CZASOPISMO RYNKU SECURITY

№ 05
2020 (23)
wrzesień / październik

a&S POLSKA

PRZEMYSŁ 4.0

15 zł
(w tym 8% VAT)

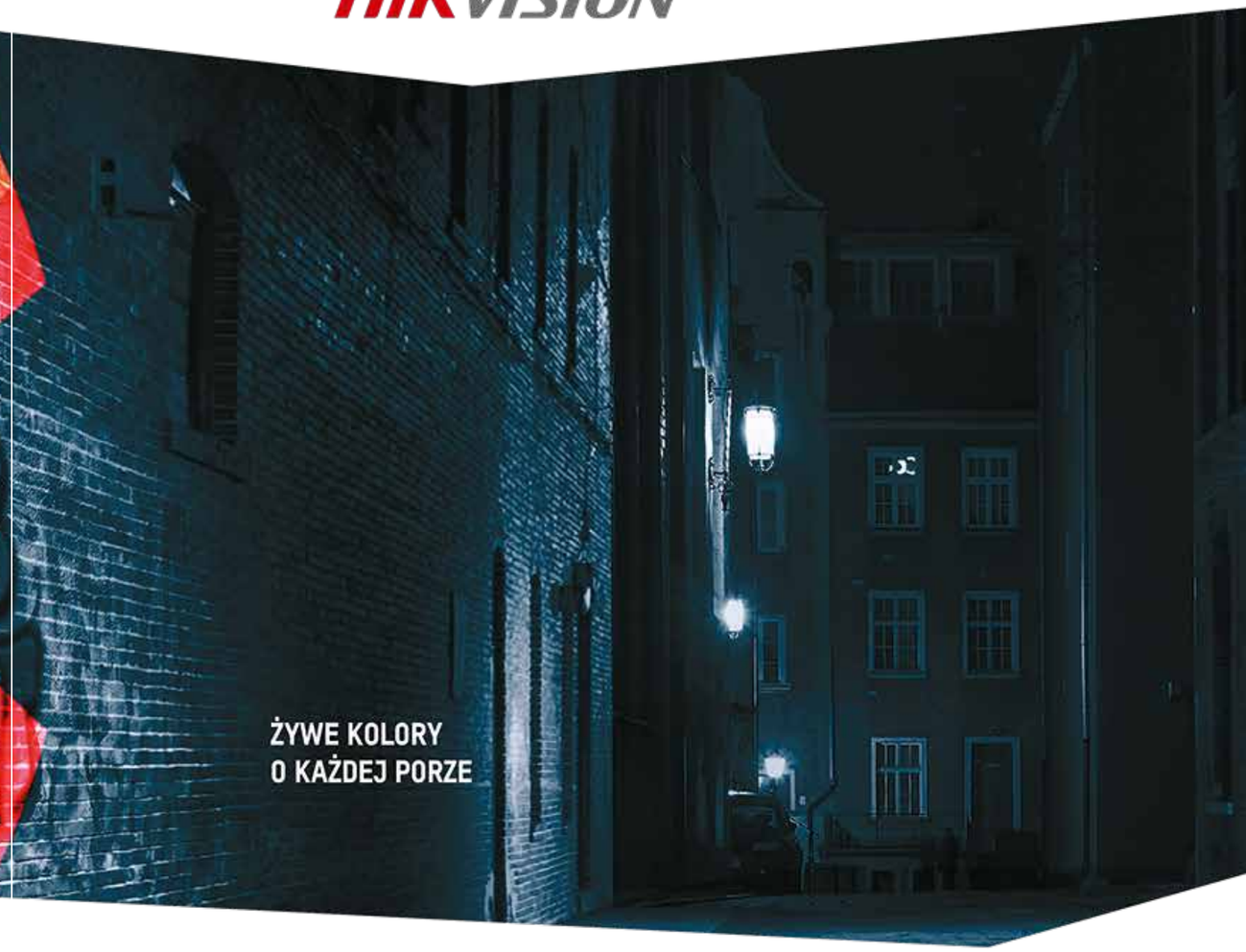
ISSN 2451-5175
05
9 772451 517703

www.aspolska.pl

TECHNOLOGIA COLORVU
ŻYWE KOLORY, NAWET W CIEMNOŚCI

Hikvision Poland
Żwirki i Wigury 16B
02-092 Warszawa
T +48 22 4600150
info.pl@hikvision.com

HIKVISION



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

Hikvision to międzynarodowy lider w dostawie produktów i rozwiązań monitoringu wizyjnego.
Nowa technologia ColorVu zapewnia jasne, kolorowe obrazy nawet w otoczeniu pozbawionym światła.
Lepsze soczewki, bardziej zaawansowane czujniki i dodatkowe miękkie oświetlenie dają obraz świetnej jakości, nawet w ciemności.

ColorVu

DOŁĄCZ DO PROGRAMU PARTNERSKIEGO HIKVISION I UZYSKAJ DOSTĘP DO WIELU KORZYŚCI.
https://partner.hikvision.com/

@HikvisionPoland
www.hikvision.com/pl/

EDYTORIAL

Drodzy Czytelnicy

Walka z pandemią COVID-19 trwa. Z jej konsekwencjami mierzymy się wszyscy. W życiu osobistym zmagamy się z groźbą zachorowania lub skutkami zakażenia. W życiu zawodowym walczymy o utrzymanie miejsc pracy i przetrwanie naszych firm. Gospodarka na całym świecie musi się dostosować do nowych warunków. O tym, jak firmy branży security radzą sobie w tych trudnych czasach, piszemy na s. 18. Ekonomiczne konsekwencje pandemii nie ominą także światowego rynku kontroli dostępu (s. 21). Pandemia to czas najtrudniejszych zagrożeń dla biznesu i dużych wyzwań dla firm ochrony. W czasach kryzysu zarządzanie bezpieczeństwem jest utrudnione ze względu na zagrożenia wewnętrzne w przedsiębiorstwie, gdyż zespoły ochronne są często skoncentrowane na bezpieczeństwie epidemiologicznym (s. 34). Firmy ochrony muszą również walczyć o klienta. Jednym ze sposobów na jego utrzymanie może być wprowadzenie opcji monitoringu na minuty (s. 30).

Koronawirus zakłóca również funkcjonowanie miast. Przykładem dla naszych włodarzy mogą być zalecenia Bristolu i Glasgow, o których piszemy w czwartej części cyklu poświęconego budowaniu odporności miejskiej na s. 80.

Tematem przewodnim tego wydania jest bezpieczeństwo obiektów przemysłowych i rozległych. Nie ulega wątpliwości, że konsekwencją COVID-19 będzie szersze zastosowanie nowych technologii. W przemyśle 4.0 będą to automatyzacja i robotyka (s. 38). Ważnym tematem jest też integracja systemów, a jej podstawową fazą – projektowanie (s. 24). Ale inwestycje w nowoczesne technologie to nie wszystko, ważna jest również automatyzacja ruchu osobowo-materiałowego (s. 54). Najważniejszym celem każdego przedsiębiorstwa jest utrzymanie ciągłości działania (wywiad na s. 42). Wiedzę najlepiej jest czerpać z doświadczeń innych, głos zabierają więc przedstawiciele różnych sektorów gospodarki (s. 56).

Zastosowanie nowoczesnych technologii wiąże się z korzyściami, ale też z zagrożeniami czyhającymi w sieci. Jak unikać cyberataków, piszemy na s. 74, a o potencjale sztucznej inteligencji w cyberbezpieczeństwie na s. 78. W zakładach produkcyjnych bardzo ważne jest również bezpieczeństwo pożarowe (s. 64). W tym wydaniu prezentujemy ofertę elektronicznych systemów ppoż. oraz różne metody gaszenia pożaru.

Ze względu na utrzymujące się zagrożenie epidemiczne podjęliśmy decyzję o zmianie formuły konferencji **Warsaw Security Summit.** Na nowe czasy proponujemy nową formułę – ***content hub.*** Konferencja nie będzie wydarzeniem transmitowanym na żywo – będą to wcześniej przygotowane profesjonalne materiały wideo gotowe do obejrzenia w wygodnym miejscu i czasie. Wzorem serwisów VoD materiały od daty premiery będą dostępne przez rok!
Wiemy, że trudno znaleźć kilka godzin w ciągu dnia na transmisję konferencji na żywo. Dlatego – jak w serwisie „wideo na żądanie" – będzie można samemu zdecydować co, kiedy i w jakiej kolejności obejrzeć...
Premiera Warsaw Security Summit w nowej formule odbędzie się 17 listopada na www.WarsawSecuritySummit.eu.

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

Dział marketingu i reklamy
Iwona Krawiec

Dział eventów i konferencji
Jolanta A. Kucharska
Aleksandra Czapska

Projekt graficzny i skład
Bogusław Kalwala

Redakcja
Aura Sky Offices
ul. M. Rodziewiczówny 1 lok. 801
04-187 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

A&S POLSKA
ZŁOTY PARTNER

AXIS COMMUNICATIONS · BCS · HIKVISION · Linc Polska Sp. z o.o. · SCHRACK SECONET · TRUSTMAN

A&S POLSKA
SREBRNY PARTNER

dahua TECHNOLOGY

A&S POLSKA
WYDANIE ONLINE
www.aspolska.pl/czasopismo

SPIS TREŚCI

№ 05

2020 (23)

wrzesień / październik

a&S POLSKA

BEZPIECZEŃSTWO BIZNESU

PRZEMYSŁ 4.0

BEZPIECZEŃSTWO POŻAROWE

CYBERBEZPIECZEŃSTWO

BEZPIECZNE MIASTO

SERWIS INFORMACYJNY

ROZWIĄZANIA 3 FAZOWE ZE WSPÓŁCZYNNIKIEM MOCY 1.0

OFERTA CPH

- Konstrukcja modułowa do nawet 100kW
- Jednostkowy Współczynnik Mocy (kVA = kW)
- Dedykowana szafa rack z dotykowym ekranem LCD lub możliwość zainstalowania w prawie każdej szafie 19”
- Możliwość rozszerzenia o dodatkowe zestawy baterii
- Praca w trybie Hot-Swap pozwalająca wymieniać baterie bez potrzeby wyłączania sprzętu
- Dodatkowe karty SNMP i oprogramowanie do zarządzania

OFERTA CPG PF1

- Jednostkowy Współczynnik Mocy (kVA = kW)
- Równoległa praca nawet 3 jednostek
- Regulowana ilość baterii (od 32 do 40 sztuk)
- Trzystopniowa konstrukcja ładowania
- Dla wygody obsługi do urządzenia dodano panel dotykowy.
- Domyślnie zamontowana karta SNPM do monitorowania sprzętu
- Wersje z (BI) lub bez jednostek bateryjnych (BE)

AXIS COMMUNICATIONS www.axis.com/pl

Nowe kamery Axis do dozoru pokładowego

Axis Communications wprowadził na rynek dwa nowe modele kamer kopułkowych z serii AXIS P39 zapewniające znakomitą jakość obrazu w każdych warunkach oświetleniowych. Doskonale sprawdzą się w dozorze pokładowym, m.in. w pociągach, autobusach czy pojazdach ratunkowych.

Nowe kamery **AXIS P3925-R i AXIS P3935--LR** spełniają wszystkie normy obowiązujące w branży transportowej, w tym **EN50155, EN45545 i NFPA 130.** Ich metalowe obudowy **klasy IK10**, **IP66** oraz **IP67** chronią je przed wodą, korozją i pyłem. Zastosowana w urządzeniach technologia **Axis Forensic WDR** umożliwia rejestrowanie wysokiej jakości obrazów w scenie z ciemnymi i jasnymi partiami, a technologia **Axis Lightfinder** zapewnia ostry, kolorowy obraz w słabych warunkach oświetleniowych.

Model AXIS P3935-LR ma wbudowane diody LED działające w podczerwieni (dł. fali 940 nm) i umożliwiające dozór w całkowitej ciemności, bez rozpraszania kierowców ani pasażerów. Dwukierunkowy tor audio i wbudowany mikrofon pozwalają na dozór dźwiękowy i audiodetekcję.

Dzięki łatwemu dodawaniu aplikacji analitycznych różnych firm nowe kamery można wyposażyć w rozbudowane funkcje analityczne. Urządzenia można montować przodem do kierunku jazdy na desce rozdzielczej pojazdu, tak aby rejestrowały zdarzenia z perspektywy kierowcy. Elektroniczna stabilizacja obrazu zapewnia nieporuszony materiał wizyjny mimo drgań oddziałujących na kamerę.

Rozwiązanie znakomicie sprawdza się także podczas rejestrowania zdarzeń na zewnątrz pojazdu.

BCS www.bcscctv.pl

System kontroli dostępu od BCS

Rodzina produktów BCS wzbogaciła się o nowy system kontroli dostępu TCP/IP. W ofercie znalazły się rozwiązania zarówno autonomiczne, do pojedynczych drzwi, jak i sieciowe, pozwalające tworzyć systemy o większej liczbie przejść, programowane i kontrolowane za pomocą oprogramowania PC.

W przypadku wersji autonomicznej mamy do dyspozycji czytniki kart zbliżeniowych lub czytniki z klawiaturą, pozwalające na otwarcie drzwi za pomocą karty, kodu lub ich kombinacji. Mają już wbudowane wyjście przekaźnikowe, do którego można podłączyć bezpośrednio elektrozaczep lub zworę elektromagnetyczną, bez potrzeby stosowania dodatkowych urządzeń oprócz zasilacza. Programowanie odbywa się w dwóch trybach: za pomocą klawiatury czytnika lub oprogramowania **Smart PSS**.

System sieciowy składa się z całej gamy czytników (w różnych wariantach wykończenia i instalacji) umożliwiających otwarcie przejścia jak w przypadku rozwiązań autonomicznych (karta, kod lub ich kombinacja). Różnica polega na tym, że jest programowany za pomocą specjalnych kontrolerów i oprogramowania na PC-ety po sieci LAN, natomiast czytniki nie mają wbudowanych wyjść przekaźnikowych, lecz jedynie komunikują się z kontrolerem, który tutaj odpowiada za wszystkie funkcje systemu, w tym za otwarcie drzwi, co podnosi poziom bezpieczeństwa w systemie.

Za pomocą oprogramowania **Smart PSS** można programować czy nadzorować nie tylko systemy **KD**, ale również systemy **CCTV BCS Line**.

CIAS www.cias.com.pl

Bariera mikrofalowa z liniową strefą detekcji

MICRO-RAY to nowatorski produkt firmy CIAS Elettronica S.r.l. łączący podstawowe zalety barier podczerwieni i barier mikrofalowych.

Zastosowanie wiązki mikrofalowej zamiast wiązki podczerwieni pozwoliło ominąć ograniczenia, z jakimi spotykają się instalatorzy barier podczerwieni: niską odporność na zakłócenia związane z ulewnym deszczem, opadami śniegu, mgłą i innymi czynnikami tłumiącymi wiązkę IR. Istotną zaletą nowego rozwiązania jest wyeliminowanie grzałek do utrzymania przezroczystości osłony, co znacząco ogranicza zużycie energii i upraszcza instalację.

Obsługa serwisowa **MICRO-RAY** jest łatwiejsza niż barier podczerwieni. Urządzenie nie wymaga regularnego czyszczenia obudowy i optyki, gdyż nie zawiera układu optycznego i nie jest wrażliwe na zabrudzenia. Obniża to koszty eksploatacji i wydłuża czas pracy bariery bez obsługi serwisowej.

Zaawansowane technologicznie rozwiązania w **MICRO-RAY** pozwalają, podobnie jak w barierach podczerwieni, na uzyskanie bardzo wąskiej liniowej wiązki, ale mikrofalowej. Dzięki temu zastosowany algorytm detekcji jest nastawiony na wykrycie przecięcia wiązki, a nie, jak w typowych barierach mikrofalowych, na sygnalizowanie spadku mocy sygnału. Umożliwia to uzyskanie jednego, jasnego kryterium alarmu – przecięcie wiązki.

Podstawowe zalety barier mikrofalowych w połączeniu z wąską liniową wiązką mikrofal i algorytmami *fuzzy logic* pozwalają na użycie **MICRO-RAY** we wszelkich typach instalacji.

Więcej szczegółów na www.cias.com.pl

DAHUA TECHNOLOGY POLAND www.dahuasecurity.com/pl

Kamera sieciowa IPC-PFW83242-A180

Kamera sieciowa o kącie widzenia 180°, z panoramicznym obrazem o rozdzielczości 32 Mpix bez efektu „rybiego oka" i niespotykanej do tej pory szczegółowości obrazu. Najnowszy model IPC-PFW83242-A180 oferuje to wszystko dzięki wykorzystaniu czterech przetworników obrazu CMOS ze skanowaniem progresywnym o rozdzielczość 8 Mpix każdy.
Dzięki zastosowaniu przetworników o **przekątnej 1/1,8"** oraz jasnych obiektywów **F1.6** możemy być pewni, że doskonała jakość obrazu będzie dostępna bez względu na to, jak oświetlona jest scena. Zwiększona została nie tylko rozdzielczość, ale również czułość kamery. Poprawiony algorytm pozwala na uzyskanie połączonego obrazu ze wszystkich przetworników bez widocznych łączeń między nimi.
Uwagę w tej kamerze zwraca nie tylko jakość obrazu, ale również funkcjonalności, jakie daje implementacja algortytmów sztucznej inteligencji. Dzięki nim możliwe jest automatyczne zliczanie pojazdów i ludzi znajdujących się w obserwowanych strefach. Ponadto dostępna jest również analiza tłumu poprzez pomiar zagęszczenia (**liczba osób/m²**).
Oczywiście, tak jak dotychczas, do dyspozycji pozostają funkcje znane z innych modeli kamer **Dahua Technology**, takie jak detekcja przekroczenia wirtualnej granicy oraz wykrycie intruza w strefie.
Standardowo kamera ma obudowę wykonaną z metalu (**klasa szczelności IP67** i odporności mechanicznej **IK10**), która gwarantuje wysoką odporność na warunki atmosferyczne oraz akty wandalizmu.

HANWHA www.hanwha-security.eu

Kamery serii Wisenet P z technologią Deep Learning

Nowoczesne kamery firmy Hanwha Techwin serii Wisenet P zostały wyposażone w zaawansowane funkcje analizy obrazu, które wspierają działania pracowników ochrony, zapewniając automatyczne wykrywanie zdarzeń w monitorowanej przestrzeni. Wisenet P z analityką wykorzystującą sztuczną inteligencję (AI) to pierwsza seria kamer, w której Hanwha Techwin wprowadziła inteligentną analizę obrazu opartą na technologii *Deep Learning*. Dzięki temu skutecznie wykrywają intruza w oparciu o klasyfikację obiektów, takich jak człowiek i pojazd, eliminując fałszywe alarmy, które mogłyby zostać wywołane np. przez zwierzęta, poruszającą się roślinność lub zmienne warunki oświetleniowe.
Ponadto kamery Wisenet P pozwalają na stosowanie dodatkowych reguł dla sklasyfikowanych obiektów, np. przekroczenie linii, naruszenie (wejście/wyjście) strefy czy rozpoznanie kierunku poruszania się obiektu. Dzięki temu pracownik ochrony zostanie automatycznie powiadomiony o osobie przekraczającej ogrodzenie, wtargnięciu do niebezpiecznej strefy lub o samochodzie, który porusza się na terenie zakładu niezgodnie z obowiązującą organizacją ruchu. Wszystko to przy ograniczeniu liczby fałszywych alarmów praktycznie do zera.
Dodatkowo kamery serii Wisenet P wyposażono w funkcje, które można wykorzystać w okresie pandemii, takie jak weryfikacja liczby osób w danej strefie/obiekcie lub detekcja osób bez maseczek. Mogą pełnić wiele funkcji, zapewniając bezpieczeństwo osób i mienia.

HIKVISION www.hikvision.com/pl

Szybsza bezpieczna kontrola osób w firmie

W czasach pandemii kontrola dostępu do obiektu została postawiona przed kolejnym wyzwaniem. Dodatkowym aspektem warunkującym przyznanie prawa dostępu stała się weryfikacja temperatury i posiadania maseczki.
Firma Hikvision stworzyła specjalną linię terminali kontroli dostępu z serii MinMoe spełniających te wymagania. Nowy terminal pomiarowy DS-K1TA70MI-T, z wyjątkiem weryfikacji karty, kodu PIN, jest w stanie rozpoznać użytkownika na podstawie wzorca twarzy w czasie poniżej 0,2 sekundy z odległości nawet 1,8 m. Podwójny moduł kamerowy z algorytmem AI pozwala sprawdzić, czy osoby wchodzące mają założoną maseczkę lub przypominać o jej założeniu. Kamera termowizyjna mierzy temperaturę użytkownika z dokładnością +/-0,5 stopnia Celsjusza. Dwa wyjścia przekaźnikowe sterujące wejściem umożliwiają wpuszczenie osoby z normalną temperaturą lub zaalarmowanie za pomocą zewnętrznego sygnalizatora o temperaturze podwyższonej. Wyjście w standardzie Wiegand pozwala na współpracę z systemami kontroli dostępu firm trzecich.
Terminal można zamontować na wolno stojącym słupku, akcesoria do bramek przejściowych są dostępne w ofercie. Urządzenie może pracować w tandemie z monitorem DS-KC001, zapewniając zachowanie bezpiecznej odległości personelowi obsługi.

LINC POLSKA www.linc.pl

Najlepsze w swojej klasie obrazowanie | FLIR Quasar™ 4K IR PTZ

FLIR wprowadził nowe funkcje do kamery Quasar™ 4K IR PTZ. Oprócz rozdzielczości 4K, która zapewnia wyraźny obraz przy słabym oświetleniu, kamera ma też wbudowane oświetlacze IR i duży zoom optyczny x31, co pozwala na uzyskanie zasięgu obserwacji do 200 m, w dzień i w nocy.

Pracuje bez względu na warunki atmosferyczne w temperaturze od **-40 do 60°C**. Wbudowana wycieraczka oraz zdalnie sterowane spryskiwacze obiektywu zapewniają możliwość ciągłej pracy w odległych lub trudno dostępnych instalacjach.
Kamera ma też ulepszony szeroki zakres dynamiki **WDR,** co gwarantuje jej wysoką skuteczność. **FLIR Quasar™** łączy w sobie najnowszą technologię **PTZ**, optykę oraz mechanikę. Jest kompatybilna z różnymi rozwiązaniami **VMS,** dzięki czemu możliwa jest wygodna integracja zarówno z innymi rozwiązaniami marki **FLIR**, jak i produktami innych producentów.
Ponadto kamera została zaprojektowana z troską o bezpieczeństwo pracy w sieci. System zabezpieczeń cybernetycznych został wzmocniony i chroni przed najnowszymi zagrożeniami. Ulepszony interfejs sieciowy ułatwia konfigurację, a aktualizacja systemu zapewnia dodatkowe zabezpieczenie dostępu.
FLIR Quasar™ 4K IR PTZ jest rozwiązaniem kompleksowym, które bardzo dobrze sprawdzi się w monitoringu miejskim, w systemach dozoru wizyjnego infrastruktury krytycznej, na lotniskach i w wielu innych obiektach zewnętrznych wymagających wysokiego poziomu ochrony.

MERAWEX www.merawex.com.pl

Nowe zasilacze ZSP100 z certyfikatem CNBOP-PIB

Firma MERAWEX wprowadziła do oferty nowe typy zasilaczy do systemów automatyki pożarowej i oddymiania z rodziny ZSP100. Serię rozszerzono o wersje z maks. prądami wyjściowymi 7,5 A, 10 A i 12 A współpracujące z akumulatorami o pojemności do 75 Ah. Jednostka zasilająca jest zabudowana w szafce wiszącej, w której mieszczą się też akumulatory. Każdy zasilacz jest wyposażony w zespół sygnalizacji lokalnej (świetlnej) i zdalnej (przekaźnikowej). Sterownik mikroprocesorowy steruje pracą i kontroluje wszystkie obwody wyjściowe i bateryjne.
Urządzenia są standardowo wyposażone w 5 wyjściowych torów zasilania **24 VDC**. Wszystkie wyjścia są zabezpieczone osobnymi bezpiecznikami, co umożliwia podłączenie większej liczby urządzeń bez stosowania dodatkowych modułów bezpiecznikowych.
Seria ZSP100 obejmuje aż 19 modeli o prądach wyjściowych od 1,5 do 12 A, współpracujących z akumulatorami od 7 do 75 Ah. To obecnie najszersza na rynku grupa certyfikowanych zasilaczy zgodnych z normami EN 54-4 + A1 + A2 i EN 12101-10.
MERAWEX dostarcza też zasilacze do systemów DSO i certyfikowane zasilacze ZUP-230 V przeznaczone do zasilania gwarantowanym napięciem 230 VAC napędów bram w systemach oddymiania. Wszystkie mają certyfikat CNBOP-PIB na zgodność z normami EN 54-4 + A1 + A2 i EN 12101-10.
Do zasilaczy dostarczane są odpowiednie akumulatory serii MX i MXL. Dla najbardziej wymagających dostępne są certyfikowane przez niemiecki VdS akumulatory MXV.
Więcej informacji na www.merawex.com.pl

MIWI URMET www.miwiurmet.pl

FIREBEAM xtra – adresowalna analogowa czujka liniowa dymu

ESP FIREBEAM xtra to liniowa czujka dymu z optyką lustrzaną, o maksymalnym zasięgu detekcji 160 m. Nowo zaprojektowana optyka urządzenia zwiększa czułość detekcji, podczas gdy zaawansowane wewnętrzne oprogramowanie czujki redukuje fałszywe alarmy.

Czujka jest dostarczana z oddzielnym sterownikiem, który pozawala na uruchomienie, monitorowanie i konserwację urządzenia z poziomu gruntu. Urządzenie oferuje zaawansowaną funkcjonalność pozwalającą na samodzielne (silnik elektryczny) mechaniczne dopasowanie głowicy do ogniska reflektora w momencie uruchomienia. Podczas normalnej pracy urządzenie stale monitoruje poziom dopasowania głowicy nadajnika/odbiornika do centrum reflektora i w razie potrzeby (np. w następstwie drgań budynków) wykonuje automatycznie kalibrację.
ESP FIREBEAM xtra ma zintegrowany moduł pętli, który pozwala na jego podłączenie do analogowej adresowalnej pętli **ESP HOCHIKI**.

Właściwości
- Standardowy zasięg detekcji od 7 do 70 m Możliwość zwiększenia zasięgu za pomocą zestawów rozszerzeń nawet do 160 m
- Certyfikat VdS EN 54-12:2015
- Automatyczna korekcja dopasowania do lustra, eliminująca problem z drganiami i ruchami budynku
- Nowy projekt rozwiązań optycznych, redukujący fałszywe alarmy
- Kontrola i regulacja z poziomu gruntu dzięki zastosowaniu dedykowanego sterownika (w komplecie)
- Pełna kompatybilność z protokołem ESP HOCHIKI

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

TP-Link EAP265 HD – punkt dostępowy do najbardziej obciążonych środowisk

Omada EAP265 HD to punkt dostępowy od TP-Link zaprojektowany do pracy w najbardziej obciążonych środowiskach (sale konferencyjne, duże open space'y). Ten pracujący w standardzie AC1750 *access point* może obsłużyć aż 500 urządzeń klienckich jednocześnie.

Najważniejsze cechy produktu:

- prędkość transmisji do **1300 Mb/s** w paśmie **5 GHz** oraz do **450 Mb/s** w paśmie **2,4 GHz**
- dwa porty Ethernet **10/100/1000 Mb/s**
- technologie **MU-MIMO,** równoważenie obciążenia pasma i profesjonalne anteny zwiększają przepustowość w obciążonych sieciach, pozwalając na łączenie się wielu urządzeń jednocześnie
- scentralizowane zarządzanie: dostęp w chmurze i aplikacja **Omada** lub sprzętowy kontroler **OC200/OC300** dla wygody i łatwości zarządzania

- płynny roaming: urządzenia tworzą jednolitą sieć Wi-Fi w całym budynku. Smartfon użytkownika zawsze połączy się z AP oferującym mu najlepsze połączenie, bez przerywania transferu
- wsparcie **PoE:** obsługa standardu **802.3af/at** oraz pasywnego **PoE** (adapter PoE w zestawie).

Instalacja i połączenie **EAP265 HD** do sieci odbywa się za pomocą jednego przewodu. Dzięki technologii **PoE** (zasilanie i integracja z siecią **LAN**) znacznie ogranicza się koszty instalacji.

Punkty dostępowe z serii **EAP** pozwalają stworzyć wydajną i bezpieczną sieć **Wi-Fi.** Oprócz podstawowych funkcji bezpieczeństwa, mamy możliwość autoryzacji dostępu z uwierzytelnianiem przez SMS, Facebooka i logowaniem za pomocą strony powitalnej, voucherów lub jednorazowych haseł dostępu.

Produkt objęty jest 5-letnią gwarancją producenta.

W2 www.w2.com.pl

Nowa seria osłon zabezpieczających do sygnalizatorów przeciwpożarowych

Polski producent urządzeń sygnalizacyjnych – firma W2 – wprowadza do oferty nową serię osłon zabezpieczających OZ-50. Osłony są dedykowane głównie do sygnalizatorów przeciwpożarowych z członem optycznym serii **SO-Pd13** oraz **SA-K7N**. Ich zadaniem jest ochrona sygnalizatorów przed uszkodzeniami mechanicznymi w miejscach takich, jak strychy, piwnice czy hale sportowe.

Osłony są wykonywane ze stali malowanej proszkowo na kolor biały i składają się z dwóch głównych elementów: podstawy i kosza. Na podstawie umieszczono dwie aluminiowe nakrętki, które pozwalają zamocować do niej sygnalizator produkcji **W2.** Dodatkowo konstrukcyjnie przewidziano w niej otwory umożliwiające montaż do podłoża oraz przeprowadzenie przewodów. Podstawę z koszem łączy się za pomocą dwóch wkrętów. Kosz został tak ukształtowany, żeby nie wpływać na bryłę światła generowaną przez sygnalizator. **Osłona OZ-50** występuje w 3 odmianach: **OZ-50-1, OZ-50-2, OZ-50-3**, które różnią się wysokością kosza. Każda odmiana jest dedykowana do ochrony innej grupy sygnalizatorów.

W swojej ofercie firma ma też osłony **OZ-40 oraz OZ-40-2**. Wszystkie osłony mogą być stosowane do ochrony innych urządzeń pasujących do nich gabarytowo.

Firma **W2** produkuje również puszki instalacyjne, wieże i kolumny sygnalizacyjne oraz sygnalizatory przeznaczone do sektora automatyki przemysłowej. Zapraszamy do zapoznania się z pełną ofertą na stronie www.w2.com.pl.

SCHRACK SECONET POLSKA www.schrack-seconet.pl

Integral WAN – nowy wymiar sieciowych systemów bezpieczeństwa pożarowego

Integral WAN – najnowsza wersja sieci central sygnalizacji pożarowej/sterowania urządzeniami ppoż. serii Integral IP (MX, CX, BX) jest przeznaczona do łączenia dużej liczby central w spójny system bezpieczeństwa pożarowego, a także do integrowania obiektów rozproszonych (niezależnych instalacji) i centralnego zarządzania nimi.

Rozwiązanie charakteryzuje się bardzo wysoką niezawodnością działania m.in. ze względu na zastosowanie redundantnych kart sieciowych z nowej generacji platform B5A i B6A systemu Integral IP. Elastyczna architektura pozwala na zastosowanie różnych topologii sieciowych (pierścień, drzewo lub sieć kratowa) spełniających wymagania konkretnego projektu.

Zależnie od topologii sieciowej i liczby torów komunikacyjnych system może być odporny na 3 niezależne uszkodzenia (topologia pierścienia) lub nawet 7 niezależnych uszkodzeń (sieć kratowa). Połączenia między centralami są realizowane za pomocą przewodów miedzianych (skrętka) lub łączy światłowodowych jedno- i wielomodowych (prędkość transmisji danych aż 100 Mb/s).

W celu zintegrowania central można wykorzystać istniejącą infrastrukturę IT obiektu (sieć LAN), a nawet rozległą typu WAN. Sieć Integral WAN umożliwia łączenie central najnowszej platformy B5A i B6A z centralami starszej generacji (kompatybilność wstecz) w spójny system.

Do zarządzania całym układem sieciowym bezpieczeństwa pożarowego Integral WAN można stosować system integrujący urządzenia ppoż. SIS-FIRE i rozwiązania technologii Integral over IP.

BRANŻA SECURITY W CZASACH PANDEMII

COVID-19 WYSTAWIŁ NA PRÓBĘ WSZYSTKIE BRANŻE NA CAŁYM ŚWIECIE. PRZEMYSŁ SECURITY, W NIEKTÓRYCH KRAJACH SKLASYFIKOWANY JAKO DOSTAWCA USŁUG PODSTAWOWYCH, UCZY SIĘ DOSTOSOWYWAĆ DO OGRANICZEŃ NAKŁADANYCH PRZEZ WYMOGI PRAWA, ABY POWSTRZYMAĆ ROZPRZESTRZENIANIE SIĘ KORONAWIRUSA I PRZYWRÓCIĆ CIĄGŁOŚĆ ŁAŃCUCHA DOSTAW.

TEKST
Eifeh Strom
a&s International

Skupiając się na krótkoterminowych skutkach pandemii, firmy branży zabezpieczeń – dostosowując się do nowych wymagań i przechodząc do wydarzeń wirtualnych – podejmują wszelkie działania, aby przetrwać na rynku.

Krótko- i długoterminowy wpływ COVID-19

Zdrowie i bezpieczeństwo pracowników ma kluczowe znaczenie, ale firmy muszą również skupić się na kondycji swojej działalności, biorąc pod uwagę zarówno krótko-, jak i długoterminowe skutki pandemii. Skutki krótkoterminowe to przede wszystkim zakłócenia w łańcuchu dostaw. Wprowadzenie blokad na całym świecie wywołało zakłócenia w dostawach urządzeń. Zgodnie z przepisami w poszczególnych krajach wielu producentów musiało tymczasowo zawiesić pracę, niektórzy przestawili się na wytwarzanie innego rodzaju, np. środków ochrony osobistej. Na globalny łańcuch dostaw wpływają również ograniczenia eksportowe.

Aby zmniejszyć wpływ zakłóceń, firmy branży zabezpieczeń muszą monitorować łańcuch dostaw pod każdym kątem. Konieczna może być zmiana organizacji transportu, współpraca z wieloma dostawcami, pozyskiwanie nowych materiałów z lokalizacji, których ograniczenia nie dotyczą, czy ścisłe monitorowanie poziomu zapasów.

– Spadek popytu, opóźnienia projektów

Projekty i wdrożenia systemów zabezpieczeń są opóźniane lub odkładane, m.in. w związku z zakłóceniami dostaw. Klienci i integratorzy czekają zwłaszcza na dostawy urządzeń do dozoru wizyjnego. Ponieważ skonfigurowanie i opracowanie projektu systemu zajmuje zazwyczaj kilka miesięcy, jest zbyt wcześnie, aby ocenić wpływ pandemii na przyszłość branży zabezpieczeń. Niektórzy eksperci uważają, że spadek popytu na produkty do monitoringu wizyjnego będzie nieunikniony przede wszystkim dlatego, że integratorzy systemów nie będą mogli pracować w obiektach klienta z powodu ograniczeń związanych z pandemią. Oczekuje się jednak, że będzie to stan tymczasowy, popyt wróci do zwykłego poziomu, a nawet wzrośnie, gdy obostrzenia zostaną złagodzone i firmy wznowią ograniczoną obecnie działalność.

– Za wcześnie, aby ocenić efekty długoterminowe

Nieznany i ciągle zmieniający się charakter pandemii COVID-19 utrudnia prognozowanie długoterminowych skutków w branży zabezpieczeń. Główni gracze zgadzają się co do tego, że rynek się zmienia. Eksperci dostrzegają nowe problemy, jakie stwarzają przepisy sanitarne w takich obszarach, jak obiekty handlowe. Samorządy przekierowują swoje standardowe cele i zadania, skupiając się na zapewnieniu bezpieczeństwa publicznego. Kluczowe znaczenie ma obecnie zdolność do szybkiego reagowania na incydenty. Wyzwaniem dla branży jest dostarczanie danych z systemów zabezpieczeń, dzięki którym decydenci będą mogli reagować szybciej, skuteczniej i wydajniej.
Niestety nie wszystkie firmy zajmujące się zabezpieczeniami wyjdą z obecnego kryzysu bez szwanku. Z powodu pandemii wiele nie będzie w stanie utrzymać działalności i zniknie z rynku. Firmy, które nie były w dobrej kondycji finansowej przed wybuchem epidemii, będą musiały zrewidować swoje modele biznesowe i ograniczać koszty, aby zapewnić kontynuację swojej działalności.

– Dokąd zmierzamy

Jedno jest pewne – COVID-19 pokazał, że wszystkie organizacje muszą zmodernizować swoją ogólną działalność i zrewidować plany dotyczące ciągłości działania. Gracze z rynku security uważają, że dzięki podejściu skoncentrowanemu na technologii będzie można wyjść z tego kryzysu w miarę obronną ręką.

Zwiększona aktywność w Internecie

Z powodu pandemii COVID-19 odwołano spotkania stacjonarne. Uaktywniły się targi wirtualne, zaczęto organizować więcej wydarzeń online. Wszystkie główne targi i konferencje poświęcone bezpieczeństwu nie odbyły się w zaplanowanym terminie, dlatego firmy zajmujące się zabezpieczeniami przeniosły targi i szkolenia stacjonarne do wirtualnych targów i webinariów szkoleniowych w Internecie.

– Webinaria

Tradycyjne imprezy, takie jak konferencje czy targi, w czasach pandemii nie mogą się odbywać stacjonarnie. Firmy security wykorzystały tę sytuację i zwiększyły swoją obecność w sieci. Aby jednak seminaria internetowe mogły odnieść sukces, wymagają innej niż tradycyjne prezentacje konfiguracji treści, różnych sposobów promocji i podejścia wielokanałowego. Każde powinno być dostosowane do wymagań określonej grupy odbiorców, czy to instalatorów, projektantów, integratorów systemów, czy partnerów dystrybucyjnych. Ze względu na swoje zalety ta forma przekazu może rozwijać się po zakończeniu pandemii.

– Szkolenia online

Ponieważ instalacje i projekty zabezpieczeń są z konieczności wstrzymane, obserwuje się wzrost liczby zgłoszeń na szkolenia online podnoszące kwalifikacje zawodowe. Instalatorzy i integratorzy po opanowaniu pandemii chcieliby móc zacząć działać. Bardzo wygodną dla nich formą jest dostępność materiałów edukacyjnych online.
Wirtualne prezentacje, seminaria internetowe i inne formy online okazują się rozwiązaniami, które sprawdzają się w tych trudnych czasach, niemniej nie mogą one zastąpić osobistych kontaktów i doświadczenia praktycznego. Mimo to firmy dostosowały się do obecnej sytuacji, a platformy online umożliwiły im szerszą obecność na rynku.

Technologie pomocne w czasach pandemii

Z powodu COVID-19 wzrosło zapotrzebowanie na rozwiązania security pomocne w czasach pandemii. Firmy otrzymują więcej zapytań od kluczowych sektorów, takich jak służba zdrowia. Zauważalny jest też wzrost zainteresowania rozwiązaniami opartymi na sztucznej inteligencji i bezdotykowej kontroli dostępu.

– Pomoc dla służby zdrowia

Na czele walki z koronawirusem stoi branża opieki medycznej. Wiele firm security zauważyło zwiększone zainteresowanie tego sektora sposobami wspomagającymi ochronę pracowników służby zdrowia i pacjentów. Dotyczy to m.in. wzrostu zapotrzebowania na takie technologie, jak zdalne monitorowanie chorych, które mogą pomóc zarówno w ochronie pracowników pierwszej linii, jak i w optymalizacji zasobów w szpitalach.

– Wykorzystanie sztucznej inteligencji i funkcji analitycznych

Firmy security i użytkownicy końcowi zainteresowali się możliwościami wykorzystania analizy wizyjnej i sztucznej inteligencji, aby funkcjonować w czasach kryzysu i dystansowania społecznego. Chociaż algorytmy przeznaczone dla rynku detalicznego opracowano głównie po to, aby pomóc handlowcom w lepszym zrozumieniu zachowania klientów, aplikacje do analizy wizyjnej mogą być wykorzystywane również do innych celów. Kamery wyposażone w narzędzia zliczające osoby dostarczą w czasie rzeczywistym informacji o liczbie osób w obiekcie, zapewniając zgodność z wszelkimi nowymi przepisami dotyczącymi dystansu społecznego.
Z kolei na podstawie danych z systemu kontroli dostępu można błyskawicznie zidentyfikować osoby, które przeszły przez drzwi w bliskiej odległości od osoby uważanej za zakażoną. Operatorzy ochrony mogą je szybko poinformować o możliwości potencjalnego zarażenia i konieczności podjęcia niezbędnych środków ostrożności.

– Bezdotykowa kontrola dostępu

Obawy dotyczące ryzyka rozprzestrzeniania się wirusa podczas korzystania ze skanerów linii papilarnych wymagających fizycznego kontaktu z urządzeniem spowodowały zwiększone zainteresowanie bezdotykowymi czytnikami kontroli dostępu. Wzrosło również zapotrzebowanie na informacje dostarczane z innych systemów, np. monitoringu wizyjnego z funkcją rozpoznawania twarzy (detekcja osób bez maseczki).

Nieznana przyszłość

Pandemia COVID-19 zmusiła branżę zabezpieczeń do ponownej oceny sytuacji na rynku i dostosowania wielu strategii, od łańcucha dostaw po marketing, do nowych możliwości. Nie wiedząc, jak długo potrwa walka z chorobą oraz jakie wywoła konsekwencje, firmy security będą musiały cały czas dostosowywać swoje biznesplany do nowych warunków, by sprostać wyzwaniom związanym z obecnym kryzysem, a także być przygotowanym na poradzenie sobie ze skutkami.

Pandemia COVID-19 zmusiła branżę zabezpieczeń do ponownej oceny sytuacji na rynku i dostosowania wielu strategii, od łańcucha dostaw po marketing, do nowych możliwości.

WPŁYW COVID-19 na rynek kontroli dostępu

W POPRZEDNIM WYDANIU „A&S POLSKA” (4/2020) OPUBLIKOWALIŚMY RAPORT BRYTYJSKIEJ FIRMY BADAWCZEJ OMDIA NT. WPŁYWU PANDEMII COVID-19 NA BRANŻĘ SECURITY. SKUPILIŚMY SIĘ NA RYNKACH DOZORU WIZYJNEGO I SYSTEMÓW SYGNALIZACJI WŁAMANIA I NAPADU. W TYM ODCINKU PREZENTUJEMY PROGNOZY EKSPERTÓW DOTYCZĄCE RYNKU SYSTEMÓW KONTROLI DOSTĘPU.

Sytuacja na rynku kontroli dostępu związana z pandemią

OGÓLNY SPADEK POPYTU	– Zamrażanie wydatków inwestycyjnych i opóźnianie dużych projektów komercyjnych – Poważne straty na rynku ropy i gazu mające wpływ na większość sektorów gospodarki – Mniejsze zapotrzebowanie na czytniki smart oraz karty zbliżeniowe
ZWIĘKSZONE ZAPOTRZEBOWANIE W NIEKTÓRYCH SEGMENTACH	– Służba zdrowia – rozbudowa placówek medycznych – Rynek transportu, małe firmy – możliwości modernizacji istniejących systemów – Budownictwo – wzrost zainteresowania inteligentnymi zamkami
PRZYSPIESZENIE ROZWOJU TECHNOLOGICZNEGO	– Biometria – urządzenia bezdotykowe, proste i higieniczne w użytkowaniu – Urządzenia mobilne – nowe możliwości zarobku na uwierzytelnianiu mobilnym – Oprogramowanie na potrzeby kontroli dostępu – zwiększone możliwości

Według analityków firmy Omdia pandemia koronawirusa doprowadzi w 2020 r. do skurczenia się rynku kontroli dostępu. Pozostanie możliwość modernizacji systemów, ponieważ wielu właścicieli obiektów komercyjnych i instytucjonalnych skorzysta z okazji i unowocześni przestarzałe systemy, gdy w obiektach nie ma pracowników. Jednak nie wszystkich właścicieli będzie stać na inwestowanie w modernizację w czasie recesji gospodarczej, a stagnacja na rynku budowlanym ograniczy możliwości wzrostu. Najbardziej dotkniętym rynkiem będzie sektor przemysłowy z powodu drastycznych ograniczeń projektów w branży energetycznej. Jeśli jesienią większość krajów rozwiniętych ponownie otworzy swoje gospodarki, a pod koniec roku nie będzie znaczącej drugiej fali zachorowań na COVID-19, w 2021 r. rynek powinien się znacznie ożywić.

Choć epidemia koronawirusa rozpoczęła się w Chinach, eksperci Omdia uważają, że w regionie Azji i Pacyfiku skutki pandemii będą miały najmniejszy wpływ na wyniki sprzedażowe w 2020 r. Wydaje się, że pierwsza fala COVID-19, która przeszła przez Chiny i Koreę Południową, zmobilizowała te kraje do walki ze skutkami gospodarczymi wywołanymi przez pandemię. Również kilka wschodzących gospodarek w Azji Południowo-Wschodniej odniosło sukces, ograniczając zakłócenia w produkcji i dostawach. Z kolei Indie, które w ostatnich latach były najszybciej rozwijającym się rynkiem sprzedaży systemów kontroli dostępu, będą w 2020 r. jedynym krajem w regionie, na który koronawirus może mieć znaczący wpływ. Sprzedaż czytników biometrycznych w regionie Azji i Pacyfiku będzie większa niż sprzedaż czytników smart i kart zbliżeniowych. Jeśli Stany Zjednoczone doświadczą przedłużających się przestojów, szczególnie zagrożony będzie rynek czytników kart zbliżeniowych, ponieważ to USA mają duży wpływ na modernizację istniejących systemów opartych na kartach proxy.

Popyt na systemy kontroli dostępu w sektorze opieki zdrowotnej w latach 2020–2021 powinien się utrzymać na stałym poziomie, ponieważ kraje dotknięte epidemią COVID-19, musząc sprostać wzmożonej zachorowalności, będą traktowały priorytetowo budowę nowych szpitali i rozbudowę istniejących placówek. Ponieważ COVID-19 jest wysoko zakaźny, kluczowe znaczenie ma ograniczenie możliwości zarówno przypadkowego, jak i celowego wejścia osób nieupoważnionych do obszarów, w których leczeni są chorzy. Placówki opieki zdrowotnej zapewne rozważą również

Pandemia koronawirusa doprowadzi w 2020 r. do skurczenia się rynku kontroli dostępu. Szansą dla firm security będą jednak przeprowadzane modernizacje systemów

uaktualnienie wykorzystywanego oprogramowania do weryfikacji tożsamości do nowych wersji, oferujących większe możliwości analityczne. Większość szpitali nie może sobie pozwolić na wyłączenie istniejących systemów KD na czas modernizacji, dlatego kluczowym parametrem będzie łatwość przeniesienia danych uwierzytelniających do nowego rozwiązania. Inwestorzy będą raczej preferować oprogramowanie oferujące bardziej elastyczne, fragmentaryczne procesy aktualizacji.

Ze względu na ograniczenia spowodowane przez COVID-19 w obiektach komercyjnych obserwuje się teraz znacznie mniejszy ruch osób. W wielu przypadkach wdrożono pracę zdalną. Ci właściciele obiektów, którzy mają możliwości finansowe, aby zmodernizować swoje systemy, mogą ten czas wykorzystać, gdyż renowacja spowoduje minimalne zakłócenia. Jest to okres szczególnie dogodny na modernizację obiektów transportu publicznego, np. lotnisk, gdyż ruch lotniczy w ciągu ostatnich kilku miesięcy spadł o ponad 60%. Wiele portów lotniczych pozbawionych pasażerów może teraz inwestować w znaczące ulepszenia infrastruktury bezpieczeństwa, bez ograniczania swojej zdolności operacyjnej.

Na stosunkowo wysokim poziomie powinna się utrzymać sprzedaż zamków elektronicznych w sektorze małych i średnich przedsiębiorstw oraz w budownictwie. Właściciele małych firm mogą rozważać zainwestowanie w zamki elektroniczne i podstawowe systemy kontroli dostępu, by chronić swoje obiekty podczas nieobecności pracowników, natomiast popyt na inteligentne zamki mieszkaniowe w tym roku raczej niewiele się zmieni. Osoby pracujące poza domem nadal będą chciały, by ich mieszkania były chronione podczas ich nieobecności, a ci wykonujący pracę zdalnie zapewne zainwestują w zabezpieczenia, gdy sytuacja się ustabilizuje, po powrocie do pracy.

Pandemia koronawirusa może przyczynić się do dalszego przyspieszenia tempa wzrostu sprzedaży czytników biometrycznych bezkontaktowych. Dostępne bezdotykowe czytniki biometryczne potrafią zeskanować i przetworzyć dane biometryczne bez konieczności zatrzymania się użytkownika przy czytniku i zainicjowania fizycznego kontaktu z urządzeniem. Najpopularniejsze są czytniki rozpoznające twarz i tęczówkę oka, chociaż w ostatnich pięciu latach rynek poszerzył się o czytniki linii papilarnych skanujące i rejestrujące dokładne obrazy 3D dłoni, gdy użytkownik poruszy ręką nad głowicą urządzenia. Najszybsze czytniki bezdotykowe mogą w ciągu jednej minuty przechwycić dane biometryczne ponad 45 potencjalnych użytkowników. Szybkość skanowania, łatwość i higiena użytkowania sprawiają, że w często uczęszczanych budynkach zastąpią one tradycyjne czytniki identyfikatorów fizycznych.

Koszt biometrycznych urządzeń bezkontaktowej kontroli dostępu zniechęcał wcześniej do ich stosowania, ale w następstwie pandemii większa liczba użytkowników końcowych może przekonać się do zainwestowania w rozwiązania, które nie wymagają fizycznego dotykania urządzeń, dzięki czemu wirusy i bakterie nie są przenoszone. Biometryczna bezkontaktowa kontrola dostępu do obiektu jest coraz popularniejsza wśród inwestorów korporacyjnych jako higieniczne i bezpieczniejsze rozwiązanie dla wszystkich osób uprawnionych do wejścia do budynku.
W ciągu kilku najbliższych lat z podobnych powodów prawdopodobnie wzrosną też wskaźniki zastosowania uwierzytelnień mobilnych. Dzięki wykorzystaniu mobilnej metody identyfikacji użytkownik uniknie dotykania karty identyfikacyjnej, pobierając aplikację na swój smartfon. Będzie to szczególnie korzystne dla właścicieli obiektów odwiedzanych przez dużą liczbę gości i wykonawców tymczasowych. Zarządcy próbowali oszczędzać na kosztach przez ponowne wydawanie tych samych fizycznych identyfikatorów kolejnym osobom, ale pandemia uświadomiła wszystkim, że ta praktyka może być postrzegana jako mało higieniczna. Zakładając, że szybkość pobierania danych identyfikacyjnych na urządzenia mobilne wzrośnie w najbliższych kilku latach, dostawcy mogą wykorzystać nowe możliwości zarobku, oferując mobilne uwierzytelnienia jako odrębną ofertę produktową.

Jeszcze przed pandemią COVID-19 oprogramowanie do systemów KD było uznawane za jeden z najszybciej rozwijających się i najbardziej konkurencyjnych produktów w tym segmencie. Koronawirus umocnił ten trend, ponieważ większość projektów modernizacyjnych będzie napędzana ulepszeniami platform oprogramowania, a nie instalacją nowych urządzeń. Postęp w zakresie oprogramowania w ostatniej dekadzie mógł radykalnie poprawić możliwości integracyjne i operacyjne systemów KD, ale inwestorzy niechętnie inwestowali w drastyczne zmiany w działających systemach. Użytkownicy końcowi wyrażali zainteresowanie zaawansowanym oprogramowaniem na potrzeby kontroli dostępu wspomaganej uczeniem maszynowym, a także możliwościami integracji z innymi systemami, ale większość wahała się przed zainwestowaniem we wdrożenie

W ciągu najbliższych kilku lat znaczną przewagę rynkową mogą uzyskać dostawcy systemów kontroli dostępu, którzy zainwestują w ulepszanie i udoskonalanie oprogramowania

tych funkcji. Natywne możliwości integracji z oprogramowaniem do zarządzania wideo (VMS) zyskały na popularności, ale szersze możliwości integracji z innymi systemami zabezpieczeń i automatyki budynkowej pozostają w tyle.

Pandemia koronawirusa stanowi spore wyzwanie dla użytkowników końcowych, którzy chcieliby zaktualizować system kontroli dostępu. Właściciele obiektów, w których mogą już być świadczone podstawowe usługi, będą prosić swoich pracowników o zgłaszanie się do pracy, ale każda dodatkowa osoba, np. instalator lub integrator systemów obecny w obiekcie, będzie stanowić dodatkowe potencjalne zagrożenie zakażenia się wirusem. Wielu mniejszych przedsiębiorców będzie starało się maksymalnie oszczędzać w obliczu bezprecedensowego spowolnienia gospodarczego. A nowy system wymaga znacznych nakładów zarówno w urządzenia, jak i towarzyszące instalacje oraz późniejsze konserwacje. Platformy oprogramowania można natomiast łatwo zdalnie aktualizować w celu udostępnienia nowych funkcji, m.in. wprowadzenia zdalnego dostępu, ulepszeń interfejsu użytkownika, konfigurowalnych pulpitów nawigacyjnych czy zaawansowanych funkcji automatycznego testowania i agregacji danych dla menedżerów ds. bezpieczeństwa. Systemy KD, zawsze narażone na cyberataki, będą wymagały inwestycji w ulepszone środki cyberbezpieczeństwa.
W ciągu najbliższych kilku lat dostawcy systemów kontroli dostępu, którzy priorytetowo potraktują ulepszanie i udoskonalanie oferty oprogramowania, mogą uzyskać znaczną przewagę rynkową nad konkurentami, którzy koncentrują się na sprzęcie.

Opracowano na podstawie raportu firmy Omdia ***Connecting the Dots: The impact of Covid-19 on physical security markets*** **(maj 2020 r.)**

INTEGRACJA: konieczność, okazja, fanaberia czy kłopoty?

TEKST
Michał Zalewski

Słowo „integracja" jest ostatnio tak samo modne, jak określenia: inteligentny budynek, Internet Rzeczy. Temat jest obszerny, sedno integracji i sposoby jej wdrażania można opisywać bez końca. Postaram się omówić pokrótce podstawową moim zdaniem fazę procesu integracji, a mianowicie projektowanie.

Należałoby zacząć od odpowiedzi na pytanie, co to w zasadzie jest owa integracja. Przeszukując zakamarki Internetu, nie znalazłem takowej, w mojej świadomości inżyniera też żadna jednoznaczna definicja się nie utrwaliła. Czy można więc omawiać coś, co jest niezdefiniowane? O tym, że normy i np. warunki techniczne w ogóle tego pojęcia nie określają, już nawet nie wspomnę. Skoro zdecydowałem się temat poruszyć, czuję się też zobowiązany do zaproponowania swojej definicji. Oto owoc moich przemyśleń:

Integracja dwóch niezależnych systemów to takie ich połączenie, dzięki któremu osiągamy dodatkowe funkcjonalności niedostępne dla systemów niezintegrowanych.

Słowo „dodatkowe" jest moim zdaniem kluczowe w tej definicji. Jeżeli dzięki integracji nie osiągamy dodatkowych funkcjonalności, należy zastanowić się nad używaniem tego słowa w dokumentacji projektowej. Być może wtedy okaże się, że mamy do czynienia z fanaberią. Sformułowanie: „integracja pojawia się w dokumentacji" nie jest przejęzyczeniem. Jakże często jedynym miejscem, w którym definiuje się w dokumentacji zakres i poziom integracji, jest właśnie taki zapis: system X należy zintegrować z systemem Y i na tym koniec! I radź sobie, wykonawco. Dlaczego tak się dzieje? Według mnie z dwóch powodów. Jednego bardzo smutnego: osoba, która to napisała, nie ma pojęcia, o czym mówi. Uważa, że wystarczy magiczny zapis i wszystko samo się jakoś wymyśli. Drugi powód, trochę mniej smutny, to brak czasu lub nie do końca sprecyzowane oczekiwania przyszłego użytkownika.

Projektant, który podejmuje się zaprojektowania integracji systemów, niezależnie od fazy projektu, musi przede wszystkim wykazać się ogromną wiedzą na temat systemów, które zamierza zintegrować, a także umiejętnością wsparcia dla przyszłego użytkownika w specyfikacji oczekiwań. Zadanie to idealnie wpisuje się w podejście znane ze zręcznych technik zarządzania projektami IT: to programista określa użytkownikowi funkcjonalność, jaką on otrzyma. Gdy to po raz pierwszy usłyszałem, byłem zaskoczony, ale teraz uważam, że jest w nim sporo sensu.

Gigantyczny rozwój technologii informatycznych powoduje, że nawet najlepiej technicznie przygotowany użytkownik nie jest w stanie optymalnie określić swoich oczekiwać. Rola projektanta z tego zakresu jest zatem ogromna, pomaga precyzyjna znajomość budynku, świadomość potrzeb operacyjnych użytkownika, a przede wszystkim znajomość systemów, od których jesteśmy zależni lub na które chcemy wpływać dzięki integracji.

Niby proste, tylko jak to zrobić? Jest kilka kroków koniecznych do wykonania, które zaprowadzą nas do celu. Zacznijmy od tego, że projektant musi uświadomić sobie, że tematem trzeba się dokładnie, dogłębnie zająć, nie wolno poprzestać na jednym zdaniu-sloganie w części opisowej, które przytoczyłem wyżej. Kto ograniczy się do takich zapisów albo – co gorsze, ale też spotykane – narysuje kreskę łączącą na schemacie blokowym dwa niezależne systemy i uważa, że to oznacza ich integrację, musi zdawać sobie sprawę, że pakuje projekt w poważne kłopoty. I każdy, kto zaakceptuje takie zapisy (inwestor, główny projektant, nadzór), podobnie wprowadza projekt na drogę do problemów. Zakwestionowanie wykonania umowy przez wykonawcę jest najmniejszą z możliwych konsekwencji.

> Projektant, który podejmuje się zaprojektowania integracji, musi przede wszystkim wykazać się ogromną wiedzą na temat systemów, które zamierza zintegrować, a także umiejętnością wsparcia dla użytkownika w specyfikacji oczekiwań

Opisałem w poprzednim artykule przykład o integracji wind z systemem kontroli dostępu. Zapraszam przy okazji do lektury, przypomnę jedną uwagę w nim zamieszczoną: nieodpowiedni dobór producentów systemów, które będziemy integrowali, może nawet uniemożliwić osiągnięcie celów integracji. To jest fakt, który dobitnie dowodzi, że tematem integracji należy zająć się dogłębnie już w fazie wstępnego doboru urządzeń i systemów. Jeżeli projektant będzie rzeczywiście przekonany o wadze tematu, nie zadowoli się lakoniczną informacją w opisie, to oznacza, że zaczęliśmy zbliżać się do sukcesu. Z tej wewnętrznej motywacji projektanta powinna wyłonić się konieczność zadawania pytań, by uzyskać od zamawiającego i jego służb technicznych jak najwięcej informacji operacyjnych i funkcjonalnych. Pomaga również zapoznanie się z innymi obiektami zamawiającego, rozmowa ze służbami technicznymi, ustalenie, co działa dobrze, a z czym mają problemy. Ta faza, odpowiednio wcześnie rozpoczęta, na pewno spotka się z wielkim oporem: *Już teraz mam zastawiać się, jak będą działały służby ochrony? Nawet nie zaczęliśmy wykopów pod fundamenty, a pytacie mnie o integrację systemów? Napiszcie w koncepcji, że mają być zintegrowane, potem się wymyśli.*

Takie słowa usłyszymy na 99 proc. Ale musimy zadawać pytania po to, by przypominać, że temat jest ważny. Gdy po raz pierwszy będziemy o to pytali, osoba w przyszłości odpowiedzialna za eksploatację budynku w projekcie nawet nie istnieje. I teraz musi „wejść do gry" doświadczony inżynier, który opracuje zręby rozwiązań, będzie potrafił określić elementy konieczne do ustalenia już na początku i takie, które można dookreślić później. Ważne, by opracować listę parametrów integracji. Z pewnością będzie się ona zmieniała w trakcie dopracowywania kolejnych elementów, ale finalnie będzie idealną check-listą do weryfikacji wykonania zadania. A że warto o to zadbać, postaram się uzasadnić kilkoma przykładami.

Integracja lokalnych sterowników urządzeń klimatyzacji w pomieszczeniach z nadrzędnym systemem BMS

Można zaprojektować pełną integrację opartą na protokołach komunikacyjnych – rozwiązanie maksymalnie bogate, ale po pierwsze kosztowne, bo narzucające konieczność wyposażenia wszystkich sterowników w karty komunikacyjne, po drugie uruchomieniowo wymagające odpowiednio skoordynowanego programowania po stronie zarówno urządzeń, jak i systemu nadrzędnego. A finalnie może się okazać, że użytkownikowi zależało tylko na prostej funkcjonalności ON/OFF, takiej zgody na pracę urządzeń, jak funkcja automatycznego wyłączenia zapomnianych urządzeń po godzinach pracy. Natomiast monitorowania parametrów w systemie nadrzędnym nie planował. Trzeba ustalić to na początku, zamiast z góry zakładać pełną funkcjonalność...

W funkcjonalności systemów zabezpieczeń częstym pomysłem i hasłem w projekcie jest integracja systemów CCTV z innymi systemami, np. KD lub SSWiN. Dobry pomysł, ale sloganowo potraktowany może wpędzić w kłopoty. Przykład: system CCTV zostanie zintegrowany z systemami KD i SSWIN w celu uruchomienia nagrywania z większą rozdzielczością zdarzeń

alarmowych na obrazie z określonej kamery. To funkcjonalność zbędna w przypadku systemu CCTV z porządną analityką obrazu i detekcją ruchu, dodatkowo z programowaną długością pamięci wstecznej kamery, wręcz nie do osiągnięcia poprzez integrację, natomiast niezbędna dla kamer obrotowych ze zmiennym zoomem. Ta sama funkcjonalność, inny system CCTV i albo fanaberia, albo konieczność i efektywne podniesienie funkcjonalności, idealnie wpisujące się w zaproponowaną definicję integracji.

I inny przykład: **integracja systemów SSP w różnych budynkach w obiektach rozproszonych.** Użytkownik zakłada centralne pomieszczenie ochrony i operowanie z tego pomieszczenia funkcjami Potwierdzenie oraz Kasowanie. Takie rozwiązanie może się okazać wręcz niezgodne z zasadami sztuki. Nie wolno umożliwić służbom technicznym kasowania alarmu z poziomu innego budynku. Jeżeli funkcjonalność zostanie zaimplementowana bez dokładnego uzgodnienia z rzeczoznawcą ppoż., możemy narazić się na zarzut błędu technicznego.

Prawidłowe określenie wszystkich potrzeb na początku projektu oszczędzi mnóstwo czasu. Inżynier odpowiedzialny za integrację doskonale wie, o czym piszę, ale rzadko dostrzega potrzebę omówienia tego z użytkownikiem, przedstawienia mu „plusów i minusów". A jeżeli dostrzega, to trudno mu się z tym przebić na wczesnym etapie inwestycji. Z braku komunikacji wynikają kłopoty techniczne. Z kolei zaimplementowanie maksymalnej funkcjonalności, niepotrzebnie dublującej różne funkcje systemu, trudno nazwać optymalnym projektowaniem. W większości umów na prace projektowe taki obowiązek jest zapisany, więc projektant może narazić się na zarzut nierzetelnego projektowania. I nie są to słowa bezpodstawne.
Gdy już przebrniemy przez fazę uzgodnień funkcjonalnych, „wyciągniemy" od użytkownika informacje operacyjne, zapiszemy je w formie uzgodnionych parametrów integracji, reszta pójdzie jak z płatka. Wystarczy podzielić te uzgodnienia na poszczególne systemy, rozesłać je do odpowiednich branżystów z prośbą o potwierdzenie, że zaproponowane przez nich urządzenia czy systemy będą zaprojektowane w sposób pozwalający na uzyskanie odpowiedniej funkcjonalności. To faza równie trudna jak poprzednia i równie potrzebna. Najczęściej odpowiedzią na prośbę o uzgodnienia jest: *odszukaj w kartach katalogowych urządzeń.* Projektant integracji nie może zaakceptować takiej odpowiedzi. Trzeba wymagać koordynacji, co nie oznacza, że np. projektant wentylacji może nie analizować założeń integracji i funkcjonalności z tego wynikających.
Należy dopilnować, by w założeniach integracji nie było np. płynnej regulacji wentylacji 0...100% dla urządzeń z lokalną automatyką urządzeń pracujących ON/OFF lub co najwyżej ze skokową regulacją, co się zdarza. I odwrotnie – sterowanie ON/OFF oświetleniem w systemie nadrzędnym, a po stronie elektrycznej system Dali i oprawy typu dim. To prosta ścieżka do zarzutów o nierzetelność projektu.
Kolejny krok po uzgodnieniu funkcjonalności – należy dokładnie zaprojektować interfejs do połączenia poszczególnych systemów, prawidłowo określić protokoły komunikacyjne lub liczba sygnałów dla interfejsów twardodrutowych. Faza ta jest bardzo trudna, wymaga ciągłej komunikacji pomiędzy projektantami poszczególnych systemów, informowania o ewentualnych zmianach urządzeń, a także, na co czasem nie można liczyć, o wszelkich zmianach oprogramowania w przypadku integracji programowej urządzeń. Jednak dopiero po tych uzgodnieniach można założyć, że faza projektowania dobiegła końca. Teraz już tylko najprostsze, czyli wybudowanie i uruchomienie.
To oczywiście mała prowokacja. Wiadomo że uruchomienie jest jeszcze trudniejsze niż projektowanie, ale bez prawidłowego projektu uruchomienie może okazać się niewykonalne! Ale to temat na inną dyskusję. Nie da się jednak zacząć uruchomień, jeżeli projektant zapomni o jeszcze jednym elemencie: odpowiednio zaplanowanym i skoordynowanym systemie okablowania budynku, tym bardziej że według założeń systemy będą integrowane z wykorzystaniem systemu okablowania strukturalnego wspólnego dla wszystkich systemów. To kolejny ważny element do skoordynowanego zaprojektowania.

Podsumowując, integracja może być zarówno koniecznością, jak i fanaberią lub kłopotem. Wszystko zależy od projektanta integracji, od jego doświadczenia, wiedzy, ale również umiejętności komunikacyjnych, które są niezbędne dla zapewnienia wsparcia użytkownika przy doprecyzowaniu wymagań. Wszystko sprowadza się do zamiany zdania: **system X należy zintegrować z systemem Y na skoordynowany projekt integracji systemów.** Marzy mi się, by ten artykuł rozpoczął wielobranżową dyskusję na temat integracji...

mgr. inż. Michał Zalewski

Absolwent Politechniki Gdańskiej i studiów podyplomowych Zarządzania Projektami Politechniki Warszawskiej. W branży od 24 lat, od 12 lat niezależny konsultant, inżynier uruchomieniowy

POWOLI, ALE NIEUCHRONNIE DRONY STAJĄ SIĘ CZĘŚCIĄ NASZEGO ŻYCIA. NIKT NIE ZWRACA JUŻ UWAGI NA KAMERY OBSERWUJĄCE NAS NIEMAL OD MOMENTU WYJŚCIA Z DOMU. WRĘCZ PRZECIWNIE, W MIEJSCACH MONITOROWANYCH CZUJEMY SIĘ BEZPIECZNIEJSI. PODOBNIE JEST Z DRONAMI, DOSTĘPNYMI DLA KAŻDEGO, CHOCIAŻ NIE ZAWSZE I NIE WSZĘDZIE MOŻNA ICH UŻYWAĆ. CO JEDNAK ISTOTNIEJSZE, MOŻLIWOŚCI DRONÓW SĄ CORAZ SZERSZE, A ZASTOSOWANIE W ZASADZIE NIEOGRANICZONE.

Drony w systemach security

Dominik Grządzielewski

Securitas Polska

Drony powszechnie wykorzystuje wojsko, sektor eventowo-rozrywkowy przy produkcjach filmowych, korzystają z nich geodeci do pomiarów terenu i tworzenia map. Drony to jednak nie tylko wygodny sprzęt do robienia zdjęć i filmów. Wyposażone w kamery termowizyjne mogą mierzyć poziom wilgotności gruntu i na tej podstawie podejmowane są decyzje o nawadnianiu upraw. Drony wyposażone w sensory mierzące poziom cząsteczek stałych PM 1/PM 2,5 oraz PM 10 monitorują stan zanieczyszczenia powietrza, a ratownicy wykorzystują drony do poszukiwań osób na wodzie i szybkiego dostarczania samonapełniających się powietrzem kamizelek ratunkowych.

A jak wygląda sytuacja w branży security? Securitas od dłuższego czasu monitoruje rozwój rynku bezzałogowych statków powietrznych (BSP) i zmiany w regulacjach prawnych. Potencjał wykorzystania dronów jest duży, choć regulacje prawne bardzo go ograniczają. Obecnie koncentrujemy się głównie na wprowadzeniu dronów do systemów bezpieczeństwa w dużych obiektach przemysłowych, logistycznych i miejscach, gdzie ochrona peryferyjna jest kluczowa.

Traktujemy je jako narzędzia wspomagające pracowników ochrony. Wyposażenie dronów w kamery wizyjne oraz termowizyjne daje dużo szersze możliwości niż ich stacjonarne wykorzystanie. Również klienci zauważają potencjał w mobilnym zastosowaniu kamer i chcą wprowadzić drony do ochrony swoich obiektów.

Wykorzystanie dronów w ochronie

• Patrole z powietrza

Dron z zamontowaną kamerą szybciej i dokładniej monitoruje znacznie większy obszar niż pracownik ochrony podczas obchodu, a nawet podczas patrolu wirtualnego. Kamera termowizyjna wykrywa intruza, który mógłby zostać niezauważony przez pracownika ochrony. W porównaniu z patrolem wirtualnym (zdalne łączenie się z obiektem za pośrednictwem kamer umieszczonych w strategicznych miejscach), dron może skontrolować każde miejsce. Głośnik zamontowany na dronie pozwala na zdalną komunikację i wezwanie intruza do opuszczenia chronionego terenu. Obraz z kamery może zostać przesłany do centralnej stacji monitorowania, gdzie zostanie przeanalizowany, a w przypadku wykrycia incydentu pracownik CMS natychmiast uruchomi odpowiednią procedurę bezpieczeństwa.

• Monitorowanie miejsc trudno dostępnych

Rurociągi i sieci energetyczne znajdują się często w miejscach, gdzie nie ma infrastruktury pozwalającej na monitoring za pomocą stacjonarnych kamer, i tu drony są niezastąpione. Ponadto umożliwiają szybką diagnozę w przypadku awarii, rozszczelnienia rurociągu czy przegrzewania się kabli energetycznych. Takie zdarzenia będą widoczne w obrazie z kamery termowizyjnej. Monitorowanie terenu dronami ma również charakter prewencyjny i jest skuteczniejsze od kamer stacjonarnych.

Innym przykładem jest kontrola składów i wagonów na bocznicach kolejowych. W przypadku wagonów otwartych można też zweryfikować ich wnętrze i stan przewożonego towaru.

• Wczesne wykrywanie zagrożeń

Pożary na składowiskach materiałów łatwopalnych (węgla, biomasy, siarki, materiałów i surowców składowanych na hałdach) są znanym problemem. Ukryte źródło ciepła w wyniku rozkładu biologicznego lub utleniania chemicznego powoduje wzrost temperatury. Jeżeli masa nie może rozproszyć ciepła szybciej, niż jest ono wytwarzane, może wystąpić samozapłon. Drony z kamerami termowizyjnymi, oprócz obserwacji terenu, dokonają bezdotykowo pomiaru temperatury. Takie rozwiązanie wczesnego wykrywania gorących miejsc i pożarów jest wysoko cenione przez sektor zajmujący się gospodarką odpadami.

• Monitorowanie pokrywy śnieżnej na dachach

Na podstawie obrazu z kamery wizyjnej można szybko określić, jak dużo śniegu zalega na dachach, zwłaszcza dużych hal produkcyjno-magazynowych, i odpowiednio wcześnie zlecić ich odśnieżanie.

• Analiza stanu bezpieczeństwa obiektu

Dzięki spojrzeniu na obiekt z szerszej, a w zasadzie z wyższej perspektywy, można też dostrzec zagrożenia niewidoczne z poziomu ziemi. Dodatkowo wykonanie aktualnych zdjęć obiektu może bardzo ułatwić przygotowanie instrukcji ochrony obiektu oraz odpowiednich procedur bezpieczeństwa.

Ograniczenia w stosowaniu

Sposobów na wykorzystanie dronów w branży security jest dużo, niestety sporo jest jeszcze ograniczeń, które hamują wdrożenie wszystkich możliwości. Średni czas lotu drona wynosi obecnie 20-30 minut, co w niektórych przypadkach ogranicza ich zadania. Jest to jednak chwilowe utrudnienie. Jeden z czołowych producentów dronów komercyjnych deklaruje, że jego nowy model może wykonywać loty aż do 55 min. Powstają również projekty dronów z silnikiem spalinowym, a także hybrydy spalinowo-elektryczne, jednak są one jednostkowe i bardzo kosztowne.

W przypadku zastosowań, które nie wymagają przemieszczania się drona, a tylko pozostawania przez długi czas w jednym punkcie na dużej wysokości (np. monitorowanie imprez masowych lub demonstracji), możliwe jest podłączenie do stałego zasilania poprzez specjalny system przewodowy.

Regulacje prawne

Drony, jako bezzałogowe statki powietrzne, podlegają – podobnie jak samoloty – przepisom ruchu lotniczego. Do zastosowań komercyjnych, a niewątpliwie takim jest świadczenie usług ochrony, bezwzględnie wymagane jest od operatora posiadanie świadectwa kwalifikacji. Obecnie w zdecydowanej większości przypadków wymienionych wcześniej zastosowań konieczne są uprawnienia BVLOS (*Beyond Visual Line of Sight*)*, czyli poza zasięgiem wzroku operatora.

Drony poruszają się w przestrzeni powietrznej, która jest trójwymiarowa. Przed przystąpieniem do lotu konieczne jest zweryfikowanie danego obszaru, czy nie znajdują się tam strefy z ograniczeniem lub całkowitym zakazem lotów dronów. Może się zdarzyć, że przed wykonaniem lotu konieczne będzie uzyskanie zgody od zarządcy danej strefy.

Dronów dotyczą również regulacje ochrony danych osobowych i prywatności. Ze względu na wykorzystanie w nich kamer należy dobrze przeanalizować, w jaki sposób i przez kogo będą gromadzone i przetwarzane zarejestrowane materiały.

* Nowe przepisy lotnicze w odniesieniu do BSP zgodne z przepisami UE wchodzą w życie 31.12.2020 r.

Koszty

Podobnie jak w przypadku wielu technologii, ceny dronów spadają, jednak problemem jest liczba dronów i dodatkowych pakietów baterii potrzebnych do wykonywania zadań. Kolejnym kosztem jest operator, który musi przejść odpowiednie szkolenia. Należy też przewidzieć jego zmiennika. Biorąc jednak pod uwagę roboczogodziny zaoszczędzone dzięki zastąpieniu tradycyjnych partoli przez patrole wykonywane za pomocą drona, a także spektrum zadań, jakie można wykonać dodatkowo, inwestycja na pewno się zwróci.

Drony Securitas

W Niemczech Securitas jako jedna z pierwszych firm wprowadził drony do obsługi kontraktu Fire & Security w obiekcie Chemical Park Bitterfeld. To jeden z największych obiektów przemysłu chemicznego w Niemczech: powierzchnia 1200 ha, ponad 360 firm (m.in. AkzoNobel, Bayer, Evonik, Heraeus, Guardian), 11 tys. pracowników. Zastosowany w obiekcie dron jest wyposażony w kamerę wizyjną HD, kamerę termowizyjną, sensory pomiarowe do wykrywania gazów palnych i innych substancji. Wykorzystywany jest m.in. do poszukiwania ludzi (wspomagane technologią termowizyjną), kompleksowej oceny bezpieczeństwa i szybkiej reakcji w przypadku zdarzenia lub zniszczenia. Drony wykonują też standardowo loty kontrolne w zakresie prac konserwacyjnych.

W Polsce jesteśmy obecnie w fazie szkolenia operatorów BSP i wyboru optymalnych rozwiązań, z których będziemy niebawem korzystać. Kolejnym krokiem będą misje testowe w wybranych obiektach. Wszystkie działania w tym kierunku powodowane są głębokim przekonaniem, że za jakiś czas drony w branży security będą codziennym narzędziem pracowników ochrony, zwłaszcza w dużych obiektach przemysłowych i logistycznych. □

Securitas Polska

Postępu 6
02-676 Warszawa
securitas@securitas.pl

Monitoring wizyjny na minuty

COVID-19 SPORO NAMIESZAŁ W BRANŻY OCHRONY. CZĘŚĆ CHRONIONYCH FIRM MUSIAŁA ZAWIESIĆ DZIAŁALNOŚĆ, INNE ZGODZIŁY SIĘ, ABY PRACA ODBYWAŁA SIĘ Z DOMU. W EFEKCIE WIELE BIUR, MAGAZYNÓW, PUNKTÓW USŁUGOWYCH STOI PUSTYCH. WŁAŚCICIELE OBAWIAJĄ SIĘ O POZOSTAWIONE TAM WYPOSAŻENIE ORAZ DOBRA. POJAWIAJĄ SIĘ PYTANIA O TO, JAK ZABEZPIECZYĆ DOROBEK ŻYCIA BEZ NADMIERNYCH KOSZTÓW MIESIĘCZNYCH.

TEKST
Daniel Kamiński

Wzrost kosztów osobowych w ochronie

Jednym ze sposobów jest skorzystanie z ochrony fizycznej. Pracownik ochrony może dopilnować ruchu osobowego oraz kołowego w obiekcie. Sprawdzi się po godzinach pracy obiektu, wykonując okresowe patrole w newralgicznych obszarach. Wezwie pomoc w przypadku naruszenia zabezpieczeń.

Niestety koszty ochrony fizycznej rosną. Wiąże się to ze wzrostem stawki minimalnej wynagrodzeń w Polsce i przekłada na koszty usług. Obostrzenia sanitarno-epidemiologiczne dodatkowo je podnoszą. Niestety znaczna część przedsiębiorców boryka się ze spadkiem przychodów, dlatego poszukuje alternatywnych metod ochrony swoich dóbr. Z jednej strony próbują oni ograniczyć liczbę posterunków ochrony w obiekcie, a zarazem rozbudowują zabezpieczenia techniczne. Z drugiej – likwidują stacjonarną ochronę fizyczną i uruchamiają usługi zdalnego monitoringu wizyjnego z reakcją grup interwencyjnych. Motywacją do zmian modelu ochrony staje się redukcja miesięcznych kosztów.

Technologiczna rewolucja w ochronie

Rozwój technologiczny sprawił, że zabezpieczenia techniczne stały się bardziej przystępne cenowo. Jednak ich popularność nie wzrosła z tego powodu drastycznie. Kłopotem jest brak wykwalifikowanej kadry, która może zaprojektować, a następnie zainstalować i uruchomić techniczne systemy ochrony.

Producenci zauważyli, że – wzorem elektroniki użytkowej – zabezpieczenia techniczne powinny być prostsze w uruchomieniu i obsłudze. W przyszłości zastosowanie rozwiązań typu *plug&play* przyspieszy rozwój rynku zabezpieczeń.

Nowe technologie wykorzystujące mobilność, dostęp do chmury i sztuczną inteligencję promują usługi pozwalające na zdalny dostęp, automatyzację oraz redukcję fałszywych alarmów. Jest to odpowiedź na potrzeby „pokowidowej" rzeczywistości – obsługa techniczna powinna spędzać jak najmniej czasu w obiekcie, aby nie stwarzać zagrożenia rozprzestrzeniania się wirusa. Ten stan rzeczy wpłynął znacząco na wzrost popularności usług zdalnych, np. monitoringu wizyjnego.

Rodzaje usług wideomonitoringu

Monitoring wizyjny ma wiele twarzy. Do wspólnego koszyka wkłada się usługi wymagające od operatora nieustannej obserwacji ekranu monitora, usługi, podczas których operator okresowo łączy się z obiektem, oraz usługi, kiedy łączy się z obiektem wyłącznie w przypadku alarmu. Mają one różne cele i różny koszt. Niestety wielu inwestorów ma mylne wyobrażenie o usługach, za które płacą.

Zdalny dozór wizyjny

Stała obserwacja obrazu z kamer na monitorach jest stosowana w Polsce od lat 90. Duże polskie banki wyprowadzały obserwację obrazów na zewnątrz, aby w przypadku np. napadu mieć możliwość podjęcia reakcji mimo sterroryzowania obsługi placówki. W tamtym czasie były to rozwiązania innowacyjne i bardzo drogie. Stacje monitorowania, które znam, nadzorowały maksymalnie po kilkanaście obiektów. Usługa była droga.

Dziś wiele firm twierdzi, że oferuje taką usługę. Jednak często nie jest ona poprawnie świadczona. Każdy operator ma ograniczenia postrzegania. Oznacza to, że może jednocześnie obserwować ok. 16 obrazów z kamer. Przy krótszych zmianach (2-, 3-godzinnych) jest zdolny obserwować nawet 64 obrazy z kamer. Ale nikt nie da rady obserwować kilkuset kamer jednocześnie. Dlatego koszt zdalnego dozoru wizyjnego jednego obiektu z 16 kamerami może przekraczać 12 tys. zł miesięcznie. Jeśli jest niższy, warto sprawdzić warunki świadczenia usług.

Wideoweryfikacja

W wielu obiektach usługa monitoringu wizyjnego zamawiana jest np. po godzinach pracy chronionego obiektu. Zakres świadczonych usług jest dodatkowo doprecyzowany, operator ma obserwować obraz z kamery tylko w momencie alarmu. Tego typu usługa wymaga integracji z systemem alarmowym lub korzystania z rozwiązań z analizą obrazu. Wtedy naruszenie czujnika ruchu lub przekroczenie linii „wirtualnego płotu" wywołuje alarm, który jest dla operatora sygnałem do podjęcia reakcji.

Systemy weryfikacji wizyjnej też mogą się różnić między sobą. Jeśli w przypadku alarmu operator musi łączyć się z obiektem, to traci sporo cennych sekund (nawet 20-30 s). W tym czasie intruza może już nie być w kadrze. Lepszym rozwiązaniem są systemy, w których to kamera łączy się z operatorem w razie alarmu. Ten drugi przypadek też może wymagać przejrzenia archiwum w celu zidentyfikowania, co wywołało alarm. To również zajmuje niestety czas. Z tego względu część rozwiązań udostępnia możliwość równoległego podglądu obrazu „live" oraz obrazu „pre-alarm" (tuż sprzed alarmu). Dzięki temu operator może błyskawicznie podjąć decyzję na temat rodzaju interwencji.

Obsługa alarmu trwa z reguły 4-5 minut. Weryfikowane są obrazy ze wszystkich kamer w obiekcie. Dzięki temu jeden operator może obsłużyć więcej obiektów. Koszty monitoringu wizyjnego w takim obiekcie wynoszą ok. 2 tys. zł miesięcznie.

Wirtualny wideopatrol

Ostatnim rodzajem usług monitoringu wizyjnego jest okresowe łączenie się z obiektem w celu weryfikacji uzgodnionych punktów kontrolnych. W obiektach handlowych mogą to być informacje o tym, czy przy kasach są zamknięte bramki, a personel nosi firmowe uniformy. W obiektach logistycznych można weryfikować, czy bramy do magazynu są zamknięte lub czy na rampie znajduje się nienadzorowana dostawa. Odstępstwa od standardu są zgłaszane działom bezpieczeństwa, które mogą wykonać kontrolę tych obiektów. Czas połączenia z obiektem wynosi 4 do 5 minut, więc operator może obsługiwać wiele obiektów – jak wiele, zależy od liczby wykonywanych patroli w obiekcie. Przy 2-3 połączeniach na dobę z obiektem koszty monitoringu wyniosą 4 do 5 tys. zł.

Sposoby rozliczeń monitoringu wizyjnego

Przy kosztach 16-18 tys. zł miesięcznie za posterunek ochrony fizycznej monitoring wizyjny w każdej z po-

staci jest korzystniejszy. Niestety powtarzające się „wpadki" firm, które świadczą usługi dozoru wizyjnego, powodują, że przedsiębiorcy zaczynają sobie zadawać pytanie, czy ten zdalny monitoring jest realizowany. Korzystając z ochrony fizycznej, pracownika ochrony widzieli w obiekcie, mieli też ustaloną stawkę godzinową. Usługi monitoringu zaś są rozliczane ryczałtem, ewentualnie opłatę uzależnia się od liczby kamer. Inwestorowi trudno określić, czy nie przepłaca, bo fizyczna obsługa zdarzenia zajmuje kilka minut.

Taka sytuacja może spowodować, że wzorem innych krajów europejskich pojawią się oferty rozliczania monitoringu wizyjnego wg użycia, tzw. *pay as you go*, znane np. z ubezpieczeń. W takich przypadkach jednostką rozliczeniową jest minuta obserwacji operatora centrum monitoringu. Oczywiście, aby wprowadzić takie rozliczanie, niezbędne będzie dostosowanie billingu do usług monitoringu wizyjnego. Jest to obszar do rozwoju naszego rodzimego oprogramowania do obsługi zdarzeń wizyjnych. Wprowadzenie takiego rozliczania może znacznie spopularyzować usługi wizyjne.

Metody popularyzacji rozliczeń minutowych

W okresie przejściowym obecne opłaty ryczałtowe można przekształcić na pakiety minut. W przypadku wirtualnego patrolu wykonywanego raz na dobę jest to 120 minut miesięcznie, a w przypadku dwóch wideopatroli na dobę – 240 minut miesięcznie. Natomiast każdy z nas wie, że oprócz tego kilka razy w miesiącu wywoływane są alarmy. Załóżmy, że w mniejszym obiekcie będzie to 6 alarmów miesięcznie (30 minut obsługi), a w większym 10 alarmów miesięcznie (50 minut obsługi).

Na tej podstawie można przygotować dwa pakiety: pierwszy obejmujący 150 minut obsługi – w jego ramach będą wykonywane wideopatrole raz na dobę oraz obsługa wizyjnej weryfikacji alarmów – oraz drugi obejmujący 290 minut obsługi – w jego ramach będą dwa wizyjne patrole na dobę oraz obsługa wizyjnej weryfikacji alarmów. W ramach pakietu jest oczywiście zawarty koszt gotowości operatorów oraz pokrycie inwestycji w infrastrukturę centrum monitoringu, przy założeniu że jedna minuta to koszt 10 zł, pierwszy pakiet kosztowałby 1500 zł, a drugi 2900 zł. Po przekroczeniu liczby alarmów każdy kolejny alarm mógłby być rozliczany wg założenia, że 1 minuta to 10 zł, co daje 50 zł za każdy kolejny alarm.

Dzięki zastosowaniu nowoczesnej technologii zabezpieczenia techniczne i reakcja operatora to już nie tylko ochrona, ale również ograniczenie strat i usprawnienie procesów

Tego typu cennik mógłby ułatwić możliwość oferowania usług oraz pomóc porównywać zakres i jakość realizowanych usług pomiędzy firmami.

Czy 10 zł za minutę monitoringu wizyjnego to dużo? Zastanówmy się. Przykładowo, do centrum monitoringu dzwoni właściciel salonu samochodowego i prosi o zdalne skontrolowanie sytuacji w obiekcie. Interesują go cztery zewnętrzne kamery. Cała operacja zajmie operatorowi ok. 1 minuty, a przedsiębiorca zaoszczędzi koszty wyjazdu i będzie miał „święty spokój". Wtedy 10 zł nie jest wielkim wydatkiem. Nawet gdyby musiał zadzwonić kilka razy w miesiącu, to wyda kilkadziesiąt złotych.

Kierunki rozwoju monitoringu wizyjnego

Jednym z istotnych kierunków rozwoju monitoringu wizyjnego jest automatyzacja. Wielu osobom pracownik ochrony kojarzy się z obsługą szlabanu (niestety). Powiem więcej, pracownik otwierający szlaban w czasach awizacji przyjazdów to dla wielu klientów anachronizm. Zastosowanie systemu awizacji gości oraz systemu rozpoznawania tablic rejestracyjnych pozwala zautomatyzować otwieranie szlabanów.

Analiza obrazu z możliwością rozpoznawania i nauki zachowań jest kolejnym narzędziem technologicznym pozwalającym na automatyzację wychwytywania sytuacji wymagających zainteresowania operatora. Towar składowany na rampie w trakcie deszczu oznacza potencjalne straty, system powinien kogoś zaalarmować. A wystarczy zaznaczyć obszar, gdzie nie powinno być towaru (funkcja detekcji obecności obiektu w scenie), i powiązać go z rozpoznaniem deszczu w kamerze lub sygnalizacją czujnika wilgotności zamontowanego na rampie.

Na zakończenie

Zabezpieczenia techniczne i reakcja operatora to nie tylko ochrona, ale również ograniczenie strat i usprawnienie procesów, dzięki zastosowaniu technologii umożliwiającej automatyczne alerty i zdalne reakcje. Takie podejście pozwoli zaoszczędzić koszty ochrony, a przy tym związać klienta ze sobą. □

BIO

Daniel Kamiński

Absolwent kierunku Telekomunikacji WAT oraz Kierowania Systemami Teleinformatycznymi AON. Od 1995 r. w branży zabezpieczeń technicznych związany z monitoringiem alarmów. Pierwsze 10 lat w grupie AAT/CMA odpowiadał za utrzymanie ciągłości działania centrum monitorowania oraz wsparcie sprzedażowe, następnie w międzynarodowych firmach G4S i ADT. W ostatnich latach jako doradca wykorzystywał swoje doświadczenie wdrażania nowych produktów i usług w firmach Juwentus oraz EBS. Od ponad 20 lat dzieli się swoją wiedzą na łamach czasopism branżowych.

Bezpieczeństwo przemysłowe zagrożenia kryzysu covidowego

Pandemia to dla biznesu czas zagrożeń. Organizacja jest skupiona na przetrwaniu: zarząd zaabsorbowany rozwiązywaniem skomplikowanych i wcześniej niespotykanych problemów, pracownicy zaniepokojeni o swój los, nasila się presja ze wszystkich stron. To niestety idealny moment na realizację najbardziej ryzykownych projektów amatorów cudzej własności.

Pandemia to niestety idealny moment na realizację najbardziej ryzykownych projektów amatorów cudzej własności

TEKST

Jacek Grzechowiak

Znane powiedzenie: „Na pochyłe drzewo wszystkie kozy skaczą" ma wiele odmian, ale zawsze wyraża przestrogę, że organizacja w tarapatach przyciąga wszelkiej maści złodziei. Trzeba się do tego przygotować.

Zagrożenia zewnętrzne

Powody tego są błahe i powszechnie znane. W skrócie: organizacja skupia się na ważniejszych problemach, pracownicy zaniepokojeni o swoją przyszłość nie przywiązują wagi do bezpieczeństwa, a dotyczy to także pracowników ochrony, i najważniejszy powód to niezawodny instynkt złodzieja. Obecne czasy wyróżniają się zaangażowaniem pracowników ochrony w bezpieczeństwo epidemiologiczne. Skutkuje to mniejszą uwagą w innych obszarach, ponieważ doszły nowe zadania, a wielkość zespołu z reguły pozostała niezmieniona.

Zagrożenia w czasie kryzysu generalnie nie różną się od zagrożeń w normalnych czasach, zwiększa się jedynie ich intensywność i częstotliwość. Odnosząc się do bezpieczeństwa biznesowego, należy wskazać wyjątek (w bezpieczeństwie publicznym jest ich zdecydowanie więcej) – w tym okresie występuje więcej zagrożeń dotyczących dewastacji mienia. Są one pochodną zarówno nastrojów społecznych, jak i sytuacji wewnętrznej. Powinny być przedmiotem szczególnej uwagi zarządzających obiektami, a nade wszystko menedżerów firm ochrony osób i mienia.

Przechodząc do tego, co w trudnych czasach jest najtrudniejsze, pojawia się z dużo większą intensywnością i ma bardziej dotkliwe skutki, czyli do zagrożeń wewnętrznych, trzeba gwoli rzetelności powiedzieć, że nie można ich traktować selektywnie, w oderwaniu od sytuacji ogólnej. Zarządzanie nimi jest w czasach kryzysu utrudnione, nasze działania wewnętrzne mogą bowiem zostać zniweczone przez oddziaływanie środowiska zewnętrznego. Przyjrzyjmy się więc zagrożeniom wewnętrznym.

Zagrożenia wewnętrzne

Utrzymująca się od kilku miesięcy sytuacja kryzysowa związana z epidemią COVID-19 powoduje, iż wiele firm zostało zmuszonych do ograniczenia kosztów personalnych, co skutkuje zwolnieniami pracowników. Procesowi temu towarzyszy nasilenie różnych negatywnych emocji. Pracownicy firmy, zaabsorbowani kwestiami dotyczącymi utrzymania miejsca pracy i związaną z tym niepewnością, a niekiedy lękiem, zwracają mniejszą uwagę na bezpieczeństwie organizacji. To reakcja naturalna.

Drugą przyczyną jest koncentracja uwagi zespołów ochronnych na sprawach bezpieczeństwa epidemiologicznego, angażowanych w wykonywanie zadań związanych z mierzeniem temperatury, egzekwowaniem wymogu stosowania sprzętu ochrony osobistej, a także zapewnieniem zachowania dystansu przez osoby przebywające w obiektach chronionych. Ochrona, podejmując się tych zadań, weszła w obszar dotychczas sobie nieznany lub znany bardzo słabo, i to tylko nielicznej grupie pracowników.

Większą uwagę poświęcono wdrażaniu tego procesu, co dodatkowo negatywnie wpłynęło na stan realizacji standardowych zadań ochronnych. Sprawy te są oczywiste, jednak powstał klimat wyjątkowo sprzyjający kradzieżom wewnętrznym. W przypadku zwolnień grupowych obserwuje się praktykę społecznego przyzwolenia na dokonywanie takich kradzieży. Podobne praktyki mieliśmy okazję zaobserwować w latach transformacji, a także podczas poprzedniego kryzysu. Trzeba więc brać to ryzyko pod uwagę na wszystkich etapach realizacji tych działań. Ochrona także powinna o tym wiedzieć. Od menedżerów kierujących zespołami ochronnymi wymaga się zdecydowanie proaktywnego podejścia.

Jak można zarządzać tym ryzykiem? Zagrożenia wewnętrzne są ze swej natury specyficznie trudne w zarządzaniu, bo najbardziej „emocjonalne". Pracownik dotychczas zachowujący się normalnie, niezdradzający żadnych negatywnych symptomów, w reakcji na bolesny impuls, jakim jest informacja o zwolnieniu z pracy, podświadomie uruchamia „scenariusz krzywdy" i sam lub pod wpływem bliskich postanawia „zrewanżować się" swojemu pracodawcy. Pracownicy działów personalnych zapewne mogliby przytoczyć setki, jeśli nie tysiące historii pokazujących ten problem.

Warto przy tym pamiętać, że kradzież może dotyczyć także informacji. I to ryzyko jest coraz bardziej prawdopodobne. Niektórzy planujący nowe życie zawodowe są skłonni wynieść know-how, aby uzyskać lepszą pracę lub założyć własną firmę. Ciekawy przykład dotyczy byłego pracownika firmy

Zagrożenia hybrydowe w biznesie, wyraźnie widoczne już obecnie, będą w przyszłości tym obszarem, na którym specjaliści ds. bezpieczeństwa bedą skupiać swoją uwagę

Google[1]. Warto go przeanalizować, mimo że incydent miał miejsce jeszcze przed kryzysem. Kradzież informacji jest najtrudniejsza do ujawnienia, gdyż często dochodzi do niej poza obiektem chronionym (choćby w domu, z poziomu komputera firmowego), a kradzione informacje mogą być z pozoru nieistotne, np. kradzież pendrive'a z plikiem Excel zawierającym formuły służące optymalizacji mieszanek paszowych, jak to miało miejsce kilka lat temu w północno-wschodniej Polsce[2].

Zakres zagrożeń jest szeroki. Ich opanowaniu służy odpowiednie zarządzanie bezpieczeństwem, ale istotne jest także prowadzenie procesu zwolnień. Proces ten, zależnie od jego przebiegu, może wspierać lub utrudniać zapewnienie bezpieczeństwa. W dobrze zarządzanych organizacjach w takich sytuacjach jest wdrażany proces *outplacementu*. Generalnie jest on ukierunkowany na zarządzanie personelem i ryzykiem personalnym, ale ma też bezpośredni pozytywny wpływ na bezpieczeństwo ogólne całej organizacji. Pierwszą korzyścią jest obniżenie poziomu negatywnych emocji wśród pracowników, a to jeden z najważniejszych czynników dla bezpieczeństwa całej organizacji, ponieważ potencjalnie zmniejsza liczbę osób skłonnych do odwetu. Drugim pozytywem jest zmniejszenie podatności pracowników na świadome lub podświadome przyzwolenie na łamanie procedur, dzięki czemu utrzymujemy (lub zmniejszamy, chociaż nieznacznie) zaangażowanie pracowników w sprawy bezpieczeństwa. Wreszcie trzeci element to należyte wykonywanie obowiązków przez pracowników, a więc wpływ na takie elementy, jak niedobory w dostawach komponentów, czyli profilaktykę bezpieczeństwa.

Brak procedur *outplacementu* nie tylko nie daje szansy na wspieranie bezpieczeństwa organizacji procesami HR, ale wręcz generuje czynniki pogarszające jego poziom. Wśród pracowników pojawia się niepewność powodująca ich nerwowość, co wpływa negatywnie na personalny czynnik bezpieczeństwa, a także inne jego aspekty. Zaczyna się od łamania procedur, np. udostępniania kart systemu KD, nierzetelnego wykonywania kontroli przyjmowanych dostaw czy traktowania incydentów w bezpieczeństwie jako dopuszczalne. Dochodzi do typowego „odwracania się plecami", czasem nawet dosłownie, a to oznacza, że system bezpieczeństwa właśnie przestał działać. Wreszcie pojawiają się drobne kradzieże, z czasem coraz większe, a także realne ryzyko sabotażu.

W procesach personalnych istotna jest także rola menedżera bezpieczeństwa. Jego zaangażowanie na możliwie najwcześniejszym etapie pozwoli mu zorientować się w topologii nowego (odnowionego) ryzyka, a tym samym umożliwi stawianie zespołowi ochronnemu zadań adekwatnych do zaistniałej sytuacji. I wcale nie musi nikomu ujawniać szczegółów związanych ze sprawami personalnymi. Doświadczony menedżer bezpieczeństwa poradzi sobie z tym bez problemu, nie ujawniając wrażliwych informacji. Współpraca menedżera bezpieczeństwa z menedżerem personalnym powinna mieć miejsce cały czas, ale okres zwolnień grupowych to czas szczególny na jej zacieśnienie. Wtedy mogą się pojawić wątpliwe decyzje menedżerskie, np. wstrzymanie wewnętrznych postępowań wyjaśniających związanych z ujawnionymi incydentami. Źródłem rekomendacji w tym zakresie są z reguły działy personalne. Działają one w dobrej wierze, bo czas zwolnień grupowych wpływa na kumulowanie się negatywnych emocji, a im ich mniej, tym lepiej także dla bezpieczeństwa organizacji. Natomiast wewnętrzne postępowanie wyjaśniające niestety takie negatywne emocje pobudza. Odwołując się do analogii medycznych – jeśli ktoś jest chory na dwie choroby, trzeba leczyć obie. Zaprzestanie leczenia jednej choroby być może ułatwia pracę innemu lekarzowi, ale druga nieleczona choroba rozwija się szybciej, bardziej agresywnie, mutując, aż w końcu...

W takim klimacie zarówno wszczynanie wewnętrznych postępowań wyjaśniających, jak i rekomendowanie ich zaniechania to trudne decyzje. Ale celem organizacji jest przecież przetrwanie, a problem niezarządzany staje się jeszcze większy. Odstępowanie w imię świętego spokoju od wewnętrznych postępowań wyjaśniających w trakcie zwolnień przyniesie, wcześniej czy później, poważny problem w innym miejscu organizacji. Z reguły dochodzi do tego właśnie wtedy, gdy firma jest najbardziej osłabiona organizacyjnie po zwolnieniach. Te trudne zadania działu bezpieczeństwa muszą być realizowane w celu wspierania przetrwania organizacji. Jest to dużo trudniejsze niż w czasach spokojnych, ale niezbędne.

Pandemia to dla biznesu także czas najtrudniejszych zagrożeń. Organizacja jest skupiona na przetrwaniu: zarząd zaabsorbowany rozwiązywaniem skomplikowanych i do tego wcześniej niespotykanych problemów, pracownicy zaniepokojeni o swój los, nasila się presja ze wszystkich stron. To niestety idealny moment na realizację najbardziej ryzykownych projektów amatorów cudzej własności, takich jak przypadek pracownika firmy Tesla, któremu zaoferowano majątek za ujawnienie tajemnic firmowych[3]. Tu raczej należałoby użyć zwrotu „zawodowców" zamiast „amatorów". I takie zagrożenia się zdarzają, trzeba je mieć na względzie. Warto pamiętać, że tego typu działanie jest poprzedzone czynnościami przygotowawczymi, także w obszarze rozpoznania systemu bezpieczeństwa organizacji, w której pracuje „obiekt" takiego ataku. Nie miejmy co do tego złudzeń – obce służby specjalne także biznes mają na celowniku. Ochrona fizyczna również może mieć w tym udział po jednej bądź drugiej stronie.

Tymczasem wciąż można spotkać miejsca, w których pracownicy ochrony nie chronią obiektów wręcz tak ostentacyjnie, że telewizor znajduje się na poczesnym miejscu w dyżurce ochrony[4]. Nie ma wątpliwości, że oglądanie meczu jest dużo ciekawsze niż prowadzenie obserwacji obiektu za pomocą kamer CCTV, ale nie ma także wątpliwości, że mecz skutecznie zneutralizuje cały wysiłek zespołu ochronnego. Takie zdarzenia w trudnych czasach pojawiają się znacznie częściej, m.in. dlatego że firmy ochrony również przeżywają trudności, profesjonalizm personelu spada, szkolenia są rzadziej przeprowadzane, a ich poziom także zaczyna coraz częściej pozostawiać wiele do życzenia. Spotyka się to z brakiem reakcji klienta, który być może zwolnił menedżera bezpieczeństwa, być może jest pochłonięty gaszeniem pożarów. W efekcie obiektów chronią pracownicy o niższych kompetencjach i gorzej wyszkoleni, a dodatkowo bardziej zaangażowanych w zadania z zakresu bezpieczeństwa epidemiologicznego. To prosta i łatwa droga do neutralizacji całego systemu bezpieczeństwa.

Oprócz kwalifikacji personelu niezbędne jest także dobre zarządzanie innymi rodzajami ryzyka, pojawiającymi się w trudnych czasach. Branża ochrony w Polsce charakteryzuje się niesłychanie dużą rotacją pracowników, z czym jest nierozłącznie związany problem niekontrolowanej dostępności mundurów. Odchodzący pracownicy często nie zwracają mundurów. Ryzyko to dotyczy wszystkich firm ochrony, jednak niektóre tym procesem już zarządzają, wiedząc, jaki to problem dla nich samych i ich klientów. Zarządzając ryzykiem przez wiele lat, znam ten problem, był on moim „stałym fragmentem gry". Mundur pozwala osobie go noszącej na przebywanie na terenie obiektu (kto sprawdza, czy pracownik ochrony faktycznie jest tym, za kogo się podaje?), wielokrotnie także w miejscach newralgicznych i nierzadko bez żadnej asysty. W konsekwencji może on być, gdzie chce, i robić, co chce. Dlatego „nieautoryzowany" mundur regularnie pojawia się w różnych incydentach.

W przypadku firm, w których za cały mundur służy sprany T-shirt z napisem „Ochrona", nieautoryzowane jego użycie jest banalnie proste. I niesamowicie groźne. Zarządzanie mundurem to element, który musi wejść jako proces do zarządzania działalnością we wszystkich firmach ochrony. Dziś – z nielicznymi wyjątkami – właściwie nie istnieje i ryzykiem tym niestety musi zarządzić klient. Zapewniam, że warto.

Zagrożenia hybrydowe

W naszej codzienności od lat funkcjonuje pojęcie wojny hybrydowej rozumianej jako strategia wojenna łącząca w tym samym czasie i na tym samym polu walki różne działania (konwencjonalne, nieregularne, cybernetyczne, terroryzm, przestępczość). Czy tego typu oddziaływania są obecne w biznesie? Czy tę strategię można (trzeba) także brać pod uwagę? Oczywiście zagrożenia biznesowe nie są kopią zagrożeń bezpieczeństwa państwa, można jednak dostrzec wiele analogii w taktyce i technice działania przestępców koncentrujących się na biznesie. W tym sensie część mechanizmów obecnych w kreowaniu zagrożeń na poziomie państwowym będzie obecna także w życiu biznesowym. Przemawiają za tym co najmniej trzy argumenty. Wraz z rozwojem gospodarki w biznesie funkcjonuje coraz więcej współzależnych systemów, tym samym dokonanie kradzieży coraz częściej wymaga ingerencji w różne punkty czy procesy w okradanej organizacji. Tak więc „w jednym miejscu i na jednym polu walki" już teraz mamy do czynienia z kompleksem różnych działań:

- konwencjonalnych – złodziej kradnie,
- cybernetycznych – kradzież z włamaniem do systemu IT, np. w celu wygenerowania dokumentu umożliwiającego wywiezienie kradzionego mienia,
- nieregularnych – także tutaj można dopatrzyć się analogii, przestępcy bowiem coraz częściej się specjalizują, a model kompletowania zespołu złodziejskiego do konkretnego zadania czy obiektu znany jest od dawna, jeśli nie od zawsze. Można zaryzykować tezę, iż to przestępcy byli prekursorami działań nieregularnych.

Dlatego zagrożenia hybrydowe, w biznesie wyraźnie widoczne już obecnie, będą w przyszłości tym obszarem, na którym specjaliści ds. bezpieczeństwa skupią uwagę.

Konkluzja nie jest optymistyczna

Trudne czasy to okres, w którym uwaga na sprawy bezpieczeństwa powinna być wyostrzona, w którym zagrożenia wewnętrzne w firmie będą pojawiały się częściej, z większą energią. Działy bezpieczeństwa będą natomiast musiały im sprostać w trudniejszych warunkach, mając na uwadze także zespół ochronny firmy chroniącej obiekt, gdyż wewnątrz niego także tkwią zagrożenia. □

1) Marek Druś, Puls Biznesu, „Były inżynier Google pójdzie do więzienia za kradzież tajemnic handlowych" (https://www.pb.pl/byly-inzynier-google-pojdzie-do-wiezienia-za-kradziez-tajemnic-handlowych-998479) [dostęp: 05.08.2020]
2) https://sip.lex.pl/orzeczenia-i-pisma-urzedowe/orzeczenia-sadow/ii-aka-2-13-wykorzystanie-informacji-jako-znamie-521388419 [dostęp: 18.09.2020]
3) Szymon Palczewski, Defence24, „Tesla celem zaawansowanej operacji Rosjan" (www.cyberdefence24.pl/tesla-celem-zaawansowanej-operacji-rosjan) [dostęp: 28.08.2020]
4) Czy Twoja ochrona Cię chroni?" w: www.riskresponse.pl/blog [dostęp: 18.09.2020]

BIO

Jacek Grzechowiak

Menedżer ryzyka i bezpieczeństwa. W ramach własnej działalności doradza organizacjom biznesowym w zarządzaniu ryzykiem. W przeszłości związany z grupami Securitas, Avon i Celsa, w których zarządzał bezpieczeństwem i ryzykiem. Absolwent WAT, studiów podyplomowych w SGH i Akademii L. Koźmińskiego. Gościnnie wykłada na uczelniach wyższych.

COVID-19 przyspieszy automatyzację i zastosowania robotyki w fabrykach

Sektor produkcyjny doświadcza dziś skrajnych skutków pandemii koronawirusa – wiele zakładów zostało zmuszonych do zwolnień pracowników lub całkowitego zamknięcia, inne, wytwarzające podstawowe produkty, są przeciążone do granic możliwości i nie mogą sprostać rosnącemu popytowi. Kadra kierownicza stanęła przed zadaniem zapewnienia zdrowia i bezpieczeństwa swoim pracownikom, przy jednoczesnym zachowaniu wysokiej produktywności i efektywności.

TEKST
Eifeh Strom
a&s International

Zdrowie i bezpieczeństwo pracowników zawsze ma najwyższy priorytet. Ze względu na wymagania dotyczące zachowania dystansu społecznego w czasie pandemii przepisy musiano jeszcze zaostrzyć. Szansą na zaspokojenie potrzeb kierownictwa i pracowników oraz na powrót na właściwe tory w świecie zaatakowanym przez koronawirusa może być m.in. upowszechnienie automatyzacji, rozwój przemysłowego Internetu Rzeczy (IIoT) i wdrożenie większej liczby robotów.

Robotyzacja zapewnia utrzymanie pracy fabryk w warunkach COVID-19

W przeciwieństwie do pracowników biurowych, którzy mogą pracować zdalnie w systemie *home office*, produkcja nadal wymaga obecności wielu robotników w hali produkcyjnej. Tylko niektóre procesy można zautomatyzować, reszta nadal wymaga obecności człowieka w miejscu pracy. W samym środku pandemii producenci zaczęli więc bardziej interesować się wdrażaniem automatyzacji elastycznej, obejmującej autonomiczne roboty mobilne (AMR) i roboty współpracujące z człowiekiem – znane również jako coboty. Wdrożenie robotów w ramach elastycznego procesu automatyzacji może pomóc w utrzymaniu ciągłości produkcji i wydajności linii produkcyjnych, a jednocześnie pozwoli pracownikom zachować wymaganą fizyczną odległość.

Robotyzacja wspomaga higienę, bezpieczeństwo i wydajność pracy

Zastosowanie robotów pozwoli firmom zautomatyzować szereg procesów, pomoże też w opracowaniu schematu powrotu do pracy i przestrzeganiu wytycznych dotyczących dystansu społecznego. AMR to klasa robotów wyposażonych w czujniki, dzięki którym rozpoznają swoje środowisko operacyjne i mogą poruszać się po obiekcie albo autonomicznie bez interwencji człowieka, albo po ustalonych trasach, jak pojazdy sterowane automatycznie (AGV). Roboty AMR mogą wykonywać rozmaite czynności, m.in. przenosić materiały z punktu odbioru do magazynu, na bocznicę, dostarczać na stanowiska robocze i przetwarzania, realizować pilne dostawy części oraz narzędzi itp.

Roboty współpracujące z człowiekiem na jednym stanowisku pracy (coboty) wspomagają jego pracę z zachowaniem wymaganego bezpiecznego dystansu. W czasach przed pandemią COVID-19 wyręczały pracowników w wykonywaniu nudnych (monotonnych), brudnych, niebezpiecznych czy uciążliwych czynności.

Wdrożenie robotów w ramach elastycznego procesu automatyzacji może pomóc w utrzymaniu ciągłości produkcji i wydajności linii produkcyjnych, a jednocześnie w zachowaniu dystansu społecznego pracowników

Roboty zarządzane w chmurze

Robotyzacja (zastosowania robotyki) niesie wiele korzyści, jednak w przypadku automatyki nieregulowanej (*fixed automation*) – pojazdy AGW i tradycyjne roboty AMR – nie jest ona pozbawiona wad. Po jej wprowadzeniu trudno dokonywać zmian, chcąc dostosować się do nowych warunków pracy lub sprostać takim wyzwaniom, jak konieczność zachowania dystansu społecznego.

Ponadto ten typ automatyzacji przez kilka miesięcy od jej implementacji wymaga obecności osoby nadzorującej. Natomiast zarządzanie w chmurze umożliwia firmie dokonywanie zmian konfiguracji pracy robota, bez konieczności fizycznego przebywania osoby nadzorującej w zakładzie produkcyjnym. Przykładowo inżynier procesu lub inżynier automatyk pracujący w domu mogą z łatwością modyfikować istniejące schematy pracy, aby np. utworzyć nowe lokalizacje odbioru lub dostosować je do zmian w pozycjach stanowisk produkcyjnych.

Oparte na chmurze systemy AMR mogą komunikować się ze sobą, by optymalizować płynność ruchu. Mogą też być integrowane z innymi urządzeniami inteligentnej fabryki za pośrednictwem Internetu Rzeczy (IoT). To jeszcze bardziej zwiększa jej wydajność.

Możliwość zdalnego zarządzania fabryką dzięki transformacji cyfrowej

Zdalne zarządzanie i konserwacja predykcyjna to tylko przykładowe metody zwiększenia wydajności fabryk w następstwie COVID-19. Przemysłowy Internet Rzeczy (IIoT) i cyfryzacja produkcji mogą wspomóc producentów w inteligentnej i wydajnej pracy. Obecnie sektor produkcyjny usiłuje przezwyciężyć przestoje wywołane przez pandemię, więc sprawą najwyższej wagi będzie sposób, w jaki IIoT zapewni wzrost produktywności, a jednocześnie ochronę zdrowia pracowników.

Eksperci przewidują, że tempo transformacji cyfrowej przyspieszy, ponieważ bezpieczeństwo danych oferowane przez Przemysł 4.0 pozwala już na zdalne monitorowanie i zarządzanie.

Zarządzanie zdalne umożliwia operatorom wiele opcji, np. dostosowywanie parametrów systemów, przeprowadzanie konserwacji i podejmowanie decyzji operacyjnych, gdy dostęp do fizycznej instalacji jest niemożliwy lub niezalecany. Aby pomóc w optymalizacji i rozwiązywaniu problemów, eksperci mogą zdalnie łączyć się z pracownikami zakładu i przekazywać polecenia personelowi na miejscu. Ograniczy to również fizyczny kontakt pracownika z powierzchniami urządzeń, umożliwiając bezdotykowe rozwiązywanie problemów i dostęp do zdalnej pomocy na poziomie zakładu.

Inną formą zdalnego zarządzania jest konserwacja predykcyjna urządzeń i robotów. Dzięki zgromadzonym danym operacyjnym szefowie produkcji mogą planować konserwacje, zapobiegać problemom z produkcją i monitorować jej wskaźniki. Podczas pandemii konserwacja predykcyjna zapewnia firmom możliwość zdalnego monitorowania ich systemów i pomaga zmniejszyć liczbę zatrudnionych pracowników. Zdalnie zarządzać można z oddzielnego pomieszczenia w firmie, z domu lub innego dowolnego miejsca.

Cyfryzacja zwiększa możliwości pracowników

Według badania przeprowadzonego przez firmę doradczą Capgemini w 2019 r. blisko 70% producentów realizowało inicjatywy dotyczące inteligentnych fabryk. Głównym celem ich inwestycji był wzrost produktywności, ale digitalizacja wiąże się też z wieloma innymi aspektami. Przy każdej transformacji cyfrowej trzeba mieć jasność, jaki problem biz

nesowy chcemy rozwiązać. Nie należy zapominać o mierzeniu wyników – zarówno w miarę postępu transformacji, jak i po jej zakończeniu. Ważne jest również, aby zrozumieć, że opłacalna strategia cyfryzacji musi uwzględniać jej wpływ nie tylko na organizację, ale także na pracowników. Usprawnienia pracy, umożliwienie wpływania na ulepszenia w sposobie prowadzenia firmy – wszystko to zwiększa zaangażowanie i podnosi ich morale.
Wdrażając transformację cyfrową, należy brać pod uwagę również takie kwestie, jak zapewnienie bezpieczeństwa, optymalizacja procesów oraz zapewnienie niezawodności i bezpiecznego funkcjonowania przedsiębiorstwa w trudnej sytuacji rynkowej.

Długoterminowe skutki COVID-19 na produkcję i fabryki

Zwiększone zainteresowanie automatyzacją i robotyką, zmiany w łańcuchu dostaw i dystans społeczny to tylko niektóre z przewidywanych długoterminowych skutków COVID-19 wpływających na sektor produkcyjny. Nie ma wątpliwości, że po pandemii na całym świecie konieczne będą zmiany w sposobie produkcji. Zakłócenia w łańcuchu dostaw i potrzeba wyższej produktywności w bezpiecznym środowisku będą wymagały od kadry zarządzającej przyjęcia większej liczby strategii automatyzacji i cyfryzacji. Oczekuje się, że pandemia przyczyni się do uzasadnienia większych nakładów na automatyzację.
Gwałtownie rosnące koszty pracy w tradycyjnych modelach *offshoringu* (przeniesienie wybranych procesów przedsiębiorstwa za granicę) zachęciły firmy do korzystania z nowych, bardziej elastycznych opcji automatyki przemysłowej, takich jak coboty. Pozwoli im to na produkcję, montaż i operacje końcowe bliżej rynków, na których mają być sprzedawane ich produkty końcowe. Więcej firm będzie też poszukiwać rozwiązań z zakresu automatyzacji i robotyki, aby zrekompensować brak wykwalifikowanej siły roboczej. Będą więc szkolić swoich pracowników w zakresie programowania i obsługi robotów oraz zarządzania automatyzacją zamiast tradycyjnego ręcznego wykonywania rutynowych czynności.

Ponowna ocena łańcuchów dostaw

Jednymi z pierwszych problemów, jakie pojawiły się w następstwie skutków COVID-19, były zakłócenia w łańcuchu dostaw związane z chwilowym zawieszeniem produkcji przez fabryki w Chinach. Na początku marca br. amerykańskie Krajowe Stowarzyszenie Producentów przeprowadziło ankietę na terenie USA, która ujawniła, że jedna trzecia uczestników doświadcza zakłóceń w łańcuchu dostaw, co skutkuje wydłużeniem czasu produkcji i utratą przychodów. Dlatego fabryki na całym świecie musiały uważnie przyjrzeć się i ponownie ocenić swoje łańcuchy dostaw.
Producenci zdali sobie sprawę, że ich łańcuchy dostaw były zbyt długie, nie zawsze są też możliwości zaopatrzenia strategicznego bliżej ich lokalizacji. Jednym z rozwiązań jest cyfryzacja łańcuchów dostaw. Pandemia koronawirusa może być katalizatorem dla większej liczby firm integrujących swoje systemy automatyzacji fabryk z systemami planowania i realizacji łańcucha dostaw. Eksperci zalecają, by tworzyć inteligentne zarządzanie operacyjne łańcuchem dostaw wspólnie z partnerami. Pozwoli to członkom łańcucha reagować w czasie rzeczywistym na szybko zmieniający się rynek lub potrzeby klientów.

> Zakłócenia w łańcuchu dostaw będą wymagały od kadry zarządzającej przyjęcia większej liczby strategii automatyzacji i cyfryzacji

Praca z zachowaniem dystansu społecznego

Dystans społeczny może stać się częścią naszej nowej rzeczywistości i aby naprawdę skutecznie spowolnić przenoszenie wirusów, będzie musiał obowiązywać również w miejscu pracy. Firmy będą musiały dostosować się do nowych przepisów zachowania odpowiedniej odległości pomiędzy stanowiskami pracy. W niektórych branżach będzie to trudniejsze niż w innych. Dla firm produkcyjnych oznacza to znalezienie nowych sposobów na zaspokojenia popytu, bez zwiększania lub narażania zdrowia obecnych pracowników.
Wprowadzenie większej automatyzacji przyniesie podwójną korzyść w postaci wzrostu produktywności, a jednocześnie zapewni pracownikom większe bezpieczeństwo. Wdrażanie tych technologii będzie jednak zależało od tego, czy można je zintegrować z istniejącym środowiskiem technicznym i procesami biznesowymi przedsiębiorstwa.

Roboty w walce z wirusami

Firmę Security Robot Guard Systems założyło dwóch pasjonatów branży ochrony, z kilkudziesięcioletnim doświadczeniem w swojej dziedzinie. Pomimo niedługiego stażu może się już pochwalić sporymi sukcesami i współpracą ze znaczącymi klientami. Firma sukcesywnie się rozwija i posiada koncesję zarówno na ochronę fizyczną, jak i na zabezpieczenia techniczne – koncesja MSW L-0332/19.

Firma zajmuje się przede wszystkim promocją i wprowadzeniem na rynek polski i europejski urządzeń robotycznych do ochrony fizycznej, tzw. robotów patrolujących. – *Naszą misją jest popularyzacja robotyki w ochronie, wykorzystywanie zdobyczy technologicznych w służbie człowieka i odciążanie go od uciążliwych lub monotonnych zajęć. Wspomagamy pracowników ochrony mobilnymi centrami monitoringu, które będą wykonywać za nich patrol, np. w miejscach o podwyższonym zagrożeniu zdrowia. Wypełniamy robotyką luki związane z niedoborem ludzi na rynku pracy* – mówi Grzegorz Wyszyński, prezes Zarządu SRGS. *Obecnie zmagamy się z pandemią COVID-19. Nasze urządzenia są przystosowane do realizowania zadań związanych z zapobieganiem rozprzestrzeniania się wirusa SARS-CoV-2 w różnego rodzaju obiektach* – dodaje.
Security Robot Guard Systems – razem dbajmy o nasze bezpieczeństwo.

Roboty mają za zadanie ułatwiać pracę firmom ochrony i sprzątającym, znacznie przyspieszają procesy związane z dezynfekcją. Szybkość działania i wydajność to ich dodatkowe atuty. Główną zaletą jest to, że dezynfekcja odbywa się praktycznie w sposób autonomiczny i proces nie wymaga obecności człowieka, co w wielu przypadkach ogranicza ryzyko zarażenia się pracownika.

Robot XT-C

Głównymi funkcjami robota sterylizująco-dezynfekcyjnego XT-C są dezynfekcja powierzchni promieniami UV i dezynfekcja ozonowa. Ma szerokie spektrum sterylizacji – niszczy mikroorganizmy i wirusy (w tym SARS-CoV-2), bakterie, zarodniki i grzyby. Robot, poruszając się po powierzchni, zapewnia dużą prędkość dezynfekcji powietrza, co sprzyja szczególnie zastosowaniom w przestrzeniach zamkniętych typu biuro, klinika, szpital.

SPECYFIKACJA	
Wymiary:	625 x 600 x 800 m
Wysokość nad podłożem:	40 mm
Prędkość pracy:	0-3,6 km/godz.
Czas pracy:	5 godz.
Temperatura pracy:	-20...+60°

Robot XT-A

Robot dezynfekcyjny XT-A został zaprojektowany do dezynfekcji powierzchni przy użyciu sprayu mikrocząsteczek do 10 mikrometrów. Urządzenie autonomicznie planuje trasę, praktyczne pokrycie powierzchni do 25 tys. m². Robot w trakcie pracy dezynfekuje obszar wokół siebie (360°). Wydajność sprayu odkażającego wynosi od 2 do 5 litrów/godz.

XT-A jest dodatkowo wyposażony w lampę UV, która wspomaga sterylizację danego obszaru, oraz w termometr, który mierzy temperaturę ciała osób przebywających w zasięgu jego czujników.

Roboty znakomicie sprawdzą się w miejscach, w których przebywa duża liczba osób, np. w szkołach, szpitalach, hotelach, laboratoriach, zakładach produkcyjnych (zwłaszcza żywności), lotniskach czy biurach.

Security Robot Guard Systems
ul. Modlińska 51/515, 03-199 Warszawa
www.srgs.pl

CIECH jest międzynarodową grupą chemiczną mającą silną pozycję na rynkach europejskich i globalnym, dysponującą wsparciem stabilnego inwestora strategicznego (Kulczyk Investments). Firma eksportuje swoje produkty do ponad 100 krajów na całym świecie, oferując sodę kalcynowaną, sodę oczyszczoną, sól, środki ochrony roślin, żywice epoksydowe i poliestrowe, pianki poliuretanowe oraz krzemiany i opakowania szklane. Spółka posiada osiem zakładów produkcyjnych w trzech krajach: Polsce, Niemczech i Rumunii. Od 2005 r. spółka CIECH notowana jest na Giełdzie Papierów Wartościowych w Warszawie, a od 2016 r. na jednej z największych giełd w Europie – Börse Frankfurt.

Kluczowe jest utrzymanie ciągłości produkcji

O KONCEPCJI BEZPIECZEŃSTWA W GRUPIE ZAKŁADÓW CHEMICZNYCH CIECH ROZMAWIAMY Z TOMASZEM GUZIKOWSKIM, DYREKTOREM ZARZĄDZANIA MAJĄTKIEM I BEZPIECZEŃSTWA.

→ Grupa chemiczna CIECH ma osiem zakładów produkcyjnych zlokalizowanych w trzech krajach – Polsce, Niemczech i Rumunii – i szeroką ofertę produktową. Tworzy dużą grupę kapitałową. Jaka jest filozofia firmy dotycząca podejścia do bezpieczeństwa? Jak została zdefiniowana?

Działalność naszej grupy opiera się na ofercie produktowej dla bardzo szerokiego grona odbiorców. Naszymi głównymi klientami są zarówno globalne koncerny chemiczne z całego świata, jak i mniejsze przedsiębiorstwa głównie z Europy, ale też z Azji, Afryki czy Ameryki Płn. Prowadzimy działalność w ramach siedmiu linii biznesowych: soda, sól, środki ochrony roślin, krzemiany, produkty szklane oraz żywice. Jeśli chodzi o bezpieczeństwo, to oczywiście jest ono kluczowym elementem filozofii i strategii, zarówno krótko-, jak i długoterminowej.

Bezpieczeństwo rozumiem bardzo szeroko: począwszy od bezpieczeństwa pracy, czyli bezpieczeństwa naszych pracowników, poprzez bezpieczeństwo mienia, informacji, procesów produkcyjnych (w tym maszyn i urządzeń), skończywszy na bezpieczeństwie łańcucha dostaw i produktu, ponieważ nasi klienci oczekują, że produkt, który dostaną na czas, będzie najwyższej jakości i w pełni bezpieczny.
W każdym z tych elementów składowych kluczową rolę odgrywają ludzie, zarówno ci na pierwszej linii frontu, jak i menedżerowie o najwyższych kompetencjach, którzy wyznaczają standardy i cele we własnych obszarach. Powołujemy zespoły multidyscyplinarne, by wspólnie, przy uzgodnieniu wszystkich aspektów, stworzyć model zarządzania bezpieczeństwem optymalny z punktu widzenia organizacyjnego i kosztowego.

Koncepcję bezpieczeństwa opracowujemy pod kątem celu, jaki chcemy osiągnąć. W tak dużej grupie kapitałowej, jak CIECH, nie da się wszystkiego zrobić w ciągu roku, dlatego projekty rozkładamy w czasie. Dynamika zmian w otoczeniu też jest różna. Musimy się dostosować do zmian zachodzących na rynku i pojawiających się nowych rozwiązań w branży zabezpieczeń. Kluczowym celem jest zapewnienie ciągłości działania organizacji.

→ A taktyka ochrony w zakładach ulokowanych w Polsce i za granicą też jest podobna?

W naszej grupie kapitałowej są zakłady różniące się nie tylko rodzajem produkcji, charakterem prowadzonej działalności czy wielkością, ale również warunkami środowiskowymi i kulturowymi. Tak jak wspomniałem, cel mamy jeden, różne są natomiast metody dojścia do niego. Tam, gdzie to możliwe, staramy się ujednolicać standardy i stosować rozwiązania wspólne dla wszystkich naszych zakładów, co ułatwia zarządzanie nimi i ich integrację. Jest to szczególnie ważne przy modernizacji i rozbudowie już istniejących systemów. A tam, gdzie widzimy, że jest to nieuzasadnione kosztowo, zamiast starego wdrażamy nowe rozwiązanie.

→ Jakie jest główne kryterium wyboru systemu? Co jest priorytetem dla menedżera do spraw bezpieczeństwa?

Prowadzimy wiele projektów mających na celu zapewnienie bezpieczeństwa naszym zakładom. Staramy się inwestować w systemy nowoczesne, ale głównym kryterium jest ich otwartość. Ważna jest możliwość elastycznej rozbudowy, a także integracji z systemami różnych producentów, które na przestrzeni lat wdrażaliśmy w naszych zakładach. W naszej grupie mamy przedsiębiorstwa, na które składają się obiekty rozproszone, zlokalizowane również na terenach leśnych. Tu trudno mówić o ochronie scentralizowanej lub tylko o wybranym jej elemencie, np. ochronie perymetrycznej. Decyzja o wyborze rozwiązania musi być poprzedzona głęboką analizą zarówno zagrożeń i ryzyka, jakie niesie za sobą brak takiego czy innego zabezpieczenia w tym konkretnym miejscu, jak i analizą kosztową. W zarządzaniu kluczową kwestią jest kontrola kosztów i wiadomo, że w czasach pandemii i spowolnienia aktywności gospodarczej naturalna tendencja to cięcie wydatków. Moją rolą jest wykazanie, że zainwestowanie w system zabezpieczeń kwoty X pozwoli na zredukowanie ryzyka i strat na kwotę Y. A nie jest to zadanie łatwe.
Kluczowym elementem jest tu identyfikacja wszystkich zagrożeń, jakie się pojawiają w poszczególnych obszarach. I nie chodzi tylko o zapewnienie bezpieczeństwa fizycznego, ale także o utrzymanie ciągłości łańcucha dostaw czy płynności sprzedaży. Zagrożenia, jakie występują na tej linii, powodują pewne zaburzenia. Znając je i identyfikując miejsca ich występowania, można nimi zarządzać. Są już systemy, które analizują przepływ danych w łańcuchu dostaw, filtrują anomalie, na których podstawie możemy identyfikować problem i podejmować decyzję o dalszych działaniach. Na bazie tych anomalii możemy raportować zarządowi, że w danej fabryce występują określone straty, i uzasadnić konieczność inwestycji w systemy bezpieczeństwa. Analiza pojedynczych incydentów, np. wychwycenie przez kamery systemu dozorowego nielegalnego wywozu towaru, stanowi kroplę w morzu potrzeb. Według mojej wiedzy jest to ok. 5% wszystkich zdarzeń w zakładach produkcyjnych.

→ Które systemy zabezpieczeń są kluczowe dla działalności firmy?

Priorytetowo traktujemy systemy sygnalizacji pożarowej. Nasze zakłady produkcyjne są w grupie ryzyka powstawania awarii przemysłowej, szczególnie CIECH Sarzyna produkujący środki ochrony roślin (agro) oraz CIECH Pianki produkujący piankę PUR, która przecież jest produktem mogącym ulec nawet samozapłonowi w procesie dojrzewania. Obowiązują w nich szczególne obostrzenia, jeśli chodzi o systemy ppoż., które stanowią nadrzędny element zabezpieczeń. Jesteśmy pod stałym nadzorem Państwowej Straży Pożarnej i Wojewódzkiego Inspektoratu Ochrony Środowiska. Na terenie naszego zakładu w Nowej Sarzynie bardzo często ćwiczenia odbywa jednostka ratownictwa chemicznego PSP, którego siedziba jest zlokalizowana tuż obok. To bardzo ważne z punktu widzenia nie tylko naszej firmy, ale także innych tego typu obiektów. Te ćwiczenia pozwalają strażakom na obeznanie się z instalacjami zakładowymi, a naszym pracownikom na zdobycie doświadczenia w prawidłowej reakcji na tego typu zdarzenia.

Tomasz Guzikowski z CIECH (po prawej) w rozmowie z Janem Grusznicem z „a&s Polska" (po lewej)

Fabryki nie da się wywieźć w kieszeni, ale można ją zniszczyć jednym przyciśnięciem guzika

W naszych zakładach bezpieczeństwo traktujemy w sposób kompleksowy. Osobom nieczującym potrzeby inwestowania w systemy zabezpieczeń zawsze powtarzam: fabryki w kieszeni wywieźć się nie da, ale można ją zniszczyć za pomocą przyciśnięcia jednego guzika. I mało kto zdaje sobie z tego sprawę. Dla nas mniej istotne jest pilnowanie przez system ochrony perymetrycznej dzików, żeby nie niszczyły ogrodzenia i nie wchodziły na teren zakładu. Kluczową sprawą jest zabezpieczenie konkretnych miejsc, konkretnych instalacji, konkretnych pomieszczeń. Realizujemy to za pomocą systemów telewizji dozorowej i kontroli dostępu. System telewizyjny informuje, kto wchodzi na teren zakładu i kto z niego wychodzi, ale też daje dyspozytorom czy aparatowym wiedzę na temat tego, co dzieje się na produkcji. Do tego celu stosujemy kamery termowizyjne oraz, ze względu na to, że mamy wiele stref zagrożonych wybuchem, kamery w obudowach odpornych na wybuchy.

Kamery dozorowe stosujemy nie tylko do obserwacji otoczenia. Wyposażone w funkcje analityczne generują alarmy, np. w przypadku naruszenia strefy przez osoby do tego nieuprawnione czy wykrycia osoby bez kasku lub kamizelki odblaskowej. Mogą też emitować komunikaty głosowe, wtedy reakcja na zdarzenie jest natychmiastowa. Szczególnie przydatne są kamery z funkcją rozpoznawania numerów tablic rejestracyjnych do automatycznego wpuszczania na teren zakładu pojazdów uprawnionych.

Bardzo istotne są dla nas kamery nadzorujące procesy produkcyjne, monitorujące temperaturę czy wibracje urządzenia. Uzyskiwane dane są interpretowane przez odpowiednie oprogramowanie, które informuje operatora o wszelkich odstępstwach od normy. To pozwala na wczesną reakcję, zanim nastąpi awaria.

→ Co ma wpływ na dobór rozwiązania?

Wybierając rozwiązania, kierujemy się zasadą dostępności na rynku i możliwościami sprawdzenia ich działania w innych zakładach o podobnym profilu. Korzystamy z tzw. wizyt referencyjnych. Obecnie wdrażamy projekt obejmujący m.in. Yard Management – system informatyczny do zarządzania dostawami połączony z kontrolą dostępu i systemem do wydawania przepustek, przy którego planowaniu również opieraliśmy się na doświadczeniach innych firm. Drugim elementem jest rachunek ekonomiczny – optymalizacja kosztów, zwłaszcza stosunek nakładów do celów, jakie uda nam się dzięki temu rozwiązaniu osiągnąć, a to wiąże się z realnymi oszczędnościami. Nakłady szacujemy w okresie nie dłuższym niż pięć lat, zarówno ze względu na specyfikę naszej działalności, jak i cykl życia urządzeń systemów zabezpieczeń.

→ Czy systemami zabezpieczeń zarządzacie centralnie, czy lokalnie? Czy korzystacie z usług firm trzecich?

Kiedy przychodziłem do organizacji, było kilka pomysłów na rozwiązanie tego dylematu. Ja uważam, że przy takim rozproszeniu obiektów, jakie jest w naszej grupie kapitałowej, zarządzanie centralne się nie sprawdzi. Testowaliśmy tego typu rozwiązanie. Podpięliśmy dwa zakłady pod system centralnego zarządzania obsługiwany przez jedną z firm ochrony, ale to okazało się nieefektywne. Dlatego zdecydowaliśmy się na zarządzanie lokalne, z osobami do obsługi poszczególnych zakładów pracującymi na miejscu. Natomiast kwestie utrzymania systemów i ochronę fizyczną zlecamy firmom trzecim.

Mamy bardzo wysokie wymagania co do bezpieczeństwa rozwiązań. Nasi wykonawcy dostają od nas szczegółowe instrukcje dotyczące sposobu wykonania systemu, wymagań dotyczących konkretnych urządzeń. Niejednokrotnie już spotkaliśmy się z rezygnacją ze względu na niemożność dotrzymania naszych wysokich standardów.

W dużych zakładach produkcyjnych kluczowe znaczenie ma utrzymanie ciągłości produkcji, na co wpływ ma również system zdalnego pomiaru stanu urządzeń. To nie tylko kamery, które rejestrują pracę poszczególnych maszyn – temperaturę, drgania itp. Ponieważ nie wszędzie da się je zainstalować, w naszych zakładach stosujemy system zwany „mobilny obchodowy". Każdy tzw. aparatowy produkcji jest wyposażony w specjalne urządzenie, ma zadany harmonogram i trasę obchodu na swojej zmianie oraz wytypowane elementy, na które powinien zwrócić uwagę. Te czynności może też wykonać za pomocą aplikacji na telefonie komórkowym. Jeśli zauważy, że coś jest nie tak, może zrobić zdjęcie, może nagrać film i te informacje wraz z komentarzem przekazać do systemu, gdzie jest generowany raport do odpowiednich służb utrzymania ruchu.

→ Nie sposób uniknąć pytania o sytuację związaną z pandemią koronawirusa. Jakie działania zostały podjęte w zakładach?

Uważam, że bardzo dobrze sobie poradziliśmy. Bardzo szybko powołaliśmy sztab kryzysowy. Procedury, które natychmiast wdrażaliśmy i które przekazaliśmy wszystkim pracownikom w przystępnej formie, odniosły zamierzony cel. Do tej pory nie mieliśmy przestojów w produkcji spowodowanych pandemią. Ustaliliśmy wiele zasad, m.in. pracowników, którzy mogą pracować zdalnie, wysyłamy na *home office*. Oczywiście pracowników produkcyjnych na pracę zdalną wysłać się nie da. Zrobiliśmy jednak wszystko, aby byli bezpieczni. Wprowadziliśmy procedury wchodzenia na teren zakładów, poruszania się po nich, obowiązek dezynfekcji rąk i noszenia maseczki, mierzyliśmy temperaturę. Do tego celu testowaliśmy różne rozwiązania, ale nie znalazłem idealnego. Nie ma na rynku systemu, który byłby skuteczny na zewnątrz obiektu, bo technologia jeszcze nie nadąża za tymi potrzebami. Zastanawialiśmy się nad przejściami kontenerowymi (dwa kontenery złączone ze sobą) z kamerą termowizyjną, ale otwieranie drzwi destabilizowało warunki i pomiary nie były wiarygodne. Testowaliśmy również systemy sensorowe, ale w rezultacie zdecydowaliśmy się na rozwiązanie tradycyjne: pracownik ochrony z termometrem w ręku. Natomiast w pomieszczeniach, tam gdzie są stabilne warunki otoczenia, np. na portierniach, w biurach stosowaliśmy pomiary termowizyjne.

Nasz sztab kryzysowy na bieżąco analizuje sytuację, systematycznie są wysyłane komunikaty do pracowników informujące o tym, co dzieje się w zakładzie. Dziś już wiemy, że można się zakazić wszędzie, na wiele sposobów. Zauważalne jest rozluźnienie dyscypliny w społeczeństwie, dlatego staramy się cały czas uczulać pracowników i podnosić ich świadomość o możliwym zagrożeniu. Dostosowujemy procedury do zmieniających się okoliczności – dziś już wiadomo, że pomiar temperatury jest nie do końca efektywny, ponieważ gorączka nie jest już głównym objawem zakażenia koronawirusem. Wszyscy teraz jesteśmy mądrzejsi i wiemy, że większość przypadków zakażenia może przebiegać bezobjawowo.

Mamy opracowane procedury postępowania na konkretne scenariusze, które zidentyfikowaliśmy jako najbardziej prawdopodobne. Jednym z działań, jakie wdrożyliśmy w ramach walki z COVID-19, było wyprodukowanie w zakładach CIECH Vitrosilicon własnych przyłbic, w zakładzie w Nowej Sarzynie powstał płyn do dezynfekcji, a w CIECH Pianki przymierzamy się do produkcji maseczek ochronnych, także tych z certyfikacją FFP1 i FFP2. Dostosowaliśmy własną produkcję do potrzeb rynku. Dzięki wdrożonym wcześniej rozwiązaniom mogliśmy elastycznie przestawić się na produkcję akcesoriów, których wiosną brakowało na rynku.

Co więcej, dzieliliśmy się naszymi produktami z innymi, np. nasz zakład CIECH Pianki przekazał do szpitala w Bydgoszczy materace, CIECH Vitrosilicon – przyłbice ratownikom medycznym na Żaganiu, przekazywaliśmy też płyn do dezynfekcji. Nie zapomnieliśmy o naszych pracownikach. Ci, którzy w czasie największego zagrożenia, nie mogąc iść na *home office*, pracowali w zakładzie, od zarządu otrzymali specjalną nagrodę pieniężną.

→ Nad czym pracujecie obecnie?

Jesteśmy teraz w fazie głębokiej transformacji. A największym problemem jest to, że nie da się wszystkiego zrobić naraz. Dlatego wdrażanie dzielimy na etapy, jesteśmy dopiero na początku drogi do zautomatyzowania zakładów. Chcemy mieć wiedzę o stanie maszyn, ale też wiedzieć, kiedy ta maszyna może się popsuć, i zrobić wszystko, aby przedłużyć czas jej bezawaryjnej pracy. Dlatego tak ważne są czujniki IoT, bo zbierane z nich dane pomagają we wdrożeniu procedur konserwacji predykcyjnej urządzeń.

→ Czego firma oczekuje od producentów i dostawców elektronicznych systemów zabezpieczeń teraz i w przyszłości?

Idealnie byłoby, gdyby dostawcy, wykonawcy – nie tylko producenci – umieli się dostosować do naszych wymagań. Chciałbym, żeby konkurowali między sobą w tym zakresie. Zakładam, że przy większej konkurencji ceny będą niższe, a jakość usług wyższa. W obszarze wykonywania usług instalatorzy powinni wykazywać się maksymalnym profesjonalizmem i zwracać uwagę na dostosowanie instalacji do potrzeb zakładu, a nie opierać się tylko na informacjach przekazanych przez producenta. Bardzo często nie zdają sobie sprawy z tego, że przecięcie jednego kabla może spowodować przerwę w produkcji i milionowe straty. Oczywiście mamy sprawdzonych dostawców, z którymi współpracujemy od dawna, ale większa konkurencja z pewnością wpłynęłaby na jakość usług.

Bardzo dobrym prognostykiem na przyszłość jest to, że coraz więcej producentów wprowadza systemy otwarte. Można je integrować z innymi systemami, co w przypadku naszej grupy jest bardzo ważne. Wybierając rozwiązanie, zawsze będę kierował się tym kryterium. Gdybym więc miał wysłać sygnał do producentów, to właśnie taki: żeby stawiali na otwartość swoich systemów. Jeśli firmy chcą się liczyć na rynku i utrzymać klienta, to muszą konkurować lepszym serwisem, ceną – co w naszych warunkach jest oczywiste – i dodatkowymi funkcjonalnościami.

→ Z dodatkowymi funkcjonalnościami wiąże się opcja chmury. Czy przewidujecie wykorzystanie w systemach zabezpieczeń elementów chmury publicznej?

Analizujemy takie rozwiązania, ale jeszcze nie planujemy ich wdrożenia. Po pierwsze ze względu na bezpieczeństwo funkcjonowania w przestrzeni cyber. Po drugie ze względu na konieczność dywersyfikowania rozwiązań. Jeśli wszystko oprzemy na jednym rozwiązaniu, w przypadku awarii istnieje ryzyko utraty ciągłości działania. A czy będziemy stosować rozwiązania chmurowe, czas pokaże.

Obiekty rozproszone zintegrowane zarządzanie bezpieczeństwem

Skuteczne zarządzanie bezpieczeństwem rozproszonych obiektów jednej organizacji jest dużym wyzwaniem – zwłaszcza gdy administratorowi zależy na zachowaniu wysokiego standardu ochrony każdej placówki przy jednoczesnym utrzymaniu efektywności ekonomicznej inwestycji.

Skuteczne zabezpieczenie wszystkich oddziałów danej organizacji można osiągnąć poprzez montaż zaawansowanych systemów SWiN – takich, które oferują możliwość wzajemnej integracji i zarządzania całą ich siecią. Przykładem są centrale alarmowe rodziny INTEGRA oraz oprogramowanie integrujące INTEGRUM firmy SATEL.

INTEGRUM umożliwia centralny nadzór nad zintegrowanymi systemami zabezpieczeń pracującymi w obiektach rozproszonych. Usprawnia procesy administracyjne, w tym zarządzanie bazą użytkowników, co przekłada się na oszczędność czasu obsługi systemu. Dzięki jego skalowalności liczba zabezpieczanych obiektów jest nieograniczona. Zdalny bieżący wgląd w stan zintegrowanych instalacji sprawia, że reakcja na określony typ zdarzeń, np. alarmy czy awarie, może nastąpić niezwłocznie.

Zalety INTEGRUM najłatwiej opisać przykładami:

Zdalne zarządzanie użytkownikami

Specjalista HR, przyjmując nowego pracownika biura w miejscowości A, tworzy mu indywidualny profil użytkownika. Wręcza też kartę zbliżeniową umożliwiającą dostęp do biura znajdującego się w sąsiedniej miejscowości. Po okresie próbnym karta automatycznie stanie się nieaktywna. Przy przedłużeniu umowy dostęp będzie odnawiany zdalnie.

Szybkość reakcji

Stacja monitoringu otrzymuje informację o alarmie w miejscowości B w strefie „Magazyn C-1" obiektu D-2. Operator stacji wybiera w panelu sterowania INTEGRUM widok planu budynku i z poziomu mapy włącza pogląd z kamer – weryfikacja alarmu możliwa jest niemal natychmiast. Fałszywy alarm może od razu skasować. Gdyby zaś sytuacja tego wymagała, może wysłać na miejsce patrol interwencyjny. Przy zarejestrowanym wydarzeniu operator umieszcza komentarz ułatwiający późniejsze odnalezienie wpisu w archiwum.

Mobilność

Koordynator ds. bezpieczeństwa, będąc w drodze na odbiór techniczny nowego budynku w mieście D, otrzymuje informację o awarii systemu alarmowego w obiekcie na drugim końcu regionu. Z tabletu loguje się do systemu, aby określić źródło problemu. Konieczna okazuje się wizyta technika – koordynator natychmiast powiadamia serwis, aby po chwili kontynuować jazdę na miejsce odbioru.

Pewność przesłania informacji

W sąsiedztwie chronionego biurowca uszkodzony zostaje światłowód, w efekcie nie ma dostępu do Internetu. Aby komunikacja między systemem alarmowym nadzorującym obiekt a centralą bezpieczeństwa organizacji nie została utracona, transmisja danych jest automatycznie przeniesiona do sieci komórkowej. Gdy łącze naziemne zostanie naprawione, komunikacja powróci na główny tor łączności.

INTEGRUM jest narzędziem umożliwiającym wygodne i pewne administrowanie bezpieczeństwem sieci obiektów – m.in. instytucji finansowych, urzędów, firm wielooddziałowych, które mieszczą się w różnych lokalizacjach. Pozwala optymalizować koszty i oszczędza czas administratorów systemów bezpieczeństwa. □

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

Rozwiązania Hikvision dla przemysłu

Zastosowanie urządzeń i systemów VSS (system dozoru wizyjnego) jest powszechnie kojarzone z prewencją i funkcjami związanymi z ochroną obiektu czy to przed wtargnięciem intruza, czy kradzieżą mienia (pozwalają rozpoznać i zidentyfikować intruza).

T E K S T
Zbigniew Morawski
Hikvision Polska

Dzięki coraz większej mocy obliczeniowej i inteligencji wbudowanej w urządzenia, systemy te pełnią również inne, ważne z punktu biznesowego, funkcje.

Zwiększenie bezpieczeństwa BHP

Zmorą dużych zakładów, w których działają firmy podwykonawcze, jest nieprzestrzeganie przepisów BHP. Poziom bezpieczeństwa życia i zdrowia osób tam pracujących można podnieść dzięki zastosowaniu kamer serii iDS-2CD7A46 wyposażonych w algorytmy głębokiego uczenia się. Jedną z funkcji tych kamer jest detekcja kasku ochronnego na głowie. Urządzenie musi najpierw rozpoznać, czy obserwowany obiekt jest człowiekiem, a następnie określić, czy nosi kask ochronny. Skuteczność algorytmu jest duża i nie powoduje zmęczenia operatora fałszywymi alarmami.

Innym przykładem urządzeń chroniących zdrowie pracowników w czasie pandemii COVID są kamery wykorzystywane do pomiaru temperatury ciała przy wejściach do zakładów. Systemy te nie muszą gromadzić danych związanych ze stanem zdrowia pracowników, żeby pełnić funkcję przesiewową i zabezpieczyć zakład przed kryzysem związanym z zakażeniem COVID-19. Hikvision oferuje zarówno kamery stacjonarne, np. DS-2TD2636B-15/P, jak i terminale do samodzielnej kontroli MinMoe.

Kontrola ruchu pojazdów

Kamery mogą kontrolować ruch pojazdów na terenie zakładu, nadzorując miejsca, gdzie niedozwolone jest zatrzymywanie, parkowanie, zawracanie czy jazda w nieodpowiednim kierunku. Dla dużych zakładów pomocne mogą być kamery PTZ serii iDS-2VS435-F840-EY z zaimplementowanymi algorytmami kontroli ruchu pojazdów. Oprócz standardowego przechwytywania obrazów mają funkcję robienia zdjęć, które można później wykorzystać do szybkiego przeszukania archiwum.
W pojazdach wykorzystywanych w procesach produkcyjnych stosuje się urządzenia mobilne, zapewniające komfort pracy operatorom oraz gromadzące materiał archiwalny, dzięki czemu łatwiej odtworzyć ewentualny przebieg wypadku. Montuje się je na dźwigach, maszynach przeładunkowych czy pojazdach specjalnych. Urządzenia dedykowane do pojazdów mają specjalną obudowę odporną na zapylenia i występujące wibracje. Przykładem jest rejestrator 32-kanałowy DS-MP3516-RH.

Zabezpieczenie przeciwpożarowe

Również i na tym polu widać powolny, ale nieuchronny postęp w kierunku zastosowań urządzeń systemów VSS. Wiosną tego roku firma Hikvision otrzymała dla swoich urządzeń certyfikaty francuskiego laboratorium CNPP potwierdzające przydatność kamer do detekcji temperatury. Warto zaznaczyć, że do niedawna na ryku nie było ocen niezależnych ośrodków dla tego typu kamer i producenci, by przekonać klienta, musieli wspomagać się własnymi badaniami i torami testowymi. Certyfikacji poddano kamery stałopozycyjne i obrotowe, co daje klientom możliwość swobodnego dostosowania urządzeń do konkretnych aplikacji. Certyfikowane kamery pracują z przetwornikami obrazu o rozdzielczości 384 x 288 oraz 640 x 512 i są dostępne w wersjach termowizyjnej oraz dualnej (z powiązaną kamerą światła widzialnego).
Kamery termowizyjne stosuje się do ochrony ppoż. takich obiektów, jak taśmociągi, stacje energetyczne, turbozespoły, składowiska paliw itd.
Ciekawą propozycją zabezpieczenia obiektów przemysłowych są kamery PTZ i na głowicach uchylno-obrotowych, mające możliwość skanowania terenu. Skanowanie odbywa się z wykorzystaniem presetów i definiowanych scen. W każdej scenie można zdefiniować do 10 regionów detekcji. □

Hikvision Poland

ul. Żwirki i Wigury 16B,
02-092 Warszawa
info.pl@hikvision.com
https://www.hikvision.com/europe/

– lider w ochronie perymetrycznej

Fiber SenSys to firma amerykańska, która od ponad 20 lat produkuje systemy ochrony obwodowej oparte na aktywnych kablach światłowodowych. Jest częścią grupy OPTEX – światowego lidera systemów ochrony zewnętrznej.

Rozwiązania Fiber SenSys wykorzystują opatentowaną technologię światłowodową i charakteryzują się wysoką skutecznością detekcji intruza, możliwością konfiguracji wielu parametrów strojenia oraz łatwą integracją z innymi elektronicznymi systemami zabezpieczeń, np. CCTV.
Koncepcja systemu jest oparta na aktywnym światłowodzie mocowanym do istniejącego ogrodzenia. Drgania ogrodzenia wywołane ingerencją intruza (wspinanie, cięcie, unoszenie) są analizowane w procesorze wysyłającym sygnał alarmowy, a specjalne algorytmy potrafią odróżnić intruzów od fałszywych pobudzeń generowanych np. przez wiatr. Systemy światłowodowe są odporne na działanie czynników środowiskowych, włączając w to zakłócenia elektromagnetyczne i radiowe (EMI/RFI), wilgoć, sól, promieniowanie UV, a nawet uderzenia pioruna. Gwarantują stabilną pracę we mgle, zapyleniu czy ciemności i mogą być stosowane w strefach zagrożonych wybuchem.

W ofercie Fiber SenSys znajdują się systemy dedykowane do zaawansowanych i rozproszonych aplikacji oraz takie, których koszt instalacji jest porównywalny np. z kosztem uruchomienia systemu aktywnych barier podczerwieni. W zależności od modelu jeden procesor może obsługiwać 2, 8 lub 25 stref detekcji, a maks. długość aktywnego światłowodu na jedną strefę wynosi od 500 m do 5 km. Alarm jest wywoływany w strefie – użytkownik może zdecydować, jaka długość strefy jest najbardziej odpowiednia dla zapewnienia właściwego sposobu weryfikacji i reagowania.
W najprostszych światłowodowych systemach alarmowych Fiber Defender procesor sterujący (APU) jest montowany na płocie. Instalacja i uruchomienie systemu są niezwykle proste, wystarczy zainstalować aktywny światłowód na ogrodzeniu, podłączyć do procesora i wybrać kilka podstawowych parametrów strojenia w oprogramowaniu. Seria FD300 oferuje szeroką gamę produktów, które można dopasować do różnych zastosowań oraz budżetów. Ich przewaga ekonomiczna nad innymi systemami jest widoczna nie tylko w niskiej cenie zakupu, ale także w niemal zerowym koszcie posiadania. Procesor sterujący będzie działał przez lata, a czujnik światłowodowy w osłonie posłuży dłużej niż ogrodzenie, na którym został zamontowany.
Najwyższy standard ochrony w obiektach wojskowych zagwarantują urządzenia serii FD34X zaprojektowane do ochrony odległych lokalizacji, w których zasilanie i łączność są niedostępne. Oprócz aktywnego światłowodu urządzenie wykorzystuje nieaktywny kabel światłowodowy, co umożliwia montaż APU nawet w odległości 20 km od chronionej strefy. Niezawodność systemu jest potwierdzona certyfikatem najwyższej klasy ochrony armii USA, zezwalającym na instalację w obiektach, w których przechowywane są materiały nuklearne.
Serię FD500 zaprojektowano do ochrony perymetrycznej rozproszonych obiektów komercyjnych i infrastruktury krytycznej. 8- lub 25-strefowy procesor APU jest dostępny m.in. w obudowie umożliwiającej montaż w standardowej szafie rack 19”, w wartowni lub centrum monitoringu oddalonym od chronionego obszaru do 10 km. System detekcji intruzów za pomocą aktywnego kabla światłowodowego prowadzonego wzdłuż granicy chronionego terenu jest w stanie wykryć nawet 5 jednoczesnych prób włamania w więcej niż jednej lokalizacji wokół całego chronionego obszaru. □

OPTEX Security zaprasza na **WEBINARIUM** poświęcone rozwiązaniom Fiber SenSys. Szkolenia organizowane w ramach Akademii OPTEX to skondensowane i merytoryczne spotkania online, w trakcie których specjaliści firmy dzielą się z uczestnikami wiedzą techniczną oraz wskazówkami instalacyjnymi na temat produktów i rozwiązań OPTEX. Szczegóły oraz rejestracja: www.optex-europe.com/pl, e-mail: optex@optex.com.pl

OPTEX Security

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

Człowiek rozsądny dostosowuje się do świata. Człowiek nierozsądny usiłuje dostosować świat do siebie. Dlatego wielki postęp dokonuje się dzięki ludziom nierozsądnym

George Bernard Shaw

Nowoczesne podejście do ochrony obwodowej

TEKST

Bartosz Golczak

RCS Engineering

W ostatnich latach nastąpił ogromny rozwój technologii. Od maszyn zajmujących niegdyś całe pokoje doszliśmy do komputerów noszonych na nadgarstkach. Telefony stacjonarne zostały zastąpione bezprzewodowymi aparatami GSM. Komputeryzacja wkroczyła niemal w każdą dziedzinę naszego życia. Branża security wiedzie prym w tym wyścigu. Kamery analogowe częściej można znaleźć w garażu niż w przestrzeni publicznej. Zabezpieczenia techniczne przeszły fazę miniaturyzacji i komputeryzacji. Dziś, wdrażając system alarmowy, trzeba być bardziej informatykiem niż elektronikiem. Postęp ten jest szczególnie widoczny w systemach ochrony perymetrycznej. Niegdyś obiekty były chronione zabezpieczeniami elektronicznymi tylko w obrębie budynków. Powoli technika umożliwiała coraz bardziej skuteczną ochronę obiektów również na zewnątrz. Podejście takie diametralnie zmieniło skuteczność całego łańcucha ochrony, pozwalając identyfikować intruzów już na granicy posesji. Umożliwiło detekcję i odstraszanie intruzów oraz podjęcie reakcji na tyle wcześnie, aby możliwy był przyjazd grupy interwencyjnej jeszcze przed potencjalnym zniszczeniem mienia. Elementem wspierającym systemy sygnalizacji włamania i napadu są rozwiązania monitoringu wizyjnego – najszybszy i skuteczny sposób weryfikowania zdarzeń alarmowych.

Niestety, jak to zwykle bywa, potrzeba było czasu, aby unowocześnić ochronę obwodową. Pierwsze systemy były bardzo podatne na wszelkiego rodzaju fałszywe alarmy. Trudne początki zniechęciły wielu inwestorów do stosowania zabezpieczeń elektronicznych zewnętrznych. Ogromna liczba fałszywych alarmów znacznie uprzykrzała również pracę służbom ochrony. Ochrona perymetryczna ewoluowała również, jeśli chodzi o sposoby zabezpieczenia. Producenci prześcigali się w tworzeniu takiego typu rozwiązań – począwszy od czujek zewnętrznych (zarówno mikrofalowych, jak i laserowych), poprzez bariery (mikrofalowe czy podczerwieni), na zabezpieczeniu samego ogrodzenia kończąc. To właśnie systemy napłotowe znacznie przyspieszyły możliwość wczesnego alarmowania i poprawiły skuteczność ochrony obiektu. Już na etapie próby sforsowania ogrodzenia, czyli tam, gdzie inwestor może najwcześniej reagować, można wykryć potencjalnego intruza. Dzięki temu służby ochrony mają więcej czasu na reakcję, a sam intruz często rezygnuje ze swojego działania, nie wchodząc nawet na teren chroniony.

Systemy napłotowe permanentnie podlegały transformacji i rozwojowi. Największym problemem była dość niska skuteczność systemów kablowych, narażonych m.in. na przegryzanie przez dzikie zwierzęta czy podatnych na szybkie przecięcie przez potencjalnego intruza. Obserwacje istniejących systemów oraz potrzeby klientów sprawiły, iż na początku XXI w. grupa inżynierów założyła spółkę Ronyo Technologies, która miała za zadanie skonfrontować potrzeby rynku z dostępną technologią i opracować nowy, innowacyjny produkt.

Po kilku latach badań i testów powstał nowoczesny, a przede wszystkim skuteczny system ochrony obwodowej VARYA PERIMETER. Główną zmianą w sposobie działania była realizacja szyfrowanej transmisji sygnału w dedykowanym paśmie 868 MHz, wykluczająca kabel zaplatany na ogrodzeniu. Zmiana ta pozwoliła znacznie przyspieszyć montaż detektorów na wszelkiego typu płotach. Oszczędność wynikająca z braku potrzeby zakupu kilometrów przewodów pozwoliła stworzyć bardzo nowoczesny system, nieodbiegający przy tym cenowo od dotychczasowych rozwiązań. Dzięki zmianie medium transmisji można było stworzyć nowoczesny system charakteryzujący się wieloma cechami, czasem nieosiągalnymi dla rozwiązania przewodowego. Osiągnięto odporność na wyładowania atmosferyczne – brak kabla wplatanego w ogrodzenie, który mógł stanowić swojego rodzaju antenę ściągającą wyładowania. VARYA PRIMETER został tak zaprojektowany, aby w jednolity sposób chronić całe ogrodzenie, łącznie z furtkami i bramami. Dotychczas wymagane było stosowanie dedykowanych barier podczerwieni.

System jest w pełni adresowalny, można zlokalizować źródło alarmu włamaniowego z dokładnością do jednego przęsła ogrodzenia, co daje rozdzielczość nawet jednego metra. Projektanci skupili się na znacznym unowocześnieniu detektorów w stosunku do istniejących rozwiązań ochrony obwodowej. Każdy z detektorów jest wyposażony nie tylko w znane u konkurencji czujniki mierzące przyspieszenie liniowe (akceleratory), ale również doposażony w pomiar położenia kątowego (żyroskop). Zastosowanie dwóch technik pomiaru zdecydowanie zwiększa skuteczność całego systemu, eliminując przy tym fałszywe alarmy.

Ważnym aspektem, na jaki zwracano uwagę przy tworzeniu systemu, był również wygląd zewnętrzny. Estetyka to często podkreślany przez inwestorów element charakteryzujący rozwiązanie VARYA PERIMETER. Nie dość, że na ogrodzeniu nie widać plątaniny kabli i trzymających je opasek kablowych, to zamontowane detektory mają estetyczne obudowy, które już na etapie produkcji można dopasować do ogrodzenia, wybierając kolor detektora z szerokiej palety RAL.

Od ponad 10 lat Ronyo Technologies wraz z dystrybutorami systemu ochrony obwodowej VARYA PERIMETER dopracowywali szczegóły i reagowali na potrzeby rynku. Ogromna liczba prezentacji i indywidualnych testów na terenach obiektów infrastruktury krytycznej zaowocowała pierwszymi strategicznymi realizacjami w zachodniej części Europy, w tym m.in. więzienia w Niemczech, giganta petrochemicznego w Niemczech, obiektów wojskowych NATO w Europie czy magazynów podziemnych gazu na Słowacji. Realizacje dotyczyły zarówno obiektów mniejszych, jak i bardzo rozległych – nawet do 20 km obwodu.

Od 2014 r. VARYA PERIMETER jest obecny na naszym lokalnym rynku i reprezentowany przez generalnego dystrybutora – firmę RCS Engineering. System został sprawdzony i przetestowany w wielu miejscach w Polsce. Od samego początku inwestorzy doceniali wiele innowacyjnych aspektów i wskazywali dotychczasowe problemy z systemami kablowymi. Pierwsze wdrożenia w Polsce dotyczyły infrastruktury krytycznej – m.in. obiekty KGHM Miedź Polska SA czy MPWiK, aż po rozległe obiekty wojskowe. System znalazł uznanie również w sektorze prywatnym, w koncernach KIA, 3M Group, Mercedes czy Volkswagen. Najnowszą realizacją w Polsce jest jedna z największych inwestycji w naszym kraju – fabryka silników w Jaworze dla koncernu Daimler / Mercedes. Oprócz pełnej redundancji systemu VARYA PERIMETER zastosowano szereg integracji z systemem CCTV i megafonami sieciowymi Axis Communications.

Więcej szczegółów na stronie www.rcse.pl.

Wybrane parametry systemu Varya Perimeter

- W pełni adresowalny detektor dwupomiarowy do ochrony ogrodzenia z dokładnością detekcji do jednego przęsła i redundancją wszystkich elementów systemu.
- Komunikacja poprzez zaszyfrowany, odporny na zakłócenia, protokół pracujący na częstotliwości 868 MHz
- Typ sensorów: akcelerometr 3-osiowy i żyroskop
- Obudowa IP67
- Maks. długość chronionego ogrodzenia z jednej jednostki centralnej: 5 tys. m
- Detektory rozmieszczane standardowo, co drugie przęsło (ok. 5 m), możliwość montażu co przęsło
- Dokładność detekcji, w zależności od ogrodzenia nawet do 50 cm
- Montaż na każdym typie ogrodzeń
- Możliwość dowolnego podziału perymetru na strefy alarmowe
- Inteligentny pomiar mechanicznych właściwości ogrodzenia
- Szybkość transmisji sygnału alarmowego: do 1 s
- Autotest systemu: raz na 12 lub 24 h
- Odporność na fałszywe alarmy spowodowane warunkami pogodowymi, w tym wyładowania atmosferyczne - zaszyty algorytm WAV
- Jednolite zabezpieczenie również bram i furtek – detektory wyposażone w czujniki Hallotronowe
- Zakres temp.: -40 do + 70°C
- Wej/wyj alarmowe: wejścia logiczne, wyjścia przekaźnikowe, wyjścia logiczne 2EOL (wszystkie zabudowane w centralce lub dostępne przez dedykowane moduły rozszerzeń)
- Szybki montaż i demontaż – dzięki komunikacji radiowej, na płocie montuje się tylko detektory
- Certyfikat GRADE 4 zgodnie z normą PN-EN 50131
- Zgodność z Normą Obronną
- Integracje z PSIM, VMS, kamerami CCTV oraz megafonami sieciowymi

RCS Engineering

ul. 28 Czerwca 1956 r. 406, 61-441 Poznań
https://rcse.pl/
biuro@rcse.pl

Ochrona perymetryczna Axis łączy wszystko w spójną całość

Ochrona perymetryczna połączona w spójny system powinna obejmować otoczenie zewnętrzne – ogrodzenie (obwód), obszar wewnątrz obwodu (strefa peryferyjna) oraz budynki i obiekty wymagające ochrony. Systemy ochrony perymetrycznej zabezpieczają rozległe, rozproszone obiekty przemysłowe, a także duże strefy podlegające, ze względów bezpieczeństwa, szczególnemu nadzorowi – lotniska, strefa graniczna, rozległe obiekty sportowe czy infrastruktura telekomunikacyjna oraz krytyczna, w tym cywilna, np. ujęcia wody pitnej.

Ogromne przestrzenie oraz infrastruktura wymagająca takiej ochrony muszą być pod stałym dozorem, aby móc szybko i skutecznie eliminować wszelkie zagrożenia mienia i życia ludzkiego – począwszy od ataków terrorystycznych, poprzez wyrządzenie szkody materialnej na skutek zniszczenia czy zakłócenia pracy obiektów, na zdrowiu i życiu osób obsługujących dany obiekt skończywszy.

Mowa nie tylko o zagrożeniach, które zależą od działań człowieka, ale także o zagrożeniach losowych powodowanych przez zjawiska naturalne, takie jak katastrofy wywoływane ekstremalnymi zjawiskami atmosferycznymi. Dlatego na system ochrony perymetrycznej składają się różne, adekwatne rozwiązania – zarówno czujki i detektory ochrony zewnętrznej, jak i niezbędne w przypadku zabezpieczania dużych obiektów systemy kontroli dostępu oraz takie rozwiązania i technologie, jak termowizja, radary, czujniki ruchu czy klasyczne systemy dozoru wizyjnego.

Jednym z najnowocześniejszych systemów tej klasy jest **system ochrony perymetrycznej Axis**. Trzystrefowe rozwiązanie Axis obejmuje w pierwszej kolejności dozór wizyjny strefy obwodowej (wzdłuż różnego typu ogrodzeń), zamykającej obszar chroniony, w drugiej zabezpieczenie przestrzeni peryferyjnej, w trzeciej zaś zabezpieczenie budynków i obiektów znajdujących się w strefie peryferyjnej.

Axis Perimeter Defender (ochrona obwodowa) zapewnia wykrywanie, lokalizację i identyfikację potencjalnego intruza wzdłuż ogrodzenia i przy bramach w czasie rzeczywistym. Tutaj wykorzystywane są kamery termowizyjne i wizyjne PTZ, które automatycznie przybliżają obraz i podążają za wykrytymi osobami i obiektami będącymi w ruchu. Systemy dozoru Axis zaprojektowane do tych celów pracują w trudnych warunkach oświetlenia, a nawet w całkowitej ciemności. Wbudowane inteligentne narzędzia analityczne uruchamiają ostrzeżenia i alarmują pracowników ochrony, eliminując fałszywe alarmy oraz zbędny czas i koszty rutynowych patroli. Ponadto mają możliwość generowania komunikatów audio na żywo lub odtwarzania nagranych wcześniej komunikatów, których celem jest odstraszanie intruzów.

Druga strefa systemu Axis – ochrona przestrzeni peryferyjnej – pozwala wykrywać i weryfikować wszelkie działania intruza, a także śledzić personel i pojazdy w wielu miejscach jednocześnie. Dostarcza cennych informacji o lokalizacji i prędkości przemieszczania się, a nawet o odległości między nimi i trasie ruchu.
W tej strefie brak oświetlenia czy rozległość obszaru również nie stanowią dla systemu Axis przeszkody, ponieważ wykorzystuje on kamery obrotowe z obrazem panoramicznym 360° i kamery PTZ z promiennikiem podczerwieni. W przypadku zaobserwowania niepożądanej aktywności szczególnie przydatna jest możliwość generowania komunikatów audio, istotną zaletą rozwiązania jest też zdalna obsługa systemu z dowolnego miejsca.

Trzecią strefę ochrony stanowi dozór budynków, w tym szczególnie ważna kontrola dostępu do obiektu. Umożliwia monitorowanie wejść i wyjść personelu – uprawnień dostępu do danych stref, a nawet pokojów pracowników czy urządzeń w danym budynku. Ponadto wspiera zarządzanie wizytami gości i pojazdów uprawnionych do wjazdu na chroniony teren. Rozwiązanie wspiera nowoczesny dozór budynków, pozwala przykładać mniejszą wagę do tradycyjnych fizycznych zabezpieczeń typu bramy czy drzwi, digitalizując zarządzanie dostępem w inteligentny, zaprogramowany sposób.

Należy dodać, że rozwiązanie Axis – obok zapobiegania nieautoryzowanemu dostępowi, umożliwia także monitorowanie działań personelu. Sprawny dozór nad pracą i pewność, że właściwi pracownicy są we właściwych lokalizacjach i wykonują odpowiednie czynności stanowi o bezpieczeństwie i ciągłości pracy organizacji.

Trzystrefowe rozwiązania ochrony perymetrycznej Axis odpowiadają za pełen proces dozoru w rozproszonych i dużych obiektach – poczynając od automatycznych powiadomień w czasie rzeczywistym o wykryciu incydentu, a następnie zidentyfikowaniu potencjalnego intruza, z możliwością jego odstraszenia i śledzenia. Trzeci element procesu – *following incident* – obejmuje już warstwę zarządzania zdarzeniami z poziomu centrali, umożliwiając blokowanie punktów krytycznych (bramy, wejścia, obiekty) oraz zarządzanie personelem ochrony, który musi interweniować, gdy techniczne rozwiązania dozoru wizyjnego i kontroli dostępu bez wsparcia nie będą mogły zapewnić bezpieczeństwa.

Kompleksowa, skuteczna ochrona osób i mienia w obiektach rozproszonych jest możliwa dopiero wtedy, gdy osoba zarządzająca i odpowiedzialni za bezpieczeństwo mają pełną świadomość zdarzeń, a jakość rejestrowanego obrazu pozwala na wykorzystanie go w materiałach dowodowych. □

Axis Communications Poland

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

Automatyzacja kontroli ruchu osobowo--materiałowego

Współczesne przedsiębiorstwa działają w warunkach gospodarki rynkowej i cechującej ją konkurencyjności. Chcąc odnosić coraz większe sukcesy i nieustannie się rozwijać, nie tylko nie mogą pomijać w swojej działalności aspektów bezpieczeństwa, ale wręcz muszą nadać mu szczególną rangę w katalogu potrzeb i celów.

T E K S T
Wincenty Ignatowski

Zakłady przemysłowe nie są tutaj wyjątkiem, a biorąc pod uwagę ich rozproszony charakter, dla wielu specjalistów ds. bezpieczeństwa stanowią nie lada wyzwanie, jakim jest sprawne wypełnianie różnego rodzaju zobowiązań. Przedmiotem szczególnej troski w kontekście bezpieczeństwa powinna być ochrona m.in.:

- zasobów ludzkich,
- zasobów materialnych,
- informacji,
- środowiska.

Ważnym elementem, którego nie można pomijać w trakcie projektowania systemu bezpieczeństwa zakładu przemysłowego, są jego zasoby materialne. Aby były bezpieczne, system musi chronić je przed kradzieżą, zniszczeniem lub niewłaściwym użyciem. Firmy dbające o bezpieczeństwo we wspomnianym wyżej zakresie powinny stosować określone działania kontrolne. Dobrze zaprojektowany system kontroli powinien być oparty na analizie zagrożeń mającej na celu zapewnienie hermetyczności dużego zakładu przemysłowego. Nie wchodząc w szczegółowe rozważania na temat analizy zagrożeń, każdy system kontroli powinien być tak zorganizowany, aby nie był uciążliwy dla przewoźników i pracowników logistyki, ponieważ mogliby oni odbierać proces kontroli jako przyczynę straty czasu.

Wszelkie działania na rzecz zbudowania skutecznego systemu kontroli ruchu osobowo-materiałowego powinny być poddane ocenie pod względem skuteczności, a inwestycje ponoszone na jego wprowadzenie muszą być uzasadnione i przynosić zakładane korzyści finansowe. Stąd konieczność zastosowania pełnej automatyzacji kontroli. Będzie ona wprawdzie stanowiła liczoną w tysiącach złotych jednorazową inwestycję, ale nakład zwróci się w zaledwie 18 miesięcy. Jednym z najważniejszych składowych zwrotu inwestycji będzie optymalizacja liczby roboczogodzin pracowników ochrony dokonujących kontroli towarów na bramach dużych zakładów przemysłowych.

Zastosowanie w jednym z zakładów produkcyjnych w pełni zautomatyzowanego i zintegrowanego systemu kontroli zarządzanej centralnie jest przykładem tego, że warto poszukać takich rozwiązań, które będą stanowiły niewątpliwą korzyść finansową wynikającą ze zmniejszenia obsady pracowników, a przy tym system zapewni hermetyczność zakładu przemysłowego.

październik **2020**

Dobrze zaprojektowany system kontroli ruchu materiałowego musi być skuteczny i efektywny, ale nie może być uciążliwy dla przewoźników i pracowników logistyki

Poniżej przykład automatyzacji kontroli pojazdów (bez szczegółów technicznych rozwiązań) poprzez zastosowanie zintegrowanej kontroli dostępu zarządzanej centralnie.

Wjazd do zakładu przemysłowego
Opis procesu:

1. Kierowca samochodu podjeżdża pod szlaban bramy towarowej.
2. Jeżeli system kamer LPR nie rozpoznaje tablicy rejestracyjnej w ewidencji pojazdu, kierowca wychodzi z samochodu i przechodzi do terminala, gdzie znajduje się panel do wprowadzania zamówienia.
3. Po wprowadzeniu danych ewidencyjnych na elektronicznym panelu, przeprocesowaniu procedur BHP (jeśli to konieczne, pobraniu środków ochrony osobistej) wydawana jest karta zbliżeniowa identyfikująca zamówienie oraz papierowy bilet z numerem kolejkowym i numerem stanowiska załadunkowego.
4. System automatycznie informuje kierowcę, czy ma udać się na parking kolejkowy, czy też bezpośrednio na terminal wagowy i pod załadunek surowca.
5. Kierowca wraca do samochodu i otwiera szlaban, zbliżając kartę zbliżeniową do czytnika. Szlaban otwiera się i kierowca wjeżdża na teren zakładu.

Proces załadunku surowca
Opis procesu:

1. Jeśli nie ma kolejki pojazdów oczekujących, kierowca podjeżdża bezpośrednio na terminal wagowy.
2. Kierowca opuszcza pojazd, przykłada kartę do czytnika w celu zważenia pojazdu (tara), po czym przejeżdża bezpośrednio pod wskazany na bilecie numer stanowiska załadunkowego (towar luzem lub workowany).
3. Kierowca podjeżdża pod stanowisko załadunkowe wskazane na bilecie kolejkowym, ustawia cysternę pod zasypem, korzystając z obrazu z kamery wyświetlanego na panelu załadunkowym.
4. Po ustawieniu zasypu kierowca wprowadza kartę zbliżeniową do panelu i rozpoczyna załadunek. Po zakończeniu załadunku panel zwraca kartę zbliżeniową i kierowca przejeżdża na wagę wyjazdową w celu dokonania końcowego ważenia lub udaje się na parking postojowy.

Opisany system automatyzacji kontroli towaru składa się z kilku ważnych elementów:

- System znakowania palet
- System wydawania palet (terminal wózków widłowych)
- System kontroli poprawności załadunku palet (brama)
- System kolejkowania załadunku (towar luzem)
- System kolejkowania załadunku (towar w workach)
- System obsługi BHP
- System zarządzania ruchem na parking
- System zarządzania pracą szlabanów

Szczególną rolę w obsłudze tego systemu odgrywa przeszkolony i profesjonalnie przygotowany operator zintegrowanego systemu obsługiwanego centralnie. Z powodzeniem zastępuje on kilku pracowników ochrony.

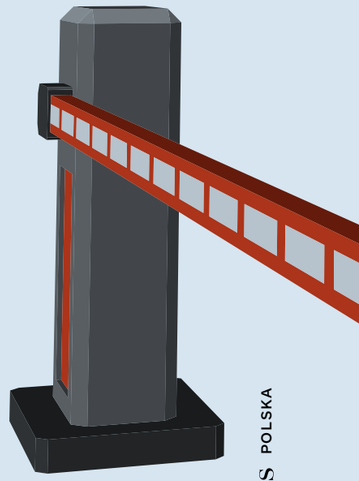
Reasumując, w naszych rozważaniach nt. bezpieczeństwa w zakładach przemysłowych skupiliśmy się na jednym z ważniejszych elementów systemu bezpieczeństwa, czyli omówieniu automatyzacji systemu kontroli osobowo-materiałowej. Automatyzacja zapewnia nie tylko korzyść finansową wynikającą ze zmniejszenia obsady pracowników, ale także hermetyczność zakładu przemysłowego.

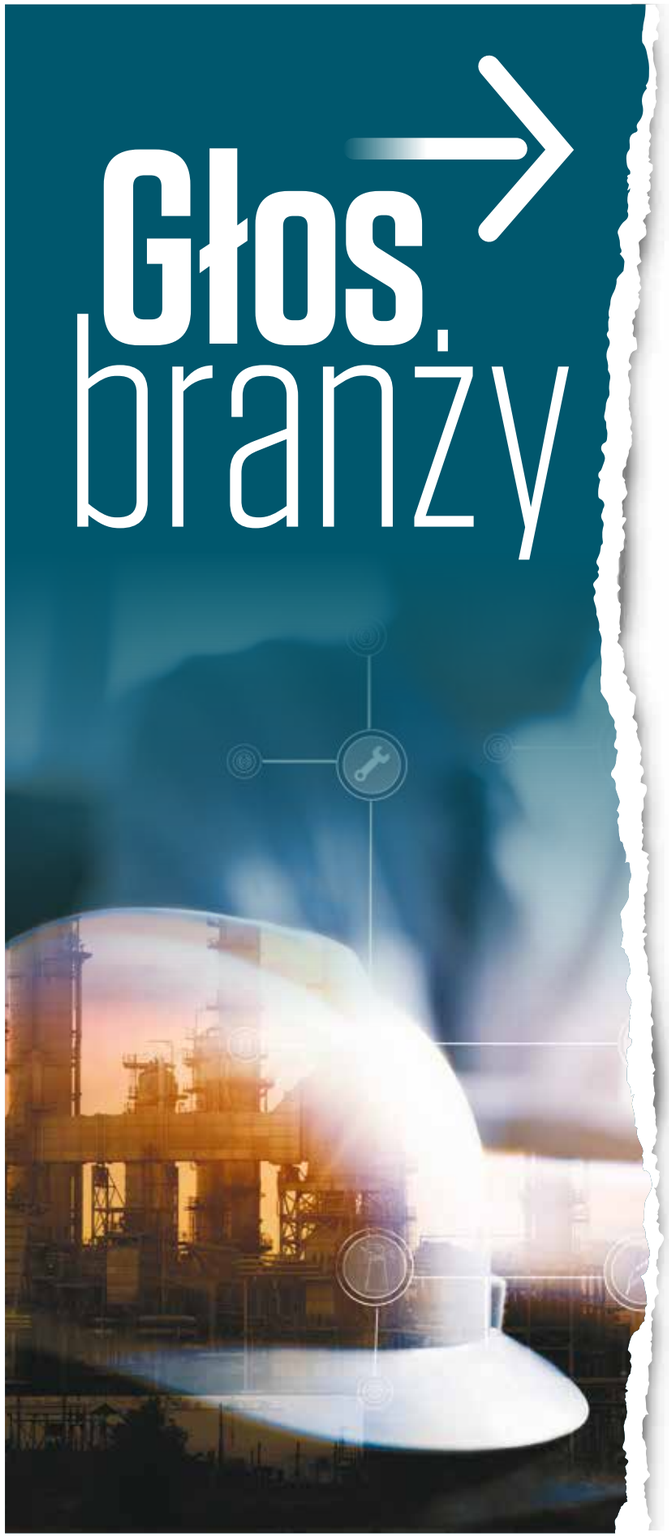
Nie sposób też nie wspomnieć o sytuacji wywołanej koronawirusem. Naruszona została równowaga ekonomiczna wielu gospodarek, a funkcjonowanie z COVID-19 w tle stało się dla wielu firm wyzwaniem. Zwłaszcza funkcjonowanie dużych zakładów przemysłowych jest cały czas niezwykle trudne. Można np. wyobrazić sobie prowadzenie działalności handlowej przez firmy internetowe czy też zachowanie aktywności przez wiele biur i instytucji, w których pracownicy z powodzeniem mogą pracować zdalnie, natomiast nie jest możliwe zdalne wyprodukowanie większości towarów. Zapewnienie bezpieczeństwa ludziom i ochrona mienia w zakładach produkcyjnych jest w okresie pandemii kwestią priorytetową, dlatego m.in. automatyzacja działań kontrolnych jest tutaj nie do przecenienia. Troska o bezpieczeństwo pracowników stała się żywotnym problemem każdego biznesu. □

B I O

Wincenty Ignatowski

Absolwent UW (Wydział Socjologii) oraz studiów podyplomowych z zakresu Bezpieczeństwa Biznesu w Wyższej Szkole Finansów i Zarządzania w Warszawie. Od 2001 r. menedżer ds. bezpieczeństwa w międzynarodowych korporacjach z branży logistycznej, handlowych, usługowych i produkcyjnych w Polsce i Europie. Specjalizuje się w polityce zapobiegania stratom *(Loss Prevention Policy)*, *Corporate Security,* bezpieczeństwie procesów operacyjnych oraz kwestiach związanych z polityką ***compliance***.





JAK BRANŻA SECURITY MOŻE POMÓC W ZAPEWNIENIU BEZPIECZEŃSTWA OBIEKTÓW PRZEMYSŁOWYCH, ZWŁASZCZA W DOBIE PANDEMII? GŁOS ZABIERAJĄ PRZEDSTAWICIELE RÓŻNYCH SEKTORÓW GOSPODARKI.

Artur Pollak

APA Group

Kluczowe aspekty bezpieczeństwa

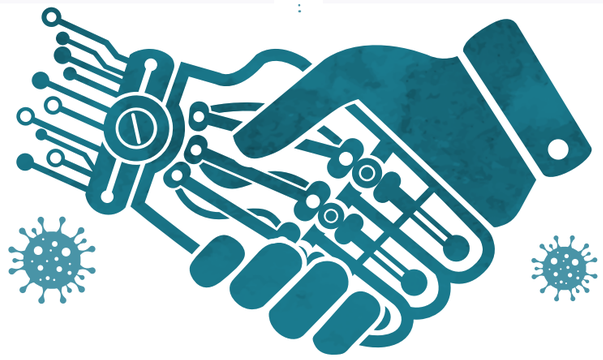
Można wyróżnić dwa kluczowe aspekty bezpieczeństwa związane z technologią, na które należy patrzeć całościowo, gdyż jeden jest zależny od drugiego. Pierwszym jest technologia, która rozwija się w ekspresowym tempie. Jesteśmy w stanie pozyskiwać bardzo dużo danych z różnych infrastruktur przemysłowych. Przez świat przetacza się potężna fala przemysłowego Internetu Rzeczy (IIoT). Postęp następuje, można śmiało przyznać, geometrycznie. Skutkuje to sytuacją, w której wcześniej pilnie strzeżone dane są narażone na nowe zagrożenia i znacznie trudniej je chronić.

Najsłabszym ogniwem w tym procesie okazuje się człowiek. To ludzie, którzy nawet nie starają się zrozumieć nowych procesów i zależności na płaszczyźnie człowiek-maszyna, powodują wyrwy w systemach bezpieczeństwa. Kluczowe zatem we wdrażaniu nowych technologii w zakładach przemysłowych staje się precyzyjne planowanie i projektowanie procesów w najdrobniejszych szczegółach. A można to osiągnąć jedynie za pomocą obserwacji z zewnątrz i drobiazgowej analizy danych. Wyciągnięte wnioski uprawniają do przedstawienia bezpiecznego dla człowieka oraz przedsiębiorstwa modelu funkcjonowania.

Drugim aspektem bezpieczeństwa, uwypuklonym przez trwającą pandemię, stała się mobilność użytkowników cyfrowych zasobów przedsiębiorstwa. Dzisiaj już wiemy, że nawet osoby zatrudnione w największych światowych organizacjach potrafią skutecznie pracować w trybie zdalnym. Ludzie jednak mają to do siebie, że posiadają ograniczoną zdolność do zapamiętywania haseł, lekceważą potrzebę ich okresowej zmiany i dbania o podstawowe procedury cyberbezpieczeństwa. Przechodząc na telepracę, nie do końca rozumieją, że te hasła chronią nie tylko dostęp do laptopa i umieszczonych w nim informacji, ale także zabezpieczają znacznie szerzej – przede wszystkim przechowywane w chmurze dane całej organizacji.

Następuje wypaczenie systemów bezpieczeństwa. Jak wtedy, gdy okazało się, że na środku pustyni można było zlokalizować i dokładnie określić kształt baz wojskowych dzięki nieodpowiednio użytkowanym i zabezpieczonym smartwatchom żołnierzy znajdujących się przy ogrodzeniach.

Świat pędzi w kierunku automatyzacji i uproszczeń. To jednak nie służy jakościowej ochronie danych. Sytuacje wyjątkowe, jak ta pandemiczna obecnie, z jednej strony umożliwiają niesamowity rozwój technologiczny, bo tworzymy rozwiązania, na które wcześniej nie było czasu lub środków. Z drugiej zaś otwierają luki w systemach bezpieczeństwa. Moją rekomendacją jest planowanie i wdrażanie rozwiązań Przemysłu 4.0. To on na bazie posiadanych zbiorów danych *(Big Data)* pozwala na robienie pilotaży i precyzyjną predykcję zagrożeń na każdym już dzisiaj wycinku zakładu przemysłowego. A współczesne platformy technologiczne działające wg założeń Przemysłu 4.0 mają już zaszyte skuteczne systemy cyberbezpieczeństwa.



Dagmara Pomirska

Axis Communications

Systemy wizyjne wsparciem dla przemysłu

W ostatnim czasie branża przemysłowa ma do czynienia z jeszcze trudniejszymi wyzwaniami niż zwykle. Za sprawą pandemii zakłady przemysłowe muszą bowiem radzić sobie z produkcją w obliczu pracy zdalnej, jednocześnie dbając o bezpieczeństwo zakładu i pracowników.

Tak jak w przypadku ochrony samych przestrzeni przemysłowych, również w kontekście ochrony pracowników z pomocą przychodzą systemy wizyjne. Mogą one wspierać przedsiębiorców w dostosowywaniu się do nowych przepisów sanitarnych.

Przykładowo, inteligentne kamery połączone z odpowiednim oprogramowaniem mogą natychmiast zweryfikować, czy osoba przebywająca na terenie zakładu nosi odpowiednie środki ochronne, np. maseczkę. Zautomatyzowane systemy pozwalają także na wydzielanie specjalnych stref lub linii, po których przekroczeniu przez pracownika zostaje wygenerowany automatycznie komunikat audio przez głośnik. Może to być przydatne narzędzie do egzekwowania zachowywania odpowiednich odległości pomiędzy pracownikami, a także sposób przypominania im o zasadach bezpieczeństwa, np. o konieczności korzystania ze środków do dezynfekcji dłoni. Nietrudno sobie wyobrazić, jak karkołomnym zadaniem byłaby próba kontroli w sposób niezautomatyzowany.

Monitoring może wspierać przedsiębiorców nie tylko w kontekście przestrzegania obecnie obowiązujących zasad sanitarnych, ale także w bezproblemowej kontynuacji procesów produkcyjnych. Ich monitorowanie pozwala bowiem zdalnie rozwiązywać problemy i pomagać pracownikom w zakresie konserwacji i właściwego zarządzania sprzętem. To szczególnie ważne dzisiaj, kiedy tak wielu z nich zostało poniekąd zmuszonych przez panującą sytuację do pracy z domu.

Dzięki aplikacjom wizyjnym można zweryfikować występujące podczas produkcji problemy z oznakowaniem produktu, ciśnieniem, przepływami, temperaturą czy wyciekami i podjąć działania, zanim powstaną straty. Taki monitoring pozwala na zdalną obserwację temperatury krytycznej. Nowoczesne systemy wizyjne umożliwiają utworzenie stref alarmowych, z których zostanie wysłane powiadomienie, gdy temperatura osiągnie poziom wyższy lub niższy od określonych wcześniej progów.

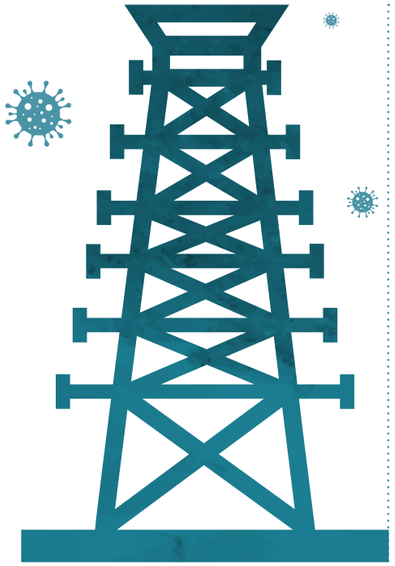
Podsumowując, dzięki połączeniu technologii kamer IP z detektorami ruchu, technologią radarową oraz odpowiednią analityką, możliwe jest zabezpieczenie całej infrastruktury zakładu przemysłowego na miarę Przemysłu 4.0.

Przemysław Bańko

Omniconnect

System na miarę

Planując wdrożenie systemu ochrony rozproszonych obiektów przemysłowych, należy przede wszystkim wziąć pod uwagę ryzyka wystąpienia naruszeń bądź incydentów związanych



nie tylko z atakami cybernetycznymi – co modne – ale także fizycznymi atakami na obiekty. Zabezpieczenie, w mojej ocenie, ma służyć wsparciu organizacji w utrzymaniu ciągłości działania. Obserwując różne formy zabezpieczania, mam wrażenie, że zbyt często są one „odrealnione", oderwane od miejsca i możliwych zagrożeń. Bardzo często też trudno określić, jaki cel przyświecał wyborowi konkretnego rozwiązania. Problemem jest również oderwanie zabezpieczeń technicznych od procedur funkcjonujących w obiektach, strefach czy systemach. Wdrażając zabezpieczenia, powinniśmy wypracować pewien prosty schemat działania, który skrótowo można opisać następującą sekwencją zdarzeń:

– określenie kontekstu dla organizacji i biznesu; na tym etapie poznajemy wymagania prawne, regulacje, otoczenie, zagrożenia naturalne, dostęp do dostawców i odbiorców etc.
– określenie kluczowych procesów w organizacji,
– zinwentaryzowanie zasobów i aktywów realizujących dane procesy,
– zarządzanie ryzykiem, a więc identyfikacja zagrożeń – określenie prawdopodobieństwa ich wystąpienia i ewentualnego wpływu na zidentyfikowane procesy,
– wybór środków zabezpieczeń redukujących zdiagnozowane ryzyka.

Dopiero wykonanie w prawidłowej kolejności prac planistycznych pozwoli nam na „uszycie" systemu bezpieczeństwa na miarę. Poznamy prawdziwe zagrożenia, zweryfikujemy koszty ich implementacji i będziemy w stanie określić budżet na wdrożenie zabezpieczeń, odpowiedni dla przeciwdziałania ewentualnym stratom wynikającym z braku zabezpieczeń. I jeszcze jedno, o czym nie wolno zapomnieć – każde, nawet najlepsze rozwiązanie techniczne będzie niewystarczające, jeśli nie uwzględnimy procedur organizacyjnych oraz szkoleń dla uprawnionego personelu i pracowników.

Norbert Bartkowiak

Ela-compil

Jak zapewnić bezpieczeństwo

Systemy zabezpieczenia technicznego stosowane w przemyśle zwykle nie różnią się od systemów instalowanych w innych obiektach. Bywa, że ze względu na trudne warunki panujące np. w halach przemysłowych, jak choćby atmosfera grożąca wybuchem, wyższe wymagania stawia się prowadzonym instalacjom oraz zastosowanym czujkom, czytnikom KD czy kamerom. Tym, co jednak zasadniczo różni instalacje przemysłowe od pozostałych, nazwijmy je „cywilnymi", jest cel ich stosowania – nie tylko ochrona mienia, ale także zapewnienie ciągłości procesów produkcyjnych. Istnieje wiele zagrożeń mogących ją zakłócić. Zatem to, czego przede wszystkim oczekuje się od zastosowanych systemów technicznej ochrony mienia, można określić maksymą Hipokratesa *primum non nocere* – po pierwsze nie szkodzić.

W każdym przypadku fałszywe alarmy są dokuczliwe, jednak w przemyśle mogą generować poważne konsekwencje. Nietrudno sobie wyobrazić, jakie skutki może wywołać system sygnalizacji pożarowej, który automatycznie wykona scenariusz polegający na automatycznym zatrzymaniu procesu produkcyjnego. Przekonał się o tym jeden z producentów samochodów, kiedy wskutek alarmu pożarowego została zatrzymana linia robotów lakierniczych. Systemy technicznej ochrony mienia często również wspierają procesy zapewniające utrzymanie odpowiedniego poziomu bezpieczeństwa i jakości wytwarzanych produktów. Systemy kontroli dostępu stosuje się np. do wymuszenia odpowiednich „ścieżek technologicznych" w zakładach produkujących leki czy żywność. Obowiązuje tam taka zasada komunikacji, aby osoby mające kontakt z produktami przeszły do swojego stanowiska strefą „czystą", a dopiero po zakończeniu pracy opuściły miejsce pracy przez strefę „brudną". W tych procesach, gdzie może dojść np. do uszkodzenia opakowania szklanego i co za tym idzie dostania się odłamków szkła do żywności, wykorzystuje się systemy telewizji dozorowej.

Pełną efektywność uzyskuje się wtedy, gdy poszczególne systemy są zintegrowane w jeden system, który pozyskuje dane również z systemów wykorzystywanych w automatyzacji produkcji, np. systemy odpowiedzialne za etykietowanie, liczenie czy transport produktów. Jednym z przykładów jest integracja systemu telewizji dozorowej i kontroli dostępu z systemem ważenia pojazdów dostarczających surowce i/lub wywożących gotowe produkty. Takie rozwiązanie ma na celu uszczelnienie systemu dostaw, który w przypadku dużych zakładów jest często narażony na różnego rodzaju nadużycia.

Najważniejszy w procesie budowania bezpieczeństwa jest dobrze wykonany projekt, oparty na prawidłowym doborze urządzeń, a później zbudowana na jego podstawie instalacja systemu zabezpieczeń, która daje wymierne korzyści – począwszy od zapewnienia bezpieczeństwa pracownikom po możliwość uzyskania odpowiednich zniżek w ubezpieczeniu majątkowym dzięki skuteczniejszej eksploatacji instalacji. Integracja systemów bezpieczeństwa w zaawansowanym PSIM *(Physical Security Information Management)* zapewnia sprawne funkcjonowanie i zachowanie ciągłości produkcji, umożliwiając w ten sposób poprawne funkcjonowanie obiektu.

Obecnie nie można już bezpiecznie zarządzać bezpieczeństwem bez rzetelnej analizy danych zebranych przez poszczególne systemy i aplikacje bezpieczeństwa. Przetwarzanie danych, ich analiza i wyciągnięte wnioski pomogą zbudować procedury, których przestrzeganie zapewni bezpieczeństwo w obiektach. Posiadanie systemu integrującego, takiego jak GEMOS, łączy te wszystkie systemy, umożliwiając agregowanie tych informacji w centralnym miejscu. Nie bez znaczenia jest także możliwość zdalnego zarządzania obiektem z jednej platformy opartej na przeglądarce internetowej.

Zbigniew Morawski

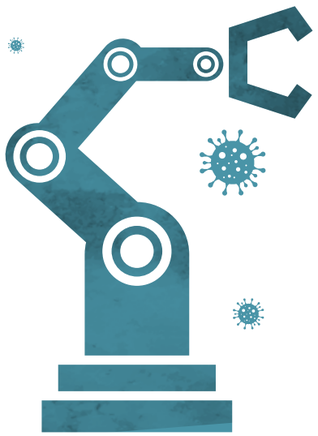
Hikvision Poland

Wyzwania w przemyśle

Obiekty przemysłowe ze względu na ich specyfikę można podzielić na dwie grupy: zakłady scentralizowane, które często mają dużą powierzchnię, oraz zakłady o rozproszonej infrastrukturze o budowie liniowej. Przykładem tych drugich są np. gazociągi pracujące z wykorzystaniem linii przesyłowych. Każdy z tych typów przedsiębiorstw wymaga innego podejścia do bezpieczeństwa.

W zależności od charakterystyki produkcji koncepcję zabezpieczenia powinno się przygotowywać na dwóch płaszczyznach. Po pierwsze trzeba zadbać o ochronę terenu, zarówno przed wtargnięciem intruza, jak i przed zdarzeniami związanymi np. z uszkodzeniem mienia przez maszyny pracujące wewnątrz. Takie incydenty powinni wychwytywać operatorzy.

Drugim ważnym zadaniem jest zapewnienie bezpiecznej pracy załodze. W kontekście pandemii COVID-19 mówimy tu o skanowaniu przesiewowym pracowników wchodzących na teren zakładu oraz zapewnieniu odpowiedniego dystansu społecznego. W wyjątkowo trudnej sytuacji znalazły się zakłady strategiczne, które w czasie lockdownu nie mogły pozwolić sobie na model pracy zdalnej. W szybkim wykryciu osób potencjalnie chorych pomocne są urządzenia do zdalnego mierzenia temperatury ciała, gdyż gorączka jest jednym w objawów zakażenia wirusem SARS-CoV-2. Urządzeniami, które znakomicie sprawdzą się w tej roli, są kamery termowizyjne. Operatorzy mogą też wykorzystać te rozwiązania do zdalnego pomiaru stanu urządzeń, bez konieczności fizycznego kontaktu z nimi.



Wyzwaniem zarówno dla zakładów scentralizowanych, jak i przedsiębiorstw rozproszonych jest też zabezpieczenie przeciwpożarowe np. różnego rodzaju placów składowych czy liniowych systemów przesyłowych, w tym np. paliw. Dla tych zakładów z punktu widzenia procesu przemysłowego ważne jest uniknięcie awarii. Wczesne wykrycie wzrostu temperatury newralgicznych elementów przesyłowych czy produkcyjnych i odpowiednio szybka reakcja może zapobiec pożarowi, zatrzymaniu produkcji i stratom finansowym. I w tym przypadku do monitorowania temperatury można zastosować kamery termowizyjne.

Jeśli mowa o wyzwaniach dla obiektów rozproszonych, tu najistotniejsze jest zapewnienie ciągłego dozoru wizyjnego przez operatorów. Często te obiekty są rozlokowane na dużym obszarze, znajdują się na obszarach niezamieszkanych, bez oświetlenia i z utrudnionym dostępem, a jedynym zabezpieczeniem jest ogrodzenie zewnętrzne. Rozwiązaniem dla security menedżerów jest zastosowanie takich technologii, które umożliwią precyzyjny ogląd sytuacji (wyraźny obraz obserwowanego obszaru) nawet w ciemności panującej w nocy lub w czasie opadów atmosferycznych.

Chodzi tu głównie o technologię termowizyjną, ale też o systemy wizyjne zintegrowane z urządzeniami innych systemów zabezpieczeń, np. czujkami zewnętrznymi opartymi na technologii mikrofalowej czy radarowej, czy też z czujkami pojemnościowymi montowanymi na ogrodzeniu, które zapewnią niezawodną detekcję intruza. W takim systemie kamery dozorowe mogą zostać wysterowane przez sygnały ze zintegrowanych z nimi czujek. Gdy chcemy mieć dobrej jakości obraz weryfikujący szybko detekcję intruza w każdych warunkach środowiskowych czy atmosferycznych, najlepsze efekty da połączenie kamer termowizyjnych z kamerami światła widzialnego.

Piotr Kiliszek

Niezależny ekspert

Zdalny monitoring wizyjny

W obliczu pandemii COVID-19 ujawniły się nowe wyzwania związane z zapewnieniem bezpieczeństwa. Jednym z nich jest wymuszenie ochrony w warunkach wystąpienia zakażeń o charakterze masowym. W moim przekonaniu to znakomity pretekst, a zarazem impuls do rozbudowy systemu monitoringu zdalnego, realizowanego przez wyspecjalizowane w tym zakresie firmy. Wypracowany potencjał powinien uwzględniać procedury zachowania ciągłości działania i, podobnie jak to jest w rozwiązaniach wojskowych, powinny być też wskazane miejsca alternatywne w przypadku zakażeń w punktach podstawowych.

Oczywiście z punktu widzenia biznesu koszt, jaki należałoby ponieść, może być większy, ale rozwiązanie to jest skuteczne i zapewnia ciągłość ochrony obiektów. W przypadku obiektów wpisanych na listę wojewody zarządca ma obowiązek chronienia i nie ma tam mowy o włączeniach warunkowych. Jest natomiast mowa o sankcjach karnych w przypadku niezapewnienia takowej ochrony.

Mimo wyższych kosztów outsourcingu usług monitoringu to jednak przedsiębiorca może zyskać na jakości pracy służb ochrony fizycznej, dostępie do najnowszych technologii, w tym związanych z analizą obrazu. Wirtualny obchód mógłby być przyczynkiem do optymalizacji planów ochrony fizycznej, a co za tym idzie racjonalności ponoszonych kosztów. Rozwiązania takie powinny być szczególnie interesujące dla dużych grup kapitałowych, posiadających wiele zakładów w różnych lokalizacjach. Centra monitoringu byłyby odpowiednikiem branżowych SOC *(Security Operations Center)*, jakie są tworzone na potrzeby wdrażania KSC

Krajowy System Cyberbezpieczeństwa). Mogłyby być zlokalizowane w miejscach, gdzie jest dostęp do wykwalifikowanego personelu dającego rękojmię zachowania poufności. A wprowadzenie odpowiednich standardów przechowywania danych zabezpieczyłoby zarejestrowane obrazy przed dostępem osób niepowołanych albo ich upublicznieniem.
Wzajemna współpraca specjalistów mających holistyczne podejście do problemu ochrony mogłaby wyznaczyć nowe standardy ochrony.

Jakub Sobek

Linc Polska

Mądre czujniki

Gospodarka zmienia się ustawicznie i coraz częściej obiekty przemysłowe funkcjonują jako centra danych, serwerownie lub punkty obsługi klienta. Jak istotne jest bezpieczeństwo takich miejsc i ciągłość ich działania, pokazują sytuacje, w których nagle jesteśmy zmuszeni do przejścia na pracę zdalną.
Wszystkie analizy gospodarcze pokazują, że do kluczowych obiektów przemysłowych w przyszłości nie będą wcale należały fabryki, a właśnie centra danych lub miejsca alokacji chmury obliczeniowej. Gdy tylko dojdzie do wstrzymania funkcjonowania takich obiektów oraz wdrożonych w nich rozwiązań sztucznej inteligencji (AI) zauważymy, jak wiele obszarów jest już przez te produkty wspieranych. Skala ta oczywiście będzie systematycznie rosnąć, a ten obszar gospodarki będzie zyskiwać na znaczeniu.
Przestoje w pracy takich miejsc są kosztowne, a gdyby dodatkowo doszło do utraty danych, to konsekwencje mogą być bardzo poważne. Dlatego bezdyskusyjnie bardzo istotne jest zabezpieczenie techniczne takiego obiektu. Wszystkie elementy infrastruktury, takie jak serwery, urządzenia sieciowe, zasilacze itp. są podatne na usterki i przegrzewanie, co w efekcie może zainicjować pożar. Obecnie istnieją już możliwości detekcji takich „punktów zapalnych" jeszcze na ich wczesnym etapie - z pomocą przychodzą radiometryczne kamery termowizyjne. Pozwalają one na obserwację np. wybranego obszaru serwerowni i stałe monitorowanie zmian temperatury urządzeń i elementów. Jeśli w jakimś systemie zidentyfikują stały trend wzrostu temperatury, to wygenerują alarm. Taka koncepcja ma na celu nie tylko poprawę bezpieczeństwa całej infrastruktury, lecz także pracowników znajdujących się w obiekcie.
Alternatywą dla kamer termowizyjnych są mniejsze i tańsze czujniki oparte właśnie na przetwornikach termowizyjnych. Pozwalają nie tylko skutecznie monitorować temperaturę w wybranych obszarach pomieszczenia, ale także mogą dostarczać dodatkowe informacje o próbie sabotażu, obecności dwutlenku węgla, jakości lub wilgotności powietrza. Ponadto czujniki można wykorzystać do sprawdzenia liczby osób w pomieszczeniu. To bardzo przydatna funkcja np. w momencie, kiedy dojdzie do zadymienia pomieszczenia i konieczna jest szybka ewakuacja.

Paweł Pirański

ArcelorMittal

Ograniczenie rozprzestrzeniania się pandemii

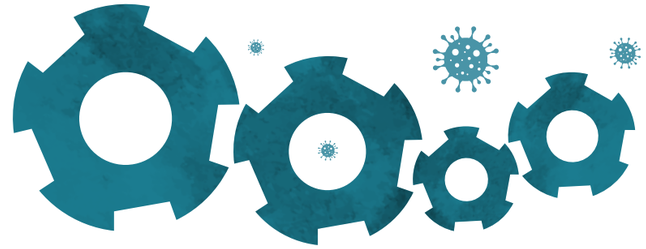
Rok 2020, od początku naznaczony pandemią COVID-19, jest wyjątkowy pod względem ilości wyzwań stojących przed pionami bezpieczeństwa wszystkich gałęzi gospodarki, w tym przemysłu. Realizując swoje kluczowe zadania związane z zapewnieniem bezpieczeństwa fizycznego pracowników i obiektów oraz kontynuacją procesów przed „tradycyjnymi" zagrożeniami, zostaliśmy postawieni w sytuacji nieznanej i absolutne zaskakującej. Istniejąca i użytkowana dotąd infrastruktura wspierająca zdania służb security okazała się dalece niewystarczająca, jeśli chodzi o funkcjonowanie firm w obecnej, pandemicznej rzeczywistości.
Wplecenie i wykorzystanie istniejących systemów CCTV, alarmowych czy KD w procedury ochronne i zapobiegawcze związane z COVID-19 okazało się jednym z elementów zarządzania bezpieczeństwem, w tym epidemicznym, chronionych jednostek. Sprawne i uważne (pomimo pilności) inwestowanie w dotąd niestosowane rozwiązania np. kontroli stanu zdrowia (pomiar temperatury) pracowników i klientów, które głównie obsługują przecież służby security, mogą być w przyszłości wykorzystane jako elementy uzupełniające i wzbogacające klasyczne instrumenty służące poprawie czy zapewnieniu bezpieczeństwa; a w przypadku zaistnienia takiej potrzeby użyte niejako z marszu, gdyby sytuacja (miejmy nadzieję, że nie) się powtórzyła.
Działania te z oczywistych względów muszą być realizowane w porozumieniu z innymi pionami firmy: IT, BHP, administracją, produkcją (operacją), natomiast koordynowane powinny być w sposób naturalny na szczeblu zarządu/dyrekcji wykonawczej w formie sztabu kryzysowego/zarządzającego.
Ze względu na zaangażowanie dużej części personelu security do działań, które w normalnym czasie nie stanowią jego podstawowej działalności, potrzebne jest właściwe utrzymanie systemów wspomagających pracę ochrony. W obiektach przemysłowych (szczególnie o dużej powierzchni i rozproszonych) warunkiem koniecznym do prowadzenia skutecznego procesu ochronnego, przy szczupłych zasobach ludzkich, staje się zapewnienie wysokiej sprawności i niezawodności wszystkich dostępnych narzędzi i systemów wspomagających.

Krzysztof Pohorecki

Ekspert Business Resilience

Potrzeba dostosowania się do sytuacji

„Rok 2020 głęboko zmienił branżę i podejście do bezpieczeństwa" – często spotykam się z takimi opiniami. Nie jestem do końca przekonany o ich trafności. Oczywiście sytuacja pandemiczna wymusiła podjęcie mniej lub bardziej skoordynowanych czy racjonalnych działań, ale bardzo często miały one i nadal mają cechy doraźne. Przypominają starą metodę „zróbmy coś" albo lepiej „zróbcie coś", ewentualnie „niech oni coś zrobią".
Pojawiło się sporo „nowych" propozycji na bazie modyfikacji już istniejących oraz znacznie mniej rzeczywistych innowacji. Nadal w mojej ocenie nie obserwujemy zmian fundamentalnych ani po stronie szeroko rozumianej branży bezpieczeństwa, ani po stronie odbiorców jej usług i produktów.
Zdecydowane wyhamowanie gospodarcze spowodowało konieczność szukania oszczędności budżetowych i nie ominęły one sfery bezpieczeństwa. W wielu przypadkach projekty planowane zostały odłożone „na lepsze czasy". Nowa sytuacja spowodowana pandemią i zmianami regulacyjnymi przez nią wywołanymi zmusza praktycznie wszystkie branże do podjęcia kroków dostosowawczych, ale z moich obserwacji wynika, że mają one najczęściej charakter powierzchowny i nie wykraczają poza *basic compliance*.
Trudno prorokować rozwój sytuacji (ten rok pokazał to nad wyraz boleśnie). Gdybym jednak chciał pokusić się o jakąś projekcję przyszłości branży i rynku jej odbiorców w „covidowym i „postcovidowym" świecie, to nie spodziewam się głębokich czy fundamentalnych zmian w podejściu do bezpieczeństwa oraz jego znaczenia i roli w biznesie. Spodziewam się raczej nieco szybszej ewolucji przez krótki okres, a następnie powrotu do „normy". Rewolucji moim zdaniem nie będzie. I dobrze.



Janusz Syrówka

innogy Polska

Najważniejsze jest planowanie

W roku 2020 bezpieczeństwo obiektów przemysłowych nie może być postrzegane inaczej niż z perspektywy pandemii. Skala problemów, jaka pojawiła się wraz z koronawirusem, mogła zaskoczyć nawet największego pesymistę, a pojęcie „czarny łabędź" nabrało nowego znaczenia – i to nie jako abstrakcyjny termin, ale realny stan.
Na początku pandemii spotkałem się nawet z głosami, że „całe to zarządzanie kryzysowe i zapewnianie ciągłości działania jest nic niewarte. Na pierwszy rzut oka racja – kto bowiem miał plan na zamknięcie „wszystkiego"? Jednak bardzo szybko okazało się, że to stary „Ike" Eisenhower miał rację, mówiąc, że „plany są niczym, a planowanie wszystkim". Firma posiadająca zaszytą w swojej kulturze organizacyjnej politykę zapewnienia ciągłości działania nie miała większych problemów z adaptacją swoich planów do nowej sytuacji – nawet tak nieprzewidywalnych. Przez zaszycie w kulturze organizacyjnej rozumiem ciągły proces doskonalenia, aktualizacji i testowania. Coś zupełnie przeciwnego od zrywów, ambitnych pomysłów bez realizacji czy też nicnierobienia, bo może się uda.
Poza wagą zarządzania kryzysowego i utrzymania ciągłości działania pandemia dokonała dużego przewrotu, który trochę zniknął przykryty wiadomościami o liczbie zainfekowanych i kwarantannach. Mam na myśli niesamowite przyspieszenie w zakresie rozwiązań mobilnych i cyfrowych. Nie chodzi tu tylko o pracę zdalną i platformy do telekonferencji. Sytuacja wymusiła także zmiany w procesach biznesowych, które bez pandemii czekałyby jeszcze na wdrożenie przez jakiś czas. Prawdziwym wyzwaniem nadchodzącej przyszłości będzie właściwa ocena skutków tej zmiany i właściwe potraktowanie wszystkiego, co ze sobą niesie – ponieważ oprócz rzeczy wspaniałych przynosi także nowe zagrożenia...

Jacek Tobiasz

Grupa Eurocash

Ważne są kompetencje

Czas pandemii pokazał, że plany ciągłości biznesowej (BCP) budowane w wielu organizacjach i zakładające wiele różnych scenariuszy kryzysowych bardzo często nie przewidywały skali globalnego kryzysu, który przywędrował także do nas na początku tego roku. Początkowo wydawał się nierealny, nieprawdopodobny, gdzieś tam, daleko...
Oczywiście wyłączenie dostępności części zasobów ludzkich czy też poszczególnych obiektów jest typowym elementem BCP. Życie pokazało jednak, że tego, co może się wydarzyć, nie da się do końca przewidzieć. Owszem, niektóre elementy można, ale prawdopodobieństwo wydaje się tak nikłe, że nie bierzemy tego pod uwagę. Budowa scenariuszy i zapewnienie niezbędnej infrastruktury dla każdego możliwego rozwiązania doprowadzi

do absurdu i ogromnych nakładów pracy oraz nieakceptowalnie wysokich kosztów. Co zatem zrobić ? Jak organizować działalność, by w zderzeniu z takimi wyzwaniami i nieznanymi wcześniej problemami nie przegrać? W mojej ocenie kluczem i rozwiązaniem są właściwie przygotowani ludzie. Mam na myśli pracowników, którzy są kompetentni i gotowi szybko reagować na zmiany, potrafią poszukiwać nowych rozwiązań, nie działają schematycznie, ale są gotowi na podjęcie ryzyka związanego z kreatywnym i nowatorskim podejściem do problemu. W konsekwencji potrafią omijać pojawiające się przeszkody, zamiast zderzać się z nimi.

Zatem jak zapewnić bezpieczeństwo dużych lub rozproszonych obiektów przemysłowych? Jak sprawnie wspierać biznes, zapewniając bezpieczne środowisko do jego funkcjonowania? W mojej ocenie wymaga to nowych, inteligentnych, odważnych i kreatywnych rozwiązań. Skoro prawie wszystkie nowe urządzenia systemów działają dziś cyfrowo, to możemy sami kreować całkowicie nowe możliwości ich wykorzystania. Integrując je ze sobą, możemy otrzymać wartość dodaną i nową jakość, większe możliwości detekcji problemu i szybszej reakcji. Wydawać się może, że takie podejście generuje wysokie dodatkowe koszty. Pozornie tak, ale z moich doświadczeń wiem, że można zbudować efektywny model działania, który w dość krótkim czasie przynosi zwrot nakładów i generuje oszczędności w kosztach stałych na przyszłość.

Marcin Walczuk

BCS

Korzyści technologii IP

Wielkie obiekty przemysłowe wymagają szczególnej ochrony. Zwłaszcza gdy w procesie produkcyjnym wykorzystuje się niebezpieczne materiały, które w razie ataku terrorystycznego lub nieumyślnego działania człowieka mogą stanowić poważne zagrożenia zdrowia i życia ludzi.

Skuteczne zabezpieczenie tego typu obiektów stanowi nie lada wyzwanie dla projektantów. Podstawowym problemem jest wielkość takich przedsiębiorstw, które dodatkowo mogą składać się z wielu mniejszych zakładów rozsianych nawet na obszarze całego kraju. Niejednokrotnie klient chciałby scentralizować system bezpieczeństwa, aby móc nim zarządzać z jednego miejsca.

Wykorzystanie systemów telewizji dozorowej opartych na technologii IP pozwala w łatwy sposób przesłać strumień wideo w dowolne miejsce na Ziemi, dzięki czemu tworzenie centrów monitoringu wizyjnego nie stanowi już większego problemu. W tym celu konieczne będzie zapewnienia odpowiednio wydajnego łącza internetowego oraz aplikacji, która umożliwi zarządzanie wieloma obiektami równocześnie.

Aby wyjść naprzeciw tym wymaganiom, BCS proponuje swoje autorskie rozwiązanie w postaci aplikacji BCS Manager. Pozwala ona na podłączenie i podgląd teoretycznie nieograniczonej liczby kanałów na nieograniczonej liczbie monitorów. W praktyce będzie ona oczywiście ograniczona możliwościami stacji roboczej, na której aplikacja zostanie zainstalowana. Główną zaletą naszego rozwiązania jest obsługa nie tylko produktów BCS, ale również innych wiodących producentów systemów telewizji dozorowej oraz wsparcie dla protokołu Onvif, co oznacza możliwość podłączenia każdego urządzenia CCTV, które taki protokół obsługuje.

Oczywiście aplikacja nie zastąpi urządzeń, które pracują na pierwszej linii i zabezpieczają sam obiekt. Dlatego też i w tym wypadku najlepiej sprawdzą się rozwiązania IP CCTV. Zapewniają one możliwość pracy w wyższych rozdzielczościach oraz dostęp do zaawansowanych funkcji analizy obrazu wideo. Dzięki tym cechom i ich umiejętnemu wykorzystaniu można bardziej precyzyjnie zabezpieczyć teren i wywoływać alarmy tylko ze zdarzeń, które mogą być potencjalnie niebezpieczne, redukując do minimum liczbę fałszywych alarmów.

Jacek Figarski

Schrack Seconet

Bezpieczeństwo pożarowe obiektów przemysłowych

Infrastruktura obiektów przemysłowych charakteryzuje się dużą złożonością i zróżnicowaniem występujących zagrożeń, co w praktyce oznacza, że inwestor i projektant często muszą indywidualnie podchodzić do doboru zabezpieczeń ppoż., aby zapewnić optymalne dla danego obiektu rozwiązania. Duże obiekty przemysłowe zazwyczaj mają budynki rozproszone na swoim terenie lub są zlokalizowane w kilku miejscach na terenie Polski, stanowiąc spójną infrastrukturę danego biznesu. Wszystko to ma wpływ na podjęcie decyzji o zastosowaniu certyfikowanego zintegrowanego systemu zarządzania bezpieczeństwem pożarowym.

Inwestor, chcąc wnikliwie przeanalizować ochronę ppoż. swoich obiektów w celu wyboru najlepszego rozwiązania, konsultuje z projektantami i dostawcami/producentami urządzeń ppoż. i systemów bezpieczeństwa możliwości urządzeń i systemów oferowanych na rynku. Podczas takich konsultacji pojawiają się często zagadnienia związane z połączeniem w jeden spójny system sieciowy central sygnalizacji pożarowej i sterowania gaszeniem, zapewnieniem wymaganej niezawodności działania urządzeń z zastosowaniem redundancji w zakresie central i połączeń czy zastosowania zabezpieczeń także w obszarach zagrożonych wybuchem (strefy Ex).

Niezbędne w takim przypadku jest zorganizowanie centrum nadzoru w zakresie bezpieczeństwa pożarowego, z uwzględnieniem podległych placówek, które ma za zadanie ujednolicenie rozwiązań ppoż. i nadzór nad obiektami objętymi zintegrowaną ochroną ppoż.. Projektant/konsultant korzysta wówczas z zapisów norm i wytycznych, np.: PN-EN54, NFPA, VdS, CNBOP.

Inwestorzy często też pytają, czy certyfikowany i zintegrowany system powinien obsługiwać wszystkie funkcje systemów teletechnicznych związanych z bezpieczeństwem. Skoro podczas zdarzenia pożarowego operator ma za zadanie właściwie obsłużyć urządzenia ppoż., to takie systemy, jak CCTV czy KD powinny go wyłącznie wspomagać w zakresie szybkości podejmowania decyzji.

Czy operator w krytycznej sytuacji myśli np. o funkcjach komfortu w zakresie automatyki budynku, konfiguracji kart kontroli dostępu itp.? – Raczej nie! Te dodatkowe rozwiązania teletechniczne powinny mieć swoją niezależną organizację działania i w momencie alarmu być podporządkowane systemom bezpieczeństwa pożarowego.

W wielu przypadkach inwestorzy posiadający w swojej infrastrukturze kilka rozproszonych obiektów dowiadują się o zdarzeniu pożarowym dopiero *post factum*, tzn. gdy służby zewnętrzne powiadomią ich o ugaszeniu pożaru! Aby uniknąć takich sytuacji i móc na bieżąco analizować zagrożenia pożarowe, należy zastosować certyfikowany system zarządzania bezpieczeństwem pożarowym, który umożliwi pełną integrację z centralami SSP i innymi urządzeniami ppoż. Taki system może się niezależnie łączyć z indywidualnymi centralami lub z centralą nadrzędną utworzonego rozbudowanego systemu sieciowego Integral WAN.

W zależności od liczby central, stopnia rozproszenia obiektów, budynków czy instalacji dostępnych jest kilka konfiguracji połączenia central w jedną spójną sieć, a także możliwość odpowiedniej organizacji przepływu danych oraz hierarchii pod względem zarządzania. Jako medium komunikacyjne można zastosować połączenia miedziane, światłowodowe lub opcjonalnie połączenia z wykorzystaniem infrastruktury IT obiektu (dla zwiększenia bezpieczeństwa dane można szyfrować z wykorzystaniem sieci VPN). W zakresie struktury systemu dostępne są topologie pierścienia lub sieci kratowej, które pozwalają na elastyczną rozbudowę systemu, przy zapewnieniu wymaganego stopnia niezawodności działania (odporność na min. trzy jednoczesne uszkodzenia sieciowe).

Dzięki zastosowaniu Integral WAN zamawiający/inwestor nie musi realizować kontraktu na zabezpieczenia ppoż. przez jednego integratora.

Każdy autoryzowany partner producenta może, korzystając z sieci Integral WAN, realizować swoje zadanie bez wpływu na innych równoległych wykonawców. Natomiast każdy z wykonawców odpowiada serwisowo za wykonany przez siebie zakres prac. W celach serwisowych można „zamrozić" działanie danego podsystemu, aby dany wykonawca mógł zrealizować swoje zadanie, nie naruszając zabezpieczenia pozostałej sieci central i systemu SSP+SUG. Wskazują na to zapisy np. wytycznych Ubezpieczyciela VdS.

W przypadku takiej organizacji inwestycji ważna jest odpowiednia koordynacja prac na etapie realizacji i późniejszej eksploatacji. Jeden z dostawców pełni rolę wiodącą i odpowiada za komunikację między podsystemami, całość działania zintegrowanego systemu sieciowego oraz jego współpracę z systemem integrującym urządzenia ppoż.

Systemy sygnalizacji pożarowej są obecne na rynku budowlanym od kilku dziesięcioleci. Swój najbardziej intensywny rozwój technologiczny przeżywały w latach 80. i 90. ubiegłego wieku, kiedy to systemy konwencjonalne zaczęły być stopniowo unowocześniane i powoli wypierane przez coraz bardziej nowoczesne systemy adresowalne.

System sygnalizacji pożarowej

ZETTLER PROFILE FLEXIBLE

technologie jutra dostępne już dziś

Wydaje się, że od początku XXI w. rozwój technologiczny systemów sygnalizacji pożarowej nieco wyhamował i nie jest już tak intensywny. Ale jest to spostrzeżenie nieco chybione, ponieważ w tym czasie powstało wiele nowoczesnych rozwiązań, które wpłynęły nie tylko na szybkość i skuteczność wykrywania pożarów. Rozwiązania opracowane w ostatnich 20 latach miały znaczący wpływ na niezawodność, odporność i wygodę użytkowania systemów sygnalizacji pożarowej.

Zettler – lider nowoczesnych technologii w detekcji pożarów

Marka produktów sygnalizacji pożarowej Zettler od lat korzysta z wielu nowoczesnych rozwiązań mających nie tylko zapewnić skuteczne wykrywanie pożarów, ale również takich, które w znacznym stopniu ułatwiają użytkownikowi końcowemu bezproblemowe korzystanie z systemu przez długi czas. Podstawą funkcjonowania najnowszych centrali Zettler Profile Flexible jest autorska technologia MZX, i jej dwa główne filary:

1. **Protokół komunikacyjny MZX Digital** – cyfrowy protokół komunikacji, z którego korzystają wszystkie elementy pętlowe w systemach opartych na technologii MZX: czujki pożarowe, ręczne ostrzegacze pożarowe, adresowalne moduły pętlowe. Jego unikalną cechą jest możliwość tworzenia w zasadzie dowolnej topologii pętli dozorowej i bardzo wysoka odporność na zakłócenia elekromagnetyczne pochodzące ze źródeł zewnętrznych. Jest to istotna zaleta, zwłaszcza w budynkach pełnych nowoczesnych technologii oraz pokrytych gęstą siecią okablowania i łączności bezprzewodowej. Protokół oparty jest na technice modulacji częstotliwości sygnału *(Frequency-Shift Keying, FSK)*, która pozwala na stosowanie okablowania nieekranowanego czy instalowanie pętli dozorowej w strefach potencjalnie narażonych na zakłócenia EMC, bez wpływu na stabilność i skuteczność komunikacji centrali z urządzeniami pętlowymi.
2. **Algorytm detekcji FastLogic** – powstały we współpracy z Uniwersytetem w Duisburgu, oparty na algorytmach logiki rozmytej *(Fuzzy logic)*. Odgrywa kluczową rolę w niezawodnym wykrywaniu pożarów przez czujki optyczne dymu, zapewniając jednocześnie maksymalną odporność przed alarmami fałszywymi. FastLogic jest podstawowym narzędziem central Zettler Profile Flexible stosowanym w celu szybkiej, bezbłędnej oceny zagrożenia pożarowego, pozwalającym jednocześnie odrzucić potencjalnie fałszywe zadziałania czujek dymu od takich źródeł, jak para wodna, kurz czy pył.

Czujki wirtualne

Technologia detekcji w nowoczesnych systemach sygnalizacji pożarowej coraz częściej bazuje na stosowaniu czujek wielosensorowych. Wprawdzie takie rozwiązanie nie jest nowe i stosuje je wielu producentów, ale Zettler zadbał o szereg innowacji również w tym zakresie. Podstawową cechą czujek wielosensorowych Zettler 6. generacji jest możliwość zastosowania techniki czujek wirtualnych, co daje projektantowi i inżynierowi uruchomień zupełnie nowe możliwości w kwestii doboru trybów pracy i sposobu współdziałania poszczególnych sensorów w obszarze pojedynczej czujki.
Kluczową cechą jest tu możliwość niezależnego zaprogramowania każdego z sensorów w danej czujce, co pozwala np. „stworzyć" dwie lub nawet trzy niezależnie działające czujki, mimo że znajdują się one w jednej fizycznej obudowie. Co więcej, te wirtualne czujki pożarowe mogą również ze sobą współpracować (np. na zasadzie koincydencji), dając dodatkowe narzędzie np. w celu wykluczenia przypadkowego zadziałania systemu sygnalizacji pożarowej. □

Więcej informacji na stronie www.zettlerfire.com

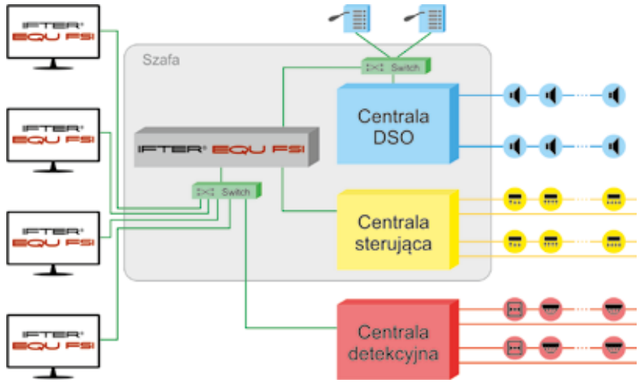
Johnson Controls International
ul. Krakowiaków 50
02-255 Warszawa
pawel.jozwik@jci.com

IFTER EQU FSI – dedykowany do systemów ppoż. system wizualizacji i integracji

W Rozporządzeniu Ministra Inwestycji i Rozwoju z 13 czerwca 2018 r. w grupie wyrobów budowlanych objętych obowiązkiem sporządzania Krajowej Deklaracji Właściwości Użytkowych oraz Krajowego Systemu Oceny i Weryfikacji Stałości Właściwości Użytkowych znalazła się grupa wyrobów zdefiniowana jako „Systemy integrujące urządzenia przeciwpożarowe – zestawy: systemy do wizualizacji i/lub sterowania". Skutkiem wejścia w życie tego rozporządzenia po 31 grudnia 2020 r. jest prawny zakaz instalacji wizualizacji do systemów ppoż. nieposiadających stosownej deklaracji i oceny.

W odpowiedzi na zapotrzebowanie rynku na system spełniający wymagania rozporządzenia firma IFTER stworzyła nową linię produktową IFTER EQU Fire Systems Integrator. To kontynuacja produkowanych przez naszą firmę od 20 lat systemów integracyjnych i wizualizacyjnych, znanych i cenionych przez instalatorów i inwestorów.
IFTER EQU FSI składa się nie tylko z oprogramowania, ale też z urządzeń, które zostały poddane szczegółowym badaniom w CNBOP. Całość jest zamknięta w kompaktowej (jak na liczbę wykorzystywanych elementów) obudowie o klasie szczelności IP54, zapewniającej ochronę przed próbami penetracji drutem, ochronę przed pyłem i bryzgami wody z dowolnego kierunku. Tak wysoki poziom ochrony umożliwia montaż szafy w miejscach trudnych eksploatacyjnie i poprawną jej pracę podczas akcji gaszenia pożaru. Dzięki temu ekipy gaszące mają stały podgląd na rozprzestrzenianie się pożaru, a nie tylko sam moment jego wykrycia.

Dużą uwagę poświęcono zasilaniu systemu – ma ochronę przeciwprzepięciową 20 kA i zabezpieczenia wyłącznikami nadprądowymi. Kolejny stopień zabezpieczeń stanowią zasilacze buforowe certyfikowane, o odpowiedniej liczbie akumulatorów, zasilające nie tylko centralę sterującą i DSO, ale także serwer. Wydzielenie mechaniczne sekcji zasilania 230 VAC i zasilanie wszystkich urządzeń napięciem bezpiecznym podnosi poziom bezpieczeństwa i ułatwia pracę serwisowi. Również wszelkie podłączenia urządzeń zewnętrznych do sieci komputerowej są zabezpieczone do 150 A, co praktycznie uniemożliwia przedostanie się do szafy przepięć od strony infrastruktury sieciowej.



IFTER EQU FSI, oprócz obsługi wielu typów central sygnalizacji pożarowej, może też – dzięki swobodnie definiowanym algorytmom pożarowym – wykonywać samodzielnie sterowania poprzez wbudowaną centralę sterującą. Każda z central może obsługiwać od 2 do 6 pętli z maks. 762 modułami sterującymi. Innowacją względem konkurencji jest pełna integracja z DSO, poczynając od swobodnego sterowania (z wizualizacji) komunikatami głosowymi, po sterowania wyjściami i monitorowanie wejść kontrolnych. Wbudowane algorytmy analizy zagrożeń, w zależności od lokalizacji pożaru i trudności np. z otwarciem drzwi ewakuacyjnych, będą dynamicznie zmieniały kierunek ewakuacji w celu jej optymalnego przeprowadzenia. Wspierając operatora, może dynamicznie sterować mikrofonem centrali DSO i informować go, do których stref powinien nadać komunikat.

IFTER EQU FSI integruje systemy SSP, SSWiN, KD, CCTV (VSS) czy automatyki budynkowej, ma również rozbudowane możliwości wizualizacyjne tych systemów. Oprócz klasycznej wizualizacji można wykonywać widoki oparte na podkładach wektorowych, w pełni skalowalne i z przesuwaniem planów architektonicznych, oraz widoki oparte na przeglądarkach WEB. Zwłaszcza wykorzystanie wizualizacji WEB pozwala na wyposażenie ochrony w urządzenia mobilne umożliwiające stałe monitorowanie rozprzestrzeniania się pożaru czy też zmianę kierunków ewakuacji poza pomieszczeniem monitoringu.

Celem stworzenia IFTER EQU Fire Systems Integrator było nie tylko umożliwienie inwestorom spełnienia wymagań nowego rozporządzenia, ale przede wszystkim dostarczenie nowoczesnego i innowacyjnego rozwiązania, upraszczającego obsługę skomplikowanych rozwiązań i zwiększającego skuteczność ochrony. □

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

Technologia gaszenia mgłą wodną

Idea gaszenia mgłą wodną nie jest nowa. W 1880 r. amerykańska firma F.E. Myers wyprodukowała system przenośny wytwarzający kropelki wody. Był używany głównie do gaszenia małych pożarów lasów. Zaledwie dziesięć lat później Frederick Grinnell opracował zraszacz nazwany „pieprzniczką" *(pepper pot)*, który do gaszenia pożarów również wykorzystywał małe kropelki wody. W 1930 r. pojawiło się już kilka firm, które zaczęły zajmować się aplikacją mgły wodnej. Wśród nich była niemiecka firma Lechler, której główną innowacją była dysza wielootworowa, nazywana w latach trzydziestych XX w. dyszą pyłu wodnego. W latach czterdziestych XX w. dział inżynieryjny Factory Mutuals zaczął przeprowadzać pierwsze testy z użyciem małych dysz kropelkowych.

Mimo pierwszych sukcesów zainteresowanie mgłą wodną przez następne dziesięciolecia pozostawało niewielkie. Badaniami zajmowali się naukowcy z instytutów badawczych w Europie i USA, ale z komercyjnego punktu widzenia technologia ta nie miała wielkiego wpływu na rozwój rynku ppoż. Dopiero w latach 90. XX w. zaczęła się upowszechniać.

Dwa zdarzenia, które utorowały drogę do zastosowań mgły wodnej

Pierwszym z nich było przyjęcie Protokołu Montrealskiego w sprawie „substancji zubożających warstwę ozonową" pod koniec lat 80. XX w., co doprowadziło do wycofania halonu z użycia. Drugim był pożar promu pasażerskiego „Scandinavian Star", który wybuchł 7 kwietnia 1990 r. Zginęło w nim 158 osób – prawie połowa pasażerów. Pożar ten doprowadził do zaostrzenia wymagań bezpieczeństwa przeciwpożarowego Międzynarodowej Organizacji Morskiej (IMO). Opracowano wytyczne dotyczące instalacji oraz procedury testów ogniowych dla alternatywnych systemów tryskaczowych.

Nieco ponad dwa miesiące po katastrofie poproszono Matsa Rosandera i Kristera Giselssona, dwóch szwedzkich naukowców, którzy badali możliwości ochrony ppoż. pokoi hotelowych i kabin pasażerskich z wykorzystaniem mniejszych kropelek wody, o przedstawienie wyników swoich badań. Niedługo potem powstały dwie firmy produkujące systemy gaszące mgłą wodną: UltraFog i Marioff.

Osiem lat później powołano Międzynarodowe Stowarzyszenie Mgły Wodnej (International Water Mist Association – IWMA) jako forum m.in. dla producentów, instytutów badawczych, towarzystw ubezpieczeniowych i organizacji wydających akty prawne. Platformą wymiany wiedzy IWMA jest International Water Mist Conference (IWMC). Dwudziesta edycja tego wydarzenia odbędzie się 21 i 22 kwietnia 2021 r. w Warszawie.

Jak działa mgła wodna?

Aby pożar się rozwinął, potrzebne są trzy elementy, tworzące tzw. trójkąt ognia: paliwo, ciepło i tlen. Mgła wodna redukuje ciepło i tlen. Odbywa się to poprzez wtryskiwanie wody przez specjalnie zaprojektowane dysze. Wraz ze wzrostem ciśnienia w systemie maleje wielkość kropel, zajmują one coraz większą przestrzeń, w efekcie woda zamienia się w parę wodną, co prowadzi do szybkiego obniżenia temperatury czoła płomieni. Ze względu na działanie chłodzące mgła wodna zapobiega również wtórnemu zapłonowi.

Technologia mgły wodnej jest bardzo ekonomiczną metodą ochrony przeciwpożarowej, ponieważ do gaszenia zużywa mniejsze ilości wody. Jest również przyjazna dla środowiska, nie powoduje zubożenia warstwy ozonowej, nie przyczynia się do globalnego ocieplenia, nie powoduje szkód wywoływanych przez kontakt z wodą i nie szkodzi ludziom. Lista zastosowań jest imponująca: tunele kablowe, biura, maszynownie, wieżowce itp.

Jest wiele norm i wytycznych, które wspierają tę technologię, m.in. FM 5560, NFPA 750, VdS 3188, wkrótce ukaże się europejska norma EN 14972. ▫

International Water Mist Association

Poststraße 33,
D-20354 Hamburg,
Niemcy
tel. + 49 (0) 40 35085-215
www.iwma.net

Mgła wodna – przełomowe rozwiązanie dla przemysłu

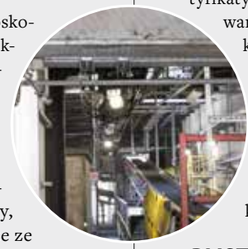
W obiektach przemysłowych występuje wiele zagrożeń pożarowych, które w krótkim czasie mogą przekształcić się w pożary trudne do opanowania. Dla większości z nich skutecznym rozwiązaniem są systemy gaszenia mgłą wodną. Ta nowoczesna forma ochrony przeciwpożarowej może być z powodzeniem stosowana również tam, gdzie skuteczność tradycyjnych systemów gaśniczych jest ograniczona.

Zalety mgły wodnej

- skutecznie gasi pożary przy użyciu niewielkiej ilości czystej wody, co ogranicza do minimum wielkość szkód i czas przestojów,
- w gaszonych pomieszczeniach zachowuje się jak gaz – rozprowadzana jest równomiernie, skutecznie gasząc ogień nawet na obszarach o ograniczonej dostępności,
- zapewnia szybkie schłodzenie gaszonych przestrzeni, ułatwiając ewakuację i ograniczając wielkość strat,
- nie wymaga szczelności zabezpieczanych obiektów,
- elementy instalacji mogą być montowane w najbardziej skomplikowanych konstrukcjach i ograniczonych przestrzeniach,
- niewielkie średnice rur i rozmiary pozostałych elementów instalacji umożliwiają prosty i szybki montaż w obiektach już istniejących, ograniczając do minimum zakres ingerencji,
- redukuje ilość szkodliwych produktów spalania,
- jest w pełni bezpieczna dla ludzi, chronionych obiektów i środowiska.

Zastosowanie technologii mgły wodnej w przemyśle

Systemy mgły wodnej doskonale sprawdzają się jako aktywne zabezpieczenia przeciwpożarowe obiektów i urządzeń przemysłowych, jak układy nawęglania, tunele kablowe, turbiny gazowe i turbozespoły, transformatory, generatory prądotwórcze ze zbiornikami paliwa, maszynownie, lakiernie, maszyny CNC, prasy hydrauliczne i inne.



Jedna z wiodących na świecie technologii wysokociśnieniowej mgły wodnej została opracowana przez inżynierów FOGTEC. Wykorzystuje ona bardzo małe krople klasy I (NFPA 750), a jej skuteczność została potwierdzona podczas wielu pełnowymiarowych testów i akcji gaśniczych w warunkach rzeczywistych.

Wybrane zastosowania systemów wysokociśnieniowej mgły wodnej FOGTEC w obiektach przemysłowych:

- tunel kablowy Singapur Power o długości 35 km,
- maszynownie i transformatory – elektrownia szczytowo-pompowa nad jeziorem Limmern (Szwajcaria),
- turbiny parowe i prasy hydrauliczne – Südzucker AG (Niemcy),
- hydrauliczne młoty matrycowe i linia produkcji felg – Otto Fuchs (Niemcy, Węgry),
- przenośniki taśmowe – Marl Chemical Park / Evonik (Niemcy),
- maszyna do elektrolitycznego powlekania stali o długości 180 m – ThyssenKrupp AG (Niemcy),
- ochrona 72 stanowisk testowych silników – Daimler AG (Niemcy),
- hale produkcyjne i biura zakładu przetwórstwa tworzyw sztucznych THULE (Niemcy).

Systemy FOGTEC mają aprobaty i certyfikaty VdS, FM i TÜV dla zastosowań m.in. w tunelach i kanałach kablowych, obszarach maszynowych, jako zabezpieczenie generatorów, turbin, transformatorów, frytownic, kabin lakierniczych, maszyn CNC, komórek testowych silników czy do lokalnej ochrony maszyn.

PLISZKA – gwarancja jakości

Wyłącznym dystrybutorem technologii wysokociśnieniowej mgły wodnej FOGTEC w Polsce jest firma PLISZKA – krajowy lider w zakresie aktywnych zabezpieczeń przeciwpożarowych. Firma PLISZKA od ponad 30 lat świadczy usługi w zakresie projektowania, montażu i kontroli systemów ppoż., obejmujących automatyczne systemy gaszenia gazem, instalacje tryskaczowe, mgły wodnej, pianowe oraz systemy automatyki pożarowej.

Stosowanie najnowszych technologii, szeroka gama usług oraz kompletna oferta produktowa pozwalają firmie PLISZKA kompleksowo chronić przed ogniem nawet najbardziej wymagające inwestycje, optymalnie dopasowując zabezpieczenia ppoż. do potrzeb klienta. ▫

Poż-Pliszka

ul. Miałki Szlak 52,
80-717 Gdańsk
www.pliszka.pl

GASZENIE POŻARU
może doprowadzić twoją firmę do bankructwa!

TEKST
Paweł Zbrożek

Właściwy dobór środka gaśniczego do rodzaju chronionych materiałów jest podstawą skutecznego ugaszenia pożaru – to logiczna i utrwalona zasada stosowana nie tylko przez strażaków. Czy kierując się tylko tą zasadą, zabezpieczysz swoją firmę przed skutkami pożaru, jeśli takowy wystąpi?

Zgodnie z tą regułą pożar będzie ugaszony skutecznie, ale czy:
- wyładowanie środka gaśniczego nie zagrozi bezpieczeństwu osób, nie zniszczy twoich dóbr i danych, nie uszkodzi sprzętu?
- czas przestoju związany z przywróceniem obiektu do funkcjonowania i naprawa szkód nie będą zbyt kosztowne?

Użytkownicy będą dążyli do stanu, aby na powyższe pytania odpowiedź brzmiała NIE. Fakty wskazują, że złudne poczucie bezpieczeństwa u wielu użytkowników, których obiekty były wyposażone w urządzenie gaśnicze, zweryfikował incydent gaszenia pożaru – do bankructwa włącznie...

Przykład serwerowni

Chyba nikt nie rozważa gaszenia ich wodą, ale np. aerozolami już tak. Wiele destrukcyjnych incydentów zadziałania generatorów aerozoli w serwerowniach spowodowało, że raczej się ich tam unika. Porównajmy wybrane systemy o tanich, ekologicznych środkach gaśniczych, tj. na mieszaninę gazów obojętnych Inergen i na mgłę wodną.

Mgła wodna w wysokiej dyspersji

Badania* przeprowadzone na Rutgers University potwierdziły znaczny wpływ wilgotności na awaryjność w serwerowniach. Dane te pokrywają się z faktami dość częstych awarii i usterek w serwerowniach zgłaszanych tuż po lub w krótkim czasie po wyładowaniu tam mgły wodnej.

Inergen stanowi mieszaninę azotu, argonu i CO_2

Inergen jest zupełnie pozbawiony wilgoci, dlatego nie wpływa na awaryjność w serwerowniach. Gaszenie Inergenem polega na zmniejszeniu stężenia tlenu poniżej granicy spalania gaszonego materiału (około 14%), ale nie mniej niż 12%, którą można traktować jako ostrzegawczy próg bezpieczeństwa dla ludzi. Niewielki dodatek CO_2 do Inergenu ma na celu poprawę reakcji fizjologicznych u ludzi, czyniąc tę mieszankę jeszcze bardziej bezpieczną niż samych jednoskładnikowych gazów obojętnych, np. azotu.

Inergen, w przeciwieństwie do mgły wodnej, nie skrapla się na gaszonych powierzchniach i przegrodach, ale dyfunduje do osłoniętych przestrzeni, osiągając tam i w całej przestrzeni równomierne stężenie.

Stosowanie systemu Inergen ma na celu całkowite ugaszenie pożaru (*extinguish*), a urządzenia gaśnicze mgłowe do tego typu aplikacji są dopuszczane na tłumienie pożaru (*suppress*). Oznacza to, że po wyładowaniu mgły wodnej może zajść konieczność ręcznego dogaszenia „stłumionego" w serwerowni pożaru. Poza tym po akcji gaszenia mgłą wodną konieczne jest niezwłoczne usunięcie wody z powierzchni, na których mgła się skropliła – problem ten nie dotyczy Inergenu.

Potwierdzeniem powyższego jest zapis w wytycznych FM Global Data Sheet 5-32 punkt 2.5.1.2.1 mówiący o tym, że *w celu zmniejszenia ryzyka uszkodzeń w serwerowniach i skrócenia czasu przestoju spowodowanego gaszeniem należy stosować certyfikowane przez FM Global urządzenie na czysty środek gaśniczy.*

System Inergen wykorzystuje taki właśnie środek, a przy tym jest certyfikowany nie tylko przez FM Global, ale wiele innych uznanych na świecie organizacji, co jest dowodem jego wysokiej jakości i niezawodności.

Dystrybutorem Inergenu – IG541 w Polsce jest firma DEKK Fire Solutions.

DEKK Fire Solutions

ul. Zielona 52
05-500 Piaseczno
http://dekk.pl
info@dekk.pl

* Manousakis I., Sankar S., McKnight G., Nguyen T. D., Bianchini R., Environmental Conditions and Disk Reliability in Free-cooled Datacenters. In Proceedings of the 14th USENIX Conferenceon File and Storage Technologies (2016).

Obiekty dydaktyczne
Bezpieczeństwo i edukacja

SCHRACK SECONET TO DOŚWIADCZENIE, INNOWACYJNOŚĆ I PRZEDE WSZYSTKIM BEZPIECZEŃSTWO NA NAJWYŻSZYM ŚWIATOWYM POZIOMIE. PRODUKTY SĄ OPARTE NA NAJNOWSZYCH ROZWIĄZANIACH TECHNIKI, INTUICYJNE W OBSŁUDZE I NIEZAWODNE W DZIAŁANIU. ROZWÓJ GODNYCH ZAUFANIA SYSTEMÓW PRZECIWPOŻAROWYCH STAŁ SIĘ TRADYCJĄ FIRMY.

Inwestowanie na szeroką skalę w badania i rozwój, praca w międzynarodowych zespołach, współpraca z uczelniami technicznymi, organami Państwowej i Ochotniczej Straży Pożarnej oraz ośrodkami badawczymi zapewniają nie tylko zastosowanie najlepszych rozwiązań technicznych w naszych produktach, ale również pomagają utrzymać przodującą rolę w misji zabezpieczania ludzkiego życia oraz mienia. Lista referencyjna Schrack Seconet to ponad 6000 dużych i średnich obiektów, m.in. najsłynniejsze i największe sieci hoteli, obiekty sportowe, wysokiej klasy biurowce, obiekty magazynowe, lotniska, obiekty przemysłowe i wojskowe (NATO).
Urządzenia Schrack Seconet zastosowano również w obiektach edukacyjnych, m.in. w wielu uczelniach technicznych. Chronią życie i zdrowie osób przebywających tam na co dzień, a także zabezpieczają bezcenne zbiory znajdujące się w np. w bibliotekach uniwersyteckich. Prezentujemy kilka rozwiązań w budynkach uczelnianych.

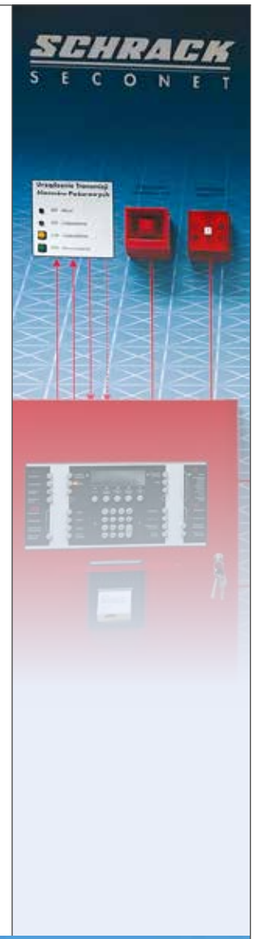
W latach 2003-2004 przy **Szkole Aspirantów Państwowej Straży Pożarnej w Poznaniu** zabezpieczony został internat szkolny, w którym wówczas zainstalowano system sygnalizacji pożarowej Integral C Evolution. Była to centrala przeznaczona do małych i średnich obiektów, umożliwiająca podłączenie maks. 128 elementów do 2 pętli dozorowych. Elementami pętlowymi były m.in. czujki optyczne dymu OSD 2000, ręczne ostrzegacze pożarowe MCP 535, a także elementy monitorująco-sterujące, np. moduły BA-OI3. W latach 2015-2017 budynek szkoły poddano modernizacji, co spowodowało konieczność rozbudowy instalacji SSP, a tym samym wymiany centrali na wersję modułową, która byłaby w stanie sprostać wymaganiom projektowym. Dotychczasowa centrala została zastąpiona najnowszym rozwiązaniem Schrack Seconet – centralą serii Integral IP MXF.
W związku z rozbudową instalacji pojawiły się elementy pętlowe w technice X-LINE, tj. interaktywne czujki wielokryteriowe (dymu, ciepła) CUBUS MTD 533X pracujące w zakresie pożarów testowych TF1-TF9, ręczne ostrzegacze pożarowe MCP545X, a także elementy monitorująco-sterujące, np. moduły BX-OI3. Sala wykładowa oraz internat są doskonałym przykładem potwierdzającym jedną z wielu cech charakterystycznych dla rozwiązań Schrack Seconet, jaką jest gwarancja kompatybilności „wstecz" i „w przód". Oznacza to, iż każda nowa generacja systemu sygnalizacji pożarowej produkcji Schrack Seconet jest w pełni kompatybilna zarówno z już istniejącymi systemami, jak i z tymi, które powstaną w przyszłości. Daje to duże możliwości modernizacji i rozbudowy systemu w bliskiej i dalekiej przyszłości, a dostępność części zamiennych dla wycofywanych z produkcji urządzeń przestaje być typowym problemem producenta.
W 2011 r. firma Schrack Seconet zabezpieczyła **Bibliotekę Uniwersytecką we Wrocławiu**. Cały obiekt składa się z trzech budynków stanowiących zabytki architektury oraz nowego budynku głównego, scalającego w jednym miejscu księgozbiory i zespoły funkcjonale. Biblioteka została wyposażona w doskonałe systemy zabezpieczeń, w tym również systemy sygnalizacji pożarowej Schrack Seconet. W obiekcie zainstalowano łącznie prawie 1,6 tys. wielokryteriowych czujek CUBUS MTD 533 wykrywających wszystkie pożary testowe (TF1-TF9).
Co więcej, mogą być one zastosowane jako czujki dymu, ciepła lub jako czujki dualne dymu i ciepła, a dzięki technice interaktywnego działania CUBUS Nivellierung mogą dostosowywać swoją czułość detekcji do zmieniających się warunków otoczenia. System składa się z pięciu modułowych central sygnalizacji pożarowej Integral IP, których architektura jest oparta na idei 100% redundancji sprzętowej i programowej. Każda z nich może zapamiętać do 65 tys. zdarzeń. Pracę poszczególnych komponentów nadzoruje efektywny system wizualizacji SecoLOG – wielostanowiskowe, efektywne narzędzie graficzne z przyjaznym użytkownikowi interfejsem – umożliwiający przegląd zarejestrowanych zdarzeń i obsługę całego systemu sygnalizacji pożarowej.

W roku 2011 do listy referencyjnej Schrack Seconet obiektów o charakterze naukowym dołączyły dwa kolejne, zlokalizowane w Kielcach: **Uniwersytet im. Jana Kochanowskiego** i **Politechnika Świętokrzyska**. Wszystkie obiekty uczelniane – 25 budynków dydaktycznych o łącznej powierzchni ok. 77 tys. m² – są częściowo wyposażone w systemy sygnalizacji pożarowej Integral IP i ponad 300 innowacyjnych wielokryteriowych czujek CUBUS MTD 533. Politechnika Świętokrzyska, najstarsza wyższa uczelnia w tym regionie, w 2011 r. zyskała kolejny budynek dydaktyczny, charakteryzujący się przede wszystkim innowacyjnością, nowatorskimi rozwiązaniami pozyskiwania i akumulowania ciepła oraz nowoczesnymi technologiami informacyjnymi do celów sterowania i monitoringu. Najwyższy poziom bezpieczeństwa budynku zapewniają również innowacyjne systemy sygnalizacji pożarowej Schrack Seconet Integral IP oraz system wczesnej detekcji AirSCREEN ASD 535.
Jeśli mowa o placówkach dydaktycznych, w których znajdują się rozwiązania Schrack Seconet, należy również wspomnieć, że w ostatnich latach przekazaliśmy nasze urządzenia także do celów edukacyjnych. Wyposażenie sal w najnowsze rozwiązania pomogło nie tylko stworzyć wymarzone miejsce do nauki, ale także wesprzeć ofertę edukacyjną uczelni technicznych. Nasze zaangażowanie nie kończy się jedynie na przekazaniu sprzętu – Schrack Seconet czuwa również nad tym, by urządzenia były we właściwy sposób wykorzystane. Studenci zyskują szansę, by podczas zajęć poznawać nasze rozwiązania od strony praktycznej, a także mieć kontakt z zawodowcami, którzy dzielą się swoją wiedzą. Dzięki temu uczelnia może lepiej kształcić studentów, podnieść poziom wiedzy i umiejętności swoich absolwentów, którzy w przyszłości mogą stać się specjalistami z zakresu ochrony ppoż. Obie strony odnoszą wymierne korzyści, łącząc siły, by móc funkcjonować na współczesnym rynku.

W 2012 r. w **Akademii Górniczo-Hutniczej im. Stanisława Staszica w Krakowie** zainstalowano tablicę demonstracyjną o wymiarach 1,1 m x 1,5 m z centralą Integral IP MXF, która jest modułowym, redundantnym systemem sygnalizacji pożarowej, zbudowanym z odpowiednio dobranych podzespołów, konfigurowanym i programowanym pod kątem

spełnienia konkretnych potrzeb danej instalacji. Każda podcentrala stanowi samodzielną jednostkę z własnym zasilaniem i akumulatorami, do każdej można podłączyć, oprócz grup detektorów i układów sterowania, zewnętrzne panele obsługi, panele obsługi dla straży pożarnej, drukarki itp.
Schrack Seconet przekazał także czujki wielokryteriowe CUBUS MTD 533X, ręczne ostrzegacze pożarowe MCP 545X, moduł wejścia/wyjścia BX-OI3 z jednym wyjściem przekaźnikowym z programowalnym położeniem *fail-safe*, dwa wejścia do sterowania styków bezpotencjałowych i jedno wyjście z separacją galwaniczną (optoizolator) do nadzorowania napięcia zewnętrznego oraz moduł sterujący wejść/wyjść BX-O2I4, który jest przystosowany do pracy w technice Integral X-LINE – zawiera dwa wyjścia przekaźnikowe z możliwością pracy pulsacyjnej i cztery wejścia do nadzorowania styków bezpotencjałowych. W zestawie znalazł się także sygnalizator akustyczny pętlowy BX-SOL.

W roku 2013 w **Wyższej Szkole Menedżerskiej w Warszawie** zamontowano tablicę demo o wymiarach 1,2 m x 1,2 m. Salę wyposażono w wielostrefową centralę sterowania gaszeniem Integral IP MXF, a także wielokryteriowe czujki CUBUS MTD 533X, które mogą być stosowane jako czujka dymu, czujka ciepła lub jako czujka dualna dymu i ciepła. Dodano ostrzegacz pożarowy MCP 545X służący do ręcznego wyzwalania alarmu pożarowego (typ A zgodnie z EN 54-11). Wyzwolenie alarmu następuje w wyniku zbicia szybki, skasowanie alarmu wymaga wymiany szybki na nową po skasowaniu alarmu na panelu obsługi. Przycisk dostępny jest w różnych wersjach (klasa IP, kolor obudowy). Przycisk START GASZENIA MCP 535X (kolor żółty) służy do ręcznego uruchamiania procedury gaszenia stałych urządzeń gaszenia gazem zgodnie z EN 12094-3. Podłączany jest w technice pętli dozorowych X-LINE. Uruchomienie funkcji gaszenia odbywa się poprzez zbicie szybki i wciśnięcie przycisku. Stan alarmowy wskazuje wbudowana dioda LED.
Moduł sterujący wejść/wyjść BX-OI3, przystosowany do pracy w technice Integral X-LINE, zawiera wyjście przekaźnikowe z programowalną pozycją w razie uszkodzenia (*fail-safe*), dwa wejścia do nadzorowania zestyków bezpotencjałowych oraz jedno wejście z optozłączem, które w razie potrzeby może służyć do nadzorowania napięcia zewnętrznego. Moduł wejścia/wyjścia BX-O2I4 ma dwa bezpotencjałowe bistabilne wyjścia przekaźnikowe o maks. obciążeniu prądowym 2 A i maks. napięciu 230 V (maks. moc 60 W) oraz cztery wejścia do nadzorowania zestyków bezpotencjałowych, a także sygnalizatory optyczne i akustyczne. Ponadto są przyciski symulujące przerwy, zwarcia, doziemienia, uaktywnienia czujki specjalnej i info o przesłaniu sygnału do PSP. Dodatkowo zainstalowano aplikację Integral Desktop (wirtualne pole obsługi centrali) na stanowisku komputerowym.



LABORATORIA SYSTEMÓW BEZPIECZEŃSTWA

Warto wspomnieć, że w 2006 r. otworzono pierwszą w Polsce specjalność Bezpieczeństwo Obiektów i Informacji na Wydziale Informatyki Stosowanej i Technik Bezpieczeństwa Wyższej Szkoły Menedżerskiej w Warszawie. Ta wówczas nowa specjalizacja była przyczynkiem budowy Zespołu Laboratoriów Systemów Bezpieczeństwa – ZLSA. Zbudowanie unikalnego laboratorium było ogromnym wyzwaniem. Ze względu na wysokie koszty budowę rozpoczęto w 2008 r. dzięki zaangażowaniu wielu sponsorów. Uroczyste otwarcie Zespołu Laboratoriów Systemów Bezpieczeństwa nastąpiło w marcu 2009 r. Dwa stanowiska wyposażone zostały w rozwiązania Schrack Seconet. Stanowisko 27. współpracuje, za pośrednictwem łącza transmisyjnego, z cyfrowym systemem przeciwpożarowym IP firmy Schrack Seconet, a kolejne stanowisko umożliwia symulowanie różnych zagrożeń pożarowych.

W tym samym roku wyposażyliśmy także **Szkołę Główną Służby Pożarniczej w Warszawie**. Na ściennej tablicy demonstracyjnej o wymiarach 1,35 m x 1,5 m umieszczono centralę Integral IP MXF. Centrala stanowi samodzielną jednostkę z własnym zasilaniem i akumulatorami, do której można podłączyć, oprócz grup detektorów i układów sterowania, zewnętrzne panele obsługi, panele obsługi dla straży pożarnej itp. Za pomocą sieci Integral LAN można podłączyć do 16 podcentral w jeden system, z wykorzystaniem techniki sieci kratowych. W sali zainstalowano także wielokryteriową czujkę MTD 533X, która dla zapewnienia optymalnej detekcji pożaru samodzielnie monitoruje warunki otoczenia, w jakich pracuje, adaptując się do nich w sposób dynamiczny i w pełni automatyczny.
Ręczne ostrzegacze pożarowe MCP 545X zostały przystosowane do pracy w technice Integral X-LINE. Są wyposażone w izolator zwarć i wskaźnik alarmowy LED. Alarm jest wywoływany zbiciem szybki lub poprzez wciśnięcie panelu z tworzywa sztucznego. Stan alarmowy pozostaje aktywny do momentu wymiany szybki na nową lub skasowania (wersja z panelem). Do kontroli działania służy kluczyk testowy, natomiast do wstrzymania uruchomionej procedury gaszenia instalacji gaśniczej gazowej – przycisk STOP GASZENIA MCP 535X (kolor niebieski). Przyciski wyzwalające MCP 535X przeznaczone są do montażu natynkowego; w kolorze żółtym mają stopień ochrony obudowy IP52 lub IP54 (dodatkowa uszczelka), a w niebieskim IP54. Są wyposażone w zintegrowany izolator zwarć.
Moduł BX-OI3 jest przeznaczony do przyłączenia czujek specjalnych (np. liniowe czujki dymu, czujki płomienia, systemy zasysające) w technice Integral X-LINE. Adresowanie modułu i ustawienie parametrów przyłączanych do niego czujek specjalnych (tj. reakcja podczas alarmu lub uszkodzenia) odbywa się za pomocą oprogramowania PC podłączonego do centrali sygnalizacji pożarowej. Moduł wejścia/wyjścia BX-O2I4 zawiera dwa bezpotencjałowe, bistabilne wyjścia przekaźnikowe o maks. obciążeniu prądowym 2 A. Dodano też przyciski symulujące przerwy, zwarcia, doziemienia, uaktywnienia czujki specjalnej.
Dodatkowo stacja z PC ma zaimplementowaną aplikację Integral Desktop – program przeznaczony do obsługi i nadzorowania instalacji na komputerach stacjonarnych. Wyświetla on odwzorowany 1:1 panel obsługi centrali Integral IP, stanowiąc tym samym narzędzie do prostego i wygodnego użytkowania w czasie rzeczywistym. Wersja językowa interfejsu może być dostosowana do preferencji operatora i dowolnie zmieniana – nawet podczas pracy oprogramowania. Zainstalowany jest również system wizualizacji zdarzeń SecoLOG.

W roku 2017 tablicę demo o wymiarach 4,5 m x 3,0 m zamontowano w **Wojskowej Akademii Technicznej im. Jarosława Dąbrowskiego w Warszawie.** Zainstalowana na niej centrala Integral IP MXF to modułowy, redundantny systemem sygnalizacji pożarowej, zbudowany z odpowiednich podzespołów, konfigurowany i programowany dla spełnienia konkretnych potrzeb danej instalacji. Znalazły się na niej także elementy peryferyjne w technice X-LINE, przyciski symulujące przerwy, zwarcia, doziemienia, uaktywnienia czujki specjalnej. W sali demo zainstalowano również centralę sterowania gaszeniem Integral IP CXE (1 strefa gaszenia) oraz system zasysający z najnowszym technologicznie, wysokoczułym detektorem HD.
Ten system wczesnej detekcji dymu AirSCREEN ASD 535 (*Aspiration Smoke Detection*) składa się z jednego lub dwóch układów orurowania z otworami ssawnymi oraz jednostki oceniającej, wyposażonej w jeden lub dwa czujniki dymu o bardzo wysokiej czułości. Powietrze z nadzorowanego pomieszczenia jest zasysane i transportowane do jednostki oceniającej, a czujnik dymu kontroluje skład powietrza pod względem obecności cząstek dymu w zakresie zdefiniowanych parametrów granicznych. W przypadku ich pojawienia się, detektor natychmiast wyzwala alarm, umożliwiając odpowiednim służbom zwalczanie zjawisk pożarowych we wczesnej ich fazie.
Salę demo wyposażono ponadto w system wizualizacji SecoLOG IP V2.0. – efektywne narzędzie graficzne oparte na najnowocześniejszej technologii IP, służące do głównego dozoru systemu sygnalizacji pożarowej przez grupy interwencyjne: straż pożarną, ochronę budynku lub służby techniczne. Wszystkie komunikaty i stany podłączonych central sygnalizacji pożarowej mogą być prezentowane w przejrzysty sposób na jednym lub kilku stanowiskach obsługi komputerowej.

Naszym ostatnim przedsięwzięciem był montaż systemów pożarowych w lutym 2020 r. w **Państwowej Wyższej Szkole Zawodowej im. Angelusa Silesiusa w Wałbrzychu**. Na tablicy demonstracyjnej o wymiarach 1,5 m x 2,2 m zamontowano centralę Integral IP MXF, czyli modułowy, redundantny systemem sygnalizacji pożarowej wraz z elementami peryferyjnymi w technice X-LINE. Technika linii pętlowych Integral X-LINE jest dostępna we wszystkich centralach z rodziny systemów Integral IP i oferuje rozszerzone funkcje związane z nadzorowaniem i sterowaniem. Do jednej linii pętlowej (o maks. dł. 3500 m) można podłączyć do 250 elementów. Krótkie czasy inicjalizacji pętli umożliwiają szybkie jej uruchamianie również w przypadku podłączenia maksymalnej liczby elementów. Dodatkowo zamontowano przyciski symulujące przerwy, zwarcia, doziemienia i uaktywnienia czujki specjalnej. □

Schrack Seconet Polska

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

Cyberataki na systemy przemysłowe

Środowiska, w których stosuje się techniki operacyjne, są coraz częstszym celem cyberprzestępców. Jednocześnie nakłady finansowe na cyberbezpieczeństwo rosną, ponieważ zarządy firm dostrzegają jego kluczową rolę w zapewnianiu ciągłości biznesowej i produkcyjnej.

TEKST
Fortinet
www.fortinet.com

Zakłady przemysłowe i użyteczności publicznej, służba zdrowia, transport publiczny, obiekty energetyczne i obejmujące infrastrukturę krytyczną w coraz większym stopniu organizują ochronę procesów związanych z technikami operacyjnymi (OT). Zabezpieczenie przemysłowych systemów kontroli przed cyberzagrożeniami to jeden z priorytetów dla osób zarządzających tym obszarem. Tym problemom zostało poświęcone badanie przeprowadzone przez Fortinet wśród osób odpowiedzialnych za techniki operacyjne w przedsiębiorstwach z branż: produkcyjnej, energetycznej, użyteczności publicznej, ochrony zdrowia i transportowej.

Skala ataków jest ogromna

Z wydanego na podstawie badania *Raportu o stanie bezpieczeństwa technik operacyjnych* wynika, że tylko 8% firm w ciągu ostatnich 12 miesięcy nie zaobserwowało żadnego przypadku naruszenia bezpieczeństwa technik operacyjnych. W tym samym czasie 90% respondentów doświadczyło co najmniej jednego włamania, 72% – trzech lub więcej włamań, a 26% – sześciu lub więcej włamań.

Ponad połowa badanych (51%) przyznała, że w wyniku ataków ich firma odnotowała spadek wydajności, 37% stwierdziło, że przestoje operacyjne miały wpływ na osiągane dochody. Według 39% ankietowanych atak miał wpływ na fizyczne bezpieczeństwo, co stanowi poważny problem, biorąc pod uwagę charakter pracy i strategiczne znaczenie obiektów przemysłowych.

Wśród najczęstszych rodzajów zagrożenia wymieniano użycie złośliwego oprogramowania (60%), *phishing* (43%), *ransomware* (37%), ataki typu DDoS (27%) oraz wewnętrzne naruszenia bezpieczeństwa informacji (18%).

CISO zajmie się bezpieczeństwem OT?

Osoby odpowiedzialne za techniki operacyjne w razie zaobserwowania problemów zazwyczaj zgłaszają się do osób wyższych rangą w przedsiębiorstwie, takich jak przedstawiciele zarządu czy dyrekcja. Zdecydowana większość z nich (80%) jest również regularnie zaangażowana w podejmowanie decyzji dotyczących cyberbezpieczeństwa (przy czym połowa ma prawo do ostatecznego głosu), a 71% jest regularnie zaangażowanych w strategię bezpieczeństwa IT.

Warto zwrócić uwagę, że kwestie związane z bezpieczeństwem OT wkrótce staną się obowiązkiem CISO (dyrektora ds. bezpieczeństwa informacji). Ta zmiana jest nieuchronna: większość (61%) respondentów oczekuje, że ich CISO przejmie wszystkie obowiązki związane z bezpieczeństwem OT w ciągu nadchodzącego roku. Jest to prawdopodobnie spowodowane zwiększonym ryzykiem związanym z coraz częściej obserwowanym łączeniem systemów OT i IT oraz ich wpływem na zachowanie ciągłości funkcjonowania przedsiębiorstwa.

Podstawowe środki cyberochrony nie występują powszechnie w infrastrukturach OT

Raport opracowany przez Fortinet ukazał również występowanie luk w zabezpieczeniach infrastruktury OT w wielu firmach. W 40-50% badanych przedsiębiorstw brakowało rozwiązań zapewniających bezpieczeństwo informacji i zarządzanie zdarzeniami (SIEM), technicznego centrum operacyjnego (TOC), centrum operacyjnego ds. bezpieczeństwa (SOC), sieciowego centrum operacyjnego (NOC), wewnętrznej segmentacji sieci, kontroli dostępu do niej czy uwierzytelniania wieloskładnikowego.

Ponad połowa (58%) przedsiębiorstw dysponuje w 2020 r. wyższymi budżetami, natomiast 15% doświadcza spadków finansowych, co może być związane m.in. z utratą przychodów w związku z pandemią COVID-19.

Analiza bezpieczeństwa pozostaje wyzwaniem

Wśród najczęściej wykrywanych i zgłaszanych problemów z bezpieczeństwem znajdują się: podatności (64%), włamania (57%) oraz redukcja kosztów wynikająca z działań w zakresie cyberbezpieczeństwa (58%). Mniej niż połowa przedsiębiorstw (43%) raportuje wyniki analiz ryzyka, a połowa (50%) nie udostępnia rutynowo podstawowych danych nt. cyberbezpieczeństwa kadrze kierowniczej wyższego szczebla.

Jako jedne z najważniejszych rozwiązań z zakresu bezpieczeństwa wymieniano także narzędzia do analizy i monitorowania zagrożeń, przy czym większość respondentów (58%) umieściła je w pierwszej trójce.

Jednocześnie 53% badanych stwierdziło, że rozwiązania ochronne utrudniają elastyczność operacyjną, a według połowy ankietowanych powodują większy stopień skomplikowania środowiska technik operacyjnych.

Jako jedne z najważniejszych rozwiązań z zakresu bezpieczeństwa wymieniano narzędzia do analizy i monitorowania zagrożeń, przy czym większość respondentów (58%) umieściła je w pierwszej trójce

Cyberbezpieczeństwo czyli dobra i zła SI

Czasy mamy ciężkie, więc zaawansowane, a często też perfidne ataki wykorzystujące sztuczną inteligencję i uczenie maszynowe mnożą się jak grzyby po deszczu.

TEKST
Tomasz Jurczak

Pandemia rozochociła cyberprzestępców. Nasiliły się ataki na firmy świadczące usługi i na konsumentów, na koncerny i instytucje publiczne. Żniwo jest obfite, bo mnóstwo osób pozostających w domach przeniosło swoje życie i pracę do sieci.

Phishing na WHO

Jeden z najbardziej spektakularnych i perfidnych ataków hakerzy przypuścili na Światową Organizację Zdrowia (WHO), której rola w globalnej walce z koronawirusem jest pierwszoplanowa. Wykorzystując powszechne zamieszanie i niepewność, przestępcy, by wyłudzić od ludzi dane, zastosowali *phishing*. W fałszywych mailach z logo WHO, które rozsyłali, informowali o najczęstszych objawach zarażenia koronawirusem i zachęcali do pobrania dokumentu na temat sugerowanych przez organizację środków bezpieczeństwa. Link przekierowywał użytkownika na stronę przypominającą serwis WHO, zawierającą m.in. prośbę o zweryfikowanie adresu e-mail oraz podanie hasła do skrzynki. W ten sposób przestępcy zyskiwali dostęp do danych logowania ofiary.

W maju br. firma Kaspersky poinformowała o serii ataków na organizacje przemysłowe w różnych regionach świata. Ich celem były systemy w Japonii, Włoszech, Niemczech oraz Wielkiej Brytanii, głównie należące do podwykonawców. Grozi to nie tylko utratą poufnych danych, lecz także atakami na przedsiębiorstwa za pośrednictwem używanych w firmach narzędzi zdalnej administracji.

Wyścig po bezpieczeństwo

Coraz częstsze są też akcje *phishingowe* skierowane na użytkowników popularnych usług VOD, firmy kurierskie czy sklepy internetowe. Atakujący podszywają się pod firmy i organizacje, wykorzystując, jak w przypadku WHO, niebezpieczne linki lub tzw. steganografię, czyli zaszywanie niebezpiecznych linków w metadanych obrazków.
Zażegnaniem problemu mogą być rozwiązania z obszaru SI. Jak wskazuje raport Capgemini z 2019 r., firmy przyspieszają inwestowanie w systemy sztucznej inteligencji, by bronić się przed kolejną generacją cyberataków. Dwie trzecie z nich przyznaje, że bez SI nie będzie w stanie reagować na krytyczne zagrożenia. Rozwój technologii chmurowych, IoT i 5G oznacza większą liczbę urządzeń, sieci i interfejsów użytkownika końcowego, co wymusza na firmach używanie coraz lepszych systemów ochrony i szybkiego reagowania. Eksperci stwierdzili w raporcie, iż unikalne możliwości tej technologii pozwalają organizacjom na ciągłe modyfikowanie parametrów wykrywania ataków. SI znajduje również zastosowanie w przewidywaniu zagrożeń, skanując ogromne ilości danych. Gorzej jest z automatyczną reakcją na te zagrożenia, choć i tu w najbliższych latach spodziewana jest poprawa.

Sztuczna inteligencja mogłaby wykrywać słabe i subtelne sygnały dotyczące nieznanych dotychczas niebezpieczeństw

Przykładem użycia przetwarzania kognitywnego jest np. Watson for Cyber Security – sztuczna inteligencja opracowana przez IBM

Rój botów i inne metody

W kwietniu brytyjski think tank Royal United Services Institute for Defence and Security Studies (RUSI) opublikował raport o zagrożeniach dla bezpieczeństwa narodowego Wielkiej Brytanii, wynikających z cyberataków z użyciem sztucznej inteligencji. O przygotowanie opracowania zwrócił się do RUSI brytyjski wywiad elektroniczny. Jeden z kilku wniosków zawartych w raporcie mówił o konieczności wykorzystania SI na rzecz cyberbezpieczeństwa, bo przestępcy nie zawahają się użyć jej przeciw Brytyjczykom.
Jak twierdzą eksperci, liczba zaawansowanych ataków, które wykorzystują sztuczną inteligencję i uczenie maszynowe, wyraźnie rośnie. Wiele współczesnych narzędzi przestępczych zawiera już funkcje pozwalające inteligentnie omijać oprogramowanie antywirusowe lub inne narzędzia wykrywania zagrożeń.

W ciągu kilku ostatnich lat wykształciła się na przykład nowa technika ataku nazywana rojem botów. Do atakowania w ten sposób sieci oraz podłączonych do nich urządzeń wykorzystuje się uczenie maszynowe i sztuczną inteligencję, które pomagają infiltrować sieci, blokować pracę wewnętrznych mechanizmów obronnych oraz wyszukiwać i wykradać dane – zauważa Paweł Wojciechowski, Business Development Manager w Fortinet.

Czynnik ludzki pozostanie

Eksperci RUSI zaznaczają, że dotychczas wykorzystywane narzędzia identyfikują znane już zagrożenia, natomiast sztuczna inteligencja mogłaby wykrywać słabe i subtelne sygnały dotyczące nieznanych dotąd niebezpieczeństw. Wspominają także o skuteczności algorytmów przetwarzania kognitywnego. Stosowane są one m.in. w semantycznych bazach danych, które rozpoznają obrazy, przetwarzają język i same się uczą.
Przykładem użycia przetwarzania kognitywnego jest np. *Watson for Cyber Security* – sztuczna inteligencja opracowana przez IBM. Uczy się znajdować powiązania między zagrożeniami i dostarczać wartościowych informacji na ich temat. W rezultacie na zagrożenia można reagować szybciej, ponosząc przy tym mniejsze ryzyko.
Skuteczność sztucznej inteligencji w cyberbezpieczeństwie nie wynika jednak wyłącznie z jej zdolności do zastępowania człowieka. Czynnik ludzki, jego wiedza i nadzór, pozostaje kluczowy.
SI jest naszym sprzymierzeńcem w walce z cyberzagrożeniami. Pozwala porządkować ogromną ilość danych, szybciej wykrywać nowe zagrożenia czy kolejne warianty złośliwego oprogramowania – zauważa Paweł Wojciechowski. *Już teraz pomaga m.in. w gromadzeniu i analizowaniu zdarzeń w sieci, dzięki czemu można wychwytywać zjawiska odbiegające od normy. Używana jest też w statycznej i dynamicznej analizie zagrożeń typu zero-day* (to zagrożenia i ataki przeprowadzone, zanim firmy zdążą przygotować odpowiednią aktualizację, czyt. załatają dziurę w systemie – red.) *w automatycznej ochronie urządzeń końcowych czy aplikacjach webowych. Ważne, by takie rozwiązania miały zdolność samokształcenia, co poprawi skuteczność analizy danych i umożliwi lepsze reagowanie na anomalie w sieci.*

Wetware, czyli dwa w jednym

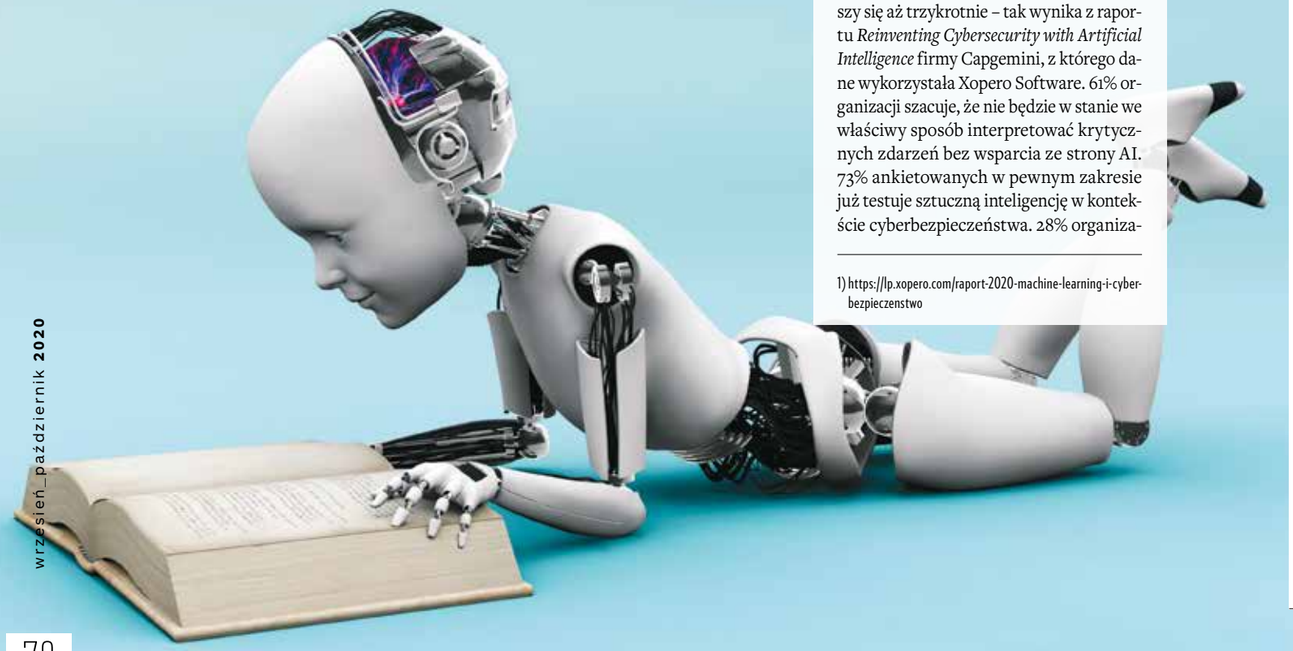
Sztuczna inteligencja jako przede wszystkim narzędzie (systemy eksperckie, analizatory czy sieci neuronowe) może zostać użyta i w dobrym, i w złym celu – podkreśla Łukasz Formas z firmy Sophos. – *Skomplikowane systemy i algorytmy mogą budować zabezpieczenia, ale także je łamać. Obie strony barykady coraz lepiej rozwijają tę technologię.*
Uczenie maszynowe pomaga dziś chronić systemy i sieci, wykrywać złośliwe aktywności, zagrożenia i anomalie. Cyberprzestępcy wykorzystują je z kolei np. do tworzenia przekonujących, lecz fałszywych treści w atakach opartych na socjotechnice.
Algorytmy bazujące na sieciach neuronowych mogą udawać głos danej osoby czy generować sfałszowane wideo. Tego typu deep fakes mogą stwarzać coraz większe zagrożenie, bo odróżnienie ich od prawdziwych informacji będzie coraz trudniejsze. W przyszłości mogą też przyczyniać się do rozwijania bardziej zautomatyzowanych socjotechnik i ataków zwanych wetware, czyli łączących automatyczne tworzenie treści z działaniami człowieka. Systemy maszynowe świetnie sprawdzają się bowiem w analizie dużych ilości danych, ale trudno wymagać od nich abstrakcyjnego myślenia. Ono nadal pozostaje domeną ludzi – dodaje Łukasz Formas.

Artykuł ukazał się na portalu www.sztucznainteligencja.org.pl

Sztuczna inteligencja i uczenie maszynowe w cyberbezpieczeństwie

– marketingowa mrzonka czy realny potencjał?

Od początku epoki cyfrowej naukowcom towarzyszyło marzenie nauczenia maszyn myślenia i podejmowania decyzji w sposób, w jaki robią to ludzie. Jednak uczenie maszynowe to nic innego jak zespół technik matematycznych, które pozwalają przetwarzać dane, odkrywać wzorce i wyciągać wnioski. Wszystko po to, aby adekwatnie przewidywać przyszłe zdarzenia, w tym cyberataki.



Sztuczna inteligencja (AI – *artificial intelligence*) *i* uczenie maszynowe *(machine learning)* w mniejszym bądź większym stopniu wpłynęły właściwie na każdą branżę: od produkcji, przez rolnictwo, po finanse. Jaki potencjał drzemie w tej technologii w kontekście bezpieczeństwa IT? Czy AI przekłada się na rzeczywisty wzrost cyberbezpieczeństwa? Na te pytania spróbowali odpowiedzieć specjaliści z firmy Xopero Software w swoim raporcie *Machine Learning i Cyberbezpieczeństwo*[1].

W latach 2017–2023 ruch w Internecie zwiększy się aż trzykrotnie – tak wynika z raportu *Reinventing Cybersecurity with Artificial Intelligence* firmy Capgemini, z którego dane wykorzystała Xopero Software. 61% organizacji szacuje, że nie będzie w stanie we właściwy sposób interpretować krytycznych zdarzeń bez wsparcia ze strony AI. 73% ankietowanych w pewnym zakresie już testuje sztuczną inteligencję w kontekście cyberbezpieczeństwa. 28% organizacji korzysta z rozwiązań, które posiadają wbudowane moduły, 30% – z własnych wypracowanych algorytmów, a pozostałe 42% w ciągu kolejnych dwunastu miesięcy zaczną stosować gotowe rozwiązania lub własne algorytmy.

1) https://lp.xopero.com/raport-2020-machine-learning-i-cyberbezpieczenstwo

Sztuczna inteligencja w biznesie, czyli jak zaimplementować AI w firmie?

Raport *Machine Learning i Cyberbezpieczeństwo* przybliża pięć kolejnych etapów wdrożenia AI w firmie. Pierwszym zadaniem jest przygotowanie zbioru danych dobrej jakości, na których podstawie będzie można testować modele uczenia maszynowego. Badania pokazują jednak, że dla blisko połowy firm jest to największe wyzwanie podczas implementacji AI. Problemy pojawiają się także w trakcie integracji rozwiązania z infrastrukturą IT, wykorzystywanymi systemami danych i aplikacjami. Kolejnym wyzwaniem jest płynna aktualizacja danych, na których pracują algorytmy. Następnym krokiem jest dobór odpowiednich zbiorów use case. W tym zakresie warto rozważyć współpracę z platformami zewnętrznymi (np. Facebook Threat Exchange czy IBM X-Force Exchange). Ważnym elementem wdrożenia AI jest również zatrudnienie odpowiednio wykwalifikowanych analityków.

Ogromną barierą w rozwoju sztucznej inteligencji jest brak specjalistów posiadających wiedzę z zakresu uczenia maszynowego. Firmy mają w zasadzie do wyboru dwie drogi: szkolenie własnych pracowników lub skorzystanie z zespołów zewnętrznych. Ostatnim krokiem w procesie jest wprowadzenie mechanizmów kontroli – zdefiniowanie roli i zakresu obowiązków czy wdrożenie odpowiednich procesów monitorujących i naprawczych.

Uczenie maszynowe dla każdego? Czy małe firmy mogą sobie pozwolić na eksperymenty ze sztuczną inteligencją?

– *Wdrożenie w organizacji AI pochłania znacznie więcej zasobów – ludzi oraz nakładów finansowych – niż rozwiązania tradycyjne. Nie da się ukryć, że produkty oparte na frameworkach AI należą także do tych kosztowniejszych* – mówi Karolina Dzierżyńska, redaktor Centrum Bezpieczeństwa w Xopero Software. – *Dla małych i średnich firm mogą więc okazać się nieosiągalne. Mniejsze podmioty mogą jednak skorzystać z rozwiązań udostępnianych w modelu SECaaS (security-as-a-service).*
Wykorzystanie elementów sztucznej inteligencji w podstawowych produktach z branży cyberbezpieczeństwa, takich jak programy antywirusowe, sprawia więc, że są one dostępne dla każdego – małych firm, a nawet użytkowników domowych.

Uczenie maszynowe a cyberbezpieczeństwo

Podstawowym celem uczenia maszynowego jest analiza ogromnych zbiorów danych i automatyzacja jak największej liczby procesów. Coraz częściej sięga się po nią przy projektowaniu systemów bezpieczeństwa IT. Monitorowanie zachowań użytkowników w sieci, analiza parametrów z urządzeń sieciowych i logów użytkowników, analiza behawioralna czy wykorzystanie danych biometrycznych – to tylko kilka aspektów jej wykorzystania.
System bezpieczeństwa oparty na uczeniu maszynowym musi więc ustalić, czy każdy plik przesyłany siecią firmową nie zawiera *malware*, czy każda próba logowania nie jest wynikiem wykradzenia danych uwierzytelniających, a każdy mail nie jest wiadomością *malspam*. Ponadto zweryfikuje, czy każde żądanie nie jest próbą ataku *denial-of-service* (DoS) albo próbą kontaktu z serwerami C&C. Sztuczna inteligencja również może zostać wykorzystana do detekcji anomalii czy analizy *malware*. W jaki sposób? Algorytmy uczenia maszynowego mogą dokonać dynamicznej analizy na podstawie podobieństw między dwoma lub więcej obiektami. Takie badanie omija błędy typowe dla dopasowań statycznych i uwzględnia np. rozwój *malware* w czasie.

Druga strona medalu

Należy pamiętać, że sztuczna inteligencja i uczenie maszynowe mogą zostać wykorzystane po drugiej stronie barykady i posłużyć przestępcom do przeprowadzenia ataków opartych na szczegółowej analizie danych. Na szczęście nie są one jeszcze powszechnie stosowane, przestępcy wolą bowiem sprawdzone rozwiązania, które przyniosą im zyski szybko i tanio. Niewykluczone jednak, że wraz z upowszechnianiem się uczenia maszynowego i sztucznej inteligencji wkrótce usłyszymy o spektakularnych atakach z ich wykorzystaniem. □

Przetrwają odporni

cz. 4

BUDOWANIE ODPORNOŚCI MIEJSKIEJ TO ZADANIE DLA MIAST RÓŻNEJ WIELKOŚCI. NAJCZĘŚCIEJ ROZWAŻA SIĘ JĄ W KONTEKŚCIE MEGAPOLIS, A TAKICH W EUROPIE WŁAŚCIWIE NIE MA. PARYŻ I LONDYN ZBLIŻAJĄ SIĘ DO NICH, ALE JEDYNIE W UJĘCIU CAŁYCH AGLOMERACJI. O SWOJE PRZETRWANIE POPRZEZ ŚWIADOME BUDOWANIE ODPORNOŚCI MUSZĄ WALCZYĆ WSZYSTKIE MIASTA, BEZ WZGLĘDU NA WIELKOŚĆ.

Pandemia wymusza konkret, pandemia weryfikuje!

TEKST
Jacek Tyburek

Mniejsze miasta to inna skala problemu i inne metody działania. Porównując funkcjonowanie takich metropolii jak Seul, Singapur czy nawet Nowy Jork do średniej wielkości miast europejskich, ma się wrażenie, że to zupełnie inny świat, również w sensie zarządzania podczas pandemii. Przyjrzyjmy się więc dwóm miastom z Wysp Brytyjskich: Bristolowi i Glasgow. To miasta średniej wielkości, dynamicznie rozwijające się, włączające do swoich strategii rozwojowych programy odporności miejskiej.

Glasgow

Glasgow w 2019 r. liczyło ponad 633 tys. mieszkańców[1], całą metropolię Greater Glasgow zamieszkiwało około 1,2 mln osób. Strategia odporności miasta opiera się na czterech filarach i piętnastu celach, które wyznaczają długoterminową trajektorię Glasgow Resilience. W ich ramach zidentyfikowano czterdzieści dziewięć działań, które mają zostać wdrożone w najbliższych dwóch latach.

Filar pierwszy za cel działań stawia:
- zagwarantowanie równego dostępu do wysokiej jakości lokalnych usług, które sprzyjają dobrobytowi,
- wzmocnienie pozycji liderów społeczności lokalnej dzięki współpracy między partnerami miast a trzecim sektorem,
- wykorzystanie istniejących zasobów do stworzenia zdrowej, bezpiecznej i sprzyjającej integracji przestrzeni zmniejszającej izolację społeczną,
- możliwość wpływania na program rządu szkockiego na odporność społeczną.

Drugi filar strategii zawiera się w postulacie stworzenia przykładu odporności mierzącej się z lokalnymi skutkami zmian klimatu i uwolnienia potencjału pustych miejsc. Wymienia się:
- poprawę jakości powietrza i zmniejszenie emisji dwutlenku węgla,
- połączenie infrastruktury transportowej firmowej i publicznej,
- dostępność niedrogich ekologicznych sposobów przemieszczania się mieszkańców Glasgow,
- efektywną energetycznie przyszłość,
- inwestycje i miejsca pracy w społecznościach lokalnych,
- dobry dostęp do infrastruktury fizycznej i cyfrowej.

Trzeci filar jest ukierunkowany na ekonomiczny rozwój Glasgow. Jego celem jest wspieranie nowych rozwiązań miejskich i firm, nauka oparta na najlepszych praktykach i podnoszenie umiejętności mieszkańców. Cel ma zostać zrealizowany dzięki:
- ułatwieniom rozwoju kreatywnych i innowacyjnych rozwiązań miejskich, które zwiększają wartość fizyczną, społeczną i ekonomiczną tkanki Glasgow,
- nowemu podejściu do przedsiębiorczości, wspieraniu rozwoju firm,
- założeniu postindustrialnej podgrupy miasta z partnerami 100RC, aby dzielić się najlepszymi praktykami i uczyć się od nich,
- przeciwdziałaniu ubóstwu, w tym ubóstwu wśród osób pracujących, zapobieganiu skutkom ubóstwa oraz łagodzeniu ich,
- stałemu doskonaleniu i zdobywaniu nowych umiejętności osób w wieku produkcyjnym.

Czwarty filar strategii odporności Glasgow koncentruje się wokół aktywizacji mieszkańców do ich głębszej partycypacji w budowę odpornego miasta.

Bristol

Bristol to wysoko rozwinięte i w ostatnich latach intensywnie rozwijające się miasto w południowo-zachodniej Anglii liczące ponad 460 tys.[2] mieszkańców. To dziewiąte co do wielkości miasto w Wielkiej Brytanii, bardzo zróżnicowane pod względem etnicznym, religijnym i językowym.

Strategia Bristol Resilience obejmuje dynamiczną wizję tego, jak Bristol może wyglądać za 50 lat. Określa zakres działań chroniących miasto przed potencjalnymi wstrząsami i stresami w przyszłości. Zakłada rozwiązywanie najważniejszych problemów Bristolu, takich jak zakorkowane ulice, drogie mieszkania, zanieczyszczone powietrze i ubóstwo społeczne, zwłaszcza eliminowanie skutków ubóstwa dzieci. Przyjęte założenia mają dać ludziom większy wpływ na decyzje podejmowane przez samorządy. Dokument został sporządzony przy pomocy lokalnych interesariuszy i stanowi uzupełnienie nowej Strategii Korporacyjnej na lata 2017–2022. Wdrażanie strategii odporności będzie nadzorowane przez nowy urząd miasta, skupiający kluczowych interesariuszy i organizacje z całego miasta w celu wypracowania rozwiązań w najważniejszych kwestiach.

Opracowując ambitną długoterminową perspektywę, Bristol dołącza do innych myślących przyszłościowo globalnych miast w 100 Resilient Cities Network, w tym Nowego Jorku, San Francisco, Rotterdamu i Rio de Janeiro, które już nakreśliły swoje plany na przyszłość. Strategia opiera się na pięciu wizjonerskich filarach opisujących wyniki, jakie miasto ma nadzieję osiągnąć.

1. Filar oznaczony kodem **Miasto uczciwe** – zgodnie z nim każda osoba mieszkająca w Bristolu ma atuty i możliwości, aby cieszyć się wysokim poziomem życia.
2. Kod **Miasto dobre do zamieszkania** – centrum miasta i dzielnice mają być wspaniałymi miejscami do życia, pracy, nauki i zabawy dla osób w każdym wieku.
3. Kod **Zrównoważony rozwój** – miasto i region prosperują w granicach środowiskowych dzięki przyjmowaniu nowych zachowań i technologii.
4. Kod **Smart city** – obywatele i władze Bristolu podejmują skuteczne decyzje oparte na wspólnie ustalonych priorytetach i informacjach w czasie rzeczywistym.
5. Kod **Integracja mieszkańców** – silna sieć społeczności i organizacji lokalnych promuje zaufanie, współpracę i wspólne działania w całym mieście.

Pandemia koronawirusa

Wielka Brytania ma niejednoznaczną historię przechodzenia przez pierwszą falę pandemii. Począwszy od całkowitego zignorowania zagrożenia, łącznie z wygłoszeniem przez premiera Borisa Johnsona (niegdyś popularnego mera Londynu) tezy, że to tylko kolejny wirus, na którego trzeba się uodpornić, po zupełną zmianę przekazu, gdy odnotowano kilka przypadków zachorowania wśród członków rządu, a premier ciężko przechodził chorobę. Ponieważ temat dotyczy Wielkiej Brytanii, jednej z kolebek współczesnej standaryzacji, rząd w maju 2020 r. opublikował dokument *OUR PLAN TO REBUILD: The UK Government's COVID-19 recovery strategy.*

Taka właśnie jest Wielka Brytania. Za jej podejście do problemu my, bezpiecznicy, powinniśmy ten kraj darzyć szczególnym szacunkiem. Tam bardzo szczegółowo bada się istotę zdarzenia czy zjawiska oraz szuka, w sposób usystematyzowany, metodyczny rozwiązań i rekomendacji. Fraza *recovery strategy* powinna być szczególnie bliska każdemu specjaliście od bezpieczeństwa i odporności organizacji.

1) https://statistics.gov.scot/

2) https://www.bristol.gov.uk/

Przyjęte przez brytyjskie miasta metody reakcji promują działania społeczne, rozwiązania technologiczne stanowią opcję drugiego wyboru

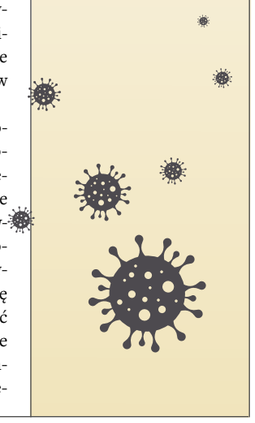
Nie będę opisywał cudów techniki, które miałyby pomóc przejść przez okres pandemii z możliwie najmniejszymi stratami. Zaprezentuję inne podejście. Znacznie bardziej analityczne, stawiające na regulacje administracyjne, wyznaczające kierunki rekomendacjami i działaniami standaryzującymi działania oraz premiujące wysiłki wspólnoty. Nie jest moją ambicją oceniać, co może być bardziej skuteczne. Stoimy u progu potencjalnej drugiej fali pandemii. Nie wiemy, co się wydarzy. Z tego punktu widzenia nasycanie miasta technologiami versus budowanie struktur jest intelektualnie bardzo ciekawą rozgrywką.

Co przewiduje strategia Wlk. Brytanii?

Zaproponowano czternaście programów wspierających. Aby zwiększyć zaufanie w zarządzaniu nowymi przypadkami, rząd UK musi nadal realizować założenia narodowego systemu zdrowia (*National Health System – NHS*) i zapewniać opiekę zdrowotną na trwałych podstawach, udostępniając pracownikom odpowiednie środki ochrony indywidualnej (ŚOI) we wszystkich placówkach służby zdrowia i opieki.

Priorytetem rządu w zakresie opieki społecznej dla dorosłych jest kontrola zakażeń podczas pandemii COVID-19. Szczególnie narażone są domy opieki dla osób starszych, ponieważ ich mieszkańcy są najbardziej podatni na zakażenie ze względu na wiek i choroby współistniejące, a także zamknięty charakter tych instytucji, co wpływa na szybkie rozprzestrzenianie się wirusa. W kwietniu rząd opublikował kompleksowy plan działań, mający na celu wsparcie 25 tys. różnych dostawców opieki społecznej przez cały czas epidemii COVID-19, w tym przeprowadzanie testów czy kontrolę dostarczania środków ochrony indywidualnej.

W Wielkiej Brytanii zidentyfikowano około 2,5 mln osób, które są szczególnie podatne na zakażenie koronawirusem. Zalecano im pozostawanie w domu i unikanie bezpośredniego kontaktu do końca czerwca. Rząd i władze lokalne zaoferowały dodatkowe wsparcie, w tym dostawę żywności i podstawowych produktów, opiekę i dostęp do leków, jeśli nie mogą uzyskać pomocy rodziny i przyjaciół. Jednym ze sposobów na ograniczenie skutków pandemii i ukierunkowanie się na ograniczenia społeczne jest zrozumienie poziomów ryzyka w różnych grupach populacji.



Sukces każdej strategii opartej na usuwaniu obecnych ograniczeń społecznych przy jednoczesnym utrzymaniu epidemii na możliwym do zarządzania poziomie będzie zależał od zdolności rządu do dokładnego monitorowania pandemii, a także szybkiego wykrywania i zwalczania dużej części ognisk. Będzie to szczególnie trudne w miesiącach zimowych, biorąc pod uwagę, że COVID-19 ma wiele objawów przeziębienia i grypy.

Rząd ogłosił jeden z najbardziej hojnych i wszechstronnych pakietów wsparcia na świecie, zapewniający bezpieczeństwo i pomoc osobom chorym lub niezdolnym do pracy oraz pomoc pomostową dla firm w celu ochrony miejsc pracy. Zwiększono wsparcie oferowane poprzez system zasiłków na pokrycie kosztów mieszkaniowych i dla osób samozatrudnionych, wprowadzono moratorium na eksmisje w sektorze prywatnego wynajmu mieszkań, utworzono nowy fundusz ubóstwa i zapewniono wsparcie osobom żyjącym w trudnych warunkach. Kredytodawcy oferują wakacje hipoteczne dla kredytobiorców borykających się z trudnościami finansowymi i niezdolnych do spłaty w wyniku COVID-19.

Brytyjczycy postawili na planowanie, szczegółowe wytyczne w stylu British Standard, z rozpisaniem ram działania. Liczba powstałych dokumentów i inicjatyw jest imponująca. Większość z nich to efekt refleksji po pierwszej fali wirusa i jego konsekwencji dla ekonomii i życia społecznego. Powstające inicjatywy współpracy na rzecz zabezpieczenia mieszkańców przed kolejnymi skutkami pandemii i ciała zarządzające do złudzenia przypominają zespoły robocze ds. tworzenia strategii odporności miejskiej.

Pewnym zaskoczeniem jest inicjatywa dotycząca zadbania o sprawną dystrybucję żywności. Przed obecną pandemią Rada Miasta Bristolu (BCC) była na zaawansowanym etapie wdrażania ambitnego planu *One City,* z kampanią *Going for Gold* (*GFG*) – jednego z kluczowych projektów. BCC dąży do uzyskania złotego statusu w ramach inicjatywy *Sustainable Food Places,* prowadzonej przez Food Matters we współpracy z Soil Association and Sustain. To uczyniłoby Bristol pierwszym miastem, które uzyskało to wyróżnienie. BCC prowadzi ogólnokrajowe działania na rzecz rozwoju społecznego i gospodarczego, skupione wokół długoterminowego podtrzymywania sektora spożywczego w Bristolu, a także zapewnienia poprawy zdrowia publicznego.

Aby osiągnąć status określony jako Gold, miasto musi wykazać postęp w trzech kluczowych obszarach: zrównoważony catering i zaopatrzenie, zredukowanie otyłości wśród dzieci i ograniczenie marnotrawstwa żywności. Bristol ma dobrze prosperującą sieć małych restauracji, kawiarni i niezależnych sprzedawców detalicznych, oferujących szeroki wybór dań i możliwości zakupów dla mieszkańców. Sukces kampanii wzmocniłby i rozszerzył istniejącą sieć, a także otworzył możliwości dla nowych lokalnych przedsiębiorstw spożywczych. Nadrzędnym celem jest stworzenie w Bristolu sieci żywienia zbiorowego obejmującego etyczną, zrównoważoną produkcję i opartego na zdrowej diecie.

Wybuch epidemii uwypuklił znaczenie lokalnych przedsiębiorstw spożywczych i dostawców zarówno w Bristolu, jak i w całym kraju. W efekcie kampania GFG zyskała na znaczeniu dla przyszłości miasta i jako sztandarowy projekt, na którym władze innego miasta mogą oprzeć swoją politykę dotyczącą sektora spożywczego. Po wygaszeniu pandemii konieczna będzie drastyczna restrukturyzacja, zapewniająca przetrwanie wielu przedsiębiorstw i sieci gastronomicznych zarówno dużych organizacji komercyjnych, jak i małych niezależnych. W przyszłości miasto ma również zadbać o powszechną dostępność żywności dobrej jakości. Kampania GFG jest projektem w toku i po powrocie do normalności BCC mogłoby zintegrować dalsze środki na zwiększenie odporności istniejących systemów żywienia zbiorowego na przyszłe trudności i zakłócenia.

Pandemia COVID-19 spowodowała, że wiele firm zmieniło swoje modele biznesowe, dostosowując się do sytuacji, a to może mieć korzystny wpływ na ożywienie gospodarcze. Jednak ważne jest to, aby rząd nadal wdrażał politykę wspierającą transformację cyfrową i umiejętności MŚP. Jeszcze przed pandemią Wlk. Brytania stanęła w obliczu niepokojącej luki w umiejętnościach cyfrowych, która teraz się pogłębiła. Milionom ludzi i znacznej liczbie firm brakuje niezbędnych umiejętności cyfrowych, co grozi pogłębieniem podziałów społecznych i ma wpływ na konkurencyjność Wielkiej Brytanii. Pandemia COVID-19 przyspieszy powszechne zastosowanie Internetu Rzeczy (IoT), sztucznej inteligencji (AI), 5G i pełnego dostępu szerokopasmowego. Nieprzygotowani do korzystania z nowych technologii znajdują się w niekorzystnej sytuacji, szczególnie w dostępie do pracy i usług publicznych.

Idea *smart city*

Profesor Paweł Kubicki z UJ w artykule „Odporność miast musi być oparta na wspólnocie" pisze: *Siłą miast zawsze było to, że ich przedsiębiorczość miała silne oparcie we wspólnocie. Także w okresie przed pandemią można było obserwować zwrot w takim kierunku. Rozwijała się ekonomia współdzielenia, kooperatywy: ogrodnicze, spożywcze, mieszkaniowe itp., także korporacje coraz bardziej zwracały uwagę na społeczną odpowiedzialność biznesu* (CSR). *Wciąż jednak stanowiło to niszę. Patrząc z obecnej perspektywy, to w takim modelu gospodarki miejskiej można upatrywać przyszłości miast. Prawdziwymi resilient cities będą te, których siła i odporność wynika z ducha wspólnoty.*

Według prof. K. Kubickiego pandemia powinna sprzyjać faktycznemu zastosowaniu idei *smart city.* Inteligentne czy raczej sprytne miasto wymyśla sposoby, jak zapewnić jakość życia mimo kurczących się dochodów. Dotychczasowe praktyczne zastosowanie idei *smart city* nie kojarzyło się z kreatywnością, ale raczej z „błyskotkami" – drogimi, jednak mało funkcjonalnymi inwestycjami.

Inicjatywy Bristolu

Miasto we współpracy z partnerami wydało 30 czerwca br. dokument *Bristol Local Outbreak Management Plan*, który jest planem dla miasta i jednocześnie częścią sieci planów władz lokalnych w Anglii. Zapewnia ramy następnej fazy życia z koronawirusem. Obejmuje następujące inicjatywy:

- *Bristol One City Partnership* – biuro w Bristolu koordynuje prace mające na celu wsparcie miasta i rady w odpowiedzi na kryzys COVID-19 oraz rozpoczęcie prac nad strategią pomocy. Urząd miejski przygotowuje zintegrowane, obejmujące całe miasto podejście do naprawy oparte na celach zrównoważonego rozwoju ONZ. Zorganizował szereg warsztatów i seminariów internetowych z partnerami miejskimi ze wszystkich sektorów, aby reakcja całej wspólnoty na COVID-19 była holistyczna.
- *Bristol Health and Wellbeing Board* – Rada kieruje pracami nad poprawą zdrowia i zmniejszeniem nierówności w dostępie do usług medycznych w Bristolu. Jej członkowie wywodzą się z sektora publicznego, wolontariatu i *Bristol Race Commission*. Interesuje się zarówno bezpośrednim wpływem wirusa na społeczeństwo, jak i szerszym jego wpływem na zdrowie całej populacji oraz pogłębiające się nierówności.

Reakcja na COVID-19

W miarę łagodzenia ograniczeń Rada Miejska Bristolu odgrywa kluczową rolę we wspieraniu powrotu do normalnego życia miasta (w miarę możliwości), jednocześnie chroniąc mieszkańców przed rozprzestrzenianiem się choroby. Opracowano plany pomocy dla miejskich usług i lokalnego biznesu oraz osób słabszych społecznie i zdrowotnie.

Glasgow, oprócz programów społecznych i wspólnotowych realizowanych (podobnie jak Bristol) poprzez Izbę Gospodarczą Glasgow, promuje możliwie jak najszersze wykorzystanie technologii. W wyniku COVID-19 na masową skalę zastosowano najnowsze rozwiązania umożliwiające kontakty z rodziną, przyjaciółmi, nauczycielami czy współpracownikami. Internet Rzeczy (IoT) to kluczowy element składowy inteligentnych miast – bezpiecznej pracy i reanimowania gospodarki światowej. Wdrożenie IoT nie tylko ma kluczowe znaczenie w powstrzymywaniu rozprzestrzeniania się wirusa, ale także może przyspieszyć ożywienie gospodarcze. Dlatego decydenci na szczeblach lokalnym, regionalnym i krajowym powinni rozpocząć planowanie strategii inteligentnego miasta z IoT.

Zarówno dzisiaj, gdy jest wdrażany w rozwiązaniach technicznych pomocnych w zapewnianiu dystansu społecznego i niezbędnego wczesnego ostrzegania, jak i bardziej futurystycznych, ale już możliwych do zrealizowania, czyli szerszego zastosowania robotów w usługach publicznych.

Podsumowując, podane przykłady brytyjskich miast, przyjęta przez nie perspektywa i metody reakcji promują raczej działania społeczne, natomiast odważne rozwiązania technologiczne stanowią opcję drugiego wyboru – przynajmniej teraz, u wrót jesieni 2020, kiedy nie można przewidzieć kierunków dalszego rozwoju pandemii. □

BIO

Jacek Tyburek

Menedżer bezpieczeństwa organizacji. Doświadczenie zdobywał w różnych obszarach bezpieczeństwa; od przemysłu i logistyki, przez BPO, po bezpieczeństwo w rzeczywistości wirtualnej. Promotor pojęcia *Organisational Resilience*. Entuzjasta bezpieczeństwa miast, realizujący swoją pasję w powstającej pracy doktorskiej.

Regaty
DMSI CUP 2020

Trzecia edycja regat DMSI CUP 2020 odbyła się 14-16 września br. Ta impreza plenerowa o charakterze integracyjno-sportowym kolejny raz gościła w Rynie w ośrodku Bocianie Gniazdo na Szlaku Wielkich Jezior Mazurskich.

Organizatorem regat była firma DMSI Software – dostawca platformy chmurowej do monitoringu i zarządzania bezpieczeństwem Safestar. Partnerami były firmy: CBC Poland, Genevo oraz Linc Polska. Pierwszego dnia partnerzy imprezy zaprezentowali własne prezentacje, nagrodzili też swoich klientów. Wśród wyróżnionych firm znalazły się: Alfa Group, Dogmat, Nova System, Safespace, Security Gdańsk, Security Office Rzeszów, SPIE Polska, Taurus Ochrona Group.

W części artystycznej wystąpił zespół Korzuh, z którym uczestnicy bawili się do późnej nocy.

Przy fantastycznej pogodzie drugiego dnia rozegrano zawody. Regaty wygrała drużyna w składzie: Marek Ważny i Wojciech Górecki (Security Gdańsk), Sebastian Cybulski (Alfa Group), Beata Trzebiatowska (Genevo). Zwycięzcom wręczono statuetki, a wszyscy uczestnicy otrzymali pamiątkowe medale.

Organizator i partnerzy dziękują wszystkim uczestnikom i już dziś zapraszają na kolejne regaty w przyszłym roku.

Filmową relację z regat można obejrzeć na YouTubie (linki na stronie organizatora i portalu „a&s Polska”). □

DMSI Software

Zmiana terminu
Międzynarodowych Targów Zabezpieczeń SECUREX

Mając na uwadze najwyższą jakość biznesową wydarzeń organizowanych przez Grupę MTP, a także wsłuchując się w głosy wystawców, stowarzyszeń i pozostałych partnerów, z którymi współpracują Targi SECUREX, Zarząd Grupy MTP podjął decyzję o przełożeniu terminu Międzynarodowych Targów Zabezpieczeń SECUREX na 26-28 kwietnia 2021 r.

Zawsze dokładamy najwyższych starań, by organizowane przez Międzynarodowe Targi Poznańskie wydarzenia przynosiły ich uczestnikom maksymalne korzyści biznesowe. Jesteśmy przekonani, że organizacja targów w nowym terminie pozwoli jeszcze bardziej podnieść merytoryczną jakość imprezy i przyczyni się do obecności większej liczby odwiedzających ją specjalistów.

W imieniu całego zespołu organizacyjnego pragniemy wszystkim serdecznie podziękować za merytoryczne wsparcie, pomoc i zaangażowanie w organizację SECUREXU. Głęboko wierzymy, że nowy termin będzie odpowiedni dla wszystkich uczestników targów, które angażują tak liczne grono profesjonalistów. Czas dzielący nas od kolejnej edycji SECUREXU chcemy wykorzystać na stworzenie jeszcze ciekawszego programu, oferty targowej i platformy nawiązywania nowych relacji biznesowych. □

Zespół Targów SECUREX

Chroń. Zapobiegaj. Analizuj
Rozwiązania termowizyjne MOBOTIX

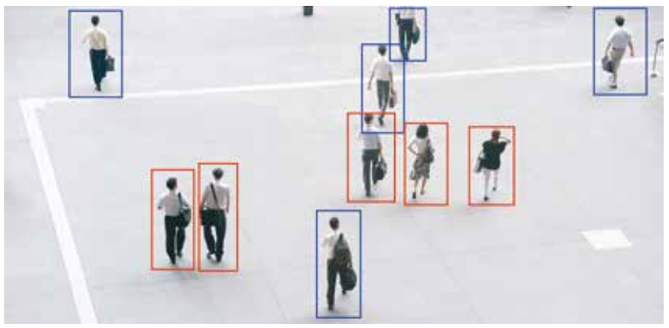
Technologia termowizyjna wraz ze swoimi unikatowymi cechami stała się niezbędnym elementem wielu systemów dozoru wizyjnego. Coraz większa liczba przedsiębiorstw, instytucji publicznych, władz oraz innych agencji stosuje technologię termowizyjną do ochrony swoich pracowników i klientów.

Inteligentny system wizyjny w połączeniu z wysokiej jakości przetwornikiem termowizyjnym pozwala w pełni wykorzystać potencjał kamery MOBOTIX M16 TR. Skrót „TR" oznacza technologię termowizyjno-radiometryczną. Innymi słowy, dzięki skalibrowanemu przetwornikowi obrazu kamera wykonuje pomiar promieniowania cieplnego dla każdego piksela na całym obszarze obserwowanego, zdefiniowanego obrazu.
Dokładność pomiarów temperatury zależy od zdolności emisyjnej danego obiektu oraz warunków, w jakich ten pomiar jest wykonywany. Kamera termowizyjna M16 automatycznie wyzwala alarm w momencie przekroczenia określonego progu temperaturowego, np. 37°C. Umożliwia to wczesne wykrycie sytuacji krytycznych, takich jak podwyższona temperatura ciała osób wchodzących do budynku lub powstrzymanie rozwoju pożaru na wczesnym jego etapie.
Zastosowanie tzw. ciała doskonale czarnego *(Black Body)* tuż obok obiektu, który jest poddawany pomiarowi, zapewnia odpowiednią wartość referencyjną pomiaru i poprawia jego dokładność. Im jest bliżej obiektu i im stabilniejsze są warunki otoczenia, tym dokładniejszy jest pomiar.
Aktualne informacje o możliwości zakupu gotowego zestawu termowizyjnego do pomiaru temperatury znajdują się na stronie internetowej www.linc.pl/oferta-specjalna-mobotix/. Zestaw zawiera kamerę termowizyjną M16 Thermal, z przetwornikiem obrazu światła widzialnego oraz ciało doskonale czarne Black Body.

Więcej na www.linc.pl

Hanwha Techwin udostępnia aplikację
do pomiaru dystansu społecznego

Firma Hanwha Techwin wprowadziła do oferty aplikację do pomiaru dystansu społecznego wykorzystującą analizę obrazu wspomaganą algorytmami AI i Deep Learning. Jej zadaniem jest wsparcie firm w zakresie spełniania wymagań zachowania odpowiedniego dystansu między osobami w obliczu pandemii COVID-19.



Opracowana przez firmę A.I. Tech – wielokrotnie nagradzanego partnera technologicznego Hanwha Techwin – aplikacja serwerowa precyzyjnie mierzy odległość między osobami znajdującymi się w polu widzenia kamery, a w razie nieprzestrzegania obowiązujących zaleceń zachowania odległości generuje stosowny alarm. Użytkownicy mogą również otrzymywać powiadomienia w sytuacji, gdy liczba osób w danym obszarze przekracza wyznaczony limit.
Aplikacja jest kompatybilna ze wszystkimi kamerami Wisenet. Stworzono ją z myślą o takich miejscach pracy, jak biura czy fabryki. Sprawdza się też w galeriach sztuki, muzeach, miejscach kultu religijnego. Działa dobrze zarówno wewnątrz budynków, jak i na terenie zewnętrznym. Oferuje bardzo skuteczne narzędzie wspomagające kontrolę przestrzegania zasad zachowania dystansu w środkach transportu publicznego czy w centrach miast, gdzie władze lokalne starają się monitorować ludzi gromadzących się licznie w popularnych lokalizacjach.
Aplikacja jest zintegrowana z oprogramowaniem VMS Wisenet WAVE. Użytkownicy mogą korzystać z panelu użytkownika oraz dashboardu A.I. Tech, który pozwala na przeglądanie i zarządzanie alarmami i zdarzeniami z wielu kamer. Dane można też przedstawiać w postaci wykresów, tabel i obrazów.
Ponadto informacje można z łatwością wyeksportować do formatu .csv, .jpeg lub .pdf na potrzeby systemów zewnętrznych. Dedykowany dashboard, do którego można uzyskać dostęp z komputera, smartfonu lub tabletu, jest w pełni konfigurowalny, dzięki czemu spełni praktyczne wymagania użytkowników.

Więcej na www.hanwha-security.eu/pl/

a&S POLSKA

Warsaw Security Summit

2020 ONLINE EDITION

PREMIERA: **17.11.2020**

Bezpieczeństwo w nowych czasach

T E M A T Y K A :

- → TRENDY SECURITY
- → HANDEL I USŁUGI
- → OFFICE, HOME OFFICE
- → INDUSTRY 5.0
- → NEW SECURITY MANAGEMENT

warsawsecuritysummit.eu

NOWA FORMUŁA NA NOWE CZASY

Nowatorska formuła **content hub** – wzorem serwisów VoD materiały wideo z konferencji od samej premiery będą dostępne w dowolnym czasie. Uczestnik sam decyduje: co, kiedy i w jakiej kolejności chce obejrzeć...