów, pamięci, dysków itp.; Raportowanie z usterek zasilania i klimatyzacji, UPS-ów, systemów gaszenia itp.
Ośrodek Szkolenia Służby Więziennej	Ochrona	Wartownia OSSW	Nadzór nad systemami bezpośrednio w pełnym zakresie; Zarządzanie systemami i urządzeniami bezpośrednio w pełnym zakresie; Nadzór nad pracą operatorów; Raportowanie i statystki funkcjonowania systemów bezpieczeństwa
	Kwatermistrze	Technik	Raportowanie ze stanu urządzeń; Raportowanie z zużycia mediów; Raportowanie z usterek zasilania i pracy agregatów prądotwórczych, UPS-ów itp.
	Informatyka i Łączność	Technik	Raportowanie ze stanu urządzeń; Nadzór nad systemami łączności, serwerowni, obciążeniem procesorów, pamięci, dysków itp.; Raportowanie z usterek zasilania i klimatyzacji, UPS-ów, systemów gaszenia itp.
Zakład Karny / Areszt Śledczy	Ochrona	Wartownia ZK/AŚ	Nadzór nad systemami ZK/AŚ, OZ bezpośrednio w pełnym zakresie Zarządzanie systemami i urządzeniami ZK/AŚ, OZ bezpośrednio w pełnym zakresie Nadzór nad pracą operatorów ZK/AŚ, OZ; Raportowanie i statystki funkcjonowania systemów bezpieczeństwa ZK/AŚ, OZ
		Monitorowy	Obsługa systemu dozoru wizyjnego w zakresie stałego monitorowania zachowania osadzonych
		Bramowy	Obsługa systemów i urządzeń w zakresie kontroli i wejścia do jednostki
		Oddziałowy	Obsługa systemów i urządzeń w zakresie oddziału mieszkalnego; Nadzór nad rozmowami telefonicznymi osadzonych
		Kierownik Działu Ochrony	Raportowanie ze stanu i funkcjonowania systemów i urządzeń; Analiza zdarzeń, alarmów, usterek; Powiązanie zdarzeń z zapisem sygnału wizyjnego; Nadzór nad rozmowami telefonicznymi osadzonych
	Kwatermistrze	Technik	Raportowanie ze stanu urządzeń; Raportowanie z zużycia mediów; Raportowanie z usterek zasilania i pracy agregatów prądotwórczych, UPS-ów itp.
	Informatyka i Łączność	Technik	Raportowanie ze stanu urządzeń; Nadzór nad systemami łączności, serwerowni, obciążeniem procesorów, pamięci, dysków itp.; Raportowanie z usterek zasilania i klimatyzacji, UPS-ów, systemów gaszenia itp.
Oddział Zewnętrzny ZK/AŚ	Ochrona	Wartownia Oddziału Zewnętrznego	Nadzór nad systemami OZ bezpośrednio w pełnym zakresie; Zarządzanie systemami i urządzeniami OZ bezpośrednio w pełnym zakresie; Nadzór nad pracą operatorów OZ; Raportowanie i statystki funkcjonowania systemów bezpieczeństwa OZ
		Bramowy	Obsługa systemów i urządzeń w zakresie kontroli wejścia do jednostki
		Oddziałowy	Obsługa systemów i urządzeń w zakresie oddziału mieszkalnego; Nadzór nad rozmowami telefonicznymi osadzonych

RYS. 2. PRZYKŁAD WIELOPOZIOMOWEJ, HIERARCHICZNEJ WIZUALIZACJI W SYSTEMIE PSIM



Źródło: opracowanie własne autora na podstawie materiałów BIS CZSW i Ela-compil

nostce organizacyjnej jest zainstalowany system integrujący, ale nie jest on klasy PSIM, to nie będzie możliwe zastosowanie integracji globalnej wszystkich jednostek z hierarchią zarządzania.

Hierarchiczny system zarządzania bezpieczeństwem obiektów Służby Więziennej

W systemie PSIM można nadawać uprawnienia operatorom w szerokim zakresie wykorzystania systemu, począwszy od operatora zarządzającego bezpieczeństwem obiektu, przez technika odpowiedzialnego za eksploatację i naprawy, administratora systemu, na uprawnieniach związanych z analizą danych skończywszy. W *tabeli 1* przedstawiono koncepcję przydziału operatorów w hierarchicznej strukturze PSIM wraz z przykładowymi uprawnieniami. Od operatora, w zależności od celu systemu i jego zadań, będą wymagane odpowiednie predyspozycje, wiedza i umiejętności lub nie będą, jeśli pracuje wyłącznie z generowaną statystyką z systemu (np. informacje o zużyciu energii elektrycznej, gazu, wody itp.). Kwatermistrz dostaje informację z systemu o liczbie i czasie trwania awarii zasilania, startach i czasie pracy agregatów prądotwórczych, UPS-ów, zapotrzebowaniu mediów itp.

Systemy PSIM umożliwiają także taką konfigurację uprawnień w hierarchii struktury organizacji, która pozwala na przekierowanie kontroli nad systemami w całości lub w części. Stanowisko Dowodzenia Okręgowych Inspektoratów Służby Więziennej (SD OISW) np. przejmuje kontrolę, nadzór nad systemem ZK lub OZ w sytuacji wystąpienia zdarzenia, braków etatowych lub częściowo w porze nocnej.

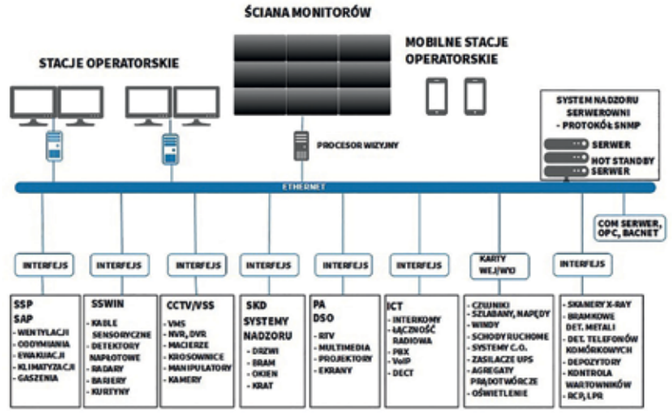
Poszczególne moduły systemu PSIM pozwalają na podział zadań w zależności od przypisanej kompetencji stanowiska operatora w zakresie bezpieczeństwa i eksploatacji obiektów. Przykładowe uprawnienia:

- obsługa systemów zabezpieczeń elektronicznych;
- raportowanie usterek – eksploatacja systemów;
- wykorzystanie urządzeń, alarmy;
- nadzorowanie deponowania kluczy, broni, radiotelefonów;
- nadzorowanie rozmów telefonicznych osadzonych;
- raportowanie IT/ICT;
- raportowanie pracy agregatów;
- generowanie statystyk zadań operatorów, użytkowników, detekcji itp.

Stanowiska dowodzenia SD, wartownie, „monitorowi", „bramowi", „oddziałowi" muszą być dedykowanymi stanowiskami do służby wielozmianowej, pozostali operatorzy jednozmianowi, np. kierownicy ochrony, kwatermistrze, obsługa techniczna, specjaliści OISW i CZSW mogą natomiast posiadać zainstalowaną aplikację w komputerze biurowym. Kiedy występuje hierarchia zarządzania obiektami? Z przypadkiem pracy lokalnej mamy do czynienia np. w sytuacji utraty komunikacji WAN. Gdy komunikacja WAN jest zachowana, odbywa się nadzór systemów z jednostki nadrzędnej, a w określonych przypadkach, np. wystąpienia zdarzenia, może nastąpić przejęcie kontroli nad częścią lub całością zabezpieczeń jednostki organizacyjnej (przejęcie kontroli nad systemami całkowite lub częściowe przez innego operatora w danej jednostce organizacyjnej lub poza nią). System umożliwia także utworzenie operatora mobilnego. Hierarchiczna struktura organizacji, jaką jest Służba Więzienna SW (*rys. 1*), może zostać przeniesiona w hierarchiczną strukturę systemu kategorii PSIM (*rys. 4*). Centralne trójpoziomowe zarządzanie podległymi jednostkami (CZSW – OISW – ZK/AŚ) pozwala na utworzenie struktury, w której występuje zgodny z kompetencjami nadzór nad podległymi jednostkami, a w razie potrzeby umożliwia przekierowanie kontroli nad systemami danego obiektu do innego w strukturze. W CZSW oraz każdym OISW znajdują się stanowiska dowodzenia SD, w których pełniony jest 24-godzinny dyżur. W ZK/AŚ stanowisko dowodzenia jest uruchamiane w sytuacji wystąpienia zdarzenia, jednak te jednostki mają wartownie z 24-godzinnym dyżurem. Przykładową strukturę PSIM przedstawiono na *rys. 3*.

Wizualizacja, jako element *Human Machine Interface*, jest kluczowym elementem systemu PSIM przede wszystkim w zakresie bezpieczeństwa obiektu,

RYS. 3. PRZYKŁADOWY SCHEMAT BLOKOWY INTEGRACJI SYSTEMÓW ZABEZPIECZEŃ I URZĄDZEŃ DLA ZAKŁADU KARNEGO LUB ARESZTU ŚLEDCZEGO



Źródło: opracowanie własne na podstawie Ela-compil

szybkości i efektywności pracy operatora. Prawidłowo wykonana integracja systemów i urządzeń pozwala na efektywną ich obsługę, wymaga często wizualizacji wielopoziomowej (*rys. 2*), optymalizacji i automatyzacji zdarzeń, aby operatorzy byli w stanie obsługiwać pojawiające się sygnały z wielu urządzeń. W średniej wielkości systemie zawierającym kilkaset urządzeń detekcyjnych i kontroli dostępu systemy potrafią generować ponad 1000 sygnałów technicznych i alarmowych na godzinę.

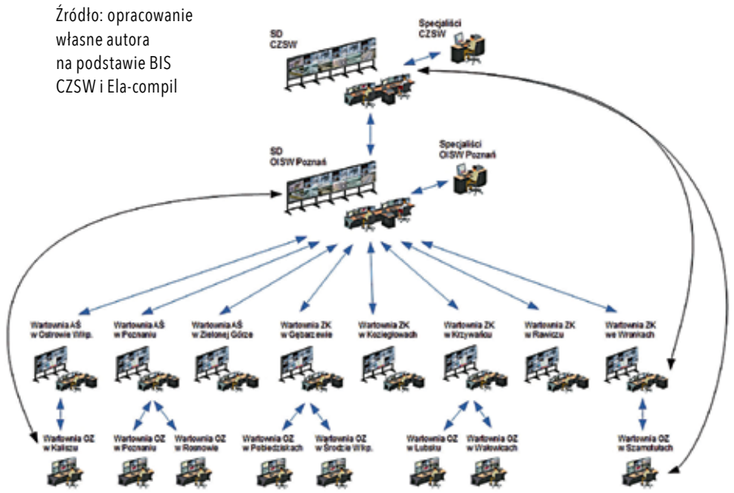
Wizualizacja i aplikacja integratora powinna obejmować:

- plan ogólny obiektów infrastruktury krytycznej,
- plan ogólny obiektu jednostki organizacyjnej,
- plan szczegółowy obiektu, budynku, obszaru z naniesionymi urządzeniami,
- informacje dot. urządzeń,
- powiązanie z obrazem z kamer,
- podpowiedź w postaci procedury dla operatora, a także generować historie zdarzeń oraz umożliwiać analizę danych gromadzonych w systemie i inne.

Podsumowując, nowoczesne, zoptymalizowane i efektywne zarządzanie bezpieczeństwem infrastruktury krytycznej, w której funkcjonuje tak wiele urządzeń i systemów w każdym obiekcie rozproszonej lokalizacji na terenie całego kraju, jest możliwe wyłącznie przy zastosowaniu systemu integrującego opartego na platformie zarządzania bezpieczeństwem klasy PSIM. ▫

RYS. 4. HIERARCHIA ZARZĄDZANIA PSIM NA PRZYKŁADZIE OISW POZNAŃ

Źródło: opracowanie własne autora na podstawie BIS CZSW i Ela-compil



BIO

Cezary Mecwaldowski

Wykładowca zajmujący się szkoleniami zawodowymi i specjalistycznymi z zakresu zabezpieczeń elektronicznych, stosowania urządzeń do kontroli, nowych rozwiązań w dziedzinie systemów alarmowych. Projektant z praktyką zagraniczną. Absolwent Politechniki Łódzkiej o specjalizacjach: energetyka przemysłowa i informatyka stosowana.

Ekosystem Hikvision

Natywna integracja systemów zabezpieczeń

Konwergencja, synergia, integracja – często słyszymy te pojęcia w różnych aspektach naszego życia. Integracja to proces tworzenia całości z części lub włączanie danego elementu w całość. Bardzo często pojęcia te pojawiają się w kontekście technologicznym, np. w odniesieniu do IoT czy w bardzo popularnych systemach smart home. Główną motywacją odbiorców tego typu systemów jest poprawa komfortu użytkowania.

TEKST
Łukasz Lik

Czy w przypadku systemów zabezpieczeń konwergencja, synergia i integracja to pojęcia nowe?
Wręcz przeciwnie, trend ku integracji istnieje tutaj już od dawna i w nowoczesnych systemach bezpieczeństwa to standard. To m.in. dlatego że w obiektach działają różne systemy zabezpieczeń elektronicznych, takie jak ppoż., CCTV, SSWiN i SKD, zależnie od charakteru budynku czy prowadzonej działalności, można tam także spotkać systemy automatyki budynkowej, dystrybucji kluczy, antykradzieżowe, parkingowe i wiele innych. Taka mnogość systemów sprawia, że zarządzanie nimi z poziomu dedykowanej dla każdego z nich stacji obsługi jest, łagodnie mówiąc, kłopotliwe. Wymaga większej obsługi osobowej, a przede wszystkim jest mało efektywne. Systemy odpowiedzialne za bezpieczeństwo powinny także wymieniać między sobą informacje w celu wprowadzenia automatyzacji różnego rodzaju zdarzeń i procesów.
W takich przypadkach klienci mogą posiłkować się aplikacjami dedykowanymi, np. typu PSIM, które pomogą im zintegrować wszystkie systemy. Platforma PSIM jest idealna do dużych i złożonych środowisk.

Lecz nie każda organizacja, bez względu na to, na ile świadomie podchodzi do bezpieczeństwa, wymaga rozwiązania tak specyficznego i złożonego, jak PSIM. Często jest to inwestycja kosztowna, gdyż takie oprogramowanie jest tworzone pod kątem danego obiektu i w związku z tym nieosiągalne dla przedsiębiorców SMB oraz klientów indywidualnych.
W celu m.in. redukcji kosztów ponoszonych przez inwestorów firma Hikvision, jako producent wielu rozwiązań dedykowanych bezpieczeństwu, wprowadziła natywną integrację systemów znajdujących się w jej portfolio. Oferuje rozwiązania zaprojektowane tak, by działając razem, tworzyły ekosystem bezpieczeństwa.

Idea polega na tym, że systemami zabezpieczeń elektronicznych, takimi jak telewizja dozorowa, kontrola dostępu, sygnalizacja włamania czy wideointerkomy, użytkownik może zarządzać z poziomu jednej bezpłatnej platformy IVMS 4200 v3.1 oraz z poziomu jednej aplikacji mobilnej HikConnect. Takie rozwiązanie znacząco upraszcza proces integracji i zarządzania obiektem oraz poprawia komfort pracy operatorów systemu. Składowe ekosystemu wymieniają między sobą informacje, umożliwiając tworzenie różnych scenariuszy alarmowych. Wykorzystując np. telewizję dozorową do weryfikacji alarmów w przypadku różnego rodzaju naruszeń stref w systemie alarmowym czy sygnałów z kontroli dostępu, można wyświetlać obrazy z kamer powiązanych z konkretnym miejscem czy zdarzeniem, wprawiać w ruch kamery PTZ, uruchamiać śledzenie, rejestrację w lepszej jakości, tagować materiał w celu ułatwienia późniejszego dostępu.
Sama analiza obrazu dostępna w kamerach dostarcza operatorom wielu cennych informacji, np. o przeszkodach na drogach ewakuacyjnych czy zajętości miejsc parkingowych. Innym ciekawym przykładem jest coraz powszechniejsze używanie kamer termowizyjnych, które np. podczas zadymienia w sposób ciągły przekazują do centrum nadzoru dobrej jakości informacje obrazowe pozwalające obsłudze trafniej podejmować decyzje. Większą popularnością zaczynają się cieszyć również systemy telewizji dozorowej wyposażone w algorytmy sztucznej inteligencji, stając się najważniejszym elementem naszego ekosystemu.

Coraz dokładniejsza klasyfikacja obiektów, rozpoznawanie cech, twarzy i zachowań przyczyniło się do podniesienia skuteczności ochrony m.in. dzięki znaczącej redukcji fałszywych alarmów spływających do systemu. Rozbudowując ekosystem o urządzenia wyposażone w algorytmy AI i bardziej zaawansowane oprogramowanie, klient ma możliwość rozszerzenia integracji w kierunkach bardziej biznesowych. Łączenie obrazów z kamer z systemami kas fiskalnych (tzw. POS) czy skanerami kodów kreskowych itp. przyczyniło się do szybszej weryfikacji reklamacji klientów. Sygnał z kamery rozpoznającej płeć i wiek osób przechodzących przed banerem reklamowym wysłany do systemu *digital signage* uruchamia dedykowany dla tej grupy content reklamowy. Kamery zliczają klientów, obliczają współczynnik konwersji, informują o tworzących się kolejkach czy brakującym towarze na półkach. I są to rozwiązania już wdrażane u naszych klientów, opisywaliśmy je na łamach czasopisma „a&s Polska”.
Ciekawym zjawiskiem potwierdzającym, jak ważna dla Hikvision jest integracja systemów, jest jej wpływ na działy R&D firmy. Coraz powszechniejsze przenikanie się różnych systemów w warstwie programowej powoduje przeniesienie integracji na warstwę sprzętową, co prowadzi do powstania urządzeń hybrydowych, mających wspólne cechy spotykane dotychczas w oddzielnych systemach. Przykładem może być np. terminal kontroli dostępu z funkcją rozpoznawania twarzy. Komponent CCTV z dwiema kamerami, wykorzystujący efekt stereoskopii, by widzieć w „3D” z algorytmem wykrywającym cechy życia osoby uwierzytelniającej się (nie można go oszukać, przykładając np. zdjęcie), plus elementy kontroli dostępu, interfejs komunikacyjny oraz elementy wykonawcze.
Innym przykładem jest kamera bispektralna – element termowizyjny wykrywający wzrastającą temperaturę czy płomień oraz kamera dozorowa światła widzialnego z algorytmem detekcji dymu jako rozwiązanie wspierające system SSP. Lub coś z pogranicza systemu SSWiN i CCTV, czyli kamera wyposażona w czujkę PIR, lampę błyskową i głośnik pełniący funkcję syreny lub nadający spersonalizowane komunikaty głosowe.

Praktyka integracji systemów zabezpieczeń staje się coraz bardziej zaawansowana, idąc w kierunku kompleksowego zarządzania różnymi systemami. Dużo łatwiej ją osiągnąć, będąc producentem wszystkich rozwiązań, zarówno programowych, jak i sprzętowych. Kluczowe znaczenie ma też odpowiednie podejście do projektowania systemów uwzględniające rozwój technologii. Pojawiają się np. integracje systemów HR z systemami zabezpieczeń – gdy osoba przyłącza się do zespołu lub opuszcza firmę, w systemie dokonują się automatycznie zmiany.
Należy też pamiętać, że integracja systemów zabezpieczeń wymaga bezpiecznej sieci IT. Bezpieczeństwo fizyczne i bezpieczeństwo IT coraz bardziej się zazębiają i w wielu organizacjach osoby odpowiedzialne za każdy z tych elementów często pracują w tych samych działach. Ciekawym przykładem jest np. spadek połączeń telefonicznych z działami wsparcia IT, gdy pracownicy mogą korzystać z jednego poświadczenia, by uzyskać dostęp zarówno do obszarów roboczych, jak i komputerów.
Integracja ma przede wszystkim wspomagać pracę ludzi, a dzięki ekosystemowi Hikvision proces ten jest niezwykle prosty, więc jest sens, by ją wdrażać. □

Hikvision Poland

ul. Żwirki i Wigury 16B, 02-092 Warszawa
tel. 22 460 01 50
faks 22 464 32 11
e-mail:
info.pl@hikvision.com

„Współczesne algorytmy analizy obrazu nadal się do niczego nie nadają. Miały działać tak fantastycznie, a okazuje się, że niczego nie wykrywają albo jest mnóstwo fałszywych alarmów. Trzeba za to płacić, a i tak nie działają tak jak powinny…”

Widzieć więcej

TEKST
Jakub Sobek

CZĘSTO MOŻNA USŁYSZEĆ TAKIE OPINIE I ZARZUTY FORMUŁOWANE POD ADRESEM WSPÓŁCZESNYCH SYSTEMÓW WIZYJNYCH WYPOSAŻONYCH W RÓŻNEGO RODZAJU ALGORYTMY ANALITYCZNE. OCZYWIŚCIE MOŻNA SPOTKAĆ ROZWIĄZANIA BARDZO NISKIEJ JAKOŚCI, KTÓRE SKUTECZNIE DZIAŁAJĄ TYLKO „NA ULOTCE”. JEDNAK WIELE ROZWIĄZAŃ RADZI SOBIE Z DETEKCJĄ INTRUZÓW BARDZO DOBRZE. CHARAKTERYZUJĄ SIĘ WYSOKIM POZIOMEM SKUTECZNOŚCI DETEKCJI PRZY ZACHOWANIU NISKIEGO PROGU FAŁSZYWYCH ALARMÓW.

Dlaczego zatem, nawet przy zaawansowanych algorytmach analizy wizyjnej, efekt działania systemów wizyjnych jest czasem niezadowalający? Czy zostały źle zaimplementowane? Czy to błędy w konfiguracji, projektowaniu, czy doborze sprzętu? Odpowiedź tak naprawdę jest dość prosta – jeśli na wejściu danego algorytmu obraz będzie niskiej jakości, efekt nigdy nie będzie zadowalający. Jeśli ludzkie oko ma problem z zauważeniem na ekranie intruza, to tym bardziej nie można spodziewać się pozytywnego rezultatu po algorytmie wizyjnym.

Działanie analizy wizyjnej

Na początek trzeba przynajmniej skrótowo wyjaśnić, jak działa analiza wizyjna. Choć użytkownik systemu efekty pracy analizy wizyjnej może zobaczyć na obrazie wysokiej jakości, np. w postaci obwiedni pojawiających się wokół obiektów, to trzeba pamiętać, że algorytmy nie pracują na takim obrazie, jaki jest widoczny na ekranie.
Przykładowo, jeśli w systemie stosujemy kamerę o rozdzielczości 3 Mpix, generującą obraz z prędkością 25 kl./s, to praktycznie żaden algorytm nie skorzysta ani z takiej jakości obrazu, ani z takiej liczby klatek. **Pierwszym krokiem jego działania będzie obniżenie liczby klatek na sekundę, np. do 5-10, oraz obniżenie rozdzielczości obrazu do znacznie mniejszych rozmiarów.** W zależności od producenta są to rozdzielczości między QCIF a VGA. Taki zabieg na wejściu algorytmów jest konieczny. Chodzi bowiem o obniżenie mocy obliczeniowych potrzebnych do przeanalizowania obrazu w wysokiej rozdzielczości i z dużą liczbą klatek. Algorytm musi działać w czasie rzeczywistym, nie może dochodzić do jakichkolwiek nawarstwiających się opóźnień w jego funkcjonowaniu. Wymusza to wprowadzanie obrazu na wejściu w sposób strumieniowy. Nawet jeśli jakaś klatka nie dotrze w sposób prawidłowy, nie wykonuje się jej kolejnych retransmisji. Każda ponowna próba przesłania powodowałaby bowiem kolejne opóźnienia w czasie. W systemach zabezpieczenia technicznego powiadomienie alarmowe z analizy wizyjnej musi być generowane w czasie rzeczywistym. Nie ma mowy o kompromisie.
W drugim kroku każda klatka wcześniej przygotowanego strumienia wizyjnego w większości algorytmów jest poddawana procesowi binaryzacji, czyli konwersji obrazu kolorowego lub w skali szarości do obrazu o dwóch poziomach – obrazu binarnego. Zazwyczaj są to kolory biały i czarny, choć można spotkać rozwiązania stosujące kolory, np. czarny i czerwony. Dla skuteczności działania analizy wizyjnej dobór kolorów nie ma specjalnego znaczenia, istotne jest ich skontrastowanie między sobą. Przeprowadzenie binaryzacji na obrazie znacząco redukuje ilość przesyłanych informacji. Operacja binaryzacji najczęściej jest wykonywana metodą progowania. Ustala się tzw. wartość progową, poniżej której piksele przyjmują np. kolor biały, a powyżej kolor czarny (rys. 1). Binaryzacja pozwala na redukcję informacji zbędnych na obrazie i oddzielenie informacji istotnych z punktu widzenia dalszej analizy. Idea ta opiera się na założeniu, że dwie dominanty histogramu reprezentują dwie klasy obiektów – obiekty zainteresowania oraz tło. Takie założenie jednak nie musi być poprawne. Dlatego algorytmy bardziej zaawansowane wykorzystują inne, bardziej złożone metody progowania, np. progowanie iteracyjne metodą Otsu czy metodami entropijnymi. Każda z nich daje inne rezultaty i wymaga innej złożoności obliczeniowej. Dlatego dobór metody uzależnia się od dostępnej mocy procesorów sygnałowych oraz celów stawianych przed daną analizą wizyjną.

Jeśli w systemie stosujemy kamerę o rozdzielczości 3 Mpix generującą obraz z prędkością 25 kl./s, to praktycznie żaden algorytm nie skorzysta ani z takiej jakości obrazu, ani z takiej liczby klatek

Tak przetworzony obraz jest kolejno poddawany różnym operacjom morfologicznym, polegającym m.in. na odszumianiu obrazu i oczyszczaniu z ewentualnych artefaktów, które mogą przeszkadzać we właściwym działaniu algorytmu detekcji.

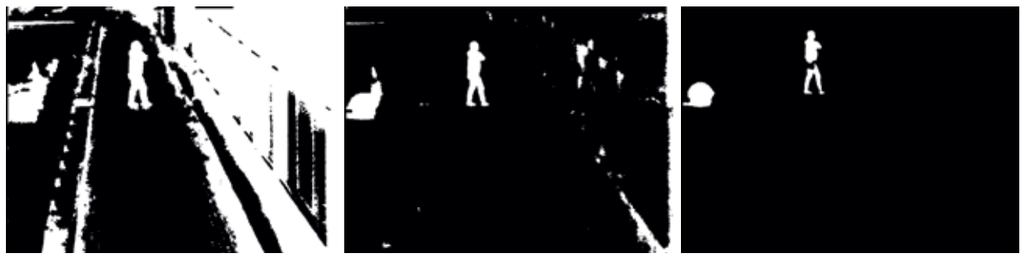
Dopiero na tak przygotowanym obrazie zaczynają działać algorytmy wizyjne. Większość z nich korzysta z estymacji tła na bazie kilku wcześniejszych klatek, natomiast klatka bieżąca trafiająca do analizy jest odejmowana od tła. Dzięki temu analizowane są jedynie nowe obiekty pojawiające się w scenie. To, czy dany algorytm uzna obiekt za obiekt zainteresowania, zależy od jego wielkości, sposobu ruchu, przebytego dystansu w scenie lub czasu przebywania w monitorowanym obszarze. Jeśli obiekt spełnia założenia kryterium alarmowego, generowane jest zdarzenie alarmowe. Mając pojęcie, jak działa większość algorytmów wizyjnych, należy zastanowić się, co ma wpływ na poprawę skuteczności ich działania. Skoro algorytmy działają na niskiej rozdzielczości, to wiadomo że wybór kamer o wysokich rozdzielczościach nie będzie miał wpływu na poprawę skuteczności. Z tego powodu jeśli wybierzemy kamerę IP o wysokiej rozdzielczości i kamerę analogową o tym samym kącie widzenia, przy założeniu że jakość obrazu z obu kamer jest porównywalna, to skuteczność wybranego rozwiązania analizy wizyjnej powinna być praktycznie taka sama. Warto więc pamiętać, że podnoszenie rozdzielczości kamer stosowanych w systemie nie zawsze podniesie skuteczność detekcji.
Zasięg detekcji danego algorytmu wizyjnego możemy natomiast poprawić, zmieniając kąt widzenia kamery – im węższy kąt obserwacji, tym większy zasięg pracy. Spowodowane jest to faktem, że zawężając kąt widzenia, zwiększamy szczegółowość obrazu w dalszych obszarach. Obiekt może zostać poprawnie wykryty przez dany algorytm, jeśli liczba pikseli reprezentująca obiekt w scenie będzie wystarczająca. W języku angielskim mówimy o parametrze *Pixel on Target* – określającym ile minimum pikseli musi zajmować np. osoba w scenie przy danej rozdzielczości, aby istniała możliwość skutecznej detekcji przez dany system.
Kolejnym bardzo istotnym czynnikiem wpływającym na jakość detekcji jest rodzaj zastosowanej kamery. W tym wypadku często projektanci lub instalatorzy stają przed wyborem typu kamery – kamera z wbudowanym oświetlaczem, zewnętrznym oświetlaczem, a może kamera termowizyjna? Tutaj wpływ na jakość działania algorytmów jest na tyle duży, że należy przyjrzeć się temu nieco uważniej.

Jaka kamera?

Ludzkie oko widzi część spektrum promieniowania elektromagnetycznego, zwanego potocznie światłem widzialnym. Nie widzi światła ultrafioletowego ani podczerwieni. Jeśli chodzi o kamery, mamy możliwość wyboru pomiędzy kamerami, które widzą w spektrum zbliżonym do ludzkiego oka, i takimi, które korzystają z innych zakresów fal.
Jednym z często powtarzanych błędów jest opinia, że podczerwień i emisja ciepła to dokładnie to samo. Tak jednak nie jest. Podczerwień można podzielić na pasma – bliska podczerwień obejmuje pasmo z zakresu 700-1000 nm, natomiast obrazowanie termiczne, czyli widzenie „ciepła", to fale znacznie dłuższe.

Kamera z wbudowanym oświetlaczem

Są jednymi z najczęściej wybieranych kamer w systemach dozoru wizyjnego ze względu na wysoką ich dostępność oraz niską cenę takich rozwiązań. Instalacja kamer IP tego typu jest bardzo prosta – montując jedno urządzenie, instalujemy zarówno oświetlacz, jak i kamerę. Łatwe jest także okablowanie takiego systemu. Większość kamer wraz z oświetlaczem można zainstalować za pomocą pojedynczego przewodu ethernetowego, który podłącza urządzenie do sieci oraz pozwala na zasilanie przez PoE/PoE+. Dzięki temu w miejscu instalacji nie jest konieczne stosowanie dodatkowego zasilacza.



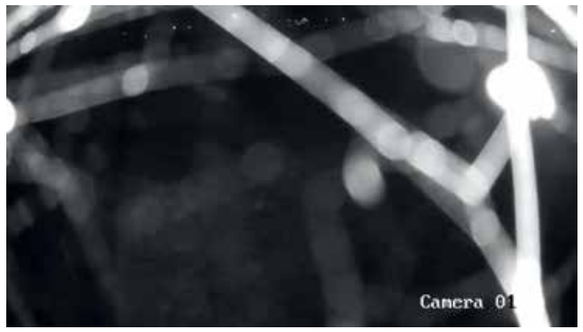
Rys. 1. Obraz termowizyjny po operacji binaryzacji wykonany dla trzech różnych wartości progowania

Czy takie z pozoru bardzo wygodne i przemyślane rozwiązanie ma jakieś wady? Niestety dość dużo. Oświetlacze w kamerach mają zazwyczaj bardzo niską jakość. Z tego powodu scena jest oświetlona bardzo nierównomiernie, niektóre obszary obrazu są bardzo mocno prześwietlone, a niektóre niedoświetlone. Często można także zauważyć niedopasowanie wbudowanego oświetlacza do kąta widzenia kamery – objawia się to niedoświetleniem boków monitorowanej sceny (*rys. 2*). Ponadto wbudowane oświetlacze wykorzystują zazwyczaj pasmo o długości fali 750 nm, emitują więc nie tylko podczerwień, lecz także fale widoczne dla ludzkiego oka. Zatem patrząc w ciemności w kierunku kamery, widać palące się na czerwono diody. Sprawia to, że monitoring nie jest już dyskretny i trudny do zauważenia. Jedną z najistotniejszych wad tego rozwiązania jest przyciąganie owadów przed obiektyw. Podlatują one do oświetlacza i przy dużym prześwietleniu przez znajdujący się blisko oświetlacz mogą wzbudzić wiele fałszywych alarmów. Taki oświetlacz prześwietla bardzo mocno także nawet niewielkie pajęczyny znajdujące się na obiektywie. Czasem prześwietlenie jest na tyle duże, że praktycznie nie widać monitorowanej sceny.

Kamera z zewnętrznym oświetlaczem

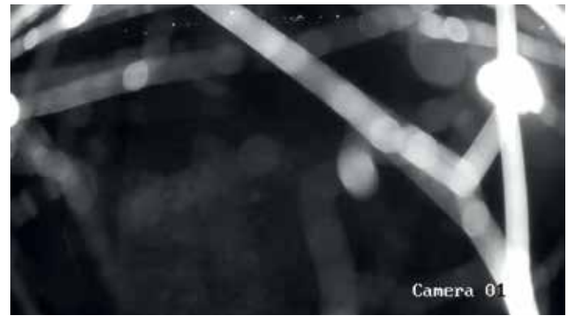
Dodanie zewnętrznych oświetlaczy do kamer pozwala na zastosowanie większych i znacznie silniejszych źródeł światła. Obszar może być oświetlony na znacznie większym dystansie i dzięki temu zasięg działania analizy wizyjnej w ciągu dnia oraz w nocy może pozostawać na podobnym poziomie. Zewnętrzne oświetlacze dobrej jakości także znacznie równomierniej oświetlają scenę dzięki możliwości zastosowania w takich lampach większej liczby diod IR oraz soczewek odpowiednio rozpraszających światło. Takie rozproszenie światła eliminuje prześwietlenia lub niedoświetlenia fragmentów sceny. Na rynku jest bardzo wiele modeli oświetlaczy, zarówno o mniejszej mocy z szerokim kątem świecenia, jak i znacznie mocniejsze o wąskim kącie, które są szczególnie przydatne np. w ochronie perymetrycznej. Są też dostępne oświetlacze o długości fal np. 950 nm, niewidocznej dla ludzkiego oka.

Rys. 2. Kąt świecenia wbudowanego oświetlacza niezgodny z kątem widzenia kamery. Brzegi obserwowanej sceny są zupełnie nieoświetlone



Rys. 3. Kamera z silnie prześwietlonymi pajęczynami na obiektywie

Zwiększenie rozdzielczości kamer w systemie nie zawsze podniesie skuteczność detekcji



Rys. 4. Kamera z silnie prześwietlonym pająkiem na obiektywie. Wykrycie obiektów jest niemożliwe – system jest w takim momencie niezdatny do pracy

Wadą zewnętrznych oświetlaczy jest także nieco wyższy koszt od rozwiązania zintegrowanego, konieczna jest bowiem instalacja dwóch osobnych urządzeń. Od strony instalacyjnej oświetlacze zewnętrzne mogą być zasilane na dwa sposoby – albo klasycznie z zasilacza, albo przez przewód sieciowy z wykorzystaniem PoE/PoE+. Na rynku są także oświetlacze, które można zdalnie konfigurować przez wbudowany web serwer. Dzięki temu lampę można zdalnie włączać lub wyłączać, a także np. sterować mocą świecenia. Rozwiązania typu VMS pozwalają na integrację takich rozwiązań i zarządzanie nimi.
Korzystając z analizy wizyjnej, trzeba pamiętać, by zewnętrzny oświetlacz był zainstalowany w pewnej odległości od kamery (np. 1 metr pod kamerą). Dzięki temu„odciągamy" owady od obiektywu kamer, a to skutkuje znacznym zmniejszeniem liczby fałszywych alarmów. Przy instalacji lamp trzeba zwrócić uwagę na kierunek ich świecenia i właściwy dobór mocy, aby oświetlacz, pracując z jedną kamerą, nie oślepiał pozostałych. Oświetlacz IR nie może być też zainsta-

lowany zbyt nisko. Taka pozycja montażu powoduje, że nawet małe obiekty będą miały bardzo długi cień. Analiza obrazu może wówczas małe obiekty klasyfikować jako znacznie większe i system będzie generował dużą liczbę niepożądanych alarmów.

Rys. 5. Zewnętrzny oświetlacz podczerwieni umożliwia równomierne oświetlenie obserwowanej sceny.

Kamera termowizyjna

To kolejne rozwiązanie pozwalające na widzenie w paśmie podczerwieni. Najpopularniejsze i najczęściej stosowane w systemach zabezpieczenia technicznego wykorzystują fale o długości z zakresu 7-14 µm. Rzadziej spotyka się kamery działające w paśmie 3-5 µm ze względu na ich znacznie wyższą cenę.
Kamery termowizyjne charakteryzuje możliwość pracy w zupełnej ciemności – nie potrzebują one żadnych dodatkowych źródeł światła (np. oświetlacza IR), ponieważ nie wykorzystują efektu rejestracji światła odbitego. Kamera termowizyjna korzysta z emisji podczerwieni z obiektów obserwowanych. Każdy obiekt cieplejszy od zera stopni Kelvina, czyli tzw. zera bezwzględnego, emituje takie właśnie promieniowanie termiczne (cieplne).
Od wielu już lat kamery termowizyjne są coraz powszechniej stosowane w systemach dozoru wizyjnego. Duży wpływ na to ma spadek ceny, coraz więcej też osób docenia zalety tych rozwiązań. Jednym z atutów takich kamer jest znacznie skuteczniejsza obserwacja za ich pomocą nawet w trudnych warunkach atmosferycznych, np. w czasie mgły, opadów deszczu lub gęstego śniegu. Wprawdzie w takich warunkach może skracać się skuteczny dystans obserwacji, jest on jednak znacznie większy niż w przypadku tradycyjnych kamer.
Bardzo istotna jest także wysoka czułość kamer termowizyjnych wynosząca 30-50 mK. Pozwala to na rozróżnienie obiektu od tła przy tak niewielkiej różnicy ich temperatury, jak 0,03-0,05 stopnia Celsjusza. Dzięki temu nawet obiekty pojawiające się w scenie są bardzo mocno skontrastowane z tłem. Wysoki kontrast obrazu ma bardzo pozytywny wpływ na znacznie skuteczniejsze działanie analizy obrazu. W takich strumieniach wizyjnych znacznie łatwiej dokonać wyodrębnienia obiektu z estymowanego tła. Znacznie łatwiej także wyznaczyć realne krawędzie obiektu i dużo precyzyjniej określić jego wielkość. To właśnie parametry opisujące wielkość obiektu często decydują, czy obiekt jest pozytywnie klasyfikowany, np. jako potencjalny intruz.
Kamera termowizyjna nie widzi światła widzialnego, dlatego nie widzi nawet długiego cienia za obiektem. Nie zakłóca jej widzenia światło zachodzącego lub wschodzącego słońca. Tradycyjne kamery mogą być przez światło słoneczne oślepiane, co uniemożliwia skuteczną obserwację chronionego obszaru i prawidłowe funkcjonowanie analizy wizyjnej. Kamery termowizyjnej nie można celowo oślepić nawet przez najsilniejsze źródło światła widzialnego lub wiązkę lasera, ponieważ są to długości fal, których taka kamera nie widzi.

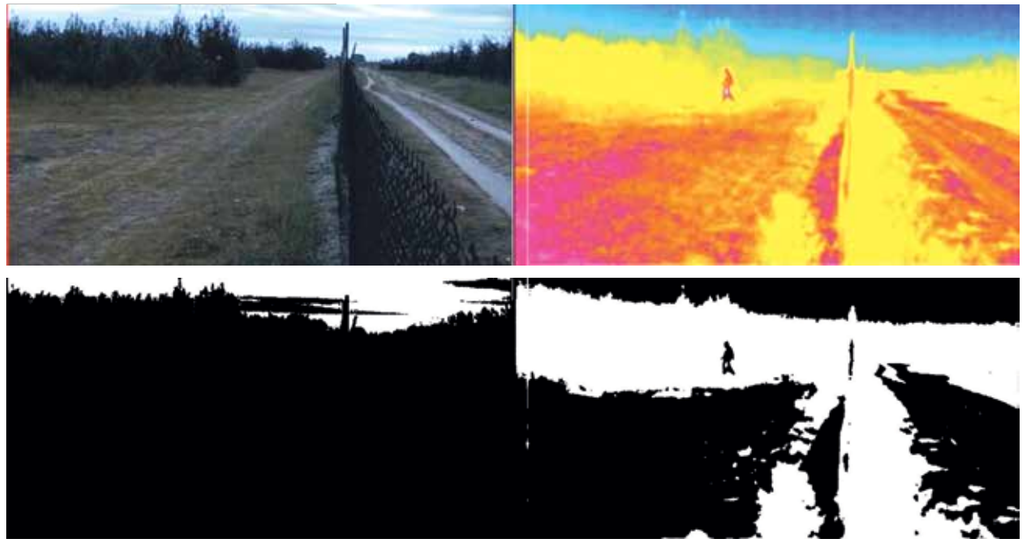
Olbrzymią przewagą kamer termowizyjnych jest ich wysoka czułość na pojawiające się w scenie obiekty. Analiza obrazu na takich strumieniach działa znacznie skuteczniej, nawet przy dużych odległościach obserwacji

Kolejną zaletą stosowania kamer termowizyjnych jest brak problemu przelatujących owadów, drobnych pajęczyn itp. przed obiektywem. Nawet jeśli owady przelatują przed kamerą, nie wpływają one na działanie analizy wizyjnej.
Choć wiele osób nadal wskazuje, że cena tych kamer jest wyższa od rozwiązań tradycyjnych, należy pamiętać, że kamera termowizyjna może obserwować znacznie większe dystanse. Wiele algorytmów analizy wizyjnej zoptymalizowanych do działania z takimi kamerami potrzebuje o połowę mniej pikseli na cel niż kamery z oświetlaczem. Tradycyjne kamery w ochronie perymetrycznej powinny być instalowane co ok. 50 m, natomiast kamery termowizyjne mogą być instalowane np. co 200-300 m, więc może ich być znacznie mniej. To duża oszczędność także kosztów instalacji, przestrzeni dyskowych potrzebnych do rejestracji obrazu czy np. liczby licencji w systemie VMS do wszystkich kamer.

Czy kamery termowizyjne mają jakieś wady?

Często stawianym im zarzutem jest niższa rozdzielczość i brak możliwości rozpoznania twarzy osoby wchodzącej np. w strefę perymetryczną. Pamiętajmy, że zazwyczaj osoba próbująca wtargnąć na obiekt i tak ma zamaskowaną twarz, więc nawet tradycyjna kamera nie ma możliwości jej zidentyfikowania. Podstawowym celem kamer w systemach dozoru wizyjnego jest skuteczna detekcja intruza i maksymalne skrócenie czasu reakcji na zdarzenie. Takie możliwości zapewniają właśnie kamery termowizyjne. Zatem lepiej szybko zareagować na pojawiające się zagrożenie, niż po fakcie, na podstawie zarejestrowanego wizerunku twarzy próbować odnaleźć osobę, która dokonała szkody. Lepiej zapobiegać zagrożeniom, niż działać po fakcie.

Rys. 6. Analiza wizyjna pracująca w kamerze termowizyjnej. Binaryzacja obrazu termowizyjnego została zaprezentowana na rys. 1



Rys. 7. Porównanie obrazu z kamery termowizyjnej oraz tradycyjnej, poniżej te same obrazy po operacji progowania.

Podsumowanie

Choć nadal znacznie popularniejsze są kamery z wbudowanym lub zewnętrznym oświetlaczem podczerwieni, bardzo łatwo wskazać, jak wiele wad mają, gdy korzystają z wizyjnej analizy obrazu. Osoba, która ma nieco większą wiedzę na temat działania takich systemów, bez problemu oszuka większość algorytmów. Wystarczy odpowiedni strój oraz sprzyjające warunki pogodowe i oświetleniowe, by w sposób niezauważony wejść na teren chronionego obiektu.
Rozwiązaniem tego problemu jest dodatkowe wsparcie urządzeniami opartymi na innych technologiach detekcji. Mogą to być np. dodatkowe czujki PIR, bariery mikrofalowe, radary czy systemy światłowodowe.Korelacja takich systemów pozwala zwiększyć zabezpieczenie techniczne całego obiektu.

Olbrzymią przewagą kamer termowizyjnych jest ich bardzo wysoka czułość na pojawiające się w scenie obiekty. Analiza obrazu na takich strumieniach działa znacznie skuteczniej, nawet na dużych odległościach. Liczba ewentualnych fałszywych alarmów także jest znacznie niższa, mniejsze jest obciążenie operatorów pracujących w zdalnych centrach monitorowania alarmów, wyższa ich wydajność pracy. Jeden operator może obsługiwać większą liczbę obiektów. W przypadku dużej liczby fałszywych alarmów z tradycyjnych kamer z analizą wizyjną dochodzi do uśpienia czujności operatora centrum monitoringu. Wówczas nietrudno o pomyłkę i przeoczenie wśród wszystkich alarmów tego jednego, istotnego i realnego.

Obecnie zauważalnym trendem jest obniżanie kosztów obsługi i czasu potrzebnego na zdalną obsługę obiektów. Zatem naturalnym kierunkiem jest popularyzacja kamer termowizyjnych. Każdy, kto chociaż raz wypróbuje współpracę kamer termowizyjnych z analizą obrazu, nie będzie chciał już wracać do kamer tradycyjnych. □

LITERATURA:

1. C. M. Lee, K. E. Schroder, E. J. Seibel: Efficient image segmentation of walking hazards using IR illumination in wearable low vision aids, The Human Interface Technology Laboratory, University of Washington, Seattle, 2002
2. M. C. Maki, M. C. Dickie: New Options in Using Infrared for Detection, Assessment and Surveillance, Senstar, Canada 1996
3. Tae-Hyun Oh, Joon-Young Lee, In So Kweon: Real-time motion detection based on discrete cosine transform, Robotics and Computer Vision Lab, KAIST, Korea 2012
4. K. Verma, D. Ghosh, D. Pundir, A Kumar: Target Detection and Tracking in Infrared Videos Using Frequency Domain Analysis and Machine Learning for Surveillance, 5th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON) 2018
5. P. Battalwar, J. Gokhale, U. Bansod: Infrared Thermography and IR Camera, International Journal of Research In Science & Engineering e-ISSN: 2394-8299 Volume: 1 Issue: 3, 2013

BIO

Jakub Sobek

Absolwent Politechniki Poznańskiej na Wydziale Robotyki i Automatyki, specjalność Systemy wizyjne i multimedialne. Po studiach rozpoczął pracę w firmie Linc Polska na stanowisku trenera technicznego. W 2012 r. zdał egzamin trenera technicznego MOBOTIX, do dziś jest jedynym certyfikowanym trenerem MOBOTIX w Polsce. Posiada także certyfikat trenera rozwiązań FLIR Security Products. Od roku 2015 jest pracownikiem dydaktycznym oraz doradcą zarządu PISA.

www.axis.com/pl

Axis: AXIS Q1942-E sieciowa kamera termowizyjna

Wyjątkowo skuteczna detekcja i szybka weryfikacja

- ➜ Obrazowanie termowizyjne w wysokiej rozdzielczości
- ➜ Wyjątkowy kontrast pozwalający zarejestrować więcej szczegółów
- ➜ Wysoka jakość detekcji dzięki wbudowanym aplikacjom do analizy treści wizyjnej
- ➜ Elektroniczna stabilizacja obrazu
- ➜ Technologia Zipstream firmy Axis

Kamera AXIS Q1942-E zapewnia skuteczną detekcję, szybką weryfikację i reakcję na różnorodne zdarzenia w warunkach od całkowitej ciemności po jasne słońce. To doskonały wybór do dozoru w sytuacjach krytycznych.

Kamery termowizyjne z inteligentnymi funkcjami analizy wykrywają ludzi, przedmioty i zdarzenia w całkowitej ciemności lub w innych trudnych warunkach, takich jak obszary o dużym zapyleniu lub zadymieniu. Wysoki poziom kontrastu obrazów termowizyjnych zapewnia dużą dokładność przy korzystaniu z kamer termowizyjnych wyposażonych w funkcje analizy obrazu: fałszywe alarmy są ograniczone do absolutnego minimum, ponieważ warunki środowiskowe (zmiany oświetlenia, deszcz, śnieg, poruszająca się roślinność, owady, odbicia i cienie) mają minimalny wpływ na ich pracę.

Dzięki oprogramowaniu AXIS Perimeter Defender lub AXIS Guard Suite kamery wysyłają powiadomienia informujące personel o sytuacjach wymagających interwencji. Można też włączyć kamery klasyczne, aby rozpocząć rejestrację lub wykonać zbliżenie, gdy kamera termowizyjna wykryje intruza.

AXIS Q1942-E ma rozdzielczość termowizyjną 640 x 480 VGA, jedna kamera rejestruje zdarzenia na dużym obszarze i z dużej odległości. Z kolei elektroniczna stabilizacja obrazu eliminuje zakłócenia nawet w przypadku narażenia kamery na drgania. W rezultacie otrzymujemy wyjątkowe możliwości detekcji i szybką wzrokową weryfikację charakteru wykrytych zdarzeń. Zdarzenia można odrzucić lub podjąć odpowiednie działania, aby zminimalizować liczbę fałszywych alarmów.

www.bcscctv.pl

BCS: Kamera bispektralna BCS-TIP42101-TW

Kamera bispektralna BCS-TIP42101-TW to ciekawe nowoczesne rozwiązanie mogące stosunkowo niewielkim kosztem znacząco podnieść stopień zabezpieczenia obiektu i uwrażliwić system monitoringu wizyjnego na zagrożenia zupełnie nowego typu.

Kamera charakteryzuje się zwartą budową, jak to ma miejsce w przypadku zwykłych kamer tubowych, jednak w tym przypadku znalazło się miejsce na umieszczenie dwóch modułów kamerowych. Jeden z nich to zwykła 2-megapikselowa kamera działająca w połączeniu z promiennikiem IR, zapewniająca użytkownikowi wszystko to, czego oczekuje od tego typ urządzenia – dostęp do funkcji analizy obrazu, praca w warunkach niedostatecznego oświetlenia czy zdalny podgląd i konfiguracja są tutaj standardem.

Drugi moduł natomiast to kamera termowizyjna, dzięki której obserwacja każdej scena prezentowana w nowych, umownych kolorach nie zależy od warunków oświetlenia. Tego typu rozwiązanie sprawdzi się zarówno w nocy, jak i za dnia, wskazując miejsca mogące stanowić poważne zagrożenie. Kamera może odpowiednio szybko zaalarmować w momencie np. wykrycia pożaru, lub skorzystać z funkcji analizy obrazu niezależnych od tych ustawionych w drugim module. Dzięki takiemu rozwiązaniu można zwiększyć czułość detekcji obiektów, które mogłyby umknąć analizie w zwykłej kamerze, np. ze względu na niesprzyjające warunki atmosferyczne, bez wpływu na liczbę generowanych fałszywych alarmów.

Kamera bispektralna emituje dwa strumienie wizji (normalny i termowizyjny), dzięki czemu mamy możliwość podglądu obu strumieni jednocześnie, wyboru jednego z nich lub hybrydy wyświetlanej w trybie PIP.

www.dahuasecurity.com/pl

DAHUA: Kamera bispektralna TPC-BF5400

Kamery termowizyjne długo były kojarzone z technologią dostępną jedynie dla wojska lub ochroną dużych obiektów infrastruktury krytycznej. Mimo że ta technologia sprawdza się rewelacyjnie przy obserwacji rozległych, nieoświetlonych terenów, mało kto decydował się na stosowanie takich kamer ze względu na wysokie ceny urządzeń.

W 2017 r. Dahua Technology wprowadziła do oferty nowe bispektralne kamery termowizyjne z funkcją fusion, która w unikalny sposób na obraz o rozdzielczości full HD nakłada obraz z modułu termowizyjnego. Model TPC-BF2120 łączy zalety kamer termowizyjnych i kamer tradycyjnych, niwelując ich potencjalne wady, a powstała technologia jest dostępna nawet dla odbiorców indywidualnych.

Opracowanie nowego, bardzo czułego detektora (czułość 40 mK), pracującego w zakresie 7-14 m zaowocowało nową linią profesjonalnych kamer tulejowych – TPC-BF5400. Matryca detektora o wymiarach 400 x 300 pikseli rozwiązuje częsty problem zbyt małej szczegółowości popularnych detektorów o rozdzielczości CIF i zbyt wysokiej ceny detektorów o rozdzielczości VGA.

Kamery nowej linii mogą być wyposażane w obiektywy szerokokątne umożliwiające detekcję obiektów z odległości nawet 4000 m oraz w funkcje analizy treści obrazu, m.in. wykrycie intruza, przekroczenie linii czy detekcja źródeł ognia.

Zadbano także o interfejs użytkownika. Model TPC-BF5400 wykorzystuje komunikację zarówno IP, jak i analogową. Standard HDCVI umożliwia pracę kamery z wykorzystaniem istniejącego okablowania koncentrycznego, zapewnia też zdalne sterowanie kamerą i zmiany trybów prezentacji kolorów.

Firma Dahua Technology rozwija segment kamer termowizyjnych – podstawę doskonalszych systemów ochrony, dostępnych dla większej liczby odbiorców.

www.hikvision.com/pl

HIKVISION: Kamera termowizyjna DS-2TD1217-2/3/6'V1

Firma Hikvision od wielu lat dostarcza najwyższej jakości kamery termowizyjne. Popularność i niezawodność rozwiązań wymusiła wprowadzenie urządzeń, które nadają się do mniejszych obiektów.

Model DS-2TD1217 jest dostępny w trzech wersjach: z obiektywami 2, 3 i 6 mm. Wbudowany procesor graficzny, który obsługuje algorytmy sztucznej inteligencji, może realizować bardzo precyzyjnie funkcje VCA, takie jak przekroczenie linii czy detekcję intruza oraz dodatkowo algorytm detekcji ognia i pomiar temperatury, z możliwością elastycznego ustawiania progów alarmowych.

W sytuacjach zagrożenia bezpieczeństwa niezwykle istotnym czynnikiem jest wideoweryfikacja. Termowizja pozwala zobaczyć to, czego w ciemności lub trudnych warunkach atmosferycznych (mgła, dym, opady) tradycyjna kamera oraz ludzkie oko nie są w stanie dostrzec. Ta sama zasada obowiązuje również w drugą stronę. DS-2TD1217 łączy dwie technologie. W modelu tym, tuż obok modułu termowizyjnego o rozdzielczości 160 x 120 pikseli, został umieszczony moduł optyczny o rozdzielczości 1920 x 1080 pikseli. Mimo małych rozmiarów w obudowie znaleziono miejsce również na oświetlacz IR o zasięgu do 15 m. Funkcje kamery umożliwiają wyświetlanie obrazów z obu modułów na jednym podglądzie. Funkcja *Picture in Picture* nakłada obraz termowizyjny na obraz z modułu optycznego. Kolejnym benefitem, jaki daje kamera bispektralna, jest fuzja obrazów polegająca na nałożeniu szczegółów (kontury obiektów), które widzi kamera „tradycyjna", na obraz z kamery termowizyjnej.

Warto podkreślić fakt, że w kamerach termowizyjnych marki Hikvision standardem jest odświeżanie 25 fps, co zapewnia duży komfort podglądu obrazu oraz wysoką skuteczność detekcji.

Do tej pory termowizja kojarzyła się z rozwiązaniami bardzo drogimi i często nieosiągalnymi. Przedstawiona seria kamer Hikvision zdecydowanie zmienia sytuację. Jest to kompletne urządzenie idealnie nadające się do zastosowań security. Połączenie obu przetworników w jednej obudowie zapewnia wysoki poziom bezpieczeństwa, a także szybką i sprawną weryfikację zdarzeń. Wyjątkowo małe ogniskowe obiektywu oraz szerokie kąty widzenia umożliwiają korzystanie z tego urządzenia w takich miejscach jak serwerownie. Kamera sprawdzi się również w ochronie perymetrycznej niewielkich obiektów.

www.linc.pl

Linc Polska: FLIR Saros – znacznie więcej niż kamera termowizyjna...

Kamera termowizyjna Saros marki FLIR Systems Inc. (FLIR) została opracowana do ochrony obwodowej. To kompaktowe rozwiązanie łączy technologię termowizyjną z technologią światła widzialnego oraz analizą wizyjną. FLIR Saros to 4 w 1:

1. dwa przetworniki termowizyjne;
2. przetwornik światła widzialnego o rozdzielczości 1080p lub 4K;
3. oświetlacze LED w zakresach bliskiej podczerwieni i światła widzialnego;
4. wbudowana analiza wizyjna.

FLIR Saros umożliwia wykrycie potencjalnego intruza z wykorzystaniem termowizji i zaawansowanej analizy obrazu, a następnie ułatwia weryfikację tego obiektu przez kamerę światła widzialnego w rozdzielczości nawet 4K, z doświetleniem sceny oświetlaczami LED w paśmie światła widzialnego i bliskiej podczerwieni.

Wykorzystanie kamer FLIR Saros umożliwia:

- całodobowy monitoring bez konieczności stosowania dodatkowych kamer tradycyjnych;
- dwukierunkową transmisję audio w czasie rzeczywistym;
- integrację z dodatkowymi czujnikami alarmowymi poprzez wejścia I/O;
- działania prewencyjne z wykorzystaniem światła białego;
- zmniejszenie liczby fałszywych alarmów przy zachowaniu dobrej wykrywalności i klasyfikacji;
- identyfikację niechcianych przedmiotów i obiektów;
- integrację z centralnymi platformami monitoringu i systemami zarządzania wizją.

Dzięki kompaktowej budowie i połączeniu wielu technologii w jednym urządzeniu FLIR Saros jest atrakcyjnym – technologicznie i cenowo – rozwiązaniem. To produkt łatwy i szybki w montażu. Jego zastosowanie może przyczynić się do wygenerowania oszczędności już na poziomie instalacji i wdrożenia. FLIR Saros szczególnie dobrze sprawdzi się w ochronie perymetrycznej. Możliwości jego zastosowania są praktycznie nieograniczone.

www.bcscctv.pl

BCS: Kamera BCS-TIP8501IR-Ai z promiennikiem podczerwieni

Kamera tubowa z promiennikiem podczerwieni o zasięgu do 50 m oraz inteligentnymi funkcjami analizy obrazu – najnowsze rozwiązanie w ofercie BCS Line umożliwia efektywniejsze wykorzystanie danych z prezentowanego obrazu. Kamera charakteryzuje się zwartą budową (jak to ma miejsce w przypadku kamer tubowych), zmiennoogniskowy obiektyw o szerokim zakresie ogniskowej od 2,7 do 13,5 mm pozwala zdalnie dopasowywać ogniskową z poziomu zarówno rejestratora, jak i aplikacji mobilnej. Zintegrowany w kamerze promiennik podczerwieni o zasięgu do 50 metrów umożliwia prowadzenie obserwacji przy całkowitym braku światła widzialnego. Dodatkową możliwością ułatwiającą podgląd jest dopasowanie zasięgu promiennika poprzez zmniejszenie lub zwiększenie zasięgu diod IR. Funkcja inteligentnego dopasowania się do sceny pozwoli uniknąć efektu prześwietlenia obiektu pojawiającego się blisko kamery. Przetwornik o rozdzielczości 5 Mpix Star Light daje obraz znakomitej jakości w słabych warunkach oświetleniowych.

Dopełnieniem funkcjonalności kamery jest zaawansowana analiza obrazu „zaszyta" w urządzeniu. Funkcje takie, jak przekroczenie linii czy pojawienie się obiektu w strefie można klasyfikować dla konkretnych obiektów, np. samochody lub ludzie, i dopiero wówczas uzyskiwać alarm. Detekcja twarzy z możliwością określenia wieku, płci oraz włączenia mozaiki na twarzach idealnie sprawdzi się w obiektach handlowych. Każda z funkcji analizy obrazu jest kompatybilna z rejestratorami BCS Line, poszerzając możliwości standardowego systemu telewizji dozorowej. Podłączenie kamer do rejestratorów pozwoli przeszukiwać archiwum poprzez konkretne atrybuty związane np. z kolorem, detekcją konkretnej twarzy czy też wielkością przejeżdżającego samochodu.

Połączenie kamery z promiennikiem podczerwieni, wspierającym funkcje analityczne oraz rejestratorem BCS z serii Ai znacząco zwiększa szybkość dostępu do interesujących nas informacji w archiwum.

Rozwój robotyzacji w polskim przemyśle

Dynamiczny rozwój robotyzacji polski przemysł ma dopiero przed sobą, jednak już dziś wiele firm zdaje sobie sprawę, że bez wdrożenia odpowiednich procesów mogą pozostać daleko w tyle za zachodnimi konkurentami.

Światowa sprzedaż robotów rośnie z roku na rok – wg raportu Międzynarodowej Federacji Robotyki (IFR) w ciągu ostatnich 12 miesięcy rynek powiększył się o 31%. Poziom nasycenia polskiej gospodarki robotami przemysłowymi jest jednak nieznaczny – na 10 tys. pracowników przypadają jedynie 32 roboty. Dla porównania, w Czechach 128, a na Słowacji 135 robotów. Najwięcej inwestują kraje azjatyckie – Chiny, Japonia i Korea Płd. notują największy wzrost zakupu maszyn w stosunku do roku poprzedniego.

Procesy automatyzacji są nieuniknionym etapem rozwoju przedsiębiorstw związanych z sektorem przemysłowym. Większy udział maszyn powinien przede wszystkim oznaczać wsparcie pracowników, a nie tworzenie konkurencji, na co również zwraca uwagę IFR we wspomnianym wyżej raporcie. Najważniejsze zmiany na rynku robotyki i automatyki związane są z wykorzystaniem informacji w procesach przemysłowych w ramach koncepcji przemysłu 4.0 . Wicedyrektor Biura Rozwoju i Innowacji Agencji Rozwoju Przemysłu SA Paweł Pacek zwraca uwagę że roboty i inne urządzenia będą coraz częściej wyposażone w sensory pozwalające zbierać szczegółowe informacje na temat ich pracy. Dzięki zebranym danym oraz algorytmom sztucznej inteligencji możliwe będzie np. przewidzenie awarii urządzenia lub optymalizacja całego procesu produkcji.

Czy roboty mogą przejąć wszystkie zadania wykonywane przez człowieka? Doktor Robert Muszyński z Katedry Cybernetyki i Robotyki Politechniki Wrocławskiej twierdzi, że obecnie nie jest to możliwe: *– Dynamiczny rozwój technologii i algorytmów sterowania sprzyja dostarczaniu na rynek robotów o coraz to nowych funkcjonalnościach. Jednakże nie spodziewałbym się, że w niedalekiej przyszłości roboty przejmą w procesie produkcji wszystkie zadania człowieka. Wciąż największe zapotrzebowanie jest na dostępne od lat tradycyjne roboty przemysłowe, znajdujące zastosowanie na liniach produkcyjnych w takich gałęziach, jak przemysł motoryzacyjny. Biorąc pod uwagę to, że stopień zrobotyzowania polskiego przemysłu jest ciągle dużo mniejszy niż u naszych zachodnich czy nawet południowych sąsiadów, zapewne tu możemy spodziewać się dużego przyrostu „zatrudnienia" robotów, które wykonują jednak przede wszystkim zadania monotonne, uciążliwe, niechętnie wykonywane przez ludzi.*

Zwraca on uwagę również na to, że robotyzacja stwarza nowe możliwości. Na rynku pojawiają się nowej klasy roboty współpracujące, tzw. coboty, które od przemysłowych mają o wiele bardziej zaawansowane układy sterowania. Ich zadaniem jest wspomaganie pracy ludzi, jednak nie są w stanie zastąpić w pełni człowieka. Obecność tego typu robotów to okazja dla małych i średnich przedsiębiorstw, w których maszyny mogą z powodzeniem pełnić swoją funkcję, w przeciwieństwie do robotów przemysłowych wykorzystywanych w dużych koncernach. Na pojawienie się wspieranych przez sztuczną inteligencję robotów mogących konkurować z człowiekiem będziemy musieli poczekać jeszcze wiele lat.

Koncepcja współpracy maszyn i ludzi będzie miała istotny wpływ na kształt rynku pracy. Warto to zjawisko postrzegać jako wyzwanie, które niekoniecznie oznacza całkowite zastąpienie pracowników robotami. Wiele obszarów pozostaje wyłączonych z możliwości zagospodarowania maszynami. Eksperci twierdzą, że trend związany z rynkiem specjalistów nadal będzie rósł. Raport przygotowany przez portal pracuj.pl w I półroczu 2019 r. wskazuje, że pracodawcy kierują swoje oferty w szczególności do specjalistów zajmujących się handlem (29% ofert), obsługą klienta (22%) oraz branżą IT (15%), czyli obszarami nadal niedostępnymi dla robotów. Liczba ogłoszeń kierowanych do pracowników fizycznych wzrosła aż o 43% rok do roku, wśród nich bardzo istotny procent stanowią oferty pracy dla osób wykwalifikowanych, posiadających dodatkowe uprawnienia do obsługi maszyn.

Właściwie wdrożone technologie mogą stanowić wartość dodaną dla przedsiębiorstwa i zwiększać jego konkurencyjność. Dla firm robotyzacja oznacza nie tylko nowe możliwości, ale również wyzwania, na które powinny się przygotować. Z pewnością polski przemysł wiele traci, nie inwestując w technologie w takim stopniu, jak inne kraje europejskie. Czas, by efektywnie rozwijać robotyzację w Polsce, właśnie nadszedł.

Matriał prasowy

Czy grozi nam dyktatura procedur i algorytmów?

Dynamiczne rozpowszechnianie się w przodujących technologicznie krajach urządzeń zinformatyzowanych – w tym robotów i cobotów – w ramach tzw. informatyzacji rzeczy, procedur edukacyjnych i administracyjnych, a nawet technik medycznych, budzi niepokój nie tylko środowisk naukowych.

TEKST
Marek Ryszkowski

Współpracę z robotami można powierzyć tylko odpowiednio wyszkolonym do tego pracownikom. Jak zatem zapewnić akceptowalne bezpieczeństwo współpracy człowieka z robotem na wspólnym stanowisku pracy? Należało skonstruować i wdrożyć do współpracy z człowiekiem robota współpracującego – cobota. Ogólne wskazówki, jak należy to zrobić, sformułował już dawno Isaac Asimov w swoich trzech zasadach robotyki[3], uzupełnionych przez jego następców o jeszcze jedną zasadę.

A oto wskazania bardziej szczegółowe.

1. **Ograniczyć energię ruchów ramion robota** lub przemieszczania się jego korpusu w granicach stanowiska pracy do takiego poziomu, by w kontakcie z ciałem człowieka – gdy zawiodą inne stosowane środki bezpieczeństwa, o których niżej – nie był on w stanie stworzyć poważniejszego zagrożenia zdrowia lub życia człowieka.
2. **Zastosować „zabezpieczające zatrzymanie monitorowane”** (*safetyrated monitored stop*), np. z wykorzystaniem czujek ruchu PIR, które potrafią wykryć osobę zbliżającą się niebez-

Dotychczas nie udało się zapewnić bezwzględnej przewidywalności działania tych urządzeń ich konstruktorom, a przede wszystkim osobom współpracującym z nimi na wspólnych stanowiskach roboczych, ani w innych zastosowaniach, np. w systemach nadzoru działania autonomicznych lub quasi-autonomicznych dronów uzbrojonych o przeznaczeniu militarnym lub policyjnym. Wielu przewiduje, że te ostatnie – na razie w wersji nieuzbrojonej, ale wkrótce uzbrojone – mogą znaleźć się w wyposażeniu SUFO.

Roboty i coboty[1] to – trywializując – wysoce zinformatyzowane maszyny o różnym przeznaczeniu i technicznym skomplikowaniu, składające się (jak każde urządzenie informatyczne) z hardware'u i software'u, czyli z tego, co materialne, i z oprogramowania. W części sprzętowej są one z reguły urządzeniami elektro-, pneumo- lub hydromechanicznymi, obudowanymi różnym oprzyrządowaniem dostosowanym do indywidualnego przeznaczenia każdego z nich. Dla zapewnienia wymaganej niezawodności działania hardware'owego komponentu robotów i cobotów i jego oprzyrządowania podlegają one w okresie swojej eksploatacji doraźnej „alimentacyjnej obsłudze technicznej”, okresowej obsłudze technicznej realizowanej metodą „wg resursu” lub nieregularnej obsłudze technicznej realizowanej w razie potrzeby metodą „wg stanu technicznego”[2]. Wraz z rozwojem technik informatycznych coraz częściej stosowaną metodą obsługiwania technicznego nie tylko robotów i cobotów staje się obecnie metoda „wg stanu technicznego” uzupełniana „obsługami alimentacyjnymi”.

Każdy rodzaj robotów i cobotów wymaga specjalistycznego oprogramowania, bez którego te najbardziej wyrafinowane urządzenia techniczne będą bezużytecznymi przedmiotami (podobnie jak szpadel, motyka czy topór, jeśli nie weźmie ich do ręki człowiek). I obecnie to jakość oprogramowania robotów i cobotów decyduje, czy zapewniają one wymaganą niezawodność, precyzję i szybkość działania, a jednocześnie akceptowalne bezpieczeństwo dla współpracujących z nimi ludzi. To ostatnie dotyczy szczególnie cobotów.

Ułomności oprogramowania są przyczyną incydentów polegających na pojawianiu się zachowania danego urządzenia, którego jego oprogramowanie nie przewidywało i którego pojawieniu się oprogramowanie to powinno przeciwdziałać. Nieprzewidziane zachowanie się urządzenia zinformatyzowanego może być spowodowane także celowym działaniem człowieka (hakerstwo) czy smogiem elektromagnetycznym.

Twój nowy współpracownik – cobot

Dla laików roboty wydają się być nieszkodliwymi, łatwymi do sterowania urządzeniami, które zastępują ludzi przy niebezpiecznych dla nich pracach na liniach produkcyjnych, i nie tylko. Niestety roboty przemysłowe mogą być niebezpieczne również dla człowieka. Opinia ta wynika z doświadczeń wieloletniego ich stosowania. Do niedawna robot przemysłowy – maszyna potężna i „inteligentna inaczej”, pracując obok ludzi, musiał być od nich odizolowany barierami mechanicznymi i/lub elektronicznymi. Mimo to zdarzały się wypadki, także śmiertelne, gdy pracownik nieopatrznie znalazł się w strefie jego pracy, a jakaś czujka bezpieczeństwa nie zadziałała lub robot wykonał czynność, której nie powinien wykonać, bo nie przewidywało tego jego oprogramowanie, gdyż człowiek znalazł się w jego strefie pracy.

> Każdy rodzaj robotów i cobotów wymaga specjalistycznego oprogramowania, bez którego te najbardziej wyrafinowane urządzenia techniczne stają się bezużyteczne, podobnie jak szpadel, motyka czy topór, jeśli nie weźmie ich do ręki człowiek.

[1] Coboty to specjalnego typu roboty, tzw. roboty współpracujące z ludźmi w tej samej strefie roboczej.

[2] Przykładowo samochody są obsługiwane metodą „wg resursu” mierzonego upływem czasu, liczbą przejechanych kilometrów albo wykonaniem określonej liczby cykli pracy, do której zostały zaprojektowane. Bez dokonywania „obsług alimentacyjnych”, czyli uzupełniania paliwa, płynu hamulcowego, płynu do spryskiwania szyb, oleju silnikowego albo płynu niezamarzającego (zimą), daleko takie auto nie zajedzie. W bardziej zaawansowanych technicznie pojazdach komputer pokładowy sygnalizuje kierowcy, już często głosem, ile może jeszcze przejechać kilometrów bez uzupełnienia paliwa, zwraca uwagę na niskie ciśnienie powietrza w konkretnym kole, na zbyt niski poziom oleju lub płynów. Można to już nazwać obsługą pojazdów metodą „wg stanu technicznego”, zwłaszcza gdy komputer sygnalizuje także np. konieczność wymiany klocków hamulcowych, luzy w układzie kierowniczym czy zużycie amortyzatorów w zawieszeniu pojazdu.

[3] M. Ryszkowski: Roboty i coboty w systemach safety i security osób i mienia, „a&s Polska” nr 1/2019.

piecznie blisko do robota i wyłączyć go. Jest to sposób dość łatwy do wdrożenia, może jednak prowadzić do częstych przestojów robota, by zapewnić należyte bezpieczeństwo poruszających się w jego pobliżu osób. Częste przestoje robota na taśmie przemysłowej nie są mile widziane przez menedżerów produkcji.

3. **Zastosować w systemie bezpieczeństwa robota** zestaw czujek ultradźwiękowych (sonarów) i/lub czujek reagujących w podczerwieni (lidarów). Zawęzi to strefę wyłączania robota, która zostanie otoczona strefą jego spowalniania w momencie, gdy człowiek zbliży się do jego strefy roboczej. Zatrzymania i przestoje robota będą wówczas rzadsze niż przy użyciu tylko czujek PIR. Rozwiązanie to określa się jako „monitorowanie prędkości i separacji" (*speed and separation monitoring*). Sprawdza się w wielu zastosowaniach, ale z powodu wirtualnej klatki z nim zintegrowanej przenoszenie robota w inne miejsce wymaga oddzielenia go od stanowiska wraz z wirtualną klatką. Taki zintegrowany system „robot – wirtualna klatka" będzie wymagał ponownego zainstalowania i sprawdzenia poprawności funkcjonowania w nowym miejscu pracy, także w zakresie bezpieczeństwa współpracowników.
4. **Wykonać ruchome elementy robota i jego efektora końcowego** (np. chwytaka) z miękkiego, giętkiego materiału, co zmniejszy skutki zetknięcia się jego elementów z ciałem człowieka. Jednak elastyczne elementy robota nie zapewniają wystarczającej dokładności i precyzyjnej powtarzalności ruchu lub przyczepności niezbędnej do wykonania zadań (wymagających precyzji działania robota np. z dokładnością do 0,1 mm). Należy zatem poszukiwać innych rozwiązań technicznych zapewniających bezpieczeństwo zetknięcia się ciała ludzkiego z ramieniem roboczym lub innym elementem cobota.
5. **Projektować i instalować w robotach oprogramowanie** odporne na nieuprawnione modyfikacje zewnętrzne, smog elektromagnetyczny w przestrzeni otaczającej stanowisko pracy robota, zanieczyszczenia stanowiska pracy robota szkodliwymi płynami i/lub gazami technicznymi albo spalinami, a także na oddziaływania mechaniczne środowiska pracy (wibracje, drgania, hałas itp.).

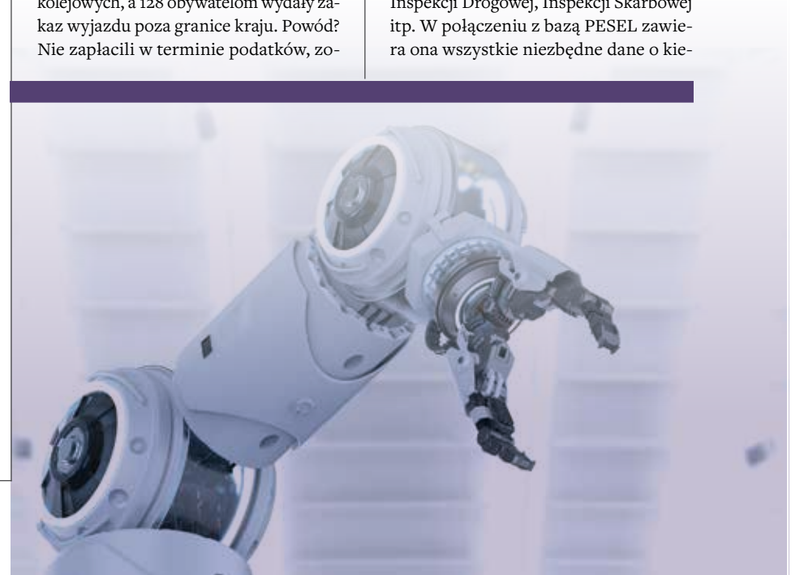
Jakość oprogramowania robotów i cobotów decyduje, czy zapewniają one wymaganą niezawodność, precyzję i szybkość działania, a jednocześnie akceptowalne bezpieczeństwo dla współpracujących z nimi ludzi

Na rynku wytwórców robotów już działają firmy oferujące modernizację wielu typów tradycyjnych robotów do klasy cobotów lub fabrycznie nowe, produkowane przez siebie coboty. Są wśród nich także firmy polskie. Rozpowszechniania się cobotów nie da się już zatrzymać, gdyż w wielu zastosowaniach są one bardziej przydatne od tradycyjnych robotów. Interesujące są możliwości zastosowania cobotów w systemach safety & security, co może wywrzeć istotny wpływ na funkcjonowanie tej branży w Polsce, i nie tylko.

Czy to już rządy, a nawet dyktatura algorytmów i procedur?

Algorytmy/procedury (A/P) już współrządzą w większym lub mniejszym stopniu w wielu krajach, także tych, które cieszą się ustrojem liberalnej demokracji[4]. Sterowane nimi komputery tworzą olbrzymie bazy danych tzw. profili publicznych obywateli, częściej nazywanych także profilami zaufania społecznego. W niektórych krajach, np. w ChRL, to już codzienność. Niedawno władze chińskie ogłosiły, że do końca 2018 r. sądy odmówiły ponad 17 mln obywateli prawa zakupu biletów lotniczych (także na loty wewnątrzkrajowe), ponad 5 mln – prawa zakupu biletów kolejowych, a 128 obywatelom wydały zakaz wyjazdu poza granice kraju. Powód? Nie zapłacili w terminie podatków, zostali więc wpisani do wspomnianej bazy danych jako obywatele niegodni zaufania społecznego. Może wkrótce i ci obywatele polscy, którzy z jakiegoś powodu mają problemy z fiskusem, odejdą „z kwitkiem" od lotniczej, kolejowej lub innej kasy biletowej albo dowiedzą się w banku, że co prawda mają „zdolność kredytową", lecz ze względu na ich „nędzny profil zaufania społecznego" algorytm kredytowy banku odmawia udzielenia im jakiegokolwiek kredytu.

W Polsce od niedawna kierowcy nie mają obowiązku posiadania w prowadzonym przez siebie pojeździe dowodu rejestracyjnego tego pojazdu i własnego prawa jazdy. Przy sobie muszą mieć jedynie dowód osobisty. Dobrze jest mieć także odpowiednią ilość biletów NBP o wysokich nominałach lub kartę bankomatową, najlepiej kredytową, na opłatę ewentualnych mandatów, grzywien lub kosztów holowania pojazdu w razie zdarzenia drogowego, uniemożliwiającego dalszą nim jazdę. Dlaczego taki zaszczyt spotkał kierowców? Bo zbudowano w Polsce olbrzymią bazę danych kierowców i pojazdów, do której zdalny internetowy dostęp mają funkcjonariusze policji drogowej i inni funkcjonariusze publiczni, np. ze Straży Granicznej, Inspekcji Drogowej, Inspekcji Skarbowej itp. W połączeniu z bazą PESEL zawiera ona wszystkie niezbędne dane o kierowcach – obywatelach polskich. Także zapewne o tych, którym sądy odebrały na stałe lub na czas określony prawo jazdy. Czy zatem możemy uważać, że w polskiej administracji publicznej nie tworzy się „profili zaufania społecznego" poszczególnych obywateli?



Algorytmy A/P bywają niedoskonałe, podobnie jak ludzie, którzy je tworzą. Nawet gdyby okazały się doskonałe, niezawodne i nieomylne w działaniu, to mogą działać tylko na podstawie danych, które do ich baz wprowadzą ludzie. A wśród nich zdarzają się i tacy, którzy się mylą, są leniwi albo – z sobie tylko wiadomych powodów – świadomie nie dbają o to, by w bazach danych, np. PESEL-u czy pojazdów i kierowców, znajdowały się tylko dane aktualne, prawdziwe i wprowadzane bądź usuwane niezwłocznie, gdy otrzymają polecenie wykonania którejś z tych czynności. O tym, że tacy ludzie w obsłudze różnych baz danych są, świadczą informacje, że w bazie PESEL znajdowało się – a może jeszcze się znajduje – wiele „martwych dusz", czyli dane osób zmarłych. Skutkowało to pobieraniem przez nieuprawnione do tego osoby bliskie zmarłym ich emerytur. Takie lub inne nieaktualności w bazach danych być może skutkują także błędnymi decyzjami administracyjnym w innych dziedzinach. Zatem czy możemy mieć pewność, że np. w bazie pojazdów odnotowano dane wszystkich skradzionych samochodów albo wszystkich tych, które nie mają aktualnego badania technicznego? Czy w bazie kierowców znajdują się np. dane wszystkich piratów drogowych, którym decyzjami administracyjnymi lub sądowymi odebrano prawa jazdy na stałe czy zatrzymano choćby tylko na czas określony? Nie mam takiej pewności.

Zinformatyzowane systemy podejmowania decyzji administracyjnych dały już o sobie znać w negatywny sposób w Szwecji (odbierając tysiącom osób prawo do należnych im zasiłków dla bezrobotnych), a także w Australii (nakazując zwrot pobranych świadczeń wypłaconych przez tamtejszy ZUS jako nienależnych, podczas gdy należały się jak najbardziej osobom dotkniętym tymi decyzjami). W Polsce zdarzyło się (we Wrocławiu), że zinformatyzowany system kwalifikowania dzieci do żłobków zapisał trzysta dzieci płci obojga, które jednak nie powinny być zapisane, bo ich prawni opiekunowie nie spełniali wszystkich kryteriów. Spowodowało to zapewne niemałe zamieszanie i niepokoje wielu rodziców, którzy ubiegali się o miejsce dla swojego malucha w tamtejszych żłobkach. Coraz więcej danych wskazuje na to, że świat „pełznie" ku rządom wspomaganym przez A/P. Świat, w którym „znaczne obszary życia będą zarządzane przez [...] kody cyfrowe, którym trudno będzie się [...] przeciwstawić i okiełznać je regulacjami (prawnymi – przyp. M.R.)"[5]. A na pewno nie będzie się można do nich dodzwonić, by cokolwiek wyjaśnić.

Jak w niedalekiej przyszłości mogą działać SUFO?

Najpierw nieco o tym, co się działo w styczniu br. na Cosumers Electronics Show w amerykańskim Las Vegas. Otóż w sektorze motoryzacyjnym tej wystawy jedna z firm chińskich prezentowała pierwszy terenowy samochód elektryczny, podobno bogato oprzyrządowany (wariantowo) na potrzeby różnych użytkowników: od myśliwych, poprzez straże leśne, po patrole policyjne i wojskowe. Niewiele wiadomo o wariantach możliwego uzbrojenia tego pojazdu ani o jego prędkości marszowej i zasięgu w jeździe po bezdrożach. Można sobie jednak łatwo wyobrazić, w co może być on wyposażony do użytku przez patrol wojskowy lub SUFO (w ochronie rozległego obszarowo obiektu wojskowego lub obiektu infrastruktury krytycznej).

Najbardziej interesująca na tej wystawie w sektorze motoryzacyjnym była ekspozycja prototypów samochodów latających. Podobno szczególnie oblegane było stoisko jednej z firm koncernu, na którym prezentowano auto ze składanymi skrzydłami. Ten dwumiejscowy pojazd podobno był w stanie w ciągu minuty przestroić się z jazdy na latanie. Jego osiągi w locie: prędkość – 100 km/h, zasięg – 650 km, pułap – ok. 3000 m. Podobny prototyp samochodu jeżdżąco-latającego o zbliżonych parametrach lotu prezentowała na tej wystawie firma japońska. Jeszcze inna firma przedstawiała prototyp drona do przewozu ludzi. Łącznie pokazano kilkanaście prototypów „samochodolotów", niektóre z nich były „pionowzlotami" o zdolności pionowego startu i lądowania. Wszystkie one miały napęd elektryczny; niektóre wyposażono w elektronikę/awionikę, zapewniającą im autonomię poruszania się po drogach publicznych i w przestrzeni powietrznej, z funkcją autonomicznego powrotu po wykonaniu zadania do miejsca startu.

Jak więc w nieodległej przyszłości może wyglądać ochrona fizyczna rozległych obiektów podlegających obowiązkowi ochrony, wyposażonych w systemy kontroli dostępu, wykrywania intruzów i sygnalizowania napadu,

Świat „pełznie" ku rządom wspomaganym przez aplikacje i procedury. Znaczne obszary życia będą zarządzane przez kody cyfrowe, którym trudno będzie się przeciwstawić i okiełznać je regulacjami

[4] J. Winiecki: Rządy algorytmów, „Polityka" nr 11(3203) z 2019 r., str. 42-44.

[5] Patrz przypis 4 – cytowany artykuł w „Polityce" nr 11(3202) z 2019 r., str. 44.

sygnalizowania pożaru oraz dozoru wizyjnego. Wszystkie te systemy zwykle są zintegrowane w obiektowym centrum monitorowania alarmów podłączonym do lokalnego centrum monitorowania alarmów i lokalnego komisariatu policji. Niżej przedstawiono prognozę działania ochrony rozległego obiektu.

1. Po godzinach pracy i w dni wolne od pracy wszystkie ww. systemy są aktywne. W lokalnym CMA dyżurują (w systemie rotacyjnym, np. co 2 godz.) pracownicy ochrony fizycznej.
2. Granice zewnętrzne obiektu (o współczynniku odporności na przekroczenie przez osoby nieuprawnione zależnym od znaczenia obiektu dla obronności lub bezpieczeństwa albo dla lokalnej lub ponadlokalnej infrastruktury, jeżeli zaliczono go do infrastruktury krytycznej) patroluje z powietrza np. dwumiejscowy latający samochód z załogą lub automatyczny bądź dron. Obiekt patrolujący z powietrza przesyła obraz widziany przez zainstalowany na nim zespół kamer dozorowych do obiektowego CMA, gdzie jest on zapisywany i archiwizowany przez co najmniej 30 dób. Obiekt rozległy, np. lotnisko wojskowe lub morski port wojenny, w razie potrzeby powinien być monitorowany z powietrza więcej niż przez jeden z wymienionych środków latających.
3. W chwili pojawienia się jakiegokolwiek sygnału alarmu z jednego z ww. systemów lub od obiektu latającego pracownik obiektowego CMA informuje o tym lokalne CMA i lokalny komisariat policji, przekazując – jeżeli istnieją do tego możliwości techniczne – obraz incydentu powodującego alarm albo werbalnie jego opis.
4. Obiekt latający w trybie ciągłym lub dyskretnym przekazuje obrazy incydentu do obiektowego CMA, jeżeli incydent jest w zasięgu kamer na nim zainstalowanych.
5. Jeżeli rozwój sytuacji staje się niebezpieczny, pracownik lokalnego CMA, na wniosek pracownika obiektowego CMA, wysyła zespół interwencyjny SUFO w celu odparcia próby pokonania granicy ww. obiektu przez osoby nieuprawnione. Zespół ten może poruszać się pojazdem kołowym lub np. dronem osobowym podobnym do tego, którego prototyp prezentowano w Las Vegas. Transport powietrzny zespołu interwencyjnego zapewni szybsze jego przybycie na miejsce incydentu i przystąpienie do działania niż transport kołowy.
6. Jeżeli ww. działania doprowadziły do ujęcia sprawcy incydentu, zostaje on przekazany policji do dyspozycji organów wymiaru sprawiedliwości. Sprawca poszkodowany podczas akcji SUFO jest przekazywany policji po udzieleniu mu pomocy lekarskiej.
7. Ocena ewentualnych szkód w ochranianym obiekcie i ustalenie ich sprawców. Wyniki oceny podlegają przekazaniu organom wymiaru sprawiedliwości.

> Szansą w systemach ochrony osób i mienia jest rozwój nie tylko informatyzacji urządzeń technicznych, lecz także informatycznej techniki 5G, która zapewnia znacznie szybszą od obecnej transmisję danych

To lakoniczny opis możliwego prowadzenia podobnych działań z użyciem nowych zinformatyzowanych generacji sprzętu technicznego, w który mogą być wyposażone zespoły pracowników ochrony fizycznej obiektów i urządzeń podlegających obowiązkowi ochrony. Pominięto „biurokrację i papierologię" działania, z którą muszą się uporać pracownicy CMA oraz kierujący zespołem interwencyjnym SUFO. Wytwarzana dokumentacja może zostać wykorzystana w postępowaniu przed sądem, musi więc spełniać wymagania „dokumentów procesowych".

Niewątpliwą zaletą powietrznego patrolowania granic chronionych obiektów rozległych jest zmniejszenie liczby pracowników ochrony fizycznej, którzy obecnie zapewniają ich ochronę w formie patroli pieszych lub zmotoryzowanych (quady, pojazdy terenowe jedno- i dwuśladowe), a także stałe posterunki, np. na wieżyczkach strażniczych, przy bramach i wejściach na teren obiektu. W omawianym hipotetycznym przypadku wystarczy patrolowanie z powietrza, pod warunkiem że zapewni się całodobową ciągłość patrolowania środkiem/ami lotniczym/ymi, wyposażonym/mi w kamery wideo o zdolności do obserwacji także przy słabym oświetleniu nocnym.

Szansę na taki rozwój sytuacji w systemach ochrony osób i mienia daje rozwój nie tylko informatyzacji urządzeń technicznych, o których była mowa wyżej, lecz także rozwój informatycznej techniki 5G, która zapewnia znacznie szybszą od obecnej transmisję danych między różnymi, zinformatyzowanymi urządzeniami technicznymi. Dotyczy to w naszym przypadku transmisji danych (obrazów lub filmów) z lotniczego środka patrolującego do centrów monitorowania alarmów. Im szybciej i w lepszej rozdzielczości to następuje, tym szybciej zareaguje ochrona obiektu na incydent. Technika 5G ma być wdrożona w Polsce do 2025 r., obecnie jest testowana w Warszawie i Gliwicach. ▫

Marek Ryszkowski

dr inż., ekspert KSOIN, autor licznych artykułów i kilku książek z zakresu prawa ochrony informacji niejawnych, były pełnomocnik ochrony informacji niejawnych w kilku podmiotach prawa handlowego.

Jak zapewnić bezpieczeństwo przemysłowych systemów sterowania

Cyberataki skierowane na przemysłowe systemy sterowania (*Industrial Control System* – ICS) mogą powodować przestoje w procesie produkcji, bezpośrednio wpływając na straty finansowe. Brak kontroli nad zasobami cyfrowymi w branży wytwórczej wprowadza chaos w planie produkcyjnym i znacznie utrudnia wywiązanie się z zobowiązań wobec kontrahentów. Eksperci Cisco opracowali 10 pytań, na które powinna znaleźć odpowiedź każda firma z branży przemysłowej, zanim zdecyduje o wyborze dostawcy systemów cyberbezpieczeństwa.

10 pytań, które powinna sobie zadać każda firma z branży produkcyjnej

TEKST
Artur Czerwiński
dyrektor ds. technologii w Cisco Polska.

1 JAK SKUTECZNIE WYKRYWAĆ ZAGROŻENIA I ZABEZPIECZAĆ SYSTEMY ICS?

Niezwykle ważny jest wybór dostawcy systemów cyberbezpieczeństwa, którego rozwiązania pozwolą na lokalizowanie zagrożeń i wysłanie stosownych alertów dotyczących wszelkich anomalii. Wymaga to ciągłego monitorowania środowiska ICS. Zagrożenie dla infrastruktury cyfrowej mogą stanowić nie tylko celowe działania, ale również błąd ludzki. W przypadku cyberataku analityka śledcza pozwala szybko przywrócić działanie systemu, natomiast stała edukacja użytkowników pomaga eliminować ewentualne popełniane przez nich błędy i uczulać na sytuacje potencjalnie niebezpieczne.

2 JAK WYKORZYSTAĆ WIEDZĘ RYNKOWĄ ORAZ ZAPEWNIĆ ZGODNOŚĆ Z NAJWYŻSZYMI STANDARDAMI ICS?

Branża cyberbezpieczeństwa zmienia się bardzo dynamicznie, dlatego należy śledzić najnowsze raporty i publikacje dotyczące tej tematyki. Istotne jest, aby wybrany system został zaprojektowany zgodnie z najlepszymi praktykami rynkowymi. Powinien zapewniać zgodność z najnowszymi standardami i procedurami oraz zmianami w polityce bezpieczeństwa. Warto również sprawdzić, czy dostawca usług cyberbezpieczeństwa, z którym chcemy podjąć współpracę, jest członkiem International Society for Automation (ISA).

3 JAK ZABEZPIECZYĆ BRZEG SIECI ICS?

Rozwój Przemysłu 4.0 jest nierozerwalnie związany z Internetem Rzeczy oraz wzrostem liczby czujników i urządzeń agregujących dane na różnych etapach łańcucha produkcji. Bezpieczeństwo całego ekosystemu zależy od sprawnego działania każdego jego odcinka. Odpowiedzią na to wyzwanie jest kompleksowy system cyberbezpieczeństwa, obejmujący zarówno urządzenia, czujniki, jak i aplikacje. Należy pamiętać, że poszczególne elementy ekosystemu IT wymagają różnego rodzaju zabezpieczeń.

4 JAK URZĄDZENIA, Z KTÓRYCH KORZYSTASZ, SĄ PRODUKOWANE I WSPIERANE?

Na cyberbezpieczeństwie nie warto oszczędzać. Wybór dostawcy, który oferuje jedynie podstawowe rozwiązania, bez funkcji wsparcia powdrożeniowego może spowodować, że system bezpieczeństwa będzie nieskuteczny, a jego żywotność okaże się bardzo krótka. Warto określić, na jakich elementach cyberbezpieczeństwa nam przede wszystkim zależy i jakich narzędzi potrzebujemy. Zbędne, obciążające sieć funkcje mogą powodować opóźnienia wpływające na spowolnienie pracy całego przedsiębiorstwa.

5 JAK POZIOM BEZPIECZEŃSTWA WPŁYWA NA CYFROWĄ TRANSFORMACJĘ I EFEKTYWNOŚĆ BIZNESU?

Cyfrowa transformacja biznesu wymaga skutecznej strategii, ale przede wszystkim sprawdzonych narzędzi do zarządzania zarówno fizycznym, jak i wirtualnym środowiskiem IT. Firmy z sektora produkcji muszą wdrażać nowoczesne technologie w celu usprawnienia i automatyzacji procesów w całym łańcuchu wartości. Jednym z najważniejszych źródeł wiedzy są dane pochodzące z inteligentnych urządzeń tworzących ekosystem Internetu Rzeczy. Technologia ta może stanowić o przewadze konkurencyjnej, jednak wymaga stałego dostępu do bezpiecznej sieci, a także zaufanego partnera, który będzie wspierał regularne jej monitorowanie i pomoże odpowiednio wcześnie wychwycić niepokojące incydenty.

6 CZY SYSTEM CYBERBEZPIECZEŃSTWA JEST ZINTEGROWANY Z INNYMI URZĄDZENIAMI IT I OT WYKORZYSTYWANYMI W TWOJEJ ORGANIZACJI?

Skuteczny system cyberbezpieczeństwa powinien obejmować całą organizację. „Punktowe", niezintegrowane rozwiązania nie zapewniają odpowiednich informacji, generują dodatkowe koszty i mogą wprowadzać chaos. Należy upewnić się, czy rozwiązanie, które planujemy wdrożyć, jest kompatybilne z urządzeniami, które wykorzystujemy podczas pracy.

7 JAKIEGO RODZAJU INFORMACJE DOTYCZĄCE POŁĄCZENIA SIECIOWEGO Z SYSTEMAMI ICS MOŻESZ UZYSKAĆ?

Pełen wgląd w każdy element sieci pozwala zabezpieczyć organizację przed zagrożeniami, które przeniknęły przez pierwsze warstwy bezpieczeństwa. System cyberbezpieczeństwa powinien określić, jakie maszyny produkcyjne i urządzenia sieciowe znajdują się w poszczególnych strefach, aby móc oszacować ryzyko wystąpienia cyberataku. Organizacja musi posiadać wiedzę na temat tego, jakimi informacjami wymieniają się poszczególne urządzenia podłączone do sieci, aby móc wykryć aktywność wskazującą na działalność cyberprzestępców, błąd ludzki lub usterkę.

8 CZY MOŻESZ OPISAĆ PEŁEN ZAKRES CYBERBEZPIECZEŃSTWA POŁĄCZEŃ IT I OT, KTÓRY ZAPEWNIA WYKORZYSTYWANE PRZEZ CIEBIE ROZWIĄZANIE?

Technologie informatyczne (IT) i operacyjne (OT) mają z założenia różne zastosowanie. Dział IT odpowiada za bezpieczeństwo danych, podczas gdy dział OT korzysta z systemów komputerowych do fizycznego sterowania produkcją. Zapewnienie wysokiego poziomu cyberbezpieczeństwa wymaga nie tylko ścisłej współpracy między zespołami korzystającymi z obu technologii, ale także systemów dostosowanych do pracy w obu środowiskach. Warto zwrócić uwagę, czy rozwiązanie, które planujemy wdrożyć, pozwala zapewnić zgodność z międzynarodowym standardem bezpieczeństwa przemysłowych systemów sterowania IEC-62443/ISA99.

9 JAKIE SPOSOBY IDENTYFIKACJI I UWIERZYTELNIANIA DOSTĘPU DO SIECI FUNKCJONUJĄ W TWOJEJ ORGANIZACJI?

Wdrożenie polityki i protokołów bezpieczeństwa sprawia, że organizacja może uniemożliwić niepożądanym osobom uzyskanie dostępu do sieci, nie wpływając jednocześnie na bieżące procesy. Skuteczne systemy cyberbezpieczeństwa pozwalają na przeprowadzenie uwierzytelnienia na podstawie analizy tożsamości, danych lokalizacyjnych czy historii dostępów. Administrator może ponadto ustanawiać reguły dostępowe dla poszczególnych elementów sieci.

10 SKĄD MOŻESZ MIEĆ PEWNOŚĆ, ŻE WYKORZYSTYWANE PRZEZ CIEBIE SYSTEMY BEZPIECZEŃSTWA ZINTEGRUJĄ SIĘ Z ARCHITEKTURĄ SIECI?

Wdrożenie systemu bezpieczeństwa to proces, który wymaga wsparcia dostawcy rozwiązania. Niezbędne jest określenie potrzeb danej organizacji i sporządzenie kompleksowej dokumentacji opisującej architekturę sieci. Należy ustalić sposób, w jaki będzie mierzony poziom cyberbezpieczeństwa. System powinien przejść odpowiednie testy, aby upewnić się, czy jest w stanie lokalizować zagrożenia. Warto korzystać z usług dostawców, którzy specjalizują się w rozwiązaniach z zakresu bezpieczeństwa sieci.

Cisco Systems Poland
Ul. Domaniewska 39B
02-672 Warszawa
www.cisco.com

Bezpieczeństwo w farmacji

Jak zapewnić tej branży ochronę?

TEKST
Prasanth Aby Thomas

BRANŻA ZABEZPIECZEŃ CZĘSTO ŁĄCZY SEKTOR FARMACEUTYCZNY Z OCHRONĄ ZDROWIA. MA TO UZASADNIENIE ZE WZGLĘDU NA CECHY WSPÓLNE OBU TYCH SEKTORÓW, JEDNAK FARMACEUTYCZNY SAM W SOBIE JEST NA TYLE SZCZEGÓLNY, ŻE WARTO MU POŚWIĘCIĆ SPECJALNĄ UWAGĘ.

W związku z oczekiwanym szybkim rozwojem sektora farmaceutycznego, ale też z coraz większymi obawami dotyczącymi bezpieczeństwa, można się spodziewać, że popyt na rozwiązania ochrony w tym segmencie będzie nadal rósł. Wraz z postępem technologii i stosowaniem urządzeń podłączonych do Internetu problemem staje się również cyberbezpieczeństwo. W artykule przyjrzymy się głównym zagrożeniom w sektorze farmaceutycznym, rozwiązaniom będącym na nie odpowiedzią i przykładom ich wdrożenia.

Wzrost i trendy w bezpieczeństwie sektora farmaceutycznego

Można zakładać, że USA będzie najszybciej rosnącym rynkiem branży farmaceutycznej, drugie miejsce z pewnością przypadnie Chinom. Pojawią się nowe segmenty stymulujące popyt.

Sektorowi ochrony zdrowia branża zabezpieczeń poświęca zwykle dużą uwagę ze względu na jego specyficzne wymagania. Rzadziej natomiast mówi się o potrzebach ściśle z nim powiązanego i równie ważnego sektora farmaceutycznego. Według analityków z The Business Research Company globalny rynek farmaceutyczny będzie w latach 2017-2021 rósł w tempie niemal 6 proc. rocznie. Spodziewając się takich wzrostów i odnosząc się do rynku amerykańskiego, Paul Baratta, dyrektor Axis Communications odpowiadający za rozwój biznesu w ochronie zdrowia w USA, uważa, że ta branża rozwija się głównie dzięki przejęciom i wykupom.

Czynniki wzrostu

Według P. Baratta jednym z głównych problemów związanych z rywalizacją w sektorze biofarmaceutycznym jest ochrona personelu, produktów i informacji. W ostatnim roku kilka przejętych mniejszych firm farmaceutycznych znalazło się pod parasolem ochronnym dużych podmiotów biofarmaceutycznych. Większe korporacje zainicjowały programy restrukturyzacyjne związane z presją na ograniczenie dystrybucji opioidów, przyczyniając się do zmiany ukierunkowania z produktów na badania i rozwój. Zmiana ta spowodowała zwiększenie finansowania badań klinicznych, skupienie się na rozwoju oraz poprawę ochrony przed szpiegostwem informatycznym i przemysłowym.
Ograniczanie liczby pracowników, konsolidacja, rozwój badań, a także zwiększanie poziomu bezpieczeństwa cyfrowego i ochrony przed szpiegostwem przemysłowym w dużej mierze wymusiły trwającą obecnie modernizację zarówno systemów kontroli dostępu, jak i rozwiązań wizyjnych, w tym systemów VMS, kamer i systemów audio.
Tendencja do ograniczenia personelu i większego wykorzystania technologii utrzyma się przez kilka najbliższych lat, w miarę postępu konsolidacji przedsiębiorstw. Konsolidowane są także zakłady produkcyjne, a centra dystrybucyjne powstają bliżej klientów. Rośnie też znaczenie tajemnicy przemysłowej, które mają prowadzić do uzyskania przewagi na rynku.

Zmiany stymulujące rozwój

Eric Green, menedżer ds. marketingu produktów w Honeywell, uważa, że w nadchodzących latach wraz z kontynuacją wzrostu na rynku farmaceutycznym można się spodziewać coraz ostrzejszych regulacji prawnych. Dostawców usług i integratorów systemów zabezpieczeń bardziej od wymienionych trendów być może zainteresują nowe segmenty w branży farmaceutycznej. Według Jeffa Whitneya, wiceprezesa ds. marketingu w Arecont Vision Costar, w efekcie legalizacji marihuany w wielu stanach i prowincjach w różnych częściach USA i Kanady pojawił się ważny nowy segment rynku w tej branży. Działalność rozpoczyna wiele firm, chcąc wykorzystać farmaceutyczny boom. Stwarza to nowe możliwości dla branży zabezpieczeń w obszarach produkcji, dostaw, sprzedaży, kanału dystrybucyjnego i detalicznego w biznesie farmaceutycznym. W całym jej zakresie – od zabezpieczeń mechanicznych, przez systemy dozoru wizyjnego i kontroli dostępu, aż po ochronę informatyczną (cyberbezpieczeństwo).

Trendy rynkowe w USA i innych krajach

Według firmy badawczej IQVIA Stany Zjednoczone są obecnie najszybciej rozwijającym się rynkiem farmaceutycznym, na którym w najbliższych latach można się spodziewać średnich rocznych wzrostów na poziomie 4-5 proc. Chiny plasują się tuż za USA, ze średnią roczną stopą wzrostu wynoszącą 3-6 proc. Obecnie w Stanach Zjednoczonych wznowiono debatę nt. polityki cenowej i refundacji w planach ubezpieczeniowych. O ile zmiany w polityce ubezpieczeniowej mogą nie mieć wpływu na sektor jako taki, o tyle każda zmiana cen może ograniczyć marże dla producentów, co z kolei zaszkodziłoby ich budżetom i wpłynęło na plany inwestowania w rozwiązania security.

Zagrożenia i problemy, przed którymi stoi sektor farmaceutyczny

Dla integratorów systemów zrozumienie istoty zagrożeń ma kluczowe znaczenie w dostarczaniu rozwiązań wysokiej jakości.

Ze względu na swój charakter cała branża ochrony zdrowia wymaga szczególnej uwagi. Według Erica Greena z firmy Honeywell przemysł farmaceutyczny stoi w obli-

czu wyzwań związanych z jednej strony z ochroną własności intelektualnej i reputacji marki, z drugiej – z koniecznością spełnienia surowych wymagań zgodności z przepisami. Niespełnienie któregokolwiek z nich może kosztować miliony.

Kradzież produktów i własności intelektualnej

Receptury, same leki i ich składniki są drogie, więc podatne na kradzież. Aby zapobiec problemom takim jak podrabianie leków oraz stratom finansowym, niezbędna jest ochrona ich receptury. Ponadto jeśli nie są przechowywane prawidłowo, np. wystawiane na temperaturę przekraczającą dopuszczalny zakres nawet przez krótki okres, mogą zagrażać życiu pacjentów. Jeśli firma farmaceutyczna nie jest w stanie wykazać zgodności z przepisami lub są one przez nią naruszane, to może nawet zostać zamknięta, tracąc potencjalnie miliony dolarów, swoją reputację i szansę na przyszły biznes.

Ochrona i zapobieganie szkodom

Rick Tampier, dyrektor ds. sprzedaży i strategii produktowej w firmie Red Hawk Fire & Security w ADT Commercial, zauważa, że zarządzający zakładami i laboratoriami farmaceutycznymi mają również do pokonania wyzwania dotyczące zapobiegania i ograniczania szkód i przestojów oraz ryzyka utraty życia i mienia. Każdy obiekt wymaga oceny zagrożeń w celu zidentyfikowania ryzyka i zastosowania odpowiednich zabezpieczeń. Te ostatnie mogą obejmować sieciowy system wykrywania pożaru, wyzwalający alarm w przypadku wykrycia ognia, tlenku węgla, dymu czy ciepła, a także wysokiej czułości detektory innych zagrożeń.

Cyberbezpieczeństwo

Żadna branża nie jest obecnie odporna na zagrożenia informatyczne. Biorąc pod uwagę dużą wartość własności intelektualnej, zapewnienie solidnej ochrony danych staje się dziś koniecznością. Firmy farmaceutyczne często przeprowadzają audyt z analizą ryzyka, obejmujący m.in. przegląd incydentów z przeszłości, w których doszło do naruszenia bezpieczeństwa. Mogą następnie skoncentrować się na identyfikowaniu i eliminowaniu punktów najbardziej narażonych na nielegalny dostęp, złośliwe działanie, modyfikację lub usuwanie danych. Mogą usprawnić kontrolę dostępu do systemów i danych oraz wdrażać najlepsze praktyki w zakresie cyberbezpieczeństwa, nadążające za ewolucją standardów branżowych.

Wymogi wynikające z przepisów

Firmy farmaceutyczne stoją w obliczu wielu zagrożeń – od włamań, przez rabunki czy kradzieże wewnętrzne i zewnętrzne, kończąc na niszczeniu i zanieczyszczaniu produktów. Farmacja to ściśle regulowana branża, szczególnie na rynkach rozwiniętych, takich jak USA, gdzie firmy muszą przestrzegać wielu przepisów stanowych i federalnych, w tym regulacji HIPAA, zgodności z wytycznymi Agencji Żywności i Leków (FDA) oraz specyfikacjami State Board of Pharmacy.
Wiele z tych regulacji wymaga przejścia rygorystycznych ścieżek audytu, potwierdzających zgodność z przepisami, przykładowo takimi, jak wymóg obecności farmaceuty w sytuacji, gdy inni pracownicy mają wejść na określony obszar o ograniczonym dostępie.
W USA Agencja FDA wdrożyła listę wymogów 21 CFR Part 1, narzucając kontrolę wszystkich etapów procesu, w tym walidacje systemów i elektroniczne ścieżki audytu. Podobne przepisy mają inne kraje – mówi J. Whitney z Arecont Vision Costar. Europejska Agencja Leków (EMA) określa normy produkcyjne dla krajów w UE, koordynując działania kontrolne w celu weryfikacji zgodności z normami.

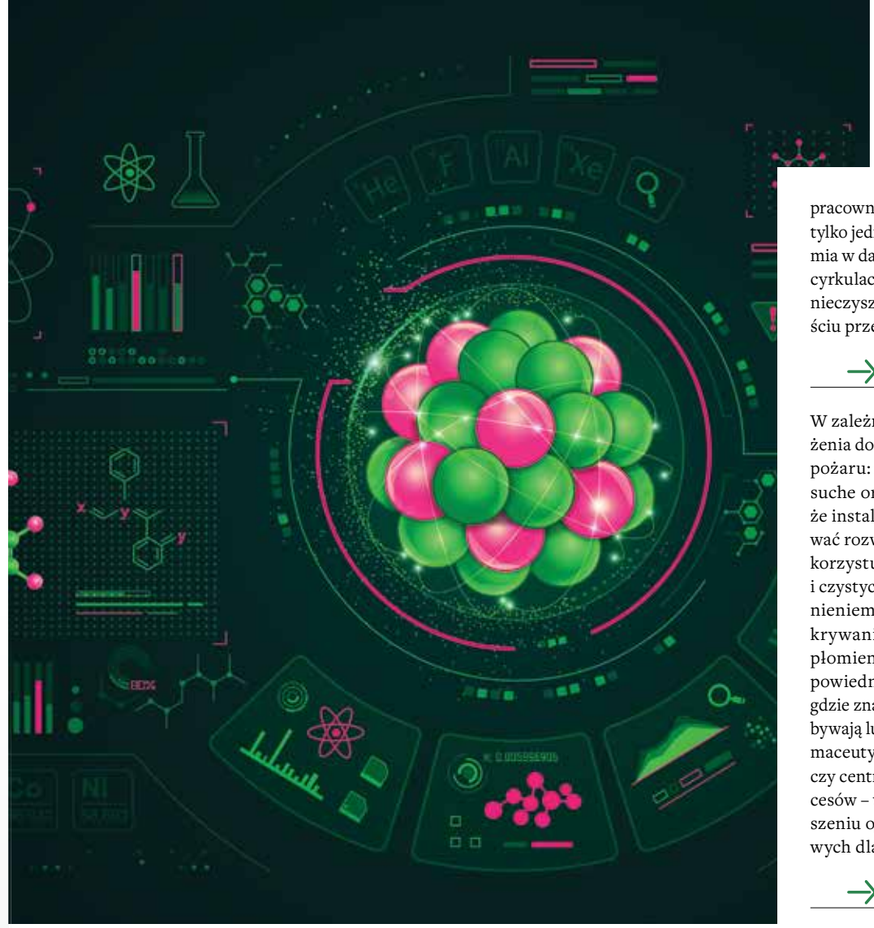
Rozwiązania w zakresie bezpieczeństwa w branży farmaceutycznej

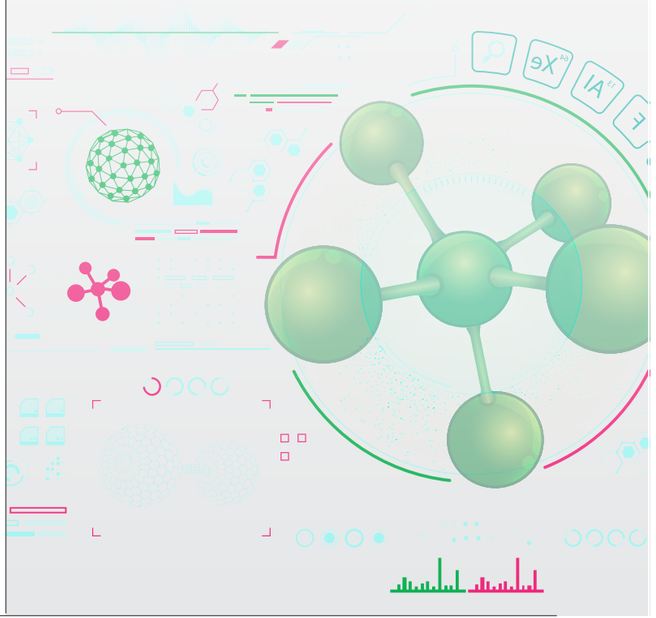
Integracja jest kluczem do zapewnienia kompleksowego zarządzania bezpieczeństwem w tej branży.

W zależności od charakteru produktów i stosowanych procesów firmy farmaceutyczne mogą potrzebować różnych rozwiązań bezpieczeństwa. Przedstawiamy poniżej te elementy, które w ujęciu wysokopoziomowym należy uznać za część zintegrowanego rozwiązania w zakresie systemów zabezpieczeń elektronicznych, przeciwpożarowych i ochrony życia.

Zintegrowane rozwiązania KD i CCTV

Najważniejszym elementem jest elektroniczna kontrola dostępu zintegrowana z wykrywaniem włamań i opartymi na protokole IP rozwiązaniami dozoru wizyjnego umożliwiającymi zdalny podgląd sytuacji. Według Ricka Tampiera z ADT Commercial skuteczne połączenie tych trzech systemów pozwala firmom na opracowanie podwójnego systemu uwierzytelnienia. Wymaga on przedstawienia ważnej karty dostępu i wprowadzenia kodu w celu uzbrojenia lub rozbrojenia systemu antywłamaniowego. Gdy dojdzie do naruszenia bezpieczeństwa, system dozoru wizyjnego oparty na protokole IP umożliwi zdalne zweryfikowanie sytuacji. System kontroli dostępu może również wysłać sygnał alarmu np. w sytuacji, gdy drzwi są forsowane lub uniemożliwiają zamknięcie.





Monitorowanie warunków krytycznych

To również bardzo istotna funkcja – ze względu na to, że nawet najmniejsze odchylenia temperatury niekorzystnie wpływają na leki lub ich składniki. Zapasy leków są warte miliony dolarów, więc w razie problemów straty dla firmy mogą być bardzo poważne. Dlatego zastosowane rozwiązania powinny wykraczać poza zwykły alarm. Rick Tampier daje przykład rozwiązań zaprojektowanych tak, by nie tylko rejestrowały alarmy, gdy temperatura szafek na leki lub sejfów przekracza dopuszczalny zakres, ale także monitorowały stan drzwi, zasilanie czy każdy możliwy wyciek czynnika chłodniczego.

Rozwiązania wymiany powietrza

Amerykańska Agencja Żywności i Leków (FDA) wymaga w pewnych przypadkach, by systemy spełniały wymagania dotyczące wewnętrznej wymiany powietrza. W takich sytuacjach sprawdzają się śluzy powietrzne – rozwiązanie wykorzystujące ciąg drzwi prowadzących do „czystego pomieszczenia" (*clean room*). Konstrukcja opiera się na blokadzie czasowej, w wyniku której pracownicy mogą otworzyć jednocześnie tylko jedne drzwi, a każde wejście uruchamia w danym obszarze wentylator w celu cyrkulacji i oczyszczenia powietrza z zanieczyszczeń. Tak dzieje się przy przejściu przez dwoje lub troje drzwi.

Rozwiązania przeciwpożarowe

W zależności od charakterystyki wdrożenia dostępne są różne opcje tłumienia pożaru: instalacje tryskaczowe mokre, suche oraz wstępnie sterowane, a także instalacje zalewowe. Można zastosować rozwiązania gazowe, pianowe i wykorzystujące mgłę, oparte na wodnych i czystych środkach gaśniczych. Uzupełnieniem będą systemy wczesnego wykrywaniem dymu i optycznej detekcji płomienia. Czyste środki ppoż. są odpowiednie do stosowania w obszarach, gdzie znajduje się wrażliwy sprzęt i przebywają ludzie, a więc w laboratoriach farmaceutycznych, salach komputerowych czy centrach monitoringu i kontroli procesów – wyglądają jak woda, ale przy gaszeniu ognia nie powodują szkód typowych dla wody.

Systemy ostrzegawcze

Systemy ostrzegania i ewakuacji mają alarmować osoby przebywające w budynkach w sytuacjach zagrożeń (klęski żywiołowe, pożary, wypadki czy akty przemocy). Dźwiękowe systemy ostrzegania natychmiast informują duże grupy ludzi, przyspieszając reagowanie na zaistniałe zagrożenie i potencjalnie ratując życie.

Rozwiązania dla aptek

Apteki wymagają wielu takich samych rozwiązań – systemów ppoż., ochrony życia i zabezpieczeń – jakie zabezpieczają oddziały banków. Będą to m.in. systemy sygnalizacji włamania z czujkami magnetycznymi (kontaktrony) i czujkami ruchu, z przewodowymi lub bezprzewodowymi przyciskami napadowymi; kamery IP zainstalowane wewnątrz i na zewnątrz obiektu; kuloodporne okna, podajniki szufladowe, systemy dojazdowe do obsługi pojazdów z dwustronną komunikacją audio-wideo.

Rozwiązania dla sejfów (vaults) i centrów dystrybucji

Ochrona pomieszczeń sejfów farmaceutycznych i centrów dystrybucji to złożony problem. Obszarom tym należy zapewnić najwyższy poziom bezpieczeństwa, bowiem często są w nich przechowywane zapasy o wartości wielu milionów dolarów oraz leki eksperymentalne. Zdaniem

Paula Baratty z Axis Communications USA system zabezpieczeń powinien zaczynać się od ochrony obwodowej (perymetrycznej) – już na granicy strefy peryferyjnej, co ma ogromne znaczenie dla jego skuteczności. Wysokie ogrodzenia z kablami sensorycznymi/czujkami ogrodzeniowymi, zakopywane czujki uniemożliwiające podkop, a także kamery termowizyjnymi i klasyczne, głośniki oraz radary to standardowe zabezpieczenia stosowane w ochronie perymetrycznej. Wykorzystuje się także system kontroli dostępu rejestrujący, kto i kiedy wchodzi do obiektu i z niego wychodzi. Współpracujące z nim kamery CCTV przy wejściach i bramach umożliwiają identyfikację osób i pojazdów. Standardem powinno być wykorzystanie algorytmów analizy wizyjnej np. do wykrywania osób kręcących się w pobliżu linii ogrodzenia lub wspinających się po barierach z zamiarem przedostania się na teren obiektu.
Wewnątrz pomieszczenia sejfowego i magazynu należy zainstalować systemy alarmowe przeciwwłamaniowe i zapewnić szerokie pokrycie kamerami CCTV, rejestrującymi ruch produktów. System można skonfigurować tak, by uruchamiał alarm powiadamiający personel ochrony lub (w razie potrzeby) także uzbrojone służby policyjne.

Cyberzagrożenia rosną, gdy IT łączy się z OT

Szczególnie wrażliwy charakter danych sprawia, że przemysł farmaceutyczny staje się celem cyberataków, które mają wpływ na ocenę ryzyka, zaufanie akcjonariuszy i aktywność operacyjną firmy.

Działy zajmujące się technologiami informatycznymi (IT) oraz technologiami operacyjnymi (OT) miały dotąd osobne doświadczenia dotyczące przestrzegania przepisów ustawowych, wykonawczych, standardów branżowych i wytycznych. Obszarem zainteresowania OT było w dużej mierze bezpieczeństwo fizyczne na wszystkich etapach produkcji, testowania, rozwoju, magazynowania i spedycji. Z kolei IT tradycyjnie koncentrowało się na ochronie sieci, systemów informatycznych i danych. Obecnie ten podział się zaciera. Urządzenia przemysłowe coraz częściej podłączane do Internetu Rzeczy (IoT) korzystają z infrastruktury sieciowej równolegle lub razem z systemami informatycznymi. IoT przynosi ogromne korzyści dla produkcji, ale bez wdrożenia nowych poziomów ochrony wprowadza także potencjalne ryzyko cyberataków – w postaci szpiegostwa handlowego, złośliwego modyfikowania procesów, terroryzmu, działań aktywistów politycznych oraz kradzieży danych i samych produktów.
Organizacje z branży farmaceutycznej, tak jak i innych sektorów produkcji wymagają obecnie audytów bezpieczeństwa i oceny ryzyka w całym łańcuchu dostaw, procesie produkcyjnym oraz fazie przechowywania produktu i jego wysyłki. Muszą być nimi objęci także partnerzy i dostawcy, a sytuacja będzie ewoluować wraz z wprowadzaniem nowych standardów bezpieczeństwa, najlepszych praktyk i różnych regulacji na całym świecie.

Bardzo popularny cel

Paul Baratta z Axis Communications USA twierdzi, powołując się na badanie Deloitte, że przemysł farmaceutyczny jest jednym z głównych celów cyberprzestępców na całym świecie. Do prób ataków na sektor biofarmaceutyczny dochodzi codziennie, straty własności intelektualnej w tej branży wynoszą miliony dolarów. Szkolenia i zwiększanie świadomości pracowników w zakresie potencjalnych zagrożeń to najlepsza i najbardziej oczywista obrona. Przykładowo, jeśli nie rozpoznajemy nadawcy wiadomości e-mail, nie otwierajmy jej ani nie pobierajmy załącznika! Jeśli znajdziemy gdzieś nieznane nośniki pamięci (np. pendrive), nigdy nie podłączajmy ich do komputerów należących do firmy. Zapory sieciowe oraz oprogramowanie antywirusowe to jedynie minimum w ochronie przed złośliwymi działaniami cyberprzestępców.

Jakie są priorytety

Wypowiadając się w podobnym tonie, Eric Green z Honeywella zauważa, że gdy chodzi o ochronę integralności danych i zasobów, często większą uwagę zwraca się na IT. Jego zadaniem takie podejście może okazać się kosztowne. Obszar OT, czyli systemy monitorujące, sterujące i zabezpieczające procesy, sprzęt i obszar operacyjny wymagają podobnej lub nawet większej ochrony w dzisiejszym sieciowym środowisku technologicznym. Jako dostawca zabezpieczeń fizycznych Honeywell jest zobowiązany do zapewnienia funkcjonalności i narzędzi zwiększających cyberochronę i bezpieczną integrację produktów ze środowiskami klientów.

Ochrona informacji firmowych

Zabezpieczenie danych – które, dostając się w niewłaściwe ręce, mogłyby zaszkodzić organizacji – jest priorytetem dla większości firm farmaceutycznych. Skuteczna ochrona (przed włamaniami, wykorzystaniem „tylnych drzwi" czy nawet funkcji serwisowych stworzonych przez producentów, a które mogą umożliwiać obcym uzyskanie dostępu do infrastruktury IT) polega na ocenie ryzyka i podejmowaniu działań zmierzających do jego ograniczenia. Wśród niezbędnych do wykonania kroków można wskazać ochronę wszystkich urządzeń (także sieciowych urządzeń zabezpieczających) przy użyciu haseł.
Konieczne jest, by w zarządzaniu bezpieczeństwem i podatnościami korzystać z silnych haseł i zapór sieciowych. Dużą uwagę należy też poświęcać testom oraz szkoleniu użytkowników i pracowników.

Wykorzystanie rozwiązań BI w sektorze farmaceutycznym

WRAZ Z POSTĘPEM TECHNOLOGICZNYM W WIELU BRANŻACH ROŚNIE GWAŁTOWNIE LICZBA GENEROWANYCH DANYCH. CORAZ CZĘŚCIEJ TEŻ INFORMACJA STAJE SIĘ BEZCENNA. ROZWIĄZANIA ANALITYKI BIZNESOWEJ – *BUSINESS INTELLIGENCE* (BI) TWORZĄ DOSKONAŁĄ OKAZJĘ DO WYKORZYSTANIA GROMADZONYCH DANYCH. KORZYSTAJĄC Z BI, FIRMY MOGĄ POPRAWIĆ SWOJĄ WYDAJNOŚĆ I ROZWIJAĆ BIZNES.

T E K S T
Prasanth Aby Thomas

Jest kilka powodów, dla których firmy farmaceutyczne powinny sięgać po rozwiązania *Business Intelligence*. Najważniejszymi są zachowanie zgodności z przepisami i zapewnienie jakości, w dalszej kolejności usprawnienie sprzedaży oraz opracowanie skuteczniejszych strategii marketingowych. W naszym artykule przyjrzymy się największym wyzwaniom, przed którymi stoją firmy farmaceutyczne, oraz sposobom wdrażania rozwiązań BI w celu przezwyciężenia tych problemów.
Przedstawimy także studium przypadku, w którym firma farmaceutyczna, korzystając z analityki biznesowej, zadbała o spełnienie określonych wymogów.

Największe wyzwania dla sektora farmaceutycznego

Wraz ze wzrostem popularności gadżetów medycznych rośnie zaangażowanie pacjentów w proces leczenia.

Pomimo obaw o tempo wzrostu sektor farmaceutyczny stale się rozwija. Według raportu ProClinical ceny leków są najwyższe w historii, a produktywność badań wzrosła po spadku sprzed dwóch lat. Farmaceutyki biopodobne i postęp technologiczny tworzą wiele nowych możliwości dla tego sektora. Wciąż jednak istnieją wyzwania, z którymi firmy farmaceutyczne muszą się mierzyć. Jedne pro-

blemy wynikają bezpośrednio z postępu technologicznego, inne tworzy sytuacja na rynku. Przedstawiamy przegląd największych przeszkód, jakie ma do pokonania ta branża.

Ochrona zdrowia inicjowana przez pacjenta

Dzięki coraz większej wydajności i popularności urządzeń medycznych klasy konsumenckiej, takich jak gadżety do noszenia (różnego typu *wearables*), pacjenci mogą lepiej kontrolować swój stan zdrowia. Sprawiło to, że odgrywają coraz bardziej aktywną rolę w swoim leczeniu. Dla sektora farmaceutycznego oznacza to zarówno wyzwania, jak i nowe możliwości. Zgodnie z raportem ProClinical najważniejszym zadaniem w 2019 r. będzie określenie sposobu wykorzystania potencjału technologii medycznych i zmiana priorytetu – z partnerstwa ze środowiskiem medycznym na partnerstwo bezpośrednio z konsumentem. Według analityków w 2019 r. i latach następnych to konsument może stać się najbardziej strategicznym partnerem firmy farmaceutycznej. W kontaktach z konsumentem firma farmaceutyczna może mieć przewagę w uzasadnianiu wysokości cen i przekazywaniu wartości. Za sprawą reklam farmaceutycznych nastąpił zwrot w kierunku konsumpcjonizmu. Można spodziewać się, że tendencja ta będzie narastać, ponieważ firmy farmaceutyczne mają większe możliwości dotarcia do konsumenta za pomocą urządzeń do noszenia i podobnych rozwiązań.

Produkty biopodobne i ich przyszłość

Zdaniem analityków z Infinity Research, chociaż oferowane w przystępnej cenie leki biopodobne mogą pomóc pacjentom, duże firmy farmaceutyczne są im przeciwne, gdyż ogranicza to ich zarobki. ProClinical sugeruje, że produkty biopodobne będą w ciągu najbliższych pięciu lat stanowić ponad 20 proc. rynku. Wciąż jednak to leki małocząsteczkowe będą miały większy udział w rynku, ponieważ rozwój produktów biopodobnych jest na wielu rynkach ograniczony sporami patentowymi.

Rynkowe i polityczne obawy

Przewiduje się, że w nadchodzących latach wzrosty na niektórych głównych rynkach zwolnią. W Stanach Zjednoczonych np. do 2021 r. wzrost będzie jednocyfrowy, co w porównaniu z 12 procentami w 2015 r. (dane z raportu QuintilesIMS) oznacza spadek.
Globalna konsumpcja leków ma do 2021 r. zwiększyć się tylko o 3 proc., co nie koresponduje z oczekiwanym wzrostem liczby ludności i zmianami demograficznymi. Głównym tego powodem są wysokie ceny leków, trudności w dostępie do nich na rynkach wschodzących oraz przewaga leków generycznych. Dochodzi do tego niepewność natury politycznej, m.in. brexit, który jest poważnym powodem do niepokoju. Zaobserwowano, że firmy farmaceutyczne z siedzibą w Unii Europejskiej, które zależą od Wielkiej Brytanii, gromadzą zapasy leków. Rosną obawy dotyczące badań partii produktów, dostępności narządów i krwi oraz zmian w przepisach, które mogą ograniczyć lub spowolnić dostawy leków do Wielkiej Brytanii po brexicie.

Jaką rolę mogą odgrywać rozwiązania BI w sektorze farmaceutycznym

Kluczowe znaczenie ma monitorowanie danych. Jednak to nie jedyne zastosowanie analityki biznesowej, czyli Business Intelligence.

W czasach, gdy firmy stale udoskonalają swoje strategie w celu uzyskania przewagi konkurencyjnej, rozwiązania *Business Intelligence* stają się coraz bardziej popularne w wielu branżach. W sektorze farmaceutycznym mają one przede wszystkim pomóc w pokonaniu dwóch wyzwań. Jednym z nich są badania i rozwój nowych leków, a drugim osiągnięcie przełomu, zanim dokona tego konkurencja.
Dane analityków z Research and Markets wskazują, że globalny rynek BI w ochronie zdrowia był wart 3,8 mld USD w 2017 r. Szacuje się, że do 2026 r. sięgnie on 15,9 mld USD, przy średniej rocznej stopie wzrostu wynoszącej 17,4 proc. Ograniczanie kosztów oraz podejmowanie decyzji medycznych oparte na danych to tylko niektóre czynniki stojące za szybkim rozwojem tego rynku.
Według ChristianSteven, firmy dostarczającej rozwiązania BI dla sektora farmaceutycznego, istnieją cztery obszary, w których technologia jest wykorzystywana w tej branży. W niedawno opublikowanym w Internecie dokumencie firma zdefiniowała te obszary i ich znaczenie dla producentów.

Cele operacyjne

Istotne dla działalności biznesowej firmy jest monitorowanie ogromnej liczby danych generowanych w jej rozległej sieci. Dane te powinny być przekształcone w przydatne informacje, które można wykorzystać w celu usprawnienia biznesu. Źródła informacji, które należy śledzić w ten sposób, obejmują również łańcuch dostaw, poziom produkcji oraz cechy produktu. Oprócz tego, chcąc zapewnić efektywne wykorzystanie zasobów, należy monitorować koszty, produktywność pracowników, wydajność operacyjną itp.
ChristianSteven zauważa, że ze względu na coraz większe wyzwania w sektorze farmaceutycznym firmy z tej branży muszą wyprzedzać konkurencję. *Business Intelligence* zapewnia firmom farmaceutycznym szczegółowe raporty analityczne, graficzne kokpity menedżerskie i nieograniczony dostęp użytkownika. Dzięki integracji wszystkich informacji z wielu źródeł mogą działać bardziej wydajnie, optymalizować swoją przewagę konkurencyjną i zwiększać przychody.

Analiza danych klinicznych

Wprowadzanie produktu na rynek w najszybszym możliwym tempie, przy jednoczesnym utrzymaniu możliwie najniższych kosztów, jest jednym z głównych wyzwań dla firm farmaceutycznych. Zarządzanie danymi klinicznymi staje się kluczowe, ponieważ stanowią one podstawę produktu dostarczanego przez te firmy. Przykładowo, wyniki prób i testów klinicznych muszą być stale monitorowane, a generowane z nich dane powinny być właściwie wykorzystywane.
Według Christian Steven oprogramowanie BI dodaje możliwości analityczne do śledzenia wszystkich tych informacji, pozwala też na identyfikowanie najbardziej wydajnych praktyk i usprawnianie dystrybucji zasobów. Ponadto, gromadząc dane z wielu źródeł, BI umożliwia firmom farmaceutycznym identyfikowanie trendów i zawirowań oraz kontrolowanie ryzyka podczas opracowywania i wprowadzania produktu na rynek.

Cele marketingowe

Co roku firmy farmaceutyczne na całym świecie wydają na marketing ogromne kwoty. Nic dziwnego, że chcą wiedzieć, jak faktycznie przekładają się na sprzedaż. Ulepszanie strategii i efektywniejsza dystrybucja budżetu na marketing wymaga śledzenia wyników sprzedaży i zachowań konsumenckich.
BI pozwala firmom identyfikować produkty, które przynoszą największy dochód, wykorzystując odpowiednie wskaźniki KPI, takie jak segmentacja klientów, analizy kampanii i udziału w rynku. Umożliwia także monitorowanie zachowań konsumentów związanych ze wznawianiem recept i zakupami produktów, sporządzanie wykresów kampanii marketingowych i analizowanie rentowności wg produktu, klienta, danych demograficznych i innych czynników, twierdzi ChristianSteven.

Analiza finansowa

Finalnie wydajność każdej firmy spada do takiego poziomu, na jakim jest ona w stanie zarządzać posiadanymi pieniędzmi i zarabiać. Dane finansowe są integralną częścią każdego przedsiębiorstwa komercyjnego. W celu uzyskania wiedzy, na co są wydawane środki i jakie przynosi to wyniki, konieczne jest dokładne ich monitorowanie.
Rozwiązania BI pomagają firmom farmaceutycznym monitorować transakcje finansowe i z dużym wyprzedzeniem przewidywać potrzeby i ewentualne problemy. Dzięki takiemu proaktywnemu podejściu organizacja może przygotować się na wszelkie nieoczekiwane sytuacje lub ich unikać. W tym celu rozwiązania BI mogą m.in. generować niezbędne raporty kwartalne, roczne i inne. □

CASE STUDY: BI W FARMACJI

Do dostawcy rozwiązań Business Intelligence (BI), firmy SAS, zwróciła się po pomoc firma farmaceutyczna AstraZeneca. Chciała, by produkcja leku Turbuhaler stała się bardziej opłacalna i miała mniejsze odchylenia. Wyzwaniem stojącym przed producentem leku było stworzenie rozwiązania, które byłoby zdolne obsłużyć wszystkie dane związane z produkcją i składowane w wielu rozproszonych systemach.

„Astra Zeneca poprosiła SAS o opracowanie prototypu rozwiązania BI, potrafiącego przechowywać i analizować informacje oraz generować raporty dla wielu różnych grup użytkowników" - stwierdza SAS w dokumencie na swojej stronie internetowej. „Celem było zwiększenie wydajności, poprawa jakości, zminimalizowanie zmian i oszczędność czasu. Korzystając z rozwiązania SAS, firma AstraZeneca, mająca 26 zakładów w 18 krajach, osiągnęła opartą na jakości i efektywną kosztowo produkcję leku Turbuhaler – dzięki automatyzacji szeroko zakrojonych działań w zakresie zarządzania danymi i analityki".

Wymagania

Jak twierdzi Eva Nossborn, inżynier ds. procesów w AstraZeneca, firma miała ściśle określone wymagania dotyczące rozwiązania SAS. „Czyste dane produkcyjne połączone z danymi ze źródeł pomocniczych, np. z systemów planowania i jakości, generują tabele z ogromną ilością informacji" – mówi Eva Nossborn. „W systemie jest około 1000 parametrów. Dzienna porcja danych dla pojedynczej tabeli tworzyła niedawno ok. 170 mln. Wierszy i zwiększała się każdego tygodnia o 1,5 mln. wierszy".

Co dostarczono

Według SAS częścią projektu pochłaniającą najwięcej czasu było zbudowanie systemu do gromadzenia wszystkich informacji w jednej bazie danych i zapewnienie, by wszystko spełniało wysokie standardy wymagane w branży farmaceutycznej. „Od 50 do 100 pracowników tworzy lub otrzymuje raporty z systemu" - twierdzi SAS. „Głównymi użytkownikami są inżynierowie procesów, którzy są odpowiedzialni za monitorowanie codziennej produkcji. Otrzymują oni gotowe raporty, a także są w stanie opracować własne raporty specjalne. Pozostali użytkownicy to operatorzy, statystycy, analitycy i osoby odpowiedzialne za zapewnienie jakości, a także inni menedżerowie w firmie.

Oszczędność czasu była główną korzyścią zapewnianą przez rozwiązanie SAS. Była to jednak tylko część pierwotnego celu budowy systemu. Istotne było także oparte na kompleksowym planie usprawnienie produkcji. „Stale pracujemy nad zwiększeniem wydajności" - mówi Henrik Åkerblom, inżynier procesu i jedna z osób odpowiedzialnych za wdrożenie rozwiązania SAS. „Dotyczy to wzrostu poziomu wykorzystania zasobów podczas produkcji oraz zwiększenia wydajności i jakości produktów. Korzystając z rozwiązania SAS, jesteśmy w stanie zminimalizować odchylenia w procesie produkcyjnym i zwiększyć zakres przeprowadzanych analiz.

Informacja o firmie SAS Institute

SAS Institute jest światowym liderem w zakresie analityki biznesowej oraz największym niezależnym dostawcą oprogramowania Business Intelligence. Z rozwiązań SAS korzysta na świecie ponad 83 000 firm i instytucji w 148 krajach, w tym 96 przedsiębiorstwa z pierwszej setki listy 2017 Fortune Global 500. Firma istnieje od 1976 r. i zatrudnia ponad 14 000 pracowników. W Polsce SAS Institute działa od 1992 r. i jest wiodącym dostawcą zaawansowanej analityki i BI. Rozwiązania i oprogramowanie SAS adresowane są do wszystkich sektorów gospodarki, m.in. bankowości, ubezpieczeń, telekomunikacji, energetyki, farmacji, przemysłu, handlu oraz sektora administracji publicznej.

Informacja o firmie AstraZeneca

AstraZeneca to jedna z największych firm farmaceutycznych na świecie, która dostarcza nowoczesne leki na najpoważniejsze choroby stanowiące wyzwanie dla współczesnej medycyny. W Polsce firma jest obecna od ponad 20 lat. Firma od początku swojego istnienia nieustannie kładzie duży nacisk na rozwój. Kluczowe znaczenie ma działalność badawczo-rozwojowa, ponieważ badania kliniczne są istotnym filarem innowacyjności AstraZeneca. W 2011 r. firma utworzyła w Warszawie globalne Centrum Operacyjne Badań Klinicznych jako pierwsze w tej części Europy i obecnie jedno z sześciu na świecie.

Bezpieczeństwo przemysłowe w obliczu nadchodzących zmian

FIRMY ŚWIADCZĄCE USŁUGI OCHRONY Z NATURY RZECZY SKUPIAJĄ SWOJĄ UWAGĘ NA OCHRONIE, A WIĘC PODEJMOWANIU DZIAŁAŃ ZABEZPIECZAJĄCYCH LUDZI I MIENIE. RÓWNIEŻ Z NATURY RZECZY ICH NAJWIĘKSZYM RYNKIEM SĄ KLIENCI, U KTÓRYCH – PRZEPRASZAM ZA KOLOKWIALIZM – UKRAŚĆ MOŻNA NAJWIĘCEJ I NAJŁATWIEJ. TO SKĄDINĄD DOŚĆ PROZAICZNE PODEJŚCIE LEŻY PRZECIEŻ U PODSTAW SPRZEDAŻY KAŻDEJ BRANŻY.

TEKST
Jacek Grzechowiak

Bezpieczeństwo przemysłowe – wczoraj – dziś/jutro

Trudno mieć za złe branży ochrony, iż także i tu „wielkość" docelowego rynku determinuje kierunek, tempo i atencję. Dlatego też ochrona obiektów przemysłowych od dawna była liderem wśród segmentów ochrony, gdzie próbkowano, testowano i wreszcie wprowadzano innowacyjne rozwiązania ochronne. Ta dziedzina ochrony była też chyba najściślej związana ze zmianami generacyjnymi i technologicznymi chronionej branży. Nic dziwnego, bowiem rewolucje technologiczne branży przemysłowej leżały u podstaw rewolucji lub ewolucji innych branż, były także impulsem do narodzin lub wyodrębnienia branż całkiem nowych, jak choćby logistyki. Dziś mamy okazję obserwować kolejną rewolucję przemysłową, polegającą na integracji ludzi i cyfrowo sterowanych maszyn z Internetem i technologiami informacyjnymi. Towarzyszy jej zastępowanie dotychczasowych łańcuchów komunikacji i dostaw sieciami współdziałającymi i komunikującymi się wielokierunkowo, przy jednoczesnej integracji zasobów materialnych z niematerialnymi, z których część jest wirtualna – zlokalizowana w sieci Internet.

Można więc postawić tezę, że Przemysł 4.0 prowadzi nas w kierunku unifikacji (zjednoczenia) świata rzeczywistego (człowiek, maszyna, surowiec, produkt) ze światem wirtualnym Internetu i technologii bazodanowych. Wielu ekspertów jako źródło tej rewolucji wskazuje *...przede wszystkim wzrost ilości dostępnych danych oraz możliwości obliczeniowych*[1]. Nie wdając się w dyskusję czy to rewolucja, czy ewolucja, nie ulega wątpliwości, że dzieje się ona nie gdzieś daleko od nas, ale ma miejsce także w naszym kraju, i to zarówno w odniesieniu do międzynarodowych korporacji, jak i rodzimych producentów. Dotyczy zarówno nowo budowanych fabryk, jak i modernizacji zakładów funkcjonujących od dawna[2]. Przemysł 4.0 jest już faktem.

Coraz częściej widzimy także, że rozwój klientów (firm) z segmentu produkcyjnego powoduje, iż tradycyjnie pojmowana ochrona nie spełnia już ich oczekiwań, nie chroni bowiem wszystkich aspektów działalności nowoczesnych firm produkcyjnych. Dotyczy to zresztą także innych branż. Jednak skupiając się na firmach produkcyjnych i patrząc na nie przez pryzmat wizji Przemysłu 4.0., nie sposób nie prowadzić studiów incydentów znanych z przeszłości bez symulacji zastępowania rozwiązań ówczesnych, rozwiązaniami współczesnymi. I to patrząc zarówno z perspektywy

[1] Przemysł 4.0, czyli wyzwania współczesnej produkcji", www.pwc.pl/przemysl4.0
[2] Z. Piątek, Czym w praktyce są wdrożenia z obszaru Industry 4.0? https://automatykab2b.pl/gospodarka/50196-czym-w-praktyce-sa-wdrozenia-z-obszaru-industry-4-0

działań ochronnych, jak i z perspektywy działań przestępczych. Większość z czytelników z pewnością pamięta jeden z największych incydentów kradzieżowych, jakim niewątpliwie był nagłośniony medialnie przypadek wywiezienia w styczniu 2008 r. z fabryk Sharp i Orion w Łysomicach znacznej liczby telewizorów o szacunkowej wartości 1,5 mln zł[3] przez zorganizowaną grupę przestępczą. Wskazywał on na możliwość precyzyjnej penetracji organizacji, zarówno w sferze fizycznej (lokalizacja poszczególnych obiektów, procesów), jak i proceduralnej (zdefiniowanie procedur, zasad ich stosowania, możliwości zaburzenia ich przebiegu). Skoro wtedy penetrowano całe spectrum aktywności mających wpływ na skuteczność dokonania kradzieży, a dziś część z tych zasobów przeszła ze sfery rzeczywistej do wirtualnej, oznacza to, że zmienia się jedynie miejsce dokonania penetracji i należy spodziewać się ingerencji przestępców w zasoby i procesy wirtualne.

A skoro tak, to...

Trzeba przyjąć za pewnik, że w przypadku przygotowania podobnego incydentu, penetracji będzie podlegać także ta część procesu, która w wyniku transformacji w ramach Przemysłu 4.0 przeszła do sfery wirtualnej. Nie ulega bowiem wątpliwości, że skoro zasoby i procesy chronione podlegają transformacji, to z pewnością pojawiają się adekwatne – nowe – zagrożenia. I tym samym rodzi się potrzeba nowych rozwiązań ochronnych, co wymaga odpowiedzi zarówno ze strony firm produkcyjnych, jak i firm ochrony.
Science fiction? Niekoniecznie. Na poziomie osobistym zagrożenie to zostało już zdiagnozowane jako w pełni ukształtowane i utrwalone, co spowodowało wprowadzenie rozwiązań prawnych w zakresie penalizacji. Mam tu na myśli kradzież tożsamości czy fałszywe transakcje internetowe, będące najczęściej rezultatem także penalizowanego oszustwa komputerowego. Skoro przynoszą one korzyści na poziomie osobistym, a więc niskowartościowym, to przecież Przemysł 4.0. – który z założenia wiąże aktywności rzeczywiste z wirtualnymi, w zasadzie podążając przynajmniej częściowo ścieżką rozwiązań już funkcjonujących na poziomie osobistym – bez wątpienia już teraz podlega tym samym zagrożeniom.

Skoro zasoby i procesy chronione podlegają transformacji, to z pewnością pojawiają się adekwatne – nowe – zagrożenia.
Tym samym rodzi się potrzeba nowych rozwiązań ochronnych, co wymaga odpowiedzi zarówno ze strony firm produkcyjnych, jak i firm ochrony

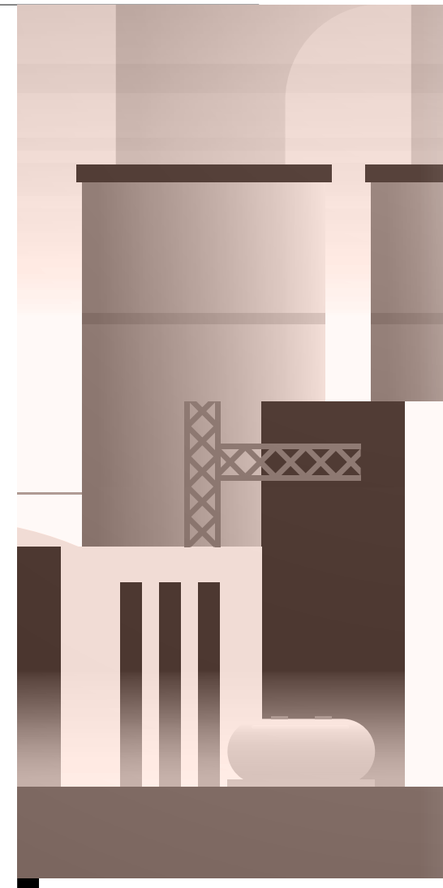
Aż prosi się przy tym dać przykład sprzed lat, kiedy to spedytor powierzył przewóz drogiej maszyny przewoźnikowi znalezionemu na internetowej giełdzie transportowej. Przewoźnik (jak najbardziej rzeczywisty) odebrał maszynę, po czym... rozpłynął się gdzieś pomiędzy naszą wschodnią a zachodnią granicą. Innym przykładem jest dość rozpowszechniony w ostatnim czasie proceder oferowania usług transportowych po bardzo niskich cenach, w wyniku czego taki przewoźnik (umówmy się – z założenia fikcyjny) wygrywa wszelkie licytacje najniższą ceną. Następnie zleca transport, wystawiając nieraz na tę samą giełdę ofertę zlecenia transportowego z ceną dużo wyższą. Transport realizuje podwykonawca podwykonawcy, ale nigdy nie dostaje za to pieniędzy. Efekt oszustwa jest oczywisty, ale może on powodować – i nierzadko powoduje – perturbacje w transporcie wyrobów gotowych czy komponentów produkcyjnych, ale to już problem producenta. Łatwo wyobrazić sobie te same mechanizmy w procesach produkcyjnych i ich skutek dla ciągłości biznesu producenta. Dlatego coraz częściej widzimy pracowników ochrony zajmujących się analizowaniem procesów logistycznych czy podobnymi działaniami, które zupełnie nie przypominają tradycyjnej ochrony, kojarzonej z otwieraniem szlabanu czy sprawdzaniem zgodności załadunku z dokumentem magazynowym.
Co oczywiście nie oznacza, że tego typu działania są zbędne. Jednak nowe procesy spowodowały powstanie nowych form ochrony. Firmy ochrony coraz częściej wdrażają model działań ochronnych bazujących na przewidywaniach z wykorzystaniem wieloaspektowych analizach danych, dzięki czemu możliwa jest aktywna alokacja sił i środków, będąca odzwierciedleniem idei Przemysłu 4.0[4].

Jak ochronić przed kradzieżą towar, którego nigdy nie było w magazynie? – taki „prowokacyjny" śródtytuł nadałem, pisząc o bezpieczeństwie przemysłowym w „a&s Polska" rok temu. Opisywałem wtedy przypadek kradzieży, która de facto miała miejsce poza chronionym obiektem, choć na pierwszy rzut oka do kradzieży miało dochodzić w całkiem zresztą dobrze zabezpieczonym magazynie. Czy Przemysł 4.0 zmieni działania złodziei i rozwiązania będące odpowiedzią firm ochrony? Czy to wciąż jeszcze przyszłość, czy jednak już teraźniejszość? Przykłady z naszego życia w postaci kradzieży tożsamości czy „przechwytywania" kodów BLIK pokazują, że na poziomie prywatnym dzieje się to już w pełnym wymiarze. Powinniśmy zatem przyjąć za pewnik, że te same rodzaje ryzyka pojawią się na poziomie przemysłowym.
Odnosząc się do idei Przemysłu 4.0 w kontekście przykładu z roku ubiegłego, widać wyraźnie, że pełna identyfikacja komponentów i produktów, która jest jedną z najważniejszych korzyści Przemysłu 4.0, daje ochronie nowe możliwości, stwarza nowe szanse, stawiając oczywiście nowe wyzwania. Na bazie tamtego przykładu ochrona mogłaby monitorować dostawę surowca już od chwili jego wysłania od dostawcy do producenta, a więc przewidując wielkość dostawy, miałaby szansę na identyfikację incydentu niemal w czasie rzeczywistym, a z pewnością na długo przed inwentaryzacją. I tak właśnie dzieje się już dziś. Na razie jeszcze nie jest to ugruntowana praktyka, ale to tylko kwestia czasu. I co ważniejsze, rola ochrony w zapewnieniu ciągłości działania, która jest główną troską niezależnie od generacyjnego rozwoju segmentu produkcyjnego, rośnie i daje wymierne korzyści. Gdzie jest wyzwanie? Niewątpliwie w kompetencjach pracowników ochrony i narzędziach stosowanych przez firmę ochrony. Oba te obszary wymagają znacznej transformacji.

Przemysł 4.0., dający pełną identyfikację produktów, a więc również pracowników je produkujących, pozwala na skrócenie nawet trudnych postępowań wyjaśniających

Czy Przemysł 4.0 może wspomagać przeciwdziałanie zagrożeniom bardziej zaawansowanym?

Rok temu przedstawiałem przypadek zakładu produkującego elementy szklane, w którym wystąpiły poważne problemy jakościowe, a których analiza „po incydencie" ujawniła przesłanki do rozważenia sabotażu. Postępowanie wyjaśniające nie było łatwe i niestety trwało dość długo, przez co straty rosły. Przemysł 4.0., dający pełną identyfikację produktów, a więc również pracowników je produkujących, pozwala na skrócenie nawet tak trudnych postępowań wyjaśniających. Tym samym także w zakresie rodzajów ryzyka trudnych do zarządzania Przemysł 4.0. pozwala na zwiększenie skuteczności ochrony. Niewątpliwie przyniesie również nowe formy sabotażu, którym zewnętrzna ochrona nie będzie w stanie przeciwdziałać. Jednak i w tym obszarze perspektywy niewątpliwie są.
Przemysł 4.0 jest bez wątpienia przyszłością, od której odwrotu nie ma. Stwarza olbrzymie możliwości firmom ochrony, dając szansę na wejście na zupełnie inny poziom usług, nie pozwalając przy tym ochronie na bierność. Tu klienci zdecydują, czego będą potrzebowali. Z punktu widzenia wewnętrznych struktur ochrony firm produkcyjnych, szanse w obszarze ochrony są jeszcze większe. Nie oznacza to, że można zapomnieć o dotychczasowych – prozaicznych – problemach przedsiębiorców i ochrony, takich jak odnotowana w ostatnim czasie kradzież owoców – liczona w tonach, a więc poważna z biznesowego punktu widzenia[5], czy zupełnie odmienna w charakterze kradzież produktów wielkogabarytowych i jednocześnie wysokotonażowych. Zagrożenia te będą obecne w naszej codzienności w dalszym ciągu. Będą te same, ale... nie takie same. Dlatego już dziś powinniśmy o nich myśleć, bo przecież – cytując Sławomira Mrożka – *jutro to dziś, tyle że jutro.* □



BIO

Jacek Grzechowiak

Menedżer ryzyka i bezpieczeństwa. Związany z grupą Securitas w Polsce, gdzie zarządza ryzykiem. W przeszłości zarządzał bezpieczeństwem polskich operacji Avon i Celsa. Absolwent WAT, studiów podyplomowych w SGH i Akademii L. Koźmińskiego. Gościnnie wykłada na uczelniach wyższych.

[3] http://wiadomosci.wp.pl/wid,9640810,kat,1342,wiadomosc.html?ticaid=1560b

[4] https://securitasfuturelab.com/the-security-officer-of-tomorrow/

[5] https://www.se.pl/warszawa/napad-100-lecia-pod-tarczynem-wynosili-swoje-lupy-w-tonach-przez-prawie-miesiac-aa-PWGY-CWZj-34aV.html

Bezpieczeństwo rozproszonych obiektów przemysłowych

Główne wyzwania

TEKST
Tomasz Guzikowski

Czy istnieje idealny system ochrony rozproszonych obiektów przemysłowych? Ochrony nie tylko przed zagrożeniami z zewnątrz, takimi jak terroryzm, cyberataki czy coraz częstsze ostatnio gwałtowne zjawiska atmosferyczne, ale również przed czynnikami wewnętrznymi, takimi jak stosowane w procesie produkcyjnym niebezpieczne substancje, błąd człowieka, niewłaściwa eksploatacja maszyn i urządzeń lub niespójne procedury awaryjne? Wiele wskazuje na to, że takiego idealnego systemu nie ma, ale warto do tego ideału dążyć po to, by zaprojektować rozwiązanie, które maksymalnie ograniczy ryzyko zagrożeń w obiektach przemysłowych.

Kluczowym elementem w projektowaniu i uruchamianiu systemów bezpieczeństwa w rozproszonych obiektach przemysłowych jest dostosowanie poziomu kosztów do przewidywanych korzyści oraz precyzyjne określenie celu ich stosowania. System bezpieczeństwa nie powinien spełniać wyłącznie funkcji chroniącej przed nieuprawnionym dostępem. System taki, w połączeniu z odpowiednimi procedurami, powinien przede wszystkim odpowiadać za utrzymanie ciągłości działania organizacji, w tym m.in. zapewniać bezpieczeństwo pracowników, procesów przemysłowych, przepływu surowców i półproduktów, a także jakości produktów.

Kolejnym elementem składowym, który trzeba uwzględnić przy projektowaniu takiego systemu, jest proces zarządzania ryzykiem. Obejmuje on z jednej strony identyfikowanie zagrożeń określając prawdopodobieństwo ich wystąpienia i ewentualny wpływ na procesy. Z drugiej strony – ustalania i wdrażania standardów bezpieczeństwa, których wynikiem będą zastosowane środki bezpieczeństwa. Te dwa pozornie przeciwstawne elementy składają się z kolei na proces oceny ryzyka pokazujący, czy poziom danego ryzyka jest akceptowalny, tolerowalny, czy też nieakceptowalny. Taka analiza daje narzędzie kierownictwu organizacji do podjęcia decyzji, w jakie środki bezpieczeństwa zainwestować i czy taka inwestycja jest uzasadniona biznesowo.

Te trzy elementy – koszt, cel (uwzględniający także utrzymanie ciągłości działania) i zaawansowany proces zarządzania ryzykiem – tworzą fundament efektywnego systemu bezpieczeństwa. To fundament, ale warto przyjrzeć się kilku rozwiązaniom operacyjnym. Bardzo ważny jest np. aspekt informacji i szkoleń. W obiektach przemysłowych opracowane procedury bezpieczeństwa, instrukcje postępowania w sytuacji zagrożenia (najlepiej jednostronicowe, w formie graficznej) i ciągłe podnoszenie świadomości oraz szkolenie pracowników, są równie ważne, jeśli nawet nie ważniejsze niż zaimplementowane systemy zabezpieczeń. To pozwala na ograniczenie ryzyka ze strony najsłabszego ogniwa w systemach bezpieczeństwa, jakim jest człowiek.

Nawet jeśli nie jest to w pełni możliwe, przy projektowaniu systemu zarządzania bezpieczeństwem zawsze należy dążyć do pełnego zapewnienia bezpieczeństwa i ograniczenia strat. Dlatego projektowanie systemu zarządzania powinno uwzględniać wszystkie aspekty bezpieczeństwa, w tym również awarie procesowe i techniczne, wypadki i choroby zawodowe oraz różne aspekty ekonomiczne. Co szczególnie ważne, potrzeba zapewnienia bezpieczeństwa powinna wynikać z wymiernych korzyści lub potencjalnych strat organizacji. W związku z tym zawsze należy utrzymywać właściwą równowagę pomiędzy celami biznesowymi a celami bezpieczeństwa realizowanymi przez system zabezpieczeń.

Podjęcie właściwych decyzji technicznych i organizacyjnych wymaga odpowiedniego rozpoznania słabości i ograniczeń. Dlatego przy projektowaniu systemu zabezpieczeń ważna jest również praca zespołowa z udziałem różnych specjalistów, która zapewnia efekt synergii i pozwala podejmować optymalne decyzje. Co więcej, tylko interdyscyplinarna wiedza inżynierska, organizacyjna i ekonomiczna umożliwia osiągnięcie zrównoważonego rozwoju organizacji.

Oczywiście w każdym procesie produkcyjnym bądź działalności człowieka występuje tzw. ryzyko resztkowe, którego nie da się całkowicie wyeliminować, dlatego tak ważna jest systematyczna, bieżąca analiza zdarzeń w otoczeniu, która pozwala uczyć się na cudzych błędach i budować własne doświadczenie. Warto także nieustannie sprawdzać, czy procedury bezpieczeństwa są właściwie realizowane, oraz redukować ryzyko, do poziomu praktycznie uzasadnionego, poprzez eliminację czynników zagrożeń i stosowanie niezawodnych wielowarstwowych systemów zabezpieczeń i ochrony.

Innym ważnym elementem systemu zarządzania bezpieczeństwem jest zdolność organizacji do szybkiej odbudowy zasobów, ale to już temat do rozważenia przy innej okazji. □

BIO
Tomasz Guzikowski

Dyrektor Biura Zarządzania Majątkiem i Bezpieczeństwa w Grupie Kapitałowej CIECH. Absolwent m.in. Akademii Ekonomicznej w Krakowie na kierunku Finanse i Bankowość oraz Politechniki Łódzkiej na kierunku Bezpieczeństwo Procesów Przemysłowych. 25 lat doświadczenia w branży bezpieczeństwa, w tym 14 lat w budownictwie, a od 2014 r. w przemyśle chemicznym.

Zalety dozoru wizyjnego w obiektach przemysłowych

Przemysł to pod względem ochrony bardzo złożona branża. Zakłady produkcyjne obfitują w obszary potencjalnego ryzyka, co obliguje do bezwzględnego przestrzegania przepisów dotyczących bezpieczeństwa i higieny pracy. W wielu obszarach działalności produkcyjnej – od parkingów, wjazdów i wyjazdów, powierzchni biurowych, miejsc dostawy i wysyłki towaru, po miejsca produkcji i montażu – niezwykle istotną rolę może odegrać dozór wizyjny.

T E K S T
Christina Behle
Axis Communications

Dostawa surowców, magazynowanie i wysyłka cennego produktu, obsługa maszyn oraz miejsca przeznaczone tylko dla upoważnionego personelu – we wszystkich tych obszarach działania przedsiębiorstwa produkcyjnego można zastosować systemy dozoru wizyjnego wraz z powiązanymi technologiami.

W ogólnym rozumieniu korzyści płynące ze stosowania dozoru wizyjnego w branży wytwórczej to:

- **bezpieczeństwo przedsiębiorstwa, parku maszynowego i produktów**
- **ochrona pracowników i gości**
- **monitorowanie procesu produkcyjnego**
- **optymalizacja procesów biznesowych**

Kompleksowe bezpieczeństwo

Bezpieczeństwo ma ogromne znaczenie dla każdej firmy. Dla producenta, którego fabryka, maszyny, surowce i produkty końcowe mają znaczącą wartość, ma znaczenie krytyczne. Skuteczna ochrona obwodowa ostrzegająca pracowników ochrony przed naruszeniami terenu, intruzami i podejrzanym zachowaniem stanowi podstawę pierwszej linii zabezpieczania obiektu. Axis posiada w swojej ofercie AXIS Perimeter Defender – aplikację do analizy wideo, która w połączeniu z kamerami sieciowymi Axis tworzy niezwykle skuteczny system automatycznie wykrywający osoby i pojazdy na terenie obiektu i reagujący na ich obecność.

W zakładach produkcyjnych, ze względu na ich specyfikę, ma miejsce stały przepływ uprawnionych osób niebędących pracownikami, które z różnych przyczyn muszą się znaleźć w obiekcie. Konieczna jest zatem skuteczna kontrola dostępu, zarówno na parkingu, od strony drzwi wejściowych, jak i na rampach załadowczych. Poza tym nawet pracownicy zakładu nie zawsze są upoważnieni do wejścia na wszystkie jego obszary. Stacje drzwiowe przekazujące obraz i dźwięk umożliwiają weryfikację wchodzących, a w razie potrzeby stanowią barierę dla nieupoważnionego personelu.

Rozwiązania kontroli dostępu Axis są oparte na otwartych protokołach, dzięki czemu można je dowolnie łączyć z najlepszym sprzętem i oprogramowaniem oraz integrować je z innymi systemami, w tym funkcjonującym systemem dozorowym. Można wykorzystywać je do różnych celów: od podstawowej identyfikacji, przez kontrolę dostępu, aż po zaawansowane zarządzanie dostępem.

Zapewnienie bezpieczeństwa pracowników

Mimo starań podejmowanych w celu minimalizowania ryzyka wypadków przy pracy zdarzają się one w każdej branży. W obiektach przemysłowych, zakładach produkcyjnych i fabrykach bywają szczególnie poważne ze względu na charakter pracy. Urazy i choroby związane z pracą wiążą się również z ogromnymi kosztami. Badania wykazały, że w Unii Europejskiej stanowią obciążenie dla firm w wysokości aż 476 mld euro rocznie. Dozór wizyjny przyczynia się do obniżenia kosztów wypadków. Obraz z kamer dozorowych może okazać się bardzo przydatny w dochodzeniu powypadkowym – pomoże ustalić, czy odpowiedzialność spoczywa na pracodawcy, czy pracowniku. Ponadto może przyczynić się do podjęcia działań w przedsiębiorstwie mających na celu wyeliminowanie podobnych zdarzeń w przyszłości, np. wprowadzenie lepiej widocznych oznakowań, barier ochronnych, a nawet nowych maszyn.

Zapobieganie wypadkom i incydentom leży w interesie zarówno pracodawcy, jak i pracownika – i tu właśnie ujawnia się niewidoczna korzyść z posiadania systemu dozoru wizyjnego. Podobnie jak jawny monitoring wizyjny odstrasza potencjalnych złodziei, kamery dozorowe w zakładach produkcyjnych wspomagają przestrzeganie zasad BHP. Doświadczenia przeprowadzane przez dziesiątki lat wykazały, że ludzie nieświadomie zachowują się lepiej, gdy wiedzą, że są obserwowani, nawet jeżeli patrzy na nich jedynie twarz z plakatu. Logiczne zatem jest, że tam, gdzie pracownicy wiedzą, że znajdują się pod okiem kamer, będą ściślej przestrzegać wewnętrznych przepisów i zasad BHP.

Monitorowanie produkcji i optymalizacja procesów

Każdy zakład produkcyjny stawia sobie za cel osiągnięcie maksymalnej wydajności. Wszelkie awarie maszyn mają poważny wpływ na produkcję, której obniżenie prowadzi do pogorszenia rentowności i niezadowolenia klientów. System dozoru wizyjnego jest w stanie monitorować cały proces produkcyjny, a dodatkowe technologie, np. obrazowanie termowizyjne, mogą sygnalizować potencjalne problemy (w rodzaju przegrzania maszyn), umożliwiając tym samym podjęcie działań wyprzedzających. Kolejną technologię – analizę obrazu – można wykorzystać do badania przepływu ludzi i produktów w całym zakładzie, co pozwoli np. określić obszary, w których przeprowadzenie niewielkich zmian może przynieść znaczną poprawę wydajności.

Poszanowanie praw pracowników

Należy zaznaczyć, że chociaż dozór wizyjny w miejscu pracy ma liczne korzyści, które w pełni uzasadniają jego stosowanie, tam gdzie jest on wykorzystywany, muszą być respektowane prawa pracowników dotyczące zapisywanego materiału. Jest to szczególnie istotne w świetle unijnego rozporządzenia o ochronie danych osobowych (RODO). W artykule opublikowanym na portalu securityprivacybytes.com[1] znajduje się przykład konkretnego wpływu przepisów RODO na dozór wizyjny w miejscu pracy. Opracowanie Axis dotyczące szerszego wpływu RODO na dozór wizyjny można znaleźć na portalu axis.com[2].

Wielorakie zalety dozoru wizyjnego – zarówno oczywiste, jak i ukryte – są teraz dostępne bardziej niż kiedykolwiek dla szerszego kręgu przedsiębiorstw różnej wielkości. Więcej informacji na temat najważniejszych aspektów projektowania systemu dozoru wizyjnego znajduje się na blogu firmy Axis[3]. □

1) https://www.securityprivacybytes.com/2018/02/the-gdprs-impact-on-cctv-and-workplace-surveillance/
2) https://www.axis.com/files/whitepaper/gd_gdpr_72045_en_1804_lo.pdf
3) https://www.axis.com/blog/secure-insights/security-surveillance-needs/

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

Dzień z życia operatora w centrum monitoringu wizyjnego

Genetec Mission Control™ umożliwia dużym zakładom przemysłowym wyjście poza proste zarządzanie zdarzeniami poprzez gromadzenie i kwalifikowanie danych z tysięcy czujników i urządzeń systemów zabezpieczeń, wykrywanie najbardziej złożonych sytuacji i incydentów oraz kierowanie zespołami ochrony w ich działaniach zgodnie z procedurami i wymogami RODO. Mission Control jest systemem zarządzania decyzjami, który pomaga operatorom centrum monitorowania w podejmowaniu właściwych decyzji – w obliczu rutynowych zadań lub nieprzewidzianych sytuacji – zapewniając natychmiastową reakcję i przepływ informacji.

Praca operatora w centrum monitoringu wizyjnego nie jest łatwa. Każdego dnia musi borykać się z niezliczonymi wyzwaniami, mając coraz szerszą listę zadań i rzeczy do śledzenia. Każdy obiekt jest narażony na inne zagrożenia, ma inne priorytety co do zakresu monitorowania. Są też typowe wyzwania, z którymi musi sobie poradzić każdy operator: fałszywe alarmy, przestrzeganie przepisów RODO i generowanie dokładnych raportów.
Wychodząc naprzeciw tym potrzebom, firma Arpol wprowadziła do oferty system zarządzania decyzjami Genetec Mission Control™ wspomagający pracę operatorów w centrach monitoringu wizyjnego.

Fałszywe alarmy to więcej niż tylko uciążliwość

Jak podaje „SC Magazine", 70% operatorów w USA czuje się przytłoczonych liczbą powiadomień, którymi muszą zarządzać. Badania IFSEC Global pokazują, że 70–90% sygnałów przychodzących do centrum monitoringu to alarmy fałszywe lub uciążliwe. Mogą być wywoływane przez różne zdarzenia, np. rośliny kołyszące się na wietrze. Biorąc pod uwagę potencjalne zagrożenie, należy zbadać każdy alarm. Ale jeśli wysoka trawa jest przyczyną większości odbieranych zdarzeń, szanse na ich priorytetowe traktowanie przy kolejnych alarmach są mniejsze.

Dużo alarmów, mało czasu

Otrzymując tak wiele fałszywych lub uciążliwych alarmów, operator zaczyna je ignorować lub wyłącza urządzenie, które je generuje. Może to mieć niebezpieczne konsekwencje. Dlatego ważne jest, aby otrzymywać kwalifikowane alarmy. Pomóc w tym może korzystanie z systemu zarządzania decyzjami Genetec Mission Control™. Gdy system wykryje zdarzenie, np. pojazd, którego numery rejestracyjne znajdują się na czarnej liście, chce wjechać na teren zakładu, naruszenie linii przy ogrodzeniu czy próbę nieuprawnionego wejścia do obiektu, tworzy się kwalifikowany incydent. Na tej podstawie system ostrzega operatora w centrum monitoringu i identyfikuje zdarzenie jako mające wyższy priorytet, wysyła też nagranie wideo powiązane z alarmem.

Zasady zgodności

Kolejnym wyzwaniem, z którym trzeba się zmierzyć, jest zgodność z przepisami RODO.
Rosnąca lista przepisów określa zasady dotyczące przechowywania danych i ochrony prywatności. Ich śledzenie i zapewnianie zgodności rozprasza uwagę, ale nieprzestrzeganie tych przepisów może spowodować poważne konsekwencje. System zarządzania decyzjami automatycznie przechowuje dane przez wymagany czas i następnie usuwa je ze względu na poszanowanie prywatności.
Oznacza to, że nie trzeba się martwić o przestrzeganie przepisów RODO, ponieważ system Genetec robi to automatycznie.

Nikt nie chce walczyć z raportami

Jednym z bieżących wyzwań dla operatora jest tworzenie codziennych raportów. Zostawiając papierkową robotę na koniec zmiany, musi polegać na swojej pamięci, aby udokumentować szczegóły wszystkich zdarzeń, które miały miejsce w ciągu dnia. Tworząc raport, musi przejrzeć różne pliki źródłowe i wyeksportować dane do Excela. Proces przygotowania raportów może być wykonywany po wielu dniach od czasu zdarzenia ze względu na inne, bieżące zadania. Wówczas kluczowe informacje, np. dokładny czas, w którym operator zareagował na zdarzenie, mogą zostać niedokładne określone.
System zarządzania decyzjami można skonfigurować tak, aby automatycznie rejestrował każde działanie podejmowane podczas reakcji na zdarzenie, a także oznaczał czasowo, szyfrował i archiwizował materiał wideo przez czas określony przepisami RODO. □

Arpol

ul. Kajki 1,60-545 POZNAŃ
tel. 61 846 21 00
www.arpol.pl
info@arpol.pl

Logistyka: Jak ERP uczy się widzieć

Technologie cyfrowe dają nadzieję na ogromne wsparcie, usprawnienia w szerokim zakresie procesów w branży logistycznej. Dallmeier, jako jeden z wiodących producentów technologii wizyjnych, od lat współpracuje z T.CON – ekspertami systemów SAP. Teraz firmy zaprezentowały swoje pierwsze wspólne rozwiązania logistyczne *Digital Gate* i *Package Measurement*.

Rozwiązania opracowane wspólnie przez Dallmeier oraz T.CON umożliwiają przesyłanie danych zarejestrowanych przez systemy wideo bezpośrednio do systemu ERP*. W wyniku współpracy między obiema firmami powstały już gotowe rozwiązania dla łańcucha dostaw, dzięki którym klienci mogą zoptymalizować główne procesy i skrócić czas cyklu. Kolejne rozwiązania z zakresu łańcucha dostaw, zasobów ludzkich i zgodności znajdują się również w programie współpracy.

Digital Gate skraca czas oczekiwania poza terenem obiektu

Dzięki innowacyjnemu portalowi (przejściu) samoobsługowemu opartemu na SAP Fiori rozwiązanie *Digital Gate* automatyzuje procesy ręcznej rejestracji pojazdów i zarządzania listami przewozowymi. System rozpoznaje ASN (zaawansowane dokumenty przewozowe) z wyprzedzeniem i identyfikuje marki oraz klasy ładowności pojazdów, numery rejestracyjne, numery identyfikacyjne oraz przewożone substancje niebezpieczne zgodnie z przepisami dotyczącymi zgodności, umożliwiając automatyczne sterowanie barierą i bramą.
Dane frachtu można uzupełniać w SAP o informacje zebrane optycznie przy użyciu standardowych obiektów SAP. Dane można następnie zintegrować bezpośrednio z SAP TM lub LE-TRA (ECC 6.0). Głównymi zaletami *Digital Gate* są znacznie krótszy czas oczekiwania na wjazd na teren zakładu i zwiększenie przepustowości. W zależności od wymagań system może być obsługiwany indywidualnie lub zintegrowany z istniejącym rozwiązaniem do zarządzania placem.

* SAP ERP to zintegrowany system informatyczny, pomagający w optymalizacji i planowaniu procesów wewnątrz firmy

Fot. 1. Rozwiązanie Digital Gate automatycznie rejestruje najważniejsze cechy przy wejściu. Wyniki są zoptymalizowanym procesem rejestracji o znacznie skróconym czasie cyklu

Package Measurement eliminuje ręczne ważenie i pomiar

Rozwiązanie *Package Measurement* umożliwia w pełni automatyczne obliczanie objętości i ważenie towarów. Do obliczeń objętości są stosowane specjalne systemy wizyjne 3D natychmiastowego pomiaru wymiarów towarów na pojeździe. W celu ustalenia masy towaru wózki widłowe zostały wyposażone w bezprzewodowe wagi zamontowane na widłach, a wszystkie procesy komplementacji zamówień są dokumentowane automatycznie. Dzięki temu firmy logistyczne mogą wyeliminować wszelkie ręczne procesy rejestrowania masy i objętości załadunku oraz wykrywanie nieprawidłowych danych wejściowych.

Dzięki zastosowaniu takiego rozwiązania dane zintegrowane później w SAP WM lub SAP EWM są poprawne. Dalsze korzyści obejmują optymalne wykorzystanie ładowności, kontrolę wiarygodności danych referencyjnych i skoordynowane strategie magazynowania. Rozwiązania do ważenia i pomiaru można wdrażać wspólnie lub osobno. □

Fot. 2. Rozwiązanie Package Measurement automatycznie rejestruje wagę i objętość pakowanych przedmiotów i integruje te informacje z SAP

Dallmeier electronic

Bahnhofstr. 16, 93047 Regensburg, Niemcy
tel +49 151 58204199
www.dallmeier.com

Czy znasz PABLA?

On pomoże poprawić bezpieczeństwo w zakładzie pracy

T E K S T
Adam Gregorczyk

System P.A.B.L.O. (Personalny Asystent Bezpieczeństwa i Lokalizacji Osób) został zaprojektowany i wyprodukowany w odpowiedzi na potrzeby zgłaszane przez użytkowników poszukujących efektywnego, bezpiecznego systemu nadzoru nad pracownikami wykonującymi pracę samodzielnie. Problematyka ta jest poruszana w środowiskach specjalistów odpowiedzialnych za sprawy BHP i Utrzymania Ruchu pod angielską nazwą „Lone Worker" (pracownika samodzielnego). Definicja „Lone Worker" określa, że jest to pracownik, który wykonuje czynności prowadzone w odosobnieniu od innych pracowników, bez bezpośredniego nadzoru. W Polsce częściej spotyka się pojęcie pracownika wykonującego pracę w pojedynkę.

Bezpośrednią korzyścią zastosowania systemu P.A.B.L.O. jest poprawa bezpieczeństwa osobistego i procesowego. Dobrym przykładem wykorzystania możliwości systemu P.A.B.L.O. jest skrócenie i zautomatyzowanie procedury czasowego meldowania się pracownika wykonującego pracę samodzielnie (Dz.U. 1997 r., nr 129 poz. 844 – Rozporządzenie Ministra Pracy i Polityki Socjalnej z 26 września 1997 r. w sprawie ogólnych przepisów bezpieczeństwa i higieny pracy § 43.1 oraz § 43.2.). W przypadku wystąpienia zdarzenia niebezpiecznego P.A.B.L.O. bez zbędnej zwłoki zaalarmuje służby odpowiedzialne za prowadzenie działań ratunkowych oraz poda lokalizację wystąpienia zdarzenia.
System P.A.B.L.O. to rozwiązanie techniczne wspierające bezpieczeństwo i nadzór nad osobami wykonującymi pracę samodzielnie.

W obszarach, na które został zaprojektowany i wykonany indywidualnie dla inwestora, zapewnia osobom posiadającym specjalnie wyposażone i oprogramowane urządzenia (radiotelefony) jednocześnie trzy funkcjonalności:
- ciągłą łączność głosową w każdym, nawet najtrudniejszym miejscu, takim jak rozległe tereny przemysłowe, gdzie występuje dużo konstrukcji metalowych oraz są duże obszary zakładów (również w miejscach, w których nie ma zasięgu sieci publicznej GSM lub w wyniku awarii sieć GSM zostaje wyłączona). System umożliwia połączenia indywidualne, wywołania grupowe i ogólne połączenia priorytetowe – niedostępne dla publicznych sieci GSM;
- lokalizację, bez zbędnej zwłoki, niezależnie czy osoba przebywa w terenie otwartym, czy wewnątrz budynków (hal, magazynów itp.);
- funkcjonalności alarmowe wyzwalane ręcznie poprzez wciśnięcie przycisku w radiotelefonie (w tym funkcjonalność czuwaka – to pomysł zaczerpnięty z bezpieczeństwa ruchu kolejowego: świadome periodyczne przyciskanie odpowiedniego przycisku mechanicznego przez osobę noszącą radiotelefon we wcześniej zaprogramowanych przedziałach czasowych) oraz wezwanie pomocy wyzwalane automatycznie (np. wykrycie upadku lub bezruchu). Wyzwalanie alarmu automatycznego poprzedza zainicjowanie tzw. prealarmu w celu zapobiegania wysyłaniu alarmów fałszywych, które w nadmiarze mogą „znieczulić" obsługę systemu.

W ramach kompletnego systemu dostarczane są urządzenia i usługi:
- wykonanie prób propagacyjnych, potwierdzających zasięg w każdej lokalizacji wskazanej przez inwestora,
- przygotowanie dokumentacji w celu uzyskania pozwolenia radiowego w UKE,
- dostawa elementów: kompletny przemiennik radiowy z odpowiednio zaprojektowanym układem antenowym, odpowiednia liczba znaczników radiowych (rozmieszczonych na terenie obiektu i realizujących lokalizację wewnątrzobiektową), ustalona liczba radiotelefonów wraz z opcjonalnymi akcesoriami audio (mikrofonogłośniki, ochronniki słuchu),
- montaż, uruchomienie, szkolenie użytkowników i służb serwisowych.

Novatel

43-155 Bieruń
ul. Turystyczna 1/9
www.novatel.pl

Głos branży

ZAPEWNIENIE BEZPIECZEŃSTWA OBIEKTOM PRZEMYSŁOWYM I ROZLEGŁYM JEST TEMATEM KOLEJNEGO GŁOSU BRANŻY. PRZEDSTAWIAMY WYPOWIEDZI ZARÓWNO EKSPERTÓW Z BRANŻY SECURITY, JAK I SECURITY MENEDŻERÓW Z TEGO RYNKU WERTYKALNEGO.

Bogumił Szymanek
Axis Communications

Bezpieczeństwo i optymalizacja procesów

Rozwiązania Axis są doceniane na całym świecie ze względu na ich wysoką jakość i niezawodność. Oczywiście zmniejszenie prawdopodobieństwa awarii, które w obiektach przemysłowych mogą wiązać się z dużymi kosztami wynikającymi np. z zatrzymania produkcji czy ograniczenia ruchu, ma bardzo duże znaczenie przy wyborze rozwiązania. Dlatego należy stawiać na te najwyższej jakości.
Warto podkreślić, że przedsiębiorstwa przemysłowe korzystają z wielu systemów, których celem jest zapewnienie bezpieczeństwa oraz optymalizacja procesów. Przenikają się więc tutaj potrzeby funkcjonalne i biznesowe. Axis w tym zakresie oferuje znacznie więcej niż tylko najwyższej jakości urządzenia – kamery, detektory, sys-

temy audio czy urządzenia I/O. W ramach rozwiązań Axis integrator ma zapewnioną wspólną otwartą platformę integracyjną, umożliwiającą stworzenie rozwiązania „szytego na miarę" i zaspokajającą skomplikowane wymagania klienta.
Dla użytkownika takiego systemu niezbędna jest stabilność rozwiązania oraz zrozumiała dokumentacja. Platforma aplikacji Axis jest rozwijana od wielu lat, charakteryzuje się czytelnymi opisami oraz API. Możliwe jest zatem rzeczywiste wykorzystanie mocy obliczeniowej urządzeń, przy jednoczesnym zmniejszeniu zapotrzebowania na zasoby sieciowe i serwerowe. A dzięki analizie i automatyzacji można ograniczyć koszty utrzymania infrastruktury IT oraz ochrony fizycznej. Ma to wielkie znaczenie, gdyż obecnie większość przedsiębiorstw korzysta z elastycznych usług w chmurze i integracja z tego typu rozwiązaniami jest bardzo istotna dla optymalizacji działania całej firmy.
Rozwiązania Axis spełniają też wyśrubowane standardy cyberbezpieczeństwa, a oprogramowanie z długoterminowym wsparciem LTS zapewnia stabilną i bezpieczną pracę systemów przez wiele lat.

Marcin Walczuk

BCS

BCS na żywo

Można zachwalać dane urządzenie z każdej strony, opisując jego niepodważalne zalety, ale ważne jest, jak taki sprzęt sprawdza się później w praktyce. Urządzenia BCS spotyka się w wielu obiektach. Najbardziej działają na wyobraźnię oczywiście duże systemy, gdzie najważniejsze są niezawodność monitoringu wizyjnego, możliwości integracji z innymi systemami i łatwość obsługi takiego systemu. Warto w tym miejscu wspomnieć o systemach opartych na największych rejestratorach dostępnych w ofercie BCS, czyli NVR12816DR-4K-II. Przedstawię kilka przykładów ich zastosowania.

Duży warszawski obiekty użyteczności publicznej. Tu szczególnie ważne jest bezpieczeństwo przebywających tam osób. Podstawowym założeniem była możliwość ciągłej obserwacji całej powierzchni w czasie rzeczywistym. Konieczne też było, aby rejestrator mógł współpracować z istniejącymi już urządzeniami systemu monitoringu, rozbudowywanym przez lata. W tym przypadku do rejestratora są podłączone 4 monitory, na co pozwala dodatkowa karta dekodująca. Wyświetlany jest na nich równocześnie obraz z ponad 70 kamer różnych producentów, a nawet pochodzący ze starych systemów analogowych.
Ośrodek rządowy. Najważniejsza jest tu ciągłość pracy, zdalna obsługa i przechowywanie nagranego materiału przez 90 dni. Na tak długi okres archiwizacji pozwala 16 dysków, 8 TB każdy, zamontowanych w rejestratorze, na których jest zapisywany obraz z blisko 60 kamer. Przewidziana jest dalsza rozbudowa systemu, stąd zastosowanie rejestratora 128-kanałowego. Zdalny dostęp ułatwia natomiast codzienną obsługę urządzenia.
Prywatny zakład przemysłowy. W takim obiekcie istotna jest doskonała jakość obrazów oraz długi czas przechowywania nagrań. W tym wypadku okazało się, że z czasem 128 kanałów w rejestratorze to zdecydowanie za mało. Konieczne było dołożenie drugiego tego typu urządzenia do obsługi nowych kamer, których w systemie łącznie jest już ponad 200. Obsługa na stacji monitoringu odbywa się za pośrednictwem aplikacji BCS Manager, za pomocą której jest prowadzony dodatkowy backup nagrań z całego systemu.

Robert Sienkiewicz

Project Manager
w Dahua Technology Poland

Bezpieczeństwo obiektów przemysłowych i rozproszonych

Systemy zabezpieczeń w obiektach przemysłowych, często rozproszonych na dużym obszarze, powinny być dobrane do wymagań danego sektora przemysłu, aby w sposób ciągły i skuteczny utrzymać procesy produkcyjne i logistyczne.
Chciałbym zwrócić uwagę na trzy interesujące przykłady zastosowania systemów zabezpieczenia technicznego. Pierwszy z nich jest oparty na technologii *machine vision*, która już dawno wyszła poza ramy rozwiązań przemysłowych, wkraczając również m.in. do branży security. Kolejne dwa dotyczą powiązania istniejących rozwiązań z technologiami przyszłości.

Ochrona wjazdu do obiektów przemysłowych – system skanowania podwozia pojazdów
System jest predestynowany m.in. do ochrony obiektów infrastruktury krytycznej, przemysłu wojskowego, narażonych na ataki terrorystyczne i szpiegostwo przemysłowe. Zapewnia pełną informację o czasie wjazdu i wyjazdu pojazdu, jego numerze rejestracyjnym i marce oraz – co ważne – czy pod autem nie zainstalowano niebezpiecznych przedmiotów (bomba, broń, nadajniki lub nośniki danych. Na przykład skanerem DH-MV-VDF5020CE-00 można skanować pojazdy o szerokości do 4,5 m poruszające się z prędkością nawet do 80 km/h, zarówno auta osobowe, jak i ciężarowe z naczepą. Wykorzystuje technologię widzenia maszynowego opartą na kamerze linijkowej, zapewniając wysoką rozdzielczość obrazu. Zastosowanie tego typu rozwiązania podnosi znacząco poziom kontroli wjazdu auta na teren chroniony.

Ochrona obwodowa obiektów IK – wizualizacja systemów w wirtualnej rzeczywistości
W ochronie perymetrycznej świetnie sprawdzają się radary (np. PFM861-B300) zintegrowane z kamerą PTZ. Radar wykrywa poruszający się obiekt i wysyła do kamery PTZ dokładną informację o jego lokalizacji i szybkości poruszania się. Kamera PTZ na tej podstawie zaczyna śledzić obiekt. Dotychczas proces śledzenia z radaru był przedstawiany na mapie 2D, nie zawsze w sposób intuicyjny. Znaczące udogodnienie zostało opracowane w Wojskowej Akademii Technicznej przez dr. Marka Piszczka, który przeniósł funkcjonalności systemu do wirtualnej rzeczywistości, co pozwoliło na określenie lokalizacji obiektu w przestrzeni 3D.

Szybkie reagowanie na zagrożenia – kamery nasobne jako element centralnego systemu nadzoru obiektu
Oprócz zabezpieczenia samego wjazdu na teren obiektu i ochrony obszarów otaczających obiekt bardzo ważnym aspektem jest szybkie reagowanie na zagrożenia wewnątrz obiektu – wtargnięcie osoby niepowołanej, pożar, wyciek wody, wypadek. Dzięki zastosowaniu kamer nasobnych (np. MPT310) można łatwo zwizualizować na mapie 3D lokalizację pracowników ochrony, wybrać najbliższą osobę, skomunikować się z nią w celu skutecznego przeprowadzenia inspekcji zagrożenia, a także przejąć obraz z akcji, aby dynamicznie zareagować na zmieniającą się sytuację. Są to kluczowe elementy, o których często zapominamy, ponieważ system monitoringu wizyjnego nie zawsze przedstawi nam pełen wgląd w sytuację.

Zastosowanie metod wizualizacji również w systemach integrujących PSIM przyniosłoby ogromne korzyści w sprawnym zarządzaniu w obiekcie z wieloma urządzeniami rozproszonych systemów CCTV, KD, SSP, SSWiN, DSO.

Reasumując, *machine visio*n tworzy nową generację zaawansowanych systemów nadzoru, które pozwalają zredukować liczbę personelu (zmniejszyć koszty), ale przede wszystkim wspomóc operatora w podejmowaniu kluczowych decyzji.
Rozwiązania osadzone w wirtualnej rzeczywistości to nowy wymiar w wizualizacji i kontakcie systemu z jego operatorem. W przyszłości sygnały z różnych urządzeń będą narzędziem w rękach programistów tworzących mobilne systemy zabezpieczenia technicznego. Zarządzanie nimi nie będzie wymagało w pełni wyposażonego centrum nadzoru, a zostanie zawężone do komputera i gogli VR.

Łukasz Lik

Hikvision Polska

Wyzwania nowej rewolucji przemysłowej

We współczesnym świecie, idącym śmiałym krokiem w kierunku „Przemysłu 4.0", automatyzacja, uczenie maszynowe czy sztuczna inteligencja odgrywają coraz bardziej znaczącą rolę i oferują rozwiązania przyczyniające się do zwiększenia wydajności i optymalizacji kosztów. Nowa rewolucja przemysłowa, jak zwykło się ją określać „Przemysł 4.0", przyniosła także nowe wyzwania. Powszechna informatyzacja systemów odpowiedzialnych zarówno za procesy produkcji, jak i bezpieczeństwo, wymusza na menedżerach ds. bezpieczeństwa zmiany podejścia do systemów zabezpieczeń. Jeszcze niedawno ich uwaga w całości skupiała się na bezpieczeństwie fizycznym obiektu. Teraz nieświadomy pracownik wkładający zainfekowaną pamięć USB do swojego komputera może stworzyć większe zagrożenie niż bezpośrednia próba włamania czy kradzieży. Co pokazuje, że mając nawet sieć IT podzieloną na segmenty lub nawet całkowicie pozbawioną połączenia z Internetem, nadal można stać się ofiarą ataku.
Ostatni atak na sieć WiFi przedsiębiorstwa przeprowadzono przez mikrokontroler Raspberry PI z modułem radiowym, wysłanym kurierem do pracownika, który to pochwalił się w mediach społecznościowych, że jest na urlopie. Paczka leżała na recepcji, pomału odszyfrowując dostęp do sieci. To na szczęście były tylko testy penetracyjne, jednak i takich scenariuszy nie można wykluczyć.
To wszystko pokazuje, że bezpieczeństwo fizyczne i cyberbezpieczeństwo będą się ze sobą łączyć w następnych latach. Przedsiębiorstwa staną przed kolejnym wyzwaniem – kosztami wdrażania zabezpieczeń. Mówimy tu o modernizacji infrastruktury, systematycznej konserwacji urządzeń oraz o profesjonalnej wyszkolonej kadrze pracowników. Aby zminimalizować ryzyko, organizacje muszą także czasem wyjść poza ograniczenia dzisiejszych przepisów i zastanowić się, jak sobie poradzą po poważnym ataku, biorąc pod uwagę coraz większe kary za wycieki wrażliwych danych.

Krzysztof Kunecki

Schrack Sconet

Zarządzanie bezpieczeństwem pożarowym obiektów rozproszonych

Obiekty o strukturze rozproszonej, do których zaliczamy m.in. rozległe zakłady przemysłowe, wymagają wdrożenia specjalnych procedur bezpieczeństwa i doboru odpowiednich urządzeń zapewniających szybką reakcję na zdarzenia krytyczne, takich jak alarm pożarowy.

Aby zapewnić możliwość centralnego zarządzania bezpieczeństwem obiektów rozproszonych, należy zadbać o odpowiednio zabezpieczoną infrastrukturę techniczną do komunikacji oraz centralny system do zarządzania bezpieczeństwem pożarowym. W praktyce najczęściej wdraża się następujące rozwiązania:

- centralny system nadzoru oparty na oprogramowaniu narzędziowym systemu sygnalizacji pożarowej, wykorzystywany do nadzoru oraz wspomagania serwisu i konserwacji instalacji sygnalizacji pożarowej,
- certyfikowany centralny system zarządzania bezpieczeństwem pożarowym, integrujący wszystkie systemy mające wpływ na bezpieczeństwo pożarowe obiektu, który w porównaniu z pierwszym rozwiązaniem pozwala również na zdalną obsługę i zarządzanie zintegrowanymi instalacjami.

Optymalnym wyborem dla zarządcy (właściciela) obiektu jest zastosowanie drugiego rozwiązania, a więc dedykowanego zintegrowanego systemu zarządzania bezpieczeństwem pożarowym, który umożliwia realizację m.in. następujących funkcji:

- wizualizację wszystkich stanów pracy i zdalną obsługę zintegrowanych systemów wspomaganą instrukcjami postępowania dla operatora w przypadku wystąpienia alarmu czy awarii,
- szybką ocenę sytuacji i reakcję na zdarzenie, takie jak alarm pożarowy, na podstawie obrazu z zagrożonego obszaru przy współdziałaniu z systemem dozoru wizyjnego (VSS),
- wsparcie w zakresie codziennej eksploatacji oraz zarządzania czynnościami serwisowymi i konserwacją systemów (elektroniczna książka eksploatacji),
- zdalne zarządzanie instalacjami z wdrożonymi funkcjami bezpieczeństwa ciągłości działania poprzez zastosowanie funkcji bezpieczeństwa w zakresie parametrów technicznych (redundancja połączeń) oraz warunków organizacyjnych (zapewnienie ciągłości realizowania funkcji sterowania/obsługi w przypadku awarii komunikacji/zasilania przez odpowiednie narzędzia i procedury operatorów lokalnych).

Krzysztof Pohorecki

dyrektor ds. Bezpieczeństwa w NOVAGO (China Everbright International)

Zrozumiała komunikacja największym wyzwaniem

Bezpieczeństwo obiektów przemysłowych to „temat rzeka", a zapewnienie jego spójnego i wysokiego poziomu w strukturze rozproszonej to morze, do którego ta rzeka wpływa. Galopujący postęp technologiczny daje wiele możliwości wspomagania i automatyzowania procesów, ale otwiera równolegle nowe obszary ryzyka. Skuteczna odpowiedź na coraz bardziej skomplikowany i coraz mniej zrozumiały dla ogółu świat cyfrowych zagrożeń wymaga transformacji klasycznego pojmowania bezpieczeństwa, a przede wszystkim głębokiej zmiany sposobów komunikacji oraz nabycia nowej wiedzy i umiejętności na wszystkich poziomach organizacji.

W mojej opinii największym wyzwaniem dla bezpieczeństwa w ogólności, a siłą rzeczy również w przemyśle, i to niezależnie od struktury, jest skuteczna komunikacja pozwalająca na zrozumienie współczesnych zagrożeń, ale również sposobów, narzędzi i coraz bardziej skomplikowanych systemów zabezpieczeń. Szczególnie ostatnio obserwuję coraz większy rozdźwięk w komunikacji pomiędzy „światem cyfrowym" a „światem realnym". Język jednego staje się coraz bardziej niezrozumiały dla drugiego.

Wymagania, jakie stawia technologia i tempo jej rozwoju, powodują paradoksalnie coraz większe problemy z jej implementacją. Ludzie i organizacje zajmujący się wysoko zaawansowanymi technologiami i systemami kreują własny, coraz bardziej hermetyczny świat i język, tym samym powoli coraz bardziej oddalają się od ludzi i organizacji, dla których te systemy tworzą. „Świat cyfrowy" daje tyle możliwości ataku, nie dając szansy na adekwatną obronę, że największe gospodarki świata w swoich krytycznych obszarach zaczynają powracać do starych, „analogowych" metod zabezpieczeń i świata, który rozumieją i są w stanie kontrolować.

„Wojna światów" może przebiegać bez udziału obcych cywilizacji. Możemy ją wywołać sami, a jej wynik może być dla nas niekorzystny. „Plemię analogowe" i „plemię cyfrowe" coraz bardziej oddalają się od siebie i coraz mniej się rozumieją.

Piotr Kiliszek

pełnomocnik Zarządu ds. bezpieczeństwa grupy kapitałowej Jastrzębska Spółka Węglowa

Ochrona spełniająca standardy

Obecnie przy zapewnieniu bezpieczeństwa obiektów rozproszonych borykamy się z brakiem wykwalifikowanego personelu, który oprócz uprawnień posiada kompetencje do zarządzania coraz bardziej profesjonalnymi systemami monitoringu. Chcąc profesjonalnie zabezpieczyć majątek wart miliardy złotych, niezbędne są wysoko wykwalifikowane kadry, którym przywrócimy etos pracy w ochronie. Konieczna jest zmiana mentalności i podejścia do tematyki ochrony. W przypadku obiektów o rozproszonej infrastrukturze wciąż dominują ochrona fizyczna i proste zabezpieczenia techniczne. Brak incydentów przynoszących wymierne szkody nie powinien uśpić czujności i chęci do rozwoju wśród osób odpowiedzialnych za bezpieczeństwo. W dobie przestępstw o różnym podłożu na świecie stale podnosi się standardy, jakim musi sprostać ochrona. Polska nie może zostać w tyle, gdyż stanie się teatrem takich działań. Obniżanie standardów światowych albo brak zabezpieczenie szczególnie w obiektach IK, nie powinno mieć miejsca. Dlatego też należy poszukiwać nowych możliwości i zwiększać efektywność posiadanego potencjału. Rosnące wymagania stawiane ochronie wymuszą zmianę podejścia i stosowanych rozwiązań. Nie dotyczy to wyłącznie pojedynczych przedsiębiorstw, ale całego sektora ochrony. Wyzwaniem, które czeka branżę, jest spowodowanie, aby organy opiniujące i zatwierdzające plany ochrony zmieniły nastawienie i zezwalały na znacznie szerszy dozór w formie elektronicznej. Przy rosnących kosztach zatrudnienia pracowników takie rozwiązanie staje się coraz bardziej opłacalne. Rachunek ekonomiczny, który niejednokrotnie ogranicza zastosowany poziom zabezpieczenia majątku, stanie się więc sprzymierzeńcem we wprowadzaniu nowych technologii i sposobu myślenia o ochronie jako takiej. Należy poważnie myśleć również o wykorzystaniu dronów na zdecydowanie większą skalę. Widzę tu dwa zastosowania: regularne patrolowanie obszarów oraz wsparcie ochrony perymetrycznej poprzez działania *first responders* przy weryfikacji sygnałów naruszenia stref chronionych.

Aby jednak zmienić model ochrony na wskazany przeze mnie, niezbędne jest wdrożenie na szerszą skalę rozwiązań umożliwiających wykorzystanie dronów autonomicznych. Systemy takie są w fazie uzyskiwania akredytacji instytucji odpowiadających za ruch lotniczy. Zapewne stanie się to wkrótce i będziemy mieli do czynienia z formą swoistej rewolucji w ochronie przedsiębiorstw, których infrastruktura jest rozproszona, obiektów branży elektroenergetycznej czy kolejowej.

Tomasz Gonta

Security Manager Agri Plus/Animex

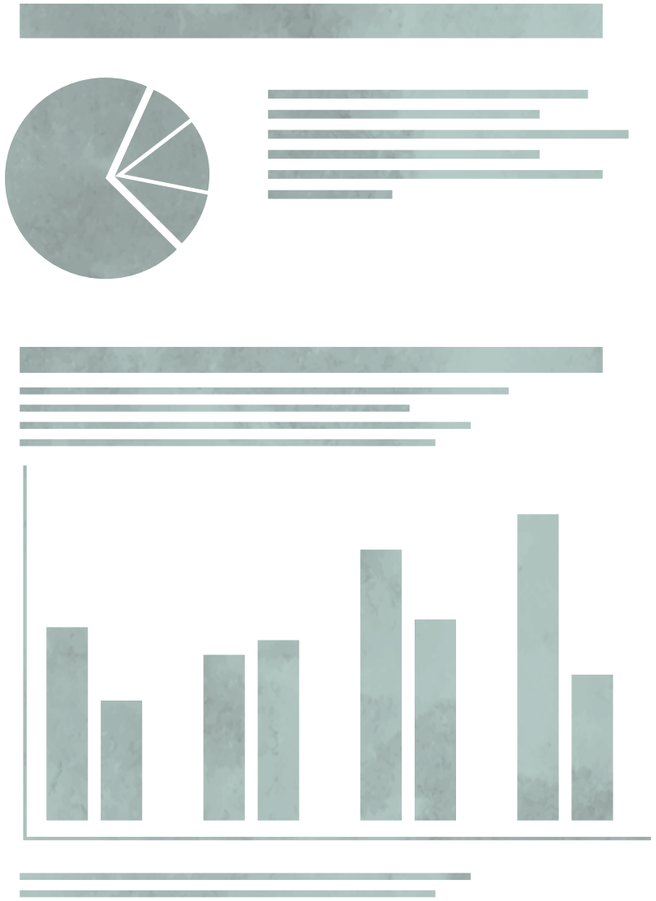
Automatyzacja procesów pozwoli na oszczędności

Rosnące z roku na rok płace minimalne pociągają za sobą wzrost cen usług opartych przede wszystkim na pracy człowieka. Zapewnienie ochrony obiektów rozproszonych, w rozsądnych kosztach, staje się coraz trudniejsze. Do tej pory w tym zakresie dążyło się do standaryzacji. Łatwiej zarządzać ochroną wielu obiektów, kiedy łańcuch osób decyzyjnych jest ograniczony do minimum, a standardy obowiązujące wszystkich – od pracowników szeregowych, po ich nadzór i procedury – są takie same w każdym obiekcie. Kierunek szukania oszczędności wydaje się więc oczywisty: automatyzacja procesów ochrony, zastępowanie ochrony fizycznej zabezpieczeniami technicznymi. Na rynku mamy mnóstwo rozwiązań i no-

winek technicznych. Elektronika nie śpi, nie chodzi na urlopy i zwolnienia lekarskie, tanieje w szybkim tempie. Niestety mimo zaawansowania technologicznego nie jest w stanie zastąpić, w każdym przypadku, pracownika ochrony. Jest ciągle wiele zadań wynikających ze specyfiki i profilu konkretnych obiektów i profili produkcji, determinujących obecność pracownika fizycznego.

Zapewne można się ze mną nie zgodzić, uważając, że wszystko da się zastąpić odpowiednimi rozwiązaniami technicznymi. Jednak w biznesach niskomarżowych nie ma olbrzymich kwot na rozwiązania techniczne, takich jakie pozwoliłyby wybierać rozwiązania z górnych półek, dużo bardziej dopracowane. Poza tym nawet najnowocześniejsze zabezpieczenia ciągle mają jeszcze mankamenty. Przykładem mogą być drony, których użycie staje się coraz bardziej popularne, to jednak ogniwa zasilające cały czas są niedoskonałe i nieefektywne. Przykład dronów pokazał też, że wykorzystywanie obcych rozwiązań może wiązać się z ryzykiem szpiegostwa przemysłowego lub co gorsza militarnego.

Jedyna nadzieja w tym, że technika będzie się dalej rozwijała w szybkim tempie, chociaż moim zdaniem to tempo niestety zwalnia. W wielu rozwiązaniach stanęliśmy przed problemami, które wymagają albo dużych nakładów pieniężnych, albo dużo czasu do ich optymalizacji. W oczekiwaniu na rozwój i spadek cen zabezpieczeń technicznych pozwolę sobie pół żartem, pół serio stwierdzić, że nie pozostaje nam innego, jak płacić frycowe lub w ostateczności, szukając oszczędności, przywrócić do łask regionalne firmy ochrony. Mają one mniejsze koszty nadzoru i są w stanie zapewnić usługę taniej. Przysporzyłoby to ponownie wszystkim więcej pracy i oznaczało oczywisty krok wstecz. Chociaż ktoś kiedyś powiedział, że „czasem trzeba zrobić krok w tył, by móc pójść naprzód". Uważam, że najbliższe pięć lat będzie dość kluczowe dla firm ochrony i spozycjonuje na nowo ten rynek i ochronę przedsiębiorstw rozproszonych.



Daniel Szyszko

administrator systemów bezpieczeństwa, DCT Gdańsk SA Deepwater Container Terminal Gdańsk

Najnowsza technologia pomaga w zapewnieniu bezpieczeństwa

Z punktu widzenia bezpieczeństwa terminala kontenerowego, stanowiącego granicę państwa najważniejszym aspektem jest ochrona granic od strony morza, lądu i powietrza. Kwestie bezpieczeństwa są rozpatrywane w oparciu o szereg procedur oraz w odniesieniu do Międzynarodowego kodeksu ochrony statku i obiektu portowego (Kodeks ISPS), którym podlega zarówno terminal, jak i każdy wpływający statek.

Największym z naszego punktu widzenia zagrożeniem są obecnie akty terrorystyczne, kradzieże oraz przemyt. Priorytetem dla nas jest stały monitoring wizyjny całego terminala wraz z jego granicami, kontrola wszystkich osób wchodzących i wychodzących, reagowanie na każde niestandardowe zachowanie oraz właściwa współpraca z załogami statków. W związku z tym staramy się rozwiązywać wszystkie te problemy, korzystając z nowych technologii monitoringu wizyjnego przestrzeni otwartych. Stosujemy wszelkiego rodzaju kamery, w tym termowizyjne, obrotowe z funkcją śledzenia obiektu. Ruch każdej osoby na obszarze terminalu jest dodatkowo monitorowany poprzez system kontroli dostępu.

Sprawdzoną koncepcją jest również integracja wszystkich systemów bezpieczeństwa w jeden spójny integralny SMS, czyli system zarządzania bezpieczeństwem w obiekcie. Niezastąpiona jest również ochrona osobowa w postaci stałych patroli ochrony. Zdajemy sobie sprawę, że wraz z postępem technologicznym zmieniają się również możliwe zagrożenia. Chcąc wyjść im naprzeciw, nasza firma podąża tym nurtem i wprowadza coraz to nowsze technologie pomocne w zapewnieniu bezpieczeństwa od strony morza, lądu i powietrza.

Jakub Sobek

Linc Polska

Perymetria i teleinformatyka

Dyskusje o bezpieczeństwie obiektów przemysłowych często dotyczą głównie zakładów produkcyjnych i wytwórczych. Gospodarka jednak się zmienia i coraz częściej obiekty przemysłowe obejmują także centra danych, serwerownie lub biura obsługi klienta.

Pożar na początku 2019 r. w hali sąsiadującej z centrum danych jednego z operatorów komórkowych spowodował, że klienci tej firmy przez kilka dni mieli poważne problemy z dostępem do niektórych usług, nie mogli też korzystać z telefonicznego wsparcia biura obsługi klienta. Choć na skutek pożaru urządzenia w serwerowni nie ucierpiały poważnie, to z powodu zniszczenia budynku konieczne było przeniesienie całej serwerowni. Przestoje w pracy zawsze są kosztowne, a dodatkowo ich konsekwencją są straty wizerunkowe, które trudno wycenić. Obnaża to podatność różnych miejsc na możliwe zagrożenia, pokazując przy tym, jak istotne jest właściwe zabezpieczenie obiektów za pomocą systemów ppoż.

Warto pamiętać, że czasami istnieje możliwość detekcji pożaru jeszcze przed jego wystąpieniem. Z pomocą przychodzą radiometryczne kamery termowizyjne, które mogą np. obserwować wybrany obszar serwerowni i stale monitorować zmiany temperatury. Jeśli na jakimś urządzeniu system wykryje ciągłą tendencję wzrostu temperatury, może wygenerować alarm. W jego wyniku będzie można np. wymienić wadliwy (przegrzewający się) zasilacz, zanim jeszcze dojdzie do jego samozapłonu. Mamy nie tylko poprawę zabezpieczenia i funkcjonowania całej infrastruktury, lecz także wzrost bezpieczeństwa pracujących i przebywających w danym obiekcie osób.

Bardzo istotne jest stworzenie także szczelnej strefy ochronnej wokół takiego budynku. Wysoki poziom bezpieczeństwa zapewnia sensoryczny przewód światłowodowy instalowany na ogrodzeniu. Umożliwia on wczesną detekcję intruza przechodzącego przez ogrodzenie, ponadto wykrywa przecinanie lub nawet próby unoszenia ogrodzenia. Kontroler światłowodowy może być także stosowany do ochrony teletechnicznej instalacji światłowodowej. Takie urządzenie pozwala na detekcję fizycznej ingerencji w światłowód telekomunikacyjny. Dzięki takim rozwiązaniom zapewniamy zarówno ochronę perymetryczną, jak i teleinformatyczną. Warto o tym pamiętać, projektując system zabezpieczeń.

Agnieszka Pitrus

SATEL

Systemy sygnalizacji włamania i napadu a ochrona obiektów przemysłowych

W obiektach przemysłowych, które coraz częściej są obarczone średnim, a nawet wysokim ryzykiem włamania, kluczowym zagadnieniem jest zapewnienie ciągłości ochrony oraz natychmiastowej reakcji na niepożądane zdarzenia. Dlatego też wdrażane elektroniczne zabezpieczenia techniczne, w tym SSWiN, muszą skutecznie zapobiegać wtargnięciu osób nieuprawnionych i wywieraniu przez nie negatywnego wpływu na newralgiczne elementy budynków oraz znajdujące się tam mienie. Jednocześnie system alarmowy powinien oferować szerokie możliwości w zakresie integracji z innymi systemami zabezpieczeń: kontrolą dostępu, monitoringiem wizyjnym i sygnalizacją przeciwpożarową. Zastosowane rozwiązania powinny być realizowane równolegle z ochroną fizyczną, świadczoną przez specjalistyczne służby i wspomagać oraz ułatwiać ich codzienną pracę.

Rozważając takie zabezpieczenie, trzeba brać pod uwagę różne aspekty. Należy zacząć od tego, że instalacja chroniąca wnętrza powinna spełniać wymagania odpowiednich aktów normatywnych, np. EN 50131 Grade 3 w przypadku obiektów infrastruktury krytycznej. W efekcie musi zapewniać m.in. szyfro-

wanie danych, sprawną wielotorową komunikację oraz mechaniczną odporność na czynniki środowiskowe, akty wandalizmu czy sabotaż polegający np. na próbach demontażu poszczególnych elementów systemu. Trzeba też pamiętać o tym, że obiekty przemysłowe to często rozległe zespoły budynków wymagające ochrony nie tylko wewnątrz, lecz także na zewnątrz. Dlatego wymagają zastosowania niezawodnych urządzeń najwyższej klasy, które mogą pracować w szerokim zakresie temperatury, w trudnych warunkach środowiskowych i są odporne na zakłócenia. W przypadku sieci zabezpieczanych obiektów strategicznym rozwiązaniem może okazać się wdrożenie oprogramowania integrującego – zapewniającego efektywne administrowanie systemami zabezpieczeń rozproszonych placówek i ich użytkowników, pozwalającego na optymalizację kosztów i oszczędność czasu. Wszystko po to, aby zarządzanie bezpieczeństwem było łatwe, wygodne i, co najważniejsze, skuteczne.

Janusz Syrówka

Dział Bezpieczeństwa/Country Security Chair, innogy Polska SA

Nowe podejście do zapewnienia ochrony

Ochrona rozproszonych obiektów przemysłowych, a zwłaszcza związanych z zapewnieniem świadczenia usług kluczowych (energetyka, telekomunikacja, wodociągi itp.) wymaga dziś nowego podejścia. Tradycyjnie koncentrowała się na zabezpieczeniu mienia przed kradzieżą lub zniszczeniem oraz uniemożliwieniu dostępu osobom nieuprawnionym. Bezpieczeństwo takich obiektów można było potraktować lokalnie i bardzo często poprzestać na środkach fizycznych, takich jak ogrodzenia, kraty w oknach czy

drzwi odporne na włamanie. Współczesne zagrożenia zmuszają do innego spojrzenia na obiekt ochrony. Informatyzacja oraz zaawansowane rozwiązania w dziedzinie automatyki przemysłowej definitywnie zamykają erę traktowania obiektów rozproszonych jako pojedynczych punktów na mapie. Obecnie tworzą one łańcuch lub raczej sieć z bardzo skomplikowanymi powiązaniami. Ma to wpływ na znaczenie (rolę) poszczególnych elementów (często niedoszacowanych w tradycyjnym podejściu do bezpieczeństwa), a także otwiera możliwość oddziaływania w przypadku sabotażu cybernetycznego poprzez jeden element na pozostałe elementy systemu. Aby skutecznie zabezpieczyć sieć obiektów, system bezpieczeństwa musi także funkcjonować jako sieć.

Stan bezpieczeństwa musi być monitorowany nieprzerwanie, a informacja o tym przekazywana w czasie rzeczywistym. Przetworzenie (jego jakość i szybkość) dużej ilości informacji weryfikuje kolejny tradycyjny element związany z bezpieczeństwem – centralny ośrodek monitorowania. Informacje związane z bezpieczeństwem obiektów służą, rzecz jasna, tradycyjnym celom, takim jak podjęcie interwencji w celu powstrzymania np. aktu wandalizmu, jednak jest to dalece niewystarczające. Stan obiektu może mieć wpływ na działanie systemu, zatem informacja o zagrożeniu musi trafiać do dyspozytora systemu.

Ważnym elementem jest także zapewnienie przepływu informacji do ośrodków bezpieczeństwa związanych z bezpieczeństwem IT i OT *(Security Operation Center)*. Sprawne zarządzanie bezpieczeństwem w takich obiektach wymaga zapewnienia efektywnej klasyfikacji i dystrybucji informacji o stanie bezpieczeństwa. Jeśli dołożymy do tego wymóg funkcjonowania w czasie rzeczywistym, w grę muszą wchodzić rozwiązania częściowo lub całkowicie zautomatyzowane. Do tego dochodzą też problemy związane z komunikacją pomiędzy obiektami a ośrodkami monitorowania, a także te zupełnie już przyziemne dotyczące utrzymania systemu bezpieczeństwa w należytej sprawności. Wyzwań jest aż nadto, nie wspominając o kwestiach związanych z kosztami.

Paweł Grzywa

dyrektor ds. kluczowych klientów, Securitas Polska

Inżynier bezpieczeństwa

Bezpieczeństwo obiektów przemysłowych jest pojęciem bardzo szerokim. Nawet gdy mówimy o obiektach rozproszonych, ale o podobnym charakterze, uwzględniając rozmieszczenie infrastruktury wewnętrznej, bram wjazdowych, dróg komunikacyjnych dla pieszych, a także obowiązujące procedury, to i tak punktem wyjścia musi być indywidualna analiza ryzyka i audyt bezpieczeństwa. Wyniki takich audytów, nawet w obiektach o bardzo zbliżonych formatach, mogą się znacznie różnić. Przytoczę przykład jednego z naszych klientów, u którego standardowo przed rozpoczęciem współpracy przeprowadziliśmy audyt bezpieczeństwa. Wynik był pozytywny i wskazywał na wysoki poziom zabezpieczeń. Drobne zalecenia, jakie rekomendowaliśmy, klient szybko wdrożył.

Niemniej jednak nasza metodyka audytowa rekomenduje sprawdzenie również otoczenia obiektu. I tak w naszym raporcie pojawiła się informacja o nie w pełni drożnym przepuście wodnym strumyka płynącego wzdłuż ogrodzenia, poza terenem zewnętrznego parkingu. Przepust ten znajdował się pod mostkiem prowadzącym do głównej bramy zakładu, z tego też powodu problem z jego drożnością mógł mieć wpływ na poziom bezpieczeństwa biznesu naszego klienta.

Nasza rekomendacja udrożnienia przepustu wodnego oraz poszerzenia kanału wodnego nie została jednak wdrożona. W czasie lokalnych podtopień skumulowana woda rozlała się na parking, podmywając jego podłoże. W efekcie część pojazdów zapadła się, ulegając uszkodzeniu. Woda wdarła się także na posterunek ochrony oraz do części hal produkcyjnych. Ciągłość procesu produkcji została zatrzymana, a to wiązało się z wymiernymi stratami finansowymi i wizerunkowymi.

Analizując bezpieczeństwo obiektów przemysłowych, coraz częściej zwraca się uwagę na łączenie czynnika ludzkiego (w ograniczanej obecnie liczbie pracowników i posterunków ze względu na postępujący proces automatyzacji i koszty pracy), z technologią, która poza standardowymi systemami sygnalizacji włamania i kontroli dostępu uwzględnia również ochronę perymetryczną.

System ochrony obwodowej wyposażony w kamery z zaawansowanymi funkcjami analitycznymi i systemami audio jest obecnie efektywną formą ochrony obiektów przemysłowych. System służy nie tylko do weryfikacji sygnałów alarmowych i odstraszania intruzów, ale również usprawnia ewakuację. Wszystkie zastosowania mają wpływ nie tylko na poprawę poziomu bezpieczeństwa, ale również na optymalizację posterunków obchodowych. Można również zintegrować wszystkie występujące w obiekcie systemy zabezpieczeń technicznych za pomocą dostępnych na rynku platform. Ma to znaczący wpływ na poziom obsługi obiektów, szybkość i jakość raportowania incydentów oraz dalszą ewentualną optymalizację posterunków.

Oczywiście nie należy zapominać, że wszystkie te działania muszą być skoordynowane przez pracownika ochrony, który z racji postępującego zaawansowania systemów powoli staje się „inżynierem ochrony" wspieranym przez skuteczne narzędzia do bieżącego raportowania. Takim narzędziem jest stosowany w Securitas system Vision, od lat z powodzeniem działający w wielu krajach Grupy Securitas. Jest to doskonałe narzędzie koordynujące pracę w obiektach, zwłaszcza rozproszonych, transparentne i co ważne – dostępne online dla klientów. Security manager może dzięki systemowi Vision szybko zweryfikować informacje o stanie bezpieczeństwa obiektu, składzie zespołu ochrony, incydentach, jakie miały miejsce, a także dowiedzieć się, jakie czynności w zakresie bezpieczeństwa obiektu zostały zaplanowane do wykonania.

Jacek Tobiasz

Security Manager/Privacy & Compliance Officer, Grupa Żywiec SA

Najważniejsza jest ocena ryzyka obiektu

Moje życie zawodowe od zawsze jest związane z przeciwdziałaniem naruszeniom zasad postępowania w biznesie oraz reguł prawa. Jednym z obszarów, którymi się zajmuję od wielu lat, jest też projektowanie i wdrażanie rozwiązań tworzących bezpieczne środowisko i infrastrukturę także dla rozproszonych obiektów przemysłowych.

Na podstawie osobistych doświadczeń uważam, że nie można efektywnie stosować tego samego wzorca czy schematu, który sprawdził się w jednej spółce, i kopiować go bez refleksji do innej. Projektowanie rozwiązań zapewniających bezpieczeństwo ludziom i towarom powinno zatem być oparte na indywidualnej i rzetelnej ocenie rzeczywistych dla danego obiektu rodzajów ryzyka.

Tradycyjne podejście oparte na zapewnianiu kontroli realizowanej przez pracownika ochrony to rozwiązanie obarczone szybko rosnącymi kosztami i niestety zawodne w praktyce.Powoli przechodzi do lamusa. Dziś, działając w warunkach ostrej konkurencji, zapewnienie bezpiecznego dla działalności spółki środowiska, wolnego od istotnych rodzajów ryzyka jest jednym z elementów, których nie sposób pominąć.

Wyzwaniem będzie zatem stworzenie maksymalnie efektywnego, „uszytego na indywidualną miarę" przyjaznego dla biznesu, wspierającego (a nie komplikującego) codzienne operacje, konkurencyjnego także pod względem kosztowym systemu bezpieczeństwa dla obiektów rozproszonych. Mam na myśli korzystanie z dostępnych narzędzi i systemów oraz najnowszych technologii, a także możliwości integracji różnych systemów (nie tylko służących bezpieczeństwu), by zbudować efektywny, ale nie generujący zbyt wysokich kosztów stałych system zapewniający bezpieczne i wolne od zagrożeń środowisko dla prowadzonej działalności.

W dobie ostrej konkurencji i rywalizacji na rynku, także w obszarze kosztów, aby móc zwyciężać, trzeba odważnie korzystać z kreatywnych, innowacyjnych, nowatorskich i nowoczesnych rozwiązań, szytych na miarę.

Musimy też akceptować małe ryzyka, starając się je minimalizować. Ich niwelacja mogłaby być znacznie droższa niż potencjalna wartość wyrządzonej szkody. Z drugiej zaś strony musimy stosować silne środki bezpieczeństwa dla każdego ryzyka krytycznego, mocno powiązanego z realizowanymi procesami operacji biznesowych.

Sektor energetyczny coraz częściej będzie ofiarą cyberataków

Kompleksowy rozwój bezpieczeństwa systemów IT i OT (*Operational Technology*) pozwoli uniknąć wielu sytuacji kryzysowych.

Określenie krytycznych systemów oraz dokonanie analizy i testów w celu wykrycia ich podatności na potencjalne cyberataki to kluczowy obszar, nad jakim powinny pracować firmy z sektora energetycznego, w szczególności w branży naftowo-gazowej (Oil&Gas). Autorzy raportu firmy doradczej Deloitte *An integrated approach to combat cyber risk. Securing industrial operations in oil and gas* ostrzegają, że w niektórych przypadkach nie jest potrzebna zaawansowana technologia czy wiedza, aby zaatakować wewnętrzne systemy informatyczne tych firm.

Straty finansowe i wizerunkowe, choć mogą być ogromne, należą do najmniej dotkliwych z możliwych skutków ataku na przedsiębiorstwo z sektora energetycznego. Efekty działania cyberprzestępców mogą być dużo bardziej rozległe i w skrajnych przypadkach oddziaływać na ludzkie zdrowie oraz życie. – *W Polsce szczególnie narażony na cyberatak jest sektor naftowo-gazowy. To właśnie operatorzy tego segmentu rynku, świadczący kluczowe usługi, stanowią strategiczny punkt na mapie nie tylko bezpieczeństwa gospodarczego czy obywateli, ale także całego kraju. To wynik aktualnej sytuacji geopolitycznej, w tym rywalizacji wielu grup wpływów. Operatorzy, ze względu na posiadane systemy automatyki przemysłowej i systemy IT, są grupą podwyższonego ryzyka* – mówi Piotr Borkowski, ekspert w obszarze cyberbezpieczeństwa w Zespole ds. Energii i Zasobów Naturalnych Deloitte.

Systemy (nie)bezpieczeństwa

W obliczu możliwych, niekiedy skrajnie różnych skutków cyberataków dziwić może niedostateczna dbałość o zabezpieczenie przed nimi lub zupełny ich brak. W wielu przypadkach twórcy systemów automatyki przemysłowej skupili się na ich niezawodności zamiast na potencjalnym zagrożeniu, jakie ich przejęcie np. przez terrorystów może oznaczać. – *Systemy IT oraz OT administrowane przez operatorów usług kluczowych mogą zostać zaatakowane zarówno przez grupy wynajęte przez konkurencyjne firmy, grupy działające na rzecz obcych państw, jak i zwykłych przestępców, którzy w takiej formie swojej aktywności mogą upatrywać zysku. Wskazane systemy muszą być również jak najlepiej przygotowane na kampanie globalne, które choć często są nieukierunkowane, to rykoszetem potrafią spustoszyć systemy niejednej dużej firmy. Tak wiele czynników ryzyka dla systemów IT oraz OT powinno skłaniać do podejmowania wszelkich dostępnych środków, aby maksymalnie ograniczyć ryzyko ich wystąpienia* – zaznacza Piotr Borkowski.

Eksperci Deloitte zwracają uwagę, że skuteczność tych działań zależy od połączenia wiedzy z zakresu IT i inżynierii oraz pogodzenia ich niekiedy rozbieżnych interesów. Specjaliści przemysłowych systemów sterowania nie zawsze bowiem w pełni rozumieją współczesne zagrożenia bezpieczeństwa informatycznego, podobnie jak specjaliści od bezpieczeństwa IT często nie rozumieją procesów przemysłowych. Bez wsparcia IT systemy sterowania produkcją niezwykle trudno jest zabezpieczyć. Wynika to m.in. z tego, że dziś funkcjonują jako część sieci, choć nie zostały do takiej interakcji zaprojektowane. Rozwój technologiczny sprzyja wydajności i obniżeniu kosztów, ale także otwiera przedsiębiorstwa na różne zagrożenia cybernetyczne.

Ostrzeżenie z USA

O skali zagrożenia najlepiej świadczą obserwowane od lat próby ataków. Już w 2003 r. jedna z amerykańskich elektrowni jądrowych w stanie Ohio została zainfekowana wirusem Slammer. Terroryści najpierw zaatakowali system firmy współpracującej z przedsiębiorstwem zarządzającym elektrownią. Potem łatwiej już było uderzyć w samą elektrownię, a wirus błyskawicznie atakował kolejne komputery. Slammer zablokował system odpowiedzialny za chłodzenie reaktora. Z kolei w 2014 r. zostały zhakowane systemy komputerowe operatora elektrowni jądrowej w Korei Południowej. Hakerzy z konkurencyjnych krajów nieustannie próbują wykraść informacje i technologie zachodnich firm energetycznych. Rozsyłają e-maile z zainfekowaną treścią, instalują szkodliwe oprogramowanie czy zmieniają treści na stronie internetowej atakowanej firmy. To ataki nieudane, gdzie straty są znikome lub nie było ich wcale. Ale w 2016 r. atak na ukraińską energetykę na dwa dni pozbawił prądu część Kijowa. Rok wcześniej w wyniku podobnego ataku 225 tys. mieszkańców zachodniej Ukrainy nie miało dostępu do energii elektrycznej. Przed cyberprzestępcami z Rosji na początku roku ostrzegał Departament Bezpieczeństwa Wewnętrznego (DHS) Stanów Zjednoczonych. Z jego analiz wynika, że scenariusz jest zazwyczaj podobny do tego w Ohio. Hakerzy atakują najpierw organizacje zewnętrzne, współpracujące z faktycznym celem ich ataku. Wirus rozprzestrzenia się poprzez zainfekowane konta pocztowe czy strony internetowe odwiedzane przez pracowników.

> Aby przedsiębiorstwo było bezpieczne, konieczne jest jego ciągłe monitorowanie oraz opracowanie mechanizmów wychwytujących potencjalny atak lub minimalizowanie jego skutków

Różne motywy, jeden cel

– *Nieznajomość wroga powinna być dużą zachętą do jak najlepszego zabezpieczenia systemów IT i OT. Dodatkowy akcelerator działań to wejście w życie w sierpniu 2018 r. ustawy o Krajowym Systemie Cyberbezpieczeństwa, która w odniesieniu do systemów IT i ich bezpieczeństwa narzuca na operatorów usług kluczowych dodatkowe wymagania* – mówi Piotr Borkowski.

Brak zabezpieczeń, nieprawidłowe testowanie systemów IT czy wdrażanie technologii bez wcześniejszych testów – to wszystko zostawia luki, z których mogą skorzystać cyberprzestępcy. Często pomijanym elementem w systemach bezpieczeństwa są także ludzie. Przez brak przeszkolenia w tym zakresie i wiedzy o ryzyku pracownicy przenoszą do systemu przedsiębiorstwa media zainfekowane złośliwym oprogramowaniem. Wiele osób wciąż jest przekonanych, że niepowodzenia czy awarie najczęściej są spowodowane warunkami atmosferycznymi, błędami ludzkimi i zmęczeniem sprzętu, a nie manipulacją cyberprzestępców.

Znalezienie podatności i ewentualnych błędów konfiguracyjnych w posiadanych systemach to priorytet dla firm naftowo-gazowych. Eksperci Deloitte zaznaczają, że pracę nad nimi powinien na bieżąco wykonać zespół specjalistów ds. biznesu, inżynierii i bezpieczeństwa IT. Niemożliwe jest zabezpieczenie wszystkiego w równym stopniu. Na szczycie listy powinny więc znajdować się krytyczne zasoby i infrastruktura. Aby przedsiębiorstwo było bezpieczne, konieczne jest jego ciągłe i automatyczne monitorowanie oraz opracowanie mechanizmów wychwytujących potencjalny atak lub minimalizowanie jego skutków. ▫

Deloitte

Biuro w Warszawie
al. Jana Pawła II 22
00-133 Warszawa

Bezpieczeństwo pożarowe instalacji technologicznych w przemyśle

TEKST
mgr inż. Janusz Sawicki
IBP NODEX

Ochrona technologii

Bezpieczeństwo procesów i instalacji technologicznych jest priorytetowym czynnikiem, zapewniającym ciągłość działania zakładów przemysłowych. W tej dziedzinie jednym z najważniejszych jest bezpieczeństwo pożarowe. Skutkiem pożaru są straty materialne spowodowane zniszczeniem urządzeń i surowców, przestojami w produkcji oraz czasami wręcz nieodwracalnymi zniszczeniami środowiska naturalnego.

Poziom bezpieczeństwa pożarowego powinny zapewniać takie rozwiązania, które

- po pierwsze, zapobiegają występowaniu warunków skutkujących wybuchem pożaru,
- po drugie, wykrywają pożar w bardzo wczesnej fazie jego rozwoju i skutecznie tłumią jego rozwój.

Zapobieganie występowaniu pożarów polega m.in. na przyjęciu i wdrożeniu rozwiązań organizacyjnych i technicznych. Rozwiązania organizacyjne polegają na opracowaniu odpowiednich procedur bezpieczeństwa związanych z procesem technologicznym, ich wdrożeniu, egzekwowaniu i nowelizacji – przynajmniej tych, które są związane ze zmianą technologii lub urządzeń.
Procedury powinny zawierać sposoby postępowania w przypadku wystąpienia sytuacji kryzysowych (w tym pożaru), typować miejsca newralgiczne i szacować ryzyko wystąpienia w nich sytuacji niebezpiecznych. Wdrożenie procedur jest związane przede wszystkim z treningiem personelu, który musi przyswoić sobie wzorce zachowań i umiejętność postępowania w sytuacjach nietypowych, mogących stać się sytuacjami kryzysowymi. Procedury takie powinny być zrozumiałe dla pracowników i nie budzić wątpliwości, które zawsze powodują zwłokę w reakcji personelu. Powinny m.in. zawierać opis negatywnego oddziaływania pożaru na zdrowie i życie ludzkie.
Trening personelu oparty na odpowiednim szkoleniu i ćwiczeniach powinien także skutkować odpowiednimi działaniami naprawczymi, nowelizacyjnymi itd. Po każdych ćwiczeniach należy przeprowadzić analizę mającą na celu usunięcie ewentualnych braków i niedoskonałości. Takie postępowanie na pewno podniesie poziom bezpieczeństwa, w tym bezpieczeństwa pożarowego.
Warunek drugi dotyczący wczesnego wykrycia pożaru i stłumienia go jeszcze w fazie nierozwiniętej (tłumienie pożaru ma na celu ograniczenie go w określonej przestrzeni i ugaszenie) polega na doborze odpowiednich urządzeń i instalacji przeciwpożarowych. Urządzenia i instalacje ppoż. są rozumiane w odniesieniu do zabezpieczenia technologii jako urządzenia ppoż. wymienione w definicji Ministra SWiA, jak i instalacje związane na stałe z technologią, urządzenia jednostkowe i specjalne wytworzone na potrzeby zabezpieczenia danego procesu technologicznego oraz urządzenia wspomagające, pozwalające na pewną weryfikację i ocenę zdarzenia pożarowego przez personel uprawniony.

W przypadku obiektów przemysłowych zawsze po wykonaniu i uruchomieniu instalacji bezpieczeństwa pożarowego należy ocenić ich skuteczność

Oczywiście w przypadku skomplikowanych i rozległych instalacji – zarówno technologicznych, jak i przeciwpożarowych – występuje problem współpracy na linii maszyna – człowiek. Współpraca taka ma na celu dostarczenie personelowi odpowiednich informacji o stanie instalacji bezpieczeństwa, które pozwolą mu na prawidłową ocenę zdarzeń w czasie rzeczywistym, podjęcie odpowiednich decyzji, a także dadzą zarówno personelowi, jak i jednostkom ratowniczo-gaśniczym (wewnętrznym i zewnętrznym) odpowiednie narzędzia pozwalające na reakcję w sytuacjach krytycznych.
Jest to związane z szeroko pojętą integracją urządzeń i instalacji ppoż., która może być realizowana za pomocą urządzeń integrujących. Urządzenia integracyjne – integratory mogą jednocześnie spełniać pierwszy warunek (zapobieganie pożarom), ponieważ mogą zawierać wszelkie niezbędne procedury postępowania oraz realizować i nadzorować czynności treningowe przeprowadzane w sposób ciągły, co jest niezmiernie ważne.

Wpływ warunków środowiskowych na działanie instalacji ppoż.

Wpływ warunków środowiskowych na poprawną pracę instalacji ppoż. jest jednym z kluczowych zadań, które należą do projektantów i wykonawców tych zabezpieczeń. Wprowadzane zakłócenia są skutkiem stałego oddziaływania środowiska na te instalacje (promieniowanie ultrafioletowe, wilgotność, atmosfera korozyjna, wyładowania atmosferyczne), a także specyfiki technologii, którą nadzorują (wibracje, promieniowanie elektromagnetyczne, zmienna temperatura, nadmierne zapylenie i zanieczyszczenie, bardzo wysoka wilgotność, oddziaływanie silnie korozyjne, atmosfera wybuchowa, zakłócenia pochodzenia elektrycznego). Przy doborze i ocenie późniejszych możliwości odpowiedniego utrzymania urządzeń i instalacji ppoż. należy brać pod uwagę oba rodzaje oddziaływań środowiska.

Oddziaływanie stałe środowiska ma wpływ na stan techniczny instalacji ppoż. i wymaga wdrożenia odpowiednich, adekwatnych do warunków środowiska działań przeglądowych, serwisowych i naprawczych. Takie podejście rzutuje jednocześnie na proces doboru urządzeń, nakazując inwestorom dobierać takie urządzenia i instalacje, dla których producent gwarantuje akceptowalny czas dostarczania części zamiennych.
Oddziaływanie środowiska wynikające ze specyfiki procesów technologicznych ma wpływ na proces doboru urządzeń ppoż. zarówno ze względu na ich odporność na tego rodzaju narażenia, jak i możliwość generowania przez nie fałszywych alarmów.

Spełnienie zarówno pierwszego, jak i drugiego warunku jest trudne do realizacji i wymaga dokładnej analizy i pomocy ze strony ekspertów. Tego rodzaju oddziaływania środowiskowe mają także znaczący wpływ na żywotność urządzeń i instalacji ppoż. Dlatego też w celu zabezpieczenia ppoż. instalacji technologicznych nie zawsze istnieje możliwość zastosowania przeciwpożarowych urządzeń posiadających odpowiednie certyfikaty. Najczęściej musimy stosować urządzenia ppoż. specjalne o odpowiedniej konstrukcji, które zagwarantują poprawną pracę w trudnych warunkach środowiskowych. W takich przypadkach należy zawsze udowodnić skuteczność tych urządzeń do wykrywania spodziewanych rodzajów pożarów w konkretnej konfiguracji, które mogą wystąpić w danych warunkach.
Z naszej praktyki wynika, że każdy obiekt przemysłowy wymaga zastosowania różnych metod zabezpieczenia pożarowego, m.in. wynikających z czasu ich funkcjonowania, i to nie tylko zależnie od branży, ale też w odniesieniu do pojedynczych obiektów.

Podsumowanie

Zagadnienia związane z ochroną technologii i oddziaływania środowiska na instalacje ppoż. są szczególnie ważne ze względu na możliwość wystąpienia poważnych strat materialnych z powodu ich nieskutecznego działania. Jednocześnie wymagają bardzo wnikliwej analizy, mającej na celu dobór, utrzymanie ruchu, odpowiednią odporność, możliwość integracji i takiej ich adaptacji, która zapewni wymagany, akceptowalny poziom bezpieczeństwa.
W przypadku obiektów przemysłowych należy zawsze po wykonaniu i uruchomieniu instalacji bezpieczeństwa pożarowego ocenić ich skuteczność. Skuteczność instalacji należy udowodnić odpowiednimi pomiarami i sporządzić protokół z prób. Określaniem skuteczności instalacji przeciwpożarowych zajmuje się IBP Nodex.
Należy pamiętać też o tym, że każda dziedzina przemysłu ma swoją specyfikę i wymaga od osób zajmujących się bezpieczeństwem technologii odpowiedniego przygotowania. □

BIO
mgr inż. Janusz Sawicki

tematyką bezpieczeństwa pożarowego zajmuje się od 70. ub. wieku, pracując jako specjalista kolejno w Ośrodku Badawczo-Rozwojowym Ochrony Przeciwpożarowej przekształconym później w Centrum Naukowo-Badacze Ochrony Przeciwpożarowej im. J. Tuliszkowskiego PIB, a następnie w Instytucie Techniki Budowlanej w Zakładzie Badań Ogniowych. Obecnie w IBP NODEX.
Na każdym etapie pracy silnie współpracował z przemysłem, realizując na jego potrzeby wiele projektów związanych z szeroko pojętym bezpieczeństwem pożarowym w zakresie obiektów budowlanych i ochrony technologii.

- **Wczesna i wiarygodna detekcja dymu i płomienia w słabych warunkach oświetleniowych**
- **Nowe obiektywy umożliwiają zwiększenie zasięgu działania**
- **Kolejny znak jakości – certyfikacja w odniesieniu do standardu CSIRO**

Kolejny krok w dziedzinie wizyjnej detekcji pożaru AVIOTEC

TEKST
Jakub Bednarz
Product Manager

Technologia wizyjnej detekcji pożaru Bosch AVIOTEC IP starlight 8000, oprócz aplikacji w obszarach o wysokich stropach i dużych otwartych przestrzeniach, od teraz może być z powodzeniem stosowana także do ochrony wąskich i długich przejść, takich jak aleje pomiędzy regałami. Jest to możliwe dzięki dostosowaniu algorytmów analizy obrazu do pracy z dwoma nowymi obiektywami o wąskim kącie obserwacji. AVIOTEC stanowi tym samym łatwe w montażu rozwiązanie, będące alternatywą dla liniowych detektorów optycznych czy systemów zasysających dym, a ponadto eliminuje typowe ograniczenia tychże technologii.

Niezawodne wykrywanie pożaru nawet w trudnych warunkach oświetleniowych

Nowa wersja AVIOTEC jest oparta na algorytmach wykrywania dymu i płomienia specjalnie opracowanych do użytku w tunelach. Algorytmy zostały zoptymalizowane w ramach kompleksowych testów w warunkach rzeczywistych. Kamery wymagają oświetlenia sceny o natężeniu tylko 7 lx, aby niezawodnie wykrywać dym i płomienie za pomocą zintegrowanej inteligentnej analizy wizyjnej. Dzięki temu zwiększono również ponad dwukrotnie zasięg detekcji z 50 do ponad 100 m. Odpowiada to typowym zasięgom czujek liniowych stosowanych w takich obszarach.

Wielozadaniowość dzięki równoległej funkcji monitoringu wizyjnego

AVIOTEC umożliwia zastosowanie tych samych urządzeń do dozoru wizyjnego oraz wykrywania zagrożeń pożarowych, a tym samym zmniejsza koszty inwestycji i eksploatacji. Dzięki wbudowanym funkcjom inteligentnej analizy obrazu kamery mogą automatycznie wykrywać pozostawione przedmioty w alejkach, monitorować ruch wózków w alei (ich prędkość poruszania się, zliczanie przekroczeń linii przez wózki), a także wykrywać ruch osób w przestrzeniach, do których ich wstęp jest zabroniony.
Podobnie jak w przypadku detekcji dymu lub płomienia, AVIOTEC generuje odpowiedni komunikat, aby ochrona obiektu mogła natychmiast podjąć niezbędne środki i zminimalizować ryzyko konsekwencji rozwoju zdarzeń.
Inteligentna analiza wizyjna jest realizowana w kamerach, nie jest więc wymagany centralny serwer, który mógłby stanowić pojedynczy punkt awarii. AVIOTEC rejestruje również metadane wszystkich scen, które można przeszukiwać automatycznie, uzyskując w ten sposób bardzo szybką analizę przyczyn powstania pożaru lub zdarzenia.

Certyfikacja wyrobu

Jeszcze przed obecną aktualizacją AVIOTEC był pierwszym rozwiązaniem wizyjnej detekcji pożaru, które przeszło wymagającą procedurę testową niemieckiego ubezpieczyciela VdS Schadenverhütung GmbH. VdS przeprowadził procedurę testową zgodnie z wytycznymi VdS 2203 „Wymagania dotyczące oprogramowania przeciwpożarowego" i „Specyfikacja testowania czujek płomienia". W kwietniu 2019 r. AVIOTEC IP starlight otrzymał również certyfikat zgodności z australijską normą CSIRO TS010 odnoszącą się do rozwiązań w zakresie wideodetekcji pożaru.
Klienci, którzy już korzystają z rozwiązania AVIOTEC, mogą dokonać uaktualnienia do nowej wersji dzięki bezpłatnej aktualizacji oprogramowania układowego. W istniejących aplikacjach, które wymagają większego zasięgu, aktualizacja może również obejmować zakup nowego obiektywu. □

Bosch Security and Safety Systems
ul. Jutrzenki 105
02-231 Warszawa
e-mail: jakub.bednarz@pl.bosch.com

KRADZIEŻE DOKONYWANE PRZEZ PRACOWNIKÓW TO PROBLEM REALNY W WIELU FIRMACH, KTÓRE KORZYSTAJĄ Z MAGAZYNÓW DO PRZECHOWYWANIA I PRZENOSZENIA WIELU TOWARÓW O RÓŻNEJ WARTOŚCI.

NIE DAJ SIĘ OKRADAĆ!

Jak chronić magazyny przed złodziejem

Na początku 2016 r. „Bloomberg News" doniósł, że Amazon – oskarżany wcześniej o złe warunki pracy w swoich biurach i magazynach – zainstalował wielkogabarytowe monitory, na których wyświetlano zdjęcia pracowników zwolnionych po tym, jak zostali przyłapani na kradzieży w pracy. Wizerunki opatrzone były napisami „Zatrzymani" lub „Aresztowani". Amazon nie skomentował publicznie obraźliwej praktyki służącej próbie zahamowania kradzieży w swoich magazynach i nie odpowiedział na prośby o udzielenie wywiadu w tej sprawie.

Według „Bloomberg News" detalista przyłapał swoich pracowników z wszelkiego rodzaju kontrabandą: od płyt DVD, iPadów, poprzez kosmetyki, etui na telefony, gry wideo, po kuchenki mikrofalowe, a nawet lunche przeznaczone dla innych pracowników. Ale pomysł z wyświetlaniem wizerunków pracowników złapanych na kradzieży wydaje się niepokojący – jeden z pracowników nazwał go przerażającym, a nawet orwellowskim, stawiając pytania, czy praktyki Amazona są powszechne... i skuteczne.

TEKST
Michał Czuma

Automatyzacja likwiduje część problemów, jednak osobom nieuczciwym tworzy nowe możliwości kradzieży

Magazyny zaopatrzone w papierosy, piwo, wino i inne alkohole oraz słodycze i kosztowne dobra szybko zbywalne (np. elektronika) były i będą zagrożone kradzieżą. Jednak w miarę wzrostu i złożoności działalności dystrybucyjnej ze względu na rozwój i rosnącą liczbę obiektów magazynowych ryzyko związane z kradzieżami zaczęło rosnąć.

Największym wyzwaniem jest tak naprawdę tylko ilość kradzionego towaru – powiedział mi kiedyś dyrektor operacyjny dużego dystrybutora napojów alkoholowych. W każdym magazynie w jego firmie, który ma kilka tysięcy metrów kwadratowych, można przechowywać ponad 1 mln sztuk opakowań w sezonie letnim, w którym sprzedaje się najwięcej tego towaru. Liczba jednostek magazynowych, wielkość zapasów, liczba samochodów ciężarowych przemieszczających się każdego dnia oznacza, że mnóstwo produktów jest w ruchu.

Aby zarządzać rosnącymi zapasami, wielu dużych dystrybutorów wprowadziło systemy zautomatyzowane, co na pewno jest korzystne, ale jednocześnie może stać się punktem wrażliwym, jeśli chodzi o zwalczanie kradzieży. Automatyka umożliwia dokładne śledzenie towaru, ale pracownik, który zna te systemy, a ma złe intencje, może znaleźć sposoby ich wykorzystania do swoich niecnych celów.

Skala kradzieży, które nękają dystrybutorów, jest różna – od pojedynczych przypadków, kiedy znika kilka produktów, po straty sięgające setek tysięcy, a nawet milionów złotych. Często wynajmowani do pracy sezonowej pracownicy mogą ulec pokusie, widząc regały zapełnione po brzegi słodyczami, butelkami z piwem, winem lub innym alkoholem. Później kadra kierownicza i magazynierzy muszą wyjaśniać wykryte braki. Innym problemem są koszty. Sama kradzież to coś więcej niż tylko wartość skradzionych produktów wyrażona w złotych czy euro. Jeśli mechanizm kradzieży nie zostanie zbadany i wyeliminowany, w firmie zapanuje toksyczna atmosfera. Pracownicy będą uważali, że zasady i reguły już nie obowiązują. Kadra kierownicza straci dyscyplinę i profesjonalizm, a to wszystko utrudnia zarządzanie magazynem. W końcu zaczyna dostrzegać problem – mimo wzrostu sprzedaży i wyeliminowaniu zbędnych kosztów zysk firmy znika.

Różnorodność sprawców przestępstw

Wspólnym mianownikiem przestępstw, z jakimi dystrybutorzy FMCG (*Fast-Moving Consumer Goods* – produkty szybko zbywalne) mogą się spotkać w pracy, jest element zaskoczenia, który dotyka nawet weteranów przemysłu. Mój serdeczny kolega jest od kilkunastu lat menedżerem ds. kontroli i zgodności w jednej z firm dystrybuujących alkohole. Opowiadał mi, że wokół magazynów leżą w połowie opróżnione butelki z popularnym szprycerem kosztującym w sklepie niecałe 6 zł. Choć miał poważne podejrzenia, złodziej nigdy nie został przyłapany. Jak twierdzi, nie tylko produkty pre-

mium są narażone na kradzież w środowisku dystrybucji. Wartość jest pojęciem względnym, komuś opłaca się zaryzykować dla butelki o poj. 0,33 l za 6 zł. Kiedy towar znika często i przez dłuższy czas, firma traci już znacznie więcej. Ale kiedy złodziej czuje się bezkarny, a widzą to inni i nie reagują, straty mogą rosnąć w większym zakresie.

Inny menedżer znanej firmy piwowarskiej zauważył butelkę piwa, która wysunęła się spod płaszcza robotnika czekającego na firmowy autobus, i rozbiła się przed nim na ziemi. Zapytał go, czy było warto, bo przecież już nie wróci do pracy w tym zakładzie. Gdyby go poprosił, dostałby zapewne całą zgrzewkę piwa, do tego schłodzonego. Czasami trudno zrozumieć ludzi.

Historie bywają też bardziej dramatyczne. Kiedy z zaparkowanej na służbowym parkingu ciężarówki pewnej firmy dystrybucyjnej zniknęły palety z produktami, policja rozpoczęła obserwację nocą. W końcu złapano winowajców – byli to miejscowi koledzy ze studiów, z których jeden pracował w firmie rok wcześniej na stażu wakacyjnym i znał harmonogram przerw w pracy zespołu kompletacyjnego. Wiedział, kiedy uderzyć. Ta zgraja była profesjonalnie przygotowana, a towar na paletach sporo kosztował. Musieli być zaskoczeni, gdy wkrótce do drzwi ich mieszkań zapukali policjanci.

Sposoby kradzieży mogą być bardziej wyrafinowane. Jeden z moich podwykonawców badał sprawę, w której pracownik wymyślił, jak drukować duplikaty etykiet zbiorczych, by załadować dodatkowe palety z towarem na ciężarówki. Przyklejał je później do zbiorczych palet z produktem, omijał kontrolerów i pilnował, by zostały załadowane na ciężarówki tych kierowców, z którymi był w zmowie. Robili to od trzech do czterech razy w tygodniu. Proceder udało się przerwać tylko dlatego, że sprawą zajęli się profesjonaliści.

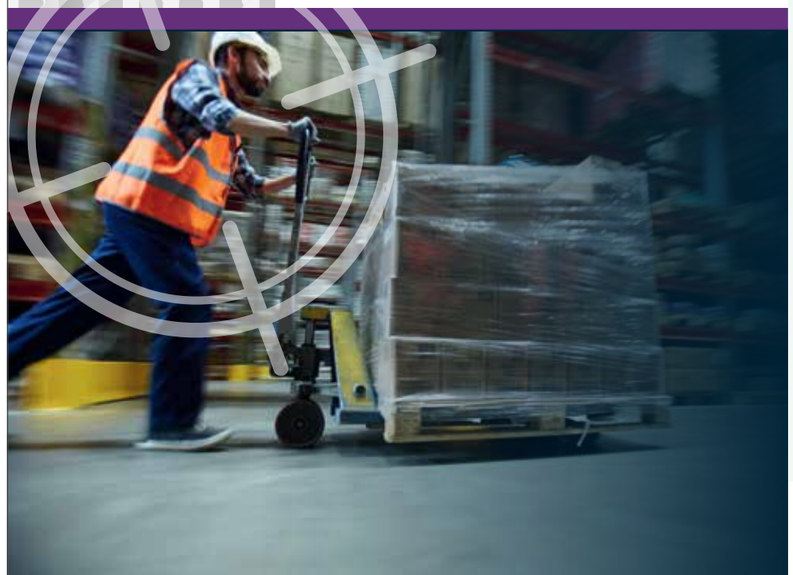
Pracownik stosował tę metodę, aby ukraść i przetransportować towar, którego wartość hurtowa wynosiła od 10 do 25 tys. zł tygodniowo. Kierowcy, z którymi się umawiał, sprzedawali „dodatkowy" produkt albo klientom na trasie, którzy za znaczne zniżki byli gotowi zapłacić gotówką, albo sprzedawcom detalicznym poza trasą. Magazynier, który drukował dodatkowe etykiety, później wyjaśniał, że kierowcy ciężarówek, które wyładowywał, prawie każdego dnia przekazywali mu listę produktów, na jakie mieli zbyt. Wiedzieli, które produkty szybko znajdują odbiorców, i ile w ten sposób zarobią. Nie jest problemem dla złodziei wygenerować straty z „dodrukowania etykiet" na poziomie nawet kilku milionów złotych w ciągu roku. U jednego z poszkodowanych klientów, znaczącego dystrybutora alkoholi, zatrzymano czterech kierowców i doprowadzono do zamknięcia 15 sklepów z winem i alkoholami, które przez ponad trzy lata aktywnie kupowały skradzione produkty. Dyrektor finansowy dystrybutora, po zapoznaniu się z zeznaniami, oszacował, że strata z tego tytułu przekroczyła 4 mln zł. A trzeba wiedzieć, że średnio straty z tytułu kradzieży zwłaszcza u producentów i dystrybutorów FMCG wynoszą 2% ich obrotów. Jeśli przekraczają poziom 2%, oznacza to, że poza kradzieżami typowo „magazynowymi" dochodzi do fraudów także w procesach zakupowych, sprzedażowych i prawdopodobnie finansowych, w tym korupcji. Zastanawiać może to, że wciąż są firmy, które bagatelizują ten problem.

Wystarczy rozbić jeden złodziejski układ, aby wszystkie poniesione koszty z nadwyżką szybko się zwróciły

Typowa kradzież w dużych obiektach magazynowych, zakładach produkcyjnych czy dystrybucyjnych wygląda dokładnie tak, jak standardowa procedura operacyjna. Nie ma specjalnych sygnałów alarmowych, które budzą z uśpienia. Ta kradzież ma miejsce w systemie. Wygląda jak codzienna czynność, co sprawia, że trudno ją wykryć bez informacji wewnętrznej. Walka z nią jest trudna także z tego powodu, że większość pracowników to ludzie uczciwi. Kradną nieliczni i właśnie dlatego wyłapanie ich jest często jak szukanie igły w stogu siana.

Sposoby walki z kradzieżą

Jedną z form walki z kradzieżami jest wynajmowanie profesjonalnych firm i zatrudnianie na różnych stanowiskach tajnych agentów. Niektórzy sprawują dozór nad grupą ponad kilkudziesięcioosobową składającą się z zatrudnionych na każdym stanowisku: kierowca, odbiorca, menedżer, ładowacz, a nawet sprzątaczki. Ci agenci czasem zarabiają bardzo dużo – pracując, otrzymują wynagrodzenie zarówno z firmy, której pilnują, jak i macierzystej firmy specjalistycznej, która ich zatrudnia. Ale ta inwestycja zwraca się błyskawicznie. Współpracujący ze mną detektyw rozbił złodziejski układ z udziałem kierownika magazynu i dwóch osób dokonujących selekcji. Detektyw zatrudniony w magazynie stał się podejrzliwy, gdy usłyszał, że kierownik magazynu polecił jednemu z selekcjonerów, aby dwie dodatkowe palety bardzo drogiego towaru, które nie znajdowały się na liście przewozowej, umieścić na ciężarówce firmy. Operator „pod przykrywką" odnotował 18 takich nadzwyczajnych zdarzeń. Zespół nadzoru ostatecznie ujawnił pięciu detalistów, którzy



JAK WYKRYĆ I POWSTRZYMAĆ KRADZIEŻ

1. SPRAWDZAJ ZATRUDNIANYCH PRACOWNIKÓW.

Chociaż wymagania RODO odcinają pracodawcę od dostępu do istotnych informacji, warto weryfikować dane, jakie nowi pracownicy umieszczają w swoich CV czy ankietach personalnych. Wynajęcie w niektórych przypadkach detektywa, który sprawdzi przekazane dane i miejsca, w których poprzednio pracował nowo zatrudniony, może ustrzec pracodawcę przed wieloma problemami. Najważniejsze, by proces personal screeningu był prawidłowo przeprowadzany. „Prześwietlanie" może pomóc w zapewnieniu uczciwości, rzetelności i ciągłości procesu zatrudniania, ale przynosi również korzyści uczciwym kandydatom. Zaufaj instynktowi – jeśli nie jesteś pewien, że ktoś jest wiarygodny, nie zatrudniaj go.

2. KSZTAŁĆ PRACOWNIKÓW W ZAKRESIE POLITYKI FIRMY DOTYCZĄCEJ KRADZIEŻY

Wszyscy pracownicy powinni wiedzieć, że firma ma politykę „zero tolerancji", jeśli chodzi o kradzież lub oszustwo. Powinni podpisać kodeks postępowania jasno określający, w jaki sposób naruszenia będą karane. Ponadto należy uruchomić anonimowe kanały zgłaszania wszelkich podejrzanych działań. Jeśli wszyscy wiedzą, że pilnują ich koledzy, odstraszy to złodziei, ponieważ istnieje większe prawdopodobieństwo, że zostaną złapani. Trzeba mówić głośno, że troska o dobro firmy będzie nagradzana, a nadużycia – surowo karane.

3. NATYCHMIAST ZAJMIJ SIĘ KRADZIEŻĄ ZGODNIE Z POLITYKĄ FIRMY

Gdy doświadczysz kradzieży lub serii kradzieży, sprawdź w rejestrze zmianowym, kto był w danym czasie na służbie. Jeśli zaczniesz zauważać zależność pomiędzy brakującymi zapasami a obecnością (albo nieobecnością) niektórych pracowników, monitoruj ich pracę w magazynie. Gdy zauważysz jakiekolwiek podejrzane zachowanie, prawdopodobnie będziesz musiał przeprowadzić dalsze dochodzenie. Warto mieć własną komórkę ds. bezpieczeństwa i nadużyć, której przeszkoleni i wyspecjalizowani ludzie zajmą się problemem. Możesz też wynająć firmę doradczą, co znacznie przyspiesza działania i wykrycie złodziei.

4. MAKSYMALIZUJ WIDOCZNOŚĆ KADRY ZARZĄDZAJĄCEJ W MAGAZYNIE

Częsta obecność kadry kierowniczej w magazynie zniechęca do kradzieży. Nie zawsze jednak szef magazynu może tu spędzać dużo czasu, ponieważ wiele z jego obowiązków wymaga pracy na komputerze w biurze. Rozważ zainwestowanie w rozwiązanie do zarządzania magazynem, oferujące komponent mobilny, aby kierownik magazynu nie był w pełni związany z biurem i biurkiem. Możesz też zlokalizować jego biuro nad magazynem, na antresoli, z widokiem na magazyn. Dzięki temu kierownictwo może przez cały czas mieć w zasięgu wzroku powierzchnię magazynową.

5. OGRANICZ DOSTĘP DO ZAPASÓW W MAGAZYNIE

Wykorzystaj fizyczny układ magazynu, aby utworzyć bariery utrudniające kradzież. W miarę możliwości oddzielaj rampy odbiorcze i wysyłkowe, by zapobiec opuszczaniu odebranych zapasów na wyjeżdżającej ciężarówce, zanim dotrze ona do magazynu. Powierzchnie magazynowe przeznaczone na przechowywanie towarów powinny znajdować się jak najdalej od obszarów wysyłki i odbioru. Jedynie magazyn zamówień wpływających i odbieranych powinien być zlokalizowany w pobliżu tych obszarów. Zapewnij odwiedzającym kierowcom ciężarówek wydzieloną strefę wypoczynku, gdzie mogliby czekać, aż zamówiony towar zostanie załadowany lub rozładowany. Tylko personel pracujący w danej lokalizacji powinien mieć dostęp do magazynu lub obszaru dystrybucji.

6. UPEWNIJ SIĘ, ŻE SYSTEMY ZABEZPIECZEŃ W MAGAZYNIE SĄ SOLIDNE

Zainstalowane elektroniczne systemy zabezpieczeń, takie jak kontrola dostępu i telewizja dozorowa, nie tylko odstraszają przestępców, ale także dostarczają dowodów kradzieży zarejestrowanej na obrazie kamery CCTV. Kamery powinny być strategicznie rozmieszczone w obszarach wysokiego ryzyka. Można również zainstalować lusterka bezpieczeństwa, aby zwiększyć widoczność i zapobiec powstawaniu martwych punktów w trudno dostępnych punktach magazynu. Inne środki bezpieczeństwa, np. nieplanowane obchody magazynu przez przełożonych lub kierowników zespołów, mogą stanowić dodatkowy czynnik odstraszający, ale muszą być nieprzewidywalne. Zatoki wysyłkowe i odbiorcze oraz wejścia i wyjścia to kluczowe obszary, które powinny być sprawdzane. Personel ochrony powinien znajdować się przy każdym wejściu do budynku i wyjściu z niego. Upewnij się, czy wszystkie pojazdy opuszczające magazyn są kontrolowane w celu wykrycia wszelkich niezaewidencjonowanych zapasów. Parking dla personelu i gości powinien być oddalony od operacji magazynowych. Żadne pojazdy prywatne nie powinny parkować w pobliżu magazynu.

7. POZNAJ I ZROZUM MOTYWACJĘ ZŁODZIEJA

Wiedza o tym, dlaczego pracownicy kradną, pomoże ograniczyć to zjawisko w bardziej efektywny sposób. DLACZEGO PRACOWNICY KRADNĄ? W idealnym świecie nie musielibyśmy zadawać takich pytań. Generalnie można wskazać trzy powody:

- Trudna sytuacja finansowa pracowników
  Zmaganie się z problemami finansowymi może skłonić pracownika do okradania pracodawcy – albo do zabierania rzeczy do domu dla rodziny, albo do sprzedawania ich za gotówkę. Uważają, że wielu rzeczy potrzebują bardziej niż pracodawca, a firma nie zauważy braku lub może sobie pozwolić na jego uzupełnienie. Nałogi i uzależnienie również skłaniają ludzi do kradzieży.

- Uprawnienia pracownicze
  Niektórzy pracownicy uważają, że firma, w której pracują, jest im coś winna. Nie postrzegają grabieży jako kradzieży – zabierają to, co im się słusznie od firmy należało.

- Oportunizm
  Pracownik-złodziej może „zapomnieć" o zasadach dla odniesienia korzyści. Ukradnie coś pożądanego tylko dlatego, że może to wziąć. Będzie wykradać przedmioty łatwo dostępne i łatwe do ukrycia – kosmetyki, ubrania, alkohol, żywność i elektronika są najbardziej narażone na kradzież

8. WDRAŻAJ SYSTEM ZARZĄDZANIA MAGAZYNEM UMOŻLIWIAJĄCY DOKŁADNIEJSZE, MNIEJ KORUPCYJNE REGULACJE

Wiedza o tym, jaka jest aktualna wielkość zapasów magazynowych (i gdzie znajdują się one w magazynie), pomaga natychmiast zidentyfikować braki. Ręczne śledzenie stanów magazynowych często prowadzi do błędów, zwłaszcza w przypadku rzadkich braków magazynowych. Wprowadzenie pełnego monitoringu obrotu produktów, monitoringu pracy, przemieszczania się pracowników, kierowców, pojazdów i towarów – wystarczy jeden system wykrywający anomalie i sprawny zespół ochrony, by zredukować straty z tytułu kradzieży nawet o 99%. Ten jeden procent ma nas mobilizować, byśmy pamiętali, jak twórczy potrafią być nieuczciwi pracownicy, którzy zawsze znajdą nowy sposób na kradzież.

Nie ma doskonałych systemów przeciwdziałania nadużyciom, ale sporo jest takich, które zastosowane kompleksowo powodują, że każda inwestycja w bezpieczeństwo obiektów i firmy bardzo szybko się zwraca i zwiększa nasze zyski.

kupowali towar, płacąc złodziejom gotówką. Na szczęście odzyskano na drodze prawnej pieniądze, którymi udało się pokryć stratę.

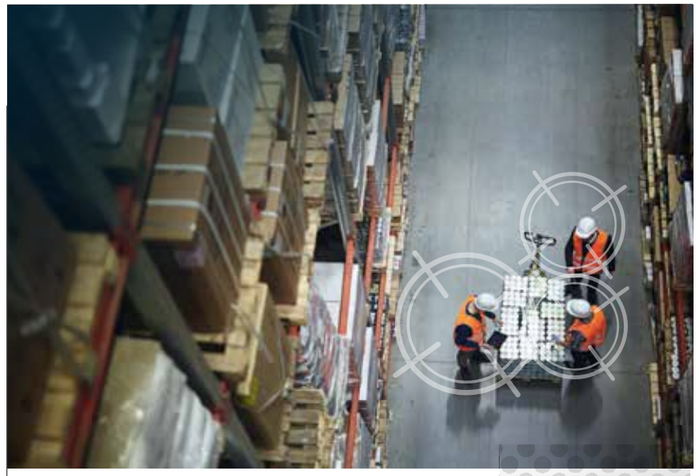
Innym skutecznym narzędziem jest informacja anonimowa. Często to właśnie pracownicy jako pierwsi zgłaszają nielegalną działalność. To proste, łatwe i tanie rozwiązanie, ale trzeba je dobrze i fachowo przygotować. Do tego świetnie nadają się pracownicy komórek *compliance*. Kiedy firma uruchomi budżet na nagrody dla sygnalistów, inwestycja nadzwyczaj szybko się zwraca. Nawet gdy na numer do powiadamiania o nadużyciach zadzwoni jedna osoba na rok, korzyści są bardzo duże. Anonimowe kanały powiadamiania to koszt kilkunastu tysięcy rocznie.

Zapobieganie kradzieżom w magazynie

Nie ma prostego rozwiązania zapobiegającego kradzieżom w magazynach. Problem wymaga połączenia wielu procesów, systemów bezpieczeństwa, oprogramowania do zarządzania magazynem i sprawdzonych kryteriów zatrudniania. Najważniejsze, by go dostrzec i upewnić się, że zapasy magazynowe są właściwie śledzone, aby odróżnić straty, które możesz ponieść, łącząc inwentaryzację i liczbę operacji cyklicznych w celu dokładnej oceny zapasów w księgach.

Czy firma posiada system magazynowy, który pozwala na większą elastyczność dokumentowania i przejście od tradycyjnych metod inwentaryzacji do zliczania cykli uzupełniania towaru? Stałe monitorowanie zapasów umożliwia wykrycie pierwszych anomalii. Sygnalizowanie braków system synchronizuje czasowo z danymi z systemów monitorowania. A to z kolei pozwala stwierdzić, kto w danym czasie był w pracy, który z kierowców przywiózł lub wywiózł towar. Gdy połączymy te dane z systemami ewidencji czasu pracy i monitoringu wizyjnego, wykrycie nadużyć nie stanowi już większego problemu. Warto pamiętać, że w magazynie rozpoczyna się efektywna działalność gospodarcza.

Im mniej dokładna jest ewidencja zapasów, tym szybciej magazyn staje się łatwym celem



Brakujące zapasy a kradzież: jak rozpoznać różnicę?

Kurczenie się zapasów w magazynie jest zjawiskiem normalnym, ale do pewnych granic. Istnieje wiele powodów utraty zapasów – analizując raporty publikowane przez wyspecjalizowane firmy audytorskie, okazuje się, że ok. 78% wszystkich zgłoszonych przypadków dotyczyło okradania załadowanych ciężarówek. W przypadku kradzieży w zakładzie odnotowano w ciągu ostatnich czterech lat wzrost o 98 proc.; o 266 proc. wzrosła wartość skradzionych towarów. W długie weekendy i weekendy wakacyjne odnotowano 40-proc. wzrost liczby kradzieży towarów, co jest zaskakujące, ale powtarza się w wielu raportach.
Najlepszym sposobem na identyfikację kradzieży w magazynie jest regularne przeprowadzanie inwentaryzacji. Im dokładniejsze są dane inwentaryzacyjne, tym szybciej wykrywamy kradzież. Bez regularnych inwentaryzacji można nawet przez wiele miesięcy nie zauważyć, że poziom zapasów podejrzanie się skurczył.

Co może wskazywać na to, że jesteś okradany?

Poziom zapasów nie zgadza się z danymi sprzedaży.
- Sprzedaż wydaje się zmniejszać w dniach, kiedy niektórzy (ci sami) pracownicy są na dyżurze.
- Krążą plotki sugerujące, że w twoich obiektach ma miejsce kradzież.
- Niektórzy pracownicy unikają wzięcia urlopu rocznego.
- Brakuje ważnej dokumentacji (np. faktur) lub pojawiają się jako duplikaty, a nie oryginały.
- Pewne ilości towaru są stale widoczne i składowane w pobliżu wyjść lub stanowisk przeładunkowych.

Bardzo trudno udowodnić kradzież z magazynu bez przyłapania osoby na gorącym uczynku. Znacznie łatwiej jest wprowadzić środki zapobiegające. Jeśli zauważysz rozbieżności inwentaryzacyjne, sprawdź je natychmiast. Im dłużej to odkładasz, tym trudniej będzie ustalić, czy brakujące elementy magazynowe zostały utracone, czy skradzione.
Wiedza o tym, gdzie znajdują się zapasy (lub ich brakuje), jest krytyczna i od tego momentu zalecamy podjęcie środków ostrożności w celu podniesienia świadomości, zidentyfikowania słabych punktów i ograniczenia możliwości kradzieży.

BIO

Michał Czuma

Niezależny ekspert, prowadzący obecnie własną działalność doradczą. Stworzył i zarządzał pierwszymi w kraju Biurami Antyfraudowymi w spółkach grupy PKO Banku Polskiego. Były wieloletni z-ca dyrektora Departamentu Bezpieczeństwa PKO Banku Polskiego.

Milestone Integration Day w Warszawie

Partnerzy firmy Milestone Systems i użytkownicy systemów dozoru wizyjnego spotkali się 5 września w warszawskim hotelu Indigo podczas Milestone Integration Day. Światowy lider oprogramowania do zarządzania materiałem wizyjnym opartego na otwartej platformie zorganizował spotkanie wspólnie z partnerami technologicznymi: Axis Communications, AnyVision, Bosch, Hanwha Techwin, Scylla, Vanderbilt i Vivotek.

Podczas konferencji omówiono działanie platformy Milestone Systems i korzyści, jakie przynosi integracja elektronicznych systemów zabezpieczeń. *Technologia i zdolność do innowacji nigdy nie były tak ważne, ponieważ firmy szukają nowych sposobów na wzrost sprzedaży, zwiększenie wydajności operacyjnej i poprawę jakości obsługi klienta. Dynamiczny postęp w zakresie Internetu Rzeczy i sztucznej inteligencji pozwala uzyskać lepszy i szybszy ogląd sytuacji, przenosząc dozór wizyjny poza obszar zastosowań systemów zabezpieczeń* – powiedział Anders Johansson, Director, Distribution & Emerging Markets.

Blisko 100 gości – partnerów i użytkowników końcowych – miało okazję poznać nowości z oferty firmy, w tym Milestone XProtect® Corporate z certyfikatem GDPR-ready. To pierwsze oprogramowanie do zarządzania materiałem wizyjnym, które otrzymało certyfikat przyznawany przez niezależny i cenion y na świecie instytut EuroPriSe. *„Certyfikacja obejmuje wszystkie podstawowe możliwości Milestone XProtect Corporate związane z cyberbezpieczeństwem. Dostarczyliśmy pełen zestaw narzędzi, w tym obszerny przewodnik z gotowymi do użycia szablonami, aby wspomóc integratorów systemów i użytkowników końcowych w projektowaniu, wdrażaniu i obsłudze systemów dozoru wizyjnego zgodnie z wymaganiami rozporządzenia RODO”* – podkreślił Dmitrij Bazajevs, Country Manager w Milestone Systems.

Dużo uwagi gospodarze poświęcili przedstawieniu zasad wsparcia technicznego, zaprezentowali też nowy panel klienta do rozwiązań w chmurze. Szerzej omówiono także rozwiązania Milestone Systems dla zastosowań *smart city* oraz sektora handlu detalicznego.

Podczas konferencji liderzy branży security zaprezentowali sposoby na szybszy wzrost wydajności operacyjnej dzięki wykorzystaniu najnowszych technologii. Ara Ghazaryan z firmy Scylla pokazał, jak można wzbogacić system dozoru wizyjnego o dodatkowe inteligentne funkcje. O tym, jak prosta może być integracja systemów, opowiadał Adam Brzezicki z Axis Communications, a zalety współpracy platformy Better Tomorrow firmy AnyVision z rozwiązaniami Milestone omówili Bogna Ettinger i Sa'ar Klein. Z kolei kompleksową ofertę systemów Bosch i Milestone zaprezentował Maciej Wróbel z Bosch Building Technologies.

Prezentowane przez gospodarzy i partnerów technologicznych rozwiązania można było również przetestować na specjalnie przygotowanych stoiskach. Spotkanie było też doskonałą okazją do wymiany poglądów i rozmów biznesowych z przedstawicielami firm.

ADI Expo 2019
po raz czwarty w Polsce

Ta branżowa impreza i tym razem była doskonałą okazją do indywidualnych rozmów z przedstawicielami czołowych producentów elektronicznych systemów zabezpieczeń, zapoznania się z nowościami produktowymi, udziału w ciekawych seminariach na temat wiodących rozwiązań.

Maciej Skalski, prezes ADI Global Distribution w Polsce
To już czwarta edycja targów ADI Expo. W tym roku znowu mamy rekordową liczbę klientów i podobnie jest z wystawcami – aż 25 kluczowych producentów naszej branży. ADI Expo są wyjątkowe zarówno w skali Polski, jak i świata – co roku organizujemy 120 tego typu imprez. Jest to możliwe właśnie dzięki skali działania naszej firmy. W tym roku mija akurat 20 lat od pierwszego ADI Expo, które odbyło się w USA.
Jeśli ktoś z Państwa jeszcze nie uczestniczył w naszych targach, serdecznie zapraszamy za rok.

Momchil Karagiozov, Solution Engineer, Milestone Systems
Wydarzenie jest dobrze przygotowane. Jest dużo klientów, w trakcie spotkania mamy możliwość poznać nowych partnerów.

Kamil Targalski, HID Global
Jestem kolejny raz na targach ADI Expo, kolejny raz jest duża frekwencja i bardzo duże zainteresowanie, jeśli chodzi o bezpieczne technologie zbliżeniowe, tak jak rekomendowany przez nas SEOS. Miałem także dużo zapytań o czytniki biometryczne, które mamy w ofercie od kilku miesięcy – nowa technologia w oparciu o nowe sensory biometryczne HDI.

Łukasz Lik, Technical Manager, Hikvision Poland
Kolejny raz gościmy na imprezie ADI Expo. Jest to dla nas szczególna impreza, bo ADI to nasz wieloletni partner i budujemy razem wspaniałe tematy i projekty. Dla gości odwiedzających nasze stoisko przygotowaliśmy pokaz natywnej integracji systemów Hikvision.

Zobacz film z wydarzenia

Kate Rose, Product Management Director EMEA, ADI Global Distribution
Na ADI Expo w Warszawie mamy wspaniały program i najlepszych dostawców z branży security. Wszyscy jesteśmy bardzo zadowoleni z tego wydarzenia. Klienci mogą zapoznać się z prezentacjami menedżerów dotyczącymi różnorodnych produktów. To wiodące w branży wydarzenie dla czołowych dostawców systemów zabezpieczeń, jesteśmy bardzo zadowoleni z oferty w branży w Warszawie.

Arkadiusz Gmitrzak, Honeywell
Frekwencja jest dużo większa niż na poprzednim ADI Expo. Pytania, które instalatorzy i integratorzy zadają, dotyczą przede wszystkim kwestii chmury. Jest to temat nośny, interesują się tym i mam nadzieję, że przyniesie w krótszej perspektywie pożytek biznesowy.

Artur Górski, Siemens
Fantastyczna organizacja, bardzo dużo dostawców i partnerów firmy ADI. Ważny dzień także dla nas, bo zaczęliśmy z ADI współpracę w zakresie dystrybucji systemów sygnalizacji pożarowej. Biorąc pod uwagę liczbę klientów, optymistycznie patrzę w przyszłość na naszą współpracę. Bardzo dobra robota ADI!

Dagmara Pomirska, szefowa sprzedaży Axis Communications
Jesteśmy bardzo zadowoleni z ADI Expo ze względu na bardzo dużą liczbę uczestników i ich aktywność. Było wiele pytań ze strony klientów i partnerów. Podoba nam się to, jak ADI zorganizowało ten event, zarówno format, jak i zaangażowanie naszego partnera.

Marcin Ruciński, Dahua Technology
To czwarta edycja, w której biorę udział. Patrząc z perspektywy czasu jest coraz więcej wystawców, którzy prezentują szeroką i bardzo ciekawą gamę produktów z rynku security. Jest także dużo więcej odwiedzających niż w poprzednich edycjach.

Krzysztof Krasowski, Sales Manager Poland, Baltics and Ukraine, Vanderbilt
Pokazujemy nowe wideodomofony, które są w naszej ofercie, a także system sygnalizacji włamania i napadu oparty na centrali SPC. Wydarzenie jest bardzo ciekawe, jestem tu po raz drugi i mam nadzieję, że w przyszłym roku również zostanę zaproszony.

Krzysztof Dulin, Country Manager Polska & kraje bałtyckie Hanwha Techwin Europe
Bardzo fajna konferencja, kolejny rok bierzemy w niej udział. Bardzo dużo ludzi przyszło na nasze stanowisko i z pewnością będziemy się wystawiać w następnym roku.

Na tegoroczną edycję Axis Partners' Day firma zaprosiła partnerów, dystrybutorów i sympatyków nowoczesnych technologii do odrestaurowanej kamienicy na warszawskiej Pradze.

Axis Partners' Day 2019

Podczas wrześniowego spotkania firma Axis Communications zaprezentowała nowości ze swojej oferty. Partnerom, którzy osiągnęli najlepsze wyniki we współpracy lub zrealizowali ciekawe projekty, wręczono okolicznościowe statuetki.
Goście mieli również okazję wysłuchać prezentacji eksperta na temat ochrony danych osobowych w systemach monitoringu wizyjnego.
Gospodarze zaproponowali ciekawą formułę prezentacji rozwiązań partnerów – firm NEC, Genetec, Citilog i Milestone. Ogłoszono też wyniki konkursu: *Gdzie jest Axis?* Nagrodzono najciekawsze zdjęcia, doceniono też inwencję twórczą autorów filmów wideo. □

Rozmawiamy z **Magnusem Zederfeldtem**, dyrektorem regionalnym na Europę Wschodnią w Axis Communications

Rynek sieciowych systemów wizyjnych rozwija się dynamicznie. W jaki sposób Axis Communications wspiera swoich partnerów w nadążaniu za tymi zmianami?
To dobre pytanie. Axis jest firmą innowacyjną. Bardzo dużo czasu i środków przeznaczamy na badania i rozwój, nasi inżynierowie R&D nieustannie wymyślają nowe rozwiązania. Trudno nadążyć za premierami, znajomość nowych produktów stanowi wyzwanie nie tylko dla naszych partnerów, ale i dla nas samych. Kluczową sprawą jest więc edukacja. Uruchomiliśmy Axis Academy, organizujemy szkolenia produktowe, różnego rodzaju wydarzenia, takie jak chociażby Axis Partner Day. O nowościach informujemy na bieżąco na stronie internetowej Axisa, dużą popularnością cieszą się też nasze szkolenia online, bardzo wygodna forma dla osób, które nie mogą uczestniczyć w szkoleniach stacjonarnych. Ale przede wszystkim zatrudniamy bardzo dużo inżynierów, którzy nie tylko szkolą, ale też wspierają naszych partnerów w zaznajamianiu ich z funkcjonalnościami nowych produktów, aby ułatwiać sprzedaż tych rozwiązań użytkownikom końcowym. Dajemy z siebie wszystko: szkolimy, oferujemy wsparcie techniczne.

W jakim kierunku będą rozwijać się sieciowe systemy monitoringu wizyjnego?
Użytkownicy oczekują dziś od urządzeń systemów monitoringu, żeby oferowały też inne funkcje niż tylko dozór wizyjny. Chcą m.in. natychmiastowego powiadomienia o zdarzeniu alarmowym, a nawet wyprzedzających informacji o możliwości jego wystąpienia, zanim jeszcze się ono zdarzy, i to z dużym prawdopodobieństwem. Zwiększamy więc inteligencję w kamerach, uzupełniamy je o inne możliwości, np. komunikaty głosowe.
Jeśli mam wskazać główny kierunek rozwoju VSS, wydaje mi się, że będziemy dążyć do tego, aby systemy dozorowe były proaktywne i inteligentne, a kamery generowały dobrej jakości, coraz bardziej szczegółowe obrazy z wyraźniejszymi kolorami nawet w najtrudniejszych warunkach oświetleniowych. Większość urządzeń to już urządzenia sieciowe, więc naturalna staje się też dbałość o ich cyberbezpieczeństwo.
Według mnie najbardziej oczywiste będą trzy kierunki: rozwój kamer sieciowych i związanej z tym jakości obrazu, implementacja inteligentnych funkcji w kamerach wykorzystanych nie tylko do celów stricte dozorowych, ale i biznesowych oraz rozwój technologii sieciowej, jako bardziej wydajnej i lepiej zabezpieczonej.
Dziękujemy za rozmowę □

SECURITY 4.0 – międzynarodowa konferencja EBS

Rok 2019 jest wyjątkowy zarówno dla firmy EBS, która obchodzi 30-lecie swojego istnienia, jak i całej branży, która przeżywa czwartą rewolucję przemysłową. Dlatego też konferencja, którą EBS organizuje już od 9 lat, przybrała w tym roku wyjątkowy charakter. W odróżnieniu od poprzednich edycji na to wydarzenie firma postanowiła zaprosić swoich Partnerów i Klientów nie tylko z Polski, ale i z 26 krajów z całego świata. 27 września w Jachrance o przemyśle 4.0 dyskutowano w gronie prawie 80 firm – dystrybutorów, integratorów, agencji ochrony.

Tematyka wydarzenia dotyczyła zagadnień globalnych, dotykała problemów branży zabezpieczeń i zmian, jakie pod wpływem rosnącej cyfryzacji, rozwoju sztucznej inteligencji oraz automatyzacji procesów dokonują się obecnie lub pojawią w ciągu najbliższych lat. Do udziału w konferencji EBS zaprosiła Partnerów – firmy Fibaro, Next, Orange, Dahua, Linc, AdInfo, Security Robot Guard Systems oraz Instytut Łączności, jako patrona naukowego. Partnerom honorowym zostały Polska Izba Ochrony, Polska Izba Systemów Alarmowych i Polski Związek Pracodawców Ochrona.

Swoje prezentacje przedstawili przede wszystkim praktycy – Krzysztof Kuźbik, Partner Avallon, wieloletni wykładowca i partner w wiodącym funduszu inwestycyjnym; Tomasz Laudy, obecnie wiceprezes EBS, który kompetencje i wiedzę zdobywał w firmach Ericsson, Siemens, Orange i Roshan; Daniel Kamiński, wieloletni praktyk i publicysta branżowy, pełniący obecnie funkcję dyrektora ds. innowacji oraz członka zarządu w EBS; Krzysztof Bartuszek, prezes Securitas Polska; Anna Śliwoń, analityk w międzynarodowej wywiadowni gospodarczej IHS Markit, pracująca na co dzień w Wielkiej Brytanii.

Bogata tematyka konferencji została podzielona na bloki tematyczne składające się na jeden EKOSYSTEM (środowisko), a zarazem element nowocześnie funkcjonujących w nim systemów: • rewolucja na świecie • rewolucja w security • urządzenia – systemy cyber-fizyczne • komunikacja IoT • chmura – *big data*, sztuczna inteligencja.

W tym zakresie swoje produkty i rozwiązania przedstawiły firmy: EBS, Orange (Paweł Dębiński), Next (Sławomir Piela), Dahua (Maciej Pietrzak) oraz Linc (Jakub Sobek). Głos zabrali również Partnerzy zagraniczni EBS: firma MaxiMan z RPA, właściciel największej agencji ochrony Chubb na kontynencie Afryki, który wdrożył algorytmy AI do swojego systemu raportowania, a także właściciel brazylijskiej firmy Setech opowiadający o nowym modelu sprzedaży urządzeń (Active Track) jako usługi.
Całości wydarzenia dopełniły warsztaty prezentujące nowe rozwiązania – m.in. integrację centrali EBS z elementami *smart home* firmy Fibaro, ActiveView Enterprise oraz wykład partnera z Polskiej Izby Systemów Alarmowych.
Po części oficjalnej miała miejsce uroczysta gala, uświetniająca jubileusz firmy EBS, z udziałem rewelacyjnej, jak zawsze, Grupy MoCarta.

Doceniając ogromny wkład merytoryczny wszystkich tegorocznych ekspertów i prelegentów, firma EBS już dziś zaprasza na kolejną konferencję za rok! □

Współpraca samorządów, obywateli i biznesu na 10. Smart City Forum

W połowie września 2019 r. w Arche Hotel Krakowska odbyła się X jubileuszowa edycja Smart City Forum. Jej jesienna edycja przyciągnęła niemal 600 uczestników. Przedstawiciele samorządów i biznesu zastanawiali się nad rozwojem miast nowej generacji, który skupi się nie tylko na nowych technologiach, ale także na potrzebach mieszkańców i ich roli w aglomeracjach.

Sprawna i komfortowa komunikacja miejska, elektromobilność, rewitalizacja, dofinansowanie, dostęp do programów senioralnych oraz inteligentna infrastruktura – to tylko niektóre zagadnienia poruszone podczas panelu inauguracyjnego, poświęconego tematyce przyjaznych miast. Podczas pierwszej debaty przedstawiciele samorządu i biznesu podkreślili, że miasta przyjazne mieszkańcom biorą pod uwagę ich konkretne potrzeby.

Zrównoważony rozwój to zagadnienie, które często pojawiało się w ramach rozmów o ewolucji inteligentnych miast. Nie zabrakło przykładów implementacji zielonych rozwiązań w strategii rozwoju małych i średnich aglomeracji.

Nie zabrakło także analizy wyzwań oraz możliwości związanych z „cloudyzacją" miast oraz zintegrowanym zarządzaniem opartym na danych. Formuła okrągłych stołów była idealną okazją do wymiany opinii i doświadczeń wokół idei *smart city*:

- Jak skuteczniej implementować ideę *smart city* w kontekście finansowania i wdrażania inteligentnych rozwiązań.
- Rowery, hulajnogi, skutery elektryczne – szansą czy problemem dla transportu miejskiego?
- Zarządzanie miastem oparte na danych.
- Gospodarka odpadami w „Zero Waste".
- Finansowanie inwestycji *smart city* z funduszy PFR.
- Efektywne systemy sterowania oświetleniem: dostępne funkcje a potrzeby miasta.

Smart City Forum to obowiązkowy punkt na mapie polskich konferencji dla wszystkich, którzy już dziś chcą brać czynny udział w procesie rozwoju miast.

Trwa Wielka Urodzinowa Loteria Hikvision!

Firma Hikvision już od 5 lat działa w Polsce i dostarcza najlepsze rozwiązania dla rynku zabezpieczeń. Dzięki rozbudowanej ofercie, zintegrowanym rozwiązaniom oraz ciągłemu, dynamicznemu rozwojowi w obszarze R&D Hikvision jest obecnie uznawana za najszybciej rozwijającego się producenta branży zabezpieczeń. Potwierdza to też stały wzrost przychodów rok do roku.

Anna Makowska, Marketing Specialist Hikvision Poland, powiedziała: *Jesteśmy dumni z tego, co udało nam się osiągnąć w ciągu mijających w tym roku, pełnych wyzwań 5 lat. Z okazji urodzin, trochę przewrotnie, to my postanowiliśmy obdarzyć prezentami naszych klientów. Każdy ma szansę wygrać, a to nasze podziękowanie za to, że klienci są z nami i wierzą w niezawodność produktów Hikvision.*

Loteria jest częścią kampanii z okazji 5. urodzin firmy. Z tej okazji Hikvision rozdaje samochody!

Jedyne, co musisz zrobić, to zarejestrować swój zakup na stronie loterii i czekać na ogłoszenie wyników losowania. Za każde wydane 1000 zł netto otrzymasz jeden los.

Szczegóły i regulamin loterii na stronie www.loteriahikvision.pl

TPC-BF2221-T Dahua – skuteczna broń w walce z palaczami

Dekadę temu Sejm RP zainteresował się problemem palenia tytoniu w miejscach publicznych, głównie w trosce o biernych palaczy. Rok później oficjalnie zabroniono palenia m.in. na terenie uczelni, w obiektach miejsc pracy, na przystankach czy w obiektach sportowych. Problem jednak pozostał.

Może to być efektem nieznajomości prawa przez turystów czy imigrantów albo ignorowania prawa przez chuliganów. Sprawa wydaje się trudna, ponieważ służby porządkowe jako priorytet stawiają bezpieczeństwo obywateli i potrzebują dodatkowego wsparcia ułatwiającego detekcję problemu oraz reagowanie.

Jak walczy się z palaczami na świecie? Kreatywność jest zaskakująca. W Szwecji np. wykorzystano billboardy zachęcające do rzucenia palenia. W reklamie pokazano jedynie czarno-białe zdjęcie twarzy mężczyzny, jednak cyfrowy billboard został wyposażony w ukryte czujki dymu. Gdy totem „wyczuwał" dym tytoniowy, mężczyzna na wyświetlaczu zaczynał głośno kaszleć. W Chinach postawiono na „wstyd społeczny". Na popularnej platformie WeChat stworzono oficjalny profil „No Smoking Beijing", na który obywatele mogą wysyłać zdjęcia osób niestosujących się do zakazu. Ulubieńcem pracowników może się okazać pomysł pewnej japońskiej firmy marketingowej. Szef korporacji zaoferował niepalącym dodatkowe 6 dni płatnego urlopu w ciągu roku. Z kolei Narodowa Agencja Środowiska w Singapurze zadecydowała o zamontowaniu 140 kamer wykrywających palaczy.

Na rynku są już dostępne rozwiązania idealne do takich wyzwań. Nowa kamera TPC-BF2221-T z budżetowej serii Dahua została wzbogacona o inteligentną analizę obrazu. Kamera ma dwa moduły: wizyjny i termowizyjny, dzięki czemu natychmiast otrzymuje się powiadomienie o wykroczeniu oraz portret palacza. Producent wyposażył ten model w diody LED i głośnik, który po wzbudzeniu alarmu może odtwarzać komunikaty ostrzegające. Kamera ta jest nowszą wersją bestsellera TPC-BF2120-T, który błyskawicznie znika z magazynów. Detektor termowizyjny w TPC-BF2221-T ma o 156% pikseli więcej niż poprzedni model.

NOWOŚĆ! Prosty system alarmowy bez centrali i skomplikowanego montażu

Niebawem na polskim rynku w ofercie OPTEX będzie dostępny moduł kamery VXi-CMOD. Rozszerza on funkcjonalność zewnętrznych czujek PIR z serii VXi.

CMOD to bezprzewodowy moduł kamery panoramicznej HD o kącie widzenia 180°, umożliwiającej rejestrację obrazu w ciemności. Razem z czujkami z serii VXi tworzy kompletne rozwiązanie do wizyjnej weryfikacji alarmów. Szczególnie dobrze sprawdza się w użytkowaniu w warunkach domowych.
Jak to działa? Czujkę VXi wraz z modułem VXi-CMOD podłączamy do prądu i Wi-Fi. Kolejnym elementem systemu jest intuicyjna w obsłudze aplikacja na telefon, dzięki której otrzymujemy powiadomienia. Możemy też sami „podejrzeć", co dzieje się w nadzorowanym obszarze.
Zestaw można wykorzystać nie tylko do detekcji intruza, ale także do monitorowania aktywności wokół domu, np. powrót domowników, przybycie kuriera czy niezapowiedziani goście.
Sprawdzona konstrukcja czujki VXi zapewnia odporność na małe zwierzęta. Innowacyjne podejście firmy OPTEX do ochrony obiektów mieszkalnych może znaleźć wiele zastosowań.
Więcej informacji na stronie www.optex-europe.com

FIRST Robotics Competition – zdolne dzieciaki z Polski potrzebują wsparcia!

FIRST Robotics Competition to międzynarodowy konkurs robotyczny, określany mianem największego i najbardziej prestiżowego konkursu tego typu na świecie. Przeznaczony jest dla uczniów w wieku 14-18 lat.

Corocznie drużyny składające się z co najmniej 12 młodych osób mają 6 tygodni na stworzenie strategii, zaprojektowanie, zbudowanie i zaprogramowanie robota. Tematyka i zadania, jakie robot ma wykonać, zmieniają się każdego roku, co niewątpliwie sprzyja rozwojowi kreatywności. Aby podołać presji czasu, każdy członek drużyny ma w niej swoje określone miejsce. Znajdziemy tutaj zatem programistów, elektroników, mechaników, a także osoby odpowiedzialne za zdobywanie partnerów i promocję. Dzięki temu konkurs przygotowuje zdolnych młodych ludzi do pracy na rynku nowych technologii i pozwala zdobyć doświadczenie w pracy zespołowej.
Uczniowie z najlepszych szkół w Polsce wezmą w nim także w tym roku udział. W rywalizacji międzynarodowej wystąpi grupa pod nazwą Team RaByte, składająca się z około 30 – zapalonych pasjonatów robotyki i nowych technologii. Wielu z nich uczestniczyło już z sukcesem w podobnych konkursach w Polsce i za granicą, przy współpracy z firmami prywatnymi oraz kołami naukowymi uczelni wyższych – Politechniki Warszawskiej czy Szkoły Głównej Handlowej w Warszawie.
Uczestnictwo w konkursie wymaga nakładów finansowych: łącznie ok. 144 tys. zł, na co składa się koszt zestawu startowego, opłata rejestracyjna, wydatki na transport i zakwaterowanie, a także koszt dodatkowych elementów konstrukcyjnych.
Dzieciaki wspiera już kilka firm i dumni rodzice. Potrzebują jednak więcej środków finansowych do realizacji swoich marzeń. Najlepsze zespoły mają szansę uczestniczyć w wielkim finale w USA, w rywalizacji obserwowanej przez setki tysięcy fanów oraz największe na świecie firmy technologiczne!
W zamian proponują hojnym sponsorom miejsce na swoich strojach konkursowych, a nawet możliwość zamieszczenia informacji o sponsorach i mecenasach na robotach (logotyp) i dedykowanych do tego celu stronach internetowych.
Jeżeli jesteś fanem nowych technologii, chcesz pomóc zdolnym młodym pasjonatom w osiągnięciu sukcesu – wesprzyj działania polskich uczniów w konkursie FIRST Robotics Competition. Dzięki temu nie tylko pomożesz innym, ale także sobie – bo o Twojej firmie może dowiedzieć się cały świat nowoczesnych technologii!
Zapraszamy na spotkanie z młodzieżą z zespołu Team RaByte do Jachranki w dniach 23-24 października, podczas tegorocznych Ogólnopolskich Dni Zintegrowanych Systemów Bezpieczeństwa Schrack Seconet i Partnerzy.
Więcej informacji na https://www.rabyte.pl/pl/
kontakt: biz@rabyte.pl

Grzegorz Ćwiek

Dobrze zaplanowana i nieprzerwana ewolucja

MARIUSZ KUCHARSKI, A&S Polska: Spotykamy się każdego roku jesienią i dyskutujemy o sprawach ważnych dla firmy Schrack Seconet i całego rynku systemów bezpieczeństwa w Polsce. Mamy za sobą trzy kwartały tego roku, przed nami chyba najważniejszy okres w roku. O czym, z Pana perspektywy, warto poinformować czytelników A&S Polska?

GRZEGORZ ĆWIEK, prezes Schrack Seconet Polska: Przede wszystkim dziękuję, że A&S nie zapomina o nas i rzeczywiście wnikliwie przygląda się naszej działalności w Polsce. To prawda, jesień jest doskonałą porą na tego typu rozmowy. Właśnie na przełomie września i października w takich firmach, jak nasza – w wymiarze zarówno krajowym, jak i międzynarodowym – podejmujemy najważniejsze decyzje, identyfikujemy wyzwania i planujemy przyszłość – tę bliższą i tę dalszą. Spraw, które się dzieją wokół nas na rynku oraz wewnątrz firmy, jest wiele i z przyjemnością podzielę się z Czytelnikami A&S naszymi spostrzeżeniami oraz planami na przyszłość, a tych zawsze jest dużo.

Jak zwykle wszelkie zmiany i nowości, które przedstawiamy, mają charakter ewolucyjny – czy to w sferze produktów i usług, czy w obszarze organizacyjnym. Jesteśmy pod tym względem chyba najbardziej stabilną firmą w naszej branży i taki charakter funkcjonowania jest wpisany w naszą misję i wizję. Z przyjemnością opowiem o kwestiach najważniejszych.

Wielkimi krokami zbliża się nasza flagowa impreza: Ogólnopolskie Dni Zintegrowanych Systemów Bezpieczeństwa Schrack Seconet i Partnerzy. W tym roku spodziewamy się zdecydowanie rekordowej frekwencji. Wydarzenie to każdego roku przyciąga nowych specjalistów chcących poszerzyć swoją wiedzę w zakresie zintegrowanych systemów bezpieczeństwa – zarówno po stronie projektantów, jak i wykonawców oraz – co ważne – samych użytkowników i właścicieli obiektów, które są chronione przez nasze urządzenia i produkty naszych Partnerów. W tym roku postanowiliśmy znowu nieco zmienić formułę tego spotkania. Chociaż zmiany będą pozornie niewielkie, powinny przynieść znaczne korzyści odwiedzającym nas gościom. Po pierwsze jako wsparcie merytoryczne dołączą do nas eksperci ubezpieczeniowi i rzeczoznawcy SITP. Przybędą zatem dwie dodatkowe sale warsztatowe, a pokaz integracji zostanie wzbogacony o komentarze najbardziej znanych i cenionych ekspertów z tych obszarów. Ponadto w reakcji na prośby uczestników naszych „jachrankowych" wydarzeń na koniec każdego z dwóch dni wszyscy Partnerzy Merytoryczni i Technologiczni będą prowadzili otwartą sesję pytań i odpowiedzi. Z pewnością w jeszcze większym stopniu umożliwi to integrację całego środowiska wokół niezwykle ważnych dla branży tematów.

Naszym celem jest wywołanie dyskusji i wspieranie komunikacji między uczestnikami naszych spotkań. W polskim prawie jest zbyt wiele niejasności, wytyczne mają zbyt wiele luk. Pragniemy, by organizowane przez nas imprezy edukacyjne ułatwiały konsolidację środowiska, wypracowywanie wspólnych praktyk – tak szczególnie ważnych na rynku systemów bezpieczeństwa.

Rzeczywiście, impreza ta stanowi ważny punkt w harmonogramie spotkań branżowych. Każdego roku obserwujemy szereg udoskonaleń w sposobie realizacji tego przedsięwzięcia. Czy w zakresie prezentowanych urządzeń i systemów także należy spodziewać się zmian i nowości?

W obszarze urządzeń prezentowanych w Jachrance staramy się także łączyć teraźniejszość z przyszłością. Zarówno nasze zespoły techniczne, jak i nasi koledzy i koleżanki z firm partnerskich starają się pokazać rozwiązania z jednej strony najbardziej innowacyjne, z drugiej – już sprawdzone. Naszą przewagą jest to, że wszystkie prezentowane przez nas urządzenia są wcześniej sprawdzane pod kątem kompatybilności połączeń, jakości i ciągłości wymiany informacji oraz niezawodności działania. Odwiedzający nas goście mogą być pewni, że jeżeli jakiekolwiek urządzenia i systemy są prezentowane podczas naszych pokazów, ich integracja została wykonana i dokładnie sprawdzona. To dość unikalny przykład współpracy firm z różnych, choć pokrewnych, branż, regionów Europy lub świata. Bywa, że budowę systemów zintegrowanych realizujemy z Partnerem, który w innym obszarze jest naszym konkurentem. Jesteśmy przy tym orędownikami standaryzowania pewnych działań wdrożeniowych i odbiorowych w dziedzinie integracji systemów zabezpieczeń i tym próbujemy zarażać innych.

Mając jedenastu Partnerów, o działaniu urządzeń i systemów oraz zasadach integracji będziemy mówili w trzynastu salach warsztatowych! Nie sposób wymienić wszystkich nowości, ale wiem, że każdy prelegent będzie chciał zaprezentować najnowsze funkcje swoich systemów i praktyczne możliwości ich zastosowania w obiektach budowlanych. Schrack Seconet pokaże cały przekrój produktowy swojej oferty: system SAP (kolejna odsłona Integrala IP) wraz z integratorem urządzeń przeciwpożarowych (SIS-FIRE), dźwiękowy system ostrzegawczy (APS-APROSYS) oraz system komunikacji szpitalnej (VISOCALL IP). Ważnymi elementami prezentacji będą także czujki specjalne (system zasysający ASD oraz liniowa czujka temperatury Listec).

Nowością w sposobie prowadzenia pokazów zadziałania urządzeń będzie nasza „matryca integracji" – narzędzie organizacyjne, które od wielu już lat współtworzymy wraz z naszymi Partnerami Technicznymi i Merytorycznymi. To zestaw wskazówek służący lepszemu zrozumieniu interakcji między różnymi systemami. Jestem ciekaw, jak zostanie ona przyjęta przez szersze środowisko.

Schrack Seconet jest znany na rynku z eksperymentowania. To właśnie Schrack po raz pierwszy wprowadził na rynek wiele nowatorskich rozwiązań technicznych, stoi za wieloma przełomowymi pomysłami w zakresie zarówno produktów, jak i organizacji czy marketingu w naszej branży. Na rynku już od kilku miesięcy mówi się o tych już dokonanych, ale i planowanych zmianach w organizacji Schrack Seconet Polska.

Jesteśmy ważnym partnerem dla wielu firm w Polsce – naszych bliższych i dalszych współpracowników, klientów. To z nimi rozwijamy naszą działalność. Nasi interesariusze wystawiają nam najlepsze oceny za produkty, a nasz zespół jest uznawany przez wielu z nich za najlepiej zorganizowany mechanizm w branży. Jako pierwsi i dotychczas jedyni na rynku systemów sygnalizacji pożarowej stworzyliśmy wzorowo działającą formułę dystrybucji produktów i usług opartą na Autoryzowanych Partnerach, z jasnymi i dobrze opisanymi zasadami współpracy.

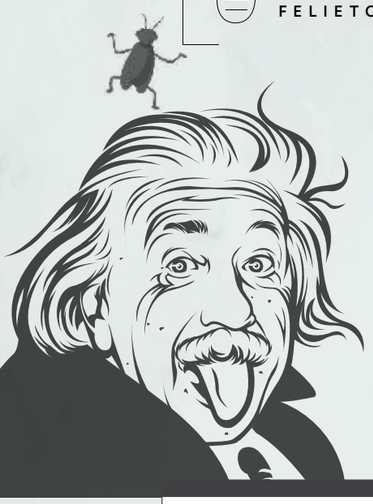
W 2019 r. dokonaliśmy kolejnej modyfikacji tego modelu oraz udoskonaliliśmy system certyfikacji. Nowe możliwości podejmowania pracy z nami na rynku mają dzisiaj Partnerzy Pre-Autoryzowani, otrzymujący od nas duży kredyt zaufania na starcie, ale posiadający wiele obowiązków jakościowych i organizacyjnych wobec nas i użytkowników końcowych. W tym roku przeprowadziliśmy proces recertyfikacji ponad 700 wdrożeniowców-programistów, a każdego roku szkolimy łącznie ponad 3500 osób – projektantów, instalatorów, wykonawców, użytkowników.

Mimo że jesteśmy spółką-córką Schrack Seconet AG, w przeciwieństwie do wielu innych przedstawicielstw firm zagranicznych w Polsce mamy dużą autonomię w działaniu i pełne zaufanie naszej spółki-matki. Dzięki temu możemy realizować i pionierskie, i czasem zwariowane pomysły, które z kolei od wielu już lat przynoszą nam wiele radości i satysfakcji. Nasza kreatywność jest przez rynek nagradzana ciągłym wzrostem zainteresowania naszymi produktami oraz napływającymi niemal codziennie zgłoszeniami chęci dołączenia do naszego zespołu. A zespół jest doskonały! Rozwija się nieustannie i dzisiaj możemy pochwalić się wieloma wybitnymi postaciami, specjalistami doskonale znanymi i szanowanymi w branży. Każdego roku notujemy też wzrost sprzedaży, bieżący zapowiada się pod tym względem znowu doskonale.
Największą zmianą w organizacji firmy w 2020 r. będzie jednak (i tu pewnie zaskoczę wielu czytelników) zmiana na stanowisku prezesa Zarządu. Taką decyzję podjąłem już wczesną wiosną tego roku i aktualnie wdrażamy program mojej sukcesji.

To duże zaskoczenie i dla naszej redakcji, i na pewno dla Czytelników A&S Polska. Proszę koniecznie przedstawić więcej szczegółów – to bardzo ważna informacja. Czy zdradzi Pan swoje plany na przyszłość?

Tak się domyślam, dlatego też – zgodnie z planem – od miesiąca realizujemy program stopniowego powiadamiania rynku o mojej sukcesji. Z informacją tą docieramy już do naszych klientów, partnerów oraz innych interesariuszy, do których wiadomość ta wcześniej nie dotarła. Przekaz ten jest bardzo ważny, bo... niczego nie zmienia. Może zabrzmiało to nieco żartobliwie, ale ponieważ moja rezygnacja z funkcji prezesa Zarządu odbywa się zgodnie z długo przygotowywanym planem oraz przy pełnej zgodzie i współpracy z naszym zespołem w Polsce oraz kolegami w Wiedniu – jest to doskonały przykład realizacji naszej misji i wizji, o której mówiłem wcześniej. Cechuje nas stabilność emocji, przekonań, celów i wartości. Dlatego także o fakcie tym powiadamiam Państwa osobiście już na rok przed zakończeniem mojej misji, którą (mam nadzieję) z powodzeniem realizuję od trzynastu już lat, będąc jednocześnie zaangażowany w sprawy firmy Schrack od ponad dwudziestu jeden lat.
Nowy prezes Zarządu, którego powołamy latem przyszłego roku, będzie kontynuował politykę i filozofię działania firmy, której byłem (wraz z całym zespołem i moimi poprzednikami) twórcą i realizatorem. Będzie z pewnością kontynuował doskonałe, wieloletnie relacje z rynkiem i nawiązywał nowe w duchu ciągłości idei, jakie nam przyświecają od ponad trzydziestu lat działalności w Polsce.
Jestem dzisiaj zaangażowany w proces sukcesji, wyboru kandydatów i za cały ten program odpowiadam. Moim celem jest nie tylko wspieranie firmy aż do momentu mojego odejścia z funkcji Prezesa Zarządu, ale także uczestniczenie w dalszym jej rozwoju, choć już nie w sposób bezpośredni.
Opuszczę w 2020 r. fotel prezesa, by zająć się poszukiwaniem nowych i ciekawych technologii i wiedzy oraz śledzić światowe rozwiązania w dziedzinach, którymi firma Schrack Seconet mogłaby być zainteresowana w przyszłości. Dotyczy to zarówno Polski, jak i rynków międzynarodowych. Moja działalność będzie zatem uwzględniała współpracę ze Schrack Seconet w Polsce i Schrack Seconet AG na świecie. Jestem także przekonany, że w jakimś zakresie pozostanę w kontakcie z czytelnikami A&S Polska i będę mógł przekazać Państwu kolejne, ciekawe wiadomości...

Czekamy na dobre wieści i życzymy dalszych sukcesów



Co ma karaluch do Einsteina

Warszawskie metro ma kłopot z nieodpowiedzialnymi użytkownikami schodów ruchomych i zaczęło z ich powodu współpracę z policją, a nawet powiadomiło ABW. Podziemna kolej posiada 142 ciągi schodów z przyciskami awaryjnego zatrzymywania. W 2017 r. naciśnięto je bez potrzeby ok. 10,5 tys. razy, a w roku ubiegłym ok. 9,5 tysiąca. Efekt – obniżenie poziomu bezpieczeństwa i stopnia niezawodności urządzeń oraz szybsze ich zużywanie.

Projektanci powinni przewidywać następstwa ruchów, jak szachiści. Tu nie domyślili się, że metrem, którym jeździ ponad 600 tys. pasażerów dziennie, jakiś promil głupawych albo złośliwych użytkowników może taki przycisk bez powodu nacisnąć. Wymyślono rozwiązanie zaradcze, które mogło zaistnieć od razu, bo to nie poziom techniki z górnej półki – zasłonięto guzik uchylną klapką z sygnałem dźwiękowym. Słychać i widać, kto alarmuje. Instalacje rozpoczęto od II linii metra i stacji Dworzec Wileński, „rekordzistki" w tej pladze.

Płoną świątynie. Wtedy czasami wychodzi na jaw, że nawet cenne zabytki nie miały obowiązkowych zabezpieczeń bądź źle realizowano procedury ochrony, jeśli w ogóle były. Dwa lata temu spłonęła duża część wieży katedry w Gorzowie. Cała Polska oglądała pożar w telewizji. Powstały nieodwracalne szkody w 700-letniej substancji zabytku, a koszt odbudowy oszacowano na ok. 20 mln zł. Obecny i były proboszcz – zarządcy obiektu – usłyszeli prokuratorskie zarzuty o uchybienia w ochronie ppoż. zagrażające życiu, zdrowiu osób i mienia w wielkich rozmiarach.

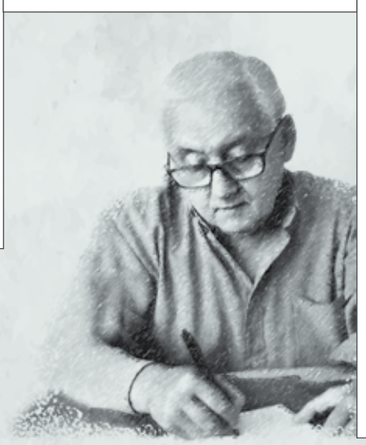
Eks-proboszcz poddał się dobrowolnie karze wymierzonej przez sąd: rok więzienia w zawieszeniu i 7 tys. zł grzywny; wyrok jest nieprawomocny. Obecny nie zgodził się z zarzutami i jego proces przebiegnie od początku. Cóż było nie tak? Brakowało sprawnego systemu sygnalizacji pożarowej i nie wykonywano badań rezystancji instalacji elektrycznej wieży. Nie oddzielono też wieży od świątyni drzwiami o odpowiedniej odporności ogniowej, choć jest ona odrębną strefą pożarową. Nie opracowano instrukcji określającej zasady prowadzenia ewakuacji, oddymiania obiektu i prowadzenia działań gaśniczych. Ta historia może być przestrogą dla innych duchownych.

Nie wszystkie nagrody Ig Nobel (tzw. Antynoble) wręczane na prestiżowym Uniwersytecie Harvarda są dziwne, śmieszne lub groteskowe. Pewien laureat Antynobla otrzymał później prawdziwego. Impreza popularyzuje naukę, bo dotyczy badań wykonywanych metodami naukowymi. Nagrody Ig Nobel mają astronomiczną wartość 10 trylionów dolarów Zimbabwe, tzn. waluty całkowicie bezwartościowej. Wśród aktualnie nagrodzonych znalazło się np. spostrzeżenie, że banknoty rumuńskich lejów są najbrudniejsze, bo najdłużej przechowują się na nich trzy rodzaje groźnych bakterii. Powodem jest zastosowanie w papierze włókna polimerowego utrudniającego podrabianie i przedłużającego trwałość banknotu... Efektem ubocznym jest jednak rozwój i przenoszenie patogenów odpornych na leki.

Nagrodzeni zostali Polacy w międzynarodowym zespole. Odkryli, że żywe karaluchy (a także inne owady) mogą wykrywać pola magnetyczne i same się magnesować. Zauważyli również, że żywe karaluchy rozmagnesowują się dużo szybciej niż... nieżywe. Temat badania jest śmieszny, ale pozornie. Wnioski rozszerzają wiedzę o różnych sposobach postrzegania świata rzeczywistego. Mogą też znaleźć odbicie w ulepszonych czujnikach zainspirowanych odpowiednikami biologicznymi.

Z RODO nie ma żartów. Prezes UODO największą do tej pory karę administracyjną nałożył na spółkę Morele.net – ponad 2,8 mln zł. Uznał, że zastosowane przez tę internetową firmę środki organizacyjne i techniczne ochrony danych osobowych nie były odpowiednie do ryzyka związanego z ich przetwarzaniem. W niepowołane ręce dostały się dane 2,2 mln klientów. Firma nie przygotowała też odpowiednich procedur reagowania na wypadek pojawienia się nietypowego ruchu w sieci.

Jakie dane może stracić klient, kupując banalną rzecz w źle chronionym sklepie internetowym? To personalia, numer telefonu, adres e-mail i doręczeniowy. Ale już w przypadku wniosków ratalnych: nr PESEL, serię i nr dokumentu tożsamości, informację o wykształceniu, adresach zameldowania i do korespondencji, źródle dochodu, wysokości dochodu netto, kosztach utrzymania gospodarstwa domowego, stanie cywilnym, wysokości zobowiązań kredytowych czy alimentów. Dla przestępców – a także ciekawskich zbierających prywatnie i służbowo wiedzę o człowieku – takie informacje są jak biblijna manna z nieba. □



TEKST
Andrzej Popielski

Dziennikarz, fotograf. Autor felietonów o bezpieczeństwie w „Systemach Alarmowych" (w latach 2005–2015).

Sztuczna inteligencja

Nowa era monitoringu wizyjnego

- **Czarna lista:** precyzyjnie zidentyfikuj podejrzanego oraz wyzwalaj alarm w czasie rzeczywistym. Przechwytuj twarze z wielu kamer oraz śledź trasy obserwowanych osób.
- **Kilenci VIP:** błyskawicznie identyfikuj klientów VIP w systemie i wyzwalaj operacje towarzyszące, w celu zwiększenia ich stysfakcji.
- **Metadane:** w szybki sposób wyszukuj interesujące fragmenty nagrań dzięki informacjom przechowywanym w postaci metadanych: wiek, płeć, ekspresja itp.
- **Wyszukuj według wzorca:** sprawnie przeszukuj nagrania używając zdjęcia, a nawet portretu pamięciowego.

Polecane modele

IPC-HFW7442H-Z

4 Mpx IR
kamera sieciowa AI

SDT5A404VA-2F

2 Mpx + 4x 4 Mpx
kamera sieciowa AI

SD8A820WA-HNF

4K 20 x zoom Starlight+
IR kamera sieciowa AI

NVR5432-16P-I

32-kanałowy 1,5U 16PoE
sieciowy rejestrator AI

CE FC ISO 9001:2000

www.dahuasecurity.com/pl

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