CZASOPISMO RYNKU SECURITY

a&S POLSKA

05
35
09/10
2022

PRZEMYSŁ 4.0

WYZWANIA OCHRONY

Kluczowym elementem ochrony obiektów przemysłowych wciąż jest człowiek, ale wsparty systemami zabezpieczeń z zaawansowanymi algorytmami. Pozwoli to zmniejszyć nie tylko liczbę fałszywych alarmów, ale też ryzyko popełniania błędów przez pracowników.

RYNEK SECURITY

SECURITY 4.0

Dział bezpieczeństwa na miarę Przemysłu 4.0 musi być jak Security 4.0! Wprawdzie nadal nie generuje przychodu, ale zapobiega stratom i kradzieżom, chroni przed przestojami produkcji i fałszywymi ewakuacjami. To zaś stanowi wymierny zysk dla przedsiębiorstwa.

BEZPIECZEŃSTWO BIZNESU

BADANIA ODPORNOŚCI ORGANIZACJI

Wiele organizacji nie ma jeszcze wykrystalizowanej wizji, jak i kto ma zarządzać ich odpornością biznesową. Warto zebrać wiedzę, która pomoże podjąć dojrzałe decyzje, przeprowadzając Przegląd Techniczny Bezpieczeństwa.

APLIKACJA MOBILNA

www.aspolska.pl

ISSN 2451-5175

9 772451 517703 05

15 zł
(w tym 8% VAT)

Drodzy Czytelnicy

Martwimy się o przyszłość. Niepokoją nas konsekwencje wojny w Ukrainie, rosnąca inflacja, wzrost przestępczości. Doszły nowe zagrożenia, na które nie byliśmy przygotowani, co wymusiło niestandardowe podejście do zabezpieczeń i ochrony. Bieżące wydanie zdominował temat bezpieczeństwa obiektów przemysłowych, a przemyślenia ekspertów (s. 36) docenią security managerowie z innych branż.

Zakłady przemysłowe, zazwyczaj stosujące mieszaną (techniczną i osobową) formę ochrony, stawiają przed zespołami ochronnymi najwięcej wyzwań. Kluczowym elementem systemu wciąż jednak pozostaje człowiek. Wsparcie techniczne, automatyzacja, zaawansowane algorytmy zmniejszają prawdopodobieństwo popełnienia przez niego błędów, ale wiąże się to z większymi nakładami na kompetencje pracownicze uwzględniające nie tylko kwestie security, ale także profil zakładu (s. 18).

Artykuł dotyczący zmian w paradygmacie bezpieczeństwa (w poprzednim wydaniu „a&s Polska") otworzył potrzebną dyskusję o roli „bezpiecznika"/security managera w organizacji. Co zatem powinien potrafić „bezpiecznik 4.0" w dobie „Security 4.0" (na wzór dziejącej się właśnie 4. rewolucji przemysłowej)? Jak wiele ze swoimi kompetencjami może wnieść do organizacji? (s. 24).

Termin „dane i analityka" (D&A) odnosi się do sposobów zarządzania informacjami, które wspierają podejmowanie decyzji i optymalizują procesy biznesowe w przedsiębiorstwie. Kontynuując tę trudną tematykę, przedstawiamy przewidywania analityków nt. przyszłości technologii D&A – fundamentalnie nową koncepcję zarządzania danymi i zmianę podejścia z analizy *big data* na *small* i *wide data*, która pozwoli efektywniej wykorzystać informacje z różnorodnych źródeł danych (s. 46).

Firmy branży security powoli odzyskują równowagę po pandemii, co jest optymistyczne. Jakie technologie i rozwiązania ochrony perymetrycznej i systemów kontroli dostępu są lub będą rozwijane i dlaczego? Eksperci z różnych firm dzielą się własnymi prognozami (s. 52).

Czytelników z obszaru bezpieczeństwa pożarowego powinna zainteresować informacja, że KE opracowała projekt zmiany rozporządzenia CPR na rzecz jednolitego (unijnego) rynku wyrobów budowlanych. Niektóre proponowane zmiany można uznać za rewolucyjne (s. 64).

Zapewnienie bezpieczeństwa biznesu stało się jeszcze trudniejsze – bardziej technologiczne i cybernetyczne, choć zagrożenia czają się głównie w sferze fizycznej wartości produktu czy kosztów przestoju produkcyjnego. Aby zadbać o odpowiedni poziom ochrony, warto rozważyć wdrożenie procedury „okresowych przeglądów technicznych bezpieczeństwa". Nawet gdyby organizacja nie zdecydowała się na zatrudnienie security managera w pełnym zakresie, to systematycznie powstająca baza danych w wyniku przeprowadzonych przeglądów będzie stanowić nieocenioną wartość (s. 76).

Marta Dynakowska
REDAKTOR NACZELNA

Jan T. Grusznic
Z-CA REDAKTORA NACZELNEGO

Mariusz Kucharski
PREZES ZARZĄDU

A&S POLSKA REDAKCJA

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

Prezes Zarządu
Mariusz Kucharski

Redaktor naczelna
Marta Dynakowska

Z-ca redaktora naczelnego
Jan T. Grusznic

Dział reklamy i marketingu
Iwona Krawiec

Dział projektów specjalnych
Jolanta A. Kucharska
Aleksandra Czapska
Michalina Nowak

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

Projekt graficzny i skład
Kalwala Studio

Adres redakcji
A&S Polska
ul. M. Rodziewiczówny 1 lok. 801
04-187 Warszawa
e-mail: info@aspolska.pl
www.aspolska.pl

Prenumerata
www.aspolska.pl/prenumerata

Redakcja zastrzega sobie prawo skracania i adiustacji zamówionych tekstów. Artykułów niezamówionych i niezatwierdzonych do druku nie zwracamy. Opinie autorów nie muszą być tożsame z poglądami redakcji. Za treść reklam redakcja nie odpowiada. Przedruki tekstów bez zgody redakcji są niedozwolone.

A&S Polska jest częścią grupy wydawniczej A&S International.

a&S POLSKA

05

35

09/10

2022

SPIS TREŚCI

PRZEMYSŁ 4.0

SPIS TREŚCI

RYNEK SECURITY

BEZPIECZEŃSTWO POŻAROWE

BEZPIECZEŃSTWO BIZNESU

SERWIS INFORMACYJNY

PRODUKT NUMERU

AXIS COMMUNICATIONS

www.axis.com/pl

AXIS Speed Monitor

AXIS WPROWADZA NA RYNEK NOWĄ APLIKACJĘ ACAP - AXIS SPEED MONITOR, KTÓRA UMOŻLIWIA PODŁĄCZENIE RADARU AXIS D2110-VE SECURITY RADAR DO WIĘKSZOŚCI ZEWNĘTRZNYCH KAMER AXIS. APLIKACJA ZWIĘKSZA WYDAJNOŚĆ KAMERY DZIĘKI IMPORTOWANYM Z AXIS D2110-VE DANYM RADAROWYM I ŁĄCZY NP. PRĘDKOŚĆ OBIEKTU Z WIDOKIEM KAMERY, A TAKŻE BUDUJE WEWNĘTRZNĄ BAZĘ DANYCH STATYSTYK SCENY.

Bezpłatna aplikacja AXIS Speed Monitor zbiera dane z radarów i wizualizuje zmierzone prędkości pojazdów do 105 km/h, a następnie prezentuje je jako kolorowe nakładki w strumieniu danych z kamery.
Oznacza to możliwość wyświetlania prędkości w czasie rzeczywistym, co pozwala szybko zidentyfikować pojazdy przekraczające prędkość. Łącząc to rozwiązanie z monitorami widoku publicznego, można wysyłać na żywo wiadomości z prośbą do kierowców przekraczających prędkość o zwolnienie.
Dane mogą być również wykorzystywane do wyzwalania innych zdarzeń, takich jak aktywacja świateł stroboskopowych, wyzwalanie alarmów czy uruchamianie nagrań z kamer.
Prezentowane rozwiązanie oferuje skuteczny sposób gromadzenia danych możliwych do wykorzystania w celu podejmowania bardziej świadomych decyzji dotyczących monitorowanej drogi.
Dane mogą być eksportowane jako plik CSV w celu tworzenia kompleksowych przeglądów graficznych, np. o liczbie pojazdów przejeżdżających w ciągu dnia i ich prędkości. Informacje te mogą być wykorzystane do określenia, czy należałoby zainstalować progi zwalniające lub inne urządzenia uspokajające ruch.

AXIS COMMUNICATIONS

www.axis.com/pl

Pierwsza kamera z ochroną przeciwwybuchową od Axis

AXIS COMMUNICATIONS WPROWADZA NA RYNEK AXIS XPQ1785 EXPLOSION-PROTECTED PTZ CAMERA, CZYLI PIERWSZĄ KAMERĘ Z OCHRONĄ PRZECIWWYBUCHOWĄ WŁASNEJ PRODUKCJI. KAMERA JEST PRZEZNACZONA DO MONITOROWANIA ROZLEGŁYCH OBSZARÓW I CERTYFIKOWANA DO UŻYTKU W MIEJSCACH NIEBEZPIECZNYCH NA CAŁYM ŚWIECIE. DZIĘKI FABRYCZNIE ZAINSTALOWANEJ APLIKACJI ANALITYCZNEJ, KTÓRA OSTRZEGA O POJAWIAJĄCYM SIĘ DYMIE, KAMERA MONITORUJE OBSZAR ZAGROŻONY ZAPŁONEM, PRZYCZYNIAJĄC SIĘ DO OCHRONY LUDZI I ŚRODOWISKA.

Nowa kamera ze stali nierdzewnej (316L) ma międzynarodowe certyfikaty Class I/II/III Div 1 oraz Zone 1/21 do użytku w miejscach niebezpiecznych (zgodnie z normami NEC, CEC, ATEX, IECEx itp.). Ta wytrzymała kamera z ochroną przeciwwybuchową ułatwia zdalne zabezpieczanie procesów produkcyjnych. Dzięki temu pracownicy muszą udać się do stref zagrożonych wybuchem tylko wtedy, gdy jest to naprawdę konieczne.
Ponadto, ponieważ kamera może korzystać z zasilania 110–240 V AC, nie jest potrzebne dodatkowe źródło zasilania. Obecność portów RJ45 i SFP ułatwia instalację urządzenia.

NAJWAŻNIEJSZE CECHY KAMERY AXIS XPQ1785:

- **Międzynarodowe certyfikaty do pracy w miejscach niebezpiecznych**
- **Aplikacja analityczna z ostrzeżeniem o dymie**
- **Technologie Zipstream i Lightfinder**
- **Rozdzielczość HDTV 1080p, 32-krotny zoom optyczny**
- **Zakres temperatury od -60°C do 60°C**

BCS

www.bcscctv.pl

W OFERCIE BCS POJAWIŁY SIĘ NOWE MODELE KAMER SZYBKOOBROTOWYCH PTZ – BCS-L-SIP2225SR10-AI1 I JEJ 4 -MPIX WERSJA BCS-L-SIP2425SR10-AI1. KAMERY TE CHARAKTERYZUJĄ SIĘ WSZYSTKIMI PODSTAWOWYMI FUNKCJAMI, KTÓRE W TEGO TYPU URZĄDZENIU POWINNY SIĘ ZNALEŹĆ. SPOŚRÓD INNYCH URZĄDZEŃ WYRÓŻNIAJĄ SIĘ NIEWIELKIMI ROZMIARAMI, DZIĘKI CZEMU NIE RZUCAJĄ SIĘ W OCZY TAK BARDZO, JAK ICH WIĘKSZE ODPOWIEDNIKI.

Kompaktowe kamery szybkoobrotowe BCS Line

Mają nieograniczony obrót w osi poziomej z prędkością do 200°/s dla sterowania ręcznego oraz do 240°/s po wywołaniu presetu. 120°/s to z kolei prędkość dla ruchu w osi pionowej, która przy wywołaniu presetu osiąga nawet 200°/s. Dodatkową zaletą charakteryzującą ruch pionowy tych modeli jest możliwość zwrócenia kamery o 15° powyżej poziomu montażu.
Kamera jest wyposażona w dwa wejścia i jedno wyjście alarmowe, wejście/wyjście audio, gniazdo kart pamięci MicroSD o pojemności do 256 GB oraz promiennik podczerwieni o zasięgu do 100 m oraz 25x zoom optyczny. Prawdziwą siłą kamer są moduły odpowiadające za inteligentną analizę obrazu, dzięki którym można maksymalnie zautomatyzować działanie systemu.
Z presetami można połączyć przekroczenie wirtualnej linii czy wkroczenie intruza w strefę z określeniem kierunku ruchu i rodzaju obiektu, który będzie uruchamiał alarm. Pozwoli to stworzyć trasę patrolową, w której każdy preset będzie monitorował innego typu zachowania.
Gromadzenie metadanych, które może zostać włączone w ogólnym trybie pracy kamery, pozwoli łatwo znaleźć na nagraniu obiekty, wybierając typ garderoby osoby czy kolor przejeżdżającego pojazdu.

C&C PARTNERS

www.ccpartners.pl

iManager – intuicyjna aplikacja do zarządzania dostępem

IMANAGER JEST APLIKACJĄ DO ADMINISTROWANIA UPRAWNIENIAMI UŻYTKOWNIKÓW, AWIZACJI, WJAZDÓW, ZARZĄDZENIEM LISTAMI POJAZDÓW W SYSTEMACH PARKINGOWYCH, BUDYNKOWYCH, MIEJSKICH WYKORZYSTUJĄCYCH SYSTEMY KONTROLI DOSTĘPU IPROTECT ORAZ INTELIGENTNĄ PLATFORMĘ CCTV VDG SENSE.

Przyjazny interfejs graficzny pozwala administratorowi na szybkie wprowadzenie użytkownika, przypisanie kart zbliżeniowych oraz tablic rejestracyjnych, z jednoczesnym zdefiniowaniem zasobów obiektu, do których dany użytkownik powinien posiadać dostęp.

Dzięki aplikacji administrowanie użytkownikami jest niezwykle intuicyjne i zajmuje znacznie mniej czasu.
iManager wymienia informacje z wieloma serwerami jednocześnie, wykorzystując do tego celu prywatną chmurę z gwarancją bezpiecznej transmisji.

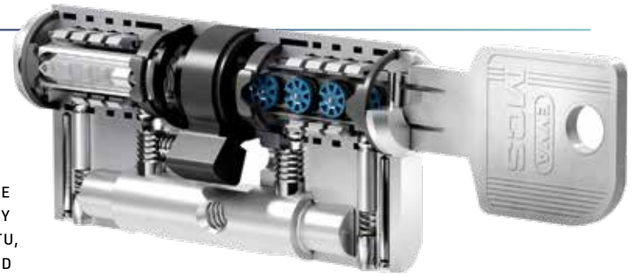
Funkcjonalności:

- **dodawanie lokalizacji / obiektu,**
- **dodawanie użytkownika aplikacji,**
- **dodawanie użytkownika systemów,**
- **dodawanie uprawnień użytkownika (pomieszczenia, strefy, parkingi),**
- **przegląd logów systemowych (zmiany w rejestrze baz danych).**

EVVA

www.evva.pl

MCS – 100% ochrony przed kopiowaniem



UNIKATOWE W SKALI ŚWIATOWEJ ZABEZPIECZENIE W SYSTEMIE MCS SPRAWIA, ŻE JEGO UŻYTKOWNICY NIE MUSZĄ SIĘ O NIC MARTWIĆ. WYNIKA TO Z FAKTU, IŻ KLUCZ JEST CAŁKOWICIE ZABEZPIECZONY PRZED KOPIOWANIEM, ORAZ Z OGROMNEGO POTENCJAŁU OBLICZENIOWEGO MCS.

System kontroli dostępu MCS doskonale nadaje się do zamknięć o złożonej strukturze i wysokich wymogach w zakresie wykonania i bezpieczeństwa (ochrona produktów wrażliwych lub których odzyskanie jest niemożliwe, np. na lotniskach, w szpitalach, instytutach badawczo-rozwojowych, budynkach rządowych itp.).

Wkładka MCS zawiera 8 swobodnie obracających się rotorów magnetycznych znajdujących się po lewej i prawej stronie rdzenia, które są przyporządkowane do krążków magnetycznych na kluczu.
Uprawniony klucz z odpowiednim kodem umieszcza rotory w pozycji zamykania, następnie mechanizm daje sygnał do zamknięcia.
Klucze MCS łączą dwie technologie zabezpieczeń, zapewniając potrójną ochronę: kod magnetyczny i dwa kody mechaniczne.

Dzięki rozbudowanym właściwościom, różnym wersjom i opcjom MCS może obsłużyć wszystkie sytuacje dostępowe w systemie zamknięć. Pozwala to na przygotowanie jasnej struktury dostępowej, obejmującej np. pomieszczenia i piętra, szafy, gabloty lub aktywowanie szlabanów i innych systemów elektronicznych. Użytkowanie obiektu jest komfortowe i bezpieczne.
Zalety systemu MCS w skrócie: ochrona przed kopiowaniem 3D, odpowiedni do dużych złożonych systemów zamknięć, wysoki poziom ochrony antywłamaniowej, ochrona patentowa.

HIKVISION

www.hikvision.com/pl

Przewodowa czujka antywłamaniowa PIR DS-PDP18-EG2(P)

PRZEWODOWA CZUJKA ANTYWŁAMANIOWA PIR DS-PDP18-EG2(P) FIRMY HIKVISION TO INNOWACYJNY MODEL WYPOSAŻONY W WIELE ZAAWANSOWANYCH TECHNOLOGII, M.IN. STREFY OPTYCZNE 3D, REGULACJĘ CZUŁOŚCI DETEKCJI (TRZY TRYBY DETEKCJI), CYFROWĄ KOMPENSACJĘ TEMPERATURY ORAZ FUNKCJĘ INTELIGENTNEJ KONTROLI OTOCZENIA.

Zasięg detekcji urządzenia wynosi 18 m / 85,9 stopni, co zapewnia dokładne wykrywanie zagrożeń w niewielkich pomieszczeniach wraz z pokryciem martwej strefy.
Czujka nie reaguje na ruch zwierząt domowych i jest odporna na cyrkulację powietrza oraz działanie owadów, ma również zabezpieczenia antysabotażowe.
Zakres wysokości montażu urządzenia wynosi 1,8 – 2,4 m, zasilanie do 16 VDC. Czujkę wyróżnia nowoczesny i kompaktowy wygląd, a jej instalacja nie zakłóca wystroju monitorowanego wnętrza.

HIKVISION

www.hikvision.com/pl

Kamery do pracy w niebezpiecznym środowisku

SERIA EXPLOSION-PROOF I ANTI-CORROSION FIRMY HIKVISION OFERUJE SPECJALNE KAMERY DO ZASTOSOWAŃ W NIEBEZPIECZNYCH I EKSTREMALNYCH WARUNKACH.

Kamery Explosion-proof wykorzystują 3,5-mm obudowę ze stali nierdzewnej oraz specjalnie zaprojektowany przegub, aby przetrwać zewnętrzne eksplozje i zapewnić ciągłość pracy w przypadku pożaru i eksplozji. Ponadto funkcje zdalnego monitorowania pozwalają uprościć i zabezpieczyć dozór bez potrzeby obecności ludzi w niebezpiecznych obszarach.
Kamery przeciwwybuchowe są idealne do zastosowań w fabrykach, zakładach chemicznych, stacjach benzynowych i naftowych.
Dzięki wieloletniemu doświadczeniu i specjalistycznej wiedzy firmy Hikvision w zakresie projektowania konstrukcji oraz zastosowaniu stali nierdzewnej 316L kamery serii Explosion-Proof przeszły rygorystyczne testy i otrzymały certyfikaty ATEX oraz IECEx.
Sól, wilgoć i zanieczyszczenia chemiczne mogą wyrządzić wiele szkód urządzeniom elektronicznym, zwłaszcza gdy są one stale narażone na działanie takich substancji. Kamery antykorozyjne Hikvision, zbudowane ze stali nierdzewnej 316L są na tyle wytrzymałe, aby pracować w większości środowisk korozyjnych. Antykorozyjna powłoka kamery jest odporna na działanie słonego powietrza morskiego, dzięki czemu nadaje się do pracy w środowiskach chemicznych, morskich, podwodnych i innych środowiskach korozyjnych.

LINC POLSKA

www.linc.pl

Radary ECHODYNE JUŻ w LINC Polska!

ECHODYNE TO AMERYKAŃSKA FIRMA PROJEKTUJĄCA I PRODUKUJĄCA INNOWACYJNE RADARY ZE SKANOWANIEM ELEKTRONICZNYM (ESA).

Dzięki własnej opatentowanej technologii MESA® (wykorzystującej metamateriały) ECHODYNE oferuje radary łączące:

- **wysoką wydajność,**
- **niewielkie rozmiary i masę,**
- **mały pobór mocy,**
- **atrakcyjną cenę.**

Marka ECHODYNE jest coraz bardziej rozpoznawalna w branży zabezpieczeń i posiada duży potencjał rozwojowy. Jej inwestorami są takie osobistości i podmioty, jak m.in. Bill Gates czy Baillie Gifford, z których inicjatywy w czerwcu tego roku zostały zebrane fundusze w wysokości 135 milionów dolarów na dalszą ekspansję firmy.
Radary marki ECHODYNE są m.in. wykorzystywane przez Departament Bezpieczeństwa Wewnętrznego USA. O jakości tych rozwiązań świadczy też fakt, że stanowią element Programu Bezpieczeństwa Armii Stanów Zjednoczonych – tzw. *US Army Surveillance Security System* (SSS). Ponadto radary ECHODYNE zostały już zintegrowane z ponad 50 systemami antydronowymi (UAV).

Możliwości wykorzystania radarów marki ECHODYNE są bardzo duże, począwszy od obiektów cywilnych po obronność i bezpieczeństwo narodowe, a co najważniejsze, są już dostępne w Polsce!

Oficjalnym przedstawicielem ECHODYNE w Polsce została spółka Linc Polska.

MIWI URMET

www.miwiurmet.pl

Integracja systemów zabezpieczeń dzięki ProtegeGX

PROTEGEGX FIRMY ICT JEST SKALOWALNYM I ZAAWANSOWANYM TECHNOLOGICZNIE NARZĘDZIEM WYSPECJALIZOWANYM W INTEGRACJI SYSTEMÓW BEZPIECZEŃSTWA W OBRĘBIE JEDNEJ PLATFORMY.
UMOŻLIWIA MAKSYMALNE WYKORZYSTANIE SYSTEMÓW ISTNIEJĄCYCH JUŻ W DANEJ ORGANIZACJI, INTEGRUJE SYSTEMY KONTROLI DOSTĘPU, SYGNALIZACJI WŁAMANIA I NAPADU ORAZ AUTOMATYKI BUDYNKU.

Dzięki szerokiej bazie opcjonalnych licencji można go zastosować w każdej, nawet rozbudowanej inwestycji.
W podstawowej licencji oprogramowanie umożliwia m.in. monitorowanie zewnętrznych urządzeń poprzez moduł Automation and Control. Dodatkowa licencja DataSync pozwala na zintegrowanie systemu z zewnętrznymi bazami danych, np. systemami płacowymi.
Zastosowanie BacNet lub ModBus umożliwia monitorowanie stanu systemu sygnalizacji pożarowej. Kolejną funkcjonalnością, na którą warto zwrócić uwagę, jest licencja na komunikację SIP, która umożliwia w prosty sposób, z poziomu oprogramowania, zarządzanie np. strefami dostaw.
Stosując wymienione protokoły, można zredukować, a nawet wykluczyć wystąpienie wielu niepożądanych zdarzeń, takich jak pozostawienie wyłączonej klimatyzacji czy oświetlenia po opuszczeniu budynku przez pracowników, zabezpieczając mienie i ograniczając wydatki na energię. To tylko niektóre narzędzia do integracji z zewnętrznymi systemami zabezpieczeń dostępne w ProtegeGX.
Aby zapoznać się z pełną funkcjonalnością systemu, prosimy o kontakt z naszym działem technicznym, pod adresem: kd@miwiurmet.pl

NEDAP SECURITY MANAGEMENT

www.nedapsecurity.com/pl/

Integracja AEOS i SIS-FIRE

STALE ROZWIJANE INSTALACJE NISKOPRĄDOWE DOSTARCZAJĄ NOWYCH FUNKCJONALNOŚCI. IDZIE TO W PARZE ZE ZWIĘKSZENIEM BEZPIECZEŃSTWA OBIEKTU, DZIĘKI CZEMU KLIENT DOSTAJE PRODUKT FUNKCJONALNY, KTÓRY SPEŁNIA WSZYSTKIE OBOWIĄZUJĄCE NORMY.

Dzisiaj system kontroli dostępu nie tylko pełni funkcję rozstrzygającą o przyznaniu autoryzacji do wejścia, lecz jednocześnie staje się centrum zarządzania budynkiem i źródłem informacji dla innych systemów.

Dzięki otwartości na integrację zarówno systemu KD AEOS, jak i SIUP SIS-FIRE firmy Schrack Seconet, możliwe było połączenie obu rozwiązań w celu dostarczenia obsłudze obiektu dodatkowych informacji pomocnych podczas normalnego użytkowania systemów oraz w trakcie zagrożenia, jakim w szczególności jest alarm pożarowy.

Protokolarna wymiana informacji pomiędzy systemami umożliwia m.in.
- monitorowanie skuteczności wysterowania przez SSP przejść na drodze ewakuacyjnej, zwiększające bezpieczeństwo przeprowadzenia sprawnej ewakuacji;
- monitorowanie położenia drzwi na drogach ewakuacyjnych. Operator SIUP ma dzięki temu pełny obraz sytuacji w obiekcie w trakcie alarmu pożarowego;
- automatyczną zmianę poziomu autoryzacji na wszystkich lub wybranych przejściach w przypadku alarmu pożarowego. Dzięki czemu system AEOS może działać zgodnie ze scenariuszem zaprogramowanym w SIS-FIRE;
- monitorowanie uruchomienia przycisków ewakuacyjnych podczas alarmu pożarowego, wskazujące możliwe miejsca zagrożenia podczas ewakuacji osób z obiektu.

OPTEX

www.optex.europe.com/pl

FlipX – czujka wewnętrzna z innowacyjnymi funkcjami

JAPOŃSKA FIRMA OPTEX WPROWADZIŁA NA RYNEK NOWĄ WEWNĘTRZNĄ CZUJKĘ RUCHU FLIPX. NASZPIKOWANA WIELOMA INNOWACYJNYMI FUNKCJAMI STANOWI IDEALNE ROZWIĄZANIE DO OCHRONY BUDYNKÓW MIESZKALNYCH I PODSTAWOWEJ OCHRONY OBIEKTÓW KOMERCYJNYCH.

Czujki OPTEX są wyposażone w udoskonaloną soczewkę sferyczną, która zapewnia perfekcyjnie ostry obraz, porównywalny z obrazem z zaawansowanych czujek PIR z optyką lustrzaną. Dzięki najnowszej funkcji – możliwości obracania soczewki – czujka jest uniwersalna. Łatwo można wybrać charakterystykę detekcji: szeroki kąt (12 m, 85°stopni) lub kurtynę (18 m).
FlipX zapewnia doskonałą ochronę przed intruzami, tolerując jednocześnie małe zwierzęta domowe. Konstrukcja nowego piroelementu Human-catch umożliwia precyzyjne rozróżnienie wielkości obiektu i optymalną czułość detekcji. Kolejną nowością jest zastosowanie algorytmu wykrywania „SMDA", który dotychczas był jedynie w czujkach zewnętrznych. Ta inteligentna funkcja znacząco zwiększa niezawodność czujek, zmniejszając jednocześnie liczbę fałszywych alarmów.
Atutem jest też elegancki design z dobrze widocznym wskaźnikiem LED i pokrywą otwieraną jednym ruchem ręki. Możliwy jest montaż zarówno na ścianie, jak i na suficie. Maksymalna wysokość montażu to 3 m. Kształt obudowy świetnie wtapia się w przestrzeń, dzięki czemu czujka jest prawie niezauważalna.
Seria FlipX standard obejmuje dwa modele: FLX-S-ST (PIR) oraz FLX-S-DT (PIR i MW).

SCHRACK SECONET

www.schrack-seconet.pl

SIS-POWER – wielofunkcyjna centrala sterująco-zasilająca urządzenia ppoż.

CENTRALA SIS-POWER WRAZ Z ZASILACZEM URZĄDZEŃ PPOŻ. S-POWER JEST PRZEZNACZONA DO STEROWANIA I ZASILANIA NAPIĘCIEM NISKIM I BARDZO NISKIM (MAKS. 1000 VAC, 1500 VDC) URZĄDZEŃ WCHODZĄCYCH W SKŁAD SYSTEMÓW KONTROLI ROZPRZESTRZENIANIA DYMU I CIEPŁA, SUG WODNYCH I INNYCH URZĄDZEŃ PPOŻ. DZIĘKI UKŁADOM SZR (SAMOCZYNNE ZAŁĄCZENIE REZERWY) CSZUP SIS-POWER LUB S-POWER MOŻNA TEŻ STOSOWAĆ JAKO GŁÓWNE ROZDZIELNICE POŻAROWE BUDYNKU.

SIS-POWER jest dostępna w różnych wersjach, zależnie od zastosowanego modułu kontrolno-sterującego S-CONTROL.
SIS-POWER/S-POWER może współpracować (protokół cyfrowy) z systemem sygnalizacji pożarowej i sterowania urządzeniami ppoż. Integral EvoxX oraz systemem integrującym urządzenia ppoż. SIS-FIRE.
Pozwala to zbudować kompleksowy, w pełni zintegrowany system bezpieczeństwa pożarowego (detekcja, sterowanie, zasilanie i zarządzanie urządzeniami ppoż. i innymi urządzeniami technicznymi obiektu).
SIS-POWER, zgodnie z dokumentami certyfikacyjnymi CNBOP-PIB, umożliwia sterowanie i kontrolę urządzeń oddymiania mechanicznego (kanałowego i bezkanałowego) i grawitacyjnego (ze stałym/zmiennym nawiewem kompensacyjnym), systemami oczyszczania z dymu, a także zasilanie komponentów systemu różnicowania ciśnień (wentylatory pożarowe, klapy ppoż. i dymowe, okna oddymiające, drzwi kompensacyjne, przepustnice powietrza kompensacyjnego, bramy, kurtyny dymowe, wyrzutnie dymu, elektromechaniczne i elektromagnetyczne urządzenia ryglujące).

TP-LINK

www.tp-link.com.pl

TP-Link VIGI C340-W – zewnętrzna kamera CCTV typu bullet, IP66

VIGI C340-W TO ZEWNĘTRZNA KAMERA SIECIOWA TYPU BULLET, KTÓRA NAGRYWA OBRAZ W ROZDZIELCZOŚCI 4 MPIX. WBUDOWANE DIODY LED ZAPEWNIAJĄ KOLOROWY OBRAZ TAKŻE W CAŁKOWITEJ CIEMNOŚCI. DZIĘKI WODOODPORNEJ I PYŁOSZCZELNEJ OBUDOWIE O KLASIE IP66 KAMERA JEST ODPORNA NA WARUNKI ATMOSFERYCZNE.

Kamera została wyposażona w mocne anteny Wi-Fi i wykorzystuje do komunikacji sieć bezprzewodową. Dzięki temu można ją zamontować w miejscach, gdzie nie ma możliwości doprowadzenia kabla sieciowego. Zastosowana kompresja H.265+ zmniejsza obciążenie sieci i obniża koszty monitoringu bez utraty jakości generowanego obrazu. Nagrania można rejestrować na rejestratorze sieciowym i karcie microSD.
VIGI C340-W oferuje dwukierunkową transmisję audio, czyli możliwość rozmowy przez urządzenie np. z kurierem, którego można poprosić o zostawienie przesyłki przed drzwiami. Dzięki aplikacji VIGI na urządzenia przenośne z systemem iOS lub Android kamerami z tej serii można zarządzać z poziomu smartfona. Kamera wyśle powiadomienie push, gdy wykryje niepożądany ruch, przekroczenie wyznaczonej granicy lub gdy ktoś zasłoni jej obiektyw. Systemem monitoringu VIGI można też zarządzać z poziomu dedykowanego oprogramowania dla komputerów i rejestratorów NVR. W ofercie TP-Link dostępne są 8-kanałowy rejestrator VIGI NVR1008H i 16-kanałowy rejestrator VIGI NVR1016H.
Wszystkie urządzenia z serii VIGI są zgodne ze standardem ONVIF.
Kamera została objęta 3-letnią gwarancją producenta.

UNICARD

www.unicard.pl

Impero 360 – pierwsza polska chmurowa kontrola dostępu

SZYBKIE I PROSTE WDROŻENIE. OSZCZĘDNOŚĆ PIENIĘDZY I PRZESTRZENI. ZALET KONTROLI DOSTĘPU (KD) W CHMURZE JEST WIELE – PRZYJRZYJMY SIĘ IM Z BLISKA NA PRZYKŁADZIE IMPERO 360, CZYLI PIERWSZEGO POLSKIEGO SYSTEMU KD W CHMURZE.

Impero 360 jest rozwiązaniem chmurowym z zakresu kontroli dostępu *(ACaaS – Access Control as a Service)*, które wykorzystuje abonamentowy model płatności. Zasadniczym atutem jest tutaj brak konieczności posiadania zaplecza IT i serwerowni, co oznacza mniejsze koszty związane z posiadaniem zaawansowanej infrastruktury. Aplikacja gwarantuje szybkie i proste wdrożenie, a dalsze konfigurowanie i praca z impero 360 są intuicyjne i proste w obsłudze.
Rozwiązanie jest skalowalne – administrator może samodzielnie dodawać do systemu KD użytkowników, zmieniać uprawnienia i nadawać nowe. Wszystko odbywa się z zachowaniem bezpieczeństwa i ochrony danych. Informacje są przechowywane na zdalnych serwerach Microsoft Azure, które są chronione szeregiem procedur.
Kontrola dostępu w chmurze impero 360 najlepiej sprawdzi się w średnich i dużych przedsiębiorstwach. Do wyboru są trzy modele rozliczeń: Standard, Premium i Enterprise. Co istotne, użytkownik KD w chmurze płaci wyłącznie za funkcje, z których faktycznie korzysta – ma więc większą swobodę wyboru niż w przypadku klasycznego oprogramowania.

Więcej o zaletach impero 360 przeczytasz na stronie www.impero360.cloud

ZKTECO EUROPE

www.zkteco.eu

Terminale ProMA firmy ZKTeco

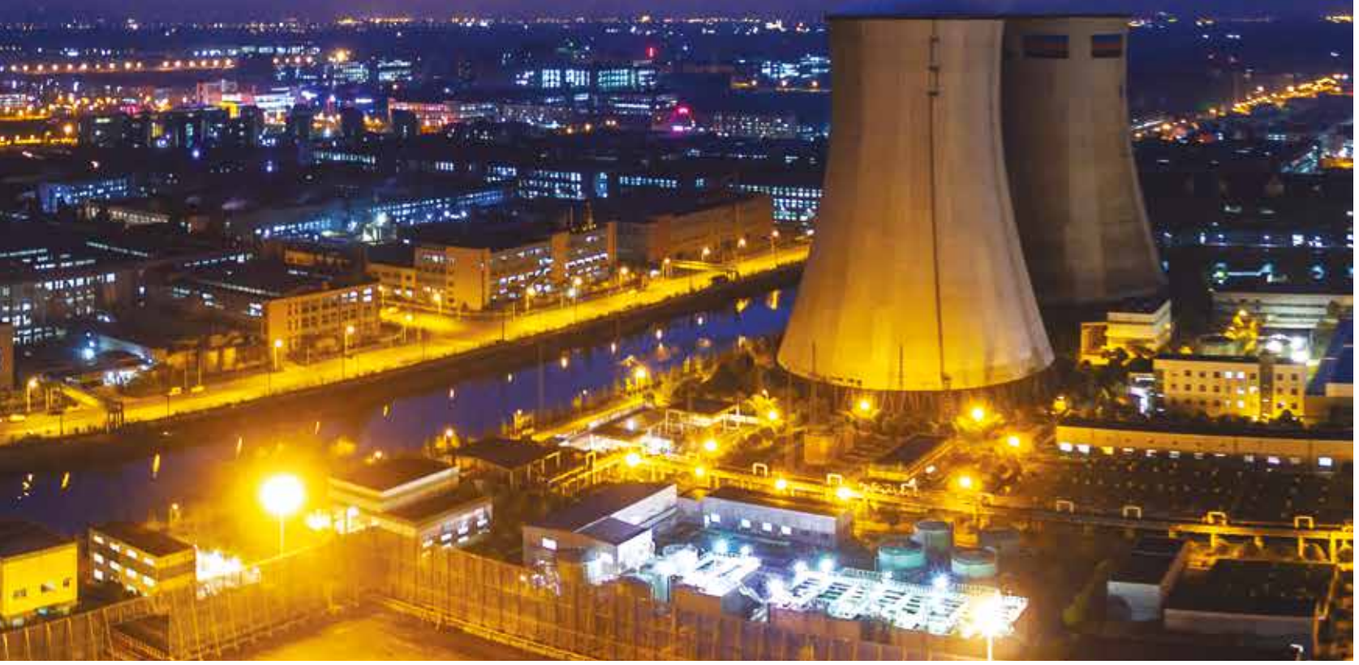
PROMA TO NAJNOWSZA GENERACJA ZEWNĘTRZNYCH MULTI-BIOMETRYCZNYCH TERMINALI DO SYSTEMÓW KONTROLI DOSTĘPU. WYKONANO JE W OBUDOWIE Z WYTRZYMAŁEGO STOPU ALUMINIUM, OSIĄGAJĄC STANDARD WODO- I PYŁOSZCZELNOŚCI IP66 ORAZ ODPORNOŚCI MECHANICZNEJ IK07 (TZW. WANDALOODPORNOŚCI).

Oferowane są trzy modele terminali, które wyposażono w różne kombinacje sposobu uwierzytelniania:

- ProMA-QR (rozpoznawanie twarzy + czytnik kodów QR + czytnik RFID),
- ProMA-RF (rozpoznawanie twarzy + czytnik RFID),
- ProMA (rozpoznawanie twarzy + czytnik linii papilarnych + czytnik RFID).

Jako opcja dostępne jest w tych modelach najnowsze rozwiązanie bezdotykowego rozpoznawania dłoni.
Pomimo niewielkich rozmiarów, możliwości uwierzytelniania tych urządzeń są na najwyższym poziomie. Obsługują do 10 tys. wzorców linii papilarnych, 30 tys. twarzy, 5 tys. dłoni, 50 tys. RFID.
Poza tym ich szybkość identyfikacji jest oszałamiająca, na rozpoznanie twarzy potrzebują mniej niż 0,3 s, bezdotykowe rozpoznanie dłoni 0,35 s i RFID 0,2 s. Wszystkie te niezwykłe funkcje czynią terminal idealnym rozwiązaniem dla większości aplikacji.
Terminale obsługują protokół komunikacyjny ZKTeco PUSH i są w pełni zintegrowane z najnowszą wersją platformy bezpieczeństwa ZKBioSecurity. Obsługują protokół PoE IEEE802.3af i czytają ponad 100 typów kart (w tym ID, IC, Legic, Desfire, EV1, EV2, HID Prox, HID iClass). Mogą pracować też jako panel zewnętrzny wideodomofonu HD z dzwonkiem, obsługiwany za pośrednictwem aplikacji mobilnej ZSmart i PC ZKBioTalk.

Wyzwania ochrony obiektów przemysłowych



Zakłady przemysłowe są obiektami łączącymi wiele funkcji i procesów. Dość często mają kilka lokalizacji, a jednocześnie masowo korzystają z podwykonawców, co sprawia, że proces produkcyjny w praktyce rzadko odbywa się w jednym miejscu. Uwarunkowania te wywołują konsekwencje także w odniesieniu do zagrożeń, które mogą mieć odmienne cechy i źródła, zależne od profilu konkretnego miejsca występowania. Przy czym suma zidentyfikowanych zagrożeń będzie większa od sumy lokalizacji i zachodzących w nich procesów, należy bowiem uwzględnić kompleks operacji logistycznych, obecnie bardzo rozbudowanych pod względem zarówno lokalizacji, jak i uwarunkowań organizacyjnych. Dlatego obiekty takie są najciekawsze, ale jednocześnie stawiają zespołom ochronnym najszersze spectrum wyzwań.

Jacek Grzechowiak

Zakłady przemysłowe są obecnie nieodłącznym elementem gospodarki. Przyzwyczailiśmy się do tradycyjnego pojmowania zadań i związanych z tymi obiektami zagrożeń, jednak produkcja nieustannie ewoluuje, co sprawia, że nadążanie za ewolucją zasobów chronionych wcale nie jest takie proste, powodując często pewien dysonans w relacjach pomiędzy klientem a dostawcą usług ochrony. Może nie wszędzie, ale wciąż jednak obserwujemy incydenty nieco archaiczne, które zdają się potwierdzać tę tezę. I dziś chciałbym spojrzeć na naszą codzienność właśnie przez pryzmat kilku takich incydentów, charakterystycznych dla trzech głównych modeli ochrony zakładów przemysłowych.

Z teoretycznego punktu widzenia, nawet zapisanego w różnego rodzaju dokumentach normatywnych (jak choćby w ***Metodyce uzgadniania planów ochrony obszarów, obiektów i urządzeń podlegających obowiązkowej ochronie)*** ochrona może być sprawowana w trzech formach:

1. Ochrona fizyczna (osobowa)
2. Zabezpieczenie techniczne
3. Forma mieszana, łącząca ochronę fizyczną i zabezpieczenie techniczne.

W zakładach przemysłowych najpowszechniejsza jest ta trzecia forma ochrony i można by nawet uznać ją za podstawową, gdyby nie to, że w praktyce zarówno kondycja systemów zabezpieczeń technicznych, ich rozmieszczenie, jak i wykorzystanie przez pracowników ochrony w bieżącej pracy jest bardzo często wadliwe lub wręcz iluzoryczne. Powoduje to, że forma mieszana w codziennej praktyce sprowadza się jedynie do ochrony fizycznej. Być może część czytelników uzna tę tezę za wątpliwą. W dalszej części artykułu rozwieję ich wątpliwości.

Z praktycznego punktu widzenia można natomiast wyróżnić dwie istotne części ochrony:

1. **Część proceduralna:** analiza zasobów chronionych oraz zagrożeń, jakim podlegają, mająca odzwierciedlenie w koncepcji ochrony, a w praktyce codziennej najbardziej obecna w procedurach działania pracowników ochrony.
2. **Część wykonawcza**, składająca się z dwóch komponentów:

   a) Komponent pierwszy to konfiguracja składu zespołu ochronnego; można w nim wyróżnić trzy zasadnicze modele:

   - **ochrona jednoosobowa,**
   - **ochrona niewielkim (2–3-osobym) zespołem, siłą rzeczy skoncentrowanym na obiekcie chronionym, można by nawet przyjąć – stosując ponownie terminologię ustawową – zespołem działającym w granicach chronionego obszaru lub obiektu.**
   - **ochrona wieloosobowa, zlokalizowana zarówno w chronionym obiekcie, jak i poza nim. W tym modelu praca pracowników ochrony w obiekcie chronionym będzie wspierana, np. 1) systemami zdalnego monitoringu sygnałów alarmowych, wideo, GPS itd. obsługiwanymi przez pracowników ochrony, którzy pracują w zewnętrznej stacji monitoringu zlokalizowanej najczęściej w agencji ochrony, 2) różnego rodzaju działaniami w ramach ochrony fizycznej doraźnej (popularnie zwanej patrolami interwencyjnymi) oraz 3) innymi działaniami, takimi jak monitorowanie stanu bezpieczeństwa w bezpośrednim otoczeniu chronionego obiektu, analizy bezpieczeństwa procesów zachodzących (planowanych) w relacjach z innymi obiektami itd. Tego typu działania w obiektach dojrzałych są jednocześnie typowymi działaniami dwukierunkowymi, pozwalając na gromadzenie danych, ich analizę w czasie rzeczywistym oraz sygnalizowanie i alarmowanie dwukierunkowe na bazie algorytmów stosowanych w tym obszarze.**

   b) Drugim komponentem są kompetencje ogólne i specjalistyczne pracowników ochrony oraz ich przygotowanie psychofizyczne do realizacji zadań ochronnych, czyli to, co sprawia, że przyjęta koncepcja ochrony będzie realizowana bądź nie.

W każdej konfiguracji niezbędne są odpowiednie kwalifikacje pracowników ochrony, zarówno realizujących zadania w obiekcie, jak i wykonujących różne zadania poza nim. Przyjrzyjmy się więc tym trzem modelom ochrony przez pryzmat rzeczywistych incydentów.

OBIEKT JEDNOPOSTERUNKOWY

Model najczęściej spotykany w niewielkich zakładach przemysłowych (budynek lub kompleks kilku budynków) zlokalizowanych w jednym miejscu. Dość często stosowany w ochronie obiektów odległych, takich jak zakłady przemysłowe wymagające specyficznej lokalizacji, np. z segmentów agro (wytwórnie pasz, elewatory, kompostownie), produkcji kruszywa, OZE (farmy wiatrowe i fotowoltaiczne, będące de facto zakładami produkującymi energię elektryczną).

W tego typy obiektach zagrożeniu głównemu, jakim jest kradzież, zniszczenie lub dewastacja mienia, towarzyszy szereg innych zagrożeń, które nie zawsze wynikają z działań przestępców, choć często tak jest, jak to miało miejsce na farmie fotowoltaicznej w Nadarzynie (woj. pomorskie) w 2021 r. Przestępcy najpierw dokonali napadu na pracownika ochrony, obezwładniając go, następnie go skrępowali i umieścili w miejscu, w którym nie stwarzał już zagrożenia (choćby wzywając pomocy), po czym przystąpili do kradzieży, której łupem padło 280 paneli fotowoltaicznych, powodując straty na kwotę ponad 130 tys. zł (a to jedynie wartość skradzionego mienia). Jak widać z tego przykładu, zastosowanie rozwiązań w zakresie szybkiej i efektywnej transmisji alarmu napadowego jest niezbędne. Podobnie jak zapewnienie właściwych zdolności psychofizycznych pracownika ochrony. I oczywiście adekwatność sił i środków ochrony do zagrożeń.

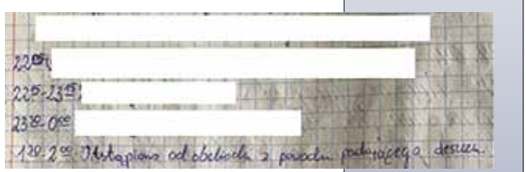
Z reguły zagrożenia wiążą się z charakterystyką miejsca wykonywania zadań ochronnych, niekiedy są związane z predyspozycjami pracowników ochrony lub wynikają z ogólnej sytuacji w branży ochrony powodującej, że powszechnie pracują oni po 24 czy 36 godzin non stop. Tajemnicą poliszynela jest to, że takie praktyki są powszechne, sprowadzając zagrożenia o różnorodnym natężeniu dla pracownika ochrony i chronionego mienia. Przykładem jest incydent z grudnia 2021 r., kiedy to w jednym z łódzkich zakładów przemysłowych pracownik ochrony zginął w pożarze dyżurki ochrony. Co było przyczyną pożaru? Potrzeba ogrzania miejsca pełnienia służby i wynikające z niej przeciążenie instalacji elektrycznej? Ale czy tylko? Być może pracownik zasłabł lub zasnął mocno i już się nie obudził? Czytelnicy zapewne pamiętają krążący na Tik-Toku film przedstawiający pracownika ochrony śpiącego tak mocno, że sygnały dźwiękowe karetki pogotowia stojącej w odległości ledwie

kilku metrów od niego nie były w stanie go obudzić.
Ponownie jawi się potrzeba monitorowania pracy pracownika ochrony w takim obiekcie. Od lat funkcjonują różnego rodzaju systemy kontroli obchodów, ale znów praktyka życia codziennego pokazuje, że są one podatne na różnego rodzaju próby neutralizujące, a jednocześnie niewiele z nich pozwala na monitoring bezczynności czy upadku i alarmowanie stacji monitoringu w takich sytuacjach. Jednak rozwiązania są dostępne i jak pokazują powyższe przykłady, niezbędne jest inwestowanie w nie.

2021-04-27 00:07:01	SAFE_0080	Odczyt punktu RFID:
2021-04-27 00:07:01	SAFE_0080	Odczyt punktu RFID:
2021-04-27 00:07:01	SAFE_0080	Odczyt punktu RFID:

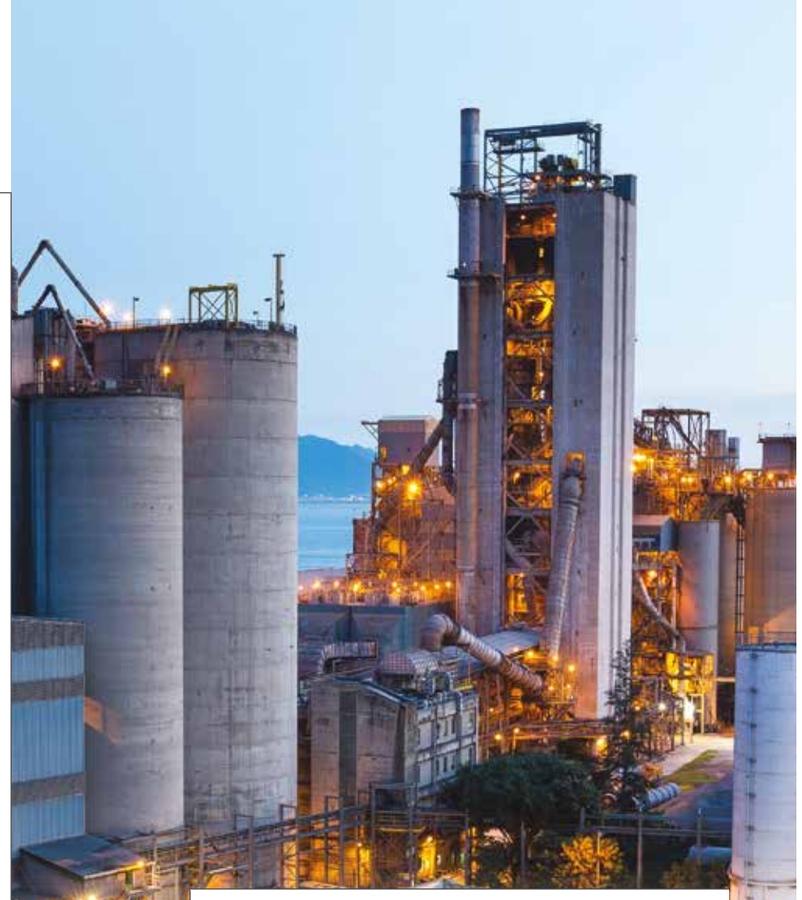
Rys. 1. Przykład odczytania trzech odległych punktów SKO dokładnie w tym samym czasie, wskazujący na możliwość faktycznego niewykonania obchodu

Innymi kwestiami są zagrożenia wynikające z konfiguracji obiektu oraz wyposażenia pracownika ochrony. Bywają obiekty, w których sporym problemem były szczury. Łatwo wyobrazić sobie konsekwencje zarówno te pracownicze – zdrowotne, jak i operacyjne. To także element, który należy brać pod uwagę, tworząc koncepcję ochrony oraz weryfikując jej realizację. Jak w praktyce wyglądają konsekwencje z pozoru prozaicznych zaniedbań, przedstawiają przypadki zaniedbań w zakresie umundurowania.
W obiektach jednoposterunkowych widać to najczęściej. Z różnych przyczyn: 1) to obiekty, w których właściciel najczęściej nie przywiązuje wagi do ochrony, 2) to tam najłatwiej wmówić klientowi, że T-shirt z napisem OCHRONA to „nasz standard”...
Konsekwencje bywają różne. Znany jest przypadek, kiedy pracownik ochrony został ukąszony przez kleszcza, innym razem na zapisie wideo widzimy kogoś ubranego w T-shirt z napisem „Ochrona”, a który... kradnie, wreszcie w dokumentacji służby można nawet znaleźć wpisy o odstąpieniu od wykonywania czynności ochronnych z powodu braku właściwej odzieży (sic!).



Rys. 2. Przykład odstąpienia od patrolowania obiektu z powodu de facto braku odzieży przeciwdeszczowej

Wszystkie te zjawiska widzimy tu i teraz. Ich rozwiązanie jest w zasięgu ręki, a jednak wciąż występują.



OBIEKTY O 2–3-OSOBOWEJ STRUKTURZE OCHRONNEJ

Najczęściej spotykane w segmencie produkcyjnym. Niekiedy – wciąż zbyt rzadko – znajdziemy tam także osobę dedykowaną do spraw bezpieczeństwa. Stąd ochrona w tych obiektach jest już realizowana w sposób zdecydowanie bardziej efektywny, co nie znaczy, że nie dochodzi do incydentów. Nie znaczy także, że agencja ochrony realizująca tam usługi ochrony potrafi sprostać wymaganiom klienta. Ograniczenia rynkowe i budżetowe sprawiają, że ochrona jest prowadzona nieadekwatnie do potrzeb, a zwłaszcza do zagrożeń.
W grudniu 2021 r. w jednej z dolnośląskich firm doszło do napadu, w którego trakcie sprawcy zaskoczyli dwie pracownice ochrony i sterroryzowali je. Po wyeliminowaniu ochrony w brutalny sposób przystąpili do kradzieży, wywożąc z zakładu wyroby charakteryzujące się zarówno dużymi gabarytami, jak i znaczną masą. Jak wynika z doniesień medialnych, obie pracownice ochrony zostały zaskoczone, a więc ponownie mamy do czynienia ze zdarzeniem związanym zarówno z niewyposażeniem pracowników ochrony w odpowiedni sprzęt, jak i brakiem odpowiednich umiejętności. Nie przesądzając, jak było faktycznie, wszak mamy jedynie informacje prasowe, kwestie wyposażenia oraz predyspozycji psychofizycznych w połączeniu ze szkoleniem jawią nam się jako te, na które trzeba kłaść duży nacisk.

DUŻE OBIEKTY PRZEMYSŁOWE

W dużych obiektach będziemy mieli do czynienia już z całą gamą zagrożeń, zarówno tych dotyczących konkretnego obiektu, jak i całego spectrum jego funkcjonowania na zewnątrz – a więc np. z zagrożeniami na styku z branżą TSL, która niekiedy przejmuje cały proces logistyczny, co powoduje, że np. zagrożenia wewnętrzne (kradzież, infiltracja, sabotaż) mogą mieć podłoże zupełnie niezwiązane z naszym obiektem. Mogą wynikać z uwarunkować firmy logistycznej, jej „szczelności”, wydajności procedur, wreszcie podejścia nie tylko do kwestii bezpieczeństwa, ale także np. zarządzania zasobami ludzkimi. W dużych zakładach przemysłowych z reguły mamy także do czynienia z zaawansowanymi procesami zarządzania jakością, w tym także jakością ochrony. Mamy więc audyty wewnętrzne, zewnętrzne, czasem także procedury kontrolne realizowane w poziomu państwowego, jak to ma miejsce w obiektach infrastruktury krytycznej czy obiektach podlegających obowiązkowej ochronie, nie będących IK.
Na drugiej szali tej wagi jest wciąż obecna w naszym życiu akcyjność działania. Widzimy przecież, że incydenty zdarzają się także w tych obiektach, a wnikliwi obserwatorzy naszej codzienności znajdą zapewne przykłady, gdy do incydentu dochodzi wkrótce po takiej kontroli. I tu ponownie w grę wchodzi człowiek. Człowiek z własnym know-how, a więc wykształceniem ogólnym, specjalistycznych, doświadczeniem życiowym i zawodowym, ale i własnymi ułomnościami. I oczywiście cały kompleks systemów zabezpieczeń technicznych.

Jeśli chodzi o człowieka, ważnym przykładem jest napad w Płocku na pracownika ochrony, który został ugodzony nożem. I można długo dywagować, jak do tego doszło, ale nie sposób pominąć taktyki ochrony i swego rodzaju erozji wiedzy dotyczącej każdego z nas. Wszak zachowywanie bezpiecznej odległości od każdej osoby jest jednym z fundamentów bezpieczeństwa pracownika ochrony, swego rodzaju elementarzem ochrony, a zagrożenia ze strony kolegów lub byłych kolegów znane nam są od czasu napadu na Kredyt Bank w Warszawie. Erozja wiedzy... to niestety poważny problem, ale możliwy do rozwiązania poprzez szkolenie i ciągłe kształtowanie świadomości pracowników ochrony. I znów kłaniają się realia rynkowe. Najniższa cena w praktyce nie daje szans na szkolenie, a jeśli daje takie szanse, to musi odbić się na jego jakości.
Odnosząc się do zabezpieczeń technicznych, to w takich obiektach stan w tym zakresie wydaje się najlepszy. Jednak nawet jeśli obiekt jest wyposażony w zaawansowane systemy bezpieczeństwa, to zdarzają się incydenty, które skłaniają do refleksji nad wykorzystywaniem tych systemów przez pracowników ochrony. Gdy w obiekcie IK dochodzi do wtargnięcia na teren, po czym osoby, które w ten sposób znalazły się – że znów zastosuję ustawową terminologię – w granicach chronionego obiektu, potrafią działać na tyle szybko, że wchodzą na ponad 100-metrowy komin, to coś jednak musiało nie zadziałać. Także w warstwie technicznej. A skoro doszło do takiego incydentu, to mogło dojść także do znacznie gorszego.
W zakładach przemysłowych ważnym elementem, wpływającym bezpośrednio na koncepcję ochrony oraz stanowiącym duże wyzwanie dla pracowników ochrony (także tych wykonujących obowiązki zdalnie) jest duży przepływ mienia o dużej różnorodności, przy zredukowanym do minimum czasie pozostawania tego mienia w strefach magazynowych (co wynika z dostaw w modelu just in time). W efekcie czas dyspozycyjny dla ochrony, pozwalający na różnego rodzaju aktywności kontrolne i weryfikujące, jest niekiedy zerowy. Taki model zarządzania przepływem mienia daje wyjątkowe możliwości osobom znającym niuanse magazynowe, a to one właśnie są niekiedy sprawcami lub pomocnikami w kradzieżach z zakładów produkcyjnych.
Dodatkowym problemem jest tu – będące także konsekwencją szybkości procesu – utrudnienie w ujawnieniu ewentualnej kradzieży, co opóźnia i utrudnia wyjaśnienie incydentu. Wydłuża się przez to czas trwania procederu, jak to miało miejsce u renomowanego producenta samochodów, powodując straty w postaci kradzieży ponad 100 silników, 500 skrzyń biegów oraz innego mienia, o łącznej wartości szacowanej na miliony euro. Stąd w dużych zakładach przemysłowych procedury wewnętrznego i zewnętrznego audytu są tak rozpowszechnione, co oczywiście nie umniejsza roli ochrony, zarówno osobowej, jak i technicznej, w końcu te silniki jakoś musiały opuścić obiekt chroniony.

Wykorzystanie systemów zabezpieczeń technicznych to temat-rzeka. Warto więc skupić się na sprawach prozaicznych. Dlaczego? Bo one występują najczęściej:

1. Monitor komputera wyświetlający obrazy z maksymalnej liczby kamer powoduje, że właściwie cały system jest bezwartościowy. To efekt czynnika ludzkiego.
2. Elementy sterujące CCTV zlokalizowane w „ostatnim kącie biurka” albo gdzieś zupełnie z boku to czytelny sygnał, że system w praktyce nie jest użytkowany. To także efekt czynnika ludzkiego.
3. Zakurzona klawiatura lub manipulator są takim samym sygnałem. To też efekt czynnika ludzkiego.

To są właśnie te obserwacje, które skłaniają mnie do wniosku, że bardzo często mieszana forma ochrony zatraca część techniczną i sprowadza się wyłącznie do ochrony fizycznej, osobowej.
Kluczowym elementem systemu ochrony wciąż jest człowiek. Wsparcie techniczne, automatyzacja, zaawansowane algorytmy bez wątpienia zmniejszają negatywny wpływ czynnika ludzkiego, jednak to nie tylko nie sprawia, że inwestycje w człowieka mogą być mniejsze, wręcz przeciwnie – wymaga dużo większych nakładów na kompetencje pracownicze, a w zakładach przemysłowych kompetencje uwzględniające nie tylko kwestie security, ale także profil zakładu.

1 https://radiogdansk.pl/wiadomosci/region/slupsk/2022/01/26/we-dwoch-mieli-ukrasc-z-budowy-280-paneli-fotowoltaicznych-uprzednio-napadlszy-stroza-oskarzeni-staneli-dzis-przed-sadem-w-slupsku/ [dostęp: 4.09.2022].
2 Agnieszka Malczewska-Błaszczyk, *Problem stresu i jego skrajnych konsekwencji u pracowników ochrony osób i mienia*, Państwo i Społeczeństwo, 2015 (XV) nr 2, Wyd. Krakowskiej Akademii im. Andrzeja Frycza Modrzewskiego
3 https://tulegnica.pl/artykul/napad-na-fabryke-w-legnicy/1257803 [dostęp: 4.09.2022].
4 https://wroclaw.tvp.pl/57976311/legnica-policja-poszukuje-sprawcow-napadu-na-fabryke [dostęp: 4.09.2022].
5 https://tvn24.pl/lodz/belchatow-ekolodzy-zeszli-z-komina-elektrowni-ra887869-2392716 [dostęp: 4.09.2022].
6 https://www.auto-swiat.pl/wiadomosci/aktualnosci/w-ciagu-dwoch-lat-wyniesli-z-fabryki-mercedesa-setki-silnikow-i-skrzyn-biegow/mydngqn [dostęp: 4.09.2022].

JACEK GRZECHOWIAK

Menedżer ryzyka i bezpieczeństwa. Absolwent WAT, studiów podyplomowych w SGH i Akademii L. Koźmińskiego. Gościnnie wykłada na uczelniach wyższych. W przeszłości związany z grupami Securitas, Avon i Celsa, w których zarządzał bezpieczeństwem i ryzykiem. Obecnie pełni funkcję pełnomocnika Zarządu ds. Ryzyka i Bezpieczeństwa w TAURUS OCHRONA.

Szukasz narzędzia, które pozwoli Ci **automatyzować procesy kontrolne?**

Znajdź rozwiązanie na stronie 44

Security 4.0

W numerze 4/2022 „a&s Polska” ukazał się artykuł Jana Kapusty na temat zmian w paradygmacie bezpieczeństwa. To ważny tekst będący potrzebnym otwarciem dyskusji o roli bezpiecznika[1] w organizacji. Z mojej – przemysłowej – perspektywy jesteśmy nie tyle w trakcie znaczącej zmiany paradygmatu bezpieczeństwa, ile raczej siedzimy w ekspresie zmian. Ekspresie, który już odjeżdża ze stacji „Security 4.0”.

Łukasz Stępień

W działalności przemysłowej można się często spotkać ze zwrotem „Industrial 4.0”. To umowne określenie czwartej rewolucji przemysłowej. Pierwszą był wiek pary, drugą wiek elektryczności, trzecią czas komputerów, a czwarty, dziejący się współcześnie, dotyczy stopniowego zanikania barier między ludźmi a maszynami oraz coraz częstszej automatyzacji procesów. Podobne cztery etapy rewolucji można wyodrębnić w obszarach security przemysłowego w Polsce[2].

Pierwszy etap obejmuje lata 90. ub. wieku – czasy dzikiego kapitalizmu i odnajdywania się w nowej rzeczywistości ustrojowej. W tym okresie jeśli bezpiecznik, to tylko po służbach, najlepiej w policji albo wojsku. Bardziej niż kompetencje takiej osoby liczyły się jej koneksje i znajomości ze służb, pozwalające „zapewnić bezpieczeństwo” organizacji.

Pierwsza dekada XXI wieku to stopniowe „ucywilnianie” funkcji „bezpiecznika”. Okazało się, że niełatwo przełożyć pragmatykę działania służb na pracę w warunkach cywilnych, co utrudniało kooperację wewnątrz organizacji. Był to też czas, kiedy specjalne strefy ekonomiczne zachęcały zagraniczny kapitał do zwiększania inwestycji w Polsce. Wiązało się to z pojawieniem się nowych, korporacyjnych i globalnych standardów w obszarach security.

W roku 2010 nastąpił intensywny rozwoju specjalizowanych zespołów i konsultantów w obszarach bezpieczeństwa. Coraz więcej organizacji zaczęło świadomie brać odpowiedzialność za obszary security. Zaczęto również dostrzegać absurdalność sytuacji, w której jedna i ta sama firma opracowuje (czytaj: kopiuje z jednego wzorca) plan ochrony, a później realizuje ochronę obiektu. To chyba jeden z niewielu przypadków w biznesie, kiedy to dostawca określa klientowi, jaki produkt, jakiej jakości i w jakim czasie będzie dostarczany.

Ze względu na rosnące koszty pracy i rozwój technologii coraz częściej zwraca się uwagę na wykorzystanie zabezpieczeń technicznych, zdecydowanie bardziej odpornych na zakłócenia niż czynnik ludzki. Stopniowo zmieniało się też postrzeganie potencjału, jakim dysponuje zespół ochrony fizycznej. Zespoły ochrony zaczęto przenosić z działów facility (utrzymanie budynku) do działów BHP albo bezpośrednio pod Zarząd.

Lata 20. XXI wieku – czas, kiedy systemy bezpieczeństwa zbierają tak dużo danych, z takiej liczby czujników, że człowiek nie jest w stanie tego samodzielnie przetworzyć. Analityka w kamerach, analityka w programach VSM, systemy wspierające decyzyjność, raporty z „odbić”, systemy RFID, PSIM i SMS. Dziesiątki możliwości o bardzo wysokim poziomie zaawansowania. Możliwości, które „na koniec dnia” i tak musi obsłużyć człowiek. Gdybyśmy odważyli się określić jednym słowem aktualną sytuację w branży przemysłowego security, bez wątpienia byłaby to „integracja”. W mojej opinii to właśnie Security 4.0 – integracja nie tylko pomiędzy człowiekiem a technologią, ale również między różnymi wysoko wyspecjalizowanymi zespołami. I jest to zmiana, która raczej nie będzie na nikogo czekać.

Jak wobec tego nie wypaść z pędzącego ekspresu? Jaka jest obecnie rola działu bezpieczeństwa w organizacji? Taka sama jak zawsze. Odpowiedź na to pytanie została już dawno udzielona w biblii bezpieczników, wydawanej od końca lat 70. książce *Effective Security Management*[3]: *Dział bezpieczeństwa powinien wykazywać maksymalne zaangażowanie w osiąganie celów organizacji. Zespół security powinien skupiać się nie tylko na problemach security, ale także być wsparciem dla całej organizacji.*

Przez wiele lat praca działów bezpieczeństwa ograniczała się do funkcji „policji zakładowej”. Działy były ulokowane w niemal anegdotycznej zaciemnionej piwnicy ogrzewanej rzędami monitorów wyświetlających obrazy z kamer, a nad drzwiami wejściowymi wisiała tabliczka „Department of NO”[4]. Takie podejście na szczęście się zmienia. To właśnie teraz jest ten czas, kiedy działy bezpieczeństwa mogą pokazać swoją wartość. Security przemysłowe powinno być tam, gdzie coś się dzieje, gdzie są nowe inwestycje, projekty i możliwości. Powinno się zadawać pytanie nie tylko „co złego może się wydarzyć”, ale także „jak możemy organizacji pomóc”.

Moja przemysłowa perspektywa nie pozwala mi zgodzić się na traktowanie działu bezpieczeństwa w kategoriach departamentu, który nie generuje przychodu. Od przynoszenia przychodu jest wprawdzie produkcja, ale wszystkie pozostały komórki organizacyjne działają na rzecz jej wsparcia. Administracja, logistyka, BHP itd. są etatowymi działami loss prevention zapewniającymi utrzymanie ciągłości operacji. Dział security może mieć udział w zapobieganiu stratom związanym z kradzieżami, przestojami produkcji bądź fałszywymi ewakuacjami. Zysk można zwiększać nie tylko poprzez podnoszenie ceny końcowej produktu, ale także obniżenie kosztów jego wytworzenia. Należy szerzej spojrzeć na wartość, jaką może wnosić security, bo to nie tylko klasyczne „łapanie złodzieja".

Brak budżetu na nowe kamery? A może wbudowana w nie analityka nie tylko wykryje wałęsanie się osób w obszarach wrażliwych, ale także pomoże zespołowi z optymalizacji procesów ustalić, gdzie np. następuje stłoczenie palet, które powinny płynnie przepływać w procesie. W obiekcie wystąpiły incydenty pożarowe? Może zespół ochrony warto zaangażować w bezpieczeństwo pożarowe w sposób faktyczny (a nie tylko pozornie). Możliwości i dobre praktyki są, np. NFPA 601 Standard postępowania dla służb ochrony w przeciwdziałaniu stratom związanym z pożarami[5], który miałem okazję wdrażać w dwóch obiektach przemysłowych, w tym w zakładzie dużego ryzyka awarii przemysłowej[6].

A jak mają się do tego kompetencje samego „bezpiecznika”? Myślę, że najlepszej odpowiedzi na to pytanie udzielił kiedyś kolega z branży Sergiusz Parszowski. Zapytany przez młodego adepta sztuki bezpieczeństwa, jakie studia po bezpieczeństwie wewnętrznym radziłby podjąć, odpowiedział krótko: *Idź na zarządzanie – znasz już przepisy, teraz naucz się zarządzać*. Coraz częściej mówi się o tym, żeby „bezpiecznicy” posługiwali się językiem biznesu. Używali ROI, ALARP i innych metod. Ale czy poza znajomością języka biznesu rozumieją też potrzeby biznesu? Czy są na bieżąco z aktualnymi trendami w zarządzaniu? Czy pracują nie tylko nad zwiększaniem budżetu, ale także nad optymalizacją procesów realizowanych wewnątrz swoje-

[1] „Bezpiecznik” – osoba będąca liderem obszaru bezpieczeństwa w swojej organizacji; może to być zarówno menedżer dużego zespołu, jak i specjalista w niewielkiej organizacji.

[2] Rozumianego jako ochrona fizyczna (osobowa) i techniczna obiektów przemysłowych. Używam świadomie terminu security, ponieważ bezpieczeństwo przemysłowe odnosi się do zapewnienia bezpieczeństwa i stabilności procesów przemysłowych, a nie do ich ochrony.

[3] W roku 2020 wyszła jej 7. edycja.

[4] Departament NIE

[5] a&s Polska 1/2020

[6] a&s Polska 2/2020

go działu? Ile procesów w dziale bezpieczeństwa jest zmapowanych, a ile działa siłą rozpędu? Jak często są realizowane wizyty w gemba[7]?

Język biznesu to nie tylko słowa, to też umiejętności korzystania z tych samych narzędzi. Kiedy jedna z niemieckich sieci handlowych umieściła ogłoszenie o pracę do działu bezpieczeństwa, jedną z wymaganych kompetencji była obsługa Power Bi i Power Query, oprogramowania służącego do zarządzania bazami danych. I w sumie nie ma w tym nic dziwnego – *In God we Trust, all others must bring data*[8] – jak mawiał William Deming, tytan nauk o zarządzaniu. Coraz częściej spotykam się z sytuacją, kiedy w praktyce „bezpiecznika" ważniejsza od znajomości wszystkich modeli kamer na rynku jest umiejętność płynnej pracy na tabelach przestawnych w Excelu, aby móc swobodnie śledzić trendy i na ich podstawie wskazywać obszary zagrożone.

Jaki w takim razie powinien być „bezpiecznik" 4.0? Multidyscyplinarny. Potrafiący poprowadzić projekt wymiany systemu monitoringu, zrealizować kampanię *security awareness*, a także zorganizować wartościowe (nie tylko pokazowe) ćwiczenia kryzysowe. A kiedy będzie taka potrzeba – na wykresie pareto zwizualizować aktualne trendy w stratach grup produktowych. Powinien być też aktywny – dyskutować, sprawdzać, testować nowe rozwiązania w obszarach security. Warto też wyjść ze swojej branżowej skorupy. Podpatrzeć, co się dzieje w obszarach BHP, z czym się mierzy środowisko IT. Może się bowiem okazać, że problemy bywają podobne, a nawet ktoś już je rozwiązał. Spojrzenie z poziomu innych działów nie tylko jest odświeżające, ale także pozwoli zapoznać się z inną perspektywą.

Warto też poruszyć temat częstej frustracji „bezpieczników", bo Zarząd nie chce, bo Zarząd nie rozumie. Zarząd może nie rozumie, ponieważ jest to mu przedstawiane nieodpowiednio, albo nie chce, bo ma inne priorytety i widzi tę problematykę w inny sposób. Dział bezpieczeństwa jest jednym z wielu. A że brak wdrożenia systemu kontroli dostępu może skutkować kradzieżą z magazynu części zamiennych? Budżety nie są z gumy, bywa, że trzeba pilnie zainwestować w naprawę maszyny, bez której produkcja nie będzie możliwa. Jednocześnie „bezpiecznik" dobrze zorientowany w organizacji będzie wiedział, że utrata części zamiennych też może wstrzymać produkcję, a na nową dostawę trzeba czekać pół roku.

Inną kwestią jest kultura organizacyjna w danej firmie. Lekceważenie potrzeb w obszarach security może wynikać ustawień systemowych/fabrycznych organizacji albo z systemowych ustawień, gdy Zarząd zakłada a priori: *To się u nas nie zdarzy.* W takiej sytuacji „bezpiecznik" może albo pracować nad świadomością Zarządu, albo… zmienić organizację. We wszystkich znanych mi standardach zarzadzania podstawą wprowadzenia skutecznej zmiany jest zaangażowanie kierownictwa. Bez tego nawet najlepszy ekspert nic nie zdziała.

W pełni zdaję sobie sprawę, że ten tekst jest obarczony wadą dowodu anegdotycznego, ponieważ opiera się tylko na wąskim doświadczeniu moim oraz moich koleżanek i kolegów. Myślę, że teraz mamy bardzo dobry czas dla „bezpieczników". Warto z niego skorzystać, żeby pokazać, jak dużo możemy wnieść do organizacji.

ŁUKASZ STĘPIEŃ

Specjalista z zakresu bezpieczeństwa i zarządzania kryzysowego. Członek Krajowego Stowarzyszenia Ochrony Przeciwpożarowej w USA.

[7] Japoński termin określający „miejsce wykonywania rzeczywistej pracy" związany z metodologią *lean management*

[8] Wierzymy Bogu, wszyscy inni muszą dostarczyć dane

„Bezpieczne” opony z Dębicy

Rozmowa z Pawłem Machetą, Facility Managerem w Firmie Oponiarskiej Dębica

Od 5 lat jest Pan Facility Managerem w Firmie Oponiarskiej Dębica. Na czym polega praca na tym stanowisku?
Zakres obowiązków jest bardzo szeroki. Zajmuję się kompleksowym zarządzaniem infrastrukturą, w tym nieruchomościami oraz sieciami mediów, które są potrzebne do produkcji. Dbam o to, aby pracownicy pracowali w bezpiecznych budynkach, wyposażonych w niezbędny sprzęt i sprawnie działające udogodnienia, a także o ciągłość dostaw mediów potrzebnych do produkcji opon. Poza tym pilnuję, aby wszystkie budynki i budowle spełniały wymagane prawem normy, współpracuję ze służbami, np. strażą pożarną. W zakres moich obowiązków wchodzi także organizacja przeglądów serwisowych urządzeń infrastruktury zakładowej, m.in. systemów zabezpieczeń technicznych. Ponadto zarządzam procesem ochrony fizycznej, czyli wykonuję obowiązki Security Managera.

To szeroki zakres zadań i duża odpowiedzialność. Jakie wyzwania dotyczące zapewnienia bezpieczeństwa stoją przed zakładem produkującym opony?
Oczywiście są zdeterminowane specyfiką zakładu. Fabryka w Dębicy jest jednym z największych tego typu obiektów, zajmuje sporą powierzchnię, na której mieszczą się liczne budynki o różnorodnym przeznaczeniu i konstrukcji. Mamy hale produkcyjne, magazyny surowców, magazyny wyrobów gotowych czy obiekty służące do przetwarzania energii. Pracuje u nas 3 tys. osób. Ponadto współpracujemy z liczną grupą podwykonawców. Nasz zakład mieści się na obrzeżach miasta, w pobliżu linii kolejowej i rzeki, a to wiąże się z koniecznością zastosowania specyficznych zabezpieczeń.
Wyzwań jest zatem sporo, codziennie analizujemy wiele różnorodnych danych, jesteśmy w stałym kontakcie z odpowiednimi służbami spoza zakładu. Jednak za najważniejsze wyzwanie uznałbym zarządzanie przepływem w fabryce. Ruch związany z zaopatrzeniem, transport wewnętrzny związany z przewozem towarów i komponentów między budynkami czy praca służb wsparcia (serwisów, usług, działów utrzymania ruchu) powoduje znaczne jego zagęszczenie. Zakład ma ograniczoną powierzchnię, dlatego dobra organizacja i zarządzanie porządkiem są kluczowe, aby uniknąć sytuacji niebezpiecznych czy zaburzeń sprawnego przepływu.

Opracowanie strategii bezpieczeństwa dla zakładu przemysłowego nie jest zadaniem łatwym, trzeba uwzględnić bardzo dużo zmiennych. Jak wygląda wdrażanie odpowiednich strategii w Dębicy?
Strategia bezpieczeństwa dla każdego obiektu przemysłowego jest inna, ale jest elementem koniecznym i obejmuje bardzo szeroki zakres. Jako zakład produkcyjny w branży motoryzacyjnej obowiązują nas także wytyczne specjalistyczne, np. standardu IATF[1]. Korzystamy również z doświadczeń firm partnerskich, m.in. renomowanej firmy ochrony fizycznej, która wspiera nas w realizacji naszych założeń.
Proces wdrażania strategii bezpieczeństwa nigdy się nie kończy, pojawiają się czynniki, które wymuszają wprowadzanie koniecznych zmian. Nasz zakład ma bogatą historię i na przestrzeni lat elastycznie dostosowywaliśmy strategię do zmieniających się warunków.
Modernizujemy nasze systemy zabezpieczeń. Możemy pochwalić się częściowo już zakończonym projektem unowocześnienia ochrony perymetrycznej polegającym na wymianie systemu monitoringu wizyjnego wzdłuż ogrodzenia na system/kamery z pełną analityką, ułatwiającą dozór granic terenu. Pracownik nie musi już cały czas wpatrywać się w ekrany monitorów, reaguje na alarm generowany automatycznie. Ponadto te zdarzenia są już wstępnie sklasyfikowane, więc liczba fałszywych alarmów została znacząco zredukowana.
Drugim takim projektem jest automatyzacja bramy wjazdowej, gdzie system odczytuje tablice rejestracyjne pojazdu i na podstawie wcześniej wprowadzonych uprawnień KD przyznaje dostęp na teren zakładu.

1 IATF to standard w branży motoryzacyjnej, który dotyczy wymagań stawianych systemom zarządzania w przemyśle motoryzacyjnym. Jest uznawany przez wszystkich producentów samochodów na całym świecie i wymagany w łańcuchu dostaw.

Firma Oponiarska Dębica to wiodący na polskim rynku producent opon do samochodów osobowych, dostawczych i ciężarowych. Od 1995 roku inwestorem strategicznym w spółce jest amerykański koncern The Goodyear Tire & Rubber Company

Powierzchnia zakładu: ponad **50 ha**

Budynki: ponad **30**

Bramy: **2** osobowe **2** samochodowe

W branży ochrony jest jeszcze wielu sceptyków stosowania najnowszych technologii. Jakie stanowisko Pan reprezentuje?
Jestem gorącym zwolennikiem cyfryzacji i zdobyczy nowych technologii. Dzięki nim możemy pozyskiwać duże ilości danych, które pozwalają nam poznać coraz dokładniejszy obraz naszej sytuacji i dobrać lepsze, bardziej adekwatne rozwiązania. Najnowsze technologie pozwalają nam działać w sposób bardziej przemyślany i efektywny. Dzięki nim po prostu sami stajemy się nowocześniejsi. Mamy to szczęście, że wreszcie doczekaliśmy się czasów, kiedy technologia odpowiednio zastosowana jest znacznie tańsza i skuteczniejsza od rozwiązań opartych głównie na zwiększaniu zatrudnienia.
W naszym zakładzie wdrażamy nowoczesne rozwiązania do systemów monitoringu wizyjnego, kontroli dostępu, mamy zautomatyzowane sterowanie ruchem przez bramy, na bieżąco monitorujemy pojawiające się zdarzenia.

W obecnej sytuacji nie może zabraknąć pytania o zawirowania spowodowane pandemią i wojną w Ukrainie. Czy odczuwacie ich skutki?
Jesteśmy obecni w Dębicy już od ponad 80 lat, mamy zatem doświadczenia poprzednich czasów dotyczące utrzymania stabilności i ciągłości działania. I z tego dziedzictwa czerpiemy. Jeśli chodzi o wojnę w Ukrainie, to na bieżąco monitorujemy sytuację, zwracamy uwagę na wszelkie sygnały i zachowujemy dynamizm w działaniu.
Natomiast pandemia COVID-19 postawiła przed chyba każdym zakładem produkcyjnym bezprecedensowe zadania. Musieliśmy działać tak, aby przede wszystkim zapewnić bezpieczeństwo sanitarne wszystkim naszym pracownikom. Firma Oponiarska Dębica kierowała się przy tym głównie wytycznymi sanepidu i aktualizowanymi na bieżąco przepisami. Najważniejszym zadaniem, jakie sobie postawiliśmy, było zachowanie bezpiecznego dystansu pomiędzy osobami i niedopuszczenie do mieszania się strumieni osób wchodzących do pracy i wychodzących z niej, ponieważ pracujemy w trybie 24-godzinnnym. W tym celu dostosowaliśmy specjalnie wejścia do zakładu i wyjścia z niego, oznakowaliśmy bezpieczne odległości, zadbaliśmy także o bezpieczeństwo sanitarne, m.in. w stołówkach zakładowych. Nasi pracownicy od początku pandemii otrzymywali maseczki, szeroko udostępnialiśmy także środki dezynfekujące do rąk i powierzchni. Całość zadań była koordynowana przez specjalny dział zajmujący się tym zagadnieniem przy współpracy z naszymi partnerami lokalnymi: firmą ochrony fizycznej oraz serwisem utrzymania czystości.
Nie da się ukryć, że odczuliśmy konsekwencje zahamowania płynności w łańcuchach dostaw, jeśli chodzi zarówno o rozbudowę systemów zabezpieczeń, jak i ich modernizację. Dostępność nowych technologii była mocno ograniczona. Na pewno wydłużył się czas oczekiwania na urządzenia, co musieliśmy uwzględnić w naszych planach.

Obudowy kamer do zadań specjalnych

Ostatnie fale upałów utrudniły życie ludziom na całym świecie. Według National Center for Environmental Information lata 2013-2021 znalazły się wśród dziesięciu najcieplejszych w historii. Jeśli ta tendencja się utrzyma, kamery CCTV do zastosowań zewnętrznych będą musiały być wyposażone w obudowy termoodporne, aby przetrwać w wysokich temperaturach.

Typowe kamery IP są zaprojektowane do pracy w temperaturze od -20 do 60°C. Tego lata w wielu miejscach na świecie temperatura dochodziła do 40°C. Kamery umieszczone wewnątrz metalowej obudowy, która jest wystawiona na działanie słońca, mogą nagrzać się nawet do 70°C. Wiele urządzeń elektronicznych jest konstruowanych tak, aby wytrzymały ogrzanie do 80°C, jednak zalecana górna granica pracy to 35°C. Utrzymujące się wysokie temperatury mogą prowadzić do trwałego uszkodzenia elektroniki. Systemy telewizji dozorowej mogą, ale nie muszą działać poprawnie w obliczu ekstremalnych warunków otoczenia.

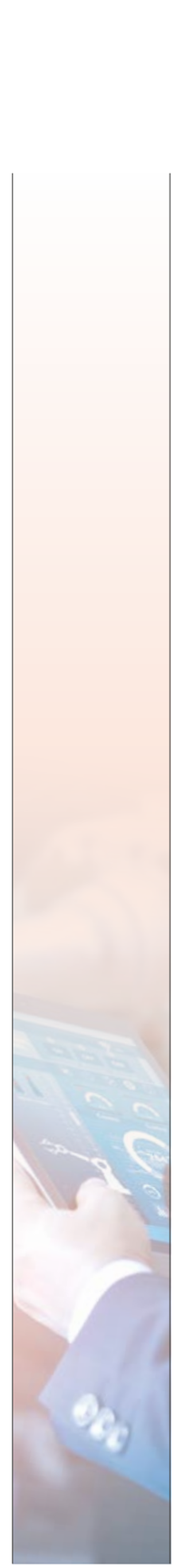
Podobny wpływ na kamery CCTV ma mroźna pogoda. Groźna może być temperatura poniżej -20°C. Wówczas mogą przestać działać np. kamery zasilane bateryjnie ze względu na szybko rozładowujące się baterie zasilające. Na rynku są dostępne przemysłowe kamery IP, które wytrzymują wysoką temperaturę, ale są to produkty niszowe, stosowane np. do dozoru pieców przemysłowych. Ich odporne mechanicznie obudowy o wzmocnionej konstrukcji zostały zaprojektowane do pracy w trudnych, niebezpiecznych lub korozyjnych warunkach dozoru zewnętrznego.

RODZAJE OBUDÓW KAMER IP

Obudowa kamery jest dla nich tym, czym skorupa dla żółwia. Jednak różne środowiska pracy będą wymagać zastosowania innego rozwiązania. Jeden rodzaj nie spełni wszystkich wymagań.
Występują trzy główne rodzaje obudów kamer przeznaczonych do pracy w niekorzystnych warunkach:

1. Odporne na ekstremalne temperatury (nadmierne ciepło i zimno/upał, siarczysty mróz)
2. Przeciwwybuchowe (iskrobezpieczne)
3. Ciśnieniowe *(pressurized bubbles)*.

Pojęcia „odporna na temperaturę” i „przeciwwybuchowa” nie mogą być stosowane zamiennie. Obudowa termoodporna umożliwia pracę kamer w temperaturach od około -30 do 150°C. Z kolei obudowy kamer w wykonaniu przeciwwybuchowym są samoistnie (dzięki konstrukcji) iskrobezpieczne, co czyni je idealnym rozwiązaniem do pracy w środowiskach wysoko łatwopalnych, takich jak rafinerie ropy naftowej i gazu. W związku z tym muszą posiadać certyfikat zgodności z określonymi normami NEMA[1] i UL[2].



OCENA LOKALIZACJI: WYBÓR ODPOWIEDNIEJ OBUDOWY I AKCESORIÓW

Przed podjęciem decyzji o wyborze obudowy warto przeprowadzić analizę terenu i ocenić środowisko pracy kamery pod kątem czynników, które mogą potencjalnie zagrażać jej poprawnemu funkcjonowaniu.

1. CZY KAMERY BĘDĄ MUSIAŁY PRACOWAĆ W EKSTREMALNYCH TEMPERATURACH?

Ponieważ warunki środowiskowe znacznie się różnią w zależności od projektu, należy brać pod uwagę charakterystykę danej lokalizacji. Obudowy kamer CCTV przeznaczonych do pracy w ekstremalnie wysokich temperaturach są zwykle wyposażone w osłonę przeciwsłoneczną i wentylator. Osłona chroni kamerę przed słońcem lub deszczem, obniżając temperaturę o 3 do 5°C. Wentylatory włączają się przy ustalonej temperaturze (zwykle 35°C), pomagając w rozproszeniu ciepła, i wyłączają się automatycznie przy 25°C.
W przypadku ekstremalnie niskich temperatur kamerę można wyposażyć w grzałkę, która włącza się przy -15°C i wyłącza przy 25°C. Kamery z grzałkami mogą pracować nawet do -35°C. Jednak części ruchome (np. wentylatory lub grzałki) są podatne na awarie. Jeśli zewnętrzna kamera dozorowa będzie narażona na działanie ekstremalnych temperatur, należy rozważyć model z mniejszym wentylatorem i o szerokim zakresie temperatury pracy.

2. CZY KAMERY BĘDĄ NARAŻONE NA DZIAŁANIE WARUNKÓW KOROZYJNYCH?

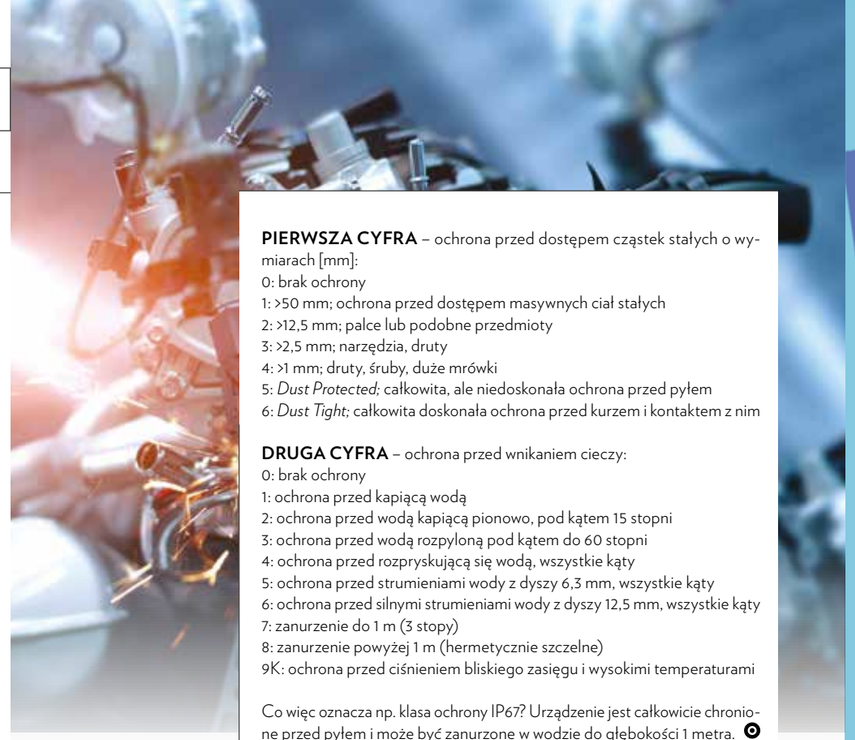
W przypadku bezpośredniego narażenia na korozję i ekstremalne warunki atmosferyczne, np. w portach morskich lub na pokładach statków, obudowa może szybko ulec zniszczeniu (skorodować), powodując zmianę pola widzenia kamery, zmianę/osłabienie zamocowania obudowy lub odsłonięcie przewodów. Może to prowadzić do wielu problemów, takich jak oderwanie obudowy czy utrata sygnału wizyjnego.
Równie ważna jest ochrona wnętrza obudowy poprzez utrzymywanie w niej nadmiarowego ciśnienia suchego azotu lub gazu innego rodzaju. Gdy ciśnienie wewnętrzne jest wyższe niż ciśnienie na zewnątrz, elementy zewnętrzne nie mogą dostać się do wnętrza, które jest skutecznie chronione przed uszkodzeniem. Największym problemem w przypadku obudów ciśnieniowych lub obudów, które są iskrobezpieczne, np. przeciwwybuchowych, jest ich konserwacja.

3. CZY KAMERY BĘDĄ NARAŻONE NA DZIAŁANIE PYŁU?

Tak jak każde urządzenie pracujące w środowisku o dużym zapyleniu, ciśnieniowa kamera kopułkowa będzie wymagała typowego czyszczenia, wycierania lub czyszczenia ciśnieniowego. Struktury wewnętrzne nie wymagają jednak konserwacji. Jeśli obudowa jest ciśnieniowa, kamera ma tendencję do stabilniejszej pracy niż jej odpowiedniki bez ciśnienia, ponieważ żadne elementy zewnętrzne nie przedostaną się do podzespołów. Gdy z kamerą dzieje się coś niepokojącego lub trzeba dostać się do jej środka, obudowę trzeba rozszczelnić.
Częsta konserwacja jest konieczna w przypadku niesprzyjającego środowiska pracy. Wystarczy kilka tygodni, aby czyszczenie było potrzebne. Niestety nie zawsze przestrzega się harmonogramu konserwacji oraz zakupu potrzebnych środków i narzędzi czyszczących. Produkty przeznaczone do bezpiecznego czyszczenia obiektywów zewnętrznych i obudów kamer w dowolnych kształtach z poziomu gruntu są dostępne.

---

[1] National Electrical Manufacturers Association (Amerykańskie Stowarzyszenie Producentów Aparatury Elektrycznej) – amerykański odpowiednik klasy ochronności IP.
[2] Underwriters Laboratories (UL) – amerykańska organizacja zajmująca się bezpieczeństwem, która wyznacza branżowe standardy dla nowych produktów.



Aby dowiedzieć się, jak wytrzymały na wodę lub pyłki jest produkt, lepiej nie polegać na uogólnionych terminach, takich jak „wodoodporny" lub „pyłoszczelny", lecz odnieść się do klasyfikacji IP produktu – *Ingress Protection* (znanej również jako *International Protection)*, np. IP55, IP67 czy IP69K.

JAK INTERPRETOWAĆ KLASY OCHRONY OBUDOWY IP

Kod IP składa się z dwóch podstawowych elementów: ochrona przed cząstkami stałymi – pierwsza cyfra (od 0 do 6) oraz ochrona przed wnikaniem cieczy – druga cyfra (od 0 do 9). Praktyczną zasadą jest to, że im wyższa cyfra, tym urządzenie jest bardziej chronione.

PIERWSZA CYFRA – ochrona przed dostępem cząstek stałych o wymiarach [mm]:
0: brak ochrony
1: >50 mm; ochrona przed dostępem masywnych ciał stałych
2: >12,5 mm; palce lub podobne przedmioty
3: >2,5 mm; narzędzia, druty
4: >1 mm; druty, śruby, duże mrówki
5: *Dust Protected;* całkowita, ale niedoskonała ochrona przed pyłem
6: *Dust Tight;* całkowita doskonała ochrona przed kurzem i kontaktem z nim

DRUGA CYFRA – ochrona przed wnikaniem cieczy:
0: brak ochrony
1: ochrona przed kapiącą wodą
2: ochrona przed wodą kapiącą pionowo, pod kątem 15 stopni
3: ochrona przed wodą rozpyloną pod kątem do 60 stopni
4: ochrona przed rozpryskującą się wodą, wszystkie kąty
5: ochrona przed strumieniami wody z dyszy 6,3 mm, wszystkie kąty
6: ochrona przed silnymi strumieniami wody z dyszy 12,5 mm, wszystkie kąty
7: zanurzenie do 1 m (3 stopy)
8: zanurzenie powyżej 1 m (hermetycznie szczelne)
9K: ochrona przed ciśnieniem bliskiego zasięgu i wysokimi temperaturami

Co więc oznacza np. klasa ochrony IP67? Urządzenie jest całkowicie chronione przed pyłem i może być zanurzone w wodzie do głębokości 1 metra.

KAMERA PRZECIWWYBUCHOWA

CBC POLAND

www.cbcpoland.pl

MAXIMUS MMX – przeciwwybuchowa kamera Full HD w kompaktowej obudowie

MAXIMUS MMX JEST PRZEZNACZONA DO SKUTECZNEGO DOZORU WIZYJNEGO I KONTROLI PROCESÓW W ŚRODOWISKACH NIEBEZPIECZNYCH Z OBECNOŚCIĄ W POWIETRZU GAZÓW PALNYCH LUB PYŁÓW, TYPOWYCH DLA SEKTORÓW PETROCHEMICZNEGO, MORSKIEGO, PRZEMYSŁOWEGO I SPOŻYWCZEGO.

Przetwornik CMOS EXMOR Full HD (1080p) zapewnia bardzo dobrą jakość obrazu nawet w skrajnie trudnych warunkach oświetlenia. Obiektyw zdalnie regulowany jest dostępny w dwóch wariantach: 3x (3 – 9 mm) oraz 10x (5,1 – 51 mm). Zaletą kamery MAXIMUS MMX jest jej niezwykle łatwy i bezpieczny montaż. Można ją zasilać m.in. w trybie PoE+, co dodatkowo upraszcza prace instalacyjne. Kamera spełnia najwyższe standardy bezpieczeństwa cyber-security, m.in. firmware szyfrowany z kryptopodpisem, dostęp do zasobów zabezpieczony hasłem (http digest), komunikacja szyfrowana https z użyciem TLS1.0|1.1|1.2|1.3, zgodność ze specyfikacją ONVIF Security Service.
Kamera MAXIMUS MMX jest gwarancją ekstremalnej wytrzymałości i niezawodności, potwierdzonej setkami testów. Mechanika, elektronika, pozycjonowanie, praca w sieci, oprogramowanie układowe są opracowywane od początku do końca przez wewnętrzny zespół VIDEOTEC z siedzibą we Włoszech.
Produkt MMX jest certyfikowany przez Lloyd's Register Specification Number 1, dlatego może być używany w zastosowaniach morskich i przybrzeżnych (*onshore/offshore*) w kategoriach środowiskowych ENV1, ENV2, ENV3 i ENV5.
Ma również certyfikaty uprawniające do użytkowania w strefach przemysłowych 1 i 2 (grupa IIB T6 lub T5 grupa – gaz) oraz w strefach 21 i 22 (grupa IIIC T85°C lub T100° – pył).
Konstrukcja całej obudowy MMX jest wykonana ze stali nierdzewnej AISI 316L zapewniającej klasy szczelności IP66/IP67/IP68/IP69 z gwarancją pełnej ochrony przed wpływem warunków atmosferycznych, włącznie z zanurzeniem w wodzie. Spełnia normy EN50130-5 oraz EN60068-2-6, a przeciwwybuchowe właściwości kamery są potwierdzone certyfikatami ATEX (EN IEC 60079-0, EN 60079-1, EN 60079-31) oraz IECEx i EAC EX.
Kolejną ważną cechą kamery MAXIMUS MMX jest rozszerzony zakres temperatury pracy od -40 do +70°C oraz wilgotności od 5% do 95%. Urządzenie ma wbudowaną funkcję rozmrażania umożliwiającą zimny start w temperaturze od -40 do -10°C.

Jak kompleksowo dbać o bezpieczeństwo

w branży przemysłowej

Obiekty przemysłowe mają kluczowe znaczenie dla gospodarek państw. Priorytetem zatem jest odpowiednie podejście do projektowania systemów dozoru obiektów przemysłowych, zarówno w kontekście ochrony perymetrycznej, jak i właściwego zabezpieczenia linii produkcyjnych. Tak szerokie spektrum potrzeb wymaga wdrożenia kompleksowych rozwiązań z zakresu monitoringu wizyjnego, technologii audio i analityki.

W przemyśle wszystkie elementy ochrony muszą być idealnie dopasowane, by zminimalizować wystąpienie incydentu, który mógłby spowodować np. spadek wydajności linii produkcyjnej. Podobnie jest z sieciowymi systemami dozoru wizyjnego – komplementarność wdrażanych rozwiązań umożliwia szybsze przekazywanie informacji między urządzeniami, tym samym wpływając na stopień ochrony danego obiektu.

Zakłady przemysłowe to przeważnie duże kompleksy wymagające stałej ochrony, także pod kątem bezpieczeństwa pracowników przebywających na terenie produkcyjnym. Dlatego też wdrożenie zintegrowanego systemu bezpieczeństwa w modelu *end-to-end* jest wartością dodaną dla przedsiębiorstwa z różnych powodów – nie tylko pod względem kompleksowej ochrony całego obiektu, ale także na potrzeby wyciągania wniosków poprawiających bezpieczeństwo i optymalizujących pracę całego obiektu.
Rozległe powierzchnie oraz infrastruktura krytyczna czy przemysłowa muszą podlegać dozorowi najwyższej jakości, aby nie doszło do zagrożeń dla życia ludzi i majątku. Rozwój technologiczny rozwiązań ochrony zewnętrznej obiektów przemysłowych obejmuje m.in. systemy wizyjnego dozoru perymetrycznego zapewniające wykrywanie i weryfikowanie potencjalnego intruza na granicy terenu zakładu w czasie rzeczywistym. Wbudowane inteligentne narzędzia analityczne mogą uruchamiać automatyczne ostrzeżenia i alarmować pracowników ochrony, eliminując zbędny czas oraz koszty rutynowych patroli i fałszywych alarmów.
Ponadto mają możliwość generowania komunikatów audio, których celem jest odstraszanie intruzów. Kolejną warstwą jest ochrona obszaru pozwalająca śledzić obiekty w ruchu, np. auta. Dostarcza cenne informacje o lokalizacji, prędkości przemieszczania się, a nawet odległości między nimi. Kamery mają również możliwość sczytywania tablic rejestracyjnych.
Trzecią warstwę stanowi kontrola obiektów, w tym szczególnie ważna kontrola dostępu. Umożliwia monitorowanie wejść i wyjść personelu upoważnionych do danych stref, a nawet pokojów pracowników czy urządzeń w danym budynku. Coraz chętniej wybierane są rozwiązania bezdotykowe, np. identyfikacja za pomocą kodów QR, które wypierają popularne karty dostępu.
Zauważalnym trendem jest także wzrost zainteresowania tymczasowymi systemami ochrony perymetrycznej. Tego typu mobilna konstrukcja może stanąć na określony czas w miejscu robót budowlanych, a następnie zostać zdemontowana, a kamery przeniesione i włączone w system dozoru obiektu.
Zarządzający zakładami przemysłowymi coraz częściej przed wyborem systemu decydują się także na jego sprawdzenie, tzw. test w polu. Głównym kryterium wyboru w przetargach staje się bowiem jakość, nie tylko cena. Tańsze kamery mogą okazać się awaryjne lub nie spełniać deklarowanych w dokumentach parametrów. Po przeprowadzeniu testów coraz więcej firm przychyla się do wyboru urządzeń o wyższej jakości, które pozwalają obniżyć koszty ich utrzymania w przyszłości, bez konieczności napraw czy wymiany.

PEŁNA OCHRONA ZAKŁADU PRZEMYSŁOWEGO

Wyobrażając sobie zakład przemysłowy, mamy na myśli ogromną halę produkcyjną z przestronnym, przynależącym do niego otoczeniem zewnętrznym. By skutecznie monitorować rozbudowaną przestrzeń, pomocne będą rozwiązania łączące możliwości dozoru wizyjnego, IP audio i kontroli dostępu. Tak rozbudowany system będzie szczególnie cenny w przypadku np. nieautoryzowanego wtargnięcia na teren zakładu. Wówczas kamery przystosowane do detekcji podejrzanego zachowania i podążania za obiektem w ruchu są w stanie wykryć niepowołaną osobę. Dzięki zainstalowanym w urządzeniu funkcjom analitycznym kamera może wysłać odpowiedni komunikat pracownikom ochrony budynku.
Z kolei urządzenia wyposażone w systemy IP audio umożliwiają emitowanie komunikatów, których zadaniem jest odstraszenie intruza. Uzupełnieniem będą też rozwiązania kontroli dostępu zezwalające na dostęp do wybranych stref tylko osobom do tego upoważnionym.

– *Technologie dozoru wizyjnego muszą być również właściwie zarządzane. Tym, co może mieć kluczowe znaczenie w administrowaniu wielowymiarowym systemem bezpieczeństwa, jest skrojone na miarę oprogramowanie do zarządzania materiałem wizyjnym – AXIS Camera Station, opracowane nie tylko z myślą o różnorodnych typach instalacji, ale także nieskomplikowane w obsłudze, zapewniające szybki dostęp do najważniejszych danych* – mówi Dagmara Pomirska z Axis Communications. – *Oprogramowanie powinno uwzględniać najważniejsze potrzeby przedsiębiorstwa: od eksportowania materiału wideo i jego analizy, po obsługę głośników sieciowych, wideodomofonów i kontakt z personelem* – dodaje.

BEZPIECZEŃSTWO PRACOWNIKÓW

Kamery rozlokowane w całym zakładzie mogą wychwycić potencjalne zagrożenia dla przebywających w nim osób. Przykładowo, kamery termowizyjne są w stanie wykryć niebezpieczny wzrost temperatury, np. na linii produkcyjnej, a następnie przekazać zebrane dane do zintegrowanego systemu powiadomień audio, który wyemituje ostrzeżenie. Zautomatyzowane systemy pozwalają również stworzyć tzw. niewidzialne linie, czyli strefy, których przekroczenie mogłoby stanowić bezpośrednie zagrożenie zdrowia pracowników. Połączone systemy audio-wideo są w stanie wykryć obecność osoby przebywającej w strefie zagrożenia, a następnie wysłać odpowiedni komunikat nakazujący opuszczenie obszaru.
Połączenie systemów dozoru wizyjnego z technologiami IP audio może również być pomocne przy weryfikacji tego, czy pracownicy stosują odpowiednie zabezpieczenia podczas przebywania na terenie zakładu, np. czy prawidłowo noszą kaski. Kamera jest w stanie wychwycić osobę, która nie stosuje wymaganych środków ochrony osobistej, i przekazać tę informację do systemu powiadomień audio.

OPTYMALIZACJA PROCESÓW I WYCIĄGANIE WNIOSKÓW DZIĘKI ANALITYCE

Dzięki integracji różnych rozwiązań sieciowych możliwa jest także analiza procesów zachodzących w zakładzie, co pozwala zwiększyć wydajność operacyjną przedsiębiorstwa i zoptymalizować prace wykonywane na terenie zakładu. Umieszczenie kamer w strategicznych miejscach, np. nieopodal linii produkcyjnej, ma kluczowe znaczenie w weryfikacji tego, czy cały proces przebiegł zgodnie z określonymi procedurami. Dane pozyskane z monitoringu są na bieżąco, nieprzerwanie analizowane w kamerze. Zastosowane algorytmy są w stanie wychwycić ewentualne błędy czy awarie maszyn. Zebrane informacje są przekazywane do oprogramowania zarządzającego materiałem wizyjnym, dzięki czemu operator ma bezpośredni wgląd w sytuację i może zasygnalizować wystąpienie problemu.

– *Jedną z największych zalet implementacji zintegrowanego systemu dozoru end-to-end jest jednoczesna zdalna kontrola wielu procesów oraz szybkie reagowanie w momencie wystąpienia zakłóceń – często bez konieczności przerywania działań. Ma to kluczowe znaczenie w przypadku weryfikacji np. sprawności urządzeń. Kamery dozorowe połączone z aplikacjami analitycznymi i systemami powiadamiania umożliwiają podjęcie natychmiastowych działań w celu zażegnania problemu na jego wczesnym etapie. To ważny aspekt pod względem działalności całego zakładu – może wpłynąć na znaczne oszczędności finansowe dzięki uniknięciu konieczności przeprowadzania kosztownych napraw* – zaznacza Dagmara Pomirska z Axis Communications.

Głos branży

JAK ZAPEWNIĆ BEZPIECZEŃSTWO I SPRAWNE FUNKCJONOWANIE OBIEKTÓW PRZEMYSŁOWYCH, ZWŁASZCZA W DOBIE ZAWIROWAŃ GOSPODARCZYCH? SWOIMI RADAMI DZIELĄ SIĘ PRZEDSTAWICIELE RÓŻNYCH SEKTORÓW RYNKU.

Janusz Syrówka

eon

Zapewnienie ciągłości działania

Doświadczenia wyniesione z pandemii oraz informacje płynące z Ukrainy dają wiele do myślenia i zrobienia w obszarze zapewnienia ciągłości działania. Wcześniejsze plany na wypadek sytuacji kryzysowych okazały się niekompletne w konfrontacji z nowymi problemami. Pandemia była wyzwaniem dla zapewnienia dostępności pracowników. Testowano różne rozwiązania, łącznie ze skrajnymi pomysłami, takimi jak „skoszarowanie" kluczowego personelu.
Jak zwykle pomocne w rozwiązaniu problemów były znajomość organizacji i procesów, sprawna komunikacji i możliwość podejmowania szybkich decyzji. Wydaje się to tak oczywiste i automatyczne niemalże, ale bez odpowiedniego wcześniejszego przygotowania organizacje są skazane na chaos w momencie, gdy kryzys przyjdzie.
Wojna w Ukrainie, poza całą tragicznością wydarzeń, uświadomiła mi, że nawet najbardziej nieprawdopodobne scenariusze mogą się zmaterializować. W tym ten zakładający kryzys totalny, który może dotknąć wszystkich aspektów działalności. Wymaga to szerokiego spojrzenia na organizację i przygotowanie jej na sytuację, gdy „wszystko" przestaje działać. Mimo że ta sytuacja wyjściowa zdaje się beznadziejna, to okazuje się, że jednak jest pole do manewru i można wypracować rozwiązania, które pozwolą przetrwać. Nie są to sprawy proste i szybkie do przeprowadzenia. Każdy dzień jest cenny i warto zainwestować uwagę i zaangażowanie, aby, jak mówią, „naprawić dach, gdy świeci słońce".
Z bardziej praktycznych aspektów zapewnienia ciągłości działania firmy ogromnym problemem pozostaje zapewnienie ciągłości łańcucha dostaw. Chodzi o zapewnienie nie tylko materiałów do produkcji, ale także ciągłości usług dostarczanych przez podwykonawców. Dotyczy to także branży bezpieczeństwa. Trzeba zadać trudne pytania, np. związane z utrzymaniem systemów bezpieczeństwa czy dotyczące ochrony fizycznej w momencie mobilizacji. Nie na wszystkie tego typu pytania przyjdzie łatwa odpowiedź, ale teraz jest ten czas, aby się z nimi zmierzyć.

Artur Pollak

APA Group

Niezbędne cyber-bezpieczeństwo

Przemysł 4.0 kumuluje dane i dostarcza dużych zbiorów danych. Składają się na nie totalna integracja na poziomie systemów kontroli dostępów, monitoringu CCTV, systemów alarmowych i przeciwpożarowych, strumieni danych infrastruktury produkcyjnej i budynkowej.
Cyberbezpieczeństwo otacza transfer danych, anonimizuje je po to, by *big data* mogła funkcjonować w sposób bezpieczny. Dane i wnioski nie mogą wpaść w niepowołane ręce. A już szczególnie w obliczu dynamicznej transformacji cyfrowej spowodowanej pandemią i toczącej się wojny w Ukrainie.
Systemy z obszaru cybersecurity to dzisiaj element niezbędny, mający zapewnić niezachwianą ciągłość procesów w organizacji. Służy temu szereg narzędzi wewnętrznych:
- automatyczny system kopii zapasowych całego środowiska wraz z harmonogramem,
- rotacja danych kopii zapasowych oraz łatwy dostęp poprzez serwery Samba i ftp,
- zabezpieczenie sprzętu i infrastruktury sieciowej przez odseparowane i zabezpieczone podsieci VLAN dla użytkowników i urządzeń Internetu rzeczy,
- rozbudowane reguły firewalla sprzętowego,
- ograniczenia dostępu dla użytkowników i urządzeń,
- strefa DMZ *(Demilitarized Zone)* jako dodatkowa ochrona usług publicznych,
- wychwytywanie zdarzeń nietypowych,
- dynamiczne listy zablokowanych IP czy odporność na ataki z sieci.

Na rynku są gotowe platformy, które można szybko włączyć w ekosystem przedsiębiorstwa. Jeżeli ktoś jeszcze o tym nie pomyślał, lepiej, aby zadziałał teraz i nie czekał na sprawdzenie się powiedzenia „mądry Polak po szkodzie" na własnej skórze.

Mirosław Lukowski

ekspert

Nowe czasy, nowe wyzwania

Zarówno pandemia, wojna w Ukrainie, jak i sytuacja gospodarcza Polski stwarzają nowe zagrożenia, a co za tym idzie nowe wyzwania dla branży bezpieczeństwa. Wojna hybrydowa powoduje, że przedsiębiorstwa, których znaczenie dla gospodarki jest wiodące, są narażone na ataki hakerów, co wymusza działania bezpieczeństwa w cyberprzestrzeni.
Niejednokrotnie systemy zabezpieczeń w zakładach przemysłowych były integrowane z wewnętrznymi sieciami w celu ułatwienia obsługi osobom odpowiedzialnym. Dziś dla wprawnych hakerów atak na ważną gałąź przemysłu nie stanowi problemu, dlatego tak istotne jest, by w świecie cyfrowym zagwarantować odpowiednie poziomy bezpieczeństwa – odseparować i zabezpieczyć systemy zabezpieczeń od sieci wewnętrznych.
Przez lata względnego spokoju bezpieczeństwo opierało się niejednokrotnie na systemach największych producentów. Dziś mamy świadomość, iż taka sytuacja niesie ze sobą zagrożenie, gdyż nie jesteśmy w stanie jednoznacznie stwierdzić, czy światowa potęga technologiczna jest po właściwej stronie konfliktu i czy jej systemy nie ułatwią dostępu hakerom biorącym udział w wojnie hybrydowej.
Co więc można zrobić, by zabezpieczyć nasze systemy?
Moim zdaniem powinniśmy zacząć od zapoznania się z najbardziej czarnymi scenariuszami i wyeliminowania potencjalnych zagrożeń, odseparowując systemy zabezpieczeń od możliwości dostania się do ich wnętrza poprzez darmowe platformy do zarządzania czy korzystanie z sieci publicznych. Istnieją platformy, takie jak PSIM, które niezależnie od zastosowanych rozwiązań technologicznych pozwalają na zarzadzanie dające kontrolę.
Dziś sektor przemysłowy z jednej strony oczekuje zwiększenia bezpieczeństwa zarówno fizycznego (inflacja, pandemia i wojna powodują, że rośnie ryzyko działań o charakterze kryminalnym), jak i bezpieczeństwa systemów wsparcia. Niestety ze względu na wyższe koszty dla wielu kluczowa jest optymalizacja. Rynek oferuje rozwiązania i wysokiej klasy technologie, które są w stanie wspierać bezpieczeństwo, ważne by przy wyborze właściwych korzystać z wiedzy i doświadczenia osób zajmujących się bezpieczeństwem. Realna ocena ryzyka, ustalenie kluczowych dla każdego, indywidualnych zagrożeń powoduje, że zastosowane technologie są efektywne i realnie poprawiają bezpieczeństwo, z korzyścią dla klienta końcowego.

Krzysztof Pohorecki

BlackOnion RC

Świadomość zagrożeń

Luty 2022 r. przejdzie do historii nie tylko jako miesiąc otwartego ataku Rosji na Ukrainę w skali otwartej wojny (poprzednie ataki były mniej lub bardziej ograniczone), ale też jako miesiąc, w którym świat biznesu, w tym branża security, został skonfrontowany z materializacją scenariusza z gatunku „mało prawdopodobne". Nauczony tym doświadczeniem nie podejmę się próby przewidywania, co się stanie w dalszej czy nawet w bliskiej przyszłości.
Spróbuję podzielić się kilkoma wnioskami, jakie wyciągam z ostatnich wydarzeń i staram się je uwzględnić w codziennej działalności.
Sprawa pierwsza: „Plan jest niczym, planowanie jest wszystkim" – w sytuacjach kryzysowych i dynamicznych dobrze zorganizowany proces, profesjonalne zespoły, szybka komunikacja i ścieżka decyzyjna stają się ważniejsze niż tomy wcześniej przygotowanych planów i procedur.
Sprawa druga: Przywództwo i świadomość zagrożeń – liderzy biznesowi powinni z wielką uwagą słuchać swoich „bezpieczników", szybko przyswajać i wprowadzać w życie ich sugestie. Włączenie branży security w najważniejsze procesy decyzyjne jest nie tylko sensowne, ale przede wszystkim dowodzi mocnego instynktu samozachowawczego.
Sprawa trzecia: Tanio już było – przyszedł czas na szybkie inwestycje w bezpieczeństwo i skorzystanie z tych wszystkich zaoszczędzonych na przycinaniu budżetów środków, o których biznes już dawno zapomniał, a sytuacja wymusza ich gwałtowne zwiększenie. Technologie, wiedza i doświadczenie dostępne na rynku dają praktycznie nieograniczone możliwości obrony, ale również ataku. Granice są tylko w głowach i budżetach. Warto korzystać z mądrych i doświadczonych zespołów i warto im bardzo dobrze płacić.

Paweł Grzywa

Securitas Polska

Zadania firm ochrony

Zmieniające się otoczenie biznesowe i sytuacja międzynarodowa sprawiają, że przed firmami ochrony pojawiają się nowe wyzwania w zakresie prowadzenia biznesu, takie jak zachowanie ciągłości łańcucha dostaw, rosnące koszty surowców i mediów oraz związane z tym spowolnienie gospodarcze.
Z kolei inflacja podtrzymuje wysokie oczekiwania płacowe pracowników i w konsekwencji rosnące koszty pracy, a pozyskanie odpowiedniej liczby doświadczonych i wykwalifikowanych pracowników ochrony powoli też staje się wyzwaniem. Przyszły rok będzie czasem wyjątkowym, po raz pierwszy w historii dwukrotnie nastąpi wzrost płacy minimalnej – i będzie to zmiana, z którą przyjdzie się nam mierzyć razem z klientami. Obiekty przemysłowe już dawno wpisały się w trend redukcji i optymalizacji posterunków ochrony, a nadchodzące zmiany rynkowe na pewno go pogłębią.
Sektor przemysłowy to także obszar optymalizacji zasobów wewnętrznych firm, a to skutkuje przekazywaniem firmom ochrony dodatkowych zadań, które nie zawsze są bezpośrednio związane z ochroną obiektów. W mojej ocenie firmy ochrony w swoich działaniach powinny koncentrować się na bezpieczeństwie, wykazywać inicja-

tywę w dostosowywaniu portfolio usług do potrzeb klientów, rekomendować integrację systemów oraz nowe, innowacyjne rozwiązania automatyzujące procesy. Wszystko to będzie miało na celu optymalizację kosztów.
Naszym zadaniem jest również wskazywać ryzyka i je minimalizować poprzez dopasowane rozwiązania techniczne, organizacyjne, zdalne i mobilne. Oczywiście działania te zawsze są poprzedzane analizą zagrożeń. W kontekście zagrożeń globalnych część obiektów przemysłowych to obiekty z infrastrukturą krytyczną, a to wymusza inne, definiowane przez ustawę rodzaje zabezpieczeń. Jedno jest pewne – otoczenie biznesowe będzie się zmieniać, zyskają na tym firmy, które z uwagą wsłuchują się w potrzeby klientów.

Bogumił Szymanek

Axis Communications

Dobór rozwiązania

Zakłady przemysłowe są obiektami, w których szczególnie ważne jest zapewnienie bezpieczeństwa pracownikom i ochrona mienia firmy. Są narażone na różnego rodzaju zagrożenia wynikające ze stosowanych technologii, przetwarzania substancji czy charakteru produkowanego asortymentu. Wymagana jest więc ścisła kontrola nie tylko procesów technologicznych, ale również transportu i przechowywania materiałów czy procedur związanych z organizacją pracy ludzi. Bez nowoczesnych systemów informatycznych i automatyki niemożliwe jest prowadzenie tego rodzaju działań.
W zakresie ochrony obiektu i optymalizacji procesów pomocne okażą się rozwiązania Axis Communications. W zależności od oceny ryzyka wydzielane są strefy, w których stosuje się innego rodzaju technologie i sprawdzone rozwiązania. Podstawowa ochrona to zabezpieczenie zakładu przed nieautoryzowanym dostępem i tym samym przeciwdziałanie stratom związanym z uszkodzeniem mienia, kradzieżą czy sabotażem. W strefie ogrodzenia zakładu instalowane są więc skuteczne systemy integrujące zastosowane detektory – kamery termowizyjne lub radary, szybkoobrotowe kamery PTZ weryfikujące zdarzenie i megafony sieciowe pozwalające na natychmiastowe działanie nawet na dużych obszarach.
Zgodnie z zasadą, że lepiej zapobiegać, niż naprawiać szkody – system dźwiękowy odstraszy intruza, zanim dojdzie do naruszenia ogrodzenia. Radary Axis w ramach rozwiązania Axis Speed Monitor można też wykorzystać do obserwacji pojazdów poruszających się na drogach wewnętrznych zakładu i weryfikacji, czy poruszają się z prędkością wymaganą standardami bezpieczeństwa.
Otwartość integracyjna Axis sprawia, że możliwe jest również elastyczne zarządzanie wizytami gości, za pomocą np. dynamicznych kodów dostępu QR odczytywanych przez interkomy Axis czy systemów automatycznego rozpoznawania tablic rejestracyjnych pojazdów. W każdym przypadku najważniejszy jest dobór rozwiązań do oszacowanego ryzyka, specyfiki obiektu i potrzeb użytkowników systemu.

Marcin Walczuk

BCS

Szczególny stopień ochrony

Zakłady przemysłowe wymagają szczególnego stopnia ochrony. Zwłaszcza gdy w procesie produkcyjnym są wykorzystywane niebezpieczne materiały, które w razie ataku terrorystycznego lub nieumyślnego działania człowieka stanowią poważne zagrożenia zdrowia i życia ludzi. Skuteczne zabezpieczenie tego typu obiektów jest nie lada wyzwaniem dla projektantów systemów zabezpieczeń. Podstawowym problemem jest ich wielkość, a dodatkowo mogą składać się z wielu mniejszych oddziałów rozsianych nawet na obszarze całego kraju. Niejednokrotnie klient chciałby scentralizować system bezpieczeństwa tak, aby móc nim zarządzać z jednego miejsca.
Wykorzystanie systemów telewizji dozorowej opartych na technologii IP pozawala na przesyłanie sygnałów wizyjnych do dowolnego miejsca na świecie, dzięki czemu tworzenie centrów monitoringu nie stanowi większego problemu. Konieczne do tego będzie odpowiednio wydajne łącze internetowe i aplikacja, która umożliwi zarządzanie wieloma obiektami równocześnie.
Wychodząc naprzeciw tym wymaganiom, BCS proponuje swoje autorskie rozwiązanie – aplikację BCS Manager. Pozwala ona na podłączenie i podgląd niemalże nieograniczonej liczby kanałów na nieograniczonej liczbie monitorów. W praktyce będzie oczywiście ograniczona możliwościami stacji roboczej, na której aplikacja zostanie zainstalowana. Główną zaletą tego rozwiązania jest obsługa nie tylko urządzeń BCS, ale również innych wiodących producentów telewizji dozorowej oraz wsparcie 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. I w tym wypadku najlepiej sprawdzą się rozwiązania IP CCTV, które zapewniają pracę w wyższych rozdzielczościach oraz dostęp do zaawansowanych funkcji analizy obrazu. Dzięki tym cechom i ich umiejętnemu wykorzystaniu można precyzyjniej zabezpieczyć teren i obsługiwać tylko zdarzenia potencjalnie niebezpieczne przy zredukowaniu do minimum liczby fałszywych alarmów.

Artur Nowakowski

Linc Polska

Zabezpieczenie obiektów rozległych

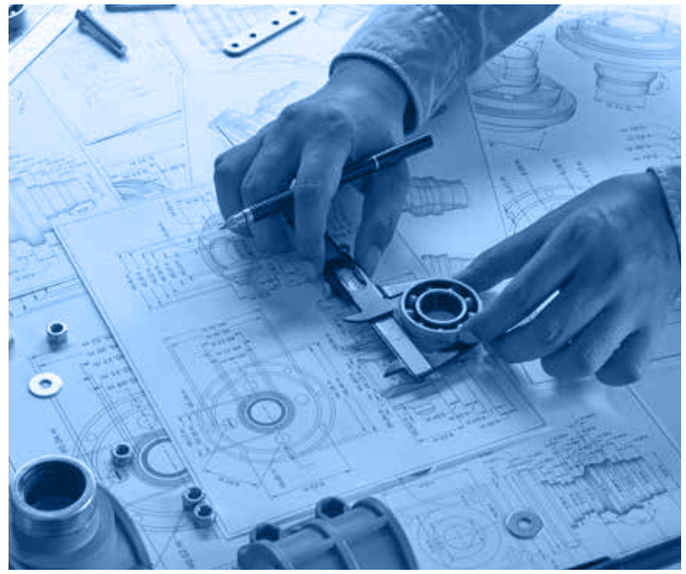
Zabezpieczanie obiektów rozległych i rozproszonych, często należących do infrastruktury krytycznej, to nie lada wyzwanie dla ich właścicieli i zarządców. Goszcząc w wielu miejscach, miałem okazję poznać te lepsze, ale również te gorsze rozwiązania. Z reguły duże obiekty mają większą rzeszę specjalistów, pokaźniejszy budżet i kwestie bezpieczeństwa są tam traktowane priorytetowo. Można w nich spotkać zabezpieczenia kolejnych stref wtargnięcia – gdyby jeden system zawiódł, inne nadal są w stanie wykryć naruszenie.
W mniejszych obiektach kwestie ich zabezpieczenia często traktuje się po macoszemu. Zazwyczaj wszystko rozbija się o cenę, bo po co kupować systemy za kwotę X, gdy można kupić inny/jeden system za połowę tej sumy. Po co nam dwa systemy, kiedy jeden też będzie działać? Konsekwencją szukania oszczędności za wszelką cenę jest niestety często „byleja kość". Tak być nie powinno!
Skuteczna ochrona nie musi być bardzo kosztowna, wystarczy zmienić podejście i np. zastosować mniej detektorów, które jednocześnie zabezpieczą większy obszar. Zabezpieczając obiekt rozległy, np. zbiornik wodny będący częścią IK, można z powodzeniem zastosować radary wykrywające wtargnięcie na teren – w tym przypadku obiekt wpływający na chroniony zbiornik. Ochrona systemem radarowym jest bardzo dobrym przykładem zabezpieczenia rozległych terenów i może stanowić uzupełnienie ochrony obwodowej bazującej np. na kablu sensorycznym czy kamerach termowizyjnych z wbudowaną analityką obrazu.
Kolejną zaletą wykorzystania systemów radarowych jest możliwość wykrywania nadlatujących dronów. Ich wczesna detekcja jest podstawą zabezpieczenia się przed nimi. Warto wspomnieć o użyciu dronów do blokady lotniska Gatwick w 2017 r. czy ataku bombowym na lotnisko w Arabii Saudyjskiej w 2021 r. Ale jak niebezpiecznym narzędziem mogą być te latające statki, pokazuje nam wojna w Ukrainie. W Polsce na szczęście nie odnotowaliśmy poważnego incydentu z udziałem dronów, ale jest to prawdopodobnie kwestią czasu. Dlatego też projektując system zabezpieczeń, bierzmy pod uwagę wszelkie zagrożenia, te z ziemi, z wody i z powietrza.

Krzysztof Kunecki

Schrack Seconet

Systemy ppoż. w obiektach przemysłowych

Doświadczamy czwartej rewolucji przemysłowej wiodącej ku nastaniu ery, która zyskała już nazwę Przemysłu 4.0. Projektowanie i wdrażanie kompleksowej ochrony przeciwpożarowej wymaga spojrzenia holistycznego na zabezpieczany obiekt przemysłowy pod kątem dobieranych elementów systemu bezpieczeństwa pożarowego (SBP), aby zapewnić nie tylko spełnienie podstawowych kryteriów funkcjonalnych (np. niezawodność działania czy odporność na warunki środowiskowe), ale również zdolność do wzajemnego współdziałania urządzeń w ramach SBP i możliwości współpracy z innymi instalacjami i urządzeniami technologicznymi obiektu.
Celem i jednocześnie wyzwaniem jest zbudowanie spójnego, w pełni zintegrowanego systemu wykrywania pożaru, sterowania, zasilania urządzeń ppoż. i innych instalacji mających wpływ na bezpieczeństwo pożarowe. Dotyczy to np. dodatkowej współpracy z systemem dozoru wizyjnego CCTV/VSS w zakresie szybszej weryfikacji zagrożenia czy z zabezpieczeniami technologicznymi obiektu. Tak zintegrowany SBP umożliwia kompleksowy nadzór i sterowanie z poziomu dedykowanego systemu zarządzania bezpieczeństwem pożarowym (systemu integrującego urządzenia ppoż. - SIUP). Dzięki temu zapewnione



jest kompleksowe zarządzanie ewakuacją w razie alarmu pożarowego oraz szczegółowa kontrola pracy urządzeń podczas codziennej eksploatacji. Celem jest skuteczna reakcja na zagrożenie, gdy ono wystąpi, ale tak samo ważne z punktu widzenia filozofii działania systemów bezpieczeństwa są działania prewencyjne zapobiegające wystąpieniu części zagrożeń i awarii.
W ramach działań prewencyjnych integracja z urządzeniami na poziomie protokołu komunikacyjnego w zintegrowanym systemie pozwala na szczegółowe informowanie o jego stanach pracy i zgłaszanie wszelkich odchyłek i niezgodności w odniesieniu do normalnego trybu pracy oraz wcześniejszą reakcję personelu technicznego, zanim dojdzie do poważnej awarii.
Nowoczesne systemy sygnalizacji pożarowej (SSP) wcześniej sygnalizują nieprawidłowe stany pracy (np. niebezpieczne zabrudzenie układów detekcyjnych czujek pożarowych, zmiana rezystancji linii dozorowych i sterujących spowodowana starzeniem się instalacji). Nadzór nad szczegółowymi stanami pracy w połączeniu z analizą zdarzeń historycznych i wzajemnej korelacji pozwala przy zastosowaniu SIUP na wdrożenie ochrony predykcyjnej SBP.
Kolejnym istotnym obszarem jest współdziałanie SBP z systemami bezpieczeństwa i kontroli innych instalacji obiektu (BMS/BAS czy SMS) w celu informowania o innych, niezwiązanych z pożarem zagrożeniach w obiekcie. Możliwość bieżącego odczytu aktualnej temperatury z czujek pożarowych zlokalizowanych praktycznie w całym obiekcie pozwala na zasygnalizowanie nieprawidłowych stanów pracy występujących w innych instalacjach i systemach, np. uszkodzenie w układach klimatyzacji serwerowni/rozdzielni elektrycznej czy zaalarmowanie o podwyższonej temperaturze w pomieszczeniach produkcyjnych.
SSP jest w tym przypadku uzupełniającym źródłem informacji, a wcześniejsze wykrycie nieprawidłowości i wezwanie serwisu jest kluczowe w zapobieganiu wystąpienia poważnej awarii, która może zatrzymać działanie np. linii produkcyjnej w obiekcie przemysłowym.
Zintegrowany system daje duże możliwości w zakresie optymalizacji procedur ochrony i współdziałania między systemami, ale stwarza też ryzyko, gdy interfejsy wejścia/wyjścia urządzeń i infrastruktura techniczna nie będą właściwie zabezpieczone. Dlatego też zaleca się wydzielenie infrastruktury dla celów bezpieczeństwa pożarowego, a wszelkie punkty styku z instalacjami zewnętrznymi należy chronić, zapewniając kontrolowany przepływ danych z zastosowaniem routerów/firewalli czy bezpiecznych połączeń w postaci tuneli VPN, gdy jest wymagane współdzielenie infrastruktury.
W ramach zintegrowanego systemu powinny być wdrażane funkcje bezpieczeństwa funkcjonalnego na poziomie indywidualnych urządzeń i systemów pozwalających na zdefiniowanie szczegółowych kryteriów działania urządzeń i ich obsługi, zależnie od stanu pracy/trybu pracy urządzeń technologicznych. Przykładowo, wykonywanie rozkazów sterujących może być uzależnione nie tylko od poziomu autoryzacji operatora, ale też od aktualnego stanu pracy instalacji. Pozwala to uniknąć błędów w zakresie obsługi czy udaremnić próbę sabotażu.
Biorąc pod uwagę aspekty współdziałania, integracji i przenikania się funkcji między systemami, kluczowa jest koordynacja prac koncepcyjnych, projektowych i instalacyjnych pomiędzy branżami systemów bezpieczeństwa oraz technologicznymi. Pozwoli to uzyskać maksymalny poziom synergii i dzięki temu osiągnąć jeszcze wyższy poziom bezpieczeństwa, komfortu obsługi i zarządzania obiektem przemysłowym.

Zarządzanie projektem

Cz. 1. Wprowadzenie w tematykę

Na łamach „a&s Polska” wielokrotnie poruszano kwestię systemów ochrony elektronicznej jako rozbudowanych, skomplikowanych systemów IT. Fora dyskusyjne są pełne opisów nieprawidłowo działających rozwiązań, dysfunkcje zazwyczaj dostrzega się już po incydentach. Jako przyczyny podaje się zazwyczaj nieprawidłowy montaż, oszczędności poczynione podczas wdrażania, błędy projektowe.

Tomasz Dacka

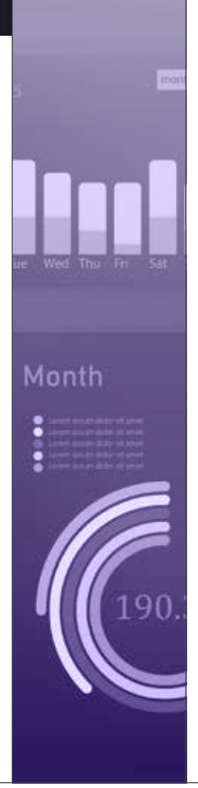
Z dużym prawdopodobieństwem można również założyć, że większość z nas spotkała się z sytuacją braku jakiejkolwiek dokumentacji dotyczącej systemów zabezpieczeń. To w znacznym stopniu utrudnia pracę i instalatorom (np. przy modernizacji), i użytkownikom końcowym przy codziennej eksploatacji. Skoro zatem dokumentacja jest tak ważna, jak zadbać o to, by była kompletna? Jakie są przyczyny powstawania błędów, dysfunkcji systemów ochrony? W jaki sposób zapewnić odpowiednią troskę na wszystkich etapach pracy systemu? Odpowiedź jest jedna: poprzez spójne zarządzanie projektem rozumianym jako cykl podjętych działań, aktywności od fazy początkowej implementacji systemu aż do fazy ostatniej.

SPÓJNY, CZYLI JAKI?

Bez względu na zakres i ciężar gatunkowy projekt systemu ochrony jest o tyle dobry, o ile będzie realizował założone cele w sposób wcześniej uzgodniony. I chociaż na początku wydaje się to oczywiste, w rzeczywistości już takie proste nie jest, a w przypadku dużych, rozbudowanych projektów dotykających różnych obszarów (a tym samym różnych interesariuszy) stanowi nie lada wyzwanie. Ważne, by w takim wypadku zachować spójność projektu, na którą składają się następujące elementy:

- metodyka rozumiana jako szkielet, fundament projektu, który prowadzi nas od założeń do celu; nie odpowiada ona na pytanie, jak mam to zrobić, tylko co należy zrobić, w jakiej kolejności i na co zwrócić szczególną uwagę na każdym etapie projektu;
- kierownik projektu (Security Project Manager – PM/SPM) to osoba, która wiąże wszystkie aktywności w całość, dba o to, by projekt przez cały czas realizacji nie wykraczał poza ramy swojego zakresu. Odpowiada za koordynację zadań, ich weryfikację, nadzór oraz rozwiązywanie napotkanych problemów. Pełni kluczową funkcję w całym procesie. Niektórzy twierdzą, że nie ma dobrych kierowników projektu, są tylko tacy, którzy mają szczęście;
- sponsor to osoba, zazwyczaj z kadry zarządzającej, pełniąca funkcję właściciela biznesowego, występująca o budżet na realizację zadania;
- komitet sterujący składający się z przedstawicieli wszystkich zaangażowanych w projekt interesariuszy oraz sponsora. Projekt na ogół swoim zakresem „przeszywa” różne obszary w organizacji, nie tylko związane z bezpieczeństwem, ale także takie działy, jak HR, rozwój biznesu, administracja.

W praktyce zazwyczaj przebiega to tak, że dział bezpieczeństwa buduje wewnętrzną potrzebę projektową, na podstawie opracowanego wcześniej planu przekonuje do niej dyrektora swojej komórki, następnie zaprasza się poszczególnych interesariuszy, których przedstawiciele są zaangażowani w prace projektowe. Sponsor występuje o akceptację budżetu, a na kolejnych spotkaniach Komitetu Sterującego kierownik projektu przedstawia postęp prac zgodnie z przyjętą na początku metodyką prowadzenia projektu.
Dla zachowania spójności projektu, zwłaszcza tego, którego czas liczony jest w latach, niezwykle istotne jest przestrzeganie jego zakresu. W zarządzaniu projektem istnieje takie pojęcie, jak *scope creep*. Spotykamy się z nim często, gdy w trakcie realizacji projektu pojawiają się nowe pomysły, zadania, których pierwotnie nie przewidywano, a które prowadzą do wyzwań związanych czy to z czasem realizacji, czy z budżetem. Przykładowo przy implementacji systemu ochrony obwodowej CCTV jeden z interesariuszy podejmuje w fazie realizacji decyzję o konieczności wdrożenia zaawansowanej analizy materiału wideo na taśmie produkcyjnej. Wiążę się to z dodatkowymi kosztami zakupu urządzeń (kamer), licencji VCA oraz konfiguracji i szkolenia, a także czasem potrzebnym na wdrożenie tej funkcjonalności. Kolejnym przykładem prowadzącym do *scope creep* jest brak odpowiedniej komunikacji i koordynacji w zespole z winy kierownika projektu, a w efekcie do powstawania wielu potrzeb nieujętych w dokumentacji projektu.



CZYM WŁAŚCIWIE JEST PROJEKT?

Słowo „projekt”, zaraz po słowie „system” w wielu sytuacjach jest odmieniane przez wszystkie przypadki, posiada wiele definicji. Projektem może być zarówno budowa zintegrowanego systemu kontroli dostępu rozproszonego po całym kraju, jak i implementacja funkcjonalności wirtualnej karty do już działającego SKD. Projektem może być również mała instalacja SSWiN. To, czy dana aktywność zostanie ujęta w formę projektu, zależy od struktury, kultury organizacji i krótkiej analizy ekonomicznej, czy warto dla danego przedsięwzięcia angażować potencjał ludzki do jego prowadzenia. Tym bardziej zasadne wydaje się pytanie, czym jest i czym charakteryzuje się projekt. Każdy projekt:

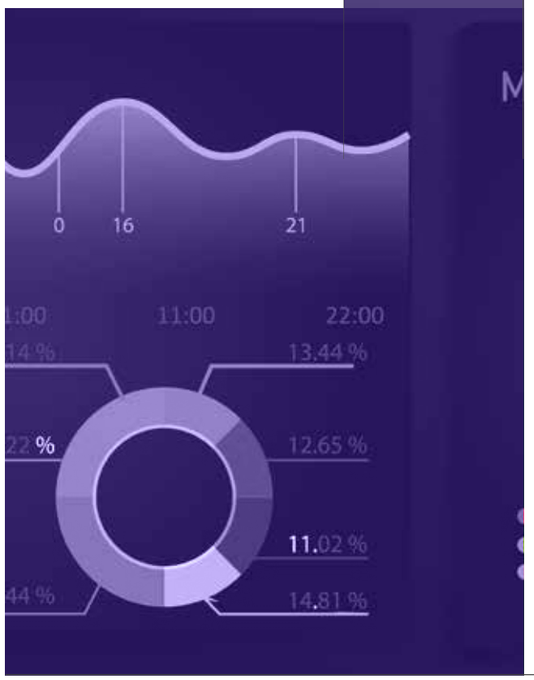
- ma określony początek i koniec trwania, nawet jeśli jest częścią większego projektu (tym głównie różnią się zadania projektowe od operacyjnych);
- ma określony budżet;
- ma określony czas, harmonogram;
- ma cele (zazwyczaj wyjątkowe/ważne) do spełnienia oraz mierniki ich skuteczności;
- jest opisany w jasno określonym zakresie;
- wymaga do realizacji określonych zasobów, tj. ludzi, budżetu, dostaw, kompetencji,

Każdy projekt cechuje trudna do przewidzenia niepewność w określeniu efektu, zasobów potrzebnych do jego realizacji czy czasu wykonania wszystkich przewidzianych zadań (może się okazać, że nie wszystkie konieczne zadania dało się przewidzieć).
Głównym zadaniem kierownika projektu jest zrealizowanie celów w założonym budżecie i czasie. Organizacja podejmuje wysiłek realizacji projektów zazwyczaj z powodu osiąganych przez nie celów przekładających się na wyraźne benefity, co w obszarze bezpieczeństwa

fizycznego może stanowić pewne wyzwanie. Niemniej jednak dobrze przygotowany plan projektu broni się sam. Nowe technologie w branży ochrony czy zmieniające się zagrożenia mają szansę przekonać kadrę zarządzającą do realizacji zadania. Łączenie kilku zadań w duży program/strategię o wieloletnim harmonogramie realizacji również może być dobrym pomysłem.
Projekt, mimo posiadania spójności w swojej formule i treści, musi być w odpowiedni sposób prowadzony i zarządzany. Wchodzimy tu zatem w tematykę zarządzania projektem, którą można określić jako zbiór ludzi, systemów i techniki potrzebnych do realizacji projektu z sukcesem.

SECURITY PROJECT MANAGER (SPM/PM)

W zarządzaniu projektem, jak w wielu innych aspektach bezpieczeństwa, kluczową rolę grają ludzie. Na czele zespołu zaangażowanego w pracę stoi kierownik projektu. Jego główne zadania opisałem wcześniej, teraz chciałbym skupić się na cechach, jakie powinien posiadać, aby móc realizować te niełatwe zadania. Najczęściej bowiem można spotkać się z sytuacją, że poszczególne podzespoły mają różne wizje tego, jak do celu projektu dążyć. Zdarzają się sytuacje wręcz konfliktowe, wymagające od PM-a umiejętnego poruszania się i zarządzania takimi wyzwaniami.



Kierownik projektu, ze względu na charakter pracy, musi:

- być dobrze zorganizowany i cechować się umiejętnością samokontroli na wysokim poziomie;
- mieć zdolności analityczne;
- odnajdować się w pracy wielozadaniowej (tzw. *multitasking*), łączyć poszczególne zadania i „pchać całość do przodu";
- pamiętać o celu nadrzędnym, do którego dąży;
- posiadać pewne cechy/umiejętności: sprawnie zarządzać (przeprowadzać procesy i ludzi przez procesy), być liderem zespołu (komunikacja wizji, wzbudzenie w zespole wiary i chęci do jej realizacji) i tzw. *team-building* (ponieważ nawet najlepszy PM nic nie osiągnie bez zaangażowania swojego zespołu) oraz osobą komunikatywną (odpowiedni przepływ informacji w projekcie jest kluczowy dla jego powodzenia), a przy tym sprawować nadzór (rozliczanie postępu prac).

Pracę PM-a można sprowadzić do trzech obszarów działania. Na każdym etapie projektu nakład sił jest inny:

- planowanie, które odgrywa kluczową rolę w fazie początkowej (np. studium wykonalności);
- koordynacja, istotna w fazie rozwoju;
- kontrola w fazie wykonawczej.

METODYKA

Na pierwszy rzut oka wydaje się, że wystarczy przemyśleć wszystkie fazy implementacji danego rozwiązania, aby przewidzieć co, kiedy i przez kogo ma być wykonywane, żeby móc z powodzeniem zakończyć zadanie. W przypadku małych instalacji rzeczywiście taki tok rozumowania może się sprawdzić, jednak przy większych wyzwaniach jest skazany na niepowodzenie. Ilość zadań, zagrożeń, interesariuszy, rozbudowany zespół projektowy – wszystko to musi być traktowane całościowo. Taką rolę odgrywa wybrana metodyka prowadzenia projektu. Dodatkowymi benefitami są:

- Jednoznaczne określenie celów i oczekiwań wobec projektu oraz przelanie ich na papier, co przekłada się na spójną komunikację i trzyma projekt w ryzach
- Udokumentowana praca; dokumentacja w projekcie odgrywa kluczową rolę
- Możliwość przyspieszenia prac projektowych, redukcji ryzyka
- Efektywne wykorzystanie wszystkich możliwych zasobów, każda osoba zaangażowana w projekt jest rozliczana ze swoich zadań
- Zazwyczaj pozwala też wcześniej dostrzec problemy, dzięki czemu można oszczędzić czas i pieniądze.

Zestandaryzowane podejście jest bez wątpienia dobrą drogą do osiągnięcia sukcesu.

FAIL TO PLAN, PLAN TO FAIL*

To powiedzenie znajduje odzwierciedlenie w prowadzeniu projektów, zwłaszcza związanych z systemami bezpieczeństwa. Już na początku, kiedy staramy się o pozyskanie budżetu, ma wręcz fundamentalne znaczenie. Jeśli nie zareklamujemy w odpowiedni sposób naszej idei, trudno będzie pozyskać środki na jej realizację. Jak to zrobić? Należy przygotować solidną dokumentację, która pozwoli odpowiedzieć na kluczowe pytania:

1. Jaką potrzebę adresuje nasz projekt? Jaki jest jego prawdziwy cel?
2. Jakie metodyki, procesy, aktywności zostały użyte w celu zdefiniowania projektu?
3. Jakie rezultaty osiągniemy, realizując cele projektu (benefity dla interesariuszy)?
4. Jaki jest priorytet projektu? Jeśli łączy się z innymi projektami w organizacji, jego rola rośnie.

* Powiedzenie Benjamina Franklina: „Jeśli nie uda ci się zaplanować, zaplanujesz porażkę". Chodziło mu o to, że sukcesu nie osiąga się przypadkiem, wymaga planowania, wiedzy o tym, dokąd zmierzamy i jak się tam chcemy dostać.

Solidna dokumentacja musi zawierać co najmniej następujące informacje:

- Podsumowanie. Dlaczego dokumentacja miałaby się zaczynać od podsumowania? Osoby decyzyjne, które często nie posiadają eksperckiej czy specjalistycznej wiedzy w obszarze bezpieczeństwa, mogą nie mieć czasu ani chęci, aby przebrnąć przez wiele stron dokumentacji. Zwięzłe, konkretne podsumowanie zapewni im odpowiednią wiedzę nt. tego, co chcemy zrobić i co nam to da.
- Benefity. Powinny być wyraźnie określone benefity biznesowe dla organizacji. Niestety argument „aby było bezpiecznie" najprawdopodobniej nie przekona nikogo do wpisania projektu do budżetu.
- Cele projektu. Określenie w sposób jasny celów prowadzących do benefitów upraszcza prowadzenie projektu. Nie powinny się zmieniać podczas trwania prac. Przyjęło się, że cele powinny zostać opisane w sposób zwięzły. Powinny również być osiągalne, mierzalne (zgodnie z kolejną maksymą projektową: jeśli czegoś nie możesz mierzyć, nie możesz tym zarządzać), realistyczne oraz określone w czasie.
- Zakres. Wyartykułowanie tego, co będzie produktem naszych aktywności, a co nie – jakich obszarów, procesów będziemy dotykać, z jakimi danymi będziemy pracować.
- Czas potrzebny do realizacji projektu oraz zespoły, które zostaną zaangażowane w określonym reżimie czasowym. Dodatkowo podstawa, na jakiej założenia zostały poczynione.
- Oszacowany koszt. Na koszt składają się głównie prace związane z zaangażowaniem czynnika ludzkiego, hardware'u, software'u, utrzymania, rozwoju, szkoleń, podróży służbowych.
- Założenia. Kluczowe jest wskazanie przyjętych przez nas założeń, które są konieczne do doprowadzenia projektu do szczęśliwego końca (np. zaangażowanie osób o określonych kwalifikacjach, zakup określonego oprogramowania).

- Ryzyko. Wskazanie głównych zagrożeń to gra fair play. Wiemy, co i jak chcemy zrobić, ale jest to związane z pewnym ryzykiem. Jedne adresujemy, tworząc być może kolejne. Zazwyczaj padają wtedy pytania typu, czy stać nas na ten projekt lub czy stać nas na to, by tego projektu nie przeprowadzać.

Artykuł jest wprowadzeniem do tematyki zarządzania projektem. Zarządzanie projektami w naszej branży w obecnych turbulentnych czasach stanowi nie lada wyzwanie. Słowo „elastyczność" pada często, budżety (nawet gdy się znajdą) mają tendencję do kurczenia się, a wciąż zmieniające się zagrożenia weryfikują pierwotne założenia projektowe.
W następnej części artykułu pochylimy się nad poszczególnymi fazami projektu na przykładzie realizacji systemu elektronicznej ochrony.

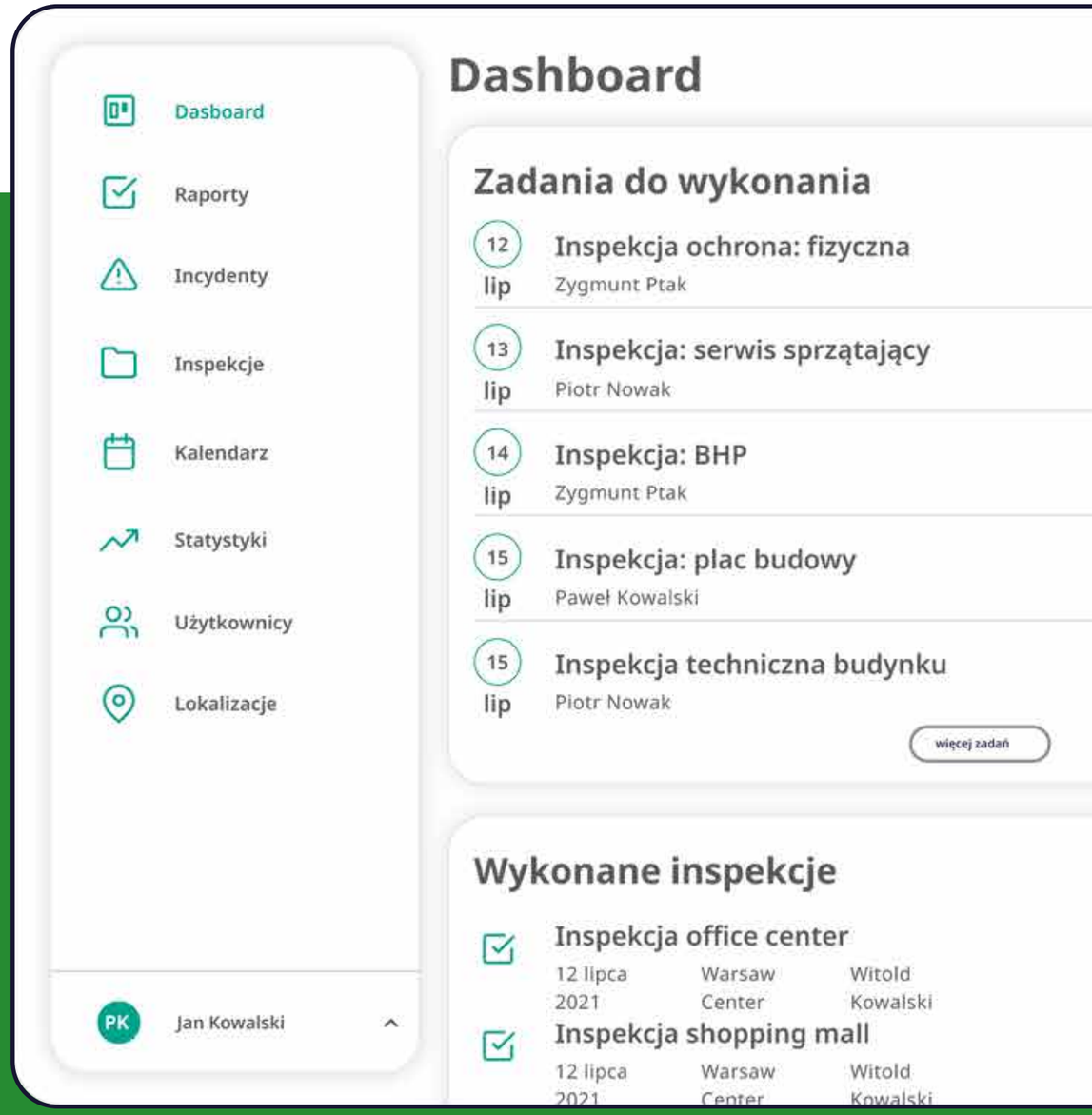
TOMASZ DACKA

Ekspert bezpieczeństwa fizycznego. Z branżą związany ponad 12-letnim doświadczeniem, zwolennik holistycznego podejścia do zarządzania bezpieczeństwem. Prywatnie entuzjasta architektury przedwojennej Warszawy.

Checly

UŁATWIA
zarządzanie jakością

WSPIERA
procesy kontrolne



wypróbuj bezpłatnie na
checly.pl

Zarządzanie danymi i wykorzystanie analityki

Cz. 2.

Dane i analityka (D&A) odnoszą się do sposobów zarządzania informacjami w celu obsługi wszystkich możliwych zastosowań dla danych i wyników ich analizy podejmowania lepszych decyzji, optymalizacji procesów biznesowych, jak i odkrywania nowych zagrożeń biznesowych, wyzwań i możliwości.

PRZYSZŁOŚĆ TECHNOLOGII DANYCH I ANALITYKI WG GARTNERA[1]

Platformy analizy danych również m.in. z dziedziny wywiadu przemysłowego, tzw. Business Intelligence, rozwijają potencjał tkwiący w nauce o danych, tworząc z kolei nowe rozwiązania i nowe platformy wykorzystujące D&A, które wspomagają proces decyzyjny. Dostawcy usług w chmurze, gdzie uruchamianych jest coraz więcej narzędzi i platform, wprowadzają dodatkowy poziom kompleksowości (w rozumieniu wszechstronności – przyp. red.) rozwiązania.
Tradycyjne platformy na rynkach danych, analizy i sztucznej inteligencji z trudem radzą sobie z obsługą rosnącej liczby przypadków użycia i przetwarzania danych, dlatego organizacje muszą równoważyć wysoki całkowity koszt posiadania istniejących rozwiązań lokalnych z potrzebą zwiększenia zasobów i nowymi możliwościami, takimi jak zapytania w języku naturalnym, eksploracja tekstu oraz analiza danych semistrukturalnych[2] i nieustrukturyzowanych[3]. Przyszłość D&A wymaga zatem od organizacji inwestycji w tzw. komponowalne[4] architektury zarządzania danymi i analityki w celu wsparcia zaawansowanej analityki.

Nowoczesne systemy i technologie D&A będą prawdopodobnie obejmować następujące elementy:

• SYSTEMY ZARZĄDZANIA DANYMI:

- Zarządzanie danymi podstawowymi *(Master Data Management* – MDM) jest wspieraną przez technologię dyscypliną biznesową, w której funkcje biznesowe i informatyczne współpracują ze sobą w celu zapewnienia jednolitości, dokładności, zarządzania, spójności semantycznej i odpowiedzialności za oficjalne współdzielone zasoby danych podstawowych przedsiębiorstwa.
- Węzły danych *(data hubs)* skupiają się na udostępnianiu danych i zarządzaniu nimi. Producenci i odbiorcy danych łączą się ze sobą za ich pośrednictwem, a kontrola zarządzania i wspólne modele są stosowane w celu umożliwienia efektywnego udostępniania danych. MDM to węzeł skupiający się wyłącznie na danych podstawowych. Katalogi danych w coraz większym stopniu wkraczają w przestrzeń zarządzania, przez co i w efekcie zaczynają stawać się węzłami danych (i analityki).
- Centra danych *(data centers)* mieszczą fizycznie serwery (w przeciwieństwie do hurtowni, które są strukturami danych umieszczonymi na serwerach lub w chmurze), a ich przyszłość zależy od stopnia, w jakim obciążenie może być przeniesione do chmury. Decyzje o migracji muszą być oparte na korzyściach biznesowych ekonomicznych z tego płynących.
- Hurtownie danych *(data warehouses)* stanowią punkt końcowy dla gromadzenia danych transakcyjnych, szczegółowych (a czasami innych typów). Wspierają przewidywalne analizy dla danych, których wartość jest dobrze ugruntowana – to znaczy dobrze znane, predefiniowane i powtarzalne analizy, które są skalowalne dla wielu użytkowników w przedsiębiorstwie.

Przekształcanie danych w wiedzę*

D&A wkroczylo w główny nurt

SZYBKA ADOPCJA

97% organizacji twierdzi, że wykorzystuje już D&A w niektórych obszarach biznesu

USA WPROWADZA D&A NA POSIEDZENIA ZARZĄDÓW

Respondenci z USA niemal dwukrotnie częściej niż w globalnej próbce odpowiadali, że używają D&A podczas podejmowania decyzji przynajmniej raz w tygodni

PIERWSZE KORZYŚCI SĄ JUŻ WIDOCZNE

86% respondentów twierdzi, że już podejmuje decyzje szybciej

67% respondentów twierdzi, że już redukuje ryzyko biznesowe

80% respondentów twierdzi, że już podejmuje bardziej dokładnie decyzje

* Źródło: *Zrozumieć DANE. Od wiedzy do wartości*, KPMG, kpmg.com/data

1 https://www.gartner.com/en/topics/data-and-analytics

2 Dane semistrukturalne to nowy model danych oparty na drzewach. Reprezentacja danych jest bardziej elastyczna niż w relacyjnych bazach danych. Schemat bazy jest często wpisany bezpośrednio w dane, można to określić jako dane „samo-opisujące się". Przykładem mogą być pliki XML. Model semistrukturalny przydaje się też przy integracji informacji ze źródeł o różnej strukturze.

3 Dane nieustrukturyzowane to informacje, które nie mają wstępnie zdefiniowanego modelu danych lub nie są zorganizowane we wstępnie zdefiniowany sposób. Informacje nieustrukturyzowane zazwyczaj zawierają dużo tekstu, ale mogą też zawierać dane, np. daty, liczby i fakty. Skutkuje to nieprawidłowościami i niejasnościami, które utrudniają zrozumienie przy użyciu tradycyjnych programów.

3 Komponowalna infrastruktura to koncepcja architektury serwera centrum danych, w której różne zasoby przetwarzania, pamięci masowej i akceleratora nie są związane z fizyczną lokalizacją, a zarządzanie nimi odbywa się za pośrednictwem interfejsu w oparciu o oprogramowanie. Pula zasobów w ramach komponowalnej infrastruktury jest tworzona automatycznie niemal w czasie rzeczywistym, dostosowując je do potrzeb wszystkich aplikacji lub obciążeń roboczych działających w przedsiębiorstwie.

Wielkie wyzwania wciąż pozostają*

POWĄTPIEWANIE W DANE

58% organizacji ma trudności z oceną jakości i rzetelności danych

POSZUKIWANIE ODPOWIEDNICH UMIEJĘTNOŚCI

14% uważa, że posiada wszystkie potrzebne talenty i zdolności potrzebne do pełnego wykorzystania D&A

– Jeziora danych *(data lakes)* gromadzą nieprzetworzone dane (w ich natywnej postaci, z ograniczoną transformacją i zapewnieniem jakości oraz wewnętrznym zarządzaniem) oraz pozwalają użytkownikom na ich eksplorację i analizę w wysoce interaktywny sposób. Jeziora danych nie zastępują hurtowni danych ani innych systemów ewidencji, ale raczej je uzupełniają, przechowując nieprzetworzone dane, które mogą mieć dużą wartość.

• DATA FABRIC

Data fabric to nowa koncepcja zarządzania danymi, która umożliwia rozszerzoną integrację i współdzielenie danych z różnorodnych źródeł danych. To coraz popularniejsze rozwiązanie, pozwalające na uproszczenie infrastruktury integracji danych organizacji i stworzenie skalowalnej architektury.
Po powszechnym wdrożeniu *data fabric* mogą w znacznym stopniu wyeliminować ręczne zadania związane z integracją danych oraz rozszerzyć (a niekiedy całkowicie zautomatyzować) projektowanie i dostarczanie integracji danych. To wciąż jednak nowa koncepcja, a żaden z dostawców nie dostarcza obecnie w sposób zintegrowany wszystkich kompletnych elementów, które są niezbędne do połączenia struktury danych. Ostatecznie to organizacje muszą zdecydować, czy chcą utworzyć własną sieć data fabric, korzystając z najnowszych możliwości obejmujących wymienione technologie oraz inne, np. aktywne zarządzanie metadanymi.
Data fabric składa się również z mieszanki dojrzałych i mniej dojrzałych komponentów technologicznych, dlatego organizacje muszą ostrożnie je łączyć i dopasowywać w miarę indywidualnego rozwoju rozwiązania.

* Źródło: *Zrozumieć DANE. Od wiedzy do wartości*, KPMG, kpmg.com/data

Przechodzenie od wiedzy do wartości*

Zbieranie spostrzeżeń, przeoczanie wartości

BRAK TRAFNOŚCI

tylko 19% ankietowanych twierdzi, że jest wysoce usatysfakcjonowanych z wiedzy, które dostarczają im narzędzia D&A

NIEWYKORZYSTANE SZANSE

81% respondentów poprawiło swoje zrozumienie klientów, ale tylko

41% stworzyło bardziej dopasowane oferty dla potencjalnych klientów

• DANE I ANALITYKA W CHMURZE

Tradycyjne platformy D&A muszą radzić sobie z coraz bardziej skomplikowaną analizą, a całkowity koszt posiadania rozwiązań lokalnych stale rośnie ze względu na ich złożoność, coraz większą zasobożerność (większe zużycie zasobów urządzeń, serwerów, dysków itp. – przyp. red.) i koszty utrzymania rozwiązania. Z kolei dane i analiza w chmurze oferują większą wartość i możliwości dzięki nowym usługom, prostocie i sprawności w zakresie modernizacji danych, a także wymaganych nowych rodzajów analiz (takich jak analiza strumieniowa), wyspecjalizowanych magazynów danych i przyjaźniejszych dla użytkownika narzędzi do obsługi kompleksowego wdrożenia.
Wdrożenie w chmurze – hybrydowej, wielochmurowej lub międzychmurowej – musi uwzględniać wiele elementów D&A, w tym pobieranie danych, integrację danych, modelowanie danych, optymalizację danych, bezpieczeństwo danych, jakość danych, zarządzanie danymi, raportowanie zarządcze, naukę o danych i uczenie maszynowe.

BIG DATA CZY SMALL DATA? A MOŻE WIDE DATA?

Termin „big data" jest używany od dziesięcioleci do opisywania danych charakteryzujących się dużą objętością, dużą szybkością i dużą różnorodnością oraz innymi ekstremalnymi warunkami. Era big data jest jednak dla firm uosobieniem zagrożeń i możliwości, a konkretnie tego, że eksplozja ruchu danych (zwłaszcza wraz ze wzrostem korzystania z Internetu i mocy obliczeniowej) stanowi bogate źródło wiedzy pozwalającej na podejmowanie lepszych decyzji, ale jednocześnie stwarza wyzwania dla organizacji w zakresie przechowywania, zarządzania i analizowania ogromnej ilości danych.
Większość organizacji znalazła sposoby pozyskiwania informacji biznesowych z big data, ale wiele z nich ma problemy z zarządzaniem i analizowaniem zróżnicowanego i szerokiego zestawu treści (w tym materiałów audio, wideo i obrazów) na dużą skalę, szczególnie w sytuacji, gdy liczba źródeł danych rośnie i zmienia się, a zapotrzebowanie na informacje jest w coraz większym stopniu zaspokajane przez zaawansowaną analizę.
Postępowe organizacje nie stosują już rozróżnienia między zarządzaniem, administrowaniem i wyciąganiem wniosków z niewielkich czy dużych zbiorów danych. Obecnie to wszystko są po prostu dane. Zamiast tego agresywnie dążą do wykorzystania nowych rodzajów danych i analiz oraz znalezienia zależności w kombinacjach różnych danych w celu poprawy decyzji biznesowych, procesów i wyników ekonomicznych.
Globalna pandemia i inne zakłócenia w działalności gospodarczej również przyspieszyły potrzebę wykorzystania większej liczby różnych danych w szerokim zakresie przypadków (zwłaszcza że historycznie duże zbiory danych okazały się mniej istotne jako podstawa przyszłych decyzji). Obawy związane z pozyskiwaniem danych, ich jakością, stronniczością i ochroną prywatności również wpłynęły na gromadzenie big data, w wyniku czego pojawiły się nowe podejścia znane jako „*small data*" i „*wide data*".
Podejście oparte na *wide data* umożliwia analizę i synergię różnych – małych i dużych – źródeł danych, zarówno wysoko zorganizowanych danych ilościowych (ustrukturyzowanych), jak i danych jakościowych (nieustrukturyzowanych). Podejście oparte na *small data* wykorzystuje szereg technik analitycznych do generowania użytecznych wniosków, ale czyni to przy użyciu mniejszej ilości danych.
W firmie Gartner używany jest obecnie termin X-analytics, aby zbiorczo opisać małe, szerokie i duże dane (w rzeczywistości wszystkie rodzaje danych). Należy się jednak spodziewać, że do 2025 roku 70% organizacji będzie zmuszonych do przesunięcia punktu ciężkości z *big data* na *small data* i *wide data*, aby efektywniej wykorzystać dostępne dane – albo poprzez zmniejszenie wymaganej objętości, albo wydobywając większą wartość z nieustrukturyzowanych, różnorodnych źródeł danych.

Ta i inne prognozy dotyczące ewolucji analityki danych zawierają ważne założenia planowania strategicznego, które pozwolą na poprawę wizji i realizacji zadań z zakresu D&A.

Uzyskiwanie wartości dodanej z inicjatyw D&A wymaga trzech komponentów: użytecznych obserwacji, silnych procesów zarządzania zmianą oraz wsparcia ze strony kierownictwa. Jednak przede wszystkim wymaga od organizacji fundamentalnie innego podejścia do D&A, które zaczyna się od zrozumienia tego, co biznes chce osiągnąć, a następnie dostosowania do tego narzędzi D&A, możliwości i posiadanych danych, tak aby odpowiednio mocno wspierały cele biznesowe.

Rosnące rozbieżności pomiędzy dobrym a świetnym*

KLUCZOWE MOŻLIWOŚCI POZOSTAJĄ NIEODKRYTE

Mniej niż jedna czwarta twierdzi, że wykorzystuje D&A do identyfikacji nowych źródeł przychodów

tylko 31% uważa, że posiada wszystkie potrzebne talenty i zdolności potrzebne do pełnego wykorzystania D&A

tylko 16% odpowiedziało, że wykorzystuje D&A do prognozowania przyszłych trendów

„D&A nie sprowadza się do umieszczenia w pokoju kilku techników z paroma fajnymi narzędziami w nadziei, że wyniknie z tego coś wartościowego. To zebranie osób technologicznych o umysłach biznesowych i ludzi biznesu o umysłach ukierunkowanych na dane, aby pracowali razem w celu kreowania rzeczywistej wartości dla biznesu" - dr. Thomas Erwin, Partner KPMG w Niemczech

* Źródło: *Zrozumieć DANE. Od wiedzy do wartości*, KPMG, kpmg.com/data

Koncentracja na ryzyku*

97% korzysta z D&A w zarządzaniu ryzykiem

87% uniknęło znaczącego ryzyka dzięki wykorzystaniu D&A

36% doświadcza trudności w przekształcaniu danych we wnioski użyteczne dla zarządzania ryzykiem

63% wykorzystuje D&A raz w miesiącu do podejmowania decyzji

7% wykorzystuje je codziennie

Zunifikowana ochrona obwodowa

Ograniczona świadomość tego, co dzieje się na granicach rozległego obiektu, może być ułatwieniem dla włamywaczy i stanowić problem obrony przed atakami. W przypadku tradycyjnego napłotowego systemu ochrony perymetrycznej operatorzy są alarmowani o potencjalnym naruszeniu strefy dopiero po kontakcie z ogrodzeniem. Innowacje w oprogramowaniu do zarządzania zabezpieczeniami elektronicznymi umożliwią zespołom ochrony spojrzenie poza linię ogrodzenia dzięki połączeniu w jednym panelu wizualizacji sygnałów z różnych urządzeń wykrywających i śledzących.

W przypadku dużych przedsiębiorstw, takich jak lotniska czy obiekty infrastruktury krytycznej, zabezpieczenie granic jest skomplikowane ze względu na rozmiar terenu. Gdy organizacja ma ograniczoną świadomość tego, co dzieje się na terenie całego swojego otoczenia, jest bardziej podatna na włamania. Duży wpływ na poziom bezpieczeństwa ma również zastosowanie urządzeń z nowymi technologiami, np. dronów. Szacuje się, że każdego miesiąca milion bezzałogowych statków powietrznych wkracza w światową przestrzeń, dlatego ich wykrywanie stało się gorącym tematem w dyskusji o ochronie granic. Niektóre z nich są używane jako latające kamery monitorujące w ramach skoordynowanych systemów zabezpieczeń, ale inne mogą być wykorzystywane w złych zamiarach. Ważne jest więc, aby wiedzieć, dlaczego dron się tam znajduje, i móc śledzić, dokąd zmierza, aby upewnić się, że jego cel jest legalny i skoordynowany.

Wiele organizacji zadaje sobie obecnie pytanie, w jaki sposób skuteczniej chronić swój obwód i zapobiegać naruszeniom. Odpowiedzią jest wdrożenie jednolitego systemu zabezpieczeń, a następnie włączenie nowych technologii jako części bardziej kompleksowej strategii ochrony obwodowej.

WARSTWOWE PODEJŚCIE DO OCHRONY OBWODOWEJ

Tradycyjnie zabezpieczenie obwodu oznaczało wdrożenie systemu zabezpieczeń, który generował sygnał alarmu w momencie kontaktu z ogrodzeniem. Takie podejście jest zbyt proste, ponieważ większość obiektów ma wiele nakładających się stref, każda ma własne prawa dostępu, poziom ryzyka i wymagania operacyjne. W rezultacie organizacja nie może polegać wyłącznie na jednej technologii detekcji intruza. Musi zbudować nową strategię ochrony obwodowej, która zapewni, że intruz będzie wykryty także, gdyby jedna metoda detekcji zawiodła. W warstwowej strategii ochrony stosuje się kombinację różnych technologii czujników tworzących więcej niż jedną aktywną linię obrony.

KLUCZOWA JEST UNIFIKACJA SYSTEMÓW

Jeśli organizacja nie unifikuje swoich systemów i technologii zabezpieczeń na jednej platformie, a zamiast tego polega na integracji z dostawcami, może to powodować luki w informacjach i/lub niekompletny obraz granicy terenu. Aby zapewnić, że te systemy działają w powiązanych silosach, ważne jest wprowadzenie ujednoliconego podejścia do krzyżowej kwalifikacji incydentów i alarmów o włamaniach.

Zunifikowana platforma zabezpieczeń łączy dane zebrane przez różne systemy, zapewniając świadomość sytuacyjną niezbędną do utrzymania bezpieczeństwa obiektów i ludzi. Przykładowo otwarta platforma Genetec™ Security Center umożliwia organizacjom integrację systemów dozoru wizyjnego, kontroli dostępu, sygnalizacji włamania, komunikacji pomiędzy systemami i automatycznego rozpoznawania tablic rejestracyjnych (ALPR) w celu lepszej ochrony i zarządzania bezpieczeństwem.

Security Center integruje się przez moduł nadzoru RSA *(Restricted Security Area)* z rosnącą gamą technologii i urządzeń RSA (np. radary i lidary), wspierając pracowników ochrony w wykrywaniu potencjalnych zagrożeń na dużych obszarach. Ruchome cele są automatycznie wyświetlane na mapach geograficznych i śledzone, dzięki czemu mogą oni oceniać i reagować na zagrożenia w krótszym czasie. Ujednolicony system umożliwia operatorom szybkie podejmowanie krytycznych decyzji, ponieważ prezentuje wszystkie informacje o naruszeniu, zagrożeniach i potencjalnych włamaniach jednocześnie. Organizacje mogą wdrożyć kamery CCTV o wysokiej rozdzielczości i dużym zasięgu, które rejestrują wyraźne obrazy w celu uzupełnienia detekcji obwodowej. System można skonfigurować w taki sposób, aby pierwsza linia detekcji obwodowej przy ogrodzeniu wywoływała alarmy, które spowodują automatyczny obrót kamery i zbliżenie obszaru docelowego w celu identyfikacji wizualnej. Zarejestrowany obraz z systemu monitoringu jest następnie przesyłany bezpośrednio do operatorów CMA lub na smartfon dyrektora ochrony w celu natychmiastowej weryfikacji i reakcji.

Zarządzanie tymi urządzeniami i alarmami bezpośrednio ze zintegrowanego systemu mapowania może też pomóc operatorom w szybkim wskazaniu innych pobliskich kamer w celu uzyskania szerszego obrazu sytuacji. Łącząc w ramach ujednoliconej platformy systemy wykrywania włamania, kamery HD i narzędzia do mapowania lokalizacji, organizacja może skrócić czas reakcji i zminimalizować ryzyko niewykrycia naruszeń.

IDENTYFIKACJA POTENCJALNYCH ZAGROŻEŃ

Wczesna identyfikacja potencjalnych zagrożeń na granicy terenu daje operatorowi czas na przygotowanie reakcji i podjęcie niezbędnych działań. Dzięki proaktywnemu rozszerzeniu ochrony o technologię LiDAR i czujniki sejsmiczne mogą oni monitorować ruch i wypatrywać potencjalnych wtargnięć poza linią ogrodzenia. Jednak wiedza o tym, że coś może naruszyć granicę, nie mówi, czy zagrożenie jest realne ani jak poważne. Czujniki mogą wykryć zwierzę, osobę lub samochód. Mając możliwość sprawdzenia, jaki obiekt zbliża się do granicy, pracownicy ochrony podejmą właściwe decyzje dotyczące poziomu zagrożenia.

Ocena incydentu na ogrodzeniu terenu lub w innym zamkniętym obszarze jest łatwiejsza, gdy pracownicy ochrony widzą, co dzieje się na miejscu zdarzenia. Klasyfikując zagrożenia wizualnie i uzyskując odpowiednie dane z wielu systemów, mogą określić, czy wtargnięcie wymaga natychmiastowego działania. Korzystając z funkcji filtrowania, mogą również filtrować obiekty (np. ludzi i zwierzęta) w różnych strefach, aby zmniejszyć liczbę uciążliwych fałszywych alarmów. W ramach oceny zdarzenia operatorzy mogą również korzystać z systemów ALPR do odczytu tablic rejestracyjnych, pomocnych w identyfikacji pojazdów. Przykładowo, jeśli tablica znajduje się na policyjnej liście zagrożeń, zespoły ochrony będą wiedziały, że należy powiadomić policję i reagować z większą ostrożnością.

Systemy zarządzania tożsamością i dostępem (PIAMS – *Physical Identity and Access Management Systems)* dodają kolejną warstwę do procesu, łącząc system kontroli dostępu z systemami biznesowymi, w tym z bazami danych klientów i pracowników. To wzajemne połączenie pozwala organizacjom na automatyczne przydzielanie lub anulowanie dostępu do określonych obszarów oparte na zasadach korporacyjnych. Gdy pracownicy odchodzą lub zmieniają funkcje w organizacji, ich dostęp do wrażliwych obszarów może być dostosowany do zmian w katalogu zasobów ludzkich lub innych powiązanych systemach.

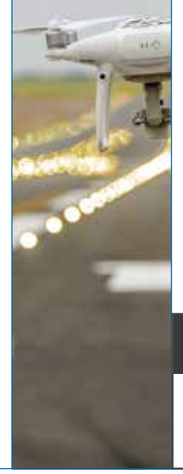
ZNACZENIE ZARZĄDZANIA WSZYSTKIMI DANYMI

W miarę jak organizacje rozmieszczają na obrzeżach kolejne czujniki, rośnie ilość napływających informacji. Może to przytłaczać pracowników ochrony, zwłaszcza gdy muszą aktywnie monitorować wszystkie dane wejściowe, aby zidentyfikować konkretne zagrożenia. Tu pomoże zunifikowany system bezpieczeństwa, który wspiera większą automatyzację. Automatyczne alarmy wraz z cyfrowymi standardowymi procedurami operacyjnymi (SOP), prowadzącymi personel krok po kroku i podpowiadającymi, jak reagować na zdarzenia, zapewniają, że potencjalne zagrożenia są identyfikowane, badane i rozwiązywane w sposób terminowy i spójny w różnych schematach zmian i u różnych osób.

W pewnych przypadkach potencjalne zagrożenie bezpieczeństwa może być trudne do wychwycenia. Przykładowo operator może nie być w stanie zauważyć związku pomiędzy niespodziewanym wejściem kontrahenta do strefy zastrzeżonej a wyłączeniem urządzenia. Zunifikowany system bezpieczeństwa łatwo skoreluje te zdarzenia i szybko je oznaczy, automatycznie ostrzegając operatora o konieczności przeprowadzenia dalszego dochodzenia.

Zdolność do łączenia danych o zdarzeniach jest również ważna dla zapewnienia bezpieczeństwa granic terenu. Operatorzy muszą rozumieć zdarzenia w trakcie ich występowania, aby podejmować świadome decyzje oparte na poziomach zagrożenia. Ujednolicony system bezpieczeństwa zapewnia operatorom większą świadomość sytuacyjną poprzez łączenie raportów i alarmów ze wszystkich modułów działających na danej platformie. Ma to kluczowe znaczenie, ponieważ umożliwia postrzeganie pojawiającej się sytuacji ze wszystkich części systemu jako pojedynczego zdarzenia, a nie serii oddzielnych incydentów.

W ochronie granic przedsiębiorstwa należy zastosować podejście warstwowe, które pozwoli na rozszerzenie bezpieczeństwa poza linię ogrodzenia. Wybierając ujednolicony system, który może obejmować szeroką gamę nowych technologii, można skuteczniej zabezpieczyć swoje obiekty dziś i w przyszłości.



Nowe rozwiązania na nowe czasy

Według wywiadowni gospodarczej Future Market Insights systemy ochrony perymetrycznej stanowią ponad połowę udziału w globalnym rynku security w 2022 r., co przypisuje się rosnącej integracji zaawansowanych sensorów. Szacuje się, że do 2028 r. wzrost tego sektora przekroczy 14% CAGR. Większy udział w rynku zanotują również systemy kontroli dostępu, zwłaszcza oparte na biometrycznych technologiach identyfikacji. Oczekuje się, że do 2031 r. sektor ten osiągnie wartość 50,4 mld USD, rosnąc w tempie 12,6% w latach 2021–2031.

Perspektywy rozwoju może jednak zakłócić niespokojna sytuacja na świecie. Firmy branży security powoli odzyskują równowagę po pandemii COVID-19, teraz wpływ na ich kondycję zaczęła wywierać wojna w Ukrainie. Które rozwiązania będą najchętniej stosowane i dlaczego? Eksperci z różnych firm przedstawiają prognozy. Niezależnie od tego, co nastąpi, można już zauważyć kilka zmian.

NOWA ORGANIZACJA PROCESÓW KD

Menedżerowie bezpieczeństwa zauważyli potrzebę zmiany sposobu zarządzania dostępem do obiektu dla pracowników, kontrahentów i gości z poziomu lokalnego na centralny i uelastycznienia nadawania uprawnień, bez obniżenia poziomu zabezpieczeń.

– Żyjemy w burzliwych czasach. Z jednej strony przeszliśmy na model pracy zdalnej i elastyczne godziny pracy, z drugiej zaś zagrożenia bezpieczeństwa cybernetycznego i fizycznego są dziś większe niż kiedykolwiek. Aby sprostać rosnącym wymaganiom, platforma bezpieczeństwa musi być elastyczna, odporna na cyberataki i w prosty sposób udostępniać pełną ocenę poziomu bezpieczeństwa chronionych obiektów. W Genetec wierzymy, że najlepszym sposobem na osiągnięcie tego celu jest skorelowanie danych z różnych czujników i urządzeń wchodzących w skład infrastruktury bezpieczeństwa.
Można to osiągnąć dzięki zunifikowaniu kluczowych systemów bezpieczeństwa, takich jak dozór wizyjny, kontrola dostępu i ANPR ze wszystkimi czujnikami IoT istotnymi z punktu widzenia bezpieczeństwa. Tak naprawdę nie zmieniliśmy filozofii projektowania rozwiązań zabezpieczeń i dziś widzimy, że kierunek obrany wiele lat temu sprawdza się w wymagających testach współczesnych wyzwań – mówi Jakub Kozak, regionalny menedżer sprzedaży na Europę Środkowo-Wschodnią, Genetec.

Jednym ze skutków pandemii jest potrzeba przyspieszenia transformacji cyfrowej i rozwoju nowych technologii, zwłaszcza rozwiązań chmurowych. Wskazują na to wyniki badań opublikowane w raporcie The 2022 State of Physical Access Control Report przygotowanym przez IFSEC Global – w 2020 r. systemom zabezpieczeń ufało 51% respondentów twierdzących, że spełniają lub przekraczają ich oczekiwania (pod kątem cyberbezpieczeństwa), w 2022 r. tylko 41%[1].

– Zarówno pandemia, jak i rosyjska agresja na Ukrainę znacznie zwiększyły świadomość realnych zagrożeń. Zdaliśmy sobie sprawę z konieczności podniesienia poziomu bezpieczeństwa ludzi, obiektów i danych. W kontekście możliwych ataków w cyberprzestrzeni konieczność ochrony danych wybrzmiewa dziś głośniej niż kiedykolwiek. Te wymagania pomogą spełnić rozwiązania oparte na chmurze. Przykładem jest impero360, pierwsza polska kontrola dostępu w chmurze (AC as a service) jako platforma do zarządzania ruchem osób, która wykorzystuje środowisko Azure Microsoft. Takie rozwiązanie podnosi poziom bezpieczeństwa, a dodatkowo zwalnia z kosztów związanych z utrzymaniem serwerowni i środowiska IT – wyjaśnia Maciej Misaczek, Product Manager impero 360, Unicard.
– Cenioną i pożądaną funkcjonalnością stało się centralne zarządzanie dostępem, począwszy od dostępu do systemów informatycznych i pomieszczeń, skończywszy na uprawieniach na poziomie zbiorów danych. Takie rozwiązanie jest możliwe dzięki integracji systemów kontroli dostępu z Active Directory jako systemem nadrzędnym. Tylko nowoczesna i skalowalna platforma otwarta na integrację może sprostać dzisiejszym oczekiwaniom. Na podstawie raportu Lucintel szacuje się, że do 2027 r. globalny rynek kontroli dostępu w chmurze urośnie do 2,1 mld USD[2].
Uzupełnieniem i dodatkowym zabezpieczeniem systemów kontroli dostępu jest możliwość samodzielnego projektowania, drukowania i kodowania identyfikatorów. Pozostawienie tego procesu wewnątrz organizacji gwarantuje zachowanie pełnej kontroli nad wydawanymi identyfikatorami – dodaje Maciej Misaczek.

INTEGRACJA W OCHRONIE PERYMETRYCZNEJ

Integracja systemów weszła w trend wzrostowy. Wiele organizacji poszukuje rozwiązań integrujących obecne systemy zabezpieczeń, aby zapewnić efektywniejsze wykorzystanie wdrożonych rozwiązań.

– W dziedzinie ochrony obwodowej nie ma cudownego rozwiązania ani panaceum, ponieważ każda technologia ma swoje zalety i ograniczenia. Wybór właściwego rozwiązania zależy od rodzajów zagrożeń, środowiska, wartości towarów i informacji, które mają być chronione, oraz infrastruktury obiektu. Największym wyzwaniem w ochronie obwodowej jest zapewnienie jej 24/7 i 365 dni w roku przy minimalnej liczbie alarmów fałszywych.
W większości przypadków wybór jednej technologii nie zapewnia w pełni bezpieczeństwa, z tego powodu często stosuje się technologie mieszane. Wyzwaniem jest odpowiednie (także pod względem ekonomicznym) zachowanie proporcji między ochroną mechaniczną a systemem ochrony elektronicznej wykrywającym nieautoryzowane wtargnięcie do danej strefy lub sygnalizującym bezpośredni atak na taką barierę – komentuje Norbert Bartkowiak, prezes Zarządu, ela-compil.
I dodaje: – Kolejnym problemem do rozwiązania jest szybka i pewna weryfikacja sygnału alarmowego. Do weryfikacji wykorzystuje się systemy telewizji dozorowej. Wybór właściwej kamery i w przypadku kamer PTZ jej pozycji dokonuje system odpowiedzialny za integrację wszystkich zabezpieczeń.

KD DOBRZE ZABEZPIECZONA

Fizyczne karty dostępu, które są niekodowane, nadal stanowią najsłabsze ogniwo systemu kontroli dostępu. Możliwość ich przekazania lub skopiowania i nieautoryzowanego użycia powoduje, że sam system KD nie jest zabezpieczony. Ale kodowanie kart kosztuje...

– Stosując identyfikatory zbliżeniowe, należy zadbać o ich odpowied-

1 *The 2022 State of Physical Access Control Report*, IFSEC Global
2 *Access Control As A Service Market: Trends, Opportunities and Competitive Analysis*, Raport Lucintel

ni dobór oraz właściwą konfigurację systemu. W ramach systemu kontroli dostępu RACS 5 istnieje możliwość zastosowania szerokiej gamy czytników obsługujących karty zbliżeniowe MIFARE®, oferujących najwyższy stopień zabezpieczeń szyfrujących (sektory SSN). Ponadto dostępna jest tzw. mobilna identyfikacja użytkowników, która umożliwia wykorzystanie telefonu jako identyfikatora. Również w tym przypadku komunikacja pomiędzy telefonem wykorzystywanym do identyfikacji użytkownika a czytnikiem podlega szyfrowaniu – podkreśla Łukasz Kanarek, dyrektor Działu Sprzedaży Krajowej i Obsługi Klienta, Roger.

Kolejnym elementem podnoszącym poziom bezpieczeństwa, na który zwraca uwagę Łukasz Kanarek jest tzw. wieloetapowa (wieloelementowa) identyfikacja użytkowników, która wymusza użycie więcej niż jednej formy autoryzacji.

– System oferuje zarówno typowe wbudowane tryby identyfikacji, takie jak „Karta + PIN" oraz „Karta + Odcisk palca", a ponadto umożliwia tworzenie własnych, bardziej złożonych trybów, np. „Karta + PIN + Linie papilarne". Zastosowanie kart zbliżeniowych MIFARE® w połączeniu z wielostopniowymi trybami identyfikacji zapewnia bardzo wysoką barierę bezpieczeństwa, która może być dodatkowo wzmocniona funkcją „Dostępu z autoryzacją zewnętrzną" oraz funkcją „Wejścia komisyjnego". Pierwsza z wymienionych funkcji uzależnia ostateczną decyzję o przyznaniu dostępu przez śledzącego pracę systemu operatora, który może wizualnie, np. przy użyciu obrazu z kamer, zidentyfikować osobę i zaakceptować prawo dostępu. W przypadku drugiej z wymienionych funkcji dostęp może być przyznany dopiero po identyfikacji dwóch użytkowników uprawnionych do danego przejścia – dodaje.

Systemy biometryczne są nieco kosztowniejsze od rozwiązań opartych na czytnikach kart RFID, choć wraz ze wzrostem ich popularności ceny produktów biometrycznych spadają.

– Zauważamy coraz większą popularność w kontroli dostępu czytników kodów QR. Produkty w nie wyposażone są tanie i wygodne w użytkowaniu, ale mają podobne wady, jak karty dostępowe – łatwo je skopiować. Aby zwiększyć bezpieczeństwo ich stosowania, ZKTeco opracował unikalne w skali światowej rozwiązanie do generowania tzw. dynamicznych kodów QR. Pomysł polega na jednorazowym lub czasowym użyciu kodu QR. Po jego użyciu jest on unieważniany, a w jego miejsce jest generowany nowy kod QR. Może być generowany przez wewnętrzne oprogramowanie kontrolera (kontrolery ATLAS) lub oprogramowanie zewnętrzne (ZK BioSecurity), a następnie wysłany do urządzenia wskazanego przez użytkownika – wyjaśnia Marek Piotrowski, Business Development Manager, ZKTeco. – Rynek ewoluuje, a ZKTeco wciąż wprowadza innowacyjne rozwiązania w kontroli dostępu, aby przewodzić tym zmianom. Przewidujemy ogromny wzrost liczby rozwiązań z kodami QR i wirtualnymi poświadczeniami, które zapewniają użytkownikom dostęp bez fizycznej interakcji, zdalnie i wydajnie.

ZABEZPIECZENIE INFRASTRUKTURY ROZPROSZONEJ

W ochronie perymetrycznej obserwujemy obecnie tendencję do unifikacji rozwiązań. Trend ten stanowi wsparcie dla pracy operatorów infrastruktury krytycznej, którzy muszą skutecznie przeciwdziałać zagrożeniom i reagować na incydenty na rozległych terenach tych obiektów, często rozsianych w oddziałach w całym kraju.

– Trend unifikacji rozwiązań jest według mnie właściwy ze względu na obsługę funkcjonalną i techniczną systemów ochrony obwodowej. Wybór odpowiedniego rozwiązania skutkuje też zachowaniem określonych, właściwych parametrów działania (poziom czułości detekcji intruza, możliwość wyeliminowania fałszywych alarmów). Jednocześnie obiekty różnią się architekturą i parametrami zewnętrznymi, środowiskowymi, co wymaga indywidualnego dostosowania różnych systemów ochrony obwodowej (system napłotowy, zewnętrzne bariery IR lub MW, radary lub systemy CCTV z analityką). Z pomocą przychodzi integracja rozwiązań na odpowiednio dobranej platformie PSIM. W tym przypadku system nadrzędny pełni funkcję optymalizacyjną, łącząc często różne rozwiązania w jednolity system bezpieczeństwa. Wybór odpowiedniego rozwiązania zapewnia także zaprojektowanie odpowiednich algorytmów detekcji, weryfikacji oraz reakcji – zauważa Marcin Stępień, kierownik Działu Systemy Bezpieczeństwa, PRODUS.

Zautomatyzowane podejście do zarządzania systemami zabezpieczeń pozwala również ograniczyć zagrożenia wewnętrzne i błędy ludzkie, zapewniając jednocześnie pełną świadomość sytuacyjną. W przedsiębiorstwach zatrudniających setki pracowników (np. w transporcie, zakładach produkcyjnych, w przemyśle naftowym i gazowym) wprowadza się zdalną kontrolę dostępu. Pojazdy, a także pracownicy i wykonawcy są weryfikowani i autoryzowani, zanim dotrą do wjazdu na teren zakładu. Ogranicza się w ten sposób zatory w ruchu i usprawnia zarządzanie dostawami.

– Parafrazując stare porzekadło, „System kontroli dostępu jest tak bezpieczny, jak jego najsłabsze ogniwo", połączenie weryfikacji pojazdu z identyfikacją kierowcy na pewno podniesie poziom bezpieczeństwa. Obecnie dostępne technologie pozwalają zachować wysoki poziom bezpieczeństwa przy dużej przepustowości ruchu. Szeroka oferta naszych rozwiązań umożliwia sterowanie ruchem pojazdów i osób za pomocą systemów rozpoznających numery tablic rejestracyjnych, kodów PIN, kart RFID, kodów QR, wzorców biometrycznych (linie papilarne, obraz twarzy, tęczówka oka). Każdy projekt systemu kontroli dostępu jest inny i wymaga indywidualnego podejścia, z uwzględnieniem różnych potrzeb. Jestem przekonany, że elastyczność i konwergencja naszych rozwiązań pozwoli zaspokoić oczekiwania nawet najbardziej zaawansowanych instalacji – mówi Grzegorz Michalski, Product Manager of Access Control, Hikvision Poland.

ZDALNE PROJEKTOWANIE I URUCHAMIANIE SYSTEMÓW

W czasie pandemii w wielu przypadkach nie było możliwości przyjazdu na miejsce realizacji inwestycji, co jest wstępem do procesu projektowania rozwiązań.

– Ta niekomfortowa sytuacja przyspieszyła zastosowanie zaawansowanych narzędzi do cyfrowego projektowania systemów. Pozwalają one projektantom na wirtualne ich tworzenie – określenie liczby i rodzaju kamer i czujek w celu zapewnienia maksymalnego zasięgu, bez potrzeby obecności na miejscu przed instalacją – podkreśla Andrea Sorri, Segment Development Manager for Smart Cities w Axis Communications.

Biorąc pod uwagę często odległe położenie wielu obiektów, można również ograniczyć konieczność podróży i związane z tym koszty, nie mówiąc o korzyściach dla środowiska.

AUTOMATYZACJA I INTEGRACJA

Czas postcovidowy to moment, gdy CSO zaczyna na poważnie analizować możliwość automatyzacji wybranych procesów zamiast ich manualnych odpowiedników głównie z powodów ekonomicznych. Jakie są zalety i wady automatyzacji?

– Klient świadomy i nastawiony na długofalowy biznes poszukuje rozwiązań, które w dłuższej perspektywie przyniosą korzyści, zarówno te związane z bezpieczeństwem, jak i finansowe. Czynnik ludzki był, jest i będzie najdroższym, a jednocześnie najbardziej zawodnym elementem. Inwestowanie w zintegrowane systemy elektroniczne wspierające, a niekiedy nawet zastępujące pracowników ochrony, jest poniekąd nieuniknione. Jeśli dzisiaj takie decyzje jeszcze nie zapadły wszędzie, to prawdopodobnie z racji oszczędności – zauważa Krzysztof Bartuszek, prezes Zarządu, Securitas Polska.

Automatyzacja niektórych procesów staje się coraz powszechniejsza. Standardem już stają się systemy automatyki wjazdów, sczytywanie tablic rejestracyjnych, automatyczna awizacja osób i zarządzanie dostępem do obiektów poprzez aplikacje i zintegrowane z nimi systemy kontroli dostępu.

– Coraz częściej zaczynamy mówić o automatyzacji procesów kontroli, zdalnych otwarciach i zamknięciach obiektów, a nawet robotyce. Niektóre rozwiązania związane są jeszcze z dość wysokimi nakładami finansowymi, ale rosnąca powszechność ich stosowania i rozwój techniki szybko doprowadzą do obniżenia kosztów implementacji oraz znalezienia nowych zastosowań – dodaje Krzysztof Bartuszek.

Dzięki zarządzaniu tymi systemami z poziomu jednego interfejsu użytkownika zwiększa się wydajność, upraszcza administracja i kontrola pojedynczych lub wielu obiektów. Jednocześnie połączenie sygnałów z systemów alarmowych i kamer dozorowych na tej samej platformie przyspiesza wykrywanie i weryfikację zdarzeń. Pozwala to na podjęcie szybszych i adekwatnych działań zapewniających, że zdarzenia nie będą eskalować, co poprawia bezpieczeństwo organizacji.

ZMIANY W FIRMACH OCHRONY

Żyjemy dziś w świecie VUCA[3], zmiany zostały już na stałe wpisane do harmonogramów naszych działań. Każde przedsiębiorstwo musi być na te zmiany przygotowane, niezależnie od tego, jak bardzo nas zaskakują.

– Firmy ochrony, podobnie jak inne organizacje, kierują się zasadami biznesowymi. Kluczowe stało się szybkie reagowanie na zmiany. To właśnie podjęte działania oraz optymizm stanowią o sukcesie lub porażce przedsięwzięcia. O ile czas reakcji jest oczywisty, o tyle wspomniany optymizm oznacza poszukiwanie szans nawet w pozornie trudnych sytuacjach – komentuje Krzysztof Bartuszek, prezes Zarządu, Securitas Polska.

Czas COVID-19 był bardzo trudny i odcisnął swoje piętno na wielu branżach, ale dał też szansę wprowadzenia wielu nowych rozwiązań. Spowodował uruchomienie nowych usług. W obliczu konieczności ograniczenia kontaktów międzyludzkich wymusił większy nacisk na technikę w procesach, spowodował wzrost świadomości.
Wojna w Ukrainie to inny rodzaj ryzyka, który wywołał zmiany głównie w obszarze prowadzonego biznesu. Sankcje i ograniczenia w wymianie handlowej, braki materiałów do produkcji to tylko kilka przykładów, które mają wpływ również na branżę ochrony.

– Klient, który z dnia na dzień został odcięty od surowców, nagle poszukuje oszczędności, a ochrona nie jest jego core businessem. Wojna i różne ograniczenia powodują również wzrost bezrobocia, biedę, a co za tym idzie zwiększenie przestępczości. Są to elementy, które mogą stymulować działalność firm ochrony. Wzrost ryzyka oznacza zwiększenie zapotrzebowania na usługi ochrony.
Część klientów decyduje się na oszczędności i cięcie kosztów ochrony. Inni, dostrzegając ryzyko, inwestują w bezpieczeństwo, otwierając się na rozwiązania techniczne i tym samym napędzają rozwój tej branży i pewnego rodzaju rewolucję technologiczną. Mając powyższe na względzie, powinniśmy spodziewać się pewnej polaryzacji rynku – dodaje Krzysztof Bartuszek.

3 VUCA pochodzi od słów: *volatility* (zmienność), *uncertainty* (niepewność), *complexity* (złożoność) i *ambiguity* (niejednoznaczność). Termin ten wprowadziła amerykańska armia, tworząc go z pierwszych liter słów opisujących specyfikę sytuacji podczas wojny. Dosyć szybko zaadaptowano VUCA na grunt biznesu, odnosząc go ogólnie do sposobu zarządzania organizacjami i różnymi dziedzinami społecznymi.

Rewolucja w cyberbezpieczeństwie

Nowoczesne systemy monitoringu wizyjnego są najczęściej oparte na transmisji danych przez protokoły internetowe (IP), wymieniają informacje między lokalną siecią wewnętrzną a siecią internetową. Kamery IP generują obraz o wysokiej rozdzielczości, a ich podgląd jest dostępny z każdego miejsca na świecie. Jednak takie udogodnienie stanowi też niebezpieczeństwo włamań hakerów. W razie cyberataku każde urządzenie w sieci lokalnej z dostępem do Internetu (kamera IP lub urządzenie mobilne) umożliwia wgląd do danych firmy, często bardzo wrażliwych, np. programów rachunkowych, systemów kontroli dostępu czy zarządzania linią produkcyjną. Haker może przekazać obraz wraz z dźwiękiem, jeśli kamera IP była wyposażona w mikrofon, niepowołanym osobom. Urządzenia IP mogą stać się narzędziem szpiegostwa przemysłowego, więc każde przedsiębiorstwo powinno zadbać o zapewnienie bezpieczeństwa cybernetycznego.

Cyberbezpieczeństwo ma kluczowe znaczenie zarówno dla nas, pojedynczych konsumentów, jak i przedsiębiorstw, w tym również organizacji rządowych. Wszyscy bowiem w różnym stopniu jesteśmy narażeni na naruszenia prywatności i wycieku poufnych danych. Kongres USA w 2018 r. uchwalił ustawę *National Defence Authorization Act* (NDAA) ograniczającą na terenie placówek rządu USA korzystanie z urządzeń CCTV i telekomunikacyjnych niektórych producentów. W 2021 r. byliśmy świadkami skutecznie przeprowadzonych cyberataków, w wyniku których hakerzy przejęli kontrolę nad urządzeniami CCTV i wykorzystali je do kradzieży informacji i wartości intelektualnych. Zdarzały się przypadki przekształcania systemów w koparki kryptowalut, a zainfekowane urządzenia rozprzestrzeniały wirusy w kolejnych sieciach.

W celu zwiększenia ochrony systemów monitoringu wizyjnego przed cyberatakami izraelska firma Provision-ISR, producent urządzeń CCTV, nawiązała współpracę ze światowym liderem w dziedzinie bezpieczeństwa internetowego, firmą Check Point. Współpraca zaowocowała wdrożeniem do urządzeń Provision-ISR dwóch kluczowych rozwiązań: Check Point Quantum IoT Protect oraz Check Point Nano Agent.

Check Point Quantum IoT Protect wielokrotnie skanuje oprogramowanie, aby upewnić się, że jest ono wolne od wszelkich znanych luk w zabezpieczeniach, w tym komponentów pochodzących od firm zewnętrznych i z otwartych bibliotek. Automatycznie identyfikuje i mapuje urządzenie IoT podłączone do sieci oraz ocenia ryzyko jego zainfekowania. Zapobiega nieautoryzowanemu dostępowi do i z urządzeń dzięki profilowaniu i segmentacji zero-trust, blokuje ataki IoT typu zero-day. Dzięki wiodącej w branży analizie zagrożeń zapewnia pełną ochronę w czasie skanowania urządzenia.

Check Point IoT Protect Nano Agent działa wewnątrz urządzeń CCTV na poziomie oprogramowania układowego, wzmacnia je i zapewnia ochronę. Po wdrożeniu monitoruje wejścia, wyjścia i stan chronionego urządzenia. Wyszukuje zarówno znane ataki, jak i anomalie, które mogą wskazywać na próbę wykorzystania luki zero-day. W przypadku wykrycia takiego ataku Nano Agent może całkowicie zablokować atak lub zaalarmować zespół ds. bezpieczeństwa organizacji.

Firma ICS Polska, jako wyłączny dystrybutor urządzeń Provision-ISR w Polsce, rozpoczęła wdrażanie urządzeń z oprogramowaniem Check Point. Rozwiązania te będą dostępne na polskim rynku już od czwartego kwartału 2022 roku. Zapraszamy zainteresowanych do kontaktu.

ICS POLSKA

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

VENOM PSIM
polska, zaawansowana platforma integracji

Platforma VENOM pozwala identyfikować, zarządzać, mierzyć i minimalizować różnego typu zagrożenia związane z bezpieczeństwem oraz odpowiednio wcześnie im zapobiegać.

System jest zaprojektowany tak, aby bez technicznych ograniczeń zapewnić przejrzyste oraz płynne wdrożenie procesów i polityki bezpieczeństwa na różnego typu obiektach i nadzorowanych obszarach.

Dzięki funkcji agregacji i analizie wrażliwych danych z różnych systemów zarządzanych przez platformę PSIM użytkownicy mogą w czasie rzeczywistym reagować na ewentualne zagrożenia i eskalować proces takiej reakcji, planować działania oraz stale poprawiać efektywność operacyjną związaną z bezpieczeństwem, optymalizując przy tym wewnętrzne koszty zapewnienia bezpieczeństwa.

RYNKI

System VENOM doskonale sprawdza się zarówno w dużych obiektach scentralizowanych (np. elektrownie, transport, logistyka, serwerownie, lotniska, fabryki, obiekty publiczne), jak i przy wielu mniejszych obiektach rozproszonych na terenie całego kraju. Jak potwierdziły ostatnie wdrożenia w sektorze energetycznym, podłączenie nawet tysiąca obiektów nie stanowi dla VENOM PSIM żadnego problemu.
Nowoczesne podejście do zagadnień zapewnienia bezpieczeństwa fizycznego polega na odejściu od klasycznego modelu obserwowania obrazów z kamer na rzecz wykorzystania:

- sztucznej inteligencji w analitykach wideo,
- korelacji zdarzeń z poszczególnych podsystemów,
- natywnej integracji z systemami firm świadczących usługi grup interwencyjnych,
- efektywnemu, elastycznemu i intuicyjnemu silnikowi procedur postępowania dla operatorów.

WDROŻENIE

Przy wdrożeniu systemu klasy PSIM warto zwrócić uwagę na możliwość i koszty jego późniejszej rozbudowy, integracji kolejnych systemów, dodania nowych obiektów czy stacji operatorskich oraz – przede wszystkim – kolejnych elementów systemów już zintegrowanych (np. kamer czy innych czujników). Kluczowym argumentem jest też zapewnienie przez producenta wsparcia realizowanego przez doświadczony zespół polskich inżynierów i programistów.

WSPÓŁPRACA

Zapraszamy do współpracy wszystkich zainteresowanych, szczególnie użytkowników końcowych oraz integratorów.

MEGAVISION TECHNOLOGY

ul. Heliotropów 1
04-796 Warszawa
www.megavision.pl
k.rybak@megavision.pl

Zapobieganie fałszywym alarmom

Tobiasz Bąkowski

Według statystyk PSP w 2021 r. interwencje straży pożarnej były wyjątkowo częste. W ubiegłym roku strażacy interweniowali 579 722 razy, w tym przy 106 465 pożarach, 428 046 miejscowych zagrożeniach oraz 45 211 fałszywych alarmach.

Porównując liczbę fałszywych alarmów z rokiem poprzednim, zwiększyła się aż o ponad 4500 zdarzeń. Duża część fałszywych alarmów jest generowana w obiektach użyteczności publicznej wyposażonych w systemy sygnalizacji pożarowej. Powodem wywołania alarmu i postawienia strażaków w stan gotowości może być papieros w toalecie, nieumyślne wciśnięcie ręcznego ostrzegacza pożarowego, zbyt duże zadymienie w kuchni itp. Mimo tak błahych sytuacji niewymagających interwencji strażacy muszą udać się na miejsce.

JAK PRZECIWDZIAŁAĆ FAŁSZYWYM ALARMOM?

Kwestia bezpieczeństwa powinna być uwzględniana przez każdego inwestora i właściciela obiektów, takich jak zakłady produkcyjne, przemysłowe, dworce, magazyny czy centra logistyczne. Zabezpieczane obiekty ze względu na różną specyfikę wymagają doboru odpowiednich urządzeń przeciwpożarowych. Niezależnie od dobranego rodzaju zabezpieczeń ppoż. pochodzących od różnych producentów skuteczność działania, a tym samym wyższy poziom bezpieczeństwa pożarowego zapewnia integracja i zarządzanie wszystkimi systemami ochrony przeciwpożarowej za pomocą integratora CC WINGUARD.

W ubiegłym roku strażacy interweniowali

579 722 razy

Wspomniany integrator spełnia obowiązujące wytyczne i normy, co potwierdzają zdobyte świadectwa i certyfikaty wydane przez CNBOP-PIB.

CZY INTEGRACJA WYSTĘPUJE WYŁĄCZNIE NA POZIOMIE SYSTEMÓW PPOŻ.?

CC WINGUARD, oprócz integracji systemów ochrony ppoż., przejmuje zarządzanie pozostałymi urządzeniami i systemami zabezpieczeń różnych producentów, co pozwala na kontrolowanie wszystkich zastosowanych systemów sygnalizacji pożarowej, również o architekturze rozproszonej, za pośrednictwem jednolitego interfejsu operatora w ramach zunifikowanej platformy sprzętowo-programowej.

Wizualizacja i możliwość sterowania systemami ppoż. za pomocą certyfikowanego integratora przyczynia się do poprawy bezpieczeństwa obiektu oraz umożliwia pracę nawet przy utracie zasilania podstawowego. Potwierdzanie lub kasowanie alarmów pożarowych, sterowanie klapami pożarowymi, zmiany scenariusza pożarowego na polecenie kierującego akcją ewakuacyjną to tylko część działań, które można szybko i sprawnie przeprowadzić z poziomu stacji operatorskiej.

CZY MOŻNA ZDEFINIOWAĆ INDYWIDUALNE PROCEDURY BEZPIECZEŃSTWA?

Można. Zasadniczy element integratora CC WINGUARD stanowi platforma WinGuard PSIM+ zarządzająca z poziomu pulpitu operatora zdarzeniami pożarowymi wykrytymi przez systemy ppoż. dowolnego producenta. W sytuacji zagrożenia pożarowego osoba kierująca akcją ratunkową może, dzięki integratorowi, podjąć odpowiednie kroki zgodnie z procedurami bezpieczeństwa zdefiniowanymi dla całego chronionego obiektu.

C&C PARTNERS
ul. 17 Stycznia 119, 121
64-100 Leszno
www.ccpartners.pl
t.bakowski@ccpartners.pl

2N aktualizuje swój system operacyjny

Aktualizacja systemu operacyjnego dodaje funkcje wspierające działanie wirtualnych recepcji – trendu, który nabiera tempa w wyniku powszechnej pracy hybrydowej. Rozszerzenia ułatwią osobom niedosłyszącym komunikację z recepcjonistami za pomocą języka migowego. Ulepszenia poprawią również bezpieczeństwo, zarówno w budynkach biurowych, jak i wysokiej klasy projektach mieszkaniowych.

2N, światowy lider na rynku interkomów i systemów kontroli dostępu z obsługą Internetu za pomocą aktualizacji systemu operacyjnego, dodał nową funkcjonalność do swoich urządzeń. Ulepszenia, jakie zapewnia aktualizacja, będą wspierać elastyczną pracę i zapewnią, że osoby niedosłyszące będą mogły używać urządzeń 2N.

Opublikowane w maju badanie Occupier Survey 2022 CBRE przeprowadzone przez agencję EMEA wykazało, że tylko 6% firm obecnie wymaga od pracowników powrotu do biura w pełnym wymiarze godzin, a 72% twierdzi, że zmierza w kierunku modelu „hybrydowego miejsca pracy". Ponad 60% firm chce zwiększyć dostępność mieszanych, współdzielonych lub mobilnych miejsc pracy, przy czym blisko 80% planuje zmniejszenie liczby dedykowanych stanowisk.

W efekcie coraz więcej firm ponownie rozważa rentowność „tradycyjnego" recepcjonisty – osoby urzędującej w recepcji przez cały dzień roboczy, aby nadzorować dostęp do budynku. Odpowiedzią na obserwowane zmiany jest nowy system operacyjny 2N, który umożliwia dwukierunkowy sygnał wizyjny dzięki 2N® IP Style – flagowemu interkomowi firmy. Pozwala on gościowi zobaczyć osobę, z którą rozmawia, i na odwrót – co ma szczególną wartość w budynkach, w których odchodzi się od dedykowanej recepcji. Recepcjonista musi oczywiście być wyposażony w telefon IP z kamerą – najlepiej nowy telefon IP D7A marki 2N.

Dwukierunkowa transmisja wideo jest też odpowiedzią na rosnące zapotrzebowanie na inkluzywność funkcjonalności urządzenia, ponieważ pozwala osobom niedosłyszącym komunikować się za pomocą języka migowego. Aktualizacja wprowadza również nowe możliwości i udogodnienia w zakresie bezpieczeństwa:

Po pierwsze, ustawienia ONVIF zostały poddane całkowitej przeróbce, a interkomy 2N obsługują teraz profile T i S. Profil S już wcześniej obsługiwał podstawowe strumieniowanie wideo, natomiast profil T umożliwia zaawansowane strumieniowanie wideo. Otwiera to szereg nowych możliwości, w tym wykrywanie ruchu i alarmy sabotażowe, a także obsługę dwukierunkowej transmisji dźwięku. Nowy system operacyjny 2N rozszerza tym samym możliwości integracji z zewnętrznymi urządzeniami zabezpieczającymi, umożliwiając klientom podłączenie urządzeń 2N do w pełni kompleksowych rozwiązań bezpieczeństwa.

Po drugie, aktualizacja systemu operacyjnego 2N poprawia jakość obrazów wysyłanych do interkomu 2N® Indoor View, 7-calowego ekranu dotykowego przeznaczonego do luksusowych projektów mieszkaniowych. Aktualizacja pozwala również powiększyć obraz na ekranie interkomu poprzez zbliżenie obrazu dwoma palcami, tak jak w telefonie, dzięki czemu użytkownik lepiej widzi twarz dzwoniącego, plakietkę lub identyfikator. Ponadto, po raz pierwszy aktualizacja pozwala odwiedzającemu pozostawić wiadomość wideo na interkomie 2N® Indoor View, gdy mieszkańca nie ma w domu.

– *Nieustannie szukamy sposobów, aby reagować na opinie naszych klientów, czyniąc nasze urządzenia jeszcze bardziej bezpiecznymi i wygodnymi. Produkty takie jak 2N® IP Style i 2N® Indoor View były już liderami w branży. Dzięki ciągłemu ulepszaniu funkcji – tak jak to zrobiliśmy dzięki aktualizacji systemu operacyjnego – zapewnimy, że pozostaną nimi* – powiedział Czesław Półtorak, Business Development Manager w 2N Telekomunikace.

2N TELEKOMUNIKACE
Pod Vinicí 20
14301 Praha 4
Czech Republic
www.2n.com

Rozwiązania na miarę potrzeb klienta

ZKTeco jest dużą międzynarodową firmą specjalizującą się w nowoczesnych technikach rozpoznawania biometrycznego. Dostarcza produkty i rozwiązania do inteligentnego zarządzania wejściem, inteligentnego uwierzytelniania tożsamości oraz inteligentnego biura. Działając w sektorze elektronicznych systemów zabezpieczeń, swoją ofertę kieruje do użytkowników usług publicznych, przedsiębiorstw i osób fizycznych.

Marek Piotrowski

Główny profil działalności firmy opiera się na opracowanych przez własnych konstruktorów algorytmach weryfikacji biometrycznej zastosowanych następnie w modułach biometrycznych, czujnikach i oprogramowaniu. Firma ma wiele zgłoszonych patentów w zakresie technik rozpoznawania linii papilarnych, linii dłoni, naczyń krwionośnych, tęczówki oka i twarzy, a także szereg wykorzystywanych do tych celów technik komputerowych.
To czyni ZKTeco liderem w liczbie innowacyjnych rozwiązań w tym zakresie. W oparciu o nie firma oferuje urządzenia stosowane w kontroli dostępu, rejestracji czasu pracy, zarządzaniu przepływem osób i wielu innych, wymagających technik oceny tożsamości, weryfikacji i uwierzytelniania – począwszy od podstawowych czytników RFID i kodów QR, po autonomiczne inteligentne urządzenia integrujące w sobie wiele technik biometrycznych.

PLATFORMY ZARZĄDZAJĄCE BEZPIECZEŃSTWEM

Kolejną grupę produktów opatentowanych przez ZKTeco stanowią różnego typu platformy integrujące do obsługi wejść, rozpoznawania osób, samochodów i innych obiektów. W swoich rozwiązaniach firma dąży do integracji hybrydowych technik weryfikacji biometrycznej i komputerowych technik wizyjnych z Internetem, IoT, *big data* i rozwiązaniami chmurowymi, budując platformy o różnym zastosowaniu. Oferuje rozwiązania zarówno dla małych i średnich firm, jak i dla dużych międzynarodowych korporacji o różnej skali integracji i przeznaczeniu, w tym rozwiązania Push i Pull, zewnętrzne i wbudowane w kontrolery (web serwer) oraz aplikacje na smartfony.
Niektóre platformy, jak np. stosowana głównie w kontroli dostępu BioSecurity, mają konstrukcję modułową, integrującą wiele funkcji. Inne rozwiązania, np. rewelacyjne oprogramowanie do rejestracji czasu pracy GoTimeCloud, jest oparte na chmurze.

Jako firma globalna ZKTeco ma swoje przedstawicielstwa

w 40 krajach

Zatrudnia

1100 inżynierów

Firma dostarcza pakiety API do integracji swojego oprogramowania z oprogramowaniem innych firm i świadczy w tym zakresie usługi.

INNE PRODUKTY FIRMY

Firma ZKTeco, oprócz wymienionych opracowań stanowiących jej *core business*, wciąż rozszerza swoją ofertę o inne grupy produktowe. Szczyci się szeroką gamą bramek przejścia i kołowrotów, często zintegrowanych z kontrolą dostępu, rozwiązaniami parkingowymi (w tym wysokiej jakości szlabanami), kamerami LPR i radarami, produktami do inspekcji (w tym wykrywaczami metali), urządzeniami do dozoru wizyjnego, inteligentnymi zamkami (w tym stosowanymi w hotelach) oraz elektrozaczepami. Co roku na międzynarodowych targach produkty firmy zdobywają nagrody za swoją wysoką jakość i innowacyjność.

Jako firma globalna ZKTeco ma swoje przedstawicielstwa w 40 krajach. Zatrudnia 3800 pracowników w produkcji i 1100 inżynierów w rozrzuconych na całym świecie biurach badawczo-rozwojowych, w tym w trzech biurach w USA, gdzie powstała.
Główna siedziba firmy znajduje się obecnie w Chinach i tu produkowana jest większość urządzeń. Podległa jej firma ZKTeco Europe kontroluje rynek europejski, zajmując się – oprócz logistyki i sprzedaży towarów – wsparciem technicznym dla klienta. Posiada Experience Center, w którym testuje jakościowo produkty, dostosowując je do specyfiki i wymagań rynku europejskiego, a także własne biuro konstrukcyjne.
Polska jest kolejnym rynkiem, który firma ZKTeco ma zamiar podbić, otwierając swoje biuro w Warszawie. Celem firmy jest być blisko klienta, dostarczając mu to, czego potrzebuje.

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

Jednolity rynek wyrobów budowlanych

– nadchodzące zmiany (certyfikacja europejska, oznakowanie CE)

Urzędnicy z Komisji Europejskiej nie są w pełni zadowoleni z rezultatów wdrożenia i funkcjonowania rozporządzenia 305/2011 (CPR) na rzecz jednolitego (wewnątrzwspólnotowego) rynku wyrobów budowlanych. Zaproponowano zmiany, które w niektórych przypadkach można uznać za rewolucyjne.

mł. bryg. mgr inż. Grzegorz Mroczko

Dokumenty i oznakowanie CE związane z oceną wyrobów budowlanych w tzw. systemie europejskim omówiłem w artykule w numerze 2/2022 „a&s". Obecne zasady obowiązują już 9 lat, wszyscy oswoiliśmy się z nimi i do nich przyzwyczaili – wiedza, świadomość i doświadczenie uczestników rynku wyrobów budowlanych w tym zakresie są na wysokim poziomie.

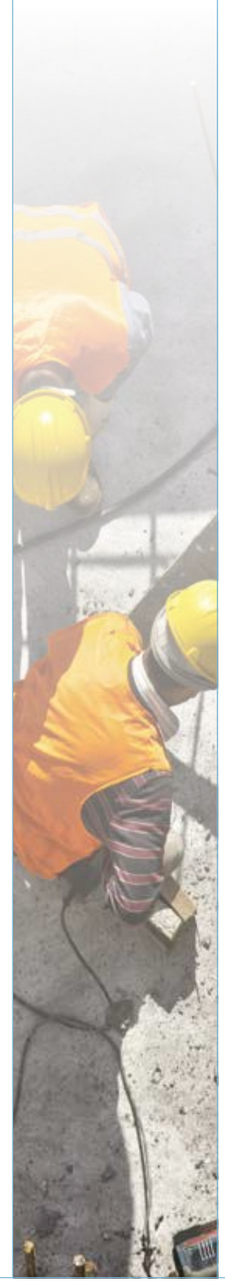
Jak pokazują wyniki analizy funkcjonowania rynku wyrobów budowlanych, jaką prowadziła Komisja Europejska (KE) we współpracy z ekspertami z wielu środowisk i branż, wystąpiły określone problemy z osiągnięciem celów, w jakich regulacje te powołano. KE zidentyfikowała następujące problemy:

1. Nie powstał jednolity rynek wyrobów budowlanych ze względu na nieprawidłowo działający proces normalizacji i harmonizacji norm.
2. Wyzwania związane z wdrażaniem na poziomie krajowym.
3. Nie dokonano uproszczenia ram prawnych.
4. Brak możliwości realizacji szerszych priorytetów politycznych UE, w tym m.in. transformacji ekologicznej i cyfrowej.

W ostatnich latach projekty norm zharmonizowanych opracowane przez Europejskie Organizacje Normalizacyjne rzadko mogły być cytowane w Dzienniku Urzędowym (OJEU) głównie ze względu na ich braki prawne. Normy zharmonizowane, w myśl CPR, mogą wskazywać jedynie wymagania i metody oceny właściwości użytkowych w odniesieniu do zasadniczych charakterystyk związanych z wymaganiami podstawowymi dla obiektów budowlanych. Nie można zatem w normach wskazywać innych wymagań, takich, które nie są związane z właściwościami użytkowymi – dla przykładu wymaganie poprawnego działania, kolorystyki czy funkcjonalności nie leży, w myśl CPR, w obszarze właściwości użytkowych. Sytuacja ta budzi spore kontrowersje i sprzeciw przedstawicieli poszczególnych branż.

Wyroby budowlane z grupy 10 *Fixed firefighting equipment* (SSP, DSO, oddymianie, SUG itp.) wyraźnie odróżniają się od typowych wyrobów budowlanych – to urządzenia elektroniczne sterowane za pomocą dedykowanego oprogramowania. Dla nich nie ma możliwości opisania wymagań jedynie w formie właściwości użytkowych. Są to często istotne kwestie właściwe dla tego typu urządzeń, np. kolorystyka obudów przycisków sterujących (ROP czerwony, RPO pomarańczowy), sygnalizacja stanu pracy systemów (zielony – dozór, żółty uszkodzenie, czerwony – alarm) czy też funkcjonalność urządzenia do ładowania akumulatorów zasilania rezerwowego central itp. Zapisanie takich wymagań w normie zharmonizowanej jest niezgodne z postanowieniami aktualnego CPR – to m.in. z tego powodu nie może zostać opublikowany i zharmonizowany projekt normy EN 12101-9, podobnie aktualizacje i zmiany do norm serii EN 54, EN 12094 czy EN 12101.
Oczywiście wiele norm zharmonizowanych z obszaru SSP, SUG takie wymagania opisuje, ponieważ zostały opublikowane i zharmonizowane w czasie obowiązywania dyrektywy budowlanej (przed rokiem 2013) lub w początkach funkcjonowania CPR. Normy w ich brzmieniu są stosowane, natomiast nie można opublikować i zharmonizować zmian czy aktualizacji tych norm. Brak cytowania nowych norm zharmonizowanych w OJEU ogranicza sprawne funkcjonowanie jednolitego rynku, tworzy bariery handlowe, dodatkowe koszty i obciążenia administracyjne dla podmiotów gospodarczych – m.in. dlatego, że zamiast paneuropejskiej certyfikacji i oznakowania CE producenci zmuszeni są do certyfikacji wyrobów w każdym kraju odrębnie.
Złożoność i niejednolitość przepisów krajowych przyczyniają się też do różnic w funkcjonowaniu i skuteczności nadzoru budowlanego w poszczególnych państwach członkowskich UE. Niejasne przepisy i różny sposób ich egzekucji w każdym kraju UE zniechęca producentów do wprowadzania wyrobów na rynek. Podobny problem występował w okresie obowiązywania dyrektywy budowlanej 889/106/EEC, a rozporządzenie 305/2011 miało ten problem rozwiązać.

Normy zharmonizowane, w myśl CPR, mogą wskazywać jedynie wymagania i metody oceny właściwości użytkowych



Kolejnym problemem jest błędne rozumienie i interpretowanie oznakowania CE. Zgodnie z rozporządzeniem 305/2011 (CPR) jest ono powiązane z oceną właściwości użytkowych wyrobu budowlanego, a nie ze zgodnością wyrobu z wymaganiami, ponieważ te nie są/nie mogą być określane w normach zharmonizowanych. Oznakowanie CE może być naniesione na wyrób w sytuacji, gdy ma on potwierdzoną jedną właściwość użytkową (np. spośród 10 wskazanych w normie zharmonizowanej). Samo oznakowanie CE nie oznacza zatem częściowej czy pełnej zgodności wyrobu z normą zharmonizowaną – dopiero lektura deklaracji właściwości użytkowych pozwala dowiedzieć się, jakie właściwości użytkowe wyrobu deklaruje jego producent.
Natomiast w innych przepisach UE oznakowanie CE oznacza właśnie zgodność wyrobu z wymaganiami, które są określone w dyrektywach i normach zharmonizowanych z tymi dyrektywami – w rozumieniu wszystkich wymagań zapisanych w tych dokumentach.

Inne przepisy CPR są niewystarczająco jasne albo nakładają się na siebie w obrębie samego CPR (np. pokrywanie się informacji wymaganych w deklaracji właściwości użytkowych i w oznakowaniu CE) lub między CPR a innymi przepisami UE. Ponadto aktualna treść CPR uniemożliwia realizację szerszych priorytetów politycznych UE, w tym m.in. transformacji ekologicznej i cyfrowej. W przypadku transformacji ekologicznej problem polega na tym, że dostępne normy zharmonizowane obejmują tylko niektóre elementy związane z oddziaływaniem wyrobów na środowisko (np. zanieczyszczenie). Wielu zagadnień nie sposób wyrazić w normach poprzez wskazanie wyłącznie metod oceny właściwości użytkowych, a inny sposób – czyli stawianie wyrobom wprost wymagań w normach zharmonizowanych – jest obecnie niezgodny z CPR.
W przypadku transformacji cyfrowej aktualne brzmienie CPR wspiera formę papierową dokumentowania właściwości użytkowych, a jako dodatkową możliwość wskazuje formę cyfrową. To sprawia, że informacje o wyrobach budowlanych w formie cyfrowej nie są wystarczająco dostępne dla uczestników rynku i tym samym cele dotyczące transformacji cyfrowej nie mogą być osiągnięte.

ABY ROZWIĄZAĆ POWYŻSZE PROBLEMY, KE OPRACOWAŁA PROJEKT ZMIANY ROZPORZĄDZENIA CPR, KTÓRA MA NA CELU:

- stworzenie sprawnie funkcjonującego jednolitego rynku wyrobów budowlanych,
- zapewnienie, by ramy mogły przyczynić się do osiągnięcia celów ekologicznej i cyfrowej transformacji, w szczególności gospodarki nowoczesnej, zasobooszczędnej i konkurencyjnej.

TE OGÓLNE CELE ZOSTAŁY UZUPEŁNIONE CELAMI SZCZEGÓŁOWYMI:

- odblokowanie systemu harmonizacji technicznej,
- zmniejszenie krajowych barier w handlu wyrobami objętymi rozporządzeniem w sprawie wyrobów budowlanych,
- poprawa egzekwowania przepisów i nadzoru rynku,
- zapewnienie większej jasności (bardziej wyczerpujące definicje, ograniczenie nakładania się przepisów, kolizja przepisów z innymi aktami prawnymi) i uproszczenie,
- zmniejszenie obciążeń administracyjnych, m.in. poprzez uproszczenie i cyfryzację,
- zapewnienie bezpiecznych wyrobów budowlanych,
- przyczynianie się do zmniejszenia ogólnego wpływu wyrobów budowlanych na klimat i środowisko, m.in. dzięki stosowaniu narzędzi cyfrowych (paszportu cyfrowego).

KE ocenia, że rewizja rozporządzenia CPR będzie korzystna dla producentów, ponieważ lepiej funkcjonujący jednolity rynek zapewni przedsiębiorstwom budowlanym dostęp do szerszej oferty wyrobów, jednak nie odbędzie się to bez kosztów. Producenci wyrobów budowlanych będą musieli wywiązać się z większej liczby zobowiązań, aby wprowadzić swoje wyroby do obrotu,

KE ocenia, że rewizja rozporządzenia CPR będzie korzystna dla producentów, ponieważ lepiej funkcjonujący jednolity rynek zapewni przedsiębiorstwom budowlanym dostęp do szerszej oferty wyrobów, jednak nie odbędzie się to bez kosztów

co spowoduje wzrost kosztów po ich stronie (szacuje się, że będzie to 8% kosztów podstawowych działalności, czyli ok. 200 mln euro rocznie). Ale jednocześnie będą mieli więcej możliwości rynkowych i nadal będą funkcjonowały uproszczone procedury dla mikroprzedsiębiorstw. Z jednej strony państwa UE będą musiały przeznaczyć więcej środków na nadzór rynku, z drugiej – zmiana zapewni im znaczne wsparcie pod względem ich odpowiedzialności za bezpieczeństwo obiektów budowlanych.

KRÓTKIE OMÓWIENIE WYBRANYCH ZMIAN PROPONOWANYCH W NOWYM BRZMIENIU ROZPORZĄDZENIA CPR

1. Nowy zakres przedmiotowy obowiązywania rozporządzenia:

- wyroby budowlane, w tym wyroby używane i wyroby poddane regeneracji,
- zbiory danych 3D wprowadzone do obrotu w celu umożliwienia drukowania przestrzennego wyrobów budowlanych objętych rozporządzeniem oraz wyrobów budowlanych i form wydrukowanych przestrzennie;
- materiały przeznaczone do wykorzystania podczas drukowania przestrzennego wyrobów budowlanych na terenie budowy lub w jej pobliżu lub do produkcji przy użyciu form na terenie budowy lub w jej pobliżu;
- wyroby budowlane produkowane na terenie budowy w celu natychmiastowego wbudowania ich w obiekty budowlane, bez konieczności podjęcia oddzielnych działań handlowych zmierzających do wprowadzenia ich do obrotu;
- części kluczowe wyrobów objętych rozporządzeniem;
- części lub materiały przeznaczone do stosowania w wyrobach objętych rozporządzeniem, jeśli wniesie o to producent tych części lub materiałów;
- zestawy lub zespoły, jeżeli ich skład określono i ujęto w zharmonizowanych specyfikacjach technicznych lub europejskich dokumentach oceny;
- prefabrykowane domy jednorodzinne jednokondygnacyjne o powierzchni użytkowej mniejszej niż 180 m2 lub dwukondygnacyjne o powierzchni użytkowej mniejszej niż 100 m2 na kondygnację.

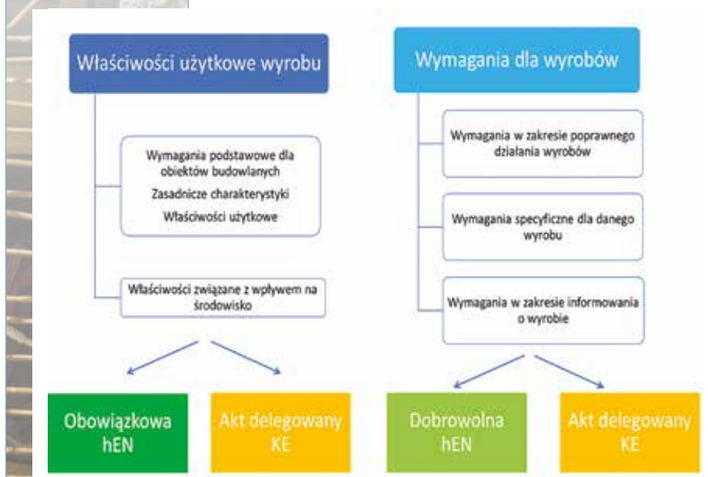
Jednocześnie z zakresu wyrobów budowlanych usuwa się wyroby objęte m.in. dyrektywami: dźwigową, w sprawie wody pitnej oraz w sprawie ścieków komunalnych:
– dźwigi (windy),
– schody ruchome i ich elementy,
– kotły, rury, zbiorniki i urządzenia pomocnicze oraz inne produkty przeznaczone do kontaktu z wodą do spożycia przez ludzi,
– systemy oczyszczania ścieków,
– urządzenia sanitarne,
– wyroby związane z sygnalizacją świetlną drogową.

2. Odblokowanie systemu harmonizacji technicznej

W zmienionym rozporządzeniu CPR proponuje się podział specyfikacji technicznych na dwie grupy:

- **Obowiązkowe normy zharmonizowane**, które nadal będą dotyczyły oceny właściwości użytkowych związanych ze spełnieniem przez obiekty budowlane wymagań podstawowych określonych w załączniku 1. do rozporządzenia CPR[1]. W oparciu o te normy, tak jak dotychczas, producenci będą oceniali i deklarowali właściwości użytkowe wyrobów.
- **Dobrowolne normy zharmonizowane**, które będą wskazywały istotne, ale nie związane z oceną ich właściwości użytkowych wymagania dla wyrobów, np. wymagania w zakresie spełnienia zamierzonego celu zastosowania; poprawnego działania wyrobu; w zakresie konstrukcji, kolorystyki i funkcji; dot. informowania o wyrobie (znakowanie, etykiety i dokumenty towarzyszące wyrobowi). Zgodnie z tymi normami producenci będą oceniali i deklarowali zgodność wyrobu z wymaganiami dla wyrobu.

W celu dalszego usprawnienia i nadrobienia zaległości w harmonizacji technicznej wyrobów KE nadaje sobie dodatkowe uprawnienia polegające na możliwości ustanawiania wymagań technicznych dla wyrobów (w zakresie zarówno właściwości użytkowych, jak i wymagań dla wyrobu) w drodze aktów delegowanych do rozporządzenia CPR. Możliwe to będzie m in. w przypadku, gdy:
– występują nieuzasadnione opóźnienia w przyjęciu norm przez europejskie organizacje normalizacyjne;
– istnieje pilna potrzeba przyjęcia bardziej zharmonizowanych specyfikacji technicznych, których nie można uregulować samymi normami;
– co najmniej jedna zasadnicza charakterystyka odnosząca się do podstawowych wymagań dla obiektów budowlanych nie jest objęta normami, do których odniesienia już zostały opublikowane w Dzienniku Urzędowym;
– normy są z innych powodów uznane za niewystarczające do pokrycia potrzeb regulacyjnych państw członkowskich lub potrzeb podmiotów gospodarczych;
– normy nie są zgodne z prawodawstwem i ambicjami UE w zakresie klimatu i środowiska.



Rys. 1. Nowe formy harmonizacji technicznej wymagań dla wyrobów budowlanych

3. Wprowadzenie nowych i modyfikacja istniejących definicji

W aktualnym brzmieniu rozporządzenie CPR wskazuje 28 definicji, projekt zmiany wprowadza ich aż 71, w tym m.in. definicje typu wyrobu, rodziny wyrobów, wyrobu używanego i poddanego regeneracji, produkowanego jednostkowo, nieseryjnego procesu produkcyjnego, a także naprawy, konserwacji, części kluczowej wyrobu, materiałów przeznaczonych do drukowania przestrzennego wyrobów, dostawcy usług drukowania przestrzennego, bezpośredni montaż, wymogów dot. wyrobów i inne. Zmieniono także brzmienie wybranych definicji, np. definicji wyrobu budowlanego i zestawu wyrobów (tabela). Doprecyzowano zatem obszar stosowania rozporządzenia i wyjaśniono kwestie dotychczas nieokreślone, które powodowały niejednolitość stosowania rozporządzenia w krajach członkowskich UE.

[1] Przy czym konkretne wymagania dot. właściwości użytkowych wyrobów mają wynikać z przepisów techniczno-budowlanych danego kraju członkowskiego, np. wymaganie w zakresie klasy odporności ogniowej elementów budynku, w zakresie ciągłości dostawy energii w warunkach pożaru dla zespołów kablowych wskazane w rozporządzeniu dot. warunków technicznych, jakim powinny odpowiadać budynki i ich usytuowanie.

DEFINICJA	AKTUALNE BRZMIENIE	NOWE BRZMIENIE
wyrób budowlany	każdy wyrób lub zestaw wyprodukowany i wprowadzony do obrotu w celu trwałego wbudowania w obiektach budowlanych lub ich częściach, mający wpływ na spełnienie wymagań podstawowych przez te obiekty	każdy uformowany lub bezkształtny element fizyczny, łącznie z jego opakowaniem i instrukcją obsługi, lub zestaw bądź zespół łączący takie elementy, który jest wprowadzany do obrotu lub produkowany w celu trwałego wbudowania w obiekty budowlane lub ich części na terenie Unii, z wyjątkiem elementów, które z konieczności najpierw zostają trwale połączone w zespół, zestaw lub inny wyrób budowlany, zanim zostaną trwale wbudowane w obiekty budowlane
trwały	–	trwający dwa lata lub dłużej
zestaw wyrobów	oznacza wyrób budowlany wprowadzony do obrotu przez jednego producenta, jako zestaw co najmniej dwóch odrębnych elementów, które muszą zostać połączone, aby mogły zostać wbudowane w obiektach budowlanych	wyrób wprowadzony do obrotu przez jeden podmiot gospodarczy jako zestaw co najmniej dwóch odrębnych elementów, z których żaden nie musi być wyrobem, przeznaczony do łącznego wbudowania w obiekty budowlane
zespół	–	zestaw co najmniej dwóch odrębnych elementów, z których jeden jest wyrobem
wyrób używany	–	wyrób, który nie jest odpadem w rozumieniu art. 3 pkt 1 dyrektywy Parlamentu Europejskiego i Rady 2008/98/WE i który został wbudowany co najmniej raz w dany obiekt budowlany oraz a) nie został poddany procesowi wykraczającemu poza naprawę, czyszczenie lub regularną konserwację, określonemu przez pierwotnego producenta w instrukcji obsługi lub uznanemu za konieczny zgodnie z powszechną wiedzą z zakresu inżynierii lądowej, b) nie został poddany procesowi wykraczającemu poza naprawę, czyszczenie i regularną konserwację lub „przygotowanie do ponownego użycia" w rozumieniu art. 3 pkt 16 dyrektywy 2008/98/WE po jego zdemontowaniu
wyrób poddany regeneracji	–	wyrób, który nie jest odpadem zgodnie z definicją zawartą w art. 3 pkt 1 dyrektywy 2008/98/WE, ale który wbudowano co najmniej raz w dany obiekt budowlany i który poddano procesowi przekształcenia wykraczającemu poza naprawę, czyszczenie i regularną konserwację
produkowany jednostkowo	–	oznacza, że ze względu na specyfikacje klienta występuje różnica dotycząca metody produkcji w porównaniu z wszystkimi innymi wyrobami wytwarzanymi dla innych klientów przez dany podmiot gospodarczy
nieseryjny proces rodukcyjny	–	oznacza proces, który nie jest ani w przeważającej mierze zautomatyzowany, ani służący produkcji z wykorzystaniem technik linii montażowej, ani też powtarzający więcej niż 100 razy w roku przez dany podmiot gospodarczy lub podmioty gospodarcze należące do tej samej grupy przedsiębiorstw, określonej przez wspólną osobę fizyczną lub prawną sprawującą kontrolę, lub tę samą strukturę organizacyjną

4. Nowe wymagania dla producentów wyrobów

W rozdziale III rozporządzenia określono prawa i obowiązki podmiotów gospodarczych, w tym m.in. producentów, upoważnionych przedstawicieli, importerów, dystrybutorów, a także obowiązki dostawców usług realizacji zamówień, brokerów, rynków internetowych, sprzedawców internetowych i sklepów internetowych oraz dostawców usług drukowania przestrzennego. Wprowadzono też nowe szczegółowe obowiązki podmiotów gospodarczych zajmujących się demontażem lub przetwarzaniem wyrobów używanych w celu ich ponownego użycia lub regeneracji.

5. Deklaracja właściwości użytkowych (DoP) i deklaracja zgodności (DoC)

Rozporządzenie wprowadza nowy obowiązek oceny i deklarowania zgodności wyrobu z wymaganiami dla wyrobu, które będą określone w dobrowolnych normach zharmonizowanych albo w aktach delegowanych KE. Wygląda na to, że dla każdego wyrobu konieczne będzie wystawienie dwóch rodzajów deklaracji – DoP i DoC. Dla ograniczenia obciążeń wprowadzono możliwość łączenia obu deklaracji w jeden dokument. To bardzo istotna, kłopotliwa i kosztowna zmiana generująca konieczność równoległego oceniania i deklarowania właściwości użytkowych wyrobów oraz zgodności wyrobu z wymaganiami dla wyrobów.

6. Oznakowanie CE i inne oznakowania na wyrobie

Oznakowanie CE umieszcza się na wyrobach, dla których producent sporządził deklarację właściwości użytkowych lub zgodności. Oznakowania CE nie umieszcza się na częściach kluczowych i na częściach, które nie są częściami kluczowymi. Oznakowania inne niż CE, np. oznakowania prywatne, można umieszczać na wyrobie wyłącznie wówczas, gdy nie odnoszą się do kwestii uregulowanych oznakowaniem CE. Na wyrobie nie można umieszczać żadnego oznakowania innego niż określone w przepisach unijnych w odległości mniejszej niż podwójna długość oznakowania CE (mierzona od dowolnego punktu oznakowania CE i innego oznakowania określonego w przepisach UE). Na deklaracji właściwości użytkowych lub deklaracji zgodności nie można umieszczać oznakowań innych niż oznakowanie CE.

PODSUMOWANIE

Treść rozporządzenia i załączników zajmuje ponad 100 stron. To skomplikowany i trudny tekst prawny, w którym – pod hasłem uproszczenia i ujednolicenia rynku wyrobów budowlanych – m.in. rozszerza się zakres przedmiotowy rozporządzenia, dokłada nowych uprawnień dla KE, wprowadza nowe obowiązki dla producentów wyrobów i jednostek notyfikowanych oceniających wyroby, a także wprowadza nowe wymagania dla wyrobów i nowy rodzaj deklaracji. Już wstępna lektura tego przepisu powoduje konsternację i liczne wątpliwości. Wdrożenie go do stosowania będzie dużym wyzwaniem dla państw członkowskich oraz wszystkich uczestników rynku wyrobów budowlanych.
Projekt zmiany rozporządzenia został zatwierdzony przez Komisję Europejską 31 marca 2022 r. Trwa proces legislacyjny, który jest obecnie na etapie pierwszego czytania w Radzie UE – Sekretariat Generalny Rady przekazał projekt do Grupy Roboczej ds. Własności Intelektualnej i Grupy Roboczej ds. Harmonizacji Technicznej.
Postępy procesu legislacji można śledzić pod adresem https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=CELEX:52022PC0144&sortOrder=asc.

Komisja Europejska przewiduje publikację zmienionego rozporządzenia w 2024 r. i ma ono zacząć obowiązywać w 2025 r. Czy proponowane zmiany pozwolą na osiągnięcie określonych przez Komisję celów?

MŁ. BRYG. MGR INŻ. GRZEGORZ MROCZKO

Absolwent SGSP, oficer PSP, pracownik Zakładu Ocen Technicznych CNBOP-PIB, koordynator ds. testowania wyrobów innowacyjnych wg procedury KG PSP, przedstawiciel Polski w TC 72 Europejskiego KT (CEN), członek KT 264 i KT 323 PKN. Od ponad 18 lat aktywny audytor jednostki certyfikującej w zakresie m.in. systemów sygnalizacji pożarowej, DSO, systemów wentylacji pożarowej, kabli i zespołów kablowych stosowanych w technicznych systemach zabezpieczeń ppoż.

Koniec fałszywych alarmów w placówkach służby zdrowia

Sektor opieki zdrowotnej jest trudnym środowiskiem, jeśli chodzi o rozważania dotyczące rozwiązań z zakresu wykrywania pożaru. Występowanie fałszywych alarmów utrudnia funkcjonowanie placówek służby zdrowia, co bezpośrednio wpływa na opiekę nad pacjentem, a w niektórych przypadkach zagraża życiu.

Oto pięć czynników, które należy wziąć pod uwagę, aby zapobiec fałszywym alarmom w placówkach służby zdrowia.

1.PROJEKTOWANIE I PLANOWANIE

Ważne jest ustalenie wymagań projektowych i operacyjnych systemu. W fazie planowania należy przeprowadzić analizę zagrożeń pożarowych i dobrać odpowiednie rozwiązania adekwatne do zagrożeń i ryzyka ich wystąpienia w poszczególnych obszarach. Równie istotnym elementem jest opracowanie scenariusza pożarowego i planu ewakuacji oraz ich uwzględnienie w projekcie systemu sygnalizacji pożarowej.

2.ODPOWIEDNIE SYSTEMY W KRYTYCZNYCH OBSZARACH

Badania wykazały, że jedną z najczęstszych przyczyn fałszywych alarmów w placówkach opieki zdrowotnej jest przyrządzanie posiłków. Skuteczne wykrywanie pożaru bez generowania fałszywych alarmów w kuchniach jest niezbędne i krytyczne dla bezpieczeństwa całego obiektu.

3.CZUJKI MULTISENSOROWE

Stosowanie czujek multisensorowych zawierających czujniki dymu, temperatury oraz CO gwarantuje wysoką niezawodność w wykrywaniu pożarów i minimalizuje ryzyko wystąpienia fałszywych alarmów szczególnie w obszarach zwiększonego ryzyka.

4.OKRES ADAPTACJI

Wprowadzenie okresu adaptacji instalacji, podczas którego działanie system jest monitorowane w odniesieniu do występowania fałszywych alarmów.

5.SERWIS I KONSERWACJA

Regularne zarządzanie systemem oraz przeglądy serwisowe i konserwacyjne pomagają zapobiegać fałszywym alarmom. Dotyczy to również budynku, w którym zainstalowany jest system detekcji. Przeciekający dach czy emisja pary mogą powodować niepożądane alarmy pożarowe.

Aby dowiedzieć się więcej o projektowaniu i planowaniu systemów detekcji pożaru, wejdź na stronę **www.zettlerfire.com**

JOHNSON CONTROLS INTERNATIONAL

ul. Krakowiaków 50
02-255 Warszawa
krzysztof.wiech@jci.com

DSO to nie tylko czytelne i zrozumiałe komunikaty głosowe

Rafał Kowal

Ciągły rozwój technologiczny systemu APS®-APROSYS produkowanego przez szwajcarską firmę g+m elektronik ag, oferowanego przez Schrack Seconet Polska, pozwala na coraz szersze wykorzystanie tego systemu w instalacjach bezpieczeństwa pożarowego. Produkt spełnia najbardziej wyrafinowane i pożądane funkcje wspomagające ewakuację, niekoniecznie związane jedynie z alarmem głosowym w obiekcie.

Mówiąc o DSO (dźwiękowym systemie ostrzegawczym), w pierwszej kolejności myślimy o systemie służącym do rozgłaszania komunikatów głosowych (automatycznych lub tych nadawanych na żywo za pośrednictwem pulpitu mikrofonowego), zazwyczaj poprzedzanych sygnałem dźwiękowym typu gong lub syrenka (najczęściej znormalizowane sygnały), mających na celu w sposób uporządkowany i jednoznaczny wspomóc proces ewakuacji ludzi z zagrożonej strefy. Krótko mówiąc, DSO jest elementem wykonawczym systemu SSP zastępującym standardowo stosowane sygnalizatory akustyczne lub akustyczno-optyczne.

Podstawową przewagą DSO nad często stosowanymi sygnalizatorami jest fakt, że o ile konwencjonalne sygnalizatory akustyczne (bez funkcji komunikatów głosowych) są w stanie wygenerować sygnał o wysokim poziomie SPL *(Sound Pressure Level),* np. 100 dB, który dodatkowo może być modulowany, by zwiększyć uwagę osób przebywających w zagrożonej strefie, o tyle jest to nadal tylko sam sygnał, po którym nie jesteśmy w stanie stwierdzić, z jakiego typu zagrożeniem mamy do czynienia i jak powinniśmy się zachować.
W przypadku DSO mamy możliwość wygenerowania krótkich sygnałów dźwiękowych (np. gong lub syrenka – poprzedzających komunikat słowny), których celem jest zwrócenie uwagi osób przebywających w danej strefie nagłośnieniowej, a następnie nadania komunikatu głosowego o konkretnej treści dostosowanej do typu, przeznaczenia obiektu i sytuacji, jaka w nim wystąpiła.
To podstawowa funkcja DSO i bezapelacyjnie pożądana w przypadku potrzeby sprawnego przeprowadzenia ewakuacji ludzi z zagrożonego obszaru/strefy. Inną kwestią jest język, w którym ten komunikat zostanie nadany. Często w ramach dobrej praktyki inżynierskiej stosuje się komunikaty dwujęzyczne, np. polsko-angielski lub nawet w trzech językach polsko-angielsko-niemiecki/ukraiński. Komunikaty te oczywiście są tego samego przeznaczenia: ostrzegawczy, ewakuacyjny lub odwołujący i odpowiednio skonstruowane zgodnie z projektem.

ROZGŁASZANIE KOMUNIKATÓW W PRZYPADKU SYSTEMU APS®-APROSYS MOŻE BYĆ ZREALIZOWANE NA RÓŻNE SPOSOBY, ZALEŻNIE OD SPOSOBU EWAKUACJI:

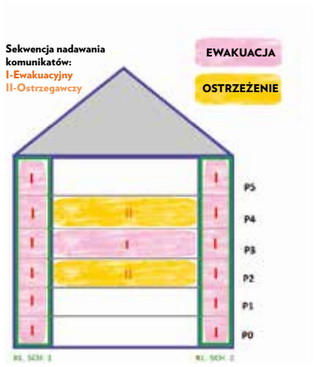
- **JEDNOETAPOWA** – po potwierdzeniu pożaru i alarmie II stopnia następuje ewakuacja całego budynku w jednym czasie *(rys. 1).*

Rys. 1. Przykład ewakuacji jednoetapowej

- **WIELOETAPOWA** z równoczesnym nadawaniem np. dwóch komunikatów – EWAKUACYJNEGO do strefy bezpośrednio zagrożonej i OSTRZEGAWCZEGO do stref przyległych *(rys. 2),*

Rys. 2. Przykład ewakuacji wieloetapowej

- **WIELOETAPOWA Z PODZIAŁEM NA NADAWANIE KOMUNIKATÓW** EWAKUACYJNEGO i OSTRZEGAWCZEGO w układzie sekwencyjnym (naprzemiennym), gdzie w pierwszej kolejności następuje ewakuacja osób ze strefy zagrożonej i klatek schodowych (I), a następnie, po zakończeniu rozgłaszania komunikatu ewakuacyjnego, następuje ostrzeganie stref przyległych (II), jak pokazano na *rys. 3.*

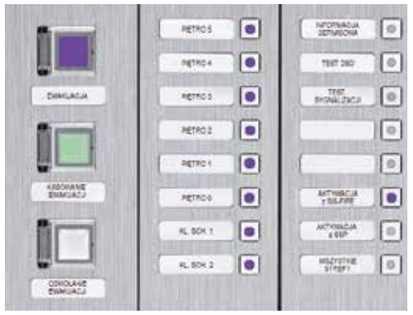


Rys. 3. Przykład ewakuacji wieloetapowej – sekwencyjnej

Opisane przykłady i odpowiedni dobór rozwiązania stanowią podstawę poprawnego zadziałania DSO w obiekcie i sprawnej ewakuacji ludzi z zagrożonej strefy. W szczególnych sytuacjach (np. w szpitalach, portach lotniczych) często stosuje się tzw. komunikaty kodowane przeznaczone dla przeszkolonego personelu. W przeciwieństwie do komunikatów ostrzegawczych czy ewakuacyjnych komunikaty kodowane powinny być tak skonstruowane, aby przede wszystkim nie wzbudzać paniki lub zaniepokojenia wśród osób przebywających w zagrożonej strefie. Mają na celu „dyskretnie" powiadomić przeszkolony personel o wykrytym zagrożeniu (może być to stan, kiedy zagrożenie nie zostało jeszcze potwierdzone – tzw. alarm pożarowy I stopnia) i pozwolić na przygotowanie do ewakuacji całego piętra/strefy.
Dodatkową i bardzo przydatną nie tylko w tego typu obiektach funkcją, jaką można znaleźć w systemie APS®-APROSYS, jest możliwość dodzwonienia się do systemu i zdalnego nadawania komunikatów w czasie rzeczywistym. Przeszkolony personel w sytuacji nadzwyczajnej (np. nagły atak agresji wśród osób przebywających w częściach wspólnych, próba sabotażu lub ataku terrorystycznego) może bezzwłocznie (bez zbędnej straty czasu na dotarcie do pomieszczenia ochrony, recepcji, gdzie zostały zainstalowane pulpity mikronowe) zawiadomić pozostały personel o zaistniałej sytuacji. Taka funkcjonalność systemu może przyspieszyć podjęcie działań przez ochronę obiektu w zakresie stłumienia lub ograniczenia zagrożenia lub w sytuacji kryzysowej związanej z niedostępnością do urządzeń obsługi DSO zarządzać ewakuacją obiektu.
Pracownicy ochrony obiektu, a zwłaszcza osoby przebywające w pomieszczeniach obsługi urządzeń ppoż. (POUP) powinny być odpowiednio przeszkolone w zakresie obsługi systemów, które im powierzono. Bardzo ważnym czynnikiem jest również klarowność przekazywanych przez te systemy informacji o zaistniałych zdarzeniach w obiekcie, co pozwoli na szybszą i trafniejszą decyzję dotyczącą reakcji i przebiegu zdarzeń. Jak wiadomo, w każdym obiekcie wyposażonym w systemy sygnalizacji pożarowej, systemy detekcji gazów, wentylacji pożarowej, kontroli dostępu, telewizji dozorowej itp. – aby te systemy mogły wesprzeć akcję ewakuacji z zagrożonej strefy – musi być przygotowany odpowiedni scenariusz postępowania na wypadek zagrożenia pożarowego, a wraz z nim matryca sterowań. Niestety nie zawsze jest tak kolorowo, w rzeczywistości zdarza się, że te scenariusze lub matryce są przygotowane na końcu etapu budowy i dostosowywane (lub nie) do już zainstalowanego wyposażenia.
W efekcie może się to wiązać z koniecznością modernizacji lub co gorsza rozbudowy dopiero co zainstalowanych (zgodnie z projektem) ww. systemów w obiekcie. W przypadku rozwiązań Schrack Seconet nie stanowi to technicznego problemu chociażby ze względu na pełną elastyczność oferowanych rozwiązań w zakresie kompleksowego bezpieczeństwa pożarowego (tj. SSP, DSO, systemy sterowania, zasilania i system integrujący urządzenia przeciwpożarowe SIUP), aczkolwiek sam fakt takiego stanu może niepotrzebnie spowodować spore zamieszanie wśród osób odpowiadających za wykonanie instalacji i dotrzymanie terminów realizacji oraz wpłynąć na wzrost kosztów wdrożenia.
Aby zapewnić jak najwyższy poziom bezpieczeństwa, coraz częściej stosuje się systemy integrujące, które służą do kompleksowego zarządzania urządzeniami ppoż. i innymi systemami mającymi wpływ na bezpieczeństwo pożarowe obiektu. W szczególności SIUP odgrywa kluczową rolę w zakresie zarządzania ewakuacją osób z obiektu, dlatego ważna jest ścisła współpraca oferowanego przez Schrack Seconet Polska SIUP SIS-FIRE z systemem sygnalizacji pożarowej i sterowania urządzeniami ppoż. Integral EvoxX oraz DSO APS®--APROSYS. Najwięcej funkcji i wartości dodanych w zakresie bezpieczeństwa i komfortu uzyskujemy w momencie wdrożenia pełnej dwukierunkowej komunikacji cyfrowej między tymi systemami.
W przypadku DSO APS®-APROSYS istnieje możliwość dodatkowego zaprogramowania pulpitów mikrofonowych w celu precyzyjnego przekazania informacji np. o źródle inicjacji alarmu/aktywacji (SSP lub SIUP) i typie rozgłaszanego komunikatu. W razie wystąpienia zagrożenia i aktywacji DSO operator może szybko ustalić, co było źródłem aktywacji.
Selektywnie i dowolnie programowalne przyciski z kolorowymi wskaźnikami LED, znajdujące się w pulpitach serii APS-3xx.2-xAL-EV, po odpowiednim zaprogramowaniu mogą dać pełny obraz sytuacji. W momencie aktywacji DSO na pulpicie podświetlą się przyciski, które będą odpowiednio opisane – np. „Aktywacja z SSP" lub „Aktywacja z SIS-FIRE" i zaprogramowane (np. możliwość wyboru różnych kolorów podświetlania LED przycisków w zależności od źródła inicjacji – SSP, SIUP), jak to przedstawiono na kolejnych przykładach.
W pierwszym wariancie *(rys. 4)* po zatwierdzeniu alarmu pożarowego II stopnia następuje aktywacja DSO i rozpoczyna się ewakuacja jednoetapowa.

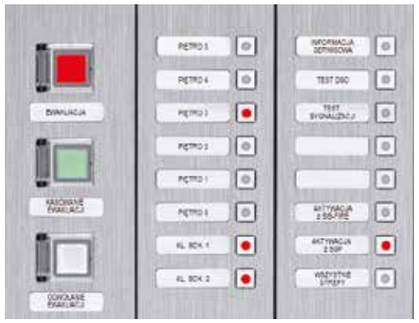
Rys. 4. Aktywacja DSO z poziomu SSP – ewakuacja jednoetapowa

W drugim przypadku *(rys. 5)* DSO został aktywowany z poziomu certyfikowanego systemu SIS-FIRE (SIUP) i również nastąpiła ewakuacja jednoetapowa.



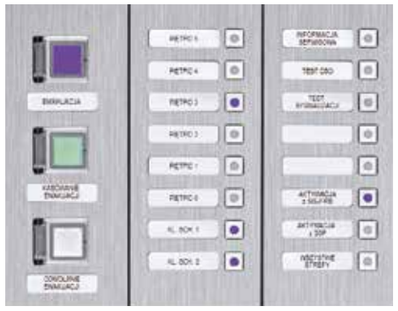
Rys. 5. Aktywacja DSO z poziomu SIS-FIRE(SIUP)
– ewakuacja jednoetapowa

Kolejnym przykładem może być sytuacja, gdy ewakuacja jest prowadzona wieloetapowo *(rys. 6)*. Wówczas po odpowiednim zaprogramowaniu w momencie rozpoczęcia ewakuacji (zgodnie z matrycą sterowań) na pulpicie zostaną podświetlone wskaźniki LED jedynie na tych przyciskach (strefach), do których jest nadawany komunikat ewakuacyjny, z jednoczesnym podaniem źródła inicjacji DSO – w tym przypadku SSP.



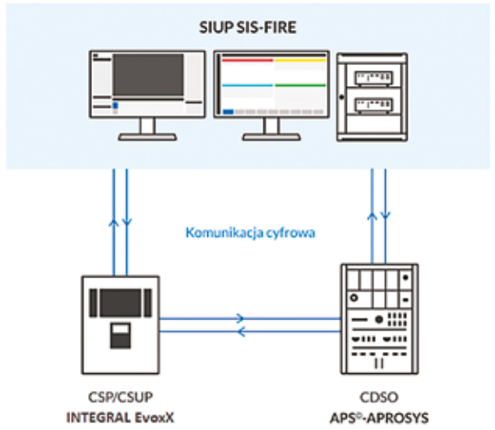
Rys. 6. Aktywacja DSO z poziomu SSP
– ewakuacja wieloetapowa

Analogicznie w przypadku tożsamej sytuacji (jak na rys. 6), ale inicjacji DSO z poziomu SIS-FIRE (SIUP) – na pulpicie mikrofonowym nastąpi odpowiednia aktywacja i zmiana koloru podświetlania przycisków. Dzięki temu operator będzie mógł szybko zorientować się, który z systemów rozpoczął proces ewakuacji osób, gdyby aktywacja DSO nastąpiła podczas jego nieobecności w pomieszczeniu POUP, gdzie został zlokalizowany pulpit mikrofonowy.



Rys. 7. Aktywacja DSO z poziomu SIS-FIRE (SIUP)
– ewakuacja wieloetapowa

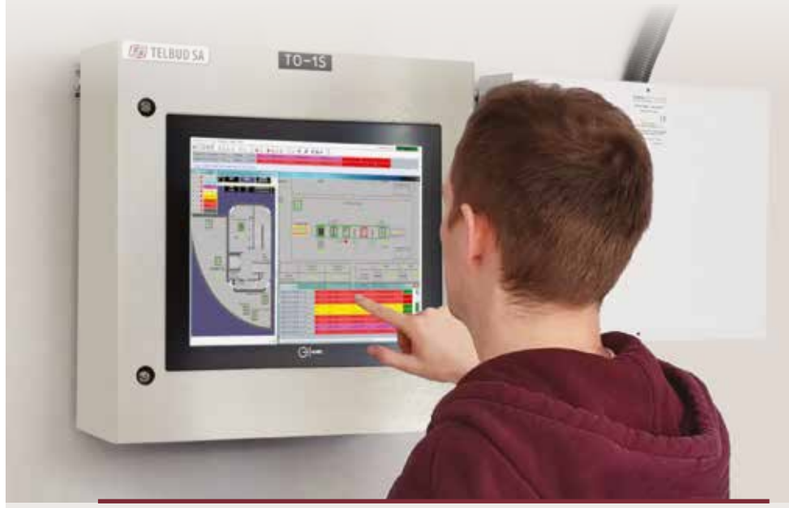
Dzięki możliwości integracji DSO z SIUP dostajemy możliwość nadrzędnego sterowania CDSO z poziomu tego drugiego. System APS®-APROSYS skomunikowany cyfrowo z SIS-FIRE *(rys. 8)* pozwala operatorowi na przerwanie scenariusza automatycznego i uruchomienie rozgłaszania komunikatów głosowych w trybie ręcznym do grupy lub wybranych stref nagłośnieniowych. Dodatkowo SIS-FIRE szczegółowo monitoruje stany działania DSO np. w zakresie zasilania podstawowego, rezerwowego czy połączenia CDSO z pulpitami mikrofonowymi, łącznie z monitorowaniem usterek poszczególnych linii głośnikowych poprowadzonych w obiekcie.



Rys. 8. Schemat integracji systemów SIUP, SSP, DSO

Ze względu na przeznaczenie i wielkość obiektów, do których dostarczana jest technologia oferowana przez Schrack Seconet Polska, to rozwiązanie jest bardzo często stosowane przez partnerów firmy i cenione zarówno przez inwestorów, jak i użytkowników końcowych.
Szczegółowe informacje dotyczące systemu APS®-APROSYS i jego możliwości można uzyskać bezpośrednio na stronie internetowej Schrack Seconet Polska oraz podczas organizowanych cyklicznie szkoleń dla projektantów Dźwiękowych Systemów Ostrzegawczych.

Terminal operatorski jako element podtrzymania obsługi SIUP



Do obsługi operatorskiej systemów integrujących urządzenia przeciwpożarowe (SIUP) stosowane są standardowo stacje robocze PC, które pracują z oprogramowaniem klienckim SIUP instalowanym na stacji lub dostępnym poprzez przeglądarkę web. Nie należą one jednak do wyrobów budowlanych w rozumieniu Rozporządzenia Parlamentu Europejskiego i Rady UE nr 305/2011 z 9 marca 2011 r., w związku z czym nie podlegają certyfikacji w ramach SIUP i nie są ujęte w świadectwie dopuszczenia CNBOP-PIB. Tym niemniej stacje robocze są integralną częścią systemu, bez których jego obsługa byłaby niemożliwa.

Brak jednoznacznych wymagań dla stacji roboczych wywołuje szereg pytań dotyczących zapewnienia odpowiedniej niezawodności sprzętu i zasilania. Jest to szczególnie istotne w przypadku stacji roboczej podstawowego stanowiska operatorskiego SIUP, które zwykle jest zlokalizowane w pomieszczeniu obsługi urządzeń przeciwpożarowych (POUP) obiektu budowlanego.
Wydaje się, że jako podstawowe urządzenie obsługi stacja ta powinna mieć taką samą niezawodność jak pozostałe elementy SIUP, w tym serwer. Jak jednak zweryfikować tę niezawodność, skoro urządzenie nie przeszło badań i kontroli w zakresie systemu oceny zgodności, a zasilanie z sieci 230 V/50 Hz jest podtrzymywane przez UPS, który nie jest zasilaczem pożarowym?
Można oczywiście wykorzystywać markowe stacje robocze znanych producentów przeznaczone (wraz z monitorami ekranowymi) do pracy 24/7 oraz wysokiej jakości zasilacze UPS podtrzymujące napięcie zasilania przez taki sam czas, jaki wymagany jest do działania SIUP w konkretnej instalacji (wg Krajowej Oceny Technicznej minimalny czas to 30 minut), albo stosować dwie redundantne stacje robocze, jednak z formalnego punktu widzenia nie rozwiązuje to problemu.

TERMINALE OPERATORSKIE OBJĘTE ŚWIADECTWEM DOPUSZCZENIA CNBOP-PIB

W tej sytuacji mogą być pomocne terminale operatorskie, które są certyfikowanymi elementami SIUP o architekturze rozproszonej, ujętymi w świadectwie dopuszczenia wyrobu. Zastosowanie takiego terminala w POUP jako niezależnego stanowiska obsługi urządzeń ppoż. o podwyższonej niezawodności gwarantuje, że w razie awarii stacji operatorskiej zostanie utrzymana możliwość nadzoru i sterowania tymi urządzeniami.

TERMINAL TO-1S – ELEMENT SYSTEMU INTEGRUJĄCEGO ARGUS RV-C

W skład komputerowego systemu integrującego ARGUS RV-C wchodzi terminal operatorski TO-1S w oddzielnej zabudowie. Jego podstawowym elementem jest przemysłowy komputer panelowy z dotykowym monitorem LCD o przekątnej 15”, 17” lub 19”. Na komputerze zainstalowane jest standardowo oprogramowanie klienckie serwera systemu.
W zabudowie terminala znajduje się ponadto zarządzalny przełącznik sieciowy, który ma 3 lub 5 portów RJ45 i 2 porty optyczne umożliwiające połączenie z serwerem poprzez ring światłowodowy. Urządzenia są zasilane napięciem 24 VDC z wewnętrznego pożarowego zasilacza buforowego z baterią akumulatorów, która zapewnia podtrzymanie zasilania przez czas do 2 h po zaniku napięcia sieci 230 V/50 Hz. Czas ten można zwiększyć nawet do 4 h, stosując zasilacz o zwiększonej mocy i baterii akumulatorów o większej pojemności.
Terminal zapewnia pełną wizualizację z możliwością sterowania zintegrowanymi urządzeniami ppoż. niezależnie od stacji roboczych obsługi operatorskiej. Wolne porty RJ45 przełącznika sieciowego pozwalają na podłączanie do nich integrowanych urządzeń.
Dodatkową zaletą terminala jest możliwość równoczesnego zainstalowania na nim oprogramowania serwera. W takiej konfiguracji terminal może pełnić funkcję redundantną w stosunku do podstawowego serwera ARGUS RV-C, względnie może pracować jako niezależny serwer.

Przegląd Techniczny Bezpieczeństwa

Inspiracją do napisania artykułu były dwie kwestie. Po pierwsze duża ilość przejeżdżanych kilometrów w celach służbowych spowodowała konieczność zrobienia przeglądu auta. Auto jest flotowe, nowe i azjatyckie, przyzwoite, ale bez ekstrawagancji. Niemniej wymaga przeglądu co 15 tys. km, bo inaczej właściciel będzie miał kłopoty z ubezpieczycielem.

Jacek Tyburek

W przypadku firmowej floty samochodów problem jest większej skali.
Jakże daleko bardziej stałego trzymania ręki na pulsie wymagają przedsiębiorstwa. Zarządzanie bezpieczeństwem przez lata ukształtowało się w nich w typologie i utarte metody działania. Temat tych metod i konieczność rozprawienia się z nimi opisał w swoim świetnym tekście pt. *Echa zmiany paradygmatu w bezpieczeństwie – przykazania współczesnego bezpiecznika* Jan Kapusta. Przesłanie tekstu jest wyraźne: rolą „bezpiecznika" nie jest zapewnienie minimum formalnych wymogów stawianych organizacji przez prawo, rynek, partnerów czy standardy, lecz spowodowanie, aby wyznaczony cel biznesowy został skutecznie doprowadzony do celu.
Dalej można by prowadzić dyskusję na temat ukształtowania standardów pracy pionu lub menedżera bezpieczeństwa. Posiadanie struktur bezpieczeństwa jest oczywistością w międzynarodowych korporacjach, których globalne struktury powielają placówki rozsiane po świecie. Moim celem jest dotarcie nie tyle do ekspertów od bezpieczeństwa, ile do osób z biznesu, które czują, że bezpieczeństwo jest ważne, ale nie są do końca przekonani, że zarządzanie bezpieczeństwem napędzi ich przewagę konkurencyjną.

Wróćmy jednak na rodzimy rynek. W Polsce jest jeszcze dużo przedsiębiorstw, w których niestety nie ma osób zajmujących się bezpieczeństwem. I to niezależnie od wielości firmy, czy to dużych o zasięgu europejskim, a bywa, że globalnym czy niewielkich rodzinnych. Organizacje te działają bardzo pragmatyczne, jednak chcąc być konkurencyjne, powinny zatrudnić doświadczone osoby do zarządza ryzykiem, bezpieczeństwem czy – jak to się ostatnio coraz częściej określa – „dbającym o odporność biznesu".

Jak to się ma do analogii z przeglądem auta? Firma zatrudniająca od kilkuset to kilku tysięcy osób, która wcześniej nie zbudowała własnej polityki bezpieczeństwa, doświadcza wielu mniejszych lub większych strat. Począwszy od prostych kradzieży i dewastacji produktów i majątku, poprzez straty w łańcuchu dostaw, skończywszy na nękających atakach cyberprzestępców. A tych strat można było uniknąć, decyzja zarządu o zatrudnieniu security managera jest jak najbardziej rekomendowana.
Jednak znalezienie odpowiedniej osoby nie jest łatwe, zwłaszcza jeśli w firmie nie ma kultury zarządzania ryzykiem, rozumianym jako ryzyka biznesowe, operacyjne, jeśli nie ma żadnych metod, procedur i świadomości bezpieczeństwa. Oczywiście oczami wyobraźni widzę już dyskusje w zarządzie nt. zasadności zatrudniania security managera (czyli domyślnie szefa ochrony). *Po co nam szef ochrony za takie pieniądze, skoro można od razu zatrudnić cybersecurity managera* (domyślnie szefa IT security, którego zarobki często przewyższają pensję prezesa zarządu).

Takich pułapek jest więcej, ponieważ bezpieczeństwo biznesu bardzo się skomplikowało. Stało się zdecydowanie bardziej technologiczne, cybernetyczne, tymczasem prawdziwe zagrożenia ciągle jednak czają się w świecie fizycznej wartości produktu, świadomości wartości przestoju produkcyjnego czy zapobieganiu manipulacjom pracowników, aby nie wyjawili krytycznych dla biznesu tajemnic lub nie ułatwili kradzież pieniędzy z kont bankowych.

Jakiego więc specjalistę firma powinna zatrudnić? Skąd w ogóle wiadomo, co jest rzeczywistym problemem w organizacji? Rozwiązaniem jest zlecenie przeprowadzenia audytu operacyjnego lub audytu bezpieczeństwa, który zbada prawdziwą kondycję przedsiębiorstwa. Niestety często raporty audytowe szybko stają się typowymi „półkownikami". Po przedstawieniu zarządowi i wywołaniu krótkotrwałego szumu lądują w zasobach informatycznych i czekają na lepsze czasy. Pozostaje tylko wspomnienie wysokiego kosztu takiego raportu.

Dlatego w przypadku organizacji, która nie ma jeszcze wykrystalizowanej wizji, jak i kto ma zarządzać jej odpornością biznesową, warto zebrać wiedzę, która pomoże podjąć dojrzałe decyzje. Dla firmy, która nigdy nie prowadziła świadomej polityki bezpieczeństwa, przeprowadzenie skomplikowanych analiz ryzyka może być zwyczajnie trudne. Często organizacja decyduje się na to dopiero w obliczu poważnego kryzysu, a wtedy może być za późno na zapobieganie stratom. Całkowicie zrozumiały jest też brak zaufania do obcych, nieznanych zarządowi ekspertów. Nie wiadomo, kim są ludzie, przed którymi mamy otworzyć drzwi. Jeśli potencjalnym partnerem nie jest jedna z wielkich rozpoznawalnych firm audytowych, to ograniczone zaufanie do mniejszej firmy jest zrozumiałe. Można oczywiście powierzyć takie zadanie agencji ochrony lub dostawcy rozwiązań technologicznych (kamery CCTV, kontrola dostępu). Problem polega na tym, że firmy technologiczne takich usług raczej nie świadczą. Firma ochrony też powinna być obszarem badania prawidłowości zapewniania bezpieczeństwa „naszej" firmy, więc nie mogą się same badać.

Rozwiązaniem może być skorzystanie z Security Self-Assessment pierwszego stopnia. To formuła komfortowa, ponieważ oprócz samego narzędzia przygotowanego przez wyspecjalizowaną firmę doradczą oferuje szereg zalet z obszaru poufności. To proste narzędzie dostosowane jest do typu działalności, skali, ogólnej wiedzy (popartej zamówioną analizą OSINT lub nie) na temat działalności przedsiębiorstwa. Badanie dotyczy zarówno fizycznych aspektów bezpieczeństwa firmy, jak i bezpiecznej organizacji łańcucha dostaw czy sfery bezpieczeństwa informacji. Narzędzie jest wzbogacone o opis metodologii przeprowadzenia badania i metody analizy uzyskania danych. Firma sama nim nawiguje, pozyskane informacje i wnioski również zostają w organizacji, co zapewnia utrzymanie poufności danych.

Ta dość tania metoda (nie może przecież kosztować dużo) pokazuje zarządowi, jakie są najsłabsze obszary w organizacji. Nie należy jednak zapominać, że najsłabszym, najbardziej wadliwym elementem procesu jest człowiek. Informacje zebrane w ten sposób należy dokładnie zweryfikować. Niemniej jednak, jeśli organizacja nie chce zapraszać do współpracy „obcych", takie narzędzie stanowi bazę do kolejnych kroków.

Uzupełnieniem Self-Assessment pierwszego stopnia jest usługa ewaluacji wyników badania przez niezależnego eksperta. Weryfikacja udzielanych odpowiedzi i zderzenie ich z wiedzą fachowca, który od lat realizuje zadania zapewniania bezpieczeństwa, stanowić będzie dodatkową wartość. Przykładem jest choćby powoływanie się na funkcjonowanie procesu w organizacji oraz sprawdzenie, jak to faktycznie działa, na jakiej podstawie i jak głęboko proces jest w firmie zakorzeniony. Zleceniodawca ma ten komfort, że nie wpuszcza zbyt głęboko osoby spoza organizacji do własnych poufnych biznesowo informacji, ale dzięki przekazanym informacjom zgromadzone dane zyskują wyższą wartość dla zarządu. Nazwijmy taki proces Security Self-Assessment drugiego stopnia.

Budując wiedzę nt. sytuacji firmy, czyli proces faktycznego „przeglądu technicznego bezpieczeństwa organizacji", należałoby zrobić kolejny krok. Jest nim analiza OSINT przygotowana przez niezależną firmę. Biały wywiad, inaczej określany jako OSINT *(Open Source Intelligence)*, to forma legalnego wywiadu gospodarczego oparta na pozyskiwaniu informacji z ogólnodostępnych źródeł, takich jak środki masowego przekazu, social media. OSINT jest od wielu lat z sukcesem wykorzystywany przez agencje wywiadowcze, policję i prywatne firmy specjalizujące się w prowadzeniu wywiadu gospodarczego. W działaniach biznesowych biały wywiad koncentruje się wokół sytuacji prawnej, finansowej, handlowej i ekonomicznej przedsiębiorstwa bądź kontrahenta w celu oszacowania ryzyka współpracy z danym podmiotem. Stosowanie OSINT pozwala pokazać zarządowi, jakie informacje na temat firmy są widoczne i łatwo dostępne. Należy przyjąć optykę potencjalnego partnera biznesowego. Czy dane uzyskane w analizie OSINT mogą zaszkodzić reputacji firmy? Czy mogą potencjalnie utrudnić lub wręcz zaprzepaścić realizację ważnego dla firmy kontraktu? Czasy kryzysu zawsze są okresami prosperity firm zajmujących się badaniem wiarygodności partnerów biznesowych.

Na tym etapie kończą się bezinwazyjne metody badania odporności organizacji. To ten moment, kiedy firma podejmuje decyzje, czy chce dalej budować wiedzę nt. swojej kondycji w sposób samodzielny, czy zaprosi do głębszej współpracy specjalistów. Tutaj kończy się etap prostej wymiany oleju i wymiany klocków hamulcowych…
Dalsze kroki wymagają nabrania większego zaufania i gotowości do otwartej współpracy. Trzymając się terminologii przeglądu technicznego, to etap podłączenia się do komputera naszej bryki. Przegląd znacznie ułatwia ocenę stanu infrastruktury informatycznej firmy, w tym zarządzanie elektronicznymi systemami zabezpieczeń. Ostatnio prasa branżowa szczegółowo opisuje podatności wybranych systemów CCTV na cyberataki. Na podobne ataki są też narażone systemy kontroli dostępu i wszystkie urządzenia podłączone do sieci. Niwelowanie tych podatności wymaga prawidłowej administracji dostępami, utrzymania swoistej higieny systemów. Polskie firmy nie mają takiego doświadczenia jak korporacje zagraniczne i trudniej im włączać do swoich struktur piony bezpieczeństwa biznesu. Jednak dziś niestety nie ma alternatywy i zarządzanie sferą bezpieczeństwa to konieczność.
Pierwszym krokiem jest wiedza o tym, z jakiego rodzaju niebezpieczeństwami i z jaką skalą ataków mamy do czynienia. Duże organizacje tworzą własne narzędzia monitujące, np. SOC *(Security Operations Center)* i SIEM *(Security Information and Event Management).* SOC to miejsce, w którym dzięki synergii wielu rozwiązań oraz wymianie informacji pomiędzy nimi można osiągnąć wyższy poziom bezpieczeństwa.
Infrastruktura IT w dzisiejszych organizacjach jest skomplikowana. Stosujemy wiele urządzeń sieciowych, nierzadko pochodzących od różnych producentów – serwery, macierze, komputery PC i laptopy, tablety czy też urządzenia mobilne, np. smartfony. Każde z nich generuje tysiące informacji, których analiza bez specjalistycznych narzędzi jest praktycznie niemożliwa. SIEM będzie jednym z kluczowych rozwiązań do pozyskiwania informacji i monitorowania urządzeń. SOC jeszcze ciągle są rzadkością – to drogie struktury, których wartość jest kształtowana dość rozbudowaną mozaiką specjalizacji i wysoko wycenianej pracy specjalistów od cyberbezpieczeństwa. Na szczęście usługi te można kupić, co jest bardziej korzystne finansowo niż tworzenie własnych SOC.
Z perspektywy firmy, która nigdy nie prowadziła pogłębionej analizy ataków, uzasadnione jest okresowe włączenie skanowania ataków i podatności na włamania. Nawet jeśli organizacja nie jest jeszcze gotowa na stałe monitorowanie i uruchomienie narzędzi obronnych, okresowe badanie w ramach „przeglądu technicznego" będzie budowało obraz rzeczywistości i lepiej przygotuje Zarząd na inwestycje w obszar bezpieczeństwa.
Wynajęcie zewnętrznego SOC wraz z narzędziami SIEM stanowi już znaczące zaproszenie podmiotu zewnętrznego do własnej infrastruktury i jako takie musi być przemyślane. Jednak dziś nie jest możliwe prowadzenie działalności biznesowej w swoistej samowystarczalności operacyjnej. Nawet usługi firmy sprzątającej czy firmy ochrony narażają na ryzyko w sytuacji, gdyby któryś z pracowników tych firm okazał się nielojalny. Tak więc korzystanie z usług wyspecjalizowanych usług stałych czy „warsztatów przeglądów technicznych" jest koniecznością.

PROPONOWANY PRZEZE MNIE PRZEPIS NA OKRESOWY PRZEGLĄD TECHNICZNY BEZPIECZEŃSTWA POWINIEN SKŁADAĆ SIĘ Z NASTĘPUJĄCEGO MENU:

1. Procedura przeprowadzenia Self-Assessment przez firmę. Biorąc pod uwagę skłonność do budowania zaufania, proponuję rozpocząć od wersji całkowicie samodzielnej. W kolejnych krokach sugeruję udział konsultanta w interpretacji wyników oraz zaproponowaniu narzędzi korygujących sytuację.
2. Przeprowadzenie badania obrazu firmy w otoczeniu informacyjnym poprzez OSINT oraz/lub analizę reputacji firmy. Sugeruję również przeprowadzenie OSINT dla kluczowych partnerów biznesowych „naszej firmy".
3. Zbadanie skali ataków cyberprzestępców, na jakie firma jest narażona. Wdrożenie badania SOC dla określonej liczby maszyn (end pointów) w organizacjach.

Pozostaje pytanie o częstotliwość takich przeglądów. W przypadku systemów zabezpieczeń technicznych, takich jak CCTV czy kontrola dostępu, bardzo często rekomenduje się przeglądy i konserwacje co 6 miesięcy. Kurz i bród osadzający się na kamerach czy innych czujnikach jest oczywiście niebezpieczny dla prawidłowego działania systemu. Bardziej niebezpieczne są widoczne i niewidoczne ataki na firmę. W związku z tym przeglądy kwartalne wydają się racjonalne.
Wdrożenie takiej procedury pozwoli zbudować bazę danych zdarzeń, które pojawiają się wokół firmy, oraz przygotować się na stworzenie odporności przeciwko niekorzystnym incydentom. Doświadczenie obecnych lub przyszłych partnerów z obszaru bezpieczeństwa i odporności również będzie stanowić skuteczniejsze wsparcie w zabezpieczeniu firmy. Nawet gdy organizacja nie zdecydowała się na zatrudnienia Security Managera w pełnym zakresie, to posiadanie narastającej w wyniku „przeglądów technicznych bezpieczeństwa" bazy danych stanowi nieocenioną wartość.
Kwestia zatrudniania security managera na pełen etat w czasie zmiany paradygmatu, o którym w artykule pisze Jan Kapusta, jest decyzją wymagającą przemyślenia. Jakiego security managera organizacja potrzebuje, z jakimi kompetencjami, do jakich zadań – czy bardziej osobę do operacji, czy ds. cybersecurity lub doradcę zarządu do „szeroko rozumianego bezpieczeństwa"? Ale to już temat na osobny tekst. Z pewnością rozwiązaniem może być skorzystanie z usług Interim Security Managera, z opcją usług na abonament uszyty na miarę i potrzeby. Rynek jest bogaty, można i należy korzystać z jego zasobów.

JACEK TYBUREK

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

System Zarządzania Ciągłością Działania (BCMS)

Część 6. Kolejne kroki – Etap 2 (BCP i DRP)

Zarządzający przedsiębiorstwem muszą dbać o rozwój firmy. Zabezpieczenie nieprzerwanego jej funkcjonowania zapewnia system zarządzania ciągłością działania. W kolejnych częściach cyklu prezentuję poszczególne etapy wdrażania tego systemu. Po analizie ryzyka przyszła pora na kolejny krok – opracowanie planów BCP *(Business Continuity Plan)* i DRP *(Disaster Recovery Plan).*

Tomasz Guzikowski

Celem tego kroku jest opracowanie planów BCP i DRP zapewniających skuteczny sposób pracy w sytuacji zagrożenia ciągłości działania organizacji. Żeby go zrealizować, należy przeprowadzić kilka poniższych działań.

OPRACOWANIE PLANÓW CIĄGŁOŚCI DZIAŁANIA (BCP) KLUCZOWYCH PROCESÓW BIZNESOWYCH

Na tym etapie następuje:

- Opracowanie planów zapewnienia ciągłości działania zawierających listę kroków niezbędnych do wykonania w celu realizacji poszczególnych procesów w przyjętych ramach czasowych w przypadku materializacji ryzyka.
- Opracowanie zakresu planu ciągłości działania podsumowującego informacje o procesie i zasobach wspierających.
- Opracowanie struktury odpowiedzialności (struktury zarządczej) za realizację i utrzymanie planu, ze wskazaniem kluczowych ról, uprawnień i odpowiedzialności dla osób i zespołów, które będą korzystać z planu; wytyczne i kryteria dotyczące tego, kto ma prawo odwołać się do planu i w jakich okolicznościach.
- Opracowanie kryteriów uruchomienia danego planu na podstawie listy kluczowych zagrożeń.
- Udokumentowanie informacji o kluczowych parametrach odtworzeniowych, w tym:
  - *Maximum Tolerable Downtime* (MTD) – wskaźnik określający maksymalny dopuszczalny przestój krytycznego procesu biznesowego, który nie wywoła żadnych negatywnych konsekwencji dla biznesu; można mierzyć go w godzinach lub dniach. Jego ustalenie jest sprawą priorytetową w kontekście wszystkich dalszych prac projektowych;
  - *Recovery Point Objective* (RPO) – wskaźnik określa, jak szybko infrastruktura IT jest przywrócona do pracy po wystąpieniu awarii lub innego incydentu;
  - *Recovery Time Objective* (RTO) – wskaźnik określa dopuszczalną ilość utraconych danych i maksymalny akceptowalny czas pomiędzy wystąpieniem awarii a backupem danych;
  - wymagania dla poszczególnych zasobów wspierających.
- Opracowanie diagramu przepływu informacji oraz wymagań dotyczących dokumentacji działań wynikających z planu ciągłości działania.
- Informacje pomocnicze dla koordynacji i komunikacji – dane kontaktowe członków zespołu i innych osób pełniących funkcje i obowiązki.
- Kryteria wycofania się – mechanizmy wycofywania się po zakończeniu zdarzenia.

OPRACOWANIE PLANÓW ODTWORZENIOWYCH DRP

Tworzy się je dla zasobów, dla których na skutek poważnego zakłócenia (katastrofy) nie jest możliwe przywrócenie normalnej działalności w podstawowej lokalizacji (w sytuacjach, w których odtworzenie w lokalizacji zapasowej jest możliwe).

Na tym etapie następuje:

- Opracowanie kryteriów uruchomienia danego planu związanych z wystąpieniem katastrofy skutkującej brakiem fizycznego dostępu do zasobów w lokalizacji podstawowej oraz koniecznością przywrócenia ciągłości działania procesu z wykorzystaniem lokalizacji zapasowej.
- Udokumentowanie informacji o kluczowych parametrach odtworzeniowych (MTD, RPO, RTO) oraz wymaganiach dla poszczególnych zasobów wspierających.
- Uzupełnienie planów odtworzeniowych o działania konieczne ze względu na wykorzystanie lokalizacji zapasowej.
- Opracowanie diagramu przepływu informacji oraz wymagań dotyczących dokumentacji działań wynikających z planu DRP.
- Informacje pomocnicze dla koordynacji i komunikacji – dane kontaktowe członków zespołu i innych osób pełniących funkcje i obowiązki.

Procedury odzyskiwania powinny obejmować również wznowienie wszystkich działań, a nie tylko określonych jako priorytetowe. Uznaje się, że działania o niższym priorytecie muszą być wznowione w pewnym momencie i również mają wymagania dotyczące zasobów, które muszą być spełnione.

PROCEDURY KOMUNIKACYJNE

Nie mniej ważne są procedury dotyczące komunikacji w sytuacjach kryzysowych. Komunikacja, która będzie dostarczana i odbierana podczas incydentu czy kryzysu, powinna być zarządzana i koordynowana. Procedury powinny zawierać:

- szczegóły dotyczące tego, w jaki sposób i w jakich okolicznościach organizacja będzie komunikować się z pracownikami i ich bliskimi oraz innymi zainteresowanymi stronami,
- szczegóły dotyczące reakcji medialnej organizacji w następstwie incydentu lub kryzysu, które obejmują:
  - strategię komunikacji w następstwie incydentu;
  - preferowany interfejs z mediami;
  - wytyczne lub szablony do sporządzenia oświadczenia dla mediów;
  - kompetentnych rzeczników upoważnionych do przekazywania informacji mediom.

Ważne, aby czas i treści komunikacji wewnętrznej i zewnętrznej były spójne. Komunikacja wewnętrzna jest priorytetem, aby zbudować pewność siebie i zaufanie. Przygotowane wcześniej informacje mogą być szczególnie przydatne we wczesnych fazach incydentu. Umożliwią one zespołowi przekazanie szczegółów dotyczących organizacji i jej działalności biznesowej, podczas gdy szczegóły incydentu są jeszcze ustalane.

EWAKUACJA

W każdej organizacji priorytetem powinno być jednak bezpieczeństwo ludzi. Szczególnie w sytuacji bezpośredniego zagrożenia życia i zdrowia zarówno pracowników, jak i wykonawców, klientów i gości. Planując odpowiednie działania w tym zakresie, należy uwzględnić co najmniej takie elementy, jak:

- zapewnienie sprawnej ewakuacji, w tym wyznaczenie i oznaczenie dróg ewakuacji oraz punktów zbiórki – najczęściej takie informacje znajdują się w Instrukcji Bezpieczeństwa Pożarowego,
- zapewnienie udzielenia pierwszej pomocy zarówno przez wyspecjalizowane służby ratownicze, jak i odpowiednio przeszkolonych pracowników,
- lokalizowanie i przeliczenie osób, które znajdowały się na miejscu zdarzenia – najczęściej poprzez wyznaczonych koordynatorów ewakuacji, którzy przekazują stosowne informacje odpowiednim służbom ratowniczym.

Dalsze kroki przedstawię w kolejnych częściach artykułach z tego cyklu.

TOMASZ GUZIKOWSKI

Menedżer z wieloletnim doświadczeniem w obszarze zarządzania bezpieczeństwem i ciągłością działania, w tym bezpieczeństwa procesowego i zawodowego, ochrony infrastruktury krytycznej, ochrony informacji niejawnych w budownictwie i dużych zakładach produkcyjnych należących do grupy zakładów dużego ryzyka powstania awarii przemysłowej. Obecnie zarządza obszarem bezpieczeństwa w globalnym koncernie chemicznym CIECH.

Bezpieczeństwo i czystość zdrożeją!

Wzrost stawki minimalnej zapowiadany przez rząd spowoduje znaczne podwyżki kosztów usług ochrony i sprzątania. Czy w związku z tym w 2023 r. pracę straci 35 tys. pracowników? Czy szpitale, urzędy, muzea, ZUS-y, sądy, prokuratury, ministerstwa i jednostki wojskowe zostaną bez ochrony? – Na pewno będzie drożej – ostrzega Polski Związek Pracodawców Ochrona zrzeszający największe firmy z branży.

Choć podwyżka minimalnej stawki wynagrodzenia (właściwie będą to dwie podwyżki: pierwsza od stycznia, druga od lipca 2023 r.) może wydawać się dobrą wiadomością dla pracowników, to jej skutkiem będą zmiany, które mogą pogorszyć sytuację wielu pracowników branży ochrony i sprzątającej.

– To niepotrzebna w obecnej sytuacji rynku pracy ingerencja państwa, która uderzy zarówno w prowadzących firmy usługowe, jak i w klientów oraz instytucje publiczne korzystające z usług agencji ochrony i firm sprzątających – mówi Tomasz Wojak, prezes Zarządu Polskiego Związku Pracodawców Ochrona (PZP Ochrona).

Dlatego Związek i firmy w nim zrzeszone uruchamiają kampanię informacyjną, która ma na celu uświadomienie zainteresowanym stronom, zarówno klientom, jak i przedsiębiorcom z branży, jak poważne skutki dla rynku będzie miała ta regulacja.

– W następstwie podwyżek firmy zrzeszone w PZP Ochrona już rozpoczynają proces renegocjacji stawek, by zwaloryzować kontrakty – zauważa Kinga Korzybska, sekretarz generalny PZP Ochrona.

Wpływ zmiany stawek na branżę będzie ogromny. Rynek wart jest 11 mld zł, z czego spory odsetek stanowią zamówienia z sektora finansów publicznych.

– Jednostki budżetowe korzystające z usług ochrony stanowią istotną część rynku. Wojsko wydaje na ochronę ponad 500 mln zł rocznie, a rynek cywilny jest kilka razy większy. W sumie w grę może wchodzić kilka miliardów złotych – podsumowuje Tomasz Wojak.

Dwukrotna w ciągu roku waloryzacja może stanowić poważny problem z zaplanowaniem budżetów wydawanych na zakup tych usług. Będą się zdarzać przypadki konieczności ogłoszenia nowego przetargu, a kwoty zaplanowane na ten cel okażą się niewystarczające, by opłacić drożejące usługi.
Wiele instytucji publicznych, a także firmy działające w obszarze infrastruktury krytycznej, znajdujące się na liście wojewodów, która kwalifikuje je do obiektów obowiązkowej ochrony, jest zobligowanych do kupowania usług ochrony świadczonych przez kwalifikowanych pracowników ochrony, często pracujących z bronią. A ponieważ brakuje ich na rynku pracy, zarobki tych pracowników też idą w górę.

Podwyżek mogą spodziewać się również mieszkańcy osiedli mieszkaniowych, których wspólnoty zatrudniają pracowników ochrony. Ochrona, sprzątanie już dziś stanowią znaczącą pozycję w czynszu obok kosztów ogrzewania, gazu i prądu. Teraz ich cena wzrośnie o co najmniej kilkanaście procent.

> *Przy rosnących kosztach pracy i towarów firmy muszą podnosić ceny. Jeśli usługobiorcy nie są w stanie tych podwyżek zaakceptować, to agencje przestają inwestować, zaczynają oszczędzać. Wzrasta wtedy ryzyko, szczególnie w branżach usługowych, że część biznesów zacznie działać w szarej strefie – komentuje Tomasz Wojak*

Usługi ochrony i sprzątania kupują także sieci handlowe i zakłady produkcyjne, można więc zakładać, że ostatecznie waloryzacja wpłynie na ceny produkowanych i sprzedawanych w nich dóbr.

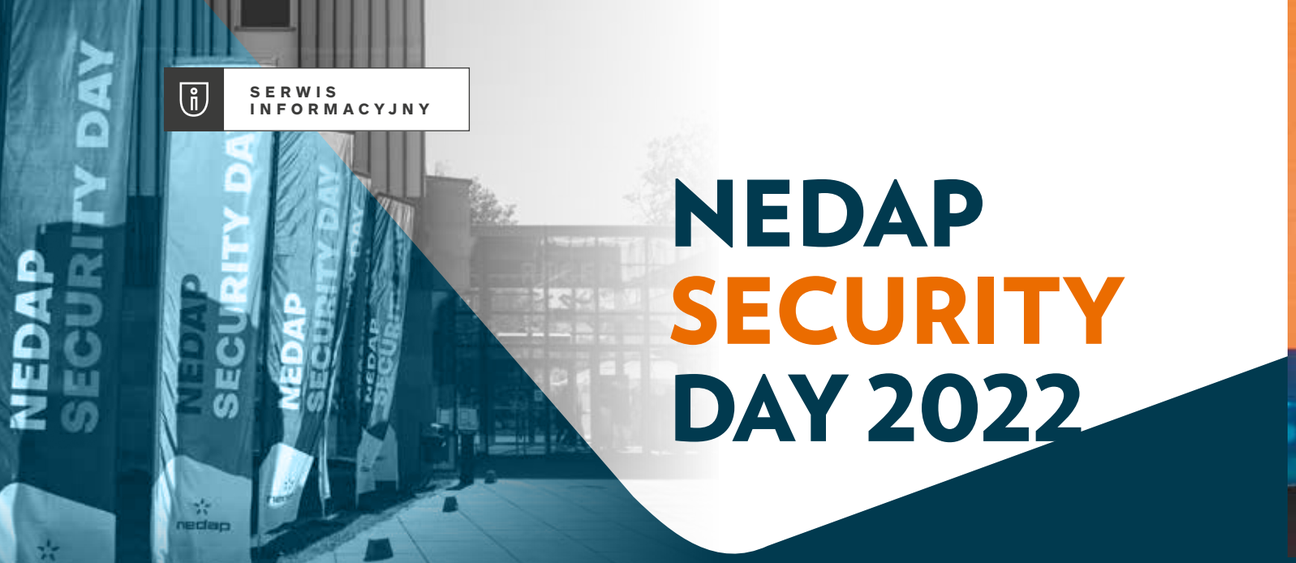
– Przy rosnących kosztach pracy i towarów firmy muszą podnosić ceny. Jeśli usługobiorcy nie są w stanie tych podwyżek zaakceptować, to agencje przestają inwestować, zaczynają oszczędzać. Wzrasta wtedy ryzyko, szczególnie w branżach usługowych, że część biznesów zacznie działać w szarej strefie – komentuje Tomasz Wojak.

Według szacunków polska branża ochrony zatrudnia dziś 250 tys. osób (podobnie blisko z nią związana branża utrzymania czystości). Jej specyfiką jest to, że większość kosztów stanowią koszty pracy fizycznej. Jedną z konsekwencji zbilansowania wzrostu stawki minimalnej może się okazać konieczność zwolnienia blisko 14% pracowników, czyli ok. 35 tys. osób. Ich miejsce stopniowo będzie zapełniała technologia.

– Koszty instalacji systemów zabezpieczenia technicznego są coraz niższe. Myślę, że wielu naszych klientów, którzy zastanawiali się nad tym rozwiązaniem, teraz się na nie zdecyduje – twierdzi Jarosław Kot, prezes regionu dolnośląskiego i członek Zarządu PZP Ochrona. – Ponadto nasi klienci na coraz większą skalę wykorzystują inteligentne systemy bezpieczeństwa do wspierania procesów sprzedażowych. Systemy te mogą np. na bieżąco informować o liczbie klientów w sklepie czy wysyłać spersonalizowane reklamy w zależności od preferencji zakupowych klienta.

Dodaje jednak, że technologia jest skuteczna jedynie w połączeniu z człowiekiem. Pracownicy ochrony zajmują się dziś nie tylko ochroną przed kradzieżą. Bardzo często ratują życie w nagłych wypadkach czy też zdarzeniach losowych, które przydarzają się klientom sklepów czy urzędów. O tym bardzo często zapominamy, a technologia jeszcze tego nie potrafi.

POLSKI ZWIĄZEK PRACODAWCÓW OCHRONA
ul. Koszykowa 61, 00-667 Warszawa
biuro@pzpochrona.pl
www.pzpochrona.pl



NEDAP SECURITY DAY 2022

Na początku września kilkadziesiąt osób spotkało się na zaproszenie Nedap Security Management w Folwarku Łochów. Zgromadzeni uczestnicy dyskutowali m.in. o przyszłości rynku security oraz pracy zdalnej, która ujawniła nowe wyzwania w zakresie cyberbezpieczeństwa. Spotkanie otworzyła prelekcja Piotra Koniecznego z Niebezpiecznik.pl pt. „Wszystko można zhakować". Obok Nedap Security Management swoje rozwiązania zaprezentowali również partnerzy technologiczni: Signal Os, STid i Hikvision.

Anna Twardowska

Nedap Security Management

Nedap Security Day jest okazją do spotkań z klientami, instalatorami, jak również partnerami technologicznymi. Bardzo się cieszymy, że mogliśmy gościć tak dużą liczbę osób. Podczas pandemii mieliśmy przerwę w tego typu kontaktach, tym bardziej doceniamy dzisiejsze wydarzenie. Motywacją do jego zorganizowania była potrzeba stworzenia miejsca do wymiany informacji z naszymi obecnymi i potencjalnymi klientami oraz integratorami systemów. Uczestnicy na żywo mogli zobaczyć, jak nasz system AEOS działa w integracji z aplikacjami innych producentów. To klientom znacznie poszerza perspektywę możliwości wyboru poszczególnych rozwiązań.

Grzegorz Kosik

Nedap Security Management

Na spotkaniu dużo mówiło się o ewolucji, ale ja podkreślę inny aspekt. Zarówno nasi partnerzy, jak i klienci zwracają uwagę na wiarygodność dostarczanych usług. I to jest absolutnie kluczowe nie tylko w naszej branży, ale w biznesie w ogóle.

Piotr Karpiński

STid

Uważam, że najważniejsze obecnie – co pokazało też dzisiejsze spotkanie – jest podnoszenie świadomości klientów na temat stosowania bezpiecznych kart. Bezpieczeństwo w kontroli dostępu zaczyna się tam, gdzie zaczyna się „podróż" karty. Jest to jedyny element systemu, który migruje poza obiekt. Karta jest narażona na klonowanie, hakowanie, na wszelkiego rodzaju ataki, próby podrobienia czy przerobienia nadanych wcześniej uprawnień.

Karol Radzajewski

Hikvision Poland

Cieszymy się, że mogliśmy uczestniczyć w tym wydarzeniu. Jest to także owoc wieloletniej współpracy między naszymi firmami. Dzisiejsze prelekcje były bardzo ciekawe – chociażby Piotra Koniecznego z Niebezpiecznika.pl. Pokazały, na jak wiele zagrożeń jesteśmy narażeni.
Nedap Security Day to również okazja do spotkania się po pandemicznej przerwie z naszymi obecnymi klientami oraz tymi potencjalnymi. Na stoisku mieliśmy możliwość porozmawiania *face to face* o naszych rozwiązaniach i oczekiwaniach co do przyszłości. To bardzo wartościowe wydarzenie, które zaowocowało wymianą doświadczeń i kontaktów.

Tomasz Felczyk

Signal OS

Z naszej perspektywy najważniejszą korzyścią dla uczestników spotkania było poznanie technologii związanych z zarządzaniem systemami budynkowymi, z ułatwieniem dostępu do nich czy też wymiana doświadczeń z korzystania z obiektu przez użytkowników końcowych. To są ciągle nowe technologie, które się rozwijają, potrzebują jeszcze trochę czasu na uzyskanie pełnej funkcjonalności. Ale chcąc być na bieżąco, trzeba już dziś zacząć się nimi interesować, powoli je wdrażać.

Grzegorz Kruszewski

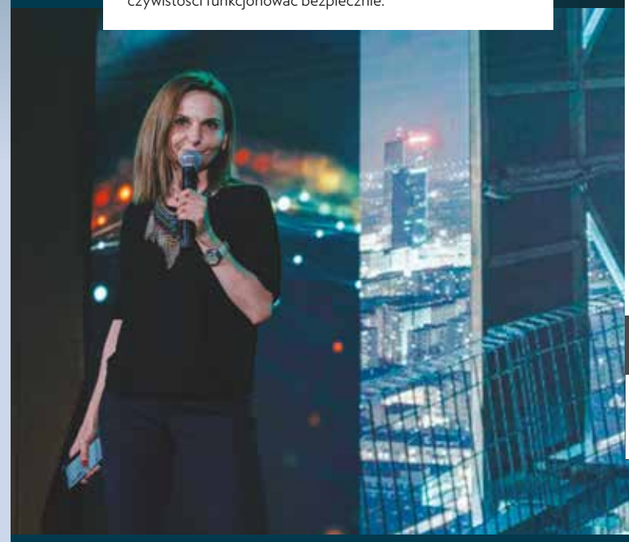
Polpharma

Pandemia pokazała nam – na co również zwracali uwagę przedstawiciele Nedap i pozostali prelegenci – że musimy bardziej dostosować się do wymogów dnia codziennego zwłaszcza w zakresie cyberbezpieczeństwa. Hakerzy mieli dużo czasu, żeby opracować systemy wykradania danych, włamywania się do zasobów, które powinny być skutecznie chronione. To dzisiaj stanowi ogromne wyzwanie. Zyskaliśmy nowe technologie, ale korzystamy z nich nie tylko my z branży security. Są dostępne dla wszystkich i jak wskazał Piotr Konieczny w pierwszym wystąpieniu, zabezpieczenia sfery cyber należy potraktować bardzo poważnie.

Piotr Sitko

Polska Wytwórnia Papierów Wartościowych

Takie spotkania są potrzebne. Po pierwsze spotykają się specjaliści branży zabezpieczeń technicznych. Po drugie jest możliwość zapoznania się z nowymi trendami w ochronie i nowymi rozwiązaniami. To jest bardzo ważne. Każdy budynek czy obiekt jest bezpieczny, dopóki nad tym pracujemy systematycznie, gdyż wiedzy na ten temat nie zdobywa się tylko raz. Trzeba ją uzupełniać codziennie. I właśnie na takich spotkaniach możemy ją pozyskać.
W czasie pandemii świat się zmienił, zmieniła się rzeczywistość i my sami, musimy więc zadbać, aby w tej nowej rzeczywistości funkcjonować bezpiecznie.



Piotr Kiliszek

PPL Porty Lotnicze

Jesteśmy w trakcie przygotowań do wprowadzenia dyrektywy cyberbezpieczeństwa NIS 2. Krajowy program ochrony lotnictwa cywilnego zakłada kontrolę dostępu jako jeden z podstawowych czynników bezpieczeństwa w ruchu lotniczym. W związku z tym zapewnienie bezpieczeństwa cybernetycznego jest dla nas istotne. NIS 2 wprowadzi nowe standardy i czeka nas rewolucja dotycząca bezpieczeństwa również w systemach kontroli dostępu. W branży ochrony zaczniemy stosować analitykę na coraz większą skalę. Pracowników, których teraz brakuje, zastąpią systemy zdalne. I myślę, że to będzie prawdziwa R-ewolucja w ochronie.

Adam Miksza

ALTEST

Dla mnie bardzo ważne jest, co podkreślali prelegenci, jak bardzo bliska jest perspektywa NIS 2. Wprowadzenie zaleceń tej dyrektywy przyczyni się do korzystania z szyfrowanych kanałów komunikacji nie tylko w kontroli dostępu, ale też w systemach monitoringu wizyjnego czy sygnalizacji włamania i napadu, co podniesie poziom bezpieczeństwa organizacji.

Grzegorz Klamut

Port Lotniczy Lublin

Zaciekawiło mnie i zaskoczyło to, że dyrektywa NIS 2 dotyczy nie tylko *stricte* cyberbezpieczeństwa znanego z płaszczyzny IT, ale również kontroli bezpieczeństwa i systemów, które są teraz z zasadzie w każdym przedsiębiorstwie. Z wejściem z życie dyrektywy NIS 2 czekają nas wielkie zmiany we wszystkich rozwiązaniach dotyczących zarówno elektronicznych systemów zabezpieczeń, jak i kontroli przemieszczania się użytkowników portu lotniczego. Pasażerowie nawet nie zauważą różnicy, natomiast Security Managerów czeka bardzo dużo pracy.

Magdalena Kolańska

Energa-Operator

Takie spotkania to na pewno wymiana doświadczeń i kontaktów, ale też praktyczne poznanie nowych rozwiązań, możliwość podejścia do stoiska i sprawdzenia działania urządzeń, które będzie można u siebie wykorzystać. Aktualnie moja organizacja ma wiele nowych zadań do zrealizowania. Jesteśmy przed projektem dużej modernizacji i właśnie na tej konferencji uzyskaliśmy niezbędną dla nas wiedzę, która pozwoli nam podejść do tego w inny, bardziej praktyczny sposób.

NEDAP SECURITY MANAGEMENT

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

AXIS D3110

Connectivity Hub

Axis Communications wprowadza na rynek węzeł komunikacyjny AXIS D3110 przeznaczony do bezpiecznego integrowania rozwiązań audio z sieciowymi systemami monitoringu. Urządzenie umożliwia podłączenie do systemu CCTV mikrofonu i głośników; wysokiej jakości dźwięk zwiększy świadomość sytuacyjną.

AXIS D3110 zapewnia połączenie z różnymi czujnikami niewizyjnymi w celu wyzwalania alarmów i powiadomień w momencie zidentyfikowania zdarzenia przez system dozoru wizyjnego.
Dzięki obsłudze nagrywania dźwięku, przesyłania strumieniowego i analizy audio jest idealnym rozwiązaniem dla systemów, które nie mają wbudowanego rozwiązania integrującego lub wymagają dodatkowych urządzeń. Najnowsza wersja platformy AXIS Camera Application Platform umożliwia uruchomienie dodatkowych, niestandardowych aplikacji.
Hub obsługuje formaty VAPIX®, MQTT i SIP, co zapewnia bezpieczną i bezproblemową integrację, stanowiąc doskonałe uzupełnienie kompleksowego rozwiązania systemów dozoru wizyjnego.
Wbudowane funkcje cyberbezpieczeństwa zapobiegają nieautoryzowanemu dostępowi i zabezpieczają system. Przykładem może być aplikacja Axis Edge Vault, która chroni identyfikator urządzenia Axis i upraszcza jego autoryzację w sieci.
Do kluczowych cech należą:

- Osiem nadzorowanych, konfigurowalnych wejść I/O
- Dwa porty audio-in, jeden port audio-out
- Integracja z protokołami VAPIX®, MQTT, SIP
- Obsługa platformy ACAP
- Wbudowane funkcje ochrony cybernetycznej.

Więcej na: www.axis.com/pl-pl

Nowe stałopozycyjne

Minikamery kopułkowe Axis

Minikamery kopułkowe — AXIS M3085-V, AXIS M3086-V i AXIS M3088-V są przystosowane do pracy w trudnych warunkach oświetleniowych. Każde z tych kompaktowych urządzeń umożliwia zaawansowane funkcje analizy wideo wspierane funkcjami głębokiego uczenia.

Wszystkie trzy nowe kamery serii AXIS M30 (model AXIS M3088-V będzie dostępny w dalszej części tego roku) oferują znakomitej jakości obrazy o rozdzielczości odpowiednio: 2, 4 i 8 Mpix. Dzięki szerokiemu zakresowi dynamiki oświetlenia WDR obraz z kamer jest wyraźny nawet wtedy, gdy obserwowana scena obejmuje ciemne i jasne partie jednocześnie. Modele AXIS M3085-V i AXIS M3086-V są wyposażone w technologię Axis Lightfinder, która pozwala uzyskiwać ostre obrazy w kolorze w słabych warunkach oświetleniowych.

Te kompaktowe minikamery umożliwiają wykonywanie zaawansowanych analiz opartych na głębokim uczeniu na brzegu sieci, co pozwala na prowadzenie szybkich i efektywnych prac wyjaśniających z wykorzystaniem przekazywanego na żywo lub zarejestrowanego materiału wideo. W kamerach zainstalowano fabrycznie aplikację AXIS Object Analytics wykrywającą i klasyfikującą obiekty z podziałem na osoby, pojazdy i typy pojazdów. Obsługują też platformę ACAP, która umożliwia zainstalowanie w kamerach aplikacji dostosowanych do potrzeb klientów.
Kamery serii AXIS M30 są także wyposażone w technologię Axis Zipstream z formatami H.264/H.265, która zmniejsza zapotrzebowanie na przepustowość i pamięć masową. Pamięć masowa typu Edge umożliwia rejestrowanie materiału na wbudowanej karcie pamięci, a funkcja Axis Edge Vault chroni identyfikator kamery i upraszcza autoryzację urządzeń Axis w sieci.
Najważniejsze cechy:

- Znakomita jakość obrazu o rozdzielczości do 8 MPix
- Kompaktowa dyskretna konstrukcja
- Szeroki zakres dynamiki oświetlenia
- Obsługa analiz z funkcją głębokiego uczenia i wbudowane cyberzabezpieczenia

Więcej na: www.axis.com/pl-pl

Kamery Hanwha Techwin

zarządzają ruchem na autostradzie

Do zarządzania ruchem na nowej autostradzie Pedemontana Veneta we Włoszech wykorzystano system wizyjny oparty na sztucznej inteligencji, stworzony przez firmy Hanwha Techwin i Sprinx. System dostarcza operatorom kluczowych informacji nt. natężenia ruchu i prędkości pojazdów.

Kamery Hanwha Techwin zostały przystosowane do współpracy z systemem traffix.ai wykorzystującym przetwarzanie obrazów i głębokie uczenie, stworzonym przez eksperta w tej dziedzinie, firmę Sprinx. System realizuje wiele funkcji analitycznych opartych na serwerze, mających na celu poprawę bezpieczeństwa użytkowników dróg i wgląd w korzystanie z autostrady przez kierowców.
Wspomniane funkcje działają w czasie rzeczywistym, automatycznie wykrywając niebezpieczne zdarzenia drogowe (zatory w ruchu i wypadki, a nawet dym lub ogień w tunelach) i natychmiast powiadamiając operatorów.
Na podstawie analizy obrazów z kamer Hanwha Techwin oprogramowanie Sprinx wykrywa też nieruchome obiekty, np. ładunki, które spadły na drogę, plamy rozlanego oleju i inne przedmioty stanowiące zagrożenie dla nadjeżdżających pojazdów, a także osoby poruszające się pieszo po autostradzie i zabłąkane zwierzęta.
Zastosowanie kamer Wisenet i sztucznej inteligencji zapewnia dodatkowe korzyści. Oprogramowanie Sprinx analizuje ruch pojazdów w polu widzenia wszystkich kamer, jest w stanie zbierać dane z dwóch pasów autostrady jednocześnie, na obu kierunkach ruchu. Uzyskane dane można analizować, rejestrować i przechowywać.
Analityka jest w pełni zintegrowana z systemem Wisenet Wave i umożliwia operatorom zliczanie pojazdów, pomiar natężenia ruchu na poszczególnych odcinkach oraz ustalanie średniej prędkości pojazdów na trasie. Informacje są udostępniane za pośrednictwem intuicyjnego interfejsu internetowego.

Więcej na: www.hanwha-security.eu

Nowa wersja

Genetec Security Center

Genetec wprowadził na rynek nową wersję swojej flagowej platformy bezpieczeństwa – Security Center. Wersja 5.11 daje dostęp do każdego modułu Security Center już po „wyjęciu z pudełka", w tym do Omnicast™ (CCTV/VSS), Synergis™ (KD), AutoVu™ (ANPR/LPR), Sipelia™ (interkom) i detekcji włamań.

Poza uproszczeniem drogi do unifikacji systemów Security Center 5.11 ma w standardzie wiele zaawansowanych funkcji, m.in. analitykę KiwiVision™ *(Privacy Protector, People Counting, Security Video Analytics* i *Camera Integrity),* zarządzanie gośćmi, zaawansowane funkcje mapowania, zarządzanie poziomem zagrożeń.
Zawiera też nową aplikację Genetec Web App z intuicyjnym interfejsem, która obsługuje mapy i działa na dowolnym urządzeniu z nowoczesną przeglądarką (Chrome, Safari, Firefox czy Edge). Dzięki temu klienci mogą monitorować obiekt, reagować na incydenty w czasie rzeczywistym, działać zgodnie z procedurami, współpracować z innymi operatorami i zarządzać posiadaczami kart, niezależnie od miejsca, w którym się znajdują.
Genetec Web App rozszerza bezpieczeństwo przedsiębiorstwa poza SOC *(Security Operations Center)* i umożliwia użytkownikom, którzy nie są tradycyjnymi operatorami ochrony, na interakcję z platformą bezpieczeństwa na podstawie ich roli i potrzeb.
Aplikacja może być używana przez kierownika ochrony, który chce zdalnie obserwować lokalizację, lub recepcjonistę, który musi zarządzać dostępem gości. Dzięki monitorowaniu zdarzeń, zarządzaniu posiadaczami kart i incydentami Genetec Web App wykracza poza monitorowanie bezpieczeństwa.
Security Center 5.11 idealnie nadaje się do zastosowania w wielu sektorach (np. bankowość, handel detaliczny, firmy z odległymi lub bezobsługowymi lokalizacjami).

Więcej na: https://www.genetec.com/product-releases/security-center-5-11

Nowe czytniki kodów QR

firmy ZKTeco

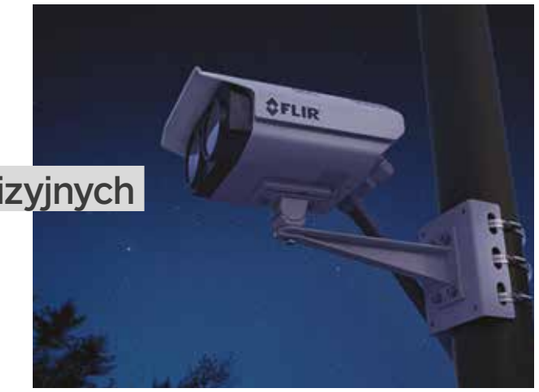
Wraz ze wzrostem popularności kodów QR, w tym również w branży systemów zabezpieczeń, rośnie dostępność rozwiązań umożliwiających ich odczyt. Do swojej szerokiej oferty tego typu czytników firma ZKTeco dodała ostatnio serię QR10M. To wysokowydajne czytniki kodów QR opracowane głównie dla integratorów systemów.

Czytniki mogą łatwo, szybko i z wysoką precyzją odczytywać dane kodów QR ze smartfonów lub materiałów drukowanych. Są zalecane do szybkiego uwierzytelniania w systemach kontroli dostępu oraz rejestracji czasu pracy.
Umożliwiają tworzenie własnych rozwiązań oraz, współpracując z istniejącymi na rynku aplikacjami, moduły QR pozwalają m.in. logować się do komputerów i innych urządzeń, zarządzać przepływem osób, płacić kodem QR, meldować się, uczestniczyć w wystawach i innych wydarzeniach lub uzyskiwać dostęp do programów lojalnościowych za pośrednictwem smartfonów.
ZKTeco zapewnia wszystkie niezbędne narzędzia i wsparcie do budowania własnych rozwiązań.
Czytniki są dostępne w obudowach: kompaktowej (IP55) z tworzywa (QR10ML), z metalu (QR10MX) wyposażonej w interfejs USB (Plug & Play) oraz w wersji przeznaczonej do zabudowy (QR10M). Dzięki zastosowaniu w nich wiodącego inteligentnego systemu rozpoznawania grafiki umożliwiają odczyt kodów ustawionych pod kątem i z dystansu, a dzięki wbudowanemu podświetleniu LED odczyt wszystkich dostępnych kodów QR i kodów kreskowych zarówno w ciągu dnia, jak i w nocy.

Więcej na: https://zkteco.eu/

Teledyne FLIR | FH-ID

– nowa seria kamer termowizyjnych z wbudowaną analityką



Nowa seria kamer termowizyjnych FH-ID marki Teledyne FLIR to połączenie wysokiej jakości kamery termowizyjnej oraz kamery światła widzialnego w jednej obudowie. W rozwiązaniu tym zastosowano analitykę obrazu opartą na technologii konwolucyjnych sieci neuronowych (CNN).

Kamera umożliwia analizę obrazu wideo zarówno w podczerwieni (termowizja), jak i w zakresie światła widzialnego. Technologia ta pozwala na precyzyjne wykrywanie i klasyfikację zagrożeń (ludzi oraz pojazdów) poruszających się z dużą lub małą prędkością, równocześnie znacząco minimalizując fałszywe alarmy oraz codzienne koszty operacyjne.
Kamera termowizyjna o rozdzielczości 640 x 512 pikseli i czułości <30 mK, w połączeniu z wysokiej jakości przetwornikiem światła widzialnego (4K) to ekonomiczne rozwiązanie gwarantujące optymalną wydajność. Dzięki tej integracji uzyskujemy możliwość oceny zagrożeń w czasie rzeczywistym oraz identyfikacji szczegółów w jakości 4K.
Seria kamer termowizyjnych FH-ID marki Teledyne FLIR to kompleksowe rozwiązanie oferujące:

- wbudowaną analitykę (CNN)
- możliwość planowania działania analizy obrazu
- łatwą integrację (ONVIF)
- monitoring w każdych warunkach wraz z identyfikacją (obraz termowizyjny i tradycyjny).

Operator ma możliwość planowania działania analityki na obrazie widzialnym lub termowizyjnym.
Kamera ta jest ściśle zintegrowana z systemem Teledyne FLIR United VMS oraz wieloma systemami VMS innych firm. Posiada wbudowaną technologię NEXUS® i jest zgodna z profilami ONVIF® S/G/T. Dzięki temu można ją zastosować zarówno w już istniejących, jak i nowych systemach.

Więcej na: www.linc.pl

RCP Master 4 Web

Zarządzanie czasem pracy z poziomu przeglądarki internetowej

RCP Master 4 Web to dodatkowy moduł systemu RCP Master 4, który umożliwia pracownikom dostęp do wybranych funkcji systemu RCP za pośrednictwem przeglądarki internetowej.

Pracownik korzystający z RCP Master 4 Web może, bez konieczności komunikacji z działem kadr, wykonać wiele czynności samodzielnie, w szczególności zapoznać się z aktualnym stanem wypracowanego czasu pracy, przejrzeć rejestr zdarzeń, złożyć wniosek o urlop lub zgłosić innego rodzaju absencję.
Moduł RCP Master 4 Web umożliwia pracownikom zdalną rejestrację zdarzeń RCP, w tym rejestrację pracy zdalnej.
Aplikacja RCP Master 4 Web udostępnia zestaw funkcji przeznaczonych dla przełożonych różnego szczebla (kierownicy, brygadziści, liderzy zespołów itp.), którzy zyskują w ten sposób wygodny i szybki sposób orientacji wewnątrz zarządzanej przez siebie grupy pracowniczej.
Wykorzystanie modułu RCP Master 4 Web jako integralnej części zainstalowanego w przedsiębiorstwie systemu rejestracji czasu pracy ułatwia pracownikom zarządzanie swoim czasem pracy. Ponadto automatyzuje i usprawnia pracę działów HR, eliminując szereg czynności i zadań związanych z obsługą pracownika.
Zarządzanie systemem rejestracji czasem pracy z poziomu przeglądarki internetowej w przedsiębiorstwie, które umożliwia RCP Master 4 Web, może być z powodzeniem wykorzystywane w wielu obszarach biznesowych, takich jak produkcja, logistyka, usługi, sektor komercyjny, sektor publiczny i wiele innych.

Więcej na: www.roger.pl

Nowa wersja

AEOS Locker Management

AEOS Locker Management firmy Nedap Security Management to inteligentny system powstały w odpowiedzi na rosnące potrzeby przedsiębiorstw w zakresie elastycznych i bezpiecznych opcji przechowywania. Jest wyróżniającym się na rynku rozwiązaniem, łączącym funkcje bezpieczeństwa z zarządzaniem szafkami i kontrolą dostępu.

Obecnie wiele osób pracuje w modelu hybrydowym, ze zmiennymi godzinami pracy. Oznacza to, że rośnie zapotrzebowanie na bezpieczną i elastyczną przestrzeń do przechowywania rzeczy osobistych, zwłaszcza w przypadku środowisk pracy opartych na współpracy i współdzieleniu. To sprawia, że szafki są niezbędną inwestycją dla wielu organizacji stosujących ten model pracy.
Inteligentny system zarządzania szafkami AEOS działa elastycznie i intuicyjnie, może zarządzać i zabezpieczać nieograniczoną liczbę różnorodnych szafek. Od zarządzania aktywami po przechowywanie, od szatni po miejsca składowania – inteligentne szafki mają wiele zastosowań.
System AEOS Locker Management jest integralną częścią platformy AEOS, znanego i wiodącego w branży systemu kontroli dostępu stosowanego przez wiele przedsiębiorstw na całym świecie. Dzięki temu rozwiązaniu zarządzanie dostępem do drzwi i szafek jest sprawniejsze.
Zmodernizowana, nowa wersja systemu oferuje różne możliwości osobistego dostępu w takich obiektach, jak biura, szkoły, szpitale, siłownie i inne. System można również dostosować do własnych potrzeb. Przykładowo, szafka może być przypisana do konkretnej osoby lub – jeśli jest to własność wspólna – do wielu upoważnionych osób.
Szafki można łatwo odblokować i zamykać za pomocą identyfikatora, telefonu komórkowego, kodu QR lub kodu biometrycznego. Dostęp do nich może być również ograniczony czasowo lub ustawiany za pośrednictwem pulpitu nawigacyjnego AEOS.
Wszystkie szafki są chronione przed włamaniami i cyberatakami w ramach rozszerzonych funkcji bezpieczeństwa.

Więcej na:
www.nedapsecurity.com/pl/

Zbyt wiele procesów cyfryzacyjnych kończy się niepowodzeniem

Aż 80 proc. menedżerów ocenia, że szybkie wprowadzanie nowoczesnych rozwiązań technologicznych decyduje o konkurencyjności przedsiębiorstwa – ale tylko 20 proc. uważa strategię transformacji cyfrowej w swojej organizacji za skuteczną. Jakie wnioski można wysnuć z *Digital Adoption Report* firmy WalkMe?

Twórcy badania rozmawiali z zarządzającymi, którzy pracują w Europie, Ameryce Płn., Australii i Nowej Zelandii. Z odpowiedzi wyłania się obraz pokazujący, że walory nowych technologii w biznesie są doceniane, jednak połączony ze świadomością, że wdrożenia często kończą się niepowodzeniem. Okazuje się, że 60 proc. przedsiębiorstw nie ma precyzyjnej strategii wprowadzania scyfryzowanych narzędzi, 59 proc. nie definiuje kluczowych wskaźników efektywności, czyli nie sprawdza skutków wdrożenia. Co więcej, 60 proc. ankietowanych jest zdania, że programy zarządzania cyfrową zmianą nie działają właściwie.

Firma w transformacji musi odrobić pracę domową

Ekspert firmy BPSC, starszy konsultant ds. wdrożeń, Marcin Samek, komentuje, że bez uporządkowania trybu wprowadzania nowych technologii nie może być mowy o dobrych efektach. *– Każde przedsiębiorstwo ma potencjał, aby przejąć pełną kontrolę nad swoimi inwestycjami cyfrowymi, ale aby to zrobić, potrzebuje odpowiedniego podejścia. Inwestor spodziewa się, że to analitycy dostawcy podsuną gotowe rozwiązania. Jednak nie jest to możliwe bez wieloetapowej współpracy. Przedsiębiorstwo musi odrobić pracę domową, a jest nią analiza procesów zachodzących w firmie, na bazie której powstaje mapa procesów biznesowych. Mapa ułatwia zespołowi wdrożeniowemu uszeregowanie i zrozumienie kolejnych procesów* – czytamy w informacji prasowej.

Zaawansowana cyfryzacja dużych i średnich organizacji

Z kolei z raportu przygotowanego w ub. roku przez „Computerworld" na zlecenie Intela i Polcomu wynika, że w Polsce 71 proc. dużych i średnich firm prowadzi procesy transformacji cyfrowej na różnym poziomie ich zaawansowania. 11 proc. nie zaczęło nadal tego rodzaju działań, 48 proc. przedsiębiorstw nie ma osobnego funduszu na cyfryzację, a pozostałe podmioty wydają na nią od 1 do 10 proc. firmowego budżetu.

W raporcie „Przemysł 4.0 – krok w kierunku bezpieczeństwa przemysłowego" czytamy jeszcze, że 83 proc. przedsiębiorstw uważa nowoczesne rozwiązania za niezbędne do elastycznego przekształcania i rozwijania swojej działalności.

Damian Kwiek, Platforma Przemysłu Przyszłości
Więcej na: https://przemyslprzyszlosci.gov.pl

BCS®

dla profesjonalistów

Cechy i funkcje aplikacji:

- podgląd na żywo
- odtwarzanie
- logi i powiadomienia
- e-mapa
- trasy i zadania
- reguły alarmów
- PC-NVR
- napisy (POS)
- obsługa chmury (P2P) BCS
- dodatkowe funkcje
- licencje

POLSKA MARKA BCS

www.bcs.pl

www.facebook.com/bcscctvpl