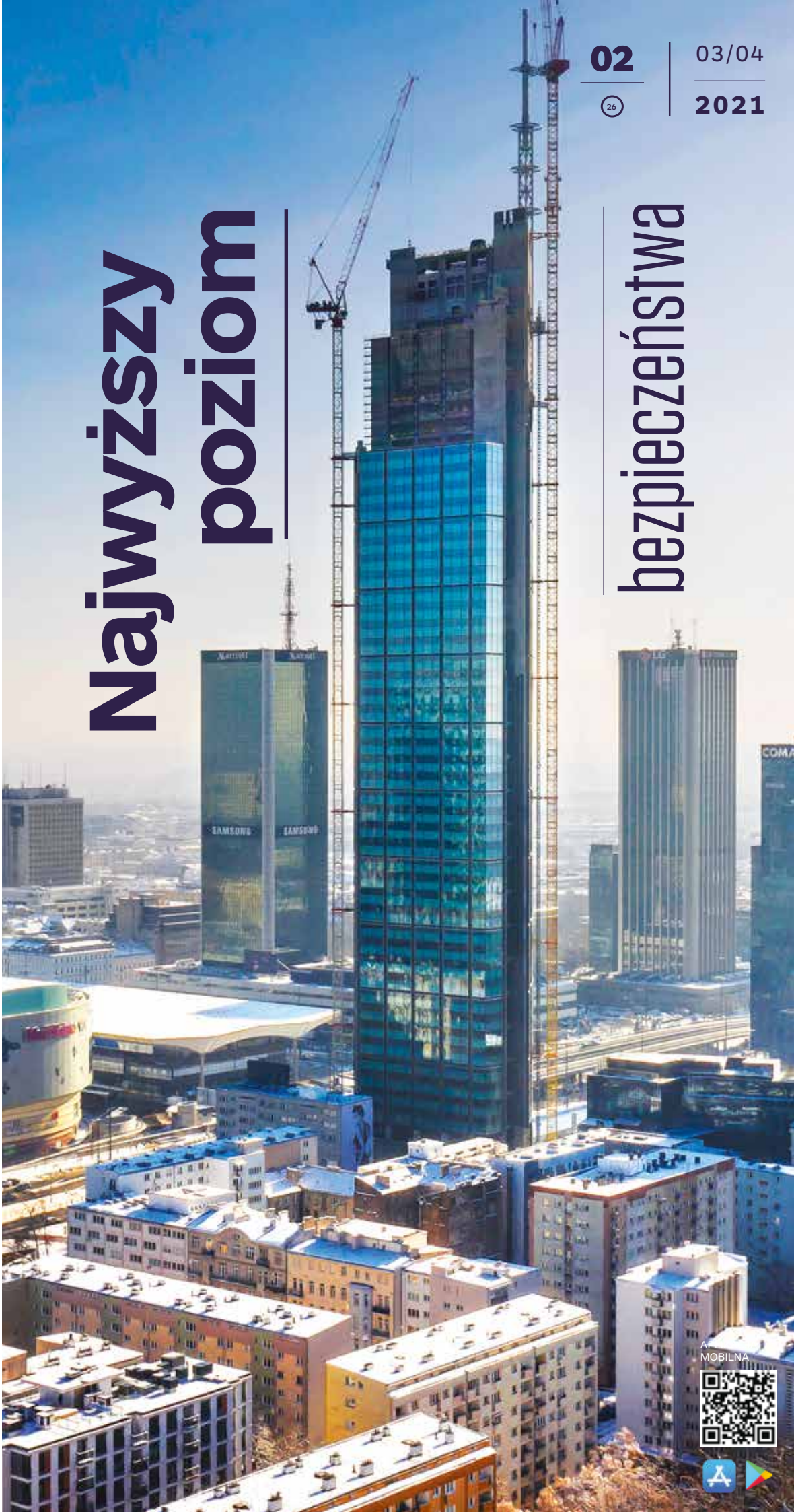
CZASOPISMO RYNKU SECURITY

a&s POLSKA

02 (26) 03/04 2021

Najwyższy poziom bezpieczeństwa



RYNEK SECURITY

PoEmat O TECHNOLOGII

Technologia Power over Ethernet doczekała się nowego standardu – IEEE 802.3bt. Pozwala on na przekazywanie znacznie większej mocy i wprowadza nowe funkcje, które zmienią sposób, w jaki patrzymy na urządzenia PoE.

INFRASTRUKTURA KRYTYCZNA

RÓŻNE OBLICZA BEZPIECZEŃSTWA

Bezpieczeństwo IK stanowi podstawę funkcjonowania państwa i obywateli, obiekty te muszą więc podlegać szczególnej ochronie. Należy budować świadomość zagrożeń tam występujących, aby móc im skutecznie przeciwdziałać.

CYBERBEZPIECZEŃSTWO

ZAGROŻENIA DLA SECURITY

Czy systemy zabezpieczeń technicznych trzeba chronić w obszarze środowiska IT, w którym pracują? Na co zwracać uwagę i jak łączyć cyberbezpieczeństwo z bezpieczeństwem fizycznym?

ISSN 2451-5175

9 772451 517703 05

15 zł (w tym 8% VAT)

www.aspolska.pl

EDYTORIAL

Drodzy Czytelnicy

Lubimy bić rekordy. Realizacja w centrum Warszawy Varso Tower – najwyższego w Europie biurowca – to marzenie niejednego architekta i inżyniera. W takim obiekcie wszystkie systemy budynkowe muszą być także na najwyższym poziomie, szczególnie zabezpieczenia przeciwpożarowe. Byliśmy tam i rozmawialiśmy o tym, jak poradzili sobie specjaliści w tym projekcie (s. 16).

Pandemia nie zahamowała prac nad rozwojem technologicznym. Technologia Power over Ethernet (PoE), która na długo przed COVID-19 zrewolucjonizowała rynek sieciowy doczekała się nowego standardu – IEEE 802.3bt. Umożliwia przekazywanie znacznie większej (nawet blisko 3-krotnie) mocy i wprowadza nowe funkcje, które zmienią sposób, w jaki patrzymy na PoE (s. 28).

Elementem niezbędnym do prawidłowego funkcjonowania urządzeń brzegowych sieci IP są przełączniki (switche) PoE. Pozwalają zmniejszyć koszty wdrożenia i wymagania dotyczące okablowania, zapewniając przy tym znacznie większą niezawodność. Sprawdziliśmy, jakie rodzaje przełączników PoE są obecnie dostępne na rynku i jak dobrać odpowiedni model do elektronicznych systemów zabezpieczeń (s. 32).

Nowoczesne rozwiązania technologiczne mogą pomóc firmom w czasie kryzysu spowodowanego pandemią. Branża ochrony fizycznej jeszcze przed COVID-19 borykała się z wieloma problemami, teraz w wielu przypadkach sytuacja uległa dalszemu pogorszeniu. Pomóc może właśnie zastosowanie nowoczesnych technologii (s. 46).

Tematem przewodnim marcowo-kwietniowego wydania jest bezpieczeństwo obiektów infrastruktury krytycznej, które – stanowiąc podstawę bezpiecznego funkcjonowania państwa i obywateli – podlegają szczególnej ochronie. Nawet niewielkie incydenty mogą powodować skutek krytyczny. Nie wolno ich lekceważyć., pamiętając że żaden scenariusz ataku nie jest absurdalny (s. 50).

Teoretycznie lista obiektów IK jest precyzyjna. Jednak coraz trudniej dziś określić, co jest lub może być za chwilę infrastrukturą krytyczną – np. Stadion PGE Narodowy funkcjonujący jako szpital tymczasowy. Co to oznacza dla branży security? Nasze systemy muszą być tak projektowane, instalowane i utrzymywane, by łatwo móc podnosić ich status bezpieczeństwa (s. 60). Jak eksperci z różnych sektorów rynku oceniają zabezpieczenia ciągłości działania infrastruktury krytycznej piszemy na s. 68.

W numerze poruszamy też bardzo ważny aspekt cyberbezpieczeństwa. Czy elektroniczne systemy zabezpieczeń trzeba chronić w obszarze środowiska IT, w którym pracują? Na co zwracać uwagę i jak łączyć cyberbezpieczeństwo z bezpieczeństwem fizycznym (s. 76)? Kontynuujemy także cykl o cyberbezpieczeństwie w firmach safety i security, omawiając przepisy organizacyjno-prawne, które musi spełnić operator usługi krytycznej lub dostawca usługi cyfrowej (s. 80).

Niezmiennie życzymy dużo zdrowia!

Marta Dynakowska
REDAKTOR NACZELNA

Jan T. Grusznic
Z-CA REDAKTORA NACZELNEGO

Mariusz Kucharski
DYREKTOR ZARZĄDZAJĄCY

A&S POLSKA REDAKCJA

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

Dyrektor zarządzający
Mariusz Kucharski

Redaktor naczelna
Marta Dynakowska

Z-ca redaktora naczelnego
Jan T. Grusznic

Dział reklamy i marketingu
Iwona Krawiec

Dział projektów specjalnych
Jolanta A. Kucharska
Aleksandra Czapska

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
Aura Sky Offices
ul. M. Rodziewiczówny 1 lok. 801
04-187 Warszawa
e-mail: info@aspolska.pl
www.aspolska.pl

Prenumerata
www.aspolska.pl/prenumerata

a&S POLSKA

02

26

03/04

2021

SPIS TREŚCI

SPIS TREŚCI

INFRASTRUKTURA KRYTYCZNA

CYBERBEZPIECZEŃSTWO

SERWIS INFORMACYJNY

AXIS COMMUNICATIONS

www.axis.com/pl

Szybka kamera PTZ od Axis do dozoru dużych i słabo oświetlonych obszarów

KAMERA PTZ AXIS Q6135-LE Z TECHNOLOGIĄ OPTIMIZEDIR I OŚWIETLACZAMI IR-LED, KTÓRE DOSTOSOWUJĄ SIĘ DO ZOOMU KAMERY, ZAPEWNIA ZNAKOMITĄ JAKOŚĆ OBRAZU W CIEMNOŚCI LUB SŁABYM OŚWIETLENIU NA ODLEGŁOŚĆ DO 250 M, A NAWET WIĘKSZĄ, ZALEŻNIE OD OBSERWOWANEJ SCENY. PROCESOR NOWEJ GENERACJI ZAPEWNIA ULEPSZONĄ OBSŁUGĘ OBRAZU, WZMOCNIONE ZABEZPIECZENIA, ROZSZERZONE FUNKCJE ANALIZ I ZNACZNIE EFEKTYWNIEJSZĄ KOMPRESJĘ.

Kamera idealnie sprawdza się w takich obszarach, jak np. parki, gdzie wymagany jest szczegółowy dozór wizyjny alei, ścieżek itp.
Została wyposażona w aplikację Autotracking 2 z funkcją „kliknij i śledź" oraz dynamiczne nakładki ułatwiające orientację w czasie śledzenia obiektów.
Z kolei aplikacja AXIS Object Analytics umożliwia detekcję i klasyfikację ludzi i pojazdów, a technologia Lightfinder 2.0 gwarantuje lepsze nasycenie kolorów na obrazach z miejsc rejestrowanych w słabym oświetleniu, a także ostrzejsze obrazy ruchomych obiektów.
Kamera AXIS Q6135-LE ma rozszerzone zabezpieczenia, takie jak podpisane oprogramowanie sprzętowe i funkcja bezpieczny start, które dają pewność, że instalowane będzie tylko autoryzowane, niezmodyfikowane oprogramowanie sprzętowe. Jest wyposażona w moduł TPM *(Trusted Platform Module)* z certyfikatem FIPS 140-2 na poziomie 2., który zapewnia bezpieczne przechowywanie wszystkich kluczy kryptograficznych i certyfikatów, dzięki czemu nawet w razie naruszenia zabezpieczeń nic im nie grozi.

BCS

www.bcscctv.pl

Nowa kamera szybkoobrotowa z serii urządzeń inteligentnych BCS Line AI

KAMERA BCS-SDIP4432AI-II TO NOWE WYDANIE DOBRZE ZNANYCH GŁOWIC SZYBKOOBROTOWYCH, KTÓRE ZYSKAŁY UZNANIE WŚRÓD KLIENTÓW. JEST TO WERSJA 4-MPIX Z SUPERCZUŁYM PRZETWORNIKIEM STARVIS I OBIEKTYWEM Z 32X ZOOMEM OPTYCZNYM, UZUPEŁNIONA O FUNKCJE ZAAWANSOWANEJ ANALIZY OBRAZU.

Obrót głowicy szybkoobrotowej w osi poziomej jest nieograniczony, a wychylenie w osi pionowej pozwala na podniesienie kamery aż o 15° względem podłoża. Kompaktowa obudowa ma klasę szczelności IP67 i odporności mechanicznej IK10. Kamerę wyposażono w promiennik podczerwieni o zasięgu do 150 m, gniazdo kart pamięci o pojemności do 256 GB, wejście/wyjście audio pozwalające na dwukierunkową komunikację audio oraz po jednym wejściu i wyjściu alarmowym.
Najważniejsze jednak w tym modelu są funkcje zaawansowanej analizy wideo. Do dyspozycji są m.in. wtargnięcie w strefę i przekroczenie linii, z możliwością klasyfikacji obiektu (człowiek, samochód), który spowodował alarm. Można je ustawiać dla każdego presetu osobno. Dostępna jest też funkcja detekcji twarzy, jednak na jednym presecie nie może ona działać równolegle z funkcjami ochrony obwodowej.
Do ustawień ogólnych kamery pracującej w trybie ścieżki lub skanowania można dodać funkcję zbierania metadanych o trzech podstawowych typach obiektów: człowiek, samochód, jednoślad. Kamera wspiera też tzw. inteligentną detekcję ruchu, z klasyfikacją obiektu. Jakość obrazu zapewniają WDR 120 dB i elektroniczna stabilizacja obrazu.

HIKVISION

www.hikvision.com/pl

Kamery Hikvision z analityką Acusense

KAMERY HIKVISION SERII 3. – DS-2CD3XX6G2 – SĄ WYPOSAŻONE W ANALITYKĘ ACUSENSE DRUGIEJ GENERACJI, OPARTĄ NA TECHNOLOGII GŁĘBOKIEGO UCZENIA *(DEEP LEARNING)*. ZMIENNE WARUNKI OŚWIETLENIOWE, PORUSZAJĄCE SIĘ CIENIE, DRZEWA CZY KRZEWY NIE WPŁYWAJĄ NA POPRAWNE DZIAŁANIE ANALIZY OBRAZU.

Funkcje analityczne kamery pozwalają na rozróżnienie poruszających się obiektów, wyodrębniając ludzi i pojazdy. Klasyfikacja obiektów pozwala także szybko przeszukiwać archiwum. Korzystając z odpowiednich filtrów w rejestratorze NVR, oprogramowaniu iVMS-4200 lub HikCentral, można zdefiniować kryterium wyszukiwania, a system w kilka sekund wygeneruje wynik w postaci listy obiektów lub kadrów.
Oprócz wbudowanej analityki wybrane modele kamer są wyposażone w głośnik i oświetlenie stroboskopowe.
Do kamery można wgrać wcześniej przygotowane nagranie audio, które będzie emitowane w monecie wykrycia intruza. Oświetlenie zaś pełni funkcję ostrzegawczą oraz zwiększa szansę nagrania twarzy intruza, który odruchowo popatrzy w kierunku mrugającego światła.

JOHNSON CONTROLS

www.dsc.com

DSC – zewnętrzne bezprzewodowe czujki PG8902 i PG8312

FIRMA JOHNSON CONTROLS SZCZEGÓLNĄ UWAGĘ POŚWIĘCA SWOJEJ OFERCIE URZĄDZEŃ DO SYSTEMÓW OCHRONY ZEWNĘTRZNEJ. W CENTRUM ZAINTERESOWANIA ZNAJDUJĄ SIĘ DWIE CZUJKI ZEWNĘTRZNE: BEZPRZEWODOWA CZUJKA KURTYNOWA PG8902 ORAZ BEZPRZEWODOWY KONTAKTRON PG8312.

PG8902 to zewnętrzna, zawansowana kurtyna o zasięgu 8 m. Tworzy wąską tarczę ochronną na okna, drzwi, balkony, podjazdy czy bramy. Czujka jest odporna na czynniki atmosferyczne, zwierzęta domowe, jest też wyposażona w system antymaskingu. Stanowi niezawodny, pierwszy pierścień wykrywający potencjalnego intruza jeszcze zanim wyrządzi szkody lub wtargnie do chronionego domu.
Zależnie od ustawień i centrali alarmowej potrafi rozpoznać kierunek przekroczenia nadzorowanej strefy oraz zmierzyć temperaturę powietrza.

PG8902

PG8312

PG8312 to zewnętrzny, bezprzewodowy kontaktron z dodatkowym wejściem przewodowym. Jego przeznaczeniem jest zabezpieczenie furtek, bram wjazdowych, garaży czy budynków oddalonych od miejsca zainstalowania centrali.
Czujka PG8312 jest w stanie pracować w temperaturze od -35°C do 66°C. Szybka instalacja, antymasking magnetyczny, szczelna konstrukcja obudowy (IP66), do 5 lat pracy na baterii to parametry, które ją charakteryzują. Ma też dużą tolerancję na przestrzeń pomiędzy czujką a magnesem, co dodatkowo zwiększa odporność na niechciane fałszywe alarmy wywołane wiatrem lub przez zwierzęta uderzające w zewnętrzne bramy.
Obie czujki wykorzystują dwukierunkową, szyfrowaną łączność PowerG.

LINC POLSKA

www.linc.pl

Jaegar – wieloczujnikowa platforma do nadzoru perymetrycznego

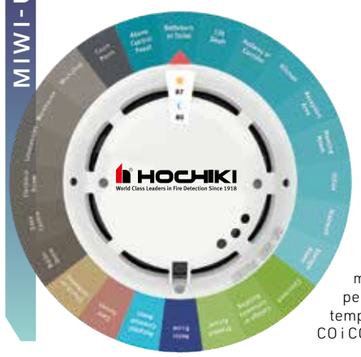
KAMERY TERMOWIZYJNE SILENT SENTINEL SĄ PRZEZNACZONE DO ZASTOSOWAŃ W OBSZARZE DOZORU WIZYJNEGO I OCHRONY. ZOSTAŁY ZAPROJEKTOWANE DO PRACY W TRUDNYCH WARUNKACH ATMOSFERYCZNYCH I W ZUPEŁNEJ CIEMNOŚCI. ZAPEWNIAJĄ OBRAZ TERMOWIZYJNY O WYSOKIM KONTRAŚCIE, OFERUJĄC DZIĘKI TEMU OPTYMALNE PARAMETRY DO PRACY Z ANALIZĄ WIDEO.

Gdy konieczna jest ochrona rozległych terenów o znaczeniu strategicznym, platforma Jaegar będzie najlepszym wyborem. Połączenie chłodzonej kamery termowizyjnej (MWIR) z tradycyjną wysokoczułą kamerą światła widzialnego zapewnia doskonały dozór dalekiego zasięgu i weryfikację zdarzenia w zdefiniowanej strefie. Oba obrazy: termowizyjny i dzienny są generowane w tym samym czasie.
Obudowa z odpornego aluminium malowanego proszkowo o klasie szczelności IP 67 zapewnia stabilną pracę w najbardziej wymagającym środowisku. Specjalny mechanizm obrotu platformy pozwala na precyzyjne sterowanie i ciągły ruch o kącie 360° oraz korektę położenia z szybkością obrotu do 45°/s. Kamera może być zintegrowana z dowolnym systemem zabezpieczeń i stanowi idealne uzupełnienie systemów radarowych zamontowanych powyżej kamery, umożliwiając pełną detekcję wtargnięć.
Platforma Jaegar jest specjalistycznym i zaawansowanym rozwiązaniem zdolnym do obsługi systemów w technologii wieloczujnikowej, do zastosowań morskich, granicznych, lotniczych, obronnych i perymetrycznych. To profesjonalne rozwiązanie dla wymagających użytkowników.

MIWI-URMET

www.miwiurmet.pl

ACD-EN – najbardziej zaawansowany wielosensorowy detektor pożarowy na rynku



ACD-EN TO ZUPEŁNIE NOWY ADRESOWALNY DETEKTOR WIELOSENSOROWY FIRMY HOCHIKI, ZASILANY Z PĘTLI, Z ELEMENTAMI WYKRYWAJĄCYMI DYM, CIEPŁO, TLENEK WĘGLA, CZYLI CZAD I POZIOM HEMOGLOBINY TLENKOWĘGLOWEJ COHB.

Ta zaawansowana czujka pożarowa oferuje aż 24 certyfikowane przez LPCB tryby pracy zgodne z EN, m.in. kombinacje wykrywania dymu, przekroczenia stałej temperatury, szybkości wzrostu temperatury oraz wykrywania CO i COHb, co czyni ją idealnym rozwiązaniem do różnych zastosowań. Tradycyjnie sensor CO zintegrowany w czujkach wielosensorowych wspomaga detekcję tlących się pożarów. Czujka ACD-EN zawiera dodatkowo zaawansowany algorytm wykrywania COHb.
Określenia trybu pracy czujki dokonuje się w centrali SSP, wybierając rodzaj pomieszczenia, w jakim będzie pracowała. Doświadczony instalator ma również możliwość ręcznej modyfikacji ustawień.
ACD-EN jest również zaawansowany pod kątem redukcji fałszywych alarmów. W trybach z funkcją *Reduced False Alarm* (+ RFA) automatycznie dostosowuje czułość detektora optycznego, ucząc się otoczenia od momentu instalacji.
Odbywa się to za pomocą zaawansowanego algorytmu, który w sposób ciągły monitoruje odczyt wartości analogowej z serii wielu próbek środowiska i oblicza wartość średnią. Ten przełomowy algorytm nazywamy *Suitable Moving AveRage Time* – SMART.
Detektor ACD działa na znanym na świecie, solidnym i niezawodnym, otwartym protokole ESP firmy Hochiki.

NEDAP SECURITY MANAGEMENT

www.nedapsecurity.com/pl/

AEOS Locker Management

W OSTATNICH LATACH SPOSÓB NASZEJ PRACY ULEGŁ DUŻEJ ZMIANIE, A OBECNIE PANDEMIA COVID-19 TE ZMIANY JESZCZE PRZYSPIESZYŁA. RÓWNIEŻ BIURA SĄ CORAZ BARDZIEJ PRZYJAZNE PRACOWNIKOM, A SAMA PRZESTRZEŃ EFEKTYWNIEJ ZAPROJEKTOWANA.

Nowe podejście do organizacji pracy umożliwia jej wykonywanie w różnych częściach biura, a nie – jak obowiązywało to w poprzednim modelu – zazwyczaj przy swoim biurku.
Taka elastyczność wymusza również zastosowanie odpowiednich rozwiązań wspierających nowy model pracy w nowoczesnym biurze. Jednym z rozwiązań jest AEOS Locker management, czyli dedykowane zamki montowane w szafkach pracowników.
Wspomniana szafka może zostać przypisana na stałe konkretnemu pracownikowi lub też można nią zarządzać w sposób elastyczny – na wyświetlaczu terminala sprawdza się, która szafka jest wolna, i ją się wybiera.
Indywidualne konfiguracje pozwalają na elastyczne grupowanie szafek, dzięki czemu system zawsze odpowiada potrzebom organizacji.
W przypadku rozwiązania firmy Nedap system Locker management jest również zintegrowany z systemem kontroli dostępu AEOS. Dzięki temu pracownicy mają możliwość używania tego samego identyfikatora (karta RFID lub wirtualna karta w smartfonie) zarówno w kontroli dostępu do obiektu, jak i dostępie do szafek.
Zarządzający natomiast mają jeden system do administracji i nadawania uprawnień, co znacznie oszczędza czas i uproszcza proces zarządzania.

OPTEX SECURITY

www.optex-europe.com/pl

Czujka LiDAR REDSCAN PRO – precyzyjna detekcja odległych obiektów

FIRMA OPTEX WPROWADZA NA RYNEK NOWĄ CZUJKĘ LASEROWĄ REDSCAN PRO O NAJWIĘKSZYM JAK DOTYCHCZAS ZASIĘGU, STANOWIĄCĄ NAJLEPSZE ROZWIĄZANIE DO OCHRONY OBSZARÓW WYMAGAJĄCYCH WYSOKIEGO POZIOMU BEZPIECZEŃSTWA.

REDSCAN PRO z niezwykłą dokładnością wykrywa intruzów na obszarze 50 x 100 m, bez luk i utraty skuteczności związanej ze wzrostem odległości. Zastosowanie pól detekcji w kształcie prostokąta eliminuje ich nakładanie się, dzięki czemu czujki doskonale nadają się do ochrony elewacji i ogrodzeń oraz otwartych powierzchni (sufity, dachy).
Dzięki inteligentnym algorytmom wielostrefowym można niezależnie dla każdej strefy detekcji określić czułość czujki, rozmiar obiektu i moc sygnału wyjściowego, dostosowując urządzenie do lokalizacji i specyfiki zagrożeń. Daje to gwarancję maks. częstotliwość przechwytywania i ogranicza występowanie fałszywych alarmów.
Na potrzeby konfiguracji i analizy zdarzenia, które wywołało alarm, wizualne wspomaganie zapewnia kamera. Zapisywany w momencie alarmu plik dziennika i obraz wideo ułatwiają analizę przyczyn zdarzenia i podjęcie określonych działań.
REDSCAN PRO charakteryzuje się nowym eleganckim wzornictwem, elastycznością opcji montażu (pochylenie pod kątem od +5 do -95°), łatwością ustawień i prostotą konfiguracji za pomocą przeglądarki sieciowej. Czujki są zgodne z protokołem ONVIF S.
Seria REDSCAN Pro obejmuje dwa modele: RLS-3060V o maks. zasięgu 30 x 60 m oraz RLS-50100V o zasięgu do 50 x 100 m.

SCHRACK-SECONET

www.schrack-seconet.pl

VISOCALL IP – system przyzywowy i komunikacji

SARS-COV-2 ZMIENIAŁ STANDARDY W OPIECE ZDROWOTNEJ. DOSTOSOWANIE PRODUKTU DO POTRZEB SZPITALA GWARANTUJĄ SYSTEMY OTWARTE, W KTÓRYCH MOŻNA ŁATWO ZMIENIĆ FUNKCJONALNOŚĆ BEZ KONIECZNOŚCI ZMIANY OKABLOWANIA. JEDNYM Z PRZYKŁADÓW JEST ZAPROGRAMOWANIE TERMINALI PACJENTÓW (SŁUCHAWEK) PRZY ŁÓŻKACH JAKO TELEFONÓW. PACJENCI MOGĄ ROZMAWIAĆ Z RODZINAMI WŁAŚNIE PRZEZ TAKIE URZĄDZENIA.

System przyzywowy powinien optymalizować proces opieki w służbie zdrowia, zapewniać cyfrową obustronną komunikację głosową, równolegle z każdą osobą w pokoju (z pacjentami, personelem).
Normą jest, że urządzenia z funkcją komunikacji głosowej pracują w standardzie IP, a terminale pacjentów - słuchawki przy łóżkach pozwalają na dyskretną rozmowę, zapewniając przestrzeganie praw pacjenta zapisanych w Rozporządzeniu o Ochronie Danych Osobowych (RODO) i ustawie z 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta.
Ważna jest również optymalizacja procesów z wykorzystaniem komunikacji głosowej i odbiorem przywołań na urządzeniach systemowych lub mobilnych, np. smartfonach, telefonach DECT/VoIP, podłączanie pętli indukcyjnych dla osób słabosłyszących do słuchawek przy łóżkach czy integracja z systemem sygnalizacji pożarowej, słuchanie programów radiowych, sterowanie telewizją czy też automatyką budynkową (KNX).
Wszystkie opisane funkcje oferuje system przyzywowy i komunikacji Schrack Seconet, z gwarancją kompatybilności z systemami produkowanymi nawet 20 lat temu.

TELESTE

www.teleste.com

Teleste S-AWARE – System Świadomości Sytuacyjnej

INNOWACYJNE ROZWIĄZANIE S-AWARE® FIRMY TELESTE UMOŻLIWIA AGREGOWANIE, ANALIZOWANIE I ZARZĄDZANIE INFORMACJAMI POCHODZĄCYMI Z RÓŻNYCH ŹRÓDEŁ W CELU UZYSKANIA CZYTELNEGO OBRAZU SYTUACYJNEGO KAŻDEGO ZDARZENIA.

Rozwiązanie to sprawia, że właściwe identyfikowanie potencjalnych i zaistniałych zagrożeń jest szybsze i bardziej efektywne. Pozwala skutecznie kontrolować i zarządzać różnego typu zdarzeniami, wspierając tym samym działania operatorów systemu i poprawiając funkcjonowanie obiektu.
W razie sytuacji kryzysowej informacje docierają do odpowiednich osób bądź jednostek we właściwej formie i na czas.
S-AWARE umożliwia integrację i zarządzanie różnego typu systemami: zabezpieczeń, informacyjnymi, a także niezwiązanymi z bezpieczeństwem obiektowym, np. systemami produkcyjnymi.
Zebrane dane są wyświetlane i zarządzane poprzez elastycznie konfigurowalny interfejs użytkownika (GUI), który obsługuje również różnego rodzaju panele *(dashboard)* oraz mapy. Generowane przez system raporty mogą być wykorzystywane do przeprowadzania analiz funkcjonowania systemu i pracy personelu, jak również do prowadzenia szkoleń.
S-AWARE jest dostępny jako samodzielny produkt lub może funkcjonować jako dodatkowa warstwa systemu S-VMX, który jest zaawansowanym systemem nadzoru i zarządzania obrazem wideo firmy Teleste.
S-AWARE jest platformą otwartą, może zostać zintegrowany praktycznie z każdym innym technicznym systemem firm trzecich.

TP-LINK

www.tp-link.com.pl

TP-Link VIGI C300P – zewnętrzna kamera CCTV typu bullet, IP67

VIGI C300P TO ZEWNĘTRZNA KAMERA SIECIOWA TYPU BULLET O ROZDZIELCZOŚCI 3 MPIX. URZĄDZENIE ZOSTAŁO WYPOSAŻONE W WODOODPORNĄ I PYŁOSZCZELNĄ OBUDOWĘ O KLASIE SZCZELNOŚCI IP67, DZIĘKI CZEMU JEST ODPORNE NA WARUNKI ATMOSFERYCZNE.

Kamera występuje w dwóch wersjach – z obiektywem o ogniskowej 4 lub 6 mm. Dzięki temu odznacza się uniwersalnością działania.
Urządzenie sprawdzi się zarówno w dozorze wizyjnym wąskich korytarzy, jak i otwartych przestrzeni.
Dzięki zgodności ze standardem 802.3af/at PoE instalacja kamery jest łatwa, bezpieczna i mniej kosztowna. Kamera może być również zasilana poprzez dołączony do zestawu zasilacz 12 V DC.
Dzięki aplikacji VIGI na urządzenia przenośne z systemem iOS lub Android kamerami można w prosty i kompleksowy sposób zarządzać z poziomu smartfona. Kamera wyśle powiadomienie push za każdym razem, gdy wykryje niepożądany ruch, zaobserwuje przekroczenie wyznaczonej granicy lub gdy ktoś zasłoni jej obiektyw.
Systemem do monitoringu VIGI można też zarządzać poprzez rejestrator lub z poziomu dedykowanego oprogramowania przeznaczonego do komputerów.
Urządzenie wykorzystuje kompresję H.264+, co w połączeniu z rejestratorem VIGI NVR1008 pozwala na nagranie i przechowywanie do 100 dni materiału wideo w wysokiej rozdzielczości.
Produkt został objęty 3-letnią gwarancją producenta.

W2

www.w2.com.pl

Sygnalizator głosowo-optyczny SGO-Pgw

W OFERCIE W2 POJAWIŁ SIĘ ZUPEŁNIE NOWY PRODUKT. SGO-PGW JEST SYGNALIZATOREM GŁOSOWO-OPTYCZNYM PRZEZNACZONYM DO STOSOWANIA W SYSTEMACH SYGNALIZACJI POŻAROWEJ (SSP).

Urządzenie jest przeznaczone do instalacji wewnątrz budynków. Jego zadaniem jest alarmowanie osób o występującym zagrożeniu pożarowym.
W tym celu SGO-Pgw generuje akustyczny sygnał ostrzegawczy wraz z komunikatem słownym oraz optyczny sygnał błyskowy. Przetwornikiem dźwięku jest głośnik, co zapewnia wysoką jakość oraz zrozumiałość odtwarzanej sekwencji alarmowej.
Sygnalizator wyposażono w potencjometr do regulacji głośności, pozwalający na dostosowanie poziomu dźwięku do specyfiki obiektu. Oprócz tego umożliwia tworzenie sieci urządzeń pracujących synchronicznie. Ponadto realizuje funkcje: autoaktualizacji, autoadresowania czy autodiagnostyki.
W celu umożliwienia sprawdzania ciągłości linii obniżoną wartością napięcia zastosowano blokadę podnapięciową.
SGO-Pgw jest dostępny w czterech wersjach (różniących się barwą światła i ułożeniem soczewki). Do sygnalizatora fabrycznie są wgrywane trzy komunikaty o różnych treściach, które są odtwarzane w trzech językach (polski, angielski, niemiecki).
Użytkownik może też wgrać do urządzenia własny komunikat, dane są kopiowane z wykorzystaniem wbudowanego złącza microUSB (analogicznie do pamięci masowej).
Sygnalizator głosowo-optyczny SGO-Pgw spełnia wymagania norm EN 54-3 oraz EN 54-23, czego potwierdzeniem są dokumenty wydane przez CNBOP-PIB.

Bezpieczeństwo pożarowe na najwyższym poziomie

O wyzwaniach związanych z zapewnieniem bezpieczeństwa pożarowego kompleksu biurowo-usługowego Varso Place z Mariuszem Melerskim, Senior Facility Managerem z firmy HB Reavis, rozmawiali Jan T. Grusznic i Iwona Krawiec z a&s Polska.

MARIUSZ MELERSKI I JAN T. GRUSZNIC NA DACHU VARSO TOWER – NAJWYŻSZEGO BUDYNKU W UNII EUROPEJSKIEJ

Realizacja takiej inwestycji jak Varso Place – a zwłaszcza najwyższego budynku w Unii Europejskiej – to marzenie wielu architektów i inżynierów, ale też mnóstwo wyzwań związanych z utrzymaniem wysokiego poziomu bezpieczeństwa. Czy musieliście zastosować jakieś nietypowe rozwiązania do jego zapewnienia?

Wszystko co mamy na Varso Place, to są osiągnięcia techniki stosowane powszechnie. Trudność tego projektu polega na jego skali, gdyż do tej pory w Polsce jeszcze nikt nie budował tak wysoko. Dlatego ten projekt jest w dużej mierze innowacyjny, a mimo bariery wysokościowej i kubaturowej tworzy spójną całość. Mamy niezawodne instalacje i zapewnioną sprawną ewakuację. Na pewno w skutecznym działaniu pomaga wyposażenie budynku w wysokociśnieniową instalację zraszaczy, pożarową instalację alarmową o wysokiej skuteczności w części zarówno detekcyjnej, jak i obsługi systemu. Jest wiele dostępnych narzędzi diagnostycznych, które pomagają przetestować sprawność działania systemu bez uciążliwego zakłócania spokoju najemcom, ponieważ cała procedura jest przeprowadzana łatwo, szybko i skutecznie.

Przypomnę, że docelowo w Varso Place mamy 150 tys. metrów kwadratowych powierzchni komercyjnej plus usługi gastronomiczne, sklepy spożywcze, salony kosmetyczne. Mamy też nietypowe przestrzenie, np. dwupoziomową restaurację na ostatnich piętrach budynku Varso Tower plus dwa tarasy publiczne dostępne dla zwiedzających z zewnątrz. Ponadto w całym Varso Place 4-poziomowy parking podziemny o pojemności 1000 miejsc, który w dużej części będzie udostępniony jako parking publiczny. Mówimy tu o dużych powierzchniach użytkowych skumulowanych na dość małej przestrzeni.

Czy zatem projekt systemu bezpieczeństwa pożarowego różnił się znacząco od innych realizacji?

Zapewnienie bezpieczeństwa pożarowego tak dużego obiektu jest procesem. Już na początku projektant musi uwzględnić wszystkie aspekty prawne, musi nałożyć na to potrzeby biznesowe, komercyjne i zaproponować rozwiązania, które użytkownik końcowy zaakceptuje i będzie ich używał.

Część wymagań z tego zakresu jest narzucana przez przepisy. Tak było w przypadku wysokociśnieniowej instalacji tryskaczowej czy wzmocnienia sygnału dla służb pożarniczych. Sama ustawa o prawie budowlanym narzuca konieczność wyposażenia budynku w określone instalacje zapewniające jego bezpieczeństwo pożarowe, np. instalacje hydrantowe, podręczny sprzęt gaśniczy czy stałe urządzenia gaśnicze. Pojawiają się też systemy związane ze specjalnymi potrzebami najemców, którzy mogą dostosować system do zmian architektonicznych, jakie chcą u siebie wprowadzić. Projekt jest adaptowany do nowej aranżacji, mogą być dodawane poszczególne elementy systemu, np. stałe urządzenia gaśnicze. Przykładowo w restauracji są to urządzenia przeznaczone do gaszenia substancji łatwo palących się, np. tłuszczy.

Obligatoryjnie w budynku musi być zainstalowany system detekcji i sygnalizacji pożaru, dźwiękowy system nagłośnienia i system oświetlenia awaryjnego oraz powiązany z nimi system wentylacji pożarowej – zarówno oddymiający, jak i napowietrzający.

Cały kompleks Varso Place składa się z trzech obiektów: dwa niższe są już oddane, trzeci – Varso Tower –

Fot. HB Reavis

VARSO PLACE

Varso Place to trzy wieżowce zlokalizowane przy ul. Chmielnej, w samym centrum Warszawy, które mieszczą biura, hotel i pasaż handlowo-usługowy, a w przyszłości także publiczny taras z widokiem na panoramę miasta. Inwestorem i deweloperem kompleksu jest firma HB Reavis specjalizująca się w tworzeniu przestrzeni pracy, którą wyróżnia dbałość o ekologię, dobrostan użytkowników budynków oraz zastosowanie innowacyjnych technologii. Najwyższy z budynków, 53-piętrowy Varso Tower ma 230 metrów (do dachu), a wraz z iglicą aż 310 metrów. To obecnie najwyższy wieżowiec w Unii Europejskiej. Po ukończeniu budowy będzie bezpośrednio połączony z przejściem do Dworca Centralnego i stacji WKD. Dwa niższe budynki kompleksu Varso Place – Varso 1 i Varso 2 – mierzą 90 i 81 metrów. Zostały wynajęte w całości jeszcze przed ukończeniem budowy, które miało miejsce wiosną 2020 r. Na parterze znajduje się ogólnodostępny pasaż handlowy z licznymi lokalami gastronomicznymi oraz przydatnymi usługami – ich otwarcie planowane jest jeszcze w tym roku.

w budowie, ma zostać oddany do użytku za rok. Każda z części składowych projektu stanowi oddzielny system, współdziałający w częściach wspólnych zgodnie z opracowanym scenariuszem pożarowym.

Które części są wspólne?
Budynki komplesku Varso Place są połączone w części podziemnej – mają wspólny podziemny parking z infrastrukturą towarzyszącą oraz lobby na parterze z pasażem zadaszonym świetlikami. Od strony pożarowej, wygrodzeń pożarowych, detekcji pożaru, rozgłaszania komunikatów alarmowych to są dalej oddzielne strefy.

Jakie przyjęliście rozwiązania, aby utrzymać wysoki standard ochrony?
Obligatoryjnie jesteśmy zobowiązani przepisami, aby co dwa lata przeprowadzać ćwiczenia pożarowe. My wykonujemy je nawet częściej. Bardzo często, aby ćwiczenia były efektywne i maksymalnie edukacyjne, korzystamy z urządzeń zadymiajacych, aby wizualnie pozkazać użytkownikom, jak faktycznie przebiega ewakuacja, jak ograniczona może być przy tym widoczność. Oczywiście pokazy robimy używając dymu teatralnego, który nieco inaczej oddziaływuje niż dym powstajacy podczas pożaru. Mam tu na myśli temperaturę dymu, ilość szkodliwych substancji, etc.). Jednak to wystarcza, aby świadomość użytkowników budynku znacząco podnieść, a głównie o to chodzi. Tu dochodzi bardzo ważny czynnik – stosowanie materiałów, które w czasie pożaru nie emitują szkodliwych substancji lub je znacząco ograniczają. Dla wszystkich instalacji wymusiliśmy zastosowanie okablowania w izolacji bezhalogenowej, która podczas pożaru instalacji minimalizuje ryzyko emisji toksycznego dymu. Zastosowane zostały również materiały klasy co najmniej NRO (nierozprzestrzeniające ognia – przyp. red.), samogasnące albo trudno palące się.
Z różną częstotliwością przeprowadzamy kontrolę systemów detekcji pożaru, stałych urządzeń gaśniczych itd. W stałej gotowości utrzymujemy dźwigi pożarowe. Są one bardzo ważnym elementem bezpieczeństwa pożarowego w budynku, zwłaszcza w sytuacjach kryzysowych.
Prowadzimy również działania prewencyjne – zatrudniamy firmę specjalizującą się w kwestiach pożarowych. Jej zadaniem jest m.in. aktualizowanie instrukcji bezpieczeństwa pożarowego. W ciągu minionego roku na projekcie Varso 1 i Varso 2 instrukcje bezpieczeńswta pożarowego były aktualizowane kilkanaście razy w zwiazku z nowymi aranżacjami. Co miesiąc specjalista od spraw pożarowych odwiedza każdą część budynku i wykonuje inspekcję. W protokole zaznacza nieprawidłowości, które należy naprawić. Teoretycznie są to detale, np. mebel blokujący dostęp do hydrantu pożarowego, ale istotne z punktu widzenia bezpieczeństwa pożarowego.
W ślad za tymi raportami dział Property kontaktuje się z najecmą, aby doprowadzić do niezwłoczengo przywrócenia sytuacji do oczekiwanego stanu.

Najwyższy budynek kompleksu Varso Place, 53-piętrowy Varso Tower ma 230 metrów (do dachu), a wraz z iglicą aż

310
metrów

I najemcy stosują się do waszych wymagań?
Z najemcami nie mamy problemu. Staramy się ułatwiać im życie i główny nacisk kładziemy na informację. Wkrótce pierwszy raz przeprowadzimy ewakuację wspólnie z hotelem, ale i tu nie przewiduję problemów. Świadomość użytkowników rośnie i coraz więcej dobrych praktyk z Europy Zachodniej dociera do naszych nieruchomości.

Jak długo trwa ewakuacja budynku?
Trwa tyle czasu, ile jest potrzebne na wyprowadzenie wszystkich osób i zgromadzenie ich w miejscach zbiórki do ewakuacji. Czyli trzeba liczyć czas na opuszczenie pomieszczenia plus czas zejścia klatką schodową do wyznaczonego miejsca. Przebiega to trochę inaczej dla kondygnacji niskich, a inaczej dla kondygnacji wysokich. Akcja powinna być przeprowadzona w minutach, od 3–4 minut do 7–8. Zdania strażaków też są podzielone, ale główna część ewakuacji z zagrożonej strefy pożarowej nie powinna trwać dłużej niż 3–4 minuty.

Również w przypadku Varso Tower, gdzie mamy kilkadziesiąt kondygnacji?
Budynek jest podzielony na strefy pożarowe, które pokrywają się z wielkością piętra. W przypadku alarmu pożarowego ewakuujemy ludzi z miejsca zagrożenia, czyli z danej strefy pożarowej, przez niezagrożoną klatkę schodową. Po tym, gdy zgromadzą się w miejscu zbiórki, potwierdzamy, czy na pewno wszyscy już wyszli. Jeśli na danym piętrze została np. osoba niepełnosprawna, która zgodnie z procedurą powinna czekać w specjalnie wydzielonym przedsionku pożarowym, informuje się o tym strażaka, który ma ją sprowadzić. W całym budynku mamy zainstalowane specjalne przegrody pożarowe, one wydzielają bezpieczne miejsce oczekiwania na ewakuację, dając więcej czasu służbom ratowniczym na wyprowadzenie osób w nich się znajdujących.

Fot. HB Reavis

Budynek jest zakwalifikowany do klasy ogniowej ZL3, spełnia wszystkie wymagania stawiane tej klasie. W części mamy klasę ZL5. To determinuje wytrzymałość ogniową przegród czy drzwi.

Dotarcie na najwyższe piętra zabiera sporo czasu, tym cenniejszego, im większe zagrożenie pożarem występuje. Jak rozwiązaliście ten problem?
Budynek jest wyposażony w windy pożarowe, które są zarezerwowane dla osób prowadzących akcję gaśniczą. Może to być strażak, funkcjonariusz policji lub przedstawicieli wojska. Pozostałe windy są w momencie alarmu sprowadzane do bezpiecznej strefy, niezależnie od tego, czy wiozły pasażerów na górę, czy w dół. Nadawany jest przy tym komunikat głosowy, żeby ludzie wiedzieli, co się dzieje.
Może się też zdarzyć taka sytuacja, że z jakiegoś powodu, np. zadymienia klatki schodowej, nie można zejść w dół do bezpiecznej strefy. Wtedy należy udać się do góry i czekać na odpowiednie służby.
Informacje o stanie ewakuacji są na bieżąco zbierane w punkcie zbornym i przekazywane służbom ratowniczym. Jeśli po określonym czasie nie ma wszystkich osób z danego piętra, na miejsce wysyłany jest strażak, który korzysta właśnie z dźwigu pożarowego. Tu istotny jest czynnik czasu. Z danych statystycznych wynika, że pożar może się rozprzestrzeniać bardzo szybko, w ciągu zaledwie kilku minut.

Fot. HB Reavis

Straż Pożarna przygotowująca się do akcji ratowniczych – ćwiczenia przeprowadzone w styczniu 2021 r.

Utrzymanie bezpieczeństwa w kompleksie wieżowców o zwartej zabudowie w centrum miasta wymaga współpracy z Państwową Strażą Pożarną, prowadzenia szkoleń i zapewne zdobycia doświadczeń ze względu na imponującą wysokość budynku. Czy odbyły się już pierwsze szkolenia PSP w Varso Tower?

Oczywiście straż pożarna przygotowuje się do akcji ratowniczych. Często przeprowadzają ćwiczenia w budynku, nawet teraz, kiedy jest jeszcze w fazie budowy. W ten sposób zapoznają się z topografią obiektu, wykorzystują specjalne wozy obsługujące coraz większe wysokości, doposażają się w zewnętrzne linie gaśnicze, żeby dodatkowo móc podać środek gaśniczy: pianę lub wodę.

Takie ćwiczenia przeprowadziliśmy w styczniu br. Straż pożarna wykorzystała w nich mobilną pompę podającą środek gaśniczy pod ciśnieniem na wysokość ponad 200 m. Korzystali ze specjalnych węży, które ekipa ratowników górskich wciągała na górę. Trzeba pamiętać, że budynek w jakimś stopniu jest już przystosowany do tego, żeby przeciwdziałać rozprzestrzenianiu się pożaru: instalacja zraszająca, hydranty, klatki schodowe, przez które można ustawić linie gaśnicze. Może się okazać, że ilość podawanej wody trzeba zwiększyć, bo pożar jest wprawdzie opanowany, ale jeszcze nie ugaszony i trzeba podjąć dodatkowe działania.

Te pierwsze ćwiczenia trwały kilka godzin, bo najpierw służby rozpoznawały teren, przygotowywały się do akcji, opracowywały strategię działania itd. Teraz, po ćwiczeniach, strażacy już wiedzą, że np. muszą mieć przygotowane nie dwie baterie do wciągarki elektrycznej, ale więcej. W trakcie ćwiczeń okazało się bowiem, że na linę z wciąganym wężem działa wiatr. Na 200 m płaskiego węża i liny działa ogromna siła, której pokonanie wymaga od wciągarki większego poboru mocy i dlatego bateria szybciej się rozładowuje. Na tych ćwiczeniach strażacy mogli przetestować najlepsze miejsca do rozstawienia sprzętu. W warunkach bojowych nie będzie czasu, by się nad tym zastanawiać, wszystko musi być już z góry przećwiczone i ustalone.

Taka interwencja to jednak ostateczność. Nim do niej dojdzie, wykonuje się cały szereg czynności związanych z odebraniem sygnału o potencjalnym pożarze, których zadaniem jest opanowanie sytuacji – jakich?

Jeśli w obiekcie dojdzie do zdarzenia pożarowego, sygnał alarmowy jest odbierany w pomieszczeniu monitoringu. Gdy jest to alarm pierwszego stopnia, jest on rozpoznawany. Obsługa potwierdza, że taki komunikat do nich dotarł, i przez wciśnięcie przycisku uruchamia sekwencję weryfikacyjną. Jeśli jest to alarm fałszywy, odnotowuje się go w dzienniku zdarzeń i procedura się kończy. W przypadku alarmu drugiego stopnia, gdy więcej niż jedno urządzenie zasygnalizowało zdarzenie, uruchamiana jest wcześniej opracowana procedura: informujemy operatora, tłuczemy ROP-a, rozpoczynamy automatyczną ewakuację. Co pewien czas uruchamiamy komunikat głosowy, że nie są to ćwiczenia.

A co się dzieje, gdy sygnały o pożarze dotrą z dwóch stref?

„Przypadłością" systemów zabezpieczenia pożarowego jest to, że jeśli w jednej strefie zostanie uaktualniny system pożarowy, to już w kolejnej zlokalizowanej w innej części budynku, nawet na innych odalonych kondygnacjach, mamy do czynienia z uruchomieniem pełnego scenariusza pożarowego wraz z ogłoszeniem ewakuacji zagrożonych części budynku, bez możliwosci weryfikacji takiego alarmów.

Czy nie wystarczy naciśnięcie ROP-a, aby wywołać takie zamieszanie?

W Varso Palce naciśnięcie ROP-a wywołuje inną sekwencję zdarzeń. Uruchamiana jest wentylacja, powiadamiane są służby, ale nie ogłasza się ewakuacji. Naciśnięcie ręcznego ostrzegacza pożarowego zawsze musi zostać potwierdzone, bo ręczne uruchomienie może być przypadkowe, ale też moe to być celowe działanie. Biarąc to pod uwagę musimy być pewni, że jest to realne zagrożenie.

Ile osób fizycznie nadzoruje budynek pod względem bezpieczeństwa pożarowego?

Trudno uwierzyć, ale tylko cztery osoby ochrony fizycznej są przypisane do każdego budynku, które nadzorują go pod względem bezpieczeństwa. Jedna jest dedykowana do funkcji dowódcy zmiany, operatora systemów, druga zastępuje pierwszą w przypadku, gdy ta opuści posterunek, inna pełni funkcję patrolową, podczas obchodów kontroluje kluczowe punkty budynku, a kolejna obsługuje ruch dostaw, np. kurierów, dostawy towarów itp. Do nadzoru budynku pod kątem pożarowym są oddelegowane dwie osoby, wspierane przez systemy. Dużą pomoc stanowi wizualizacja budynku z zaznaczonymi miejscami instalacji elementów pożarowych.

Coraz popularniejsze stają się rozwiązania mobilne, pomagające pracownikom w jak najszybszym znalezieniu w obiekcie konkretnego elementu SSP. Niektóre z nich aktywnie nawigują pracowników po obiekcie, by mogli jak najszybciej dotrzeć do właściwego miejsca. Czy zamierzacie wdrożyć takie rozwiązania?

Nie inwestujemy w wyposażenie pracowników w elektroniczne systemy do automatycznego nawigowania, bo jest to kolejne urządzenie do noszenia, a obserwacja małego ekranu odwraca uwagę od tego, co dzieje się dookoła. Drugą kwestią jest to, że urządzenie nie zapewni komunikacji, a ona jest priorytetowa. Pracownik musi więc nieść kolejne urządzenie, a ma tylko dwie ręce. Ja preferuję taką filozofię, że osoba weryfikująca alarm ma jedno proste urządzenie, ewentualnie klucz do otwarcia konkretnego pomieszczenia w części wspólnej budynku czy np. do hydrantu.

Poza tym „naszpikowanie" budynku obligatoryjnymi instalacjami wymaga potężnych nakładów finansowych. Dodatkowy koszt w postaci systemów mobilnych nie zawsze jest opłacalny biznesowo.

Już kilkakrotnie padł przykład zastosowania instalacji wysokociśnieniowej. Czy jest to rozwiązanie wybrane tylko ze względu na wysokość budynku?

Jestem zwolennikiem wyposażania budynków o dużej kubaturze powyżej 20 tys. m^2 w instalacje wysokociśnieniowe z wielu powodów. Instalacje pożarowe kojarzą się nam z „brzydkim meblem", który przeszkadza i architektom, i najemcom. Instalacja wysokociśnieniowa charakteryzuje się wysoką kulturą wykonania ze względu na zastosowane materiały ze stali szlachetnej, małe średnice rur czy kompaktowy wygląd samej głowicy. Te elementy są delikatne i czasami tak ciekawe, że mogą stanowić dekorację. W porównaniu z tradycyjnymi, te instalacje nie zajmują dużych powierzchni budynku. Można więc komercyjnie wykorzystać większą powierzchnię użytkową.

Również jej część techniczna zajmuje mniej miejsca. Urządzenia są bardziej przyjazne, generują mniej hałasu, wibracji itp. Zbiorniki zapasów wody są dużo mniejsze, zamiast setek metrów sześciennych wystarczą dziesiątki. Ta instalacja dalej spełnia swoją funkcję, jest sprawna i wydajna. W dobie, kiedy mamy deficyt wody, zwłaszcza w Polsce i Europie, bezproduktywne jej magazynowanie jest niezrozumiałe. Okresowa konserwacja dużych zbiorników wiąże się z marnowaniem wielu metrów sześciennych wody. Nie jest to zgodne z poszanowaniem środowiska naturalnego.

A czy nie spotkaliście się z zarzutami klientów, że skoro jest mniej wody, to system jest mniej efektywny?

To tak, jakby zadać pytanie, czy mniejszy silnik w samochodzie oznacza, że ten samochód będzie wolniej jechał. Trzeba pamiętać, że na pożar mają wpływ trzy czynniki: materiał, który się pali, odpowiednio wysoka temperatura i dostęp tlenu. Mgła wodna obniża temperaturę pożaru i ogranicza dostęp tlenu, czyli oddziałuje na dwa z trzech czynników. Dodatkowo cząsteczki wody obniżają też próg palności takich materiałów, jak np. papier. A wiadomym jest, że mokry papier nie pali się tak łatwo, jak suchy. Oczywiście, jeśli pożar rozwinie się już znacząco i temperatura wzrośnie, to mgła wodna już nie wystarczy i trzeba podjąć dodatkowe działania.

Ale bezpieczeństwa pożarowego nie gwarantuje pojedynczy system. Na cały proces składa się wczesna detekcja i na tym etapie można już zacząć przeciwdziałać rozwojowi pożaru, np. gaśnicą. Równolegle mamy powiadomienie do służb. Jeśli nie pomogą działania gaśnicą i w danym miejscu wzrośnie temperatura, to uruchamiają się zraszacze. Będą one ograniczały rozprzestrzenianie się pożaru i dadzą czas służbom ratunkowym na dotarcie do miejsca zdarzenia.

Certyfikowany integrator pożarowy

CC WINGUARD od C&C Partners

Kwestia bezpieczeństwa powinna być uwzględniana przez każdego inwestora i właściciela takich obiektów, jak zakłady produkcyjne, przemysłowe, dworce, magazyny czy centra logistyczne. Mają one swoją specyfikę, różnią się także rodzajami zastosowanych rozwiązań, co trzeba mieć na uwadze, wybierając odpowiednie urządzenia przeciwpożarowe. Większą skuteczność działania, a więc i większy poziom bezpieczeństwa pożarowego obiektu zapewnia integracja wszystkich systemów ochrony przeciwpożarowej.

Najwyższy poziom zabezpieczenia obiektów, dzięki możliwości zarządzania systemami ochrony ppoż., zapewnia integrator CC WINGUARD. To system klasy Premium integrujący urządzenia przeciwpożarowe, zbudowany na bazie rozwiązania niemieckiej marki Advancis – WinGuard PSIM+. Integrator CC WINGUARD od C&C Partners spełnia obowiązujące wytyczne i normy, co potwierdzają świadectwa i certyfikaty wydane przez CNBOP-PIB.

INTEGRACJA BEZ KOMPROMISÓW

CC WINGUARD integruje systemy ochrony ppoż. oraz inne urządzenia i systemy 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.
Pełną funkcjonalność integracji urządzeń ppoż. mogą zapewnić jedynie systemy certyfikowane, które mają świadectwo dopuszczenia CNBOP-PIB. I takim właśnie systemem jest CC WINGUARD.

ZDEFINIOWANE PROCEDURY BEZPIECZEŃSTWA

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.

WIN-WIN, CZYLI KAŻDY WYGRYWA

CC WINGUARD to kopalnia możliwości i korzyści na wszystkich etapach inwestycji i użytkowania obiektu – zarówno na etapie projektowania, jak i podczas eksploatacji systemów ppoż. Projektant ma wreszcie możliwość zrealizowania koncepcji działania systemów ppoż., które dotąd mogły być jedynie pomysłem. Instalator samodzielnie wykona wszystkie prace związane z wdrożeniem i późniejszą konserwacją systemu. Operator zyska komfort pracy dzięki intuicyjności rozwiązania. Inwestor natomiast będzie dysponował najwyższym poziomem bezpieczeństwa, osiągając kompromis z wymarzoną architekturą wnętrza swojego budynku.

NAJWAŻNIEJSZE ZALETY SYSTEMU:

- ponad 25 lat doświadczenia producenta na rynku systemów pożarowych,
- niezależność od urządzeń wykonawczych w zakresie sterowań i monitorowań,
- integracja wszystkich stosowanych na rynku systemów sygnalizacji pożarowej,
- rozbudowany interfejs graficzny: możliwość tworzenia własnych, niezależnych grafik systemu,
- możliwość pełnego odzwierciedlenia pulpitu strażaka,
- niezależność w konfiguracji systemu, np. przez instalatora lub integratora,
- obsługa serwisowa i wsparcie techniczne realizowane bezpośrednio przez instalatora lub integratora.

Szczegółowych informacji udziela Leszek Schmidt, kierownik działu wsparcia technicznego w C&C Partners: l.schmidt@ccpartners.pl

Ergonomia i funkcjonalność

central ZETTLER PROFILE FLEXIBLE

Najnowsze trendy w projektowaniu budynków koncentrują się na dyskretnej estetyce i funkcjonalności. Centrale SSP ZETTLER PROFILE FLEXIBLE wyposażone w graficzny interfejs użytkownika doskonale wpasowują się w ten trend.

KOLOROWY EKRAN DOTYKOWY

System ZETTLER spełnia kluczowe wymagania użytkowników dotyczące intuicyjnych i łatwych w obsłudze systemów sygnalizacji pożarowej SSP. Kolorowy i przyjazny w użytkowaniu ekran dotykowy zastępuje wyświetlacz LCD i przyciski występujące w typowych centralach. Funkcja „INFO" zapewnia intuicyjną nawigację do obsługi operacji i zawiera pomoc kontekstową, która ułatwia użytkowanie.

WIZUALIZACJA STREFY DOZOROWEJ

Centrale SSP podlegają standardom normy EN54 w zakresie informacji o stanie urządzeń wyjściowych i sposobu ich prezentacji użytkownikowi. Częstym problemem napotykanym podczas alarmu pożarowego jest trudność w dotarciu do szczegółowych informacji, które pomagają operatorowi zlokalizować źródło alarmu pożarowego.
Centrala ZETTLER nie tylko w 100% spełnia wymagania normy EN54, ale także zmniejsza wyzwania związane z identyfikacją określonych komponentów i zdarzeń, przedstawiając użytkownikowi plan strefy dozorowej objętej alarmem pożarowym. Oszczędza to cenny czas w sytuacji alarmowej oraz umożliwia użytkownikom szybkie zdecydowane działanie.

DIODY LED

Centrale ZETTLER zapewniają szybki dostęp do informacji o stanie urządzeń wyjściowych i wydajności systemu poprzez odpowiednią diodę LED na panelu sterowania. Daje to użytkownikowi dostęp do przejrzystej informacji dotyczącej statusu systemu i możliwości sterowania funkcjami urządzeń z jednego interfejsu logicznego.

KATEGORYZACJA ZDARZEŃ W RÓŻNYCH KOLORACH

Tradycyjne centrale przeciwpożarowe wyświetlają różne informacje o systemie w jednym kolorze, co może utrudniać operatorom obsługę i określenie statusu. Centrale SSP ZETTLER podsumowują informacje systemowe w trzech kolorach: żółtym / czerwonym / niebieskim, wskazując odpowiednio trzy stany: błędu, izolacji, testu / pożaru / czuwania. Pozwala to użytkownikom uniknąć niepotrzebnego zamieszania i zidentyfikować na pierwszy rzut oka z dużej odległości aktualny status systemu.

ŁATWO DOSTĘPNY PORT USB

Centrale SSP ZETTLER łączą w sobie intuicyjny interfejs użytkownika i nawigację z ulepszoną konfiguracją USB. Dzięki temu operatorzy systemu mogą pobierać istotne informacje o stanie systemu w formie przejrzystych, sformatowanych raportów. Wbudowane funkcje bezpieczeństwa zapobiegają również niewłaściwemu wykorzystaniu tych informacji, wymagając identyfikatora użytkownika i hasła w celu uzyskania dostępu do systemu przez USB.

LOGOWANIE ZA POMOCĄ KARTY DOSTĘPU

Centrale SSP zazwyczaj wymagają klucza w celu uzyskania dostępu do systemu i obsługi podstawowych funkcji. Często powoduje to problemy praktyczne, ponieważ klucze mogą zostać pozostawione przy centrali SSP, narażając system na dostęp przez niepowołane osoby, zapomniane lub zgubione. Centrale ZETTLER Profile Flexible są wyposażone w czytnik kart RFID i umożliwiają logowanie za pomocą karty dostępu, spersonalizowanej dla poszczególnych użytkowników.

WYGASZACZ EKRANU

W czasie czuwania systemu na ekranie dotykowym pojawia się wygaszacz ekranu, który może być dowolnie konfigurowany. Dzięki tej funkcji panel wyniesiony systemu SSP, zlokalizowany w reprezentatywnym lobby czy recepcji budynku, nie rzuca się w oczy oraz umożliwia promocję własnego logo lub dowolnej treści, np. listy numerów alarmowych.

Integral IP MXF/MXE

Centrala sygnalizacji pożarowej i sterowania stałymi urządzeniami gaśniczymi

System sygnalizacji pożarowej i sterowania stałymi urządzeniami gaszenia to kluczowy system bezpieczeństwa w obiekcie budowlanym, dlatego szczególną uwagę należy zwracać na odpowiedni dobór urządzeń, które spełniają wszelkie wymagania techniczne i formalne w konkretnych zastosowaniach projektowych.

Centrala sygnalizacji pożarowej i sterowania stałymi urządzeniami gaśniczymi Integral IP MXF/MXE (MXF – CSP, MXE – CSG) to flagowy produkt systemu Integral IP, skonstruowany z naciskiem na maksymalne bezpieczeństwo, funkcjonalność i elastyczność, umożliwiający realizację nawet najbardziej skomplikowanych projektów w zakresie sygnalizacji pożarowej, sterowania urządzeniami gaśniczymi i innymi urządzeniami przeciwpożarowymi w obiekcie, spełniający wszystkie wymagania techniczne i formalne.

CENTRALA MA CERTYFIKATY I ŚWIADECTWA DOPUSZCZENIA CNBOP DO REALIZACJI NASTĘPUJĄCYCH FUNKCJI:

- centrala sygnalizacji pożarowej zgodnie z **PN-EN 54-2,**
- centrala sterująca stałymi urządzeniami gaśniczymi gazowymi zgodnie z **PN-EN 12094-1,**
- centrala sterująca stałymi urządzeniami gaśniczymi wodnymi, pianowymi i aerozolowymi zgodnie z Krajową Oceną Techniczną (KOT) CNBOP-PIB-KOT-2020/0228-1009.

W CNBOP-PIB zostały wykonane dodatkowe badania w zakresie sterowania stałymi urządzeniami gaśniczymi wodnymi, pianowymi i aerozolowymi dla 100-procentowego potwierdzenia wymagań formalnych, które są kluczowe dla bezpiecznego wdrożenia systemu w obiekcie i późniejszego formalnego odbioru instalacji i bezpiecznej eksploatacji. Architektura i elastyczność systemu Integral IP pozwala, aby funkcje systemu sygnalizacji pożarowej (SSP) i sterowania urządzeniami gaśniczymi (SUG) były realizowane przez jedno urządzenie lub przez

centrale pracujące w sieci, z możliwością rozdzielania funkcji sygnalizacji pożarowej i sterowania SUG na poszczególne centrale lub wyodrębnienia niezależnych podsystemów detekcji i gaszenia. Ponadto Integral IP MXE/MXF może być wykorzystywana do sterowania urządzeniami przeciwpożarowymi w systemach kontroli rozprzestrzeniania dymu i ciepła zgodnie z projektem normy prEN12101-9 oraz sterowania i nadzorowania w ramach instalacji wodociągowych przeciwpożarowych. Spełnia także wymagania w zakresie monitorowania instalacji tryskaczowych zgodnie z VdS CEA 4001. Centrala Integral IP MXE/MXF może realizować wszystkie powyższe funkcje jednocześnie, co czyni ją najbardziej uniwersalną centralą na rynku polskim.

Cechą charakterystyczną Integral MX jest pełna redundancja sprzętowa i programowa wszystkich podzespołów centrali, co pozwoliło na dopuszczenie jej do sterowania wielu niezależnych stref gaszenia lub rozbudowanych wielostrefowych systemów SUG. Redundancja wszystkich kart rozszerzeń, paneli wskazań i obsługi zapewnia najwyższy poziom bezpieczeństwa i niezawodną realizację procedur gaszenia jednocześnie dla wielu stref gaszenia – nawet w przypadku wystąpienia awarii systemowej.

Integral IP MXE/MXF jest centralą modułową, która, w zależności od wymagań, jest wyposażana w dobierany do konkretnego projektu osprzęt w postaci kart rozszerzeń, paneli obsługi i paneli wskazań LED do wizualizacji szczegółowych stanów pracy stref gaszenia, zgodnie z normą PN-EN 12094-1. Jest dostępna w różnych wersjach, zależnie od liczby obsługiwanych stref gaszenia (SG) i konkretnych wymagań projektowych.

Przykładowo można zastosować obudowę z wbudowanym panelem obsługi MAP i panelem wskazań dla 4 SG, albo obudowę z drzwiami pełnymi z wyniesionym panelem obsługi Integral MAP i panelami wskazań dla 8 SG podłączonymi poprzez zewnętrzną magistralę MMI-BUS. Standardowo pojedyncza centrala przewidziana jest do obsługi dziesięciu stref gaszenia. W przypadku bardziej rozbudowanych instalacji stałych urządzeń gaśniczych lub większej liczby gaszonych pomieszczeń centrale mogą pracować w sieci typu Integral LAN lub Integral WAN.

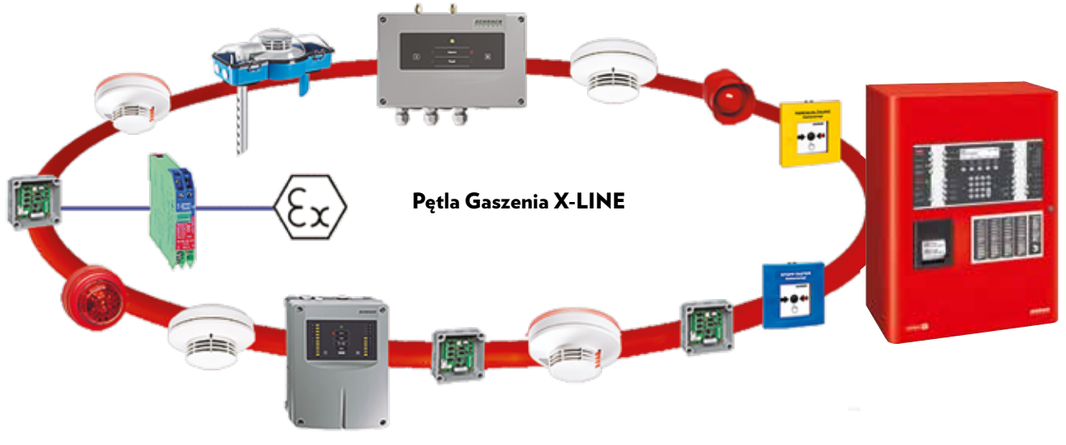
W podstawowej sieci systemowej typu Integral LAN może pracować do 16 central sterujących i nadzorujących do 32 stref gaszenia. W przypadku zastosowania sieci central możliwe jest elastyczne z punktu widzenia obsługi i zarządzania podejście do konfiguracji systemu – np. rozwiązanie, w którym wszystkie centrale są w wykonaniu z drzwiami pełnymi (bez paneli wskazań i obsługi), a w miejscu stałego dozoru instalowany jest centralny wyniesiony panel wskazań i obsługi Integral MAP wraz z wyniesionymi panelami wskazań dla 8 SG, których liczba jest adekwatna do liczby stref gaszenia. W przypadku większej liczby central lub stref gaszenia stosuje się sieć wyższego poziomu typu Integral WAN, która łączy ze sobą sieci podstawowe Integral LAN w spójny system sieciowy.

Od strony projektowej sieć Integral LAN może być przeznaczona do zabezpieczenia całego budynku w zakresie sygnalizacji pożarowej i gaszenia albo może być wdrożony podział funkcji detekcji i gaszenia na osobne sieci central. Przy takim podziale kompetencji jedna sieć to centrale realizujące funkcje detekcji i sterowania urządzeniami przeciwpożarowymi w budynku, druga zaś to centrale sterujące SUG, pełniące funkcję detekcji i sterowania instalacjami gaśniczymi.

Dzięki połączeniu cyfrowym centrale wymieniają miedzy sobą szczegółowe informacje, co wyróżnia to rozwiązanie na tle połączeń tzw. twardodrutowych poprzez interfejsy wejścia/wyjścia, gdzie przesyłane są tylko podstawowe informacje, a ponadto nie ma możliwości centralnego zarządzania wszystkimi centralami. Natomiast sieć Integral WAN łączy ze sobą ww. sieci Integral LAN w spójny system, który pozwala na centralną obsługę z jednego lub wielu stanowisk obsługi, zależnie od wymagań Inwestora. Podział systemu na osobne systemy detekcji lub gaszenia czy systemy sieci Integral LAN zabezpieczające określone obszary obiektu umożliwia od strony inwestycyjnej i organizacyjnej wdrożenie poszczególnych (pod)systemów przez różne zespoły, a nawet firmy instalatorskie.

Prace instalacyjne, podobnie jak serwis i konserwacja instalacji, mogą być realizowane niezależnie dla każdego podsystemu przez firmy specjalizujące się w danej dziedzinie. Od strony organizacyjnej ważne, by jedna z firm pełniła funkcję wiodącą, odpowiadając za integrację podsystemów we wspólny system Integral WAN. Zastosowanie systemu rozproszonego Integral WAN pozwala na zintegrowanie w jednym systemie wielu tysięcy stref gaszenia.

Centrala Integral IP MX jest bardzo elastyczna również w zakresie podłączania elementów peryferyjnych obsługujących strefę gaszenia – dzięki zastosowaniu technologii X-LINE stre-



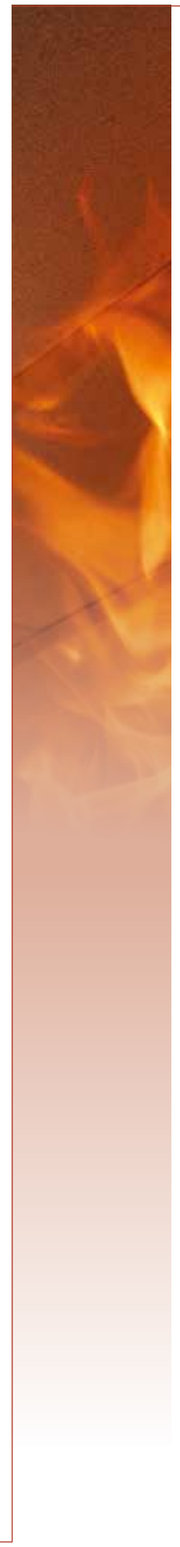
fę gaszenia mogą obsługiwać elementy podłączone standardowo w formie linii otwartych lub jednej linii pętlowej, tworząc tzw. pętlę gaszenia. Na jednej linii X-LINE instalowane są (w zależności od wymagań projektu) interaktywne czujki wielokryteriowe CUBUS MTD533X, czujki zasysające ASD 53x, przyciski uruchomiające i wstrzymujące gaszenie czy moduły wejścia/wyjścia do sterowania i nadzorowania urządzeń biorących udział w procedurze gaszenia – klapy przeciwpożarowe wentylacji bytowej, klapa odciążająca, sygnalizacja optyczna i akustyczna itp.

Zastosowanie linii pętlowej i wbudowane obustronne izolatory zwarć w każdym elemencie zapewniają ciągłość działania wszystkich urządzeń na wypadek wystąpienia przerwy lub zwarcia. Od strony projektowej mogą być też stosowane wydzielone funkcyjnie pętle. Wówczas jedna pętla odpowiada za funkcję detekcji, a druga za sterowanie (np. przycisk START Gaszenie /STOP Gaszenie), wysterowanie i monitorowanie urządzeń. Obwody sterujące zaworami instalacji gaśniczych są bezpośrednio podłączone do kart wyjść w centrali lub (opcjonalnie) do modułów wyjścia nadzorowanego BX-IOM. W przypadku takiego rozwiązania ważne jest zapewnienie wydzielonych zasilaczy zewnętrznych na potrzeby realizacji sterowania gaszeniem. W ofercie Schrack Seconet dostępne są również urządzenia peryferyjne w wykonaniu specjalnym do obsługi gaszenia w obszarach zagrożonych wybuchem (EX).

Po zainstalowaniu urządzeń wchodzących w skład instalacji gaśniczych wymagane jest właściwe uruchomienie systemu zgodnie ze scenariuszem pożarowym i zaprojektowaną procedurą gaszenia. Dla ułatwienia procesu konfiguracji i programowania systemu gaszenia producent przygotował specjalny moduł projektowo-programowy Asystent Gaszenia, który pozwala zdefiniować w sposób graficzny, w postaci schematu blokowego całą procedurę gaszenia i powiązania między wszystkimi elementami, a następnie wygenerować odpowiednią konfigurację ustawień dla wszystkich elementów logicznych systemu. Po zdefiniowaniu konfiguracji projektowej w Asystencie Gaszenia generowane są do wszystkich elementów wejścia i wyjścia szczegółowe ustawienia oraz definicje sterujące oparte na operatorach logiki Boole'a. Odbywa się to zarówno dla pojedynczych stref, jak i rozbudowanych wielostrefowych systemów gaszenia. Przed zaprogramowaniem systemu kryteria sterujące można przetestować w samym oprogramowaniu za pomocą symulatora i testera algorytmów sterujących.

Wykorzystanie bramek logicznych daje praktycznie nieograniczone możliwości wykonywania najbardziej złożonych algorytmów sterujących. Różne zależności między kryteriami wejściowymi a wykonywanymi sterowaniami pozwalają na spełnienie wszelkich wymagań formalnych i dodatkowo wprowadzenie ponadstandardowych funkcji specjalnych i bezpieczeństwa. System umożliwia programowanie specjalnych funkcji bezpieczeństwa obsługi, które uzależniają wykonanie operacji sterowania od stanu systemu i kompetencji (autoryzacji) użytkownika obsługującego system. Wyjścia krytyczne, które sterują gaszeniem, są specjalnie zabezpieczane przed ich przypadkowym uaktywnieniem.

Weryfikacja poprawnego działania skonfigurowanego systemu jedno- czy wielostrefowego poprzez praktyczne sprawdzenie jest gwarancją bezpiecznego wdrożenia i późniejszego użytkowania. Sprawdzenie algorytmu sterującego można wykonać na działającym systemie bez fizycznego uruchamiania wyjść sterujących, aby potwierdzić skuteczność wykonanej instalacji zgodnie z założeniami scenariusza i matrycy sterowań. Specjalna funkcja zamrażania wyjść (blokowania) pozwala na taką bezpieczną weryfikację, bo chroni przed przypadkowym uruchomieniem instalacji i wyzwoleniem środka gaśniczego. Centrala lub cały system sieciowy realizuje logicznie zawarty scenariusz bez uaktywnienia wyjść sterujących, co pozwala na szybką weryfikację sprawności działania wykonanego systemu. Rozkazy sterujące mogą być również przesyłane w ramach sieci central Integral LAN/Integral WAN, umożliwiając elastyczne powiązanie funkcji systemu sygnalizacji pożarowej i systemu sterowania gaszeniem.



Przykładem projektowym może być realizacja procedury ręcznego sterowania podawaniem środka gaśniczego w postaci pian i oddzielnie wody w dwóch różnych lokalizacjach. Algorytm może uwzględniać brak możliwości jednoczesnego sterowania w dwóch lokalizacjach i/lub brak możliwości równocześnie podawania piany i wody. Możliwe jest wdrożenie bardzo skomplikowanych algorytmów sterowania, np. wieloma zaworami gaśniczymi w układach sekwencyjnych, sterowania w zależnościach czasowych, z wzajemnym blokowaniem i układami rezerwy oraz dodatkowymi kryteriami, które wynikają ze specyfiki obiektu i wymagań użytkownika. Dzięki przebadaniu centrali Integral IP MX jako centrali sterującej różnymi urządzeniami przeciwpożarowymi, w tym urządzeniami w ramach systemów kontroli rozprzestrzeniania dymu i ciepła w jednym systemie, można zaprogramować całą matrycę sterowań, która będzie spójna dla wszystkich spodziewanych przypadków.

Bardzo ważną funkcją central sterowania gaszeniem serii Integral IP jest ścisła współpraca z systemem integrującym urządzenia przeciwpożarowe SIS-FIRE, który może być wykorzystywany do nadzoru i obsługi stref gaśniczych, w tym do ręcznego uruchamiania i wstrzymywania procedury gaśniczej. Ponadto dzięki integracji z Integral IP za pomocą protokołu systemowego ISP-IP i ścisłej współpracy jest możliwość odczytu dodatkowych informacji technicznych z systemu (np. aktualna temperatura, poziom CO, sygnał o zadymieniu z czujek pożarowych serii CUBUS) czy takich, jak parametry przepływu powietrza w czujkach zasysających ASD 53x. Podnosi to jeszcze poziom bezpieczeństwa, ponieważ niewłaściwe stany pracy mogą być wykrywane nie tylko w samej instalacji Integral IP, ale też w innych urządzeniach i instalacjach w ramach nadzorowanych obszarów gaszenia i całego obiektu (np. niepoprawna praca systemu klimatyzacji pomieszczenia gaszonego).

Dobór urządzeń sterujących i nadzorujących do instalacji sterowania SUG, które spełniają wszelkie wymagania techniczne i formalne, jest gwarancją bezpieczeństwa pożarowego obiektów dla wszystkich interesariuszy rynku bezpieczeństwa pożarowego.

SCHRACK SECONET POLSKA

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

Zabezpieczenia pożarowe

w obszarze IK

Obiekty infrastruktury krytycznej (IK) powinny być wyposażone w ponadnormatywne systemy zabezpieczeń, w tym przede wszystkim bezpieczeństwa pożarowego. Kluczowy charakter zadań sprawodza się nie tylko do zapewnienia ochrony przed zagrożeniami, ale też do tego, by ewentualne uszkodzenia czy zakłócenia w funkcjonowaniu trwały jak najkrócej, były łatwe do usunięcia oraz nie wywoływały dodatkowych strat dla człowieka i przedsiębiorstwa.

Już na etapie projektowania należy określić wszelkie potencjalne zagrożenia i w odpowiedzi na nie przewidzieć właściwe systemy zabezpieczeń. W obiektach IK bardzo ważne jest odpowiednie pokierowanie akcją ratowniczo-gaśniczą, której nieodzownym elementem jest bezbłędne wykonanie zaprogramowanych wcześniej, zgodnie ze scenariuszem pożarowym, sterowań urządzeniami biorącymi udział w akcji pożarowej.

System detekcyjny – bezpośrednio odpowiedzialny za błyskawiczne wykrycie zarzewia ognia – powinien stanowić wydzieloną, samodzielną część układu systemu bezpieczeństwa pożarowego obiektu.

Za realizację scenariusza pożarowego, czyli za realizację algorytmu (programu) sterującego, powinno odpowiadać wyspecjalizowane certyfikowane urządzenie, jakim jest centrala sterująca urządzeniami pożarowymi (CSUP). Centrala taka wykonuje najbardziej skomplikowane programy sterujące, których inicjacja rozpoczyna się w momencie otrzymania sygnału o zagrożeniu pożarowym z centrali sygnalizacji pożarowej.

Sterowanie przeciwpożarowe z poziomu centrali typu FPM+ pozwala na zintegrowane zarządzanie dowolnymi systemami ppoż. różnych producentów: systemy wentylacji ppoż., systemy odcięć pożarowych, systemy wspomagające ewakuację itp. Nasza technologia działa jako niezależny system sterowania urządzeniami ppoż. lub może być zintegrowana z dowolnym systemem BMS czy PSIM, np. GEMOS – co oczywiście zalecamy i promujemy.

Tylko pełna integracja systemów bezpieczeństwa pozwala na zbieranie, przetwarzanie i analizowanie informacji niezbędnych do właściwego zarządzania obiektem i niezwłocznego reagowania na zagrożenia.

Widzimy konieczność zapewnienia pełnej kontroli, monitorowania, raportowania, a więc i wizualizacji systemów i urządzeń ppoż. poprzez system integrujący urządzenia przeciwpożarowe (SIUP).

Pełna integracja, kontrola i błyskawiczne raportowanie mogących wystąpić usterek lub uszkodzeń podczas normalnej eksploatacji obiektu mają decydujący wpływ na to, jak zachowa się system ppoż. podczas realnego zagrożenia. Integracja to także możliwość dokonywania analizy potencjalnych słabych punktów i natychmiastowa informacja o wykrytych awariach i usterkach. Gromadzone dane można przetwarzać na wiele sposobów i przedstawiać je w formie najbardziej czytelnej dla każdej grupy zainteresowanych.

Sterowanie i nadzorowanie pracy wszystkich urządzeń i systemów w budynku, które będą uruchomione przez FPM+ w wypadku zagrożenia pożarem, ułatwia kontrolę nad wszystkimi urządzeniami ppoż., zwiększając tym samym poziom bezpieczeństwa pożarowego budynku, co bezpośrednio dotyczy ogólnie pojętego zabezpieczenia obiektów IK. FPM+ zapobiega rozprzestrzenianiu się ognia i przyspiesza ewakuację przebywających w budynku osób. Modułowa budowa FPM+ pozwala na szybkie stworzenie rozproszonej instalacji, opartej na centrali Fire Matrix. System jest wyjątkowo elastyczny w konfiguracji i można go bez przeszkód rozbudowywać, gdy nastąpi taka potrzeba.

Celem zarządzania kryzysowego jest zapobieganie sytuacjom kryzysowym, zapewnienie sprawności struktur decyzyjnych na każdym szczeblu zarządzania, ciągłej gotowości sił i środków do podjęcia działań oraz sprawne reagowanie i likwidacja skutków zaistniałej sytuacji. FPM+ idealnie wpisuje się w te zadania, podnosząc poziom bezpieczeństwa w obiektach, dając profesjonalne narzędzie pracownikom ochrony, którzy bronią dostępu do obiektów, urządzeń, instalacji lub usług infrastruktury krytycznej.

ELA-COMPIL

ul. Szczepanowskiego 8
60-541 Poznań
office@ela.pl
https://ela.pl

Więcej mocy z PoE!

O standardzie IEEE802.3bt

Power over Ethernet (PoE), technologia zdefiniowana w standardach IEEE 802.3af i 802.3at, umożliwiająca jednoczesne dostarczanie zasilania i danych do urządzeń IP za pośrednictwem istniejącego połączenia sieciowego, doczekała się nowej wersji. Standard IEEE 802.3bt pozwala na przekazywanie znacznie większej mocy i wprowadza nowe funkcje, które zmienią sposób, w jaki patrzymy na PoE.

Jan T. Grusznic

Technologia PoE zrewolucjonizowała światowy rynek sieciowy, zapewniając przesyłanie danych i zasilania jednym przewodem ethernetowym. Przełączniki PoE stanowią idealne rozwiązanie w wielu aplikacjach, zmniejszając koszty wdrożenia i wymagania dotyczące okablowania, zapewniając znacznie większą niezawodność. Pomimo ciągłego wzrostu liczby urządzeń przystosowanych do tej technologii jej szersze wykorzystanie było ograniczone w dwóch aspektach: moc (szeroko rozumiana) i prędkość transmisji.

Prace nad nowym standardem trwały od 2009 r. Ich efektem był dokument normatywny IEEE 802.3bt, zatwierdzony 9 lat później przez komitet normalizacyjny. Trzykrotnie większa moc zasilania urządzeń brzegowych (w porównaniu ze standardem IEEE 802.3at) oraz obsługa prędkości transmisji do 10Gb/s w przypadku urządzeń sieciowych podłączonych za pośrednictwem przewodu Cat5e stanowią kamienie milowe dla tej technologii.

Jednak zmiany w IEEE 802.3bt nie ograniczają się wyłącznie do mocy zasilania, ale idą dużo dalej i dotyczą kompleksowego zarządzania energią, np. przez zmianę czasu sygnatury utrzymania zasilania (MPS – *Maintain Power Signature),* automatyczną klasyfikację *(Autoclass)* czy wprowadzanie pojedynczej i podwójnej sygnatury urządzeń zasilanych (PD – *Powered Device).*

SYGNATURA UTRZYMANIA ZASILANIA (MPS)

MPS określa minimalne zużycie energii przez PD zapewniające jego działanie i zapobiegające odłączeniu przez urządzenie zasilające (PSE – *Power Sourcing Equipment).* Gdy sygnatura MPS nie zostanie dostarczona przez co najmniej 400 ms, PSE ma za zadanie odłączyć napięcie (w odłączonych przewodach nie ma zasilania). Krótki MPS pozwala PD osiągnąć znacznie niższą moc w stanie czuwania w porównaniu z poprzednimi standardami. Minimalna moc w trybie czuwania została zredukowana do 1/10 tego, na co pozwalają standardy af[1] i at[2] (20 mW w porównaniu z 200 mW). Dzięki temu urządzenia IoT mogą być zasilone przez PoE z zachowaniem akceptowalnej wydajności w trybie czuwania.

W systemie oświetleniowym, który jest bodaj największym beneficjentem zmian w technologii PoE, istotne jest nie tylko zredukowanie poboru prądu przez PD w stanie aktywnym, ale też w trybie *standby.* W standardach PoE af i at wyłączenie światła w budynku nadal wymaga uruchomienia trybu MPS przez zasilane urządzenie, które pobiera prąd 10 mA przez 20% czasu. W trybie MPS urządzenie PD powiadamia urządzenie PSE, że jest wciąż podłączone, choć tylko w trybie *standby.* W efekcie średni pobór prądu w trybie MPS dla af i at wynosi 2 mA. Nowy standard 802.3bt przewiduje, że w trybie MPS czas zostanie zredukowany do 1,875%, a zatem średni pobór prądu wyniesie zaledwie 0,2 mA[3]. Będzie to miało duże znaczenie w takich zastosowaniach, jak oświetlenie LED, kiedy duża liczba urządzeń jest wyłączana w nocy i w weekendy.

AUTOMATYCZNA KLASYFIKACJA

Automatyczna klasyfikacja pozwala na optymalizację przypisania mocy udostępnianej przez PSE do PD. Urządzenie zasilające „mierzy" straty w kablu Ethernet i zużycie energii przez podłączone urządzenie zasilane w zdefiniowanym okresie, stąd „wie", jaką „faktyczną" moc należy dostarczyć do niego, a nie wyższą „przypisaną" na podstawie klasy urządzenia zasilanego. Dzięki temu PSE może zasilać większą liczbę urządzeń z ograniczonego budżetu PoE.

Wszystkie urządzenia PoE (PSE lub PD) w ramach standardu są interoperacyjne[4], a jedynym ograniczeniem współpracy jest to, że PD o zapotrzebowaniu na dużą moc jej nie otrzyma, gdy PSE jest starszej generacji lub niższej klasy. W ramach standardu 802.af są trzy klasy zapewniające maksymalnie 12,95 W na urządzeniu PD. IEEE 802.3at wprowadził czwartą klasę, zapewniającą 25,5 W na PD. Nowy standard IEEE 802.3bt rozszerza je o cztery nowe klasy, podnosząc poziom mocy do 51 W dla PD typu 3. i do 71,3 W dla PD typu 4. *(rys. 1).*

POJEDYNCZA I PODWÓJNA SYGNATURA PD

Standard IEEE 802.3bt obsługuje dwie konstrukcje urządzeń zasilanych: jednosygnaturowe i dwusygnaturowe. Urządzenie zasilające musi obsługiwać zarówno jedno-, jak i dwusygnaturowe PD. Urządzenia dwusygnaturowe obsłu-

1) Skrót od IEEE 802.3af
2) Skrót od IEEE 802.3at
3) https://elektronikab2b.pl/technika/50813-dobor-wlasciwego-standardu-power-over-ethernet-do-inteligentnych-przemyslowych-systemow-oswietleniowych-led 23/03/2021
4) Zapewniają pełną współpracę między produktami, niezależnie od producenta.

Rys. 1. Poziomy mocy zdefiniowane przez standard IEEE802.3bt i odniesienie do istniejących standardów PoE

	Typ 1 (802.3af) Typ 2 (802.3at)						Typ 4 (802.3bt)	
PSE	Class 1 4 W	Class 2 7 W	Class 3 15.4 W	Class 4 30 W	Class 5 45 W	Class 6 60 W	Class 7 75 W	Class 8 90 W
	ZASILENIE NA 2 PARACH (Typ 1 i Typ 2) ZASILANIE NA 2 LUB 4 PARACH (Typ 3 i Typ 4)				ZASILENIE NA 4 PARACH			
PD	Class 1 3.84 W	Class 2 6.49 W	Class 3 12.95 W	Class 4 25.5 W	Class 5 40 W	Class 6 51 W	Class 7 62 W	Class 8 71.3 W

gują zastosowania wymagające takiej samej mocy maksymalnej, jak jednosygnaturowe, lecz zapewniają większą elastyczność różnych i izolowanych konfiguracji obciążenia.
Dobrym przykładem urządzenia dwusygnaturowego jest zewnętrzna kamera IP typu PTZ, wymagająca zasilania modułu kamerowego i modułu grzewczego (lub chłodzącego) ze względu na ekstremalne warunki środowiskowe. Kamera ta jest dostarczana z *midspanem*[5] zapewniającym moc dla urządzenia powyżej możliwości standardu PoE at. Takie rozwiązania, znane pod różnymi nazwami *(Universal PoE, High PoE* i *PoE++),* będziemy spotykać coraz rzadziej, bowiem standard IEEE 802.3bt definiuje moc maksymalną dostarczaną przez PSE jako 90 W, a moc odbieraną przez PD jako 71,3 W. Ten maksymalny spadek mocy o 18,7 W pomiędzy urządzeniem zasilającym a zasilanym wynika ze strat na całej długości przewodu (zdefiniowanego standardem Ethernet) równej 100 m.
Urządzenie zasilane pracujące w standardzie bt[6] jest w stanie zmierzyć rezystancję przewodu, obliczyć straty mocy w kablu i określić moc wystarczającą do skompensowania maksymalnej mocy rozpraszanej na kablu o długości 100 m. Co ciekawe, jeżeli odległość między PD a PSE jest mniejsza niż 100 m, urządzenie zasilane może otrzymać moc większą niż 71,3 W[7].

KLASYFIKACJA OBOWIĄZKOWA

Zaszła również zmiana zasad PSE w zakresie klasyfikacji sprzętowej. O ile PSE typu 2. nie były zobowiązane do obsługi pełnej klasyfikacji sprzętowej i mogły zamiast tego korzystać z LLDP[8] (protokół łącza danych[9]) w celu zapewnienia urządzeniu PD pełnej mocy, o tyle z nastaniem standardu IEEE 802.3bt jest to już wymóg. Protokół LLDP jest nadal wykorzystywany przez urządzenia PD do szczegółowego określania ich zapotrzebowania na moc. Otrzymał zresztą zestaw nowych definicji w ramach IEEE 802.3bt, które umożliwiają wymianę informacji nt. 4-parowej zdolności PD, Autoklasy, maksymalnej mocy, jaką dysponuje PSE, czasowego wyłączenia PD, pomiarów napięcia/prądu/mocy/energii, a nawet wymianę informacji o cenie energii elektrycznej.

5) Urządzenia PoE instalowane między przełącznikiem sieciowym a urządzeniami sieciowymi, które muszą być zasilone przez okablowanie ethernetowe. Urządzenie *midspan* jest przezroczyste dla komunikacji TCP/IP.
6) Skrót od IEEE 802.3bt.
7) https://www.digikey.pl/en/articles/power-over-ethernet-poe-ieee-802-3bt-standard-boosts-technology-iot-applications 26/03/2021
8) LLDP jest protokołem neutralnym, jeśli chodzi o dostawców sprzętu do przedstawiania tożsamości urządzenia i jego funkcji.
9) Protokół 2. warstwy z 7-warstwowego modelu ISO/OSI.

WIĘKSZA MOC, POWAŻNIEJSZY PROBLEM

Oprócz podkreślania niewątpliwych zalet nowego standardu pojawiły się uwagi co do nowej wersji technologii PoE. Są one związane z coraz wyższą mocą, a w konsekwencji coraz bardziej realnym problemem przegrzewania przewodów. A to z kolei może się przekładać na niestabilność łącza i krótszą żywotność okablowania. Producenci i konsorcja techniczne pracowały nad oceną wpływu termicznego dostarczania 100 W mocy przez 4-parowe przewody PoE. Przegrzanie okablowania skutkuje m.in. wzrostem tłumienności i w efekcie pogorszeniem jakości transmisji danych. Wzrost temperatury prowadzi do przedwczesnego starzenia się materiałów płaszczowych kabla.
W przypadku długotrwałej eksploatacji w wysokiej temperaturze płaszcz zewnętrzny może ulec uszkodzeniu i wpłynąć na konstrukcję wewnętrzną, naruszając równowagę skrętki i powodując spadek jej parametrów elektrycznych[10]. Co prawda norma TSB-184-A Stowarzyszenia Przemysłu Telekomunikacyjnego (TIA) zawiera wytyczne dotyczące instalacji kabli w systemach stosujących technologię PoE – zaleca, aby temperatura kabla nie przekraczała 15°C w środku wiązki, ale nie rozwiązuje w pełni problemu[11]. W Internecie dostępne są liczne publikacje

10) https://community.fs.com/blog/how-to-avoid-overheating-in-poe-cabling.html 26/03/2021
11) https://planetechusa.com/heat-concerns-when-powering-a-poe-device/ 26/03/2021

NOWY STANDARD POWER OVER ETHERNET 802.3BT JEST TRZECIĄ WERSJĄ SZEROKO PRZYJĘTEJ NORMY IEEE, KTÓRA OKREŚLA PRZESYŁ ENERGII NISKIEGO NAPIĘCIA DO URZĄDZEŃ SIECIOWYCH. PIERWSZY STANDARD IEEE POE, 802.3AF ZAPEWNIA 12,95 W URZĄDZENIOM, IEEE 802.3AT ZWIĘKSZA TEN LIMIT DO 25,5 W. W STANDARDZIE 802.3BT ILOŚĆ MOCY DOSTĘPNEJ DLA URZĄDZEŃ WZRASTA PRAWIE TRZYKROTNIE, DO 71,3 W, UMOŻLIWIAJĄC TWORZENIE NOWYCH APLIKACJI

Rys. 2. Użycie logo Gen1 i Gen2 EA z certyfikatem EA upraszcza identyfikację produktów PoE zaprojektowanych zgodnie ze standardami IEEE 802.3 PoE i zwiększa pewność użytkownika, że produkty PoE będą współpracować ze sobą od wielu producentów

Źródło: https://ethernetalliance.org/poecert/

rekomendujące ograniczenie wzrostu temperatury przez zastosowanie przewodów o niższej rezystancji w celu zmniejszenia tłumienności (wyższe kategorie kabla niż Cat5e), użycie mniejszej liczby przewodów w każdej wiązce lub tylko częściowe zasilanie PoE w obrębie wiązki kablowej[12].

POTRZEBA CERTYFIKACJI

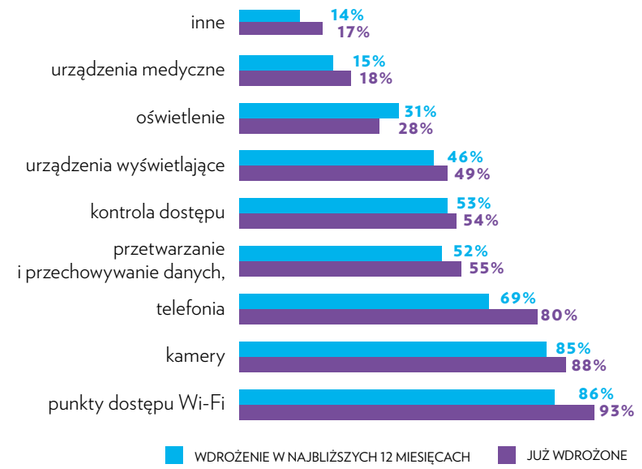
Standardy af, at i bt są jasno powiązane z technologią Power over Ethernet, natomiast samo określenie PoE nie jest zastrzeżone dla żadnego konkretnego podmiotu lub organizacji, przez co na rynku pojawia się wiele produktów wyposażonych w tę funkcjonalność, ale o całkowicie odmiennych specyfikacjach. Różni producenci stosują własne implementacje tej technologii, nie zawsze wzajemnie kompatybilne. Można wymienić rozwiązania *ePoE, Passive Poe* czy choćby *Long Range PoE*. Propozycję szczegółowej specyfikacji technologii PoE opublikowano w dokumencie *IEEE Ethernet Standard, 802.3-2015* – Rozdział 33. – *Data Terminal Equipment (DTE) Power via Media Dependent Interface (MDI).* Sam termin nie został wprawdzie wspomniany we właściwym tekście dokumentu, umieszczono go jednak w wykazie słów kluczowych.
Bazując na treści tego dokumentu, opracowano program certyfikacji urządzeń PoE, będący odpowiedzią na potrzeby rynku związane z rosnącą popularnością tej technologii. Autorem inicjatywy jest Ethernet Alliance, organizacja założona przez producentów sprzętu sieciowego[13], mająca na celu wspieranie rozwoju technologii Ethernet. Nadawany przez nią certyfikat PoE stwierdza, że urządzenie spełnia wymogi standardu IEEE 802.3.
To ważna dla użytkownika informacja, ponieważ w dużym stopniu gwarantuje brak kłopotów z kompatybilnością i interoperacyjnością produktu w środowisku sieciowym. Urządzenia o specyfikacji całkowicie lub częściowo niezgodnej ze standardem IEEE 802.3 mogą zakłócać pracę całej sieci np. z powodu braku ograniczeń prądowych, nieodpowiedniego napięcia zasilania lub niezgodności innych podstawowych parametrów elektrycznych.
Potwierdzeniem uzyskania certyfikacji PoE jest umieszczone na produkcie logo z oznaczeniem Ethernet Alliance *(rys. 2).* Stosuje się dwa rodzaje oznaczeń dla odmiennych grup produktów: PD oraz PSE. Kategoria PSE zawiera urządzenia mogące być źródłem zasilania w sieci (np. przełącznik sieciowy), zaś terminem PD oznacza się wszystkie układy wykorzystujące port Ethernet do zasilania urządzenia. Umieszczone w logo oznaczenie liczbowe informuje też o poziomie maks. poboru prądu. Jeśli liczba umieszczona na PSE jest większa lub równa liczbie umieszczonej na PD, użytkownik może mieć pewność, że odbiornik będzie prawidłowo zasilany[14].

Certyfikacja nie należy jednak do najtańszych – dla członków stowarzyszenia opłata wynosi 1000 USD za urządzenie. Niewątpliwie wpływa to na niewielką liczbę tylko 87 certyfikowanych produktów[15].
Z obserwacji trendów rynkowych wynika, że metoda PoE staje się standardem zasilania większości urządzeń budynkowych, zmieniając je w tzw. *smart buildings.* IEEE 802.3bt poważnie zmienia optykę spojrzenia na technologię Power over Ethernet, dopuszczając rozwiązanie do powszechnego zasilania tabletów, telefonów, komputerów czy oświetlenia, umożliwiając efektywny sposób zarządzania nimi.

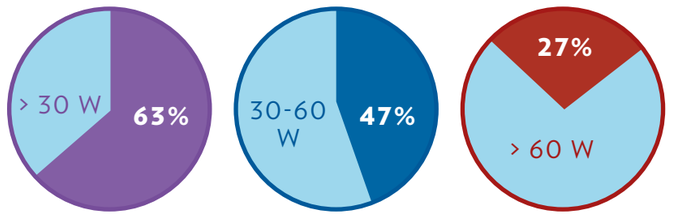
Trudno nawet wymienić wszelkie możliwe zastosowania metody PoE w życiu codziennym. Za przykład wystarczy podać Adapter firmy Microchip, który, przyjmując 90 W po PoE, dostarcza na wyjściu USB-C moc 60 W zasilającą większość urządzeń wykorzystujących USB-C do zasilania wejściowego. Adapter taki upraszcza instalację, czyniąc ją mniej zależną od infrastruktury prądu przemiennego. Bez zależności od gniazdka sieciowego nie ma już ograniczenia zasięgu do 3 m, a moc może być dostarczana na dalsze odległości.

12) https://www.5gtechnologyworld.com/what-every-engineer-should-know-about-ieee-802-3bt-poe/ 26/03/2021
13) m.in. Cisco, Hewlett Packard, Marvell Semiconductors, Intel, Broadcom, Juniper
14) https://elektronikab2b.pl/biznes/35031-wzrost-popularnosci-technologii-poe-wymusza-potrzebe-jej-standaryzacji 26/03/2021
15) https://ea-poe-cert.iol.unh.edu/ 26/03/2021

Rys. 3. Wdrażanie urządzeń PoE



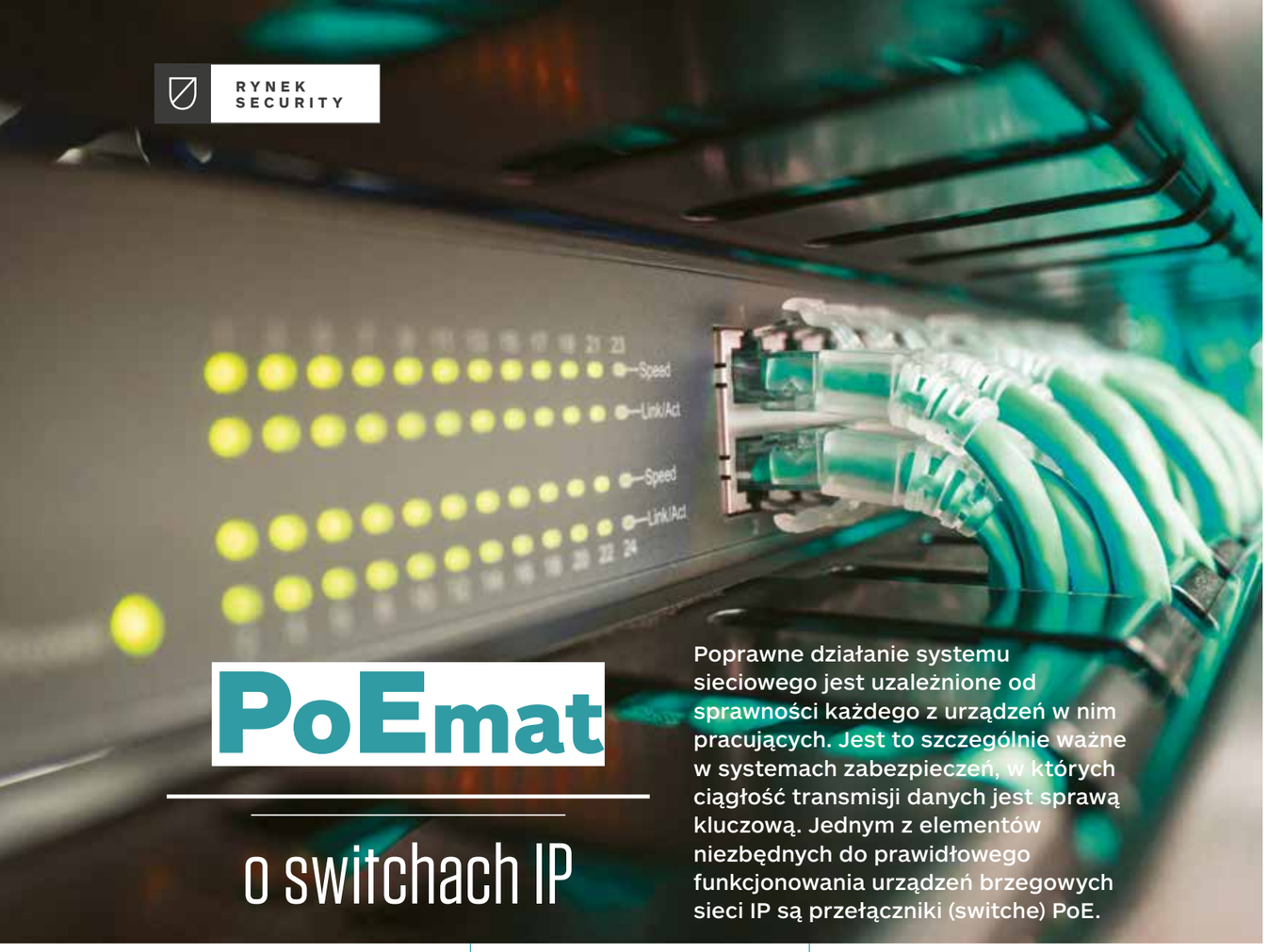
PLANY WDROŻENIA POE WEDŁUG POZIOMU PRZYDZIELANEJ MOCY)



https://ethernetalliance.org/poecert/poe-infographic/

JAN T. GRUSZNIC

z-ca red. naczelnego „a&s Polska". Z branżą wizyjnych systemów zabezpieczeń związany od 2004 r. Ma bogate doświadczenie w zakresie projektowania i wdrażania rozwiązań dozoru wizyjnego w aplikacjach o rozproszonej strukturze i skomplikowanej dystrybucji sygnałów. Ceniony diagnosta zintegrowanych systemów wspomagających bezpieczeństwo.



PoEmat o switchach IP

Poprawne działanie systemu sieciowego jest uzależnione od sprawności każdego z urządzeń w nim pracujących. Jest to szczególnie ważne w systemach zabezpieczeń, w których ciągłość transmisji danych jest sprawą kluczową. Jednym z elementów niezbędnych do prawidłowego funkcjonowania urządzeń brzegowych sieci IP są przełączniki (switche) PoE.

a&s Polska

Przełączniki PoE łączą segmenty sieci komputerowej pracujące głównie w drugiej warstwie modelu ISO/OSI (łącza danych). Mówiąc w skrócie – switch łączy ze sobą urządzenia sieciowe (hosty), odbierając i przesyłając dane do konkretnych portów, z którymi hosty są podłączone. Choć brzmi to banalnie, przez długi czas istnienia sieci opartej na stosie protokołów TCP/IP wymiana informacji była realizowana przez koncentratory (tzw. huby), które odebrane dane rozsyłały do wszystkich hostów, niezależnie od tego, czy były adresatem pakietu danych, czy nie. Taka zmasowana kanonada danych wymuszała ograniczenie liczby segmentów sieci do siedmiu (liczba aktywnych urządzeń przekazujących dane). Powyżej tej wartości dochodziło do „paraliżu" w komunikacji ze względu na zbyt dużą ilość informacji przesyłanych między hostami.

Problem ten rozwiązał m.in. pierwszy przełącznik ethernetowy wprowadzony przez firmę Kalpana w 1990 r. Od tamtej pory przeszedł on wiele modyfikacji. Jedną z nich jest pojawienie się przełącznika PoE *(Power over Ethernet)* opartego na kilku standardach przesyłania energii elektrycznej za pomocą skrętki komputerowej do urządzeń peryferyjnych, będących elementami sieci Ethernet. Wybór odpowiedniego modelu do elektronicznych systemów zabezpieczeń technicznych jest kluczowy. Zatem jakie cechy powinien mieć przełącznik sieciowy PoE? Swoimi radami na ten temat dzielą się doświadczeni menedżerowie produktowi.

DOBÓR PRZEŁĄCZNIKÓW POE

Użytkownik ma do wyboru przełączniki o różnej specyfikacji technicznej, w różnych cenach. Jak zauważa Mateusz Terlikowski z Atte: *Zły wybór urządzenia, często wynikający z oszczędności lub braku wiedzy, może się szybko zemścić. Brak świadomości o konieczności zastosowania odpowiedniego modelu do konkretnego zadania często przysparza problemów instalatorowi, a później użytkownikowi.*

Przełącznik PoE do elektronicznych systemów zabezpieczeń należy dobierać adekwatnie do liczby obsługiwanych urządzeń (np. kamer, czujników), oszacowanych prędkości transferu danych czy budżetu energetycznego PoE. Według Macieja Pietrzaka z Dahua Technology Poland: *W przypadku systemów dozoru wizyjnego specyfikacja przełącznika sieciowego powinna być dobrana adekwatnie do reszty systemu. Bardzo często elementy aktywne infrastruktury sieciowej, np. kamery, pracują w trudnych warunkach środowiskowych, dlatego warto zwrócić uwagę na temperaturę, wilgotność, zakurzenie miejsca pracy urządzenia.*

Różnice pomiędzy przełącznikami PoE determinuje również ich przeznaczenie. *Istnieją switche przeznaczone do pracy w przestrzeniach wewnętrznych, jak szafy serwerowe czy biura, oraz takie do zastosowań zewnętrznych, pracujące w trudnych warunkach środowiskowych* – dodaje Adam Brzezicki z Axis Communications.

Na inny aspekt zwraca uwagę Robert Gawroński z TP-Link: *Przede wszystkim sugerujemy dobrze zbadać oczekiwania inwestora dotyczące instalacji, a także ewentualnych możliwych planów rozbudowy, tak by nawet niewielka modernizacja nie oznaczała konieczności ponownej wymiany urządzeń. Warto również uwzględnić, czy przełączniki PoE będą wykorzystywane np. tylko do systemów monitoringu wizyjnego, czy też należy zapewnić ich kompatybilność i połączenie z innymi systemami oraz siecią lokalną.*

Z pewnością przy doborze przełącznika trzeba zastanowić się, jaką funkcję ma on pełnić w systemie. W wielu mniejszych instalacjach switch jest bowiem głównym elementem zasilania urządzeń i wymiany danych, stanowiąc jeden punkt awarii wyłączający cały system. Do awarii dochodzi najczęściej wskutek przepięć będących następstwem wyładowań atmosferycznych (głównie w systemach, w których okablowanie jest prowadzone napowietrznie) i uszkodzeń samych zasilaczy przełączników. *O ile z przepięciami możemy sobie radzić, stosując dodatkowe zabezpieczenia, o tyle na awarie zasilaczy w głównej mierze wpływ ma ich jakość. Dlatego należy wybierać urządzenia sprawdzonych producentów, których produkty zapewnią poprawne działanie* – zauważa Marek Dzioch z firmy PULSAR.

Istotną kwestią jest również odpowiednia kalkulacja budżetu mocy PoE, ponieważ moc pobierana przez wszystkie urządzenia nie może przekroczyć możliwości przełącznika. W tym przypadku rekomenduje się wyliczanie budżetu według tzw. klas.

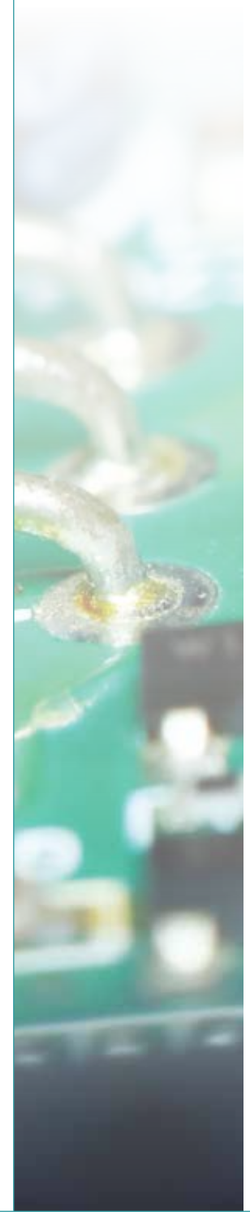
RODZAJE PRZEŁĄCZNIKÓW POE

Mnogość oferowanych przełączników PoE wynika z różnych standardów i trybów zasilania PoE czy też protokołów negocjacji, dzięki którym urządzenia odbiorcze otrzymują wymagane zasilanie. Na rynku ciągle można znaleźć dwa typy przełączników PoE mogące zasilić urządzenia końcowe – przełączniki z tzw. pasywnym PoE oraz zgodne ze standardami IEEE 802.3af/at/bt.

Pasywne PoE wymaga, aby zarówno urządzenie zasilające, jak i urządzenie zasilane stosowały to samo napięcie zasilania, np. 12 V, 24 V czy 48 V, co z kolei wymusza dostosowanie urządzeń, a to jest czasochłonne i ogranicza możliwości wyboru. To niejedyny, ale ekonomicznie dość istotny powód, dla którego warto trzymać się standardów, które – jak uważa Robert Gawroński – znacznie ułatwiają instalacje, choć przyznaje, że i sam standard PoE jest zróżnicowany. *Urządzenia w standardzie 802.3af mogą dostarczyć do 15,4 W na każdy port w przełączniku, zaś urządzeń w standardzie 802.3at do 30 W. Pojawią się również urządzenia w standardzie 802.3bt z mocą na porcie do 60 W* – dodaje.

Korzyścią z tak wielkich mocy jest choćby możliwość zasilenia kamer PTZ czy też oświetlaczy podczerwieni, które dotychczas wymagały zewnętrznego zasilacza.

Natomiast maksymalna odległości transmisji do 100 m dla przewodów miedzianych, wynikająca ze standardu, jest trudna do zaakceptowania dla wielu instalatorów, zwłaszcza pamiętających czasy zamkniętej telewizji dozorowej CCTV, tzw. analogowej. Dlatego, jak podpowiada Maciej Pietrzak, na rynku dostępne są *nowatorskie rozwiązania, jak ePoE – umożliwiające transmisję danych oraz zasilanie urządzenia na dystansie do 800 m przez skrętkę komputerową kat. 5 oraz możliwość korzystania z IP over Coax.* Co prawda uzyskanie połączenia na takim dystansie wiąże się z kompromisem w postaci prędkości przesyłania, jednak w wielu miejscach takie rozwiązanie stanowi interesującą alternatywę dla połączeń światłowodowych.



Od strony sprzętowej przełączniki sieciowe PoE różnią się przepustowością, liczbą i rodzajem portów oraz maksymalną mocą, jaka może być pobierana z poszczególnego portu PoE. *Różnice mogą dotyczyć również samej konstrukcji, użytych elementów i wykonania switcha, które pozwalają na bezpieczną pracę w różnych warunkach* – mówi Marek Dzioch. Istotnym elementem jest także oprogramowanie przełącznika i wynikające z niego możliwości. *Jeżeli switch musi spełniać zaawansowane funkcje, takie jak np. serwer DHCP, powinniśmy wybierać urządzenie, które oferuje wiele opcji konfiguracji i którym będziemy mogli zarządzać* – wskazuje Adam Brzezicki.

W bardziej rozbudowanych instalacjach wyzwaniem, z jakim często borykają się ich instalatorzy czy użytkownicy systemu, jest nieznajomość jego części logicznej spowodowana brakiem dokumentacji lub nieudokumentowanymi zmianami. *W takim przypadku sprawdzą się przełączniki sieciowe zarządzalne, zwłaszcza te z funkcją wizualizacji topologii, pokazującą, jakie konkretnie urządzenia, na których portach i w którym miejscu się znajdują* – mówi Łukasz Lik z Hikvision Poland. Switche wykorzystywane w elektronicznych systemach zabezpieczeń coraz częściej otrzymują funkcje, które ułatwiają operatorowi systemu zorientowanie się – bez konieczności wzywania specjalisty – co może być przyczyną awarii. *Przełącznik powinien mieć funkcję alarmowania na bieżąco o stanie połączeń do urządzeń, jaki ruch odbywa się na danym linku i czy przypadkiem nie mamy wysycenia połączenia, ponieważ ktoś np. uruchomił wiele sesji do jednej kamery. Często jest też tak, że osobno zarządza się systemem security i osobno warstwą IT* – tłumaczy Łukasz Lik.

Czasami problemy w warstwie sieciowej są trudne do identyfikacji i ich przyczyny poszukuje się w urządzeniach do niej podłączonych. Pochłania to dużo czasu, gdyż trzeba osobno wchodzić na interfejs switcha, osobno na interfejs systemów security. W przypadku switcha niezarządzalnego nie można sprawdzić, co na nim się dzieje. Łukasz Lik radzi więc: *Dlatego projektując system bezpieczeństwa, szukałbym rozwiązań sieciowych, które są w pełni zintegrowane z systemem zabezpieczeń, po to by operator otrzymywał na bieżąco informacje z warstwy*

IT i systemu bezpieczeństwa. Dzięki temu będzie można szybciej reagować na zdarzenia, także te z sieci. Kolejną istotną dla mnie funkcją jest proste i wygodne zarządzanie. Mam tu na myśli rozwiązania chmurowe. Na porządku dziennym są systemy bezpieczeństwa zarządzane przez chmurę, dlatego dołożyłbym tu także warstwę sieciową, by mieć wszystko w jednym miejscu i zarządzać za pomocą jednego interfejsu dostępnego z każdego miejsca.

GŁÓWNE OBSZARY ZASTOSOWAŃ

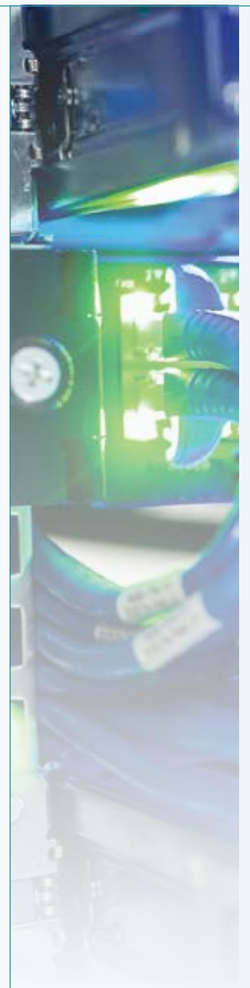
Dobrze zaprojektowana i wykonana sieć IP, niezależnie od wielkości systemu, powinna się charakteryzować pewnymi cechami, określającymi jej jakość. Są to: skalowalność, nadmiarowość, wydajność, bezpieczeństwo, łatwość utrzymania i zarządzania. Aby to osiągnąć, można zastosować model od lat proponowany przez specjalistów, m.in. przez Polską Izbę Systemów Alarmowych (PISA). Model ten zakłada wykorzystanie trzech warstw: rdzenia, dystrybucji i dostępu. W ramach elektronicznych systemów zabezpieczeń znajdziemy dwie ostatnie warstwy. *Jedna to switche umieszczone w centralnej szafie serwerowej [warstwa dystrybucji – przyp. red.], gdzie schodzą się sygnały ze wszystkich urządzeń. Druga to taka, gdzie switche umieszczone są w niedalekiej odległości od zasilanego urządzenia [warstwa dostępu – przyp. red.], np. na słupie, gdzie zainstalowana jest kamera lub w skrzynce elektrycznej* – doradza Adam Brzezicki.

Większe zarządzalne przełączniki stosuje się nie tylko w systemach CCTV IP, ale także w innych urządzeniach, takich jak punkty dostępowe Wi-Fi czy telefony IP, umożliwiając tworzenie znacznie większej sieci. Zastosowane w nich światłowodowe porty uplink 1G lub 10G umożliwiają utworzenie szybkiego połączenia wielu lokalnych punktów dystrybucyjnych (LPD) z głównym punktem (GPD) – tłumaczy Robert Gawroński. Natomiast niewielkie instalacje mogą składać się wyłącznie z połączonych ze sobą przełączników tylko w warstwie dostępowej. *Mniejsze kilku-, kilkunastoportowe urządzenia świetnie sprawdzają się w prostych systemach monitoringu wizyjnego w domach czy małych firmach, gdzie ceni się przede wszystkim niezawodność działania oraz prostą konfigurację typu plug&play* – dodaje Robert Gawroński.

CYBERBEZPIECZEŃSTWO

Dbałość o cyberbezpieczeństwo urządzeń w sieci jest dziś priorytetem. Tylko w Polsce eksperci CERT* zarejestrowali 6893 zgłoszenia naruszenia bezpieczeństwa, a liczba przeanalizowanych incydentów wyniosła 207 (dane na koniec marca br.).

Wszystkie nasze urządzenia sieciowe spełniają wysokie standardy obowiązujące w naszej organizacji. Aby zapewnić możliwie jak największy stopień bezpieczeństwa, urządzenia Axis powinny być odpowiednio zabezpieczone, dlatego dla naszych klientów przygotowaliśmy specjalny poradnik „Hardening guide", który można znaleźć na naszej stronie internetowej – rekomenduje Adam Brzezicki.



Z kolei Marcin Walczuk z BCS podkreśla zalety switchy zarządzalnych, gdy chodzi o bezpieczeństwo sieci, które *pozwalają na wprowadzenie ustawień ruchu sieciowego przechodzącego przez urządzenie. Oczywiście podstawą będzie zabezpieczenie dostępu do switcha odpowiednio silnym hasłem, które uchroni przed nieautoryzowanym dostępem.*

Na potrzebę wirtualnego wydzielenia sieci wskazuje Robert Gawroński: *Zaczynając już od małych i średnich przedsiębiorstw, rekomendujemy używanie przełączników z możliwością zarządzania i konfiguracji podstawowych funkcji zwiększających bezpieczeństwo sieci. Takim absolutnym minimum w tej kwestii jest standard 802.1Q VLAN umożliwiający odseparowanie sieci CCTV od sieci lokalnej, przeznaczonej dla pracowników czy gości, dla których tworzona jest gościnna sieć Wi-Fi.* I dodaje: *Co ważne, na sieć należy spojrzeć jako na jeden ekosystem, a nie traktować jej jako zbiór oddzielnych elementów. To wpłynie nie tylko na optymalizację w doborze rozwiązań, ale później przełoży się także na prostotę w zarządzaniu i utrzymaniu takiej sieci przez administratora.*

Fizyczne rozdzielenie instalacji CCTV IP od infrastruktury IT klienta rekomenduje też Mateusz Terlikowski: *Odpowiednie poprowadzenie instalacji oraz jej późniejsza konfiguracja znacząco utrudniają możliwość wpięcia się obcymi urządzeniami do infrastruktury IT klienta. Zabezpieczenia uniemożliwiają próby sabotażu oraz przypadkowe uszkodzenia.*

OCZEKIWANIA INSTALATORÓW

Instalatorzy poszukują przełączników przede wszystkim niezawodnych, o szerokich możliwościach konfiguracji i prostej obsłudze. *PoE ma być ułatwieniem pracy podczas instalacji. Ceniona jest szybkość i prostota uruchomienia systemu. Zaawansowane instalacje wymagają rozbudowanych możliwości konfiguracyjnych. Obie te grupy odbiorców łączy jedno – wymagają stabilnych i niezawodnie działających przełączników sieciowych* – mówi Maciej Pietrzak.

Na możliwość podłączenia zasilania rezerwowego wskazuje Marek Dzioch: *Instalatorzy i inwestorzy oczekują gwarancji działania przełączników w przypadku awarii głównego źródła zasilania. Dlatego ogromną popularnością cieszą się rozwiązania do podtrzymania zasilania buforowego switchy. Kolejnym elementem, na który coraz częściej zwracają uwagę, jest obecność gniazd SFP ze względu na szybkie upowszechnienie się techniki światłowodowej.*

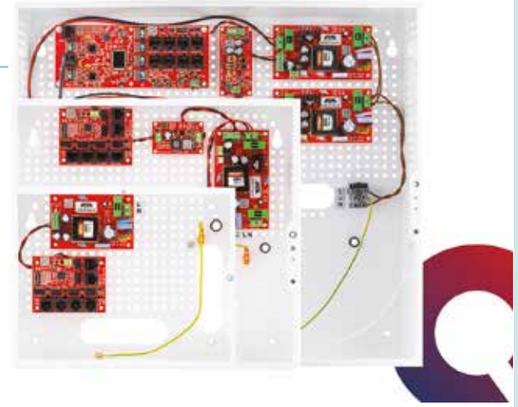
* CERT Polska to pierwszy powstały w Polsce zespół reagowania na incydenty *(Computer Emergency Response Team)* działający w strukturach NASK (Naukowej i Akademickiej Sieci Komputerowej)

ATTE

www.atte.pl

Systemy zasilania i transmisji danych do CCTV od ATTE Power

ATTE POWER JEST POLSKIM PRODUCENTEM SYSTEMÓW ZASILANIA I TRANSMISJI DANYCH DO SYSTEMÓW TELEWIZJI DOZOROWEJ. OD 15 LAT WSZYSTKIE URZĄDZENIA PROJEKTUJEMY I PRODUKUJEMY W POLSCE, CAŁY CZAS JE UDOSKONALAMY, KONTROLUJEMY ICH JAKOŚĆ I ZAPEWNIAMY OBSŁUGĘ PRODUCENTA – SZYBKIE WSPARCIE TECHNICZNE I SERWIS ORAZ SZKOLENIA PRODUKTOWE DLA DZIAŁÓW TECHNICZNYCH I HANDLOWYCH.



Buforowe zestawy ze switchem PoE są przeznaczone do współpracy z kamerami IP i innymi urządzeniami zasilanymi przez sieć. Dołączenie odpowiednich akumulatorów zapewnia bezprzerwową pracę układu zasilania przy okresowych zanikach zasilania sieciowego.

IPUPS-xx to seria gotowych punktów dystrybucyjnych dedykowanych do buforowego zasilania systemu VSS/CCTV (od 4 do 16 kamer IP) w standardach PoE 802.3at/af oraz PoE PASSIVE. Elektroniczne zabezpieczenia wyjść PoE zapewniają ciągłość pracy całego systemu podczas zwarcia lub przeciążenia pojedynczych gałęzi zasilania oraz automatyczny powrót napięcia po ustąpieniu awarii. Tryb *Long Range* zwiększa zasięg transmisji do 280 m z zastosowaniem standardowej skrętki komputerowej UTP.

Urządzenia znajdują zastosowanie w systemach wymagających zwiększonej przepustowości i niezawodności sieci, takich jak dozór 4K Ultra HD.

Wysoka sprawność energetyczna urządzeń (>90%) i eliminacja zbędnych stopni przetwarzania napięcia przekłada się bezpośrednio na oszczędności. Wyeliminowaliśmy przetwornice sinusoidalne stosowane w popularnych zasilaczach UPS. Dzięki temu w systemach opartych na naszych urządzeniach można stosować akumulatory o mniejszej o 50 proc. pojemności, zapewniając ten sam czas podtrzymania co UPS-y. Daje to jednorazową oszczędność przy zakupie akumulatorów, jak też przy każdorazowej ich wymianie.

Pojedyncze urządzenia stanowią moduły, z których buduje się większe zestawy. Ułatwia to rozbudowę i skalowanie systemów. Serwisanci, mając na stanie tylko kilka powtarzalnych modułów ATTE, mogą przywrócić do działania każdy system na nich oparty. Maksymalnie uproszczona budowa i konfiguracja urządzeń skraca czas montażu – mniej doświadczeni technicy poradzą sobie bez problemu, ci z dużym doświadczeniem w pełni wykorzystają możliwości sprzętu do budowy systemów nieosiągalnych na innym sprzęcie.

AXIS

www.axis.com/pl-pl

Przełączniki PoE od Axis Communications

W OFERCIE AXIS JEST WIELE PRZEŁĄCZNIKÓW POE PRZEZNACZONYCH DO RÓŻNYCH ŚRODOWISK – WEWNĘTRZNYCH, ZEWNĘTRZNYCH CZY PRZEMYSŁOWYCH. ŁĄCZY JE NIEZAWODNOŚĆ I INTUICYJNA OBSŁUGA.

Podstawowy model AXIS D8004 switch zapewnia dostęp do sieci i zasilanie PoE dla maks. 4 urządzeń (instalacja *plug and play*). Idealnie nadaje się do małych systemów z kilkoma urządzeniami i podstawowymi wymaganiami dot. przechowywania materiału wizyjnego. Gdy jest dostępne lokalne zasilanie, wystarczy jeden kabel do przesyłania danych od głównego przełącznika lub routera.

Bardziej zaawansowane są switche z serii AXIS T85 PoE+. Można je łatwo zainstalować za pomocą takich narzędzi, jak AXIS IP Utility i AXIS Device Manager. AXIS IP Utility automatycznie wykrywa i wyświetla urządzenia znajdujące się w sieci i pomaga nadawać adresy IP produktom. Switche z tej serii są również zabezpieczone własnym hasłem i mają prosty w użyciu kreator ustawień. Są wysoce zarządzalne, co pozwala przygotować je do pracy w każdej sieci.

Do pracy na zewnętrz jest przystosowany przełącznik AXIS T8504-E Outdoor PoE, który umożliwia szybki montaż kamer w rozległych instalacjach, np. monitoringu miejskiego czy na lotniskach. Dzięki portowi SFP nadaje się on doskonale do instalacji światłowodowych. To wytrzymałe, niewymagające częstej konserwacji rozwiązanie – ewentualne czynności naprawcze można przeprowadzić zdalnie.

Kolejną propozycją jest switch AXIS T8504-R Industrial PoE, zarządzalny przełącznik do zastosowań przemysłowych. Ma cztery porty PoE o mocy 60 W każdy oraz dwa porty danych RJ45 i dwa porty SFP. Przełącznik jest zaprojektowany do pracy przy drganiach i wstrząsach w temp. od -40 do 75°C, dzięki czemu idealnie nadaje się do instalacji o szczególnych wymaganiach (np. autostrady czy tunele).

Intuicyjny graficzny interfejs użytkownika wyświetla komunikaty dot. podłączonych urządzeń, umożliwia zarządzanie nimi, ponowne uruchamianie kamer, monitorowanie ruchu w sieci, diagnostykę okablowania i wiele więcej.

BCS

www.bcscctv.pl

Nowe switche BCS Line

W OFERCIE BCS POJAWIŁY SIĘ NOWE PRZEŁĄCZNIKI SIECIOWE (SWITCHE) SERII LINE. JEDNYM Z MODELI NALEŻĄCYM DO TEJ RODZINY PRODUKTÓW JEST SWITCH BCS-L-SP2402G-2SFP. JEST TO ZARAZEM NAJWIĘKSZY Z DOSTĘPNYCH MODELI, WYPOSAŻONY W 24 PORTY SIECIOWE POE O PRĘDKOŚCI TRANSMISJI DO 100 MB/S, DODATKOWE DWA PORTY 1000 MB/S ORAZ DWA PORTY ŚWIATŁOWODOWE.

Urządzenie dysponuje wysokim budżetem mocy dostępnym dla urządzeń wymagających zasilania, wynoszącym aż 360 W.
Wszystkie porty obsługujące PoE oferują obsługę standardu PoE+, dzięki czemu można do nich podłączyć urządzenia o zwiększonym poborze mocy, sięgającym do 30 W.

Każdy z tych portów wspiera również długodystansową transmisję danych i zasilania, której zasięg wynosi maksymalnie 250 metrów (z wykorzystaniem skrętki).

Opisywany model przełącznika jest w pełni zarządzalny, co pozwala na dodatkową konfigurację i obsługę ruchu sieciowego. Konfiguracja ta jest dostępna z poziomu przeglądarki internetowej, a dostęp do niej jest oczywiście chroniony hasłem.

Switch umożliwia konfigurację protokołu Spanning Tree, sieci VLAN, agregację połączeń, zarządzanie QoS, wsparcie dla serwerów NAS i Radius. Do funkcji poprawy bezpieczeństwa można zaliczyć zarządzanie na podstawie adresów MAC (przypisanie adresu do konkretnego portu), kontrola IGMP oraz zabezpieczenie SSL, z możliwością wygenerowania certyfikatu z poziomu switcha.
Możliwe jest monitorowanie pracy przełącznika poprzez protokół SNMP.

PULSAR

www.pulsar.pl

Uniwersalny system zasilania do switchy PoE

FIRMA PULSAR, W ODPOWIEDZI NA ZAPOTRZEBOWANIA RYNKU W SEKTORZE MONITORINGU IP, WPROWADZA DO SWOJEJ OFERTY UNIWERSALNY SYSTEM ZASILANIA DLA SWITCHY POE. TO GRUPA OBUDÓW WYPOSAŻONA W ZASILACZE Z AKCESORIAMI I ODPOWIEDNIE BLACHY MONTAŻOWE DEDYKOWANE DLA SWITCHY POE.

Seria SWS, wyposażona w zasilacze stabilizowane, obejmuje dwa modele: SWS-60 oraz SWS-150 (odpowiednio zasilacze 60 W i 150 W) i jest dedykowana głównie do switchy z 4/8 portami PoE.
Z kolei seria SWB to seria z zasilaczami buforowymi, do której należą modele: SWB-60/120/300 i SWB-300RACK. Pierwsze trzy są przeznaczone do switchy z 4/8 portami PoE, a konstrukcyjnie obudowa ma miejsce na akumulatory odpowiednio: 1 x 7 Ah/2 x 17 Ah/4 x 17 Ah.

Zastosowanie mniejszej liczby niż 4 szt. akumulatorów związane jest z zainstalowaniem przetwornic podbijających napięcie do poziomu 52 VDC (dla zapewnienia na wyjściu standardu PoE+).
Model SWB-300RACK jest już dedykowany do systemów zawierających switche PoE 16- i 24-portowe, które z racji gabarytów są montowane w profilach RACK 19". Profile RACK o wymiarze 3U, które w tej obudowie są zamontowane poziomo, pozwalają zainstalować dodatkowe elementy systemu w standardzie RACK, takie jak *patch panel* czy rejestrator. W tylnej części obudowy przewidziano przetłoczenia do zamontowania rejestratora, który nie ma uchwytu RACK, wymagane do tego są dwa pasy dostępne w ofercie jako akcesorium o kodzie ZPR.
Model SWB-300RACK, ze względu na możliwość zamontowania w nim rejestratora, ma też opcję montażu dwóch dodatkowych zamków o różnym kodzie MR008 – dla spełnienia wymogów związanych z wytycznymi RODO.
Firma Pulsar wprowadza do swojej oferty switche PoE bez zasilaczy, umożliwiające utworzenie kompletnego systemu monitoringu wizyjnego IP. Są to serie S... WP, SG....WP, SF...WP i obejmują – w zależności od serii – switche PoE 4-/8-/16-/24-portowe.
Więcej informacji nt. konkretnych parametrów i dedykowanych akcesoriów na stronie producenta.

TP-LINK

www.tp-link.com.pl

TP-Link TL-SG3210XHP-M2. Ultraszybki przełącznik zarządzalny PoE+, 2,5 Gb, z portami up-link 10 Gb

PRZEŁĄCZNIK TL-SG3210XHP-M2 TO ULTRAWYDAJNE URZĄDZENIE GOTOWE DO BUDOWY SIECI PRZYSZŁOŚCI, ZAPEWNIAJĄCE WYSTARCZAJĄCĄ PRZEPUSTOWOŚĆ DO OBSŁUGI PUNKTÓW DOSTĘPOWYCH WI-FI 6. JEST KOMPATYBILNY Z PLATFORMĄ OMADA SDN DO PROGRAMOWEGO STEROWANIA INFRASTRUKTURĄ SIECIOWĄ ZA POŚREDNICTWEM CHMURY.

Został wyposażony w 8 portów PoE+ 100/1000/2500 Mb/s zgodnych ze standardami 802.3at/af, które umożliwiają wykorzystanie pełnego potencjału punktów dostępowych Wi-Fi 6. Całkowity budżet mocy przełącznika wynosi 240 W, pozwala zasilić urządzenia odbiorcze mocą do 30 W na każdy port.
Dwa sloty SFP+ o prędkości 10 Gb/s zapewniają przełączanie w trybie *non-blocking* (redukcja opóźnienia do minimum).
Dzięki temu połączenia z serwerami i innymi przełącznikami są nawiązywane błyskawicznie i niezawodne.
Dzięki rozbudowanym funkcjom warstwy drugiej – obsługa VLAN 802.1Q tag, mirroring portów, STP/RSTP/MSTP, agregacja portów, funkcja kontroli przepływu 802.3x – przełączniki TL-SG3210XHP-M2 odznaczają się uniwersalnością działania. Funkcja IGMP Snooping pozwala na inteligentne skierowanie strumieni multicastowych tylko do określonych subskrybentów, a funkcje IGMP Throttling oraz IGMP Filtering skutecznie ograniczają nieupoważnionym użytkownikom dostęp do transmisji multicast. Z kolei obsługa funkcji statycznego routingu pozwala na segmentację sieci i zwiększa jej wydajność.
Przełącznik jest prosty w obsłudze i zarządzaniu. Jest w pełni kompatybilny z platformą Omada SDN do programowego sterowania infrastrukturą sieciową, która integruje urządzenia sieciowe od TP-Link, zapewniając kompleksowe zarządzanie centralne z chmury za pomocą interfejsu przeglądarki lub aplikacji mobilnej.
TP-Link Omada SDN umożliwia stworzenie wysoce skalowalnych sieci LAN i WLAN, co przekłada się na płynne połączenia przewodowe i bezprzewodowe niezbędne m.in. w hotelach, szkołach, biurach czy urzędach.
Produkt jest objęty 5-letnią gwarancją producenta.

TP-Link TL-SF1006P – wydajny i kompaktowy przełącznik do systemu monitoringu wizyjnego

PRZEŁĄCZNIK TP-LINK TL-SF1006P ZOSTAŁ ZAPROJEKTOWANY SPECJALNIE Z MYŚLĄ O MAŁYCH INSTALACJACH MONITORINGU IP – W DOMACH I MAŁYCH LOKALACH USŁUGOWYCH. DZIĘKI ZGODNOŚCI ZE STANDARDEM 802.3AF/AT POE+ INSTALACJA SYSTEMU JEST ŁATWA, BEZPIECZNA I MNIEJ KOSZTOWNA.

Zastosowanie trybu Extend zwiększa zasięg transmisji PoE nawet do 250 metrów, dzięki czemu TL-SF1006P to doskonałe rozwiązanie w przypadku rozmieszczania kamer IP na większym obszarze.

TL-SF1006P oferuje do 30 W mocy na każdym porcie PoE oraz 67 W łącznej mocy przełącznika. Urządzenie wyposażono w 4 porty PoE+ RJ45 10/100 Mb/s oraz w dwa dodatkowe porty RJ45 10/100 Mb/s, służące do podłączenia rejestratora NVR oraz integracji systemu monitoringu z resztą sieci.
Gdy całkowity pobór mocy przekracza 67 W, funkcja inteligentnego zarządzania zużyciem energii wyłącza zasilanie portu o najniższym priorytecie, aby zapewnić zasilanie portów o wyższych priorytetach i tym samym chronić urządzenie przed przeciążeniami. Możliwość nadania wyższych priorytetów portom 1–2 za pomocą trybu Priority, uruchamianego jednym kliknięciem, gwarantuje wysoką jakość aplikacji wrażliwych na opóźnienia, takich jak rejestracja wideo.
Ochronę wrażliwych komponentów przełącznika stanowi wytrzymała obudowa wykonana z metalu wysokiej jakości. Tak solidne zabezpieczenie gwarantuje wieloletnią i stabilną pracę urządzenia.
Przełącznik TL-SF1006P nie wymaga konfiguracji czy instalacji. Wystarczy wpiąć go do zasilania i podłączyć do niego urządzenia końcowe – urządzenie jest gotowe do pracy.
Produkt TP-Link został objęty 5-letnią gwarancją producenta.

TP-LINK

www.tp-link.com.pl

TP-Link TL-SG3428XMP, TL-SG3428MP i TL-SG2428P – 24-portowe przełączniki PoE+ z obsługą VLAN

TL-SG3428XMP, TL-SG3428MP I TL-SG2428P TO BIZNESOWE URZĄDZENIA PRZEZNACZONE DO BUDOWY PROFESJONALNYCH SIECI WYKORZYSTUJĄCYCH ZARÓWNO PUNKTY DOSTĘPOWE WI-FI, TELEFONY IP, JAK I KAMERY CCTV IP W MAŁYCH I ŚREDNICH FIRMACH. URZĄDZENIA SĄ KOMPATYBILNE Z PLATFORMĄ OMADA SDN DO PROGRAMOWEGO STEROWANIA INFRASTRUKTURĄ SIECIOWĄ ZA POŚREDNICTWEM CHMURY.

Modele TL-SG3428XMP oraz TL-SG3428MP zostały wyposażone w 24 porty PoE 10/100/1000Mb/s zgodne ze standardami 802.3at/af, mogące łącznie dostarczyć 384 W mocy. Przełączniki pozwalają zasilić urządzenia odbiorcze mocą do 30 W na każdy port.
TL-SG3428XMP ma ponadto cztery sloty SFP+ (10G) umożliwiające integrację w sieciach o wysokiej przepustowości. Z kolei TL-SG3428MP wyposażono w 4 gigabitowe sloty SFP.
Bardziej ekonomicznym rozwiązaniem jest TL-SG2428P, również wyposażony w 24 porty PoE 10/100/1000Mb/s zgodne ze standardami 802.3at/af, pozwalające zasilić urządzenia odbiorcze do 30 W na każdy port. Przełącznik może łącznie dostarczyć do 250 W mocy. TL-SG2428P wyposażono w 4 gigabitowe sloty SFP, tak jak model TL-SG3428MP.
Tworzenie bezpiecznej sieci wspomagają liczne funkcje – m.in. 802.1Q VLAN, izolacja portów, mirroring portów, agregacja portów (LACP), funkcja kontroli przepływu 802.3x, ACL, funkcje L2+ (tj. routing statyczny) oraz Quality of Service (QoS, od L2 do L4).
Przełączniki są w pełni kompatybilne z platformą Omada SDN do programowego sterowania infrastrukturą sieciową, która to platforma integruje działanie urządzeń sieciowych od TP-Link, zapewniając kompleksowe zarządzanie centralne z chmury za pomocą interfejsu webowego lub aplikacji mobilnej.
TP-Link Omada SDN umożliwia utworzenie wysoce skalowalnych sieci LAN i WLAN. Przekłada się to na płynne połączenia przewodowe i bezprzewodowe, które są niezbędne m.in. w hotelach, szkołach, biurach czy urzędach.
Urządzenia zostały objęte 5-letnią gwarancją producenta.

TP-Link TL-SL1218MP – przełącznik PoE Extend do zastosowań CCTV IP

PRZEŁĄCZNIK TP-LINK TL-SL1218MP JEST PRZEZNACZONY DO SIECI MONITORINGU WIZYJNEGO W MAŁYCH I ŚREDNICH PRZEDSIĘBIORSTWACH. DZIĘKI TECHNOLOGII POE INSTALACJA SYSTEMU JEST ŁATWIEJSZA, BEZPIECZNIEJSZA I MNIEJ KOSZTOWNA. TRYB EXTEND WYDŁUŻA ZASIĘG TRANSMISJI POE NAWET DO 250 METRÓW, TAK WIĘC TL-SL1218MP TO DOSKONAŁE ROZWIĄZANIE W PRZYPADKU ROZMIESZCZANIA KAMER IP NA DUŻYM OBSZARZE.

TL-SL1218MP został wyposażony w 16 portów PoE+ 10/100 Mb/s zgodnych ze standardami 802.3at/af. Całkowity budżet mocy przełącznika wynosi 250 W, może on zasilić urządzenia odbiorcze do 30 W na każdy port. Wysoki budżet PoE sprawia, że idealnie sprawdzi się zarówno w małych, jak i średnich firmowych systemach dozoru wizyjnego.
Przełącznik wyposażono ponadto w dwa porty RJ45 10/100/1000 Mb/s oraz dwa gigabitowe gniazda Combo SFP, które mogą posłużyć do podłączenia rejestratora oraz integracji systemu CCTV z pozostałymi elementami sieci lokalnej.
Możliwość nadania wyższych priorytetów portom 1–8 za pomocą trybu Priority uruchamianego jednym kliknięciem gwarantuje wysoką jakość aplikacji wrażliwych na opóźnienia, np. nagrania wideo.
Ochronę wrażliwych komponentów przełącznika stanowi wytrzymała obudowa wykonana z metalu wysokiej jakości. Tak solidne zabezpieczenie gwarantuje wieloletnią i stabilną pracę urządzenia.
Przełącznik TL-SL1218MP nie wymaga konfiguracji czy instalacji. Wystarczy wpiąć go do zasilania i podłączyć do niego urządzenia końcowe. Urządzenie jest gotowe do pracy.
Produkt TP-Link został objęty 5-letnią gwarancją producenta.

Urządzenia bezprzewodowe dla SSWiN i automatyki

ABAX 2

W systemach sygnalizacji włamania i napadu urządzenia bezprzewodowe wykorzystuje się przede wszystkim z racji wygody i szybkości ich montażu. Na co jeszcze należy zwrócić uwagę przy wyborze systemów wykorzystujących komunikację radiową?

Bezprzewodowe urządzenia używane do pracy w ramach SSWiN do niedawna nie miały wielu zwolenników – głównie z braku zaufania co do pewności ich działania. Obawiano się „podsłuchiwania" transmisji oraz zakłóceń komunikacji. Na rynku zaczęły się więc pojawiać zaawansowane systemy oferujące wysoki poziom bezpieczeństwa – przykładem jest ABAX 2, czyli system bezprzewodowy, którego skuteczność i niezawodność można porównać do instalacji przewodowych. Co konkretnie stoi za wyborem tego rozwiązania?

ELASTYCZNOŚĆ ZASTOSOWAŃ

Najważniejszymi urządzeniami w ABAX 2 są kontrolery ACU-220 i ACU-280. Mogą pełnić funkcję ekspanderów w systemach alarmowych bazujących na centralach serii INTEGRA lub VERSA – połączenie z kontrolerem odbywa się za pośrednictwem magistrali komunikacyjnej. Wspomniane moduły mogą pracować autonomicznie lub z dowolną centralą alarmową czy sterownikiem automatyki. Wykorzystuje się wówczas programowalne wejścia i wyjścia kontrolera lub protokół Modbus RTU.

PEWNOŚĆ KOMUNIKACJI

Dane drogą radiową przesyła się dwukierunkowo – wszystkie dostarczone transmisje są potwierdzane, dzięki czemu na bieżąco można zweryfikować obecność poszczególnych urządzeń. W ABAX 2 korzysta się z tzw. dywersyfikacji kanałów transmisji – w paśmie częstotliwości 868 MHz zostały wydzielone 4 kanały, w których stale monitoruje się poziom zakłóceń. Dane są przesyłane tym kanałem, w którym poziom interferencji jest w danej chwili najniższy. Wszystko po to, aby komunikacja była efektywna. Z kolei za jej bezpieczeństwo odpowiada szyfrowanie AES-128.

DUŻY ZASIĘG, DŁUGI CZAS PRACY

System ABAX 2 cechuje się doskonałymi osiągami. Odległość między kontrolerem systemu bezprzewodowego a współpracującymi z nim urządzeniami może wynieść nawet do 2000 m w otwartej przestrzeni. Imponujący jest także maksymalny czas pracy urządzeń zasilanych bateryjnie, który w sprzyjających warunkach może wynieść nawet 8 lat.

SZEROKA GAMA URZĄDZEŃ ALARMOWYCH

Pośród czujek ABAX 2 znajduje się kilka modeli wykrywających ruch – PIR i dualne, odporne na ruch zwierząt i kurtynowe. Niektóre z nich można montować na zewnątrz budynku. Dostępne są także czujki zbicia szyby, zmierzchu, temperatury, dymu i ciepła. Ciekawostką jest czujka uniwersalna, która może pracować w jednym z 7 trybów, m.in. jako czujka magnetyczna, wstrząsowa, przemieszczenia, zalania lub temperatury. Z kontrolerami ABAX 2 współpracują też wewnętrzne i zewnętrzne sygnalizatory. Większość ww. urządzeń spełnia wymagania Grade 2 normy EN 50131.

MOŻLIWOŚĆ STEROWANIA AUTOMATYKĄ

ABAX 2 to także dwukierunkowe piloty, za których pomocą można sterować funkcjami bezpieczeństwa i automatyki budynkowej. Do realizacji funkcji *smart home* można wykorzystać bezprzewodowe sterowniki 230 V AC przeznaczone do montażu puszkowego lub podłączane bezpośrednio do gniazd sieciowych. Z kolei ekspandery umożliwiają rozszerzenie systemu o urządzenia przewodowe.

WYGODNE PROGRAMOWANIE, ZAAWANSOWANA DIAGNOSTYKA

Do obsługi, programowania i zaawansowanej diagnostyki systemu bezprzewodowego służy program ABAX 2 Soft. Jeśli urządzenia ABAX 2 wchodzą w skład systemu alarmowego bazującego na centrali z serii INTEGRA lub VERSA – system ten konfiguruje się za pomocą manipulatorów (w tym modeli bezprzewodowych) lub programu DLOADX.
Do sprawdzania komunikacji radiowej wewnątrz ABAX 2 oraz poziomu zakłóceń przed montażem urządzeń w obiekcie służy przenośny tester.

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

OS Malevich 2.10

Oprogramowanie, które wygrywa z fałszywymi alarmami

OS Malevich 2.10 wprowadza do systemu alarmowego Ajax najlepsze światowe standardy w zakresie przeciwdziałania fałszywym alarmom. Dzięki temu oprogramowaniu system uzyskał zgodność z PD 6662:2017 – dokumentem wprowadzającym europejskie normy dotyczące systemów sygnalizacji włamania i napadu w Wielkiej Brytanii.

Systemy z oprogramowaniem OS Malevich 2.10 rozszerzają potencjalne zastosowania scenariuszy, a także komunikują się z użytkownikami w większej liczbie języków. Zapewniają ochronę przeciwpożarową znajdującym się na liście światowego dziedzictwa UNESCO zabytkowym budynkom w Bergen w Norwegii.

DOŚWIADCZENIE BRYTYJSKIE

Cechą charakterystyczną rynku brytyjskiego jest to, że policja odbiera i reaguje na sygnały alarmowe, a każda niepotrzebna interwencja jest uważana za marnowanie czasu i cennych zasobów. Powtarzające się fałszywe alarmy mogą prowadzić do konieczności rezygnacji z usług monitoringu.
Dlatego w systemie OS Malevich 2.10 firma Ajax Systems zaimplementowała zaawansowane funkcje przeciwdziałania fałszywym alarmom i odpowiedzialnego korzystania z systemów SSWiN. Malevich 2.10 wyróżniają następujące funkcje:

- **Potwierdzenie alarmu.** System przesyła oddzielne zdarzenie do Centrum Monitorowania Alarmów w celu potwierdzenia alarmu. System może wygenerować sygnał potwierdzający stan alarmu po wyzwoleniu wielu zdarzeń wykrycia włamania lub użycia przycisków alarmowych. Instalator podczas konfigurowania systemu wybiera urządzenia, których aktywacja prowadzi do potwierdzenia, oraz ustala interwał czasowy dla alarmów. Funkcję można znaleźć w ustawieniach serwisowych huba.
- **Przycisk awaryjny doskonale zabezpieczony przed przypadkowymi naciśnięciami.** System z oprogramo-waniem OS Malevich 2.10 jest obsługiwany przez DoubleButton, nowy przycisk awaryjny Ajax Systems. DoubleButton włącza alarm tylko wtedy, gdy oba przyciski zostaną wciśnięte jednocześnie – specjalna bariera zapobiega przypadkowemu uruchomieniu. Kurz i zachlapanie nie mają wpływu na działanie urządzenia. Można je bezpiecznie nosić w kieszeni jako brelok do kluczy lub zawiesić na szyi. Przycisk DoubleButton może też wygenerować potwierdzone zdarzenie alarmu napadowego. W tym celu należy dwa razy nacisnąć przyciski w różny sposób (krótkie i długie naciśnięcie) lub użyć dwóch urządzeń DoubleButton.
- **Przywrócenie stanu systemu po alarmie**. Funkcja zapobiega uzbrojeniu systemu Ajax po wcześniejszym wyzwoleniu alarmu. Ponowne uzbrojenie systemu wymaga sprawdzenia incydentu, a następnie przywrócenia stanu systemu przez uprawnionego użytkownika (PRO lub administratora). Ta funkcja pomaga inżynierom śledzić stan systemu, ponieważ alarm oznacza, że obiekt został zaatakowany lub system działa nieprawidłowo. Typy przywracanych alarmów są określane podczas konfiguracji huba.
- **Uzbrajanie dwuetapowe**. Funkcja dzieli proces uzbrajania na dwa etapy: rozpoczęcie i zakończenie. Użytkownicy mogą rozpocząć uzbrajanie za pomocą urządzenia sterującego (SpaceControl lub KeyPad). W takiej sytuacji system zostanie uzbrojony po wyzwoleniu urządzenia drugiego etapu, np. przy zamknięciu drzwi, na których zainstalowano DoorProtect. Użytkownicy mogą również rozpocząć uzbrajanie z aplikacji mobilnej Ajax: system zostanie uzbrojony, jeśli w określonym czasie nie zostaną wyzwolone żadne czujki.
- **Selektywna kontrola integralności systemu**. Instalatorzy mogą wybrać stany huba podlegające kontroli integralności podczas uzbrajania systemu. Eliminuje to niepotrzebne kontrole, np. w wypadku zepsutego czujnika sabotażu lub przerw w zewnętrznym zasilaniu huba.
- **Automatyczna dezaktywacja urządzeń.** Ta funkcja umożliwia systemowi ignorowanie zdarzeń z czujki, jeśli nie powróciła ona do stanu początkowego w określonym czasie. Jest to przydatne, gdy czujka została uszkodzona lub nieprawidłowo zainstalowana, a nie ma fizycznego dostępu do chronionego obiektu. Funkcję można znaleźć w ustawieniach serwisowych huba.
- **Opóźnienie transmisji sygnału alarmu przy rozbrajaniu.** Funkcja ta pozwala na odroczenie przesłania alarmu, jeśli upłynął czas na wejście, a system alarmowy nie został rozbrojony. Po upływie czasu na wejście system generuje alarm lokalnie: aktywuje podłączone syreny, ale nie przekazuje zdarzenia alarmowego do Centrum Monitorowania. Daje to użytkownikom dodatkowy czas na rozbrojenie systemu, bez wysyłania fałszywego alarmu. Funkcja pozwala również na użycie KeyPada (który aktywuje się dopiero po wygaśnięciu opóźnień na wejście) jako alternatywnego urządzenia rozbrajającego. Funkcję można skonfigurować w ustawieniach serwisowych huba: menu Proces uzbrajania/rozbrajania.

Linia produktów Ajax obejmuje 33 urządzenia do ochrony obiektów przed włamaniem, pożarem i zalaniem

OCHRONA DZIEDZICTWA KULTUROWEGO

Wraz z firmą Elotec, norweskim dystrybutorem systemów alarmowych i producentem przewodowych systemów sygnalizacji pożarowej, Ajax Systems będzie wdrażać zabezpieczenia przeciwpożarowe w zabytkowej zabudowie miasta Bergen.
W ramach tego projektu zespół badawczo-rozwojowy Ajax zaimplementował opóźnienia dla połączonych alarmów pożarowych (alarmy synchroniczne czujek pożarowych) oraz transmisji zdarzenia alarmowego do stacji monitorowania – wszystko w celu zminimalizowania niepotrzebnych wezwań straży pożarnej. Użytkownicy mogą opóźnić alarm od 1 do 5 minut za pomocą aplikacji, dotykając logo wyzwolonej czujki pożarowej lub używając odpowiednio skonfigurowanych urządzeń Button i KeyPad. Dzięki OS Malevich 2.10 ta funkcja jest dostępna we wszystkich hubach Ajax.

WIĘCEJ PRZYDATNYCH FUNKCJI

- **Przełączanie stanu zautomatyzowanego urządzenia za pomocą polecenia przycisku Button**. Tworząc scenariusz sterowania urządzeniami Relay, Socket lub WallSwitch za pomocą przycisku Button, można ustawić nie tylko konkretną akcję włączania/wyłączania, ale też przełączanie stanu styków na odwrotny. Umożliwia to użycie inteligentnego przycisku jako zdalnego przełącznika, ustawienie jednego scenariusza zamiast dwóch i sprawia, że scenariusze automatyzacji stają się jeszcze wygodniejsze.
- **Sygnalizacja syren po alarmie.** Ta funkcja pozwala zobaczyć, czy uzbrojony system zarejestrował jakiekolwiek alarmy: podłączone syreny migają co kilka sekund aż do rozbrojenia systemu. Podczas konfiguracji można wybrać typy alarmów sygnalizowanych przez syreny: alarmy potwierdzone, alarmy niepotwierdzone lub wyzwolenie tampera.
- **Przesyłanie przywrócenia alarmu do służb reagowania**. Teraz można skonfigurować, po jakim czasie zdarzenie przywrócenia czujki (powrót do stanu początkowego po wyzwoleniu) zostanie wysłane do stacji monitorowania: natychmiast (domyślnie) lub gdy system alarmowy zostanie rozbrojony.

Kontrola dostępu

Incedo™ Business | LITE PLUS CLOUD

idąca z duchem czasu

W czasach pandemii koronawirusa administratorzy i menedżerowie obiektów stanęli w obliczu nowych wyzwań: jak chronić swoje budynki podczas pracy zdalnej, wyeliminować obecność nieuprawnionych osób spoza organizacji oraz zapewnić potrzebne uprawnienia pracującym w systemie hybrydowym. Takie miejsca, jak biura, centra handlowe, szkoły czy szpitale wymagają szczególnej uwagi oraz gwarancji bezpieczeństwa i wygody użytkowania. Odpowiedzią na te potrzeby są nowoczesne, inteligentne rozwiązania nadążające za potrzebami współczesnych użytkowników.

TRENDY W KONTROLI DOSTĘPU

Inteligentne rozwiązania cieszą się coraz większą popularnością, a menedżerowie budynków użytkowych dostrzegają korzyści płynące z ich wdrożenia. Nic w tym dziwnego – wg raportu PwC najemcy powierzchni w inteligentnych budynkach są skłonni płacić o 8% wyższe czynsze, a nabywcy decydują się na transakcje wyższe o 24% niż w tradycyjnych obiektach. Wszystko dlatego, że inteligentne rozwiązania są dostosowane do indywidualnych wymagań użytkownika i odpowiadają na jego zmieniające się potrzeby.

ELASTYCZNOŚĆ, SKUTECZNOŚĆ I WYGODA

Coraz większy przepływ ludzi, danych i towarów, a w efekcie zmieniające się potrzeby w obszarze kontroli dostępu stanowią ogromne wyzwanie. Zmienia się zarówno sposób poruszania się użytkowników budynku, jak i ich wymagania dotyczące uprawnień zróżnicowane pod względem czasu czy punktów wejścia. Na rynku pojawiają się rozwiązania dostosowane do współczesnych wymagań życia i inteligentnego budownictwa, gwarantujące skuteczność, bezpieczeństwo, elastyczność i łatwość użytkowania.
Dla użytkownika ważne jest, aby system KD łączył w ramach jednego ekosystemu skuteczny osprzęt i elastyczne oprogramowanie z szerokim wyborem technologii i funkcji. Niezależnie od wielkości budynku i organizacji wybór jednej wszechstronnej platformy będzie krokiem w stronę zapewnienia bezpieczeństwa przy jednoczesnym umożliwieniu swobodnego przemieszczania się zależnie od bieżących potrzeb.

ASSA ABLOY OPENING SOLUTIONS POLAND

ul. Magazynowa 4, 64-100 Leszno
www.assaabloyopeningsolutions.pl
info.pl.openingsolutions@assaabloy.com

OPŁACALNA INWESTYCJA

Wdrożenie inteligentnego systemu zarządzania dostępem to inwestycja opłacalna przez wiele kolejnych lat, pod warunkiem że system będzie dostosowany do ciągle rozwijających się technologii. Przykładem jest Incedo Business firmy ASSA ABLOY, które – dzięki możliwości wyboru opcji zarządzania systemem – dopasowuje się do bieżących i przyszłych potrzeb użytkowników.
System umożliwia też integrację urządzeń zewnętrznych w miarę ich pojawiania się na rynku, dzięki czemu może być rozbudowywany i aktualizowany nie tylko o sprzęt firmy ASSA ABLOY, lecz także od dostawców zewnętrznych. Ma to na celu skuteczną i efektywną obsługę minimalizującą czas przestoju oraz zapewniającą realizację projektów przedsiębiorstwa.

DLA KOGO INTELIGENTNA KONTROLA DOSTĘPU

Nowoczesne rozwiązania do zarządzania dostępem doskonale sprawdzają się w każdym obiekcie, zapewniając bezpieczeństwo i pozwalając skupić się na rozwoju firmy. Decydujący się na nie menedżerowie zyskują efektywną kontrolę i elastyczność, instalatorzy nie muszą zmagać się z niekompatybilnymi systemami, a administratorzy mają większy wybór działań (m.in. zmiany profili dostępu oraz monitorowanie ruchu w czasie rzeczywistym).
System może być stale rozwijany, dlatego z łatwością sprosta przyszłym wymaganiom operacyjnym przy jednoczesnej kontroli budżetu. Większa wydajność umożliwi wygodne przemieszczanie się osób i zachowanie bezpieczeństwa, bez konieczności ponoszenia dodatkowych kosztów.

Starcie tytanów

czyli stara dobra ochrona fizyczna a nowoczesne technologie

Branża ochrony fizycznej jeszcze przed pandemią borykała się z wieloma problemami. Lockdowny i obostrzenia epidemiczne dodatkowo pogłębiły ten kryzys. Czy firmy ochrony przejdą do lamusa? Moim zdaniem, nie! A wspomóc je może zastosowanie nowoczesnych technologii.

Paweł Mucha

Pierwszego z konkurentów tytułowego starcia nie muszę przedstawiać. Ochrona fizyczna, a także ustawa o ochronie osób i mienia, która przez wiele lat ewoluowała, są nam znane od lat. Na przełomie wieków było wyraźne rozróżnienie pomiędzy pracownikiem ochrony fizycznej a pracownikiem gospodarczym, zwanym portierem. Istniał także podział na pracownika ochrony fizycznej posiadającego licencję pierwszego stopnia i pracownika licencjonowanego legitymującego się licencją drugiego stopnia. Niejednokrotnie w obiektach można było spotkać zarówno pracownika ochrony, jak i portiera, obaj wykonywali swoje zadania niezależnie.

Dzisiaj firmy ochrony coraz bardziej konkurują między sobą, minimalne stawki wynagrodzenia z roku na rok rosną, natomiast zamawiający usługę mają większą świadomość swoich potrzeb i konieczności redukcji kosztów utrzymania ochrony. Polski ustawodawca podał pomocną dłoń firmom ochrony, ale w ich efekcie pracownicy świadczą raczej wspomniane usługi portierskie. Mam na myśli PFRON i zatrudnianie osób niepełnosprawnych do zadań ochronnych. Prawda jest druzgocąca, gdyż w wielu obiektach – w ramach zamówień publicznych – pracują osoby, które z ochroną mają niewiele wspólnego. Temu nowemu trendowi w ochronie towarzyszą wsparcie i nadzór techniczny w celu kontroli i weryfikacji zleconych zadań. Wszystko zależy jednak od zasobności i możliwości inwestowania właścicieli czy prezesów firm zatrudniających osoby niepełnosprawne.

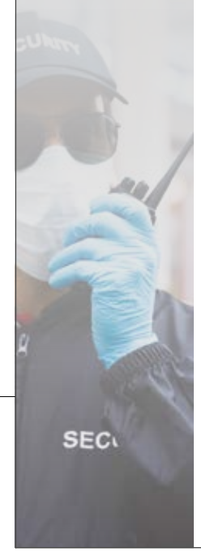
Przed nami jeszcze długa droga do uzdrowienia sytuacji. W sektorze prywatnym widać już poprawę świadomości klientów co do jakości usług ochrony, jej funkcjonalności i zadań, natomiast w sektorze zamówień publicznych – moim zdaniem – mamy do czynienia z patologią ochrony, gdyż czynnikiem decydującym o wyborze zleceniobiorcy jest w 100 proc. kryterium ceny. Co więcej, przetarg często rozpisuje osoba niekompetentna, niemająca wiedzy o ochronie. Są to przykre fakty, jednak zauważalne w większości takich przetargów. SIWZ różni się od umowy końcowej, załączniki zawierają błędy, mylone są pojęcia grupy interwencyjnej z patrolem interwencyjnym itp.

Podsumowując wątek ochrony fizycznej, wiem na pewno: nie idźmy w tę stronę.

W dobie pandemii COVID-19 klienci, którzy do tej pory korzystali z podstawowej ochrony fizycznej, z powodu zamknięcia swoich firm, fabryk, obiektów zaczęli poszukiwać alternatywnych rozwiązań, które mogą zmniejszyć koszty miesięczne przy zachowaniu dotychczasowego poziomu bezpieczeństwa obiektu.

I tutaj pojawia się drugi konkurent tytułowego starcia tytanów – nowoczesne technologie. Godna uwagi jest m.in.

1) 1 stycznia 2014 r. weszły w życie zapisy art. 9 i 13 ustawy z 13 czerwca 2013 r. o zmianie ustaw regulujących wykonywanie niektórych zawodów (Dz.U. z 2013 r., poz. 829), wprowadzające w ustawie o ochronie osób i mienia oraz w ustawie o broni i amunicji zmiany w nazewnictwie i uzyskiwaniu uprawnień kwalifikowanego pracownika ochrony. Dziś mamy kwalifikowanego pracownika ochrony fizycznej i kwalifikowanego pracownika zabezpieczenia technicznego. Kiedyś licencja pracownika była niemal równoznaczna z posiadaniem broni kat. B, obecnie większość pracowników kwalifikowanych nie ma pozwolenia na broń.



możliwość wsparcia usług agencji ochrony przez mobilną wieżę monitorującą dostępną na polskim rynku jeszcze przed pandemią. To przenośny system monitoringu wizyjnego wspierany przez algorytmy sztucznej inteligencji oraz wyposażony w głośnik IP potrzebny do emitowania komunikatów głosowych. Ze względu na swoją funkcjonalność rozwiązanie cieszy się obecnie zainteresowaniem w różnych sektorach rynku. Najczęściej można je spotkać na tymczasowych placach budów, gdzie wypierają pracowników ochrony. Zaletą zastosowania mobilnej wieży monitorującej jest możliwość szybkiej zmiany jej lokalizacji. Cały proces (nie licząc czasu transportu) nie powinien zająć więcej niż 30 minut.

Dostrzegając nową jakość zabezpieczeń, jaką oferuje mobilna wieża do monitoringu wizyjnego, wielu klientów rezygnuje z zatrudniania pracowników ochrony w godzinach nocnych. I jest to słuszny kierunek. Pracownik ochrony, znużony zwłaszcza w newralgicznych godzinach nocnych między 1.00 a 3.00, obchód obiektu wykonuje w zasadzie w sposób automatyczny. Gdy do tego dochodzą trudne warunki atmosferyczne: deszcz, śnieg, kaptur na głowie, głowa nisko, a także zmęczenie długą, ponad 20-godz. służbą, mamy efekt – zakodowana w świadomości konieczność dojścia do punktu kontrolnego i „odhaczenie się", nic więcej. Wielokrotnie zdarzały się sytuacje, że obchody były wykonywane regularnie, a rano niestety zleceniodawca informował o włamaniu.

Nowe zaawansowane wieże są wyposażone w kamery dozorowe z analizą obrazu, które monitorują obszar przez całą dobę. Oświetlacze współpracujące z kamerami pozwalają ograniczyć fałszywe alarmy. Można też zastosować wysokiej klasy kamery termowizyjne, które podnoszą poziom bezpieczeństwa chronionego obiektu, wykrywając nie tylko wtargnięcie intruza, ale także pożar w jego wczesnej fazie. System jest obsługiwany przez centrum monitorowania alarmów wizyjnych zleceniobiorcy wg określonych procedur reakcji na zaistniałe zagrożenie.

Zintegrowany z wieżą lokalny bezprzewodowy system alarmowy można obsługiwać, tak jak wieżę, z wykorzystaniem pilota lub aplikacji na telefon. Pozwala to na zabezpieczenie dodatkowych obiektów wewnętrznych (np. składowane kontenery). Głośnik zainstalowany na maszcie, wysuwany na wysokość 8 m, emituje automatyczne komunikaty głosowe, operator monitoringu może również wydawać polecenia w trybie na żywo. Przydatną cechą są komunikaty nadawane w różnych językach,

ZAPOTRZEBOWANIE NA MOBILNE WIEŻE MONITORUJĄCE NA POLSKIM RYNKU SZACUJE SIĘ NA 8–12 TYS. SZTUK

zwłaszcza na placach budów, gdzie zatrudnia się pracowników różnej narodowości. Wygodą dla użytkownika jest też możliwość zasilania wieży na trzy sposoby: standardowo z sieci 230 V, z wykorzystaniem paneli fotowoltaicznych albo też akumulatorów doładowywanych poprzez agregaty w obiekcie.
Sprawdzają się również na lokalnych wysypiskach śmieci, gdzie dzięki zastosowaniu kamer termowizyjnych monitorują obszar wysypiska pod kątem powstania pożaru. Zainteresowanie zgłaszają również urzędy gminne, zmagające się z coraz większą plagą nielegalnych wysypisk odpadów. Zastosowanie wież ułatwia fakt, że mogą one działać na własnym zasilaniu nawet w trudno dostępnych obszarach, gdzie instalacja lokalnego systemu telewizji dozorowej jest nierealna. Zwiększone zainteresowanie wieżami obserwujemy również w branży rozrywkowej. Mowa o imprezach masowych – zgodnie z ustawą MSWiA narzuca na organizatora zapewnienie monitorowania przebiegu imprezy wraz z archiwizacją nagrań. Eksperci z branży security twierdzą – podzielam ich zdanie – że rok 2021 będzie przełomowy, jeśli chodzi o wzrost sprzedaży tej nowej usługi w Polsce.

Dla równowagi muszę też wspomnieć o wadach rozwiązania, które widzę. Przede wszystkim w naszym klimacie panele fotowoltaiczne spełniają swoją funkcję zasilania wieży tylko od marca do ok. 20 października. W pozostałych miesiącach trzeba stosować doładowanie z agregatu czy akumulatorów. Trwają więc prace nad zasilaniem wiatrowym.
Drugą wadą są fałszywe alarmy, których niestety – mimo rozwoju technologii i nowych rozwiązań – nadal nie można wyeliminować. Ta „niedogodność" zapewne zostanie z nami na dłużej. I nie dotyczy tylko systemów dozorowych, ale także lokalnych systemów alarmowych. Nie ułatwia sprawy fakt, że wieża pracuje w warunkach zewnętrznych i jest podatna na wszelkiego rodzaju zakłócenia wywołane przez owady, opady atmosferyczne, refleksy świateł reflektorów przejeżdżających pojazdów czy pociągów. Bardzo to utrudnia pracę operatorów stacji monitoringu.
No i ostatnia wada (problem), na którą patrzę z niepokojem – pojawiają się dostawcy czy też firmy, które próbują swoich sił w produkcji własnych rozwiązań. Powstają one lokalnie, w przydomowych garażach, bez wiedzy nt. funkcjonowania tego typu urządzeń. Są wyposażane w standardowe kamery z rejestratorem, a obszar jest monitorowany przez operatora, który ma zareagować na widoczne na ekranach zagrożenie. To cofa usługę do czasu pierwszych systemów dozorowych.
Profesjonalne mobilne wieże monitorujące mogą znakomicie uzupełnić pracę firm ochrony. Jakie inne technologie również mogą ją wspomagać? Przyjrzyjmy się nowoczesnym systemom telewizji dozorowej. Wszystko tak naprawdę zależy od klienta/użytkownika końcowego, który ma możliwość i chce zainwestować we własny system VSS z kamerami wyposażonymi w analitykę obrazu. Ważnym kryterium jest cena dodatkowych funkcji i możliwość integracji z innymi systemami, np. SSWiN. To wygodne rozwiązanie, ponieważ uzbrajając jeden system, można automatycznie załączyć drugi.
Innym przykładem zastosowania nowych technologii są spółdzielnie mieszkaniowe, zarządcy nieruchomości oraz wspólnoty mieszkaniowe. Jeszcze jakiś czas temu zauważalny był wzrost podmiotów gospodarczych, które świadczyły tu usługi portierskie. Wzrost płacy minimalnej zweryfikował również te usługi i spółdzielnie mieszkaniowe zaczęły poszukiwać innych rozwiązań. Z pomocą przychodzą nowe technologie pozwalające stworzyć zdalne recepcje, z depozytorami kluczy, kamerami z analityką obrazu, współpracujące z firmami ochrony w celu monitorowania miejsc zagrożonych. Powodzeniem cieszy się usługa wideoobchodu, która staje się już nieodłącznym elementem zdalnego ekosystemu ochronnego danego obiektu.

Mam nadzieję, że udało mi się w przystępny sposób przedstawić zderzenie dwóch światów, z których tradycyjna analogowa ochrona fizyczna (osobowa) – w miarę rozwoju nowoczesnych technologii i rosnących cen zatrudnienia – w dużym stopniu odchodzi do lamusa. W dzisiejszym świecie ochrony osób i mienia w Polsce aplikacje i analityka obrazu stają się nieodłącznym elementem zabezpieczeń. Natomiast doświadczenie i profesjonalizm pracownika ochrony, a przede wszystkim zaufanie do niego – to czynniki, które są podstawą w budowaniu relacji z klientami. Stanowią nieocenioną wartość oferowanych usług ochrony osób i mienia. Na końcu każdego, nawet najnowocześniejszego systemu stoi człowiek, który decyduje i analizuje sygnały gromadzone, przetwarzane i odbierane w lokalnych centrach monitoringu.
Czy kiedyś doczekamy się systemów, które nie będą wymagały ingerencji człowieka? A może już takie są?

PAWEŁ MUCHA

Technik ochrony osób i mienia. W branży security od 17 lat. Były funkcjonariusz Policji Komendy Wojewódzkiej w Łodzi. Swoje doświadczenie zdobywał w różnych obszarach ochrony. Prezes jednej z firm ochrony, w której z powodzeniem wdrażał nowe technologie. Obecnie dyrektor ds. rozwoju w Agencji Ochrony Lion.

Różne oblicza bezpieczeństwa infrastruktury krytycznej

Infrastruktura krytyczna, stanowiąc podstawę bezpieczeństwa państwa i obywateli, podlega szczególnym zagrożeniom. Stąd jej bezpieczeństwo jest w interesie nas wszystkich, a tym samym kwestia świadomości bezpieczeństwa w tym obszarze jest istotna, jak nigdzie indziej.

Jacek Grzechowiak

Gdy myślimy o infrastrukturze krytycznej (IK), najpierw kierujemy swoją uwagę na regulacje prawne definiujące tę problematykę. I słusznie, gdyż obszar ten, mając rzeczywiście krytyczny wpływ na nasze życie, jest objęty ścisłymi regulacjami głównie w Ustawie z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym. Patrząc więc z tej perspektywy, infrastrukturą krytyczną są *„...systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania administracji publicznej, a także instytucji i przedsiębiorców”*. Warto zwrócić uwagę na doprecyzowanie mówiące, iż są to obiekty kluczowe dla bezpieczeństwa państwa i jego obywateli. Druga część, czyli systemy kluczowe dla bezpieczeństwa obywateli, dość często jest niesłusznie pomijana i marginalizowana. Na szczęście legislacja traktuje to równoprawnie. Przepisy prawne wskazują grupy obiektów, instalacji i usług krytycznych, którymi są systemy:

- zaopatrzenia w energię, surowce energetyczne i paliwa,
- łączności,
- sieci teleinformatycznych,
- finansowe,
- zaopatrzenia w żywność,
- zaopatrzenia w wodę,
- ochrony zdrowia,
- transportowe,
- ratownicze,
- zapewniające ciągłość działania administracji publicznej,
- produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych[1].

Zakres systemów stanowiących infrastrukturę krytyczną jest szeroki, a ich wpływ na życie obywateli nie bez powodu nazywany jest krytycznym. Dlatego m.in. znajduje tu zastosowanie drugi akt prawny – *Ustawa o ochronie osób i mienia*[2] określająca zasady ochrony obiektów tej kategorii. To jest ściśle związane z bardzo szerokim spektrum zagrożeń charakterystycznych dla tej grupy obiektów, urządzeń, instalacji i usług.

Duże znaczenie tej grupy systemów podlegających ochronie pokazuje nie tylko uregulowanie ich ustawami i rozporządzeniami, ale także *Narodowym Programem Ochrony Infrastruktury Krytycznej*[3]. Ochrona IK jest uregulowana także na poziomie europejskim, w *Dyrektywie Rady 2008/114/WE z 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony*[4].

ZŁODZIEJ ZAWSZE POWODUJE SZKODĘ, ALE NIERAZ SZKODA JEST WIĘKSZA NIŻ WARTOŚĆ SKRADZIONEGO MIENIA

Można dywagować, czy systemy zaopatrzenia w energię, surowce energetyczne i paliwa powinny być wymienione jako pierwsze, co wskazuje niejako na ich najbardziej krytyczny charakter, czy też powinno tam znaleźć się coś innego. Sądzę, że tego typu akademicka dyskusja nie jest tu potrzebna, a każdy zdaje sobie sprawę, że przecież zapewniają one funkcjonowanie całej gospodarki i administracji. Stąd także i tutaj będzie występowała kumulacja zagrożeń, poczynając od tych najpoważniejszych, czyli terrorystycznych.

Nie zmienia to jednak faktu, że znajdziemy tu również incydenty bardziej powszechne, mniejszej rangi, takie jak kradzież. Przykładem może być ujawniony w grudniu 2019 r. incydent w gminie Kosakowo, gdzie sprawcy dokonali nielegalnego podłączenia do podziemnego rurociągu, którym odprowadzali paliwo do własnego dystrybutora, czyniąc straty nie mniejsze niż 500 tys. zł[5].

Przy czym kradzież paliwa, choć duża co do wartości, jest tylko jednym z wielu zagrożeń, jakie są związane z tego typu incydentami, poczynając od zagrożeń środowiskowych, wynikających z niekontrolowanego wycieku paliwa do gleby, kończąc na zagrożeniach pożarem i wybuchem. W każdym wypadku dochodzi również zagrożenie ciągłości działania wynikające ze wstrzymania eksploatacji rurociągu czy to w celu usunięcia wycieku, czy na czas akcji ratowniczo-gaśniczej i późniejszej odbudowy rurociągu.

Z dostępnych danych wynika, że kradzione są też fragmenty rurociągu, jak to miało miejsce w tyskim kompleksie leśnym. Jak wynika z komunikatu policji, złodziej przybył na miejsce incydentu wyposażony *„w butle gazowe, palniki oraz inne akcesoria potrzebne do demontażu rurociągu. Następnie pociął kilka metrów nieczynnego rurociągu i dokonywał jego kradzieży”*[6]. Wartość skradzionego mienia nie była duża, bo wynosiła jedynie 5 tys. zł, ale powszechnie wiadomo, że złodzieje zawsze robią penetrację przestępczą, przygotowując się do swoich działań, i w ten sposób wiedzą, który rurociąg jest nieczynny, i mogą na nim prowadzić swój przestępczy proceder. A gdyby się pomylili i ukradli fragment niewłaściwego rurociągu? Wtedy straty byłyby większe i dotyczyły nie tylko właściciela rurociągu, ale także odbiorców transportowanego nim surowca, powodując wtórne straty dla właściciela w postaci potencjalnych roszczeń odbiorców.

Podobnie ta kwestia przedstawia się w odniesieniu do linii energetycznych – nielegalne podłączenia i kradzieże linii są zmorą dla ich właścicieli. Co istotnie, dotyczy to także linii wysokiego napięcia, np. z rejonu zgorzeleckiego, gdzie złodziej ukradł niemal kilometr napowietrznej linii energetycznej. I nie była to jedyna szkoda, gdyż realizując swój przestępczy proceder, złamał kratownicowy słup energetyczny[7]. Odzyskano tylko 50 m przewodu, straty bezpośrednie wyniosły 36 tys. zł. To problem widziany z perspektywy właściciela rurociągu czy linii energetycznej. Warto jednak popatrzeć także z innej strony, np. instytucji sąsiadującej z takimi obiektami lub odbiorcy usług i mediów. Widać bowiem wyraźnie, że nie będąc obiektem infrastruktury krytycznej, możemy podlegać dokładnie tym samym zagrożeniom, ponieważ wybuch czy pożar może mieć destrukcyjne oddziaływanie na obiekty i mienie, a przerwa w dostawie paliwa, gazu czy prądu może skutkować poważnym uderzeniem w ciągłość działania naszych operacji.

Trzeba też pamiętać o jeszcze jednej ważnej sprawie. Brak paliwa czy energii powoduje szkody także u odbiorców (nie bez przyczyny ten element znajduje się w wykazie systemów stanowiących infrastrukturę krytyczną na pierwszej pozycji). Przypomnę gigantyczną awarię sieci energetycznej pod Szczecinem z kwietnia 2008 r. Z oficjalnych informacji wynika, że była spowodowana obfitymi opadami śniegu, którego naporu nie wytrzymały najpierw drzewa, uszkadzając linie energetyczne i linie trakcji kolejowej. Później był już „tylko” efekt domina... padły stacje transformatorowe, wodociągi itd. Kilkaset tysięcy osób oraz tysiące przedsiębiorstw pozostało bez dostępu do energii, m.in. chłodnie pełne żywności. Pojawiło się szereg wątpliwości, czy nie było to innej przyczyny awarii, która mogła wpłynąć na wytrzymałość słupów energetycznych. Specjaliści wskazywali na wątpliwy stan techniczny słupów energetycznych[8]. Niestety wiadomo że złodzieje złomu w tego typu incydentach dość często mają swój udział – ich działalność dotyczy także kradzieży elementów słupów wysokiego napięcia. Tego typu obiekt, położony w szczerym polu, jest bardzo wygodnym celem. Czy tak było i w tym wypadku, nie ma potrzeby po tylu latach rozważać. Jednak informacje, że takie zdarzenia miały i mają miejsce obecnie, są powszechnie dostępne, np. w Sosnowcu złodzieje, kradnąc elementy słupa wysokiego napięcia, tak bardzo osłabili jego konstrukcję, że w końcu runął, powodując zerwanie linii i stwarzając szereg innych zagrożeń, przede wszystkim wybuch pożaru i porażenie prądem.

Infrastruktura krytyczna podlega wielu zagrożeniom, ważne miejsce paliw i energii jest w pełni uzasadnione, a zagrożenia z pozoru niewielkie mogą w pewnych okolicznościach spowodować krytyczny skutek, dlatego bezpieczeństwo IK ma bezpośredni i ważny wpływ na bezpieczeństwo innych obiektów.

REFLEKSJA NR 1. INCYDENTY NIEWIELKIE MOGĄ POWODOWAĆ SKUTEK KRYTYCZNY. NIE NALEŻY WIĘC ICH LEKCEWAŻYĆ.

SYSTEM IT, CZYLI BITY – SIECI – KOMPUTERY... ALE CZY TYLKO?

Wydawałoby się, że zupełnie inaczej wygląda sprawa z systemami teleinformatycznymi. W centrum uwagi są dziś zagrożenia cybernetyczne. Ale czy rzeczywiście jest inna? Popatrzmy ponownie przez pryzmat incydentów.

Faktycznie incydenty cybernetyczne są mocno reprezentowane. Swoją uwagę koncentrujemy na nieuprawnionym dostępie do danych, jednak zdarzają się także incydenty polegające na blokadzie systemu IT. Czasem takie incydenty powodują nawet dramatyczne skutki, np. atak hakerów na Universitätsklinikum Düsseldorf (UKD) z sierpnia 2020 r. W jego wyniku klinika została wyłączona z systemu medycznego i w efekcie nieprzyjęła pacjentki w poważnym stanie zdrowia, która musiała zostać przewieziona do innego szpitala i niestety pomoc dla niej przyszła za późno[9]. Jak więc widać, ataki hakerów na infrastrukturę IT mogą spowodować dotkliwe skutki, z ofiarami śmiertelnymi włącznie. Popatrzmy na inne incydenty.

Jednym z ciekawszych niecybernetycznych incydentów w systemach IT było (dość dobrze opisane medialnie) wyzwolenie środka gaśniczego z instalacji gaśniczej w serwerowni dostawcy usług internetowych, do którego doszło na warszawskim Ursynowie. Incydent ten spowodował wyłączenie tego miejsca z eksploatacji oraz uszkodzenia w infrastrukturze IT, oddziałujące na klientów tego operatora[10]. Rozmiar strat był ogromny, a zdjęcia pokazujące to miejsce bardziej przypominały krajobraz po eksplozji ładunku wybuchowego niż awarii technicznej. Kluczowe są jednak skutki operacyjne, a te – jak wynika z informacji medialnych – były poważne. Innym przykładem incydentu o znacznym oddziaływaniu może być pożar w budynku, w którym była zlokalizowana serwerownia operatora telefonii komórkowej na warszawskim Annopolu. Doszło do niego w styczniu 2019 r.[11]. Skutki operacyjne trwały wiele dni, a przecież wiele usług jest obecnie realizowanych z wykorzystaniem transmisji danych via sieci telefonii komórkowej.

Przykłady te pokazują, że bezpieczeństwo infrastruktury krytycznej słusznie jest traktowane w sposób szczególny i wymaga od osób i podmiotów za nie odpowiedzialnych patrzenia nie tylko z perspektywy tych obiektów, ale także przez pryzmat bezpieczeństwa obiektów sąsiadujących.

REFLEKSJA NR 2. ŻADEN SCENARIUSZ ATAKU NIE JEST ABSURDALNY. A PRZYNAJMNIEJ NIE POWINIEN BYĆ.

SYSTEMY RATOWNICZE...?

Rozważając kwestie bezpieczeństwa, w tym także bezpieczeństwa infrastruktury krytycznej, nie sposób nie spojrzeć na systemy ratownicze. Dobrze wiemy, że ratownictwo pełni istotną funkcję w bezpieczeństwie publicznym, dlatego znalazło swoje miejsce w infrastrukturze krytycznej. Czasami jednak szewc bez butów chodzi. Przykłady są tu na szczęście nieliczne, ale się zdarzają. Pogotowie ratunkowe? Było takie zdarzenie, np. niedawny pożar w Stacji Pogotowia Ratunkowego w Oleśnicy[12]. Policja? Tu też zdarzają się incydenty, które niekiedy mogą mieć drugie dno, jak w przypadku pożaru w listopadzie 2019 r. w Komendzie Powiatowej Policji w Raciborzu, gdzie po pożarze stwierdzono... brak broni[13].

Straż pożarna? I tutaj coś się może zdarzyć, np. pożar w województwie wielkopolskim, w wyniku którego spłonął sprzęt strażacki o wartości 80 tys. zł[14].

Co tak naprawdę mieści się w systemie ratownictwa? Postawię tezę, że w jego skład – patrząc od strony operacyjnej – wchodzi także ochrona, gdyż zespoły ochronne, realizując działania w zakresie ochrony osób i mienia, wielokrotnie prowadzą działania bezpośrednio lub pośrednio ratownicze i równie często w takich działaniach uczestniczą, wykonując czynności mające bezpośredni wpływ na skuteczność działań ratowniczych.

Przykłady? Duży zakład przemysłowy to niemal miasto. Przyjeżdzający do niego zastęp strażacki czy zespół pogotowia ratunkowego z reguły go nie znają lub znają bardzo słabo. To właśnie zespół ochronny pilotuje ich tam, gdzie ich pomoc jest potrzebna. I to od pracowników ochrony zależy, czy pomoc dotrze na czas. A jest ona zapewniana nie tylko poprzez pilotaż. To także powiadamianie i alarmowanie, wystawienie punktów regulacji ruchu, ich odpowiednie oznakowanie, kierowanie innych pojazdów na objazdy, by zapewnić maksymalną drożność dróg, a także szereg innych działań. Jeśli popatrzymy na te zadania przez pryzmat niedawnej eksplozji i pożaru w zakładach chemicznych w Oświęcimiu, zauważymy i docenimy znaczenie zespołu ochrony w realizacji działań ratowniczo-gaśniczych.

Podobnych przykładów można podać dużo więcej, a wielkość obiektu wcale nie musi tu być nomen omen krytyczna. Duży zakład przemysłowy, port lotniczy lub morski czy dowolny obiekt rozległy to przykłady niebudzące wątpliwości, ale spróbujmy sobie wyobrazić pracownika ochrony prowadzącego obserwację kompleksu leśnego. A przecież również takie zadania wykonują pracownicy ochrony. Jeśli porównać to z pożarem w Kuźni Raciborskiej – największym pożarem w Europie Środkowej po II wojnie światowej – widać znaczenie ich pracy[15]. Spójrzmy na niewielki (w kontekście powyższych przykładów) obiekt biurowy, który z natury rzeczy ma skomplikowaną architekturę wewnętrzną. Tu także czas dotarcia służb ratowniczych zależy od wsparcia pracowników ochrony. Dlatego kompetencje pracowników tego pionu, zwłaszcza znajomość topografii (zarówno zewnętrznej, jak i wewnętrznej) chronionych obiektów to sprawa niezmiernie ważna, może bowiem ułatwić, ale niestety także utrudnić, akcję ratowniczą. Pomoc pracowników ochrony jest tu nie do przecenienia, a jakość ich pracy ma bezpośredni wpływ na działania ratownicze. Tym samym – w mojej ocenie – oni także są częścią systemu ratownictwa.

1) https://rcb.gov.pl/infrastruktura-krytyczna [dostęp: 5.03.2021].
2) DzU z 2020 r., poz. 838.
3) http://rcb.gov.pl/narodowy-program-ochrony-infrastruktury-krytycznej-2/ [dostęp: 05.03.2021]
4) https://op.europa.eu/pl/publication-detail/-/publication/ba51b03f-66f4-4807-bf7d-c66244414b10/language-pl [dostęp: 5.03.2021].
5) https://policja.pl/pol/aktualnosci/183028,44-latek-zatrzymany-za-kradziez-z-wlamaniem-do-rurociagu-z-paliwem.html [dostęp: 5.03.2021].
6) https://tychy.policja.gov.pl/k27/informacje/wiadomosci/65404,Rurociag-na-zlom.html [dostęp 05.03.2021]
7) https://zgorzelec.naszemiasto.pl/zlapali-go-na-kradziezy-linii-wysokiego-napiecia-spowodowal/ar/c4-4403120 [dostęp: 5.03.2021].
8) https://gp24.pl/awaria-w-szczecinie-to-nie-byla-wina-pogody/ar/4343519 [dostęp: 5.03.2021].
9) https://www.zdf.de/nachrichten/panorama/hacker-angriff-uniklinik-duesseldorf-100.html [dostęp: 5.03.2021].
10) https://niebezpiecznik.pl/post/wybuch-gazu-w-serwerowni-netii/ [dostęp: 5.03.2021].
11) https://www.rp.pl/Telekomunikacja-i-IT/190139878-Awaria-w-T-Mobile-pozar-unieruchomil-systemy.html [dostęp: 5.03.2021].
12) https://gazetawroclawska.pl/pozar-garazy-pogotowia-ratunkowego-splonela-karetka/ar/c1-15385295 [dostęp: 5.03.2021].
13) https://wiadomosci.radiozet.pl/Polska/Raciborz.-Pozar-w-Komendzie-Policji.-Policjant-zglosil-zaginiecie-broni [dostęp: 5.03.2021].
14) https://www.tvp.info/19411804/pozar-w-remizie-strazackiej-splonal-drogi-sprzet [dostęp: 5.03.2021].
15) https://pl.wikipedia.org/wiki/Po%C5%BCar_lasu_w_nadle%C5%9Bnictwie_Rudy_Raciborskie [dostęp: 5.03.2021].

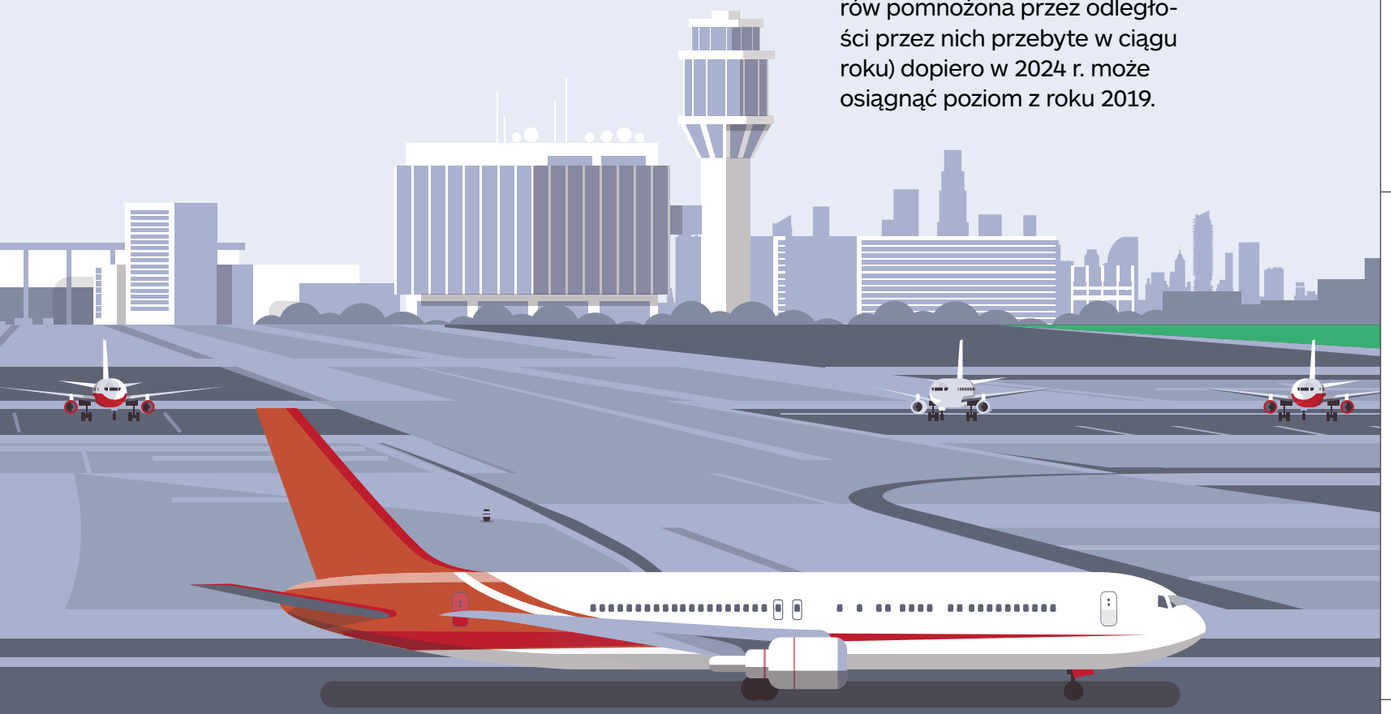
JACEK GRZECHOWIAK

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

Ruch lotniczy

Statystyki potwierdzają duże spadki

Międzynarodowe Stowarzyszenie Transportu Lotniczego (IATA) opublikowało światowe dane na temat wpływu pandemii na przemysł lotniczy. Według nich przychody pasażerskich linii lotniczych na całym świecie w 2020 r. spadły o ok. 314 mld USD (co oznacza spadek o 55% w porównaniu z 2019 r.), a wskaźnik RPK (liczba pasażerów pomnożona przez odległości przez nich przebyte w ciągu roku) dopiero w 2024 r. może osiągnąć poziom z roku 2019.



Zamknięcie ruchu pasażerskiego przyniosło straty także w całej branży lotniczej i turystycznej w Polsce. Statystyki nie są optymistyczne...

Polska Agencja Żeglugi Powietrznej zaprezentowała raport dotyczący zmian w ruchu lotniczym w polskiej przestrzeni powietrznej w 2020 r. w porównaniu z rokiem 2019. Przygotowano go na podstawie danych własnych oraz europejskiej organizacji ds. bezpieczeństwa żeglugi powietrznej Eurocontrol *(European Organisation for the Safety of Air Navigation)*. Statystyki pokazują, że ruch lotniczy cofnął się do poziomów sprzed 2010 r.

Największą liczbę operacji w polskiej przestrzeni powietrznej odnotowano w I kwartale ub. roku: w styczniu (67,1 tys.), w lutym (60,5 tys.) oraz w marcu (37,5 tys.). W styczniu i lutym zanotowano wzrost ruchu odpowiednio o 5,5% i 7%.
Największe spadki pojawiły się w czasie pierwszego lockdownu w kwietniu (-87%), maju (-85%) i czerwcu (-83%). W całym 2020 r. liczba wszystkich operacji lotniczych IFR spadła o 58,7% do poziomu 376,9 tys.
Spośród krajowych lotnisk największe spadki zanotowano w Warszawie (-59%), Krakowie (-57%), Wrocławiu i Modlinie (-56%). Najmniejsze straty w ruchu lotniczym odnotowano w Zielonej Górze (-12%), Łodzi (-38%) oraz Olsztynie-Szymanach (-38%). Całkowita liczba operacji na polskich lotniskach spadła o 56,4%, osiągając poziom 193,7 tys. operacji.

LICZBA OPERACJI LOTNICZYCH NA WSZYSTKICH POLSKICH LOTNISKACH W 2020 R.

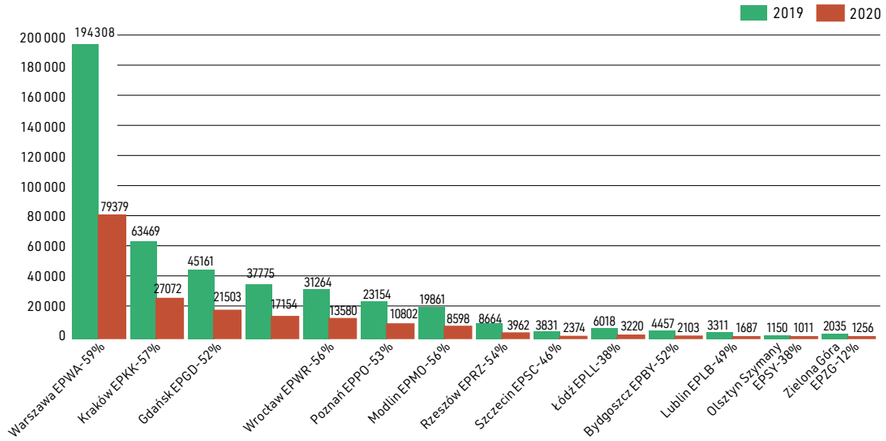
- 193 701 (444 661 w 2019 r.) – spadek o 56,4%

LICZBA WSZYSTKICH OPERACJI LOTNICZYCH, W TYM PRZELOTY TRANZYTOWE W 2020 R.

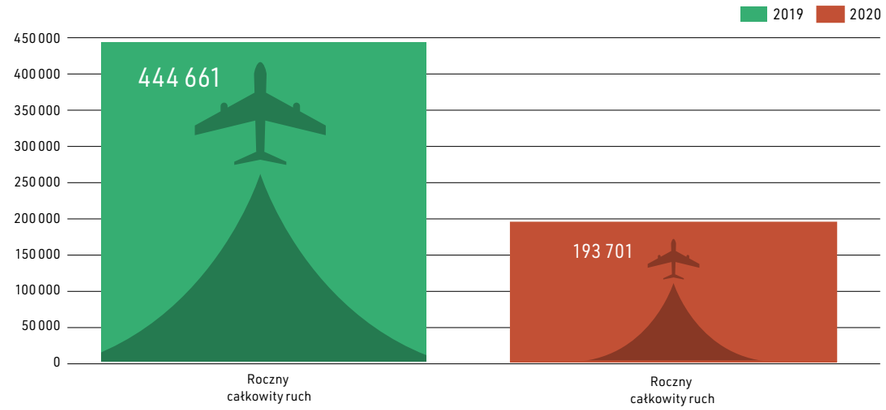
- 376 969 (912 455 w 2019 r.) – spadek o 58,7% rok do roku

Prezentowane dane pochodzą z systemów Network Managera i zawierają informacje o ruchu GAT IFR, bez uwzględnienia ruchu OAT i General Aviation.

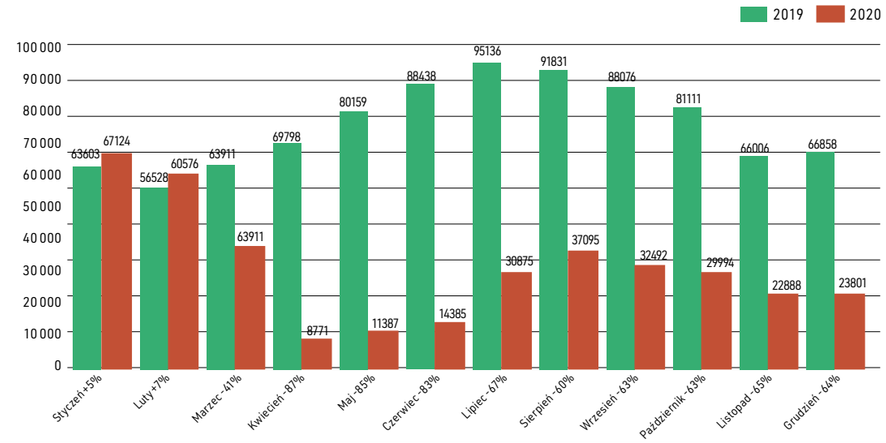
Wykres. 1. Ruch lotniczy na polskich lotniskach w 2019 i 2020 r.



Wykres. 2. Całkowity ruch lotniczy na polskich lotniskach w 2019 i 2020 r.



Wykres. 3. Ruch lotniczy w Polsce w 2020 i 2019 r.

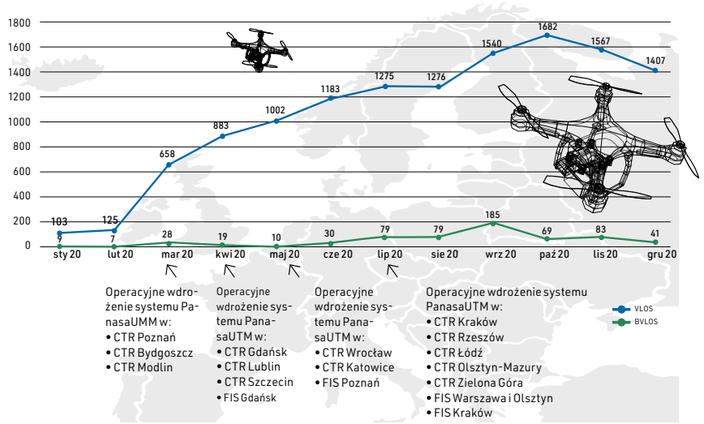


Drony nad Polską

Polska Agencja Żeglugi Powietrznej zaprezentowała raport ze statystykami lotów bezzałogowych statków powietrznych (BSP) w polskiej przestrzeni powietrznej w 2020 r.[1] Raport został przygotowany na podstawie danych własnych PAŻP z systemu PansaUTM[2] oraz aplikacji Drone Radar. Zebrane dane pokazują, że ruch BSP sukcesywnie rośnie.

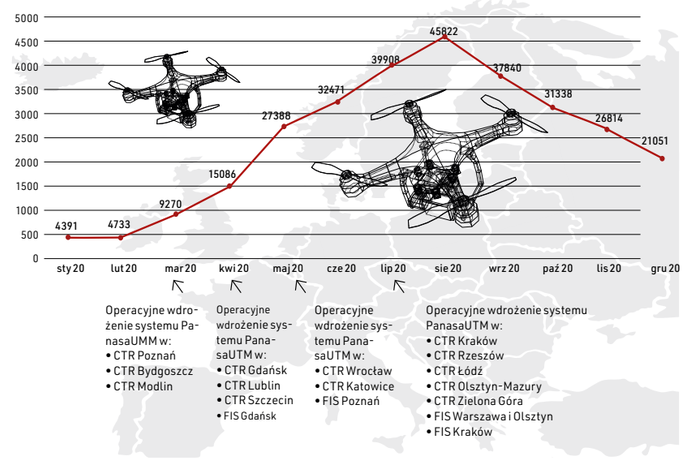
W 2020 r. liczba misji skoordynowanych w systemie PansaUTM, pozostających w zasięgu wzroku operatora (VLOS[3]) wyniosła 12 701, a poza zasięgiem wzroku operatora (BVLOS[4]) 639. Natomiast liczba misji skoordynowanych manualnie (przed operacyjnym wdrożeniem PansaUTM na kolejnych wieżach – TWR) wyniosła 949 dla VLOS i 143 dla BVLOS. Całkowita liczba zgłoszeń (check-inów) w aplikacji DroneRadar za rok 2020 to 296 112. W ubiegłym roku wydano także 143 depesze NOTAM dot. lotów BVLOS.
Największą liczbę operacji dronowych w polskiej przestrzeni powietrznej odnotowano pod koniec III kwartału i w IV kwartale ub.r. we wrześniu (1540), w październiku (1682), listopadzie (1567) i grudniu (1407).

Wykres 1. Liczba misji skoordynowanych w systemie PansaUTM w 2020 r.



Największa liczba zgłoszeń (check-inów) w aplikacji DroneRadar przypadała na okres letni: czerwiec, lipiec, sierpień i wrzesień. Najwięcej zgłoszeń wykonano w tej aplikacji w sierpniu 2020 r. – dokładnie 45 882.

Wykres 2. Liczba check-inów w aplikacji DroneRadar w 2020 r.



Liczba misji skoordynowanych przez PAŻP manualnie, wraz z wdrażaniem systemu PansaUTM na kolejnych wieżach, sukcesywnie malała.
System PansaUTM jest w Polsce stopniowo wdrażany od 2 marca 2020 r. Stanowi podstawę rozwoju koncepcji U-Space zakładającej bezpieczną i efektywną integrację lotów załogowych (SP) i bezzałogowych statków powietrznych (BSP). Na system składają się autorskie rozwiązania operacyjne PAŻP oraz część systemowa zintegrowana z najbardziej popularną wśród operatorów dronów w Polsce aplikacją mobilną Droneradar. Pozwala m.in. na szybką cyfrową, niewerbalną komunikację pomiędzy kontrolerami ruchu lotniczego i operatorami dronów.
W lutym 2021 r. wdrożono PansaUTM w wersji 1.2 z licznymi nowymi funkcjami dla pilotów BSP oraz dla kontrolerów ruchu lotniczego i informatorów służby informacji podwietrznej, m.in. funkcją tzw. automatycznych zezwoleń dla najczęściej latających pilotów czy specjalne funkcje dla służb porządku publicznego. System PansaUTM został już operacyjnie wdrożony na wszystkich aktywnych wieżach kontroli lotniska i sektorach służby informacji powietrznej w całej Polsce.

1) https://www.pansa.pl/podsumowanie-operacji-dronowych-bsp-w-2020-r/
2) PansaUTM to cyfrowa koncepcja koordynacji lotów BSP oraz cyfrowego zarządzania wnioskami i zgodami na loty w przestrzeni powietrznej, na którą składają się autorskie rozwiązania operacyjne PAŻP oraz część systemowa, zintegrowana z najbardziej popularną wśród operatorów dronów w Polsce aplikacją mobilną Droneradar.
3) VLOS – *(Visual Line of Sight)* operacje, w których operator lub obserwator bezzałogowego statku powietrznego utrzymują bezpośredni kontakt wzrokowy z bezzałogowym statkiem powietrznym w celu zapewnienia separacji od innych statków powietrznych i przeszkód.
4) BVLOS – *(Beyond Visual Line of Sight)* operacje poza zasięgiem wzroku operatora bezzałogowego statku powietrznego.

Bezpieczne lotniska

Pandemia COVID-19 odbiła się na działalności sektora lotniczego. Lockdown i ograniczenia w przemieszczaniu się ludności sprawiły, że przychody lotnisk znacznie spadły. Czy nie ograniczy to inwestycji w bezpieczeństwo? O tym i innych problemach sektora rozmawiamy z **ekspertem ds. lotnictwa, Piotrem Rotmańskim z firmy Air Innovations**.

Lotniska są jedną z tych gałęzi gospodarki, które najbardziej ucierpiały w wyniku pandemii COVID-19. Jaka jest teraz ich ogólna sytuacja ekonomiczna w Polsce?
O kondycji lotnisk świadczą dane statystyczne dotyczące ruchu, które można zaczerpnąć z dwóch źródeł. Pierwszym jest Polska Agencja Żeglugi Powietrznej, która podała, że ruch IFR w polskiej przestrzeni powietrznej spadł w 2020 r. porównaniu z rokiem poprzednim o 60%. Ruch IFR jest o tyle istotny, że jest to działalność komercyjna. Można więc przyjąć, że przychody również spadły o co najmniej 60%. Drugim źródłem jest Związek Regionalnych Portów Lotniczych, który informuje, że liczba pasażerów w 2020 r. zmniejszyła się o 65% w porównaniu z rokiem 2019. Widać więc, że pandemia i ograniczenia związane z funkcjonowaniem lotnictwa w całym kraju spowodowały, że ten czas nie był łaskawy dla tego sektora i na pewno wpłynął na duże spadki przychodów.

Te wartości są faktycznie duże, tym bardziej że nie dotyczą jeszcze pierwszego kwartału ub.r. Jaki wpływ na przychody miała wielkość lub lokalizacja portu lotniczego?
Sytuacja wygląda różnie. Wiadomo że duże lotniska traciły ruch później niż mniejsze. Było to związane z szybciej wprowadzanymi ograniczeniami w małych portach lotniczych przez samych przewoźników. Duże lotniska szybciej też odzyskiwały ruch, ponieważ przewoźnicy wracali tam, gdzie możliwość zarobku i odbudowania strat była większa. Lecz miały one większe koszty bieżące, które mogły zostać zbilansowane po wznowieniu funkcjonowania. Z kolei po utracie przychodów z powodu lockdownów zarządzający mieli problemy z utrzymaniem płynności finansowej, zwłaszcza że większość z nich nie zdecydowała się na zwolnienia, gdyż o doświadczonych pracowników w tym sektorze jest trudno. Proces pozyskania i wyedukowania nowych jest długi i kosztowny, dlatego każdy chciał zatrzymać wykwalifikowaną kadrę. W innej sytuacji były natomiast małe lotniskach, które nawet przed pandemią były często deficytowe, nie generowały zysku i trzeba było do nich dopłacać. Wspierały je najczęściej samorządy, będące ich udziałowcami, które w swoich budżetach miały na to specjalne środki.

Czy uszczuplenie budżetu nie wpłynie negatywnie na bezpieczeństwo pasażerów?
Nie wpłynie i nie może wpłynąć. Zarządzający będą musieli szukać oszczędności i pozyskiwać fundusze z innych źródeł. Bezpieczeństwo w rozumieniu safety i ochrona rozumiana jako security są w lotnictwie sprawą kluczową. Na tym się nie oszczędza, tego wymagają przepisy. Lotniska są pod ścisłym nadzorem i Urzędu Lotnictwa Cywilnego, i Straży Granicznej, jeśli chodzi o kontrolę bagażu i towaru oraz zapewnienia bezpieczeństwa pasażerów. Przepisy są cały czas aktualizowane, zgodne z wytycznymi UE, tym samym podnosi się poziom bezpieczeństwa na polskich lotniskach.

Czy w związku z pandemią zmieniły się procedury dotyczące zapewnienia bezpieczeństwa pasażerom?
Procedury są takie same, obecnie natomiast musimy pracować w reżimie sanitarnym. Obowiązuje kontrola temperatury ciała, dezynfekcja rąk za pomocą specjalnie do tego celu ustawionych stanowisk, przestrzeganie dystansu i noszenie maseczek zakrywających usta i nos. Ponadto prace porządkowe i czyszczenie filtrów klimatyzacji odbywają się częściej.

Pomocne w niezbędnej kontroli mogą być elektroniczne systemy zabezpieczeń, zwłaszcza w miarę wzrostu natężenia ruchu.
Trzeba powiedzieć otwarcie, że przed pandemią nie było potrzeby mierzenia temperatury ani podróżnym, ani pracownikom. COVID-19 wymusił na zarządzających wprowadzenie rozwiązań technologicznych do tego celu. W zależności od wielkości i natężenia ruchu są to kontrole manualne za pomocą termometru, w przypadku większych lotnisk zaawansowane systemy, czyli bramki automatycznie mierzące temperaturę przy użyciu kamer termowizyjnych.
Sytuacja spowodowana pandemią jest na tyle dynamiczna, że nie można skupić się tylko na jednym elemencie. W miarę możliwości trzeba kontrolować wszystkie aspekty bezpieczeństwa. Oczywiście poszerzamy możliwości systemu CCTV o wykrywanie maseczki czy inne funkcjonalności. To jest powtórzenie zasady DDM, czyli dystans, dezynfekcja, maseczki. Lotniska są takimi miejscami, gdzie koncentruje się duża grupa ludzi, często przyjeżdżających z różnych stron świata, więc ryzyko przenoszenia wirusa i zakażenia jest znacznie większe, dlatego ważne jest zachowanie odpowiedniego dystansu i przestrzeganie procedur sanitarnych. W tym mogą być pomocne systemy zabezpieczeń działające już na lotniskach.

Czy w przyszłości znajdą się środki na modernizację systemów zabezpieczeń?
Sytuacja będzie wymuszała znalezienie funduszy na inwestycje w bezpieczeństwo. I to na różnych płaszczyznach: od elektronicznych systemów zabezpieczeń i ochrony fizycznej po cyberbezpieczeństwo. Dużym wyzwaniem dla zarządzających lotniskami będzie ochrona przed dronami. I to zarówno w kategorii safety, kiedy ktoś nieświadomy ograniczeń przepisów ruchu lotniczego bawi się dronem i w ten sposób stwarza zagrożenie dla ruchu lotniczego, jak i bardziej intencjonalnym użyciu dronów jako środka aktu terrorystycznego. Z mojego punktu widzenia będzie to dużym wyzwaniem, gdyż dronów jest coraz więcej, znajdują zastosowanie w różnych sferach działalności gospodarczej. Siłą rzeczy incydentów z dronami będzie przybywać.

Czy uważa Pan, że obowiązujące od stycznia tego roku nowe przepisy* dotyczące wykonywania lotów dronami pomogą zapewnić bezpieczeństwo?
Konieczność rejestrowania bezzałogowych statków powietrznych (BSP) powyżej 250 g może w znaczeniu safety, czyli nieintencjonalnym zagrożeniu. Ale jeśli ktoś będzie chciał przeprowadzić atak terrorystyczny, to żadne przepisy mu nie przeszkodzą. Dziś systemy antydronowe nie utworzą „szczelnej kopuły" nad lotniskiem, a jednocześnie brakuje rozwiązań prawnych, które pozwoliłyby takie systemy zastosować. Dzisiaj nie można drona, który znalazł się w przestrzeni powietrznej lotniska, zneutralizować, bo jego właściciel mógłby domagać się odszkodowania w przypadku jego uszkodzenia...

Dużo mówiliśmy o rozwiązaniach technicznych. A jak powinna być zorganizowana ochrona fizyczna lotnisk?
Ochronę fizyczną można realizować na różne sposoby. Generalnie za system ochrony lotniska odpowiedzialny jest zarządzający. W ramach swoich kompetencji może utworzyć wewnętrzną służbę, może też wykonywanie tych czynności powierzyć wykwalifikowanej firmie ochrony. W obu przypadkach to on odpowiada za bezpieczeństwo w obiekcie. Może także zastosować model mieszany, np. ochronę posterunków czy patrole na lotnisku wykonuje służba wewnętrzna, natomiast kontrola bezpieczeństwa pasażerów jest realizowana przez firmę zewnętrzną. Te czynności są pod stałym nadzorem Urzędu Lotnictwa Cywilnego. Tam, gdzie są lotnicze przejścia graniczne, kontrolą zajmują się funkcjonariusze Straży Granicznej.

Sytuacja spowodowana pandemią jest bardzo trudna. Co można dziś coś zrobić, aby ją poprawić?
Można działać lokalnie, ale ważne jest też wsparcie państwa. Można się pokusić o takie rozwiązania, żeby np. służby ochrony lotniska i straż pożarną włączyć w struktury państwowe albo przynajmniej część tych kosztów scedować na państwo. Zgodnie z prawodawstwem UE ochrona lotnisk, w tym ppoż., należy do zadań państwa, więc albo państwo może ją samo realizować, albo może te działania finansować. Przykładowo kontrolą bezpieczeństwa na lotniskach w Stanach Zjednoczonych zajmuje się agencja rządowa TSA (Transportation Security Administration). Jej finansowanie odbywa się poprzez opłaty wliczone w cenę biletu. W takiej sytuacji jest gwarancja, że rząd ma te zadania pod swoją opieką i do żadnych nieprawidłowości nie dojdzie. Korzyścią dla zarządzających jest to, że te środki finansowe u nich zostają i mogą je przeznaczyć na inne cele. W Polsce wniosek o takie rozwiązanie został złożony w 2019 r., jeszcze przed pandemią, przez samorząd Województwa Kujawsko-Pomorskiego na komisji wspólnej rządu i samorządu terytorialnego. To byłoby dla zarządców polskich lotnisk dużym ułatwieniem.

Jak Pan widzi przyszłość lotnisk w Polsce w aspekcie zastosowania elektronicznych systemów zabezpieczeń?
Przyszłość zdecydowanie należy do systemów wyposażonych w sztuczną inteligencję i uczenie maszynowe. Już teraz widzimy wzrost automatyzacji, nie tylko w lotnictwie. Jest to już ogólny trend na rynku. Przykładowo prace nad autonomicznymi oczyszczarkami lotnisk, które nie będą wymagały nadzoru ze strony operatora-kierowcy, są już w znacznym stopniu zaawansowane. To pomaga zmniejszyć koszty, wiadomo przecież, że w każdym przedsiębiorstwie, również takim, jakim jest lotnisko, najdroższa jest praca człowieka. A tu pracuje wiele osób.
Jeśli natomiast chodzi o systemy zabezpieczeń, to nowe technologie stosujemy już od dawna. Przykładowo, jeśli na lotnisku jest zainstalowanych kilkadziesiąt lub kilkaset kamer, to sztuczna inteligencja podpowiada operatorowi, na obraz z której kamery należy zwrócić uwagę, bo tam dzieje się coś niepokojącego. Człowiek nie ma takiej podzielności uwagi, żeby jednocześnie obserwować obrazy na kilkudziesięciu monitorach (efektywnie może maks. osiem) lub nadzorować parametry ogromnej liczby innych sensorów. Również podczas kontroli bagażu to program urządzenia skanującego dokonuje szybkiej oceny, czy w danej walizce jest coś podejrzanego, na co operator powinien zwrócić uwagę, czy też można ten bagaż przepuścić.
Trzeba też pamiętać, że w dzisiejszym lotnictwie cywilnym, w przewozie komercyjnym, najwięcej różnego rodzaju zdarzeń i problemów jest niestety związanych z człowiekiem, który stanowi najsłabsze ogniwo w całym systemie bezpieczeństwa. Wsparcie pracy człowieka nowoczesnymi rozwiązaniami jest więc jak najbardziej potrzebne i oczekiwane.

* ROZPORZĄDZENIE WYKONAWCZE KOMISJI (UE) 2019/947 z 24 maja 2019 r. w sprawie przepisów i procedur dotyczących eksploatacji bezzałogowych statków powietrznych (rozporządzenie stosuje się od 31 grudnia 2020 r.)

O odpowiedzialności za bezpieczeństwo IK

Michał Zalewski

Bezpieczeństwo obiektów infrastruktury krytycznej wydaje się – powiem nieco przewrotnie – tematem mało interesującym. Lista obiektów dokładnie określona ustawą, zasady projektowania raczej znane (chociażby wytyczne Techom), projektanci i wykonawcy wyspecjalizowani i kompetentni, bezpieczeństwo infrastruktury IT dość powszechnie przestrzegane i precyzyjnie prowadzone przez działy IT przedsiębiorstw i instytucji.

W zasadzie jesteśmy w strefie komfortu, ale postaram się wyprowadzić z niej czytelnika. Zachęcić do spojrzenia z nowej perspektywy lub w nowym kontekście. Swoje rozważania zacznę od listy obiektów infrastruktury krytycznej. Teoretycznie jest ona, moim zdaniem, określona precyzyjnie, ale czy ktoś rok temu przewidywał, że obiekty Agencji Rezerw Materiałowych (oprócz magazynów paliw), system przechowywania i dystrybucji szczepionek (był w ogóle taki wcześniej?) oraz system rejestracji i obsługi pacjentów będą obiektami i usługami w powszechnym rozumieniu najwyższej (krytycznej) wagi?

Kto przewidział rok temu, że częsty w centralach obsługujących różne instytucje brak systemu kolejkowania będzie powodował ogromne problemy społeczne? Albo że Stadion Narodowy stanie się szpitalem tymczasowym? Kto się spodziewał, że Sanepid będzie jedną z ważniejszych instytucji w kraju, a osoba piastująca funkcję Głównego Inspektora Sanitarnego stanie się powszechnie znana i często zapraszana do zabierania głosu?

Podaję te przykłady dla potwierdzenia następującej tezy: coraz trudniej w dzisiejszym świecie określić, co jest albo co za chwilę będzie infrastrukturą krytyczną. Jak zareagowałby świat, gdyby największy portal społecznościowy jutro przestał działać? Z niewiadomych powodów i nie wiadomo na jaki czas. Trudno sobie wyobrazić. Na pewno dla całego świata byłby to temat numer 1.

Co to może oznaczać dla naszej branży, która ma ogromny udział w bezpieczeństwie wszelkich obiektów? Czy da się wszystkie obiekty przygotować tak, by można je było przekształcić w fortece

W DZISIEJSZYM ŚWIECIE CORAZ TRUDNIEJ OKREŚLIĆ, CO JEST ALBO CO ZA CHWILĘ BĘDZIE INFRASTRUKTURĄ KRYTYCZNĄ

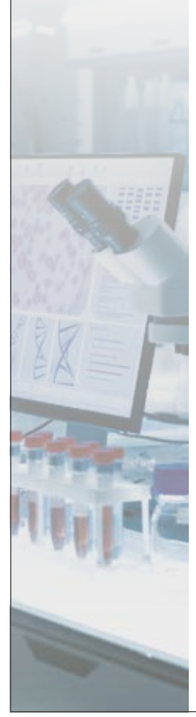
gwarantujące bezpieczeństwo przebywających w nich osób, gromadzonych danych lub towarów? Bez szans. Dlaczego zatem o tym piszę? Otóż uważam, że o ile nie da się przygotować wszystkich obiektów do spełniania krytycznych funkcji, o tyle nasze systemy zabezpieczeń muszą być tak projektowane, budowane oraz utrzymywane, by stosunkowo łatwo można było podnosić ich status na wyższe poziomy bezpieczeństwa. I co ważne, w mojej ocenie, nie stoi to w sprzeczności z normalnymi warunkami budowania systemów bezpieczeństwa. Wiele słów, mało konkretów, więc do nich przechodzę.

PO PIERWSZE: PROJEKTOWANIE I DOKUMENTACJA

Rzetelne dokumentowanie założeń technicznych będących podstawą projektowania, fundament można by powiedzieć. Kolejny krok: precyzyjne uzgodnienia na stykach branż. Co z tego, że obiekt jest wyposażony w nowoczesny system SSWiN, jeżeli z powodu braku odpowiednich uzgodnień zamiast kontaktronów wpuszczanych w elementy stolarki zastosowano nawierzchniowe, nawet po stronie chronionej, ale nawierzchniowe. Tak łatwo popełnić niemożliwy do usunięcia błąd. Na koniec dokumentacja powykonawcza, jakże ważna. A jak często spotykamy w obiektach dokumentację wykonawczą ostemplowaną jako powykonawcza! I nieodnoszącą się dokładnie do stanu faktycznego. To nie jest odosobniona praktyka.

PO DRUGIE: URUCHOMIENIA

Prawidłowe ich zaplanowanie, dokładne określenie, uzgodnienie, a następnie wyegzekwowanie warunków przeprowadzenia uruchomień. Czytelnicy wiedzą zapewne, o czym piszę. Oto przykład: co nam po doskonałym systemie KD, jeżeli drzwi się nie domykają, zacinają zamki albo blokują mechanicznie zawiasy lub skrzydła. Na wykonawcy instalacji systemu ciąży obowiązek przeprowadzenia uzgodnień, o których wspomniałem. Nie da się wybudować bezpiecznego budynku, jeżeli nie zagwarantujemy odpowiedniego czasu na uruchomienia i testy weryfikacyjne instalacji. Kto dowolnie skraca ten czas, świadomie obniża poziom bezpieczeństwa obiektu. Trzeba głośno i wyraźnie o tym mówić, to nasz obowiązek jako specjalistów.



PO TRZECIE: EKSPLOATACJA

Jakże zależna od obu wcześniejszych etapów. Prawidłowo udokumentowany obiekt, w pełni uruchomiony i dokładnie przetestowany to warunek niezbędny do rozpoczęcia bezpiecznej eksploatacji. I nie mam na myśli oświadczenia kierownika robót czy podpisanego protokołu odbioru, ale rzeczywiste efekty pracy projektanta i wykonawcy.

Zgadzam się, że eksploatacja polega na ciągłym usuwaniu usterek urządzeń, ale nie można zostawiać niedokończonych i nie do końca uruchomionych instalacji. To jest po prostu nierzetelne. I nie jest wytłumaczeniem, że po otwarciu obiektu dostęp do urządzeń jest utrudniony. Nie jest wytłumaczeniem, że było za mało czasu na testy, strojenie i kalibrację. Trzeba było głośno i wyraźnie to artykułować i walczyć o ten czas.

Ktoś to może skomentować: łatwo powiedzieć, trudniej zrobić. Wiem o tym, wypowiadam się na podstawie własnych doświadczeń. Chciałbym nieraz cofnąć czas i zrobić coś lepiej, ale nie da się. Można i trzeba jednak wyciągać wnioski z przeszłości, to nauka na przyszłość.

Wyobraźmy sobie taką historię: nieprawidłowo uruchomiony SSP na Stadionie Narodowym. Niewielkie błędy w wizualizacji. Brak możliwości identyfikacji miejsca alarmu I stopnia. W konsekwencji alarm II stopnia i niepotrzebna ewakuacja lub zbyt pochopne skasowanie alarmu i zbyt krótki czas ewakuacji. W przypadku imprezy sportowej może to oznaczać kłopoty, ale dla szpitala… to może być dramat albo tragedia. (Dla pewności: sytuacja wymyślona przeze mnie na potrzeby tego artykułu).

Podsumowując ten wątek, każdy obiekt może nagle stać się obszarem infrastruktury, od której zależy bezpieczeństwo wielu osób. Należy się więc starać, by każdy obiekt przygotować jak najlepiej do zapewniania maksymalnego poziomu bezpieczeństwa, odpowiednio dbając o jakość projektu, wykonawstwa i eksploatacji. Co ważne, niejako przy okazji umożliwiamy jego szybkie dostosowanie do wyższych wymagań w przyszłości, również takich, jakie nawet nie przychodzą nam do głowy.

Odpowiedzialność za systemy bezpieczeństwa jest ogromna. Musimy o tym pamiętać, ale również nie możemy pozwalać, by inni o tym zapominali. Kierowca autobusu nigdy nie pozwoli związać sobie jednej ręki i prowadzić pojazd bez pełnej

KIEDY INŻYNIEROWIE ODPOWIEDZIALNI ZA PROJEKTY NIE BĘDĄ MUSIELI ZAJMOWAĆ SIĘ INTERPRETACJĄ ZAPISÓW LUB PRÓBĄ POGODZENIA SPRZECZNYCH WYTYCZNYCH, ALE BĘDĄ MOGLI SIĘ SKONCENTROWAĆ NA JAKOŚCI SWOJEJ PRACY?

kontroli. Na 100% zatrzyma się w najbliższym bezpiecznym miejscu. I czytelnik-specjalista też nie powinien godzić się na ograniczanie mu możliwości zaprojektowania i wybudowania dobrze funkcjonujących systemów bezpieczeństwa. W przeciwnym razie jego obowiązkiem jest „zatrzymać pojazd" (tylko pamiętajmy o wybraniu bezpiecznego momentu zatrzymania).

Celowo nie piszę o zasadach projektowania systemów zabezpieczeń w obiektach IK. Prawdopodobnie większość czytelników je zna, podobnie jak zna specyficzne rozwiązania: czujki mikrofalowe i dualne, antymasking, funkcje anti-passback, ochrona przed zasłonięciem obrazu z kamery, zabezpieczenie przed zmianą kąta widzenia kamery, czytniki biometryczne w KD, analityka wizji w VSS/CCTV rozpoznająca twarz czy wykrywająca porzucony bagaż, kamery megapikselowe zamiast kamer obrotowych, kamery termowizyjne, systemy identyfikacji tablic rejestracyjnych czy systemy ochrony obwodowej terenu zewnętrznego. To cała paleta rozwiązań przeznaczonych do takich obiektów. Zasady ich projektowania i funkcjonalności są często omawiane na szkoleniach produktowych z pewnością dokładniej, niż ja mógłbym to zrobić. Dlatego tylko sygnalizuję ten aspekt, zainteresowane osoby odsyłam do producentów – pytajmy o innowacyjne rozwiązania, oczekujmy prezentacji (również online), bierzmy w nich udział. Poszerzajmy swoją wiedzę.

Być może czytelnik jest zaskoczony treścią artykułu, może nawet rozczarowany. Pozwolę sobie to wynagrodzić, poruszając nowy wątek w tej dziedzinie. Zastanawiając się nad artykułem i analizując problemy, które napotykałem w obiektach, którymi się zajmowałem, a także analizując formalne dokumenty opisujące problematykę, doszedłem do wniosku, że jest temat trochę zapomniany, być może nawet pomijany. Mam na myśli powiązania pomiędzy wymaganiami nakładanymi na obiekty i instalacje na gruncie warunków technicznych, przepisów ewakuacyjnych i przeciwpożarowych z warunkami i zasadami funkcjonowania obiektów infrastruktury krytycznej.

KILKA PRZYKŁADÓW WYMOGÓW FORMALNYCH WYNIKAJĄCYCH Z WARUNKÓW TECHNICZNYCH:

- Warunek wyłączenia zasilania wszystkich urządzeń za pomocą przeciwpożarowego wyłącznika prądu (PWP), z wyjątkiem urządzeń, których funkcjonowanie jest niezbędne podczas pożaru.
- Konieczność lokalizacji PWP w pobliżu wejścia głównego.
- Zwolnienie KD na drogach ewakuacyjnych w warunkach pożaru.
- Zakaz umieszczania w szybach windowych urządzeń innych niż związane z funkcjonowaniem dźwigu.
- Zjazd wind na poziom ewakuacyjny w warunkach pożaru.

To obowiązkowe działania projektowe dla budynków[1]. Nie znalazłem możliwości odstępstwa od nich w budynkach infrastruktury krytycznej. Czy to oznacza, że można je pomijać dla tych obiektów? Moim zdaniem nie można. Ale należy przeanalizować możliwość ich stosowania, a w przypadku stwierdzenia konieczności ich ominięcia należy zadbać o odpowiednie odstępstwa oraz o jasne i precyzyjne zapisy w projekcie.

I to koniecznie na etapie projektu budowlanego, by nie narazić się na niespełnienie warunków formalnych uzyskania pozwolenia na użytkowanie. Dla projektanta systemów teletechnicznych oznacza to, że musi on od wczesnego etapu projektowania precyzyjnie zadbać o pełne wparcie merytoryczne dla głównego projektanta. Powinien przedstawić listę odstępstw, z dokładnym określeniem podstaw formalnych. To pozwoli projektantowi podjąć decyzję o wystąpieniu o odstępstwa.

Dla funkcjonalności niewymagających odstępstw, ale wynikających np. z zasad projektowania systemów SSP lub KD, należy zadbać o odpowiednie technicznie precyzyjne zapisy w projekcie budowlanym. Na żadnym innym etapie, gdyż precyzyjne zapisy w tym dokumencie są podstawą do odbioru budynku. Ich brak może wymagać dodatkowych uzgodnień lub wyjaśnień czy też analiz w trakcie czynności odbiorczych przez służby. Przy określaniu tych zmian należy dokładnie podać podstawę ich wymagania, a także podstawę czy powód ich niezastosowania, jako świadomej decyzji projektanta.

Moim zdaniem to jedyna droga bezpiecznego planowania budowy i wyposażenia budynków infrastruktury krytycznej. Mam jednak nadzieję, że sytuacja covidowa spowoduje ogólny wzrost świadomości. Zaczniemy baczniej przyglądać się wymaganiom dotyczącym ważnych obiektów, lepiej dbać o prawidłowe projektowanie, planowanie prac instalacyjnych, uruchomień i eksploatacji. Uświadomi także osobom odpowiedzialnym za kształtowanie wymagań formalnych, że po pierwsze ich skrupulatność podnosi nasze bezpieczeństwo, po drugie inżynierowie odpowiedzialni za projekty nie będą musieli zajmować się interpretacją zapisów lub próbą pogodzenia sprzecznych wytycznych, będą mogli się skoncentrować na jakości swojej pracy dla dobra wszystkich.

1) Rozporządzenie Ministra Infrastruktury w sprawie warunków technicznych, jakim powinny odpowiadać budynki i ich usytuowanie (Rozporządzenie z 12 kwietnia 2002 r. (Dz.U. nr 75, poz. 90 z późn. zm., tekst ujednolicony uwzględniający zmiany wprowadzone Dz.U. z 8 grudnia 2017 r., poz. 2285).

MICHAŁ ZALEWSKI

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

Ochrona zasobów zdalnych

infrastruktury krytycznej

Spośród systemów, obiektów i technologii składających się na infrastrukturę krytyczną, zasoby zdalne i inne nieosłonięte obiekty czy urządzenia są istotnymi elementami, których zabezpieczenie jest często pomijane. Pełnią kluczowe funkcje w miastach, agencjach rządowych czy przedsiębiorstwach użyteczności publicznej i obejmują wszystko, od szaf sygnalizacji świetlnej i zaworów rurociągów po urządzenia telekomunikacyjne i podstacje energetyczne.

Aktywa te mogą być niezwykle cenne i niezależnie od tego, czy znajdują się w centrum miasta, czy w odizolowanej lokalizacji, pozostają zamknięte, dopóki nie będzie niezbędny dostęp do nich w celu konserwacji lub innej określonej czynności. Ze względu na wrażliwość, wręcz krytyczność wszystkiego, co kontrolują, muszą być zabezpieczone przed nieuprawnionym dostępem.

Są dwa istotne wyzwania związane z zapewnianiem i ograniczaniem dostępu do zdalnych lub autonomicznych zasobów. Pierwszym jest zapewnienie dostępu upoważnionym osobom przy jednoczesnym zapewnieniu wystarczającej ochrony przed niechcianym użyciem lub wejściem. Drugim jest wiedza o tym, kto uzyskał dostęp do zdalnej lokalizacji. W jaki sposób miasto lub przedsiębiorstwo może śledzić aktywność związaną z tym ważnym elementem IK?

DLACZEGO TRADYCYJNE METODY NIE WYSTARCZĄ

Pomimo zagrożeń dostęp do zdalnych zasobów nadal często odbywa się za pomocą wspólnego klucza mechanicznego. Biorąc pod uwagę to, ile takich odległych punktów ma gmina lub przedsiębiorstwo, sytuacja szybko może wymknąć się spod kontroli. Londyn np. ma ponad 3500 skrzyżowań z sygnalizacją świetlną, a Los Angeles ponad 4500, co oznacza, że miasta te muszą zarządzać tysiącami szaf sygnalizacyjnych.

Oczywiście nie jest wykonalne, by każdy pracownik nosił inny klucz do każdej szafki. Większość ma 5 lub 6 kluczy szkieletowych rozprowadzonych do różnych grup potrzebujących dostępu. Gdyby ktoś zgubił klucz, miasto musiałoby ponownie odblokować wszystkie szafki, aby zachować integralność ich bezpieczeństwa. Ze względu na czas i koszt wymiany tysięcy zamków jest to nieopłacalne.

Ale rozwiązanie problemu zgubionych kluczy to tylko część wyzwania. Na bardziej podstawowym poziomie organizacje muszą znaleźć sposoby skutecznego zarządzania dystrybucją dostępu, definiować prawa dostępu zgodnie z zadaniami na dany dzień, odwoływać je w razie potrzeby i informować, kto i kiedy uzyskał dostęp do obudów.

PRZENIESIENIE INTELIGENCJI DO KLUCZA

Rozwiązaniem jest traktowanie zdalnych zasobów jak drzwi, a następnie zarządzanie całością w ramach jednego systemu KD. Daje to organizacjom wymagany poziom kontroli, w tym możliwość blokowania kluczy i zapewnienia zdalnego dostępu, a także dane o aktywności zamków potrzebne do tworzenia raportów.

Aby to zrealizować, potrzebny jest inteligentny klucz, który zawiera zarówno element fizyczny z kluczem do fizycznego zamka, jak i element elektroniczny zasilany bateryjnie. Drugi komponent umożliwia użytkownikom skonfigurowanie klucza z określonymi edytowalnymi prawami dostępu i harmonogramami. Jest to szczególnie pomocne przy zarządzaniu wykonawcami. Zamiast zapewniać pracownikom zewnętrznym ogólny dostęp, organizacje mogą go ograniczyć do określonych zasobów w określonych porach dnia i przez ograniczony czas. Ponadto, aby utrzymać dostęp, klucze muszą zostać ponownie zatwierdzone w określonym czasie, więc nawet w razie zgubienia lub kradzieży klucza traci on swoje prawa dostępu, jeśli nie zostanie przywrócony do systemu.

Kolejną zaletą inteligentnych kluczy jest to, że przesyłają dane o zdarzeniach do systemu KD. Dzięki możliwościom raportowania użytkownicy mogą zbierać dane, aby określić, kto miał dostęp do zdalnych zasobów i kiedy. Obejmując zasoby zdalne kontrolą dostępu za pomocą inteligentnych kluczy, gminy, agencje rządowe i przedsiębiorstwa użyteczności publicznej mogą skuteczniej zarządzać tymi istotnymi elementami IK, monitorować je i zabezpieczać.

Venom
PSIM PLATFORM

Nowa jakość PSIM na rynku polskim

System Venom jest nowoczesnym polskim rozwiązaniem PSIM. Dzięki elastycznej modułowej budowie oraz zespołowi doświadczonych polskich programistów umożliwia sprawne scentralizowane zarządzanie bezpieczeństwem każdego obiektu.

ARCHITEKTURA I TECHNOLOGIA

Działanie systemu Venom jest oparte na klasycznej architekturze klient-serwer. Doskonale wpasowuje się w obiekty zarówno scentralizowane, jak i rozproszone. Aplikacje operatorskie są wykonane w technologii desktopowej, co pozwala zapewnić maksymalną wydajność, natomiast moduły przeznaczone dla operatorów mobilnych są wykonane w technologii webowej.

GŁÓWNE CECHY WYRÓŻNIAJĄCE PSIM VENOM

- modułowa budowa,
- indywidualizacja funkcjonalności,
- elastyczność,
- w 100% polski produkt i wsparcie polskich inżynierów,
- obsługa procedur postępowania dla operatorów,
- szczegółowe raportowanie,
- indywidualne GUI.

INTEGRACJE

Venom integruje systemy i zarządza praktycznie każdym systemem, który to umożliwia. Najczęściej spotykane integracje obejmują: systemy CCTV (VMS i rejestratory), SSWiN, SKD, SSP, systemy ochrony obwodowej (ogrodzenia), LPR, BMS, DSO, stacje meteorologiczne, sprzętowe bramki SMS, sterowniki przekaźnikowe, windy, kamery termowizyjne detekcji temperatury, wideodomofony, zewnętrzne głośniki rozgłoszeniowe, wykrywacze metalu, systemy wykrywające drony i radary, systemy monitorowania warunków środowiskowych, inteligentne listwy zasilające. Lista integracji jest otwarta i dostosowana do wymogów konkretnego projektu.

PROCEDURY

System Venom zapewnia elastyczny system procedur postępowania dla operatorów. Klient sam określa, które zdarzenia (lub korelacja zdarzeń) wymagają rozpoczęcia procedury. Każda procedura może się składać z dowolnej liczby kroków, a każdy krok może być różnego typu: polecenie, pytanie, akcja. Każdą procedurę można dowolnie rozwidlić w zależności od rozwoju wydarzeń. Dla administratora przewidziane jest intuicyjne narzędzie do samodzielnego zarządzania procedurami.

RAPORTY

Raporty są dostępne w formie tabelarycznej lub wykresu. Wszystkie raporty są „szyte na miarę" z danych dostępnych zarówno z systemów zintegrowanych, jak i z działań operatorów. Każdy raport można opatrzyć komentarzem, wydrukować lub zapisać w jednym z popularnych formatów.

MAPY I PLANY

W systemie Venom dostępne są mapy: wektorowe, rastrowe, georeferencyjne. Mogą być wykorzystane podkłady klienta lub wykonane nowe, np. z dronu. Każdy element systemu podrzędnego może być naniesiony na mapy oraz skorelowany nawet z trzema różnymi kamerami (w tym presety kamery PTZ).

KORELACJE

System PSIM umożliwia korelację zdarzeń i alarmów z różnych zintegrowanych systemów. Dzięki temu można szybko wyeliminować wiele źródeł fałszywych alarmów. Na przykład korelacja alarmów z sensorów napłotowych systemu ochrony obwodowej z systemem VSS z analityką wideo rozpoznającą wejście człowieka w chroniony obszar jest w stanie wyeliminować do 95% fałszywych alarmów.

BEZPIECZEŃSTWO

Dostęp do systemu jest zabezpieczony nie tylko loginem i hasłem, ale jako opcja również identyfikacją biometryczną. Komunikacja systemu jest szyfrowana.
Serwery Venom mogą pracować w środowisku zarówno wirtualnym, jak i rzeczywistym, a fizyczne maszyny mogą być zduplikowane (podwojone) wraz z mechanizmem automatycznego przełączania na zapasowy w przypadku ewentualnej awarii.

WDROŻENIE I WSPARCIE

Cały proces wdrożenia jest realizowany przez polskich inżynierów, a po jego zakończeniu czuwają oni nad dalszym funkcjonowaniem systemu Venom oraz stale współpracują z użytkownikiem nad ewentualnymi rozbudowami.

Więcej szczegółów na stronie:
www.psim.pl

MEGAVISION TECHNOLOGY

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

Nowości Hikvision

Obiekty infrastruktury krytycznej są kluczowe dla funkcjonowania społeczeństwa i gospodarki kraju, wymagają więc specjalnego, profesjonalnego zabezpieczenia. Podczas doboru odpowiednich systemów stawia się na niezawodność i najwyższy poziom bezpieczeństwa. Wychodząc naprzeciw tym potrzebom, firma Hikvision oferuje najnowocześniejsze rozwiązania spełniające rozmaite potrzeby.

HIKVISION RADAR PTZ
– NOWOŚĆ W OFERCIE MARKI

Na szczególną uwagę w ofercie Hikvision zasługuje nowa, 4-Mpiks. kamera PTZ serii iDS-2SR8xxx z 40-krotnym zoomem optycznym. To innowacyjne i przełomowe w swojej prostocie rozwiązanie jest dedykowane do monitoringu wizyjnego rozległych obszarów i zewnętrznej ochrony obwodowej. Nowa kamera wyróżnia się przede wszystkim doskonałą jakością obrazu dzięki zastosowaniu technologii Darkfighter, funkcji WDR o wartości 140 dB oraz oświetlacza IR oraz światła białego, który może pracować także w trybie stroboskopu, pełniąc funkcję odstraszającą potencjalnego intruza.

Zintegrowana w jednej obudowie z radarem mikrofalowym kamera nie wymaga skomplikowanej kalibracji, a jej konfiguracja jest znacznie uproszczona i bardziej intuicyjna. Pojedynczy interfejs sieciowy i jeden adres IP oznaczają łatwiejsze i tańsze okablowanie, a montaż nie różni się niczym od instalacji standardowej kamery PTZ.

Dzięki integracji z radarem udało się uzyskać niespotykaną dotąd dokładność i skuteczność śledzenia celów praktycznie w każdych warunkach atmosferycznych. Deszcz, śnieg, wiatr, zamiecie i takie zjawiska, jak smog lub mgła, a nawet całkowita ciemność nie stanowią przeszkody dla skutecznej detekcji i śledzenia intruzów naruszających strefę alarmową. Antena radaru o kącie widzenia 90° potrafi wykryć i śledzić do 32 celów jednocześnie. Sylwetka człowieka może być skutecznie wykryta przez radar z odległości do 100 m, a pojazd – do 120 m. Cele są wizualizowane na mapie w czasie rzeczywistym, podobnie ich prędkość i kierunek przemieszczania się oraz odległość względem anteny radaru.

ALGORYTMY GŁĘBOKIEGO UCZENIA

Pełnię możliwości nowego urządzenia ujawnia jednak sztuczna inteligencja – zastosowane zaawansowane algorytmy głębokiego uczenia. W momencie naruszenia strefy alarmowej kamera jest kierowana na współrzędne przekazane przez radar i następuje wizyjna weryfikacja celu. Jeśli celem tym jest człowiek lub pojazd, a warunki atmosferyczne pozwalają na skuteczną obserwację wizyjną, radar przekazuje prowadzenie celu do kamery. Ta za pomocą technologii automatycznego śledzenia Smart Tracking 3. generacji automatycznie podąża za wskazanym celem, analizując przy tym szczegółowo jego cechy. Analiza sylwetki osoby uwzględnia płeć, wiek, dominujący kolor ubioru, zarost, okulary, plecak i wiele innych kryteriów. Dla pojazdu możliwa jest analiza m.in. marki, modelu i koloru.

W połączeniu z rejestratorem DeepinMind możliwe jest późniejsze wyszukanie w zarejestrowanym materiale wizyjnym obiektów o wskazanych atrybutach. Skuteczność wizyjnego śledzenia celu wspomaga funkcja Rapid Focus, która gwarantuje utrzymanie stałej ostrości obrazu niezależnie od aktualnej pozycji kamery i ogniskowej obiektywu. Nowa kamera PTZ zintegrowana z radarem współpracuje z aplikacjami iVMS-4200 oraz HikCentral.

HIKCENTRAL PROFFESIONAL
– NOWA ODSŁONA

Oprogramowanie HikCentral Proffesional firmy Hikvision może sprostać różnorodnym wyzwaniom związanym z bezpieczeństwem – od zarządzania indywidualnymi systemami, takimi jak monitoring wizyjny, kontrola dostępu, sygnalizacja włamania po współpracę z wieloma systemami w ramach ujednoliconej architektury na jednej intuicyjnej platformie. Chroniąc ludzi i mienie, sprawia jednocześnie, że codzienne operacje są wydajniejsze i bardziej pomocne w podejmowaniu trafnych decyzji.

Platforma jest kompatybilna z urządzeniami Hikvision i wieloma aplikacjami, w tym z opartą na głębokim uczeniu, analizą obrazu i statystyką danych. Otwarta architektura platformy umożliwia łatwą integrację z systemami firm trzecich (OpenAPI/Database) i urządzeniami zgodnymi z ONVIF.

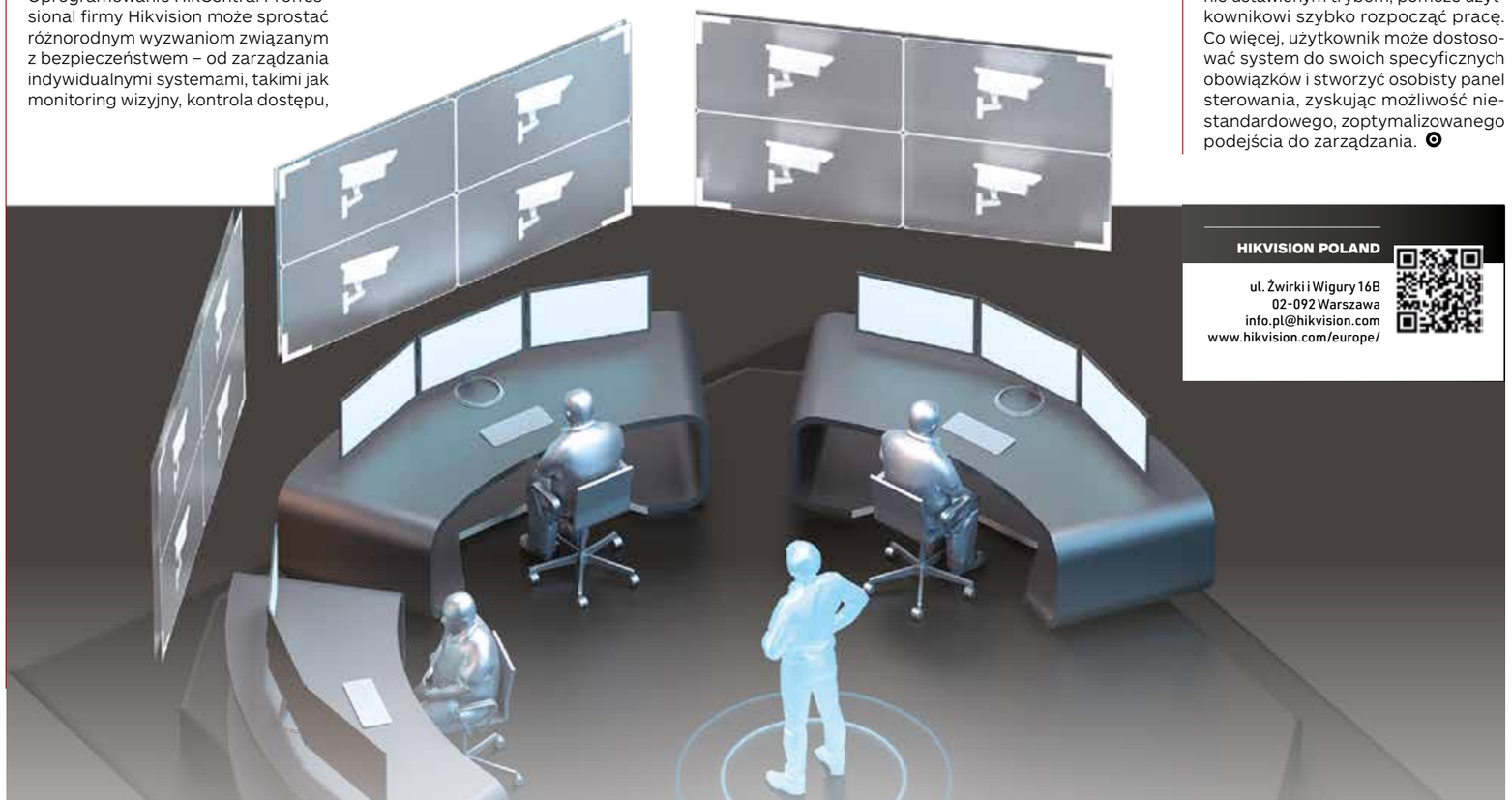
Wszystkie najważniejsze potrzeby w zakresie bezpieczeństwa są zaspokajane przez dziewięć podstawowych modułów, w tym: wizyjny, kontroli dostępu, zarządzania gośćmi, weryfikacji obecności, sygnalizacji alarmu, *digital signage* i stanu systemu.

Wszystkie aplikacje mogą być połączone w interaktywny sposób w celu stworzenia prawdziwie zunifikowanej architektury, zwiększającej wydajność operacyjną – np. alarm włamaniowy i kontrola dostępu z weryfikacją wizyjną lub zarządzanie gośćmi ze wstępną rejestracją pojazdów i wiele innych.

Spełniając minimalne wymagania systemowe – procesor Intel i3 oraz 8 GB RAM – można stworzyć własną platformę bezpieczeństwa o ograniczonych kosztach sprzętowych. Dzięki elastycznej i skalowalnej architekturze platforma może być rozbudowywana wraz z rozwojem potrzeb biznesowych. Można ją rozbudować z małego, 32-kanałowego systemu z 8 przejściami do ultraduzego systemu, który łączy do 100 tys. kanałów wideo (w trybie RSM).

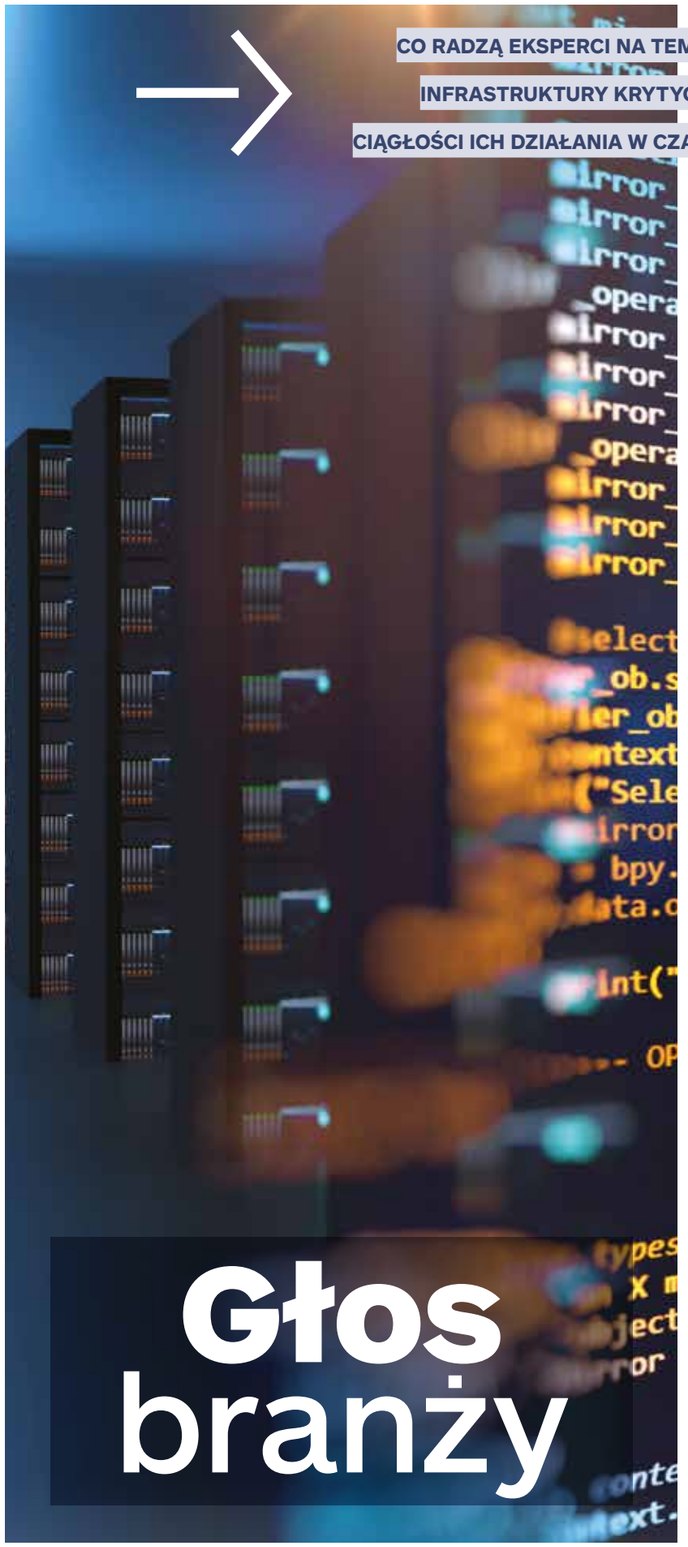
Dane zebrane z różnych aplikacji stają się łatwe do zrozumienia dzięki dynamicznemu raportowaniu i pomocnym, intuicyjnym dashboardom. Pulpit nawigacyjny umożliwia tworzenie spersonalizowanych ekranów przekazujących informacje najbardziej interesujące użytkownika, który, mając większą świadomość sytuacyjną, może podejmować słuszniejsze decyzje.

HikCentral Professional, dzięki wstępnie ustawionym trybom, pomoże użytkownikowi szybko rozpocząć pracę. Co więcej, użytkownik może dostosować system do swoich specyficznych obowiązków i stworzyć osobisty panel sterowania, zyskując możliwość niestandardowego, zoptymalizowanego podejścia do zarządzania.



HIKVISION POLAND

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



Głos branży

CO RADZĄ EKSPERCI NA TEMAT BEZPIECZEŃSTWA OBIEKTÓW INFRASTRUKTURY KRYTYCZNEJ W ZAKRESIE ZAPEWNIENIA CIĄGŁOŚCI ICH DZIAŁANIA W CZASACH PANDEMII KORONAWIRUSA

Norbert Bartkowiak

ela-compil

Pożar serwerowni OVH we Francji

W nocy z 9 na 10 marca w Strasburgu we Francji doszczętnie spłonął jeden z bloków serwerowni OVH (SBG2), w której znajdowały się serwery tysięcy różnych firm, w tym także polskich. OVH, jako największy dostawca rozwiązań chmurowych w Europie, z powodzeniem konkuruje na tym polu z takimi gigantami, jak Google, Amazon czy Microsoft.

Pożar zniszczył pięciopiętrowe centrum danych opatrzone nazwą SBG2 o powierzchni 500 m^2, uszkodzeniu uległy również 4 z 12 kontenerów serwerowni SBG1. Pozostałe serwerownie SBG3 i SGB4 udało się strażakom ochronić, ale one również zostały wyłączone z funkcjonowania.

Firma Netcraft, znana z monitorowania ruchu internetowego, opublikowała własną analizę skutków pożaru w centrum danych OVH. Twierdzi, że ofiarą pożaru padło 18 proc. adresów IP hostowanych w chmurze OVH. Na liście są np. agencje rządowe z Wybrzeża Kości Słoniowej i Francji, klienci z Polski, Walii i Wlk. Brytanii, a także serwisy kryptowalutowe. Problem dotknął portali bankowości internetowej, usług poczty internetowej, witryn z wiadomościami i sklepów internetowych. Serwis branżowy Golem podał, że prawie 2 proc. wszystkich domen .fr ucierpiało w wyniku tego incydentu, w tym paryskie muzeum Pompidou.

Przyczyna pożaru nie została jeszcze ustalona, ale założyciel OVHcloud, Octave Klaba, opisał pożar w swoim wystąpieniu w Internecie, mówiąc, że pracownicy OVHcloud zareagowali na alarmy we wtorek o godzinie 23.42, ale dotknięta pożarem część centrum danych była już wypełniona dymem: *„Dwie minuty później podjęli decyzję o odejściu, ponieważ było to zbyt niebezpieczne”*. Prawdopodobnym źródłem pożaru były dwa UPS-y, wskazują na to odczyty telewizji termograficznej używanej przez strażaków. Jak stwierdził Klaba, jeden z UPS-ów dzień wcześniej przechodził konserwację. Wygląda na to, że firma OVHcloud miała już wcześniej problemy z systemem zasilania. Świadczyć o tym może incydent z 2017 r., w którego wyniku kampus w Strasburgu stracił na jeden dzień zasilanie, a to z kolei spowodowało utratę łączności z obiektami firmy w Roubaix. Prawdopodobnie z tego powodu firma systematycznie wymieniała kable zasilające, potwierdzają to aktualizacje centrum danych Beauharmois (BHS-1).

Incydent ten będzie z pewnością analizowany, i to w wielu aspektach. Jednym z nich stanie się kwestia realnego bezpieczeństwa danych w „chmurze”. Złośliwi komentują, że był on przypadkiem realnej migracji danych do chmury. Moją uwagę zwraca fakt, że reakcja obsługi polegająca na fizycznej weryfikacji alarmu nastąpiła w momencie, kiedy w centrum zadymienie było tak silne, że stanowiło zagrożenie dla życia ludzi. Zatem albo pożar rozwijał się w bardzo szybkim tempie, albo reakcja była zbyt późna.

W 2011 r. opublikowałem w kwartalniku „Ochrona Przeciwpożarowa” artykuł omawiający możliwości zabezpieczenia serwerowni w oparciu o wielostopniowy system monitorowania zagrożeń. Wydawało mi się wtedy, że głównym zagrożeniem może być zbyt wczesne wyzwolenie stałych urządzeń gaśniczych, co mogłoby doprowadzić do niepotrzebnych przerw w pracy serwerowni, a co za tym idzie strat. Wskazywałem na korzyści ze stosowania kombinacji zarówno systemów bardzo wczesnej detekcji, jak i monitorowania parametrów pracy urządzeń sieciowych. Tego typu rozwiązanie, oparte na systemie GEMOS, zastosowano już w kilku podobnych obiektach o niewiele mniejszej skali. System sygnalizacji pożarowej o standardowej czułości miałby stanowić ostatnią linię obrony polegającą na wyzwoleniu systemu gaszącego. Wydawało mi się – i nadal jestem tego zdania – że w data center otwarty pożar o tak gigantycznej energii nigdy nie powinien mieć miejsca. Zatem z zainteresowaniem będę śledzić proces dochodzenia przyczyn.

Według tego, co podał właściciel, trwają intensywne prace nad odtworzeniem rejestracji wideo z blisko 300 kamer, które były zainstalowane w spalonym budynku. Jeżeli to się uda, możliwe będzie prześledzenie ostatniej fazy pożaru.

Rzeczą bezsprzeczną jest, że wszystkie obiekty typu data center, należące do infrastruktury krytycznej, powinny być wyposażone w ponadnormatywne systemy bezpieczeństwa, w tym przede wszystkim bezpieczeństwa pożarowego.

Marcin Buzdygan

Emitel

Przestrzeganie wymogów i współpraca z klientem

W obliczu realnego zagrożenia, jakim jest pandemia wirusa SARS-Cov-2, która w znaczący i negatywny sposób wpływa na codzienne życie obywateli, zapewnienie ciągłości dostarczania podstawowych usług niezbędnych do ich funkcjonowania nabiera nowego, szczególnego wymiaru i znaczenia. Duża część z tych usług jest świadczona z wykorzystaniem tzw. infrastruktury krytycznej (IK) przez podmioty będące operatorami IK. Mając na względzie wagę IK dla właściwego funkcjonowania państwa, w tym głównie dla zaspokajania podstawowych potrzeb społeczeństwa i obywateli, jej ochrona powinna być jednym z priorytetowych obszarów działania władz państwowych, samorządowych oraz przedsiębiorców świadczących tego rodzaju usługi.

Istota tych działań powinna sprowadzać się w głównej mierze do zapewnienia ochrony infrastruktury przed zagrożeniami, ale również wyrażać się troską, aby ewentualne uszkodzenia lub zakłócenia w jej funkcjonowaniu były możliwie krótkotrwałe, łatwe do usunięcia i nie prowadziły do trwałego lub czasowego braku świadczenia usługi.

Działania te z całą pewnością powinny być wieloaspektowe i uwzględniać obszary bezpieczeństwa określone w Narodowym Programie Ochrony Infrastruktury Krytycznej, tj. bezpieczeństwo fizyczne, prawne, techniczne, osobowe, teleinformatyczne, czy też opracowanie planów odtwarzania, mających w głównej mierze na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie zaburzenia realizowanych procesów technologicznych.

Podstawowym i najskuteczniejszym sposobem zapewnienia bezpieczeństwa IK jest przestrzeganie mających zastosowanie do danej infrastruktury aktów prawnych, norm i wymogów eksploatacyjnych, a w dobie pandemii także przestrzeganie ograniczeń, nakazów i zakazów wprowadzanych w związku z jej wystąpieniem.

Dzisiejsza sytuacja i okoliczności są wyjątkowe, zmuszają właścicieli IK do podejmowania nieszablonowych działań i poszukiwania niestandardowych rozwiązań, także w obszarze bezpieczeństwa. Niezwykle istotne jest więc, aby byli w swoich działaniach wspierani wiedzą i doświadczeniem partnerów biznesowych z branży security.

Koncentracja branży powinna dzisiaj skupiać się na zaspokojeniu oczekiwań klienta, z zachowaniem jego indywidualnych potrzeb i możliwości maksymalnego wykorzystania potencjału jego infrastruktury. Taka współpraca działa długoterminowo na korzyść obu stron oraz umożliwia realizowanie długoterminowych strategii inwestowania i rozwoju systemów bezpieczeństwa, z możliwością uwzględniania indywidualnego charakteru i specyfiki danej branży, a nawet podmiotu.

Możliwości zaprojektowania oraz wdrożenia produktu lub usługi uszytej na miarę oczekiwań klienta i dostosowanej do jego potrzeb wymagają jednak dużej elastyczności w działaniu oraz wspólnej z klientem pracy nad produktem lub usługą. Niewątpliwie stanowi to swego rodzaju wyzwanie dla branży security. Wyzwanie, któremu wielu z obecnych na rynku dostawców z branży jest z całą pewnością w stanie stawić czoło już dzisiaj.

Piotr Szufnara

Rządowe Centrum Bezpieczeństwa

Wyzwania w zapewnieniu bezpieczeństwa IK

Kompleksowe podejście do zapewnienia ochrony infrastruktury krytycznej (IK) wymaga wdrażania rozwiązań adekwatnych do zidentyfikowanych zagrożeń i przeprowadzonej oceny ryzyka. Ważne, aby operator IK właściwie dobrał środki ochrony bez generowania nadmiernych kosztów. Takie działanie

pozwala na odpowiednie wykorzystanie technicznych środków bezpieczeństwa fizycznego, zapewniających wsparcie dla personelu ochrony. Utrzymanie właściwego poziomu zabezpieczeń wiąże się z cyklicznym wykonywaniem przeglądów i konserwacją infrastruktury technicznej, ponieważ urządzenia te pracują w trybie 24-godzinnym, a wszelkie usterki czy dysfunkcje powinny być niezwłocznie naprawiane. Operator IK powinien mieć przygotowane plany i procedury postępowania awaryjnego na wypadek wystąpienia dysfunkcji któregoś z elementów zabezpieczeń i wdrożenia środków zaradczych.
W kontekście utrzymywania w sprawności podstawowych elementów zabezpieczeń, takich jak ogrodzenia, bramy, systemy kontroli dostępu, systemy sygnalizacji włamania i napadu czy monitoringu wizyjnego, należy budować świadomość, że prawidłowo funkcjonujące systemy (często zintegrowane) podnoszą odporność na zagrożenia, a w efekcie pozwalają świadczyć usługi w niezakłócony sposób. Zwiększanie odporności IK w dużej mierze zależy od współpracy administracji publicznej i operatorów IK, wymiany doświadczeń i dobrych praktyk, a także dzielenia się trudnościami, jakie pojawiły się chociażby w czasie pandemii COVID-19.
Tematem nurtującym operatorów IK jest zagrożenie ze strony bezzałogowych statków powietrznych (BSP) i osób, które mogą próbować je wykorzystać do zakłócenia funkcjonowania ważnych dla państwa obiektów. Branża security prowadzi intensywne działania na rzecz wypracowania rozwiązań umożliwiających wczesną detekcję BSP i jeżeli może stanowić potencjalne zagrożenie, do podjęcia działań zmierzających do jego (bezpiecznej) neutralizacji. Administracja rządowa i urzędy centralne wspierają w tym zakresie operatorów IK. Jednak pamiętajmy, że każda jednostka organizacyjna działa w innym środowisku operacyjnym i otoczeniu zewnętrznym, w związku z tym wybrane rozwiązanie powinno być skuteczne, a przede wszystkim zgodne z obowiązującymi regulacjami prawnymi.

Tomasz Guzikowski

CIECH SA

Integracja systemów bezpieczeństwa z procesami biznesowymi

Bezpieczeństwo infrastruktury krytycznej to obecnie nie tylko zapewnienie ochrony przed kradzieżą jej elementów, przypadkowym lub celowym uszkodzeniem lub zniszczeniem, ale również – a może przede wszystkim – przed awarią i przerwaniem ciągłości działania procesu, za który ta infrastruktura odpowiada. Szczególnym wyzwaniem jest zabezpieczenie infrastruktury rozproszonej na dużym terenie, takiej jak rozległe wieloprocesowe instalacje produkcyjne czy rurociągi.
W takiej właśnie sytuacji jest CIECH, międzynarodowy koncern chemiczny działający na rynku globalnym, w którego skład wchodzi m.in. 8 dużych zakładów produkcyjnych zlokalizowanych w trzech krajach UE. Nasza firma jest drugim w UE producentem sody kalcynowanej i oczyszczonej, największym dostawcą krzemianów w Europie oraz znaczącym producentem soli warzonej, środków ochrony roślin, pianek poliuretanowych i opakowań szklanych – swoje towary eksportuje na niemal wszystkie kontynenty. Naszymi klientami są zarówno globalne koncerny chemiczne, jak i mniejsze przedsiębiorstwa, głównie z Europy, ale też z Azji, Afryki czy Ameryki Płn. Jako odpowiedzialny partner biznesowy nie możemy sobie pozwolić na utratę ich zaufania, stąd zapewnienie stałych dostaw najwyższej jakości produktów jest dla nas priorytetem.
Obecne rozwiązania techniczne pozwalają już na pełną integrację systemów bezpieczeństwa, w tym również procesowego. Bardzo ważna jest tu kwestia monitorowania parametrów pracy urządzeń, czyli predictive maintenance. Dane muszą być zbierane i analizowane w czasie rzeczywistym, tak aby proces był na bieżąco kontrolowany i w razie potrzeby modyfikowany. Co więcej, obecne systemy same się uczą, jak najlepiej optymalizować dany proces produkcyjny.
Z naszej perspektywy bardzo ważnym elementem tych zmian było w ostatnich miesiącach wdrożenie w zakładach sodowych CIECH Soda Polska innowacyjnego systemu do nadzoru linii produkcyjnych, będącego elementem szerszych działań realizowanych przez Grupę w celu wczesnego wykrywania usterek. System „Mobilny Obchodowy" umożliwia systematyczny monitoring poszczególnych instalacji, a po integracji z systemem SAP pozwala na efektywne zarządzanie całym procesem produkcji sody, a także odpowiednią konserwację i utrzymanie kluczowych urządzeń w optymalnym stanie.
Innym elementem takiej integracji jest połączenie systemów bezpieczeństwa z innymi procesami biznesowymi, takimi jak ważenie pojazdów, logistyka i monitorowanie transportu.
Oczywiście samo monitorowanie to nie wszystko. Kluczowe jest tutaj alarmowanie o wszelkich zdarzeniach czy odchyleniach od zadanych parametrów. Informacje te muszą trafiać do odpowiednich służb, które są zobowiązane do podjęcia konkretnych działań.
Tego typu systemy przede wszystkim skracają do minimum czas reakcji osób odpowiedzialnych za dany proces. Przy sprawnie działającym systemie oceniającym w czasie rzeczywistym płynność procesów produkcyjnych i logistycznych spada liczba popełnianych błędów przez pracowników, zwłaszcza w sytuacjach kryzysowych. W konsekwencji prowadzi to do ograniczenia zarówno kosztów obsługi i utrzymania infrastruktury, jak i strat mogących wyniknąć z powodu awarii czy błędu pracownika.
Nasze oczekiwania względem branży security to przede wszystkim elastyczność i otwartość na współpracę z różnymi podmiotami i producentami systemów zabezpieczeń. Rynek jest coraz bardziej wymagający i bez rozwiązań szytych na miarę trudno będzie się przebić firmom do dużych globalnych korporacji.

Piotr Kiliszek

Niezależny ekspert

Kontrola ruchu osobowego

Okres pandemii uświadomił wszystkim, jak istotne jest nowe spojrzenie na kontrolę ruchu osobowego w obiektach, również tych należących do sektora infrastruktury krytycznej. Dzisiaj kontrola ta powinna realizować szereg nowych funkcji. Oprócz identyfikacji osób (uwzględniając nowelizację stanu prawnego), wracamy do automatycznej kontroli trzeźwości i wprowadzamy zdalny pomiar temperatury. Zastosowane urządzenia powinny również umożliwiać przeprowadzanie dezynfekcji pomieszczeń, aby zapobiegać transmisji koronawirusa. W przypadku potwierdzenia przypadku zakażenia system powinien automatycznie inicjować dekontaminację.
Wdrażanie takich rozwiązań ogranicza też fizyczny kontakt pracowników ochrony z osobami wchodzącymi na teren zakładu, a w efekcie minimalizuje ryzyko zakażenia. W wielu przypadkach wydatki na nowe rozwiązania i modernizację pomieszczeń, w których odbywa się ruch osobowy, należy traktować jako inwestycję w utrzymanie ciągłości działalności biznesowej, a nie tylko jako podnoszenie poziomu bezpieczeństwa fizycznego. Ważne jest również prawidłowe dobranie i zainstalowanie systemów, aby móc korzystać z całego pakietu oferowanych przez nie możliwości.
W tym roku czekają branżę security spore wyzwania, niezbędne będzie np. zintensyfikowanie działań uniemożliwiających kradzieże mienia. Rosnące ceny złomu i materiałów spowodują, że ryzyko kradzieży znacznie wzrośnie. W zakładach, w których realizowane są prace modernizacyjne, brak właściwego nadzoru i przestrzegania procedur niestety może skutkować zarzutami o brak należytej staranności przy realizacji umów. Branża musi podnosić kwalifikacje pracowników i ich świadomość o sposobach kradzieży.
Konieczność oszczędności przyspieszy wprowadzanie rozwiązań technicznych, które w dłuższej perspektywie zahamują wzrost kosztów świadczonych usług i spowodują przeniesienie ciężaru wydatków osobowych na techniczne. Robotyzacja patroli, drony stale patrolujące teren to przyszłość, którą trzeba zacząć wprowadzać już dzisiaj.

Andrzej Sobolewski

Polska Agencja Przemysłowo-Obronna

Zarządzanie komunikacją w dobie pandemii

Bezpieczeństwo obiektów infrastruktury krytycznej wymaga stosowania zarówno systemów zabezpieczeń z nowoczesnymi wielofunkcyjnymi urządzeniami, jak i niezawodnych systemów informatycznych – bezpiecznych, szyfrowanych i redundantnych środków telekomunikacji oraz niezawodnej łączności. Ale przede wszystkim wymaga ścisłej współpracy wszystkich pionów zarządzania.
Pandemia COVID-19 wykazała, jak wielkie znaczenie dla działalności państwa mają systemy techniczne umożliwiające przekazywanie informacji społecznej i urzędowej, usprawniające zarządzanie krajem na wszystkich szczeblach. Czy byłoby to możliwe bez nowoczesnych środków technicznych?
Odpowiedź narzuca się sama: NIE. Taka diagnoza dotyczy również IK – optymalne wykorzystanie jej zasobów wiąże się z ich precyzyjnym zarządzaniem. Ważne jest po pierwsze posiadanie rzetelnej informacji umożliwiającej wnikliwą analizę i ocenę. Po drugie wyposażenie techniczne (czyt. informatyczne) zapewniające poprawne wnioskowanie co do perspektyw rozwoju zagrożenia.
Rzetelna informacja wiąże się z bezpiecznym i bardzo szybkim systemem jej przekazu. Bezpiecznym w sensie braku technicznych zniekształceń i zakłóceń, braku możliwości zmieniania jej przez podmioty zewnętrzne, ale również stosowania jednoznacznych, zrozumiałych dla odbiorców słów i pojęć umożliwiających poprawną ich interpretację, a w konsekwencji realizację zakładanych przez decydentów działań. Szybkość przekazu ma znaczenie dla oceny, wnioskowania i zarządzania w czasie quasi-rzeczywistym. Takie wymagania spełnia sieć 5G dająca o wiele szybsze, stabilniejsze połączenia, o wiele krótsze czasy reakcji sieci niż obecne rozwiązania, a także możliwość podłączenia milionów urządzeń, w tym IoT.
Najważniejszym, a zarazem najsłabszym ogniwem zarządzania IK jest człowiek. Każdy pracownik ma swoistą mentalność, różny poziom wykształcenia i doświadczenie zawodowe oraz nawyki, które nabył w swoim środowisku. Jest bardziej lub mniej kreatywny i skłonny do stosowania innowacji. Wszystko to wpływa na jego świadomość, na umiejętność przestrzegania warunków technicznych zawartych w uregulowaniach prawnych. Znajduje to odzwierciedlenie w podejściu do przedmiotu i efektów pracy, a tym samym odpowiedzialności za jej wykonanie.
W dobie pandemii w sposób zasadniczy zmieniły się relacje międzyludzkie. Przez ograniczenia pandemiczne większość spotkań jest organizowana online w formie telekonferencji. Ograniczenia w prowadzeniu bezpośredniej rozmowy zakłócają nasze postrzeganie w odbieraniu odczuć rozmówcy.
Przekazywanie informacji służbowych następuje poprzez łączność telefoniczną, wysyłanie e-maili, komunikaty radiowe i telewizyjne. Przeprowadzenie telekonferencji z wieloma osobami wymaga dużej koncentracji i subordynacji jej uczestników, a także dobrego sprzętu o wysokiej jakości dźwięku i komfortu jego obsługi. Praktyka wykazuje, że spotkanie online z wykorzystaniem sprzętu o niskiej jakości są bardzo uciążliwe dla jej uczestników i pogarszają odbiór merytoryczny. Im lepsze zastosujemy urządzenia i media, tym lepiej zostanie zrozumiany cel merytoryczny spotkania, gdyż człowiek w ok. 95% widzi i słyszy mózgiem, a tylko 5% to informacja odebrana. Im jest lepsza jakościowo, tym lepiej rozumiana i wykorzystana w działaniu.
Istotne jest też zabezpieczenie informacyjne związane z posiadaniem informacji dotyczącej różnego złośliwego oprogramowania i wirusów krążących w sieci. Takie dane w dobie pracy zdalnej powinny być przekazywane na bieżąco wszystkim pracownikom oraz wykrywane i niwelowane przez serwery firmowe. Musi być zabezpieczony dostęp do baz danych, systemów zasilania i sieci telekomunikacyjnej. Wszystkie te działania wymagają wyposażenia w nowoczesne środki: oprogramowanie i technikę, w większym stopniu samodzielne w zakresie ich inteligencji i decyzyjności.
Wyzwania stojące obecnie, w dobie COVID-19, przed systemami zabezpieczeń technicznych IK to przede wszystkim zapewnienie pracownikom w miarę

możliwości komfortu psychicznego otrzymywania dobrej jakości informacji poprzez środki techniczne. Technika i oprogramowanie powinny zapewnić lepsze niż dotychczas autonomiczne rozwiązywanie problemów. Środki przekazu korzystające z sieci 5G zapewniają szybkie i bezpieczne przesyłanie informacji zabezpieczonej przed zakłóceniami, zniekształceniami, umożliwiając niezwłoczną realizację zakładanych przez decydentów działań. Z kolei od decydentów korzystających z nowoczesnych urządzeń przekazu powinno się wymagać precyzyjnego zarządzania personelem pracującym zdalnie, opartego na zrozumieniu i współpracy.

Janusz Syrówka

innogy Polska

Bariery infrastruktury krytycznej

Tworzenie systemów bezpieczeństwa dla infrastruktury krytycznej to temat, który ma etykietkę wiedzy tajemnej, zastrzeżonej dla nielicznych. Czy tak jest w istocie? Jak to zwykle bywa, trochę tak i trochę nie. Nazwa „infrastruktura krytyczna" nie wzięła się znikąd. Mówimy o obiektach, których sprawne i nieprzerwane funkcjonowanie jest niezbędne dla życia i bezpieczeństwa obywateli.

Skoro tak, to jest oczywiste, że pewne zagadnienia związane z funkcjonowaniem tejże infrastruktury nie są informacjami publicznymi. To jedna z naturalnych barier, która prowadzi do problemów ze stworzeniem skutecznej ochrony. Jeśli nie wiem, jak coś działa, to także nie wiem, jak to chronić.

Kolejną barierą są przepisy, które kwestie ochrony infrastruktury krytycznej regulują. Nie chcę odnosić się do samych przepisów, a wyłącznie do faktu, że one istnieją – trochę straszą, trochę zniechęcają.

Innym jeszcze problemem jest specyfika pracy w takich obiektach. W przypadku obiektów energetycznych wszelkie prace wymagają specjalnego reżimu. Mało tego, specyfika obiektu wymusza zmiany w projektach systemów bezpieczeństwa – choćby co do prowadzenia okablowania. To wszystko powoduje, że infrastruktura krytyczna to „takie cudo", o którym każdy słyszał, ale mało kto widział – zwłaszcza od środka.

Prawda jest natomiast taka, że zasady ochrony są uniwersalne. Trzeba wiedzieć, czemu ta ochrona służy i jaki efekt chcemy dzięki niej uzyskać. Wszystko to jest powiązane z brutalną ekonomią. Operator infrastruktury musi udźwignąć koszt jej zabezpieczenia. Taka sytuacja wymaga bardzo bliskiej współpracy między operatorem infrastruktury a dostawcą rozwiązań ochronnych. Nawet doświadczenia nabyte w trakcie realizacji u innych klientów nie zawsze gwarantują przewagę. Zawsze muszą to być ściśle dopasowane rozwiązania i w mojej ocenie brak obiektów IK w portfolio dostawcy nie stawia go na przegranej pozycji, szczególnie przy współpracy ze świadomym klientem.

Najnowszym wyzwaniem dla branży ochrony w działaniach na rzecz obiektów IK jest oczywiście pandemia koronawirusa. Firmy z branży ochrony muszą przestrzegać reżimu sanitarnego na najwyższym możliwym poziomie, gdyż transmisja zakażeń po stronie firmy ochrony może wpłynąć negatywnie na ciągłość działania operatora infrastruktury krytycznej.

Stanisław Dziubak

Instytut Łączności

Bezpieczeństwo obiektów teleinformatycznej infrastruktury krytycznej

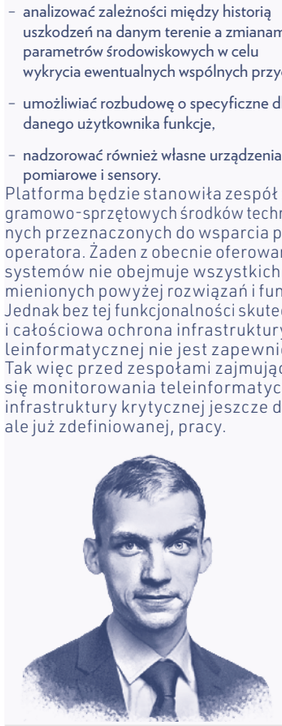
Według obecnego stanu wiedzy w skali kraju są dostępne specjalizowane systemy do monitorowania teleinformatycznej infrastruktury krytycznej o wąskim zakresie funkcji. Są przeznaczone m.in. do:

- kontroli dostępu do obiektów operatora,
- monitoringu parametrów środowiskowych, pożarów, zalania wodą oraz włamań,
- ochrony szaf dostępowych,
- monitoringu kabli miedzianych i światłowodowych.

Sytuacja ta wynika m.in. ze stopniowego wprowadzania w sieciach telekomunikacyjnych kolejnych elementów ochrony sieci. Dzisiejszym wyzwaniem dla zapewnienia bezpieczeństwa infrastruktury jest realizacja zaawansowanej platformy monitorowania obiektów telekomunikacyjnych na rzecz podmiotów odpowiedzialnych za eksploatację infrastruktury telekomunikacyjnej. Taka platforma powinna:

- dostarczać w czasie rzeczywistym dane o stanie obiektów i generować powiadomienia o stanach alarmowych,
- analizować zmiany parametrów określonych elementów, np. kabli, aby na ich podstawie wykrywać stopniowo rozwijające się uszkodzenia,
- analizować zależności między historią uszkodzeń na danym terenie a zmianami parametrów środowiskowych w celu wykrycia ewentualnych wspólnych przyczyn,
- umożliwiać rozbudowę o specyficzne dla danego użytkownika funkcje,
- nadzorować również własne urządzenia pomiarowe i sensory.

Platforma będzie stanowiła zespół programowo-sprzętowych środków technicznych przeznaczonych do wsparcia pracy operatora. Żaden z obecnie oferowanych systemów nie obejmuje wszystkich wymienionych powyżej rozwiązań i funkcji. Jednak bez tej funkcjonalności skuteczna i całościowa ochrona infrastruktury teleinformatycznej nie jest zapewniona. Tak więc przed zespołami zajmującymi się monitorowania teleinformatycznej infrastruktury krytycznej jeszcze dużo, ale już zdefiniowanej, pracy.



Jakub Sobek

Linc Polska

Jak uniknąć ataku?

Liczba czujników i sensorów monitorujących przemysłowe technologie sterowania stale rośnie. Urządzenia te, podłączone do sieci, wystawiają często całe systemy na potencjalne ataki. Jednak korzyści, jakie oferują urządzenia IoT, i komfort płynący z ich użytkowania jest na tyle duży, że rezygnacja z nich praktycznie nie jest obecnie możliwa. Im więcej podłączonych elementów do sieci, tym prawdopodobieństwo ataku jest większe, a jego skutki mogą być znacznie rozleglejsze. Wystarczy zaledwie jedno urządzenie IoT z luką bezpieczeństwa, aby stworzyć potencjalny wektor ataku. Co gorsza, eksploatacja takiej podatności, często przez wiele dni lub nawet miesięcy, może zostać niezauważona przez administratora. To daje osobie atakującej czas na penetrację całego systemu i wykradanie informacji.

Jak zatem nie rezygnować z komfortu korzystania ze współczesnej technologii i chronić pozostałe swoje systemy? Istotne jest, aby wybierać urządzenia sprawdzonych producentów, którzy przykładają najwyższą dbałość do jakości zabezpieczeń cybernetycznych w swoich urządzeniach. Niestety, na rynku istnieje wiele rozwiązań, w których kwestie bezpieczeństwa oprogramowania nie są traktowane priorytetowo. To właśnie software jest tym elementem, który najwyraźniej różnicuje produkty między sobą. Trzeba także pamiętać, że to obszar cyberbezpieczeństwa jest tym polem walki, na którym każdego dnia toczą się bitwy o bezpieczeństwo infrastruktury krytycznej.

Należy z dużą dbałością dobierać rozwiązania, korzystając tylko z oferty sprawdzonych producentów. Trzeba też przez cały czas śledzić wszystkie aktualizacje bezpieczeństwa, jakie są wydawane przez twórców oprogramowania. Duże firmy, korzystając z pomocy zespołów swoich profesjonalistów, są w stanie szybko reagować na pojawiające się nowe zagrożenia. Ponadto przeprowadzanie okresowych pentestów pozwala zweryfikować, czy wszystkie wdrożone polityki bezpieczeństwa są wystarczające.

Tomasz Goljaszewski

Hikvision Poland

Redukcja budżetów i przemiana energetyczna

Największe wyzwania dla bezpieczeństwa infrastruktury krytycznej będą w tym roku związane ze zmianami, jakie przyniosła pandemia, oraz przemianami energetycznymi, jakie będą zachodzić w naszym kraju. W przypadku infrastruktury krytycznej skutkiem pandemii jest przede wszystkim redukcja budżetów związanych z bezpieczeństwem i przeciąganie inwestycji, które to bezpieczeństwo mają zapewnić lub wzmocnić. Nadzór nad bezpieczeństwem infrastruktury krytycznej to domena państwa. Jest ona realizowana przez odpowiednie podmioty administracji państwowej ewentualnie przez odpowiednie działy spółek skarbu państwa. Wydatki związane z łagodzeniem licznych skutków pandemii, mniejsze wpływy do budżetu niestety odbiją się na wielu dziedzinach życia. Według mnie będzie po prostu mniej pieniędzy na wszystko, a więc również na realizację celów związanych z bezpieczeństwem infrastruktury krytycznej.

To będzie trudny czas dla ludzi odpowiedzialnych za jej bezpieczeństwo. Naszej branży jako całości sytuacja taka może przynieść straty, choć niektóre firmy mogą na tym skorzystać, ponieważ menedżerowie odpowiedzialni za bezpieczeństwo mogą szukać na rynku alternatywnych rozwiązań przynoszących redukcję kosztów.

Przemiana energetyczna kraju to przede wszystkim nowe inwestycje „gazowe" związane z jego transportowaniem i magazynowaniem oraz produkcja i magazynowanie energii ze źródeł odnawialnych (elektrownie wodne, farmy wiatrowe i fotowoltaiczne). Istotne też będzie poprawienie sprawności istniejących stacji energetycznych i budowa nowych, aby spełniały wymogi tworzącego się rynku prosumentów energii oraz rozwoju elektromobilności. Wszystkie te inwestycje będą wymagały nakładów związanych z bezpieczeństwem.

Mam nadzieję, że dzięki tym inwestycjom ciągle będzie zapotrzebowanie na zaawansowane rozwiązania, takie jak analityka wideo z wykorzystaniem technologii deep learning czy systemy termowizyjne. W kolejnych latach należy się spodziewać również inwestycji związanych z wytwarzaniem i magazynowaniem wodoru. I te inwestycje będą się charakteryzowały koniecznością zapewnienia wysokiego poziomu bezpieczeństwa. Ale to już przyszłość.

Anna Twardowska

Nedap Security Management

Cyberbezpieczeństwo systemów zabezpieczeń

Sprawna infrastruktura krytyczna jest coraz bardziej istotnym elementem bezpieczeństwa kraju, dlatego szczególnie ważne jest cyberbezpieczeństwo tych podmiotów. Aby przeanalizować kwestię bezpieczeństwa IK, należy przyjrzeć się wszystkim systemom włączonym do tej infrastruktury.

Świadomość potrzeby zabezpieczania systemów IT przed cyberatakami jest dziś powszechna. W coraz większej liczbie organizacji działy IT mają już opracowane zasady postępowania i narzędzia chroniące przed tego typu zagrożeniami. Wraz z rozwojem tych systemów i rozpowszechnieniem technologii IP bezpieczeństwo nabrało nowego wy-

miaru również w systemach zabezpieczeń technicznych. Większość podstawowych komponentów w tych systemach wykorzystuje standardową architekturę IT: serwery, systemy operacyjne, sieci LAN/WAN, a więc jest narażona nie tylko na próbę podrobienia karty, za pomocą której otwieramy drzwi, ale również na ataki z poziomu protokołu TCP/IP. Dlatego też systemy zabezpieczeń elektronicznych, jak wszystkie elementy architektury IT, powinny być zabezpieczane tymi samymi metodami.

Na kwestie cyberbezpieczeństwa należy spojrzeć zarówno od strony zabezpieczenia samych systemów zabezpieczeń, jak i od strony wyeliminowania niebezpieczeństwa nieautoryzowanego dostępu już na poziomie warstwy dostępu do sieci. Te zabezpieczenia powinny dotyczyć bezpiecznego przechowywania kluczy szyfrujących karty, szyfrowania wszystkich poziomów komunikacji (np. w KD szyfrowanie na styku karta-czytnik-kontroler-serwer-stacja kliencka), uwierzytelniania urządzeń dołączanych do systemu za pomocą dedykowanych certyfikatów. Należy zabezpieczyć wszystkie elementy podatne na ataki hakerów, tj. kontrolery czy czytniki KD.

Wspomnianym wcześniej elementem szerszej polityki cyberbezpieczeństwa jest zabezpieczenie przed nieautoryzowanym dostępem do sieci LAN już na poziomie warstwy dostępu do tej sieci. Można to osiągnąć dzięki implementacji modelu uwierzytelniania 802.1x (serwer RADIUS) przez wszystkie kontrolery sieciowe.

Marcin Walczuk

BCS

Najważniejsza jest ciągłość działania

W ciągu ostatniego roku z powodu panującej pandemii koronawirusa nasze życie uległo wielu zmianom. Raz po raz wprowadzane są kolejne obostrzenia mające na celu walkę z tym niewidzialnym wrogiem. Te zmiany są oczywiście dla nas dotkliwe i uciążliwe, jednak cały czas mamy dostęp do energii elektrycznej, wody, środków komunikacji i transportu czy łączności. Są to elementy wchodzące w skład tzw. infrastruktury krytycznej.

Aby uniknąć niewątpliwego wybuchu paniki i destabilizacji w kraju, jednym z priorytetów, jakie stawia przed sobą państwo polskie, jest zapewnienie bezpieczeństwa i odpowiedniego poziomu ochrony wszystkich przedsiębiorstw wchodzących w skład IK. Ważną w tym rolę odgrywają producenci i dostawcy rozwiązań związanych z szeroko pojętą branżą security. Nie chodzi przy tym tylko o zabezpieczenia techniczne, ale też o ochronę fizyczną. Czynnik ludzki jest tu tak istotny, ponieważ do obsługi elektronicznych systemów zabezpieczeń potrzebny jest wykwalifikowany operator, a pracownicy firm ochrony niejednokrotnie stanowią pierwszą linię przeciwdziałania pojawiającym się zagrożeniom.

Dopiero połączenie wszystkich tych elementów pozwoli na stworzenie sprawnie działającego systemu bezpieczeństwa, który będzie gwarantował szybką reakcję na zdarzenia, ale również, a może przede wszystkim pozwoli zawczasu eliminować sytuacje niebezpieczne, mogące zagrozić ciągłości działania przedsiębiorstwa. Nie wolno przy tym zapominać, że ciągłość działania jest konieczna w przypadku systemów zabezpieczeń, stąd niezmiernie istotną kwestią jest odpowiednia ich konserwacja i serwisowanie, co oczywiście leży po stronie dostawcy danego rozwiązania technicznego.

Dlatego też BCS, jako wiodący producent urządzeń i rozwiązań z zakresu telewizji dozorowej, dokłada wszelkich starań, aby oferowane systemy były przede wszystkim niezawodne i wyposażone w najnowocześniejsze rozwiązania techniczne. Zastosowanie rejestratorów i kamer z funkcjami zaawansowanej analizy obrazu pozwala na dokładniejsze określenie charakteru zagrożeń w wykrywanych zdarzeniach, minimalizując w ten sposób liczbę fałszywych alarmów. To z kolei przekłada się na efektywniejszą pracę operatorów systemu, a tym samych na bezpieczne funkcjonowanie przedsiębiorstw.

Marek Białek

Axis Communications Poland

Liczy się niezawodność i szybkość detekcji

Istotnym problem, z jakim aktualnie zmagają się menadżerowie odpowiedzialni za bezpieczeństwo fizyczne, jest nie tylko dobór odpowiedniego systemu zabezpieczeń, ale też opracowanie skutecznej strategii ochrony całego obiektu. W ochronie infrastruktury krytycznej liczy się przede wszystkim niezawodność i szybkość detekcji już na zewnątrz obiektu.

W pierwszym etapie budowy ochrony perymetrycznej istotne jest odpowiednie zastosowanie dostępnych technologii czy to w kamerach termowizyjnych, kamerach

wizyjnych czy radarach, a także dobrych czujek zewnętrznych montowanych np. na ogrodzeniu. Tak zaprojektowany system charakteryzuje się bardzo wysokim współczynnikiem wykrycia wtargnięcia do zabezpieczonej strefy, przy obniżonej dzięki weryfikacji wizyjnej liczbie fałszywych alarmów. System taki będzie niezawodnie działać bez względu na trudne warunki atmosferyczne, natomiast radar pozwoli szybko określić prędkość i kierunek poruszania się ewentualnego intruza. Dodatkowa integracja systemu audio umożliwi automatyczne wyzwalanie komunikatów ostrzegających i odstraszających.

Istotnym punktem wyjścia do opracowania skutecznej strategii ochrony jest świadomość, że obszarów przemysłowych nie da się podzielić na sterylne strefy. Każda strefa powinna być zintegrowana z systemami kontroli dostępu, dozoru wizyjnego z funkcjami analitycznymi oraz innymi systemami zabezpieczeń zainstalowanymi na obiekcie tak, aby nie generować niepotrzebnych alarmów, gdy w strefie znajdzie się np. pracownik.

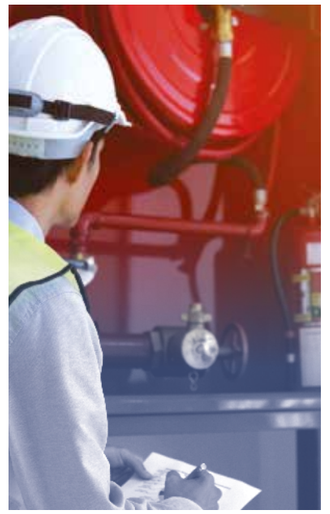
Krzysztof Kunecki

Schrack Seconet Polska

Możliwości nowoczesnych systemów bezpieczeństwa pożarowego

Obiekty infrastruktury krytycznej wymagają niezawodnych, bezpiecznych i elastycznych rozwiązań w zakresie ochrony przeciwpożarowej, aby zapewnić wdrożenie indywidualnej, dostosowanej do danego obiektu koncepcji bezpieczeństwa pożarowego. Celem głównym projektowanych i wdrażanych rozwiązań jest optymalna ochrona przeciwpożarowa, której podstawowym zadaniem jest bezpieczeństwo ludzi i mienia oraz zapewnienie ciągłości działania całej organizacji w razie pożaru. Aby zapewnić najwyższy poziom ochrony, należy zapewnić utrzymanie pełnej sprawności urządzeń, a to wymaga prawidłowej eksploatacji, serwisu i konserwacji urządzeń wchodzących w skład instalacji.

W zakresie eksploatacji bardzo ważne jest monitorowanie stanu pracy instalacji i jak najwcześniejsze zgłaszanie odchyleń od normalnego stanu pracy urządzeń, jeszcze zanim urządzenie będzie całkowicie niesprawne, co pozwoli zapobiec powstaniu poważnej awarii. Dlatego też nowoczesne systemy umożliwiają wcześniejsze zasygnalizowanie odbiegających od wymagań projektowych, nieprawidłowych stanów pracy, jak np. niebezpieczne zabrudzenie układów detekcyjnych czujek pożarowych, zmiana rezystancji linii dozorowych i sterujących spowodowana starzeniem się instalacji czy rozszczelnienia w układach pneumatycznych czujek zasysających dymu i liniowych czujek ciepła dzięki dokładnemu monitorowaniu przepływu powietrza. Ponadto, dzięki stałemu monitorowaniu temperatury przez zaawansowane wielosensorowe czujki pożarowe dymu i ciepła, można te dane przesyłać przez centrale sygnalizacji pożarowej do systemów zewnętrznych w celu monitorowania chronionych obszarów i urządzeń.



Możliwość bieżącego odczytu wartości analogowych (temperatura, zadymienie, stężenie CO) z czujek punktowych daje duże pole do współdziałania z innymi systemami instalowanymi w nowoczesnych obiektach. Dzięki tego typu funkcjonalnościom mogą być również sygnalizowane nieprawidłowe stany pracy występujące w innych instalacjach i systemach, np. uszkodzenia w układach klimatyzacji serwerowni czy podwyższona temperatura w pomieszczeniach produkcyjnych.

Do optymalnego zarządzania i dokładnego nadzorowania stanu pracy urządzeń nieodzowny jest system zarządzania bezpieczeństwem pożarowym (system integrujący urządzenia ppoż., tzw. SIUP), który dzięki cyfrowej integracji z systemami bezpieczeństwa pożarowego pozwala na szczegółową wizualizację odczytanych wartości binarnych i analogowych i w efekcie na szybką identyfikację źródła rozwijającego się problemu. System może też integrować się z innymi systemami technicznymi i bezpieczeństwa w obiekcie (BMS/BAS, SMS i inne) oraz przekazywać informacje ważne dla obszaru zarządzania obiektem.

Wcześniejsze wykrycie nieprawidłowości na wstępnym etapie i wezwanie serwisu jest tu sprawą kluczową, bo minimalizuje ryzyko wystąpienia poważnej awarii, która może zatrzymać działanie np. linii produkcyjnej w obiekcie przemysłowym. Nie bez znaczenia jest także fakt, że systemy integrujące urządzenia przeciwpożarowe, mając wszystkie wymagane dokumenty formalne, jak certyfikat stałości właściwości użytkowych oraz świadectwo dopuszczenia CNBOP, są jedynymi systemami w obiekcie, które umożliwiają pełne zarządzanie ewakuacją ludzi z obiektu. Bezpieczne zarządzanie ewakuacją ma ogromne znaczenie w przypadku innych zdarzeń krytycznych w obiekcie, np. akty terroru, uwolnienie niebezpiecznych środków chemicznych, katastrofy budowlane czy inne zdarzenia stwarzające zagrożenie.

Niektóre firmy ubezpieczeniowe (VdS, FM Global) wymagają, aby współczynnik rocznej dostępności instalacji sygnalizacji pożarowej (tzn. czas, w którym instalacje ppoż. powinny być w bezwzględnej gotowości do działania) wynosił 98-99%. Oznacza to także ograniczenie czasu przeglądów, konserwacji i napraw, które nie powinny trwać dłużej niż 180 godzin rocznie. Jeżeli te granice czasowe są przekraczane, można stwierdzić, że system ulega degradacji lub nie spełnia wymagań. Aby skrócić przerwy w pracy urządzeń podczas prac modernizacyjnych i serwisowych wymagane jest wdrożenie odpowiedniej topologii/organizacji systemu, a także wykorzystanie specjalnych funkcji systemu i narzędzi serwisowych. Dzięki temu jest możliwe np. centralne zaprogramowanie wszystkich urządzeń w ramach sieci central sygnalizacji pożarowej.

Podczas uruchomionego procesu programowania (przesyłania danych) do urządzeń system realizuje swoje funkcje w sposób niezakłócony, a dopiero po otrzymaniu nowego programu przez wszystkie centrale następuje restart. Po kilku minutach system z nowym oprogramowaniem jest w stanie pełnej gotowości.

Kolejną istotną funkcją w tym zakresie jest możliwość zamrażania (blokowania fizycznego) wyjść sterujących na czas przeprowadzania testów instalacji czy też przełączania czujek w specjalny tryb serwisowy. W tym trybie, mimo stanu odłączenia, czujki mogą przekazać informację o wykrytym pożarze, aby poinformować obsługę i uruchomić kluczowe urządzenia bezpieczeństwa pożarowego.

Aby firma serwisująca była jak najszybciej powiadomiona o ewentualnych nieprawidłowościach może skorzystać z narzędzi do zdalnego dostępu i nadzoru w celu ciągłego monitorowania instalacji. W przypadku wystąpienia uszkodzenia analiza wstępna problemu odbywa się jeszcze przed przyjazdem do obiektu. Dzięki temu serwisant, który uda się na miejsce, będzie odpowiednio przygotowany i wyposażony w niezbędne narzędzia i części zamienne. Pozwoli to szybko przywrócić pełną sprawność instalacji.

Inwestycja w zaawansowane rozwiązania przynosi wymierne korzyści - umożliwia utrzymanie wymaganej sprawności urządzeń w ramach instalacji bezpieczeństwa pożarowego dzięki dokładniejszemu nadzorowaniu instalacji i szybszej identyfikacji ewentualnych źródeł problemów. W rezultacie minimalizuje to ryzyko wystąpienia poważnych awarii wstrzymujących ciągłość działania obiektu.

Cyberzagrożenia a bezpieczeństwo fizyczne. Cz. 1

Elektroniczne systemy zabezpieczeń już dawno przestały być postrzegane jako proste autonomiczne rozwiązania wykorzystujące do transmisji standardy analogowe lub szeregowe, stając się zaawansowanymi rozwiązaniami opartymi na protokole TCP/IP. Zmiana ta przyniosła nie tylko wymierne korzyści, ale także nowe zagrożenia. Cyberbezpieczeństwo odmieniane jest przez wszystkie przypadki, a ataki na infrastrukturę krytyczną jedynie dodają temu zagadnieniu rozgłosu.

Jak w związku z tym, w kontekście bezpieczeństwa teleinformatycznego (IT), należy podchodzić do elektronicznych systemów zabezpieczeń technicznych? Czy rzeczywiście trzeba je chronić również w obszarze środowiska IT, w którym pracują? Postaram się odpowiedzieć na te pytania, wskazując, na co zwracać szczególną uwagę i jak z korzyścią łączyć cyberbezpieczeństwo z bezpieczeństwem fizycznym.

Zabezpieczenia elektroniczne stały się już istotnym aspektem każdej polityki bezpieczeństwa i śmiało wkroczyły do świata IT, a co za tym idzie, do świata bezpieczeństwa IT. Powody tego są następujące:

- Wzrasta świadomość i wiedza nt. urządzeń i systemów zabezpieczeń, które są „na pierwszej linii ognia". Cóż z tego, że wdrożymy w środowisku IT kompleksową ochronę wielowarstwową, tzw. DiD *(Defence in Depth)*, jeśli dostęp do terenu, budynku, pomieszczenia, szafy rack będzie nieodpowiednio zabezpieczony, co może doprowadzić do łatwego skompromitowania zabezpieczeń IT.
- Krajowe uregulowania prawne, tj. ustawa o Krajowym Systemie Cyberbezpieczeństwa czy ustawa o ochronie informacji niejawnych zaczęły zauważać istotę problemu, nie tylko odnosząc się do omawianej tematyki, ale także wydając oddzielne rozporządzenia wykonawcze.

Czy zatem każda osoba z branży security powinna stać się administratorem środowiska IT? Zdecydowanie nie

Tomasz Dacka

(chociaż to interesująca tematyka). Czy należy więc to ryzyko w pełni przenieść do działów IT? Nie jestem zwolennikiem tej metody. Działy Sec IT bardzo często nie rozumieją istoty sprawy, celów i zasady działania elektronicznych systemów zabezpieczeń, nie znają standardów, wytycznych czy norm. Z kolei osoby odpowiedzialne za zabezpieczenia elektroniczne nie kwapią się z dostarczaniem pomocnych informacji. Kamera CCTV lub kontroler SKD to jednak nie serwer czy środowisko wirtualne. Do tego dochodzą bariera wynikająca z braku zrozumienia podstawowych zasad zabezpieczania architektury IT przez typowych „bezpieczników" oraz brak wypracowanego wspólnego języka dwóch odrębnych działów bezpieczeństwa, grających tak naprawdę do jednej bramki. Czy można zatem te dwa światy połączyć w sposób optymalny? Uważam, że można. Ponieważ urządzenia i systemy zabezpieczeń działają w środowisku IT, a nie odwrotnie, to właśnie one głównie muszą dostosować się do standardów, prawideł świata IT. Na co zatem zwrócić szczególną uwagę?

OGÓLNE WYTYCZNE

Branża security może z powodzeniem czerpać z najlepszych praktyk *(best practices)* z branży IT, przekładając je na codzienną pracę. Branża IT wypracowała kilka tzw. *frameworków*, ogólnych wytycznych działania, metodyk, które w pewnych aspektach są zbieżne z celami branży zabezpieczeń. Wspólnie chronimy przecież aktywa. I tak w typowym świecie zer i jedynek wykorzystujemy czynniki kontrolne *(security controls)*, dzięki czemu zapewniamy zasobom odpowiedni poziom bezpieczeństwa. *Security controls* dzielą się na trzy główne obszary:

- administracyjne – określane za pomocą polityk, procedur i wytycznych sposoby postępowania w określonych sytuacjach. Można to przełożyć na zasady dostępu do obiektu, ustalenie harmonogramu przeglądów technicznych, skanów podatności, zasad obsługi incydentów lub przekazywania materiału wizyjnego zainteresowanym stronom;
- techniczne – dotyczą bezpieczeństwa urządzeń ***(appliances)***, aplikacji ***(software)*** czy środowisk systemów operacyjnych (OS). Do tego obszaru zaliczymy zabezpieczenia, tj. ACL ***(Access Control Lists)*** czy IDS ***(Intrusion Detection Systems)***, a także dobrze nam znane SKD, VSS, VMS, SSWiN;
- fizyczne – organizujące głównie ruch, np. ogrodzenie, śluza, zamki, znaki ostrzegawcze, bramki, oświetlenie itp.

ANALIZA RYZYKA

Z dużym niepokojem obserwuję w branży security niechęć do przeprowadzania analizy ryzyka na etapie koncepcji czy projektu wykonawczego, a tym samym brak wymagań po stronie inwestorów co do jej przeprowadzania. A to właśnie ten dokument wskazuje, przed czym i w jaki sposób mamy chronić. Analiza ryzyka w security IT jest wszechobecna, wiele decyzji podejmuje się właśnie na jej podstawie. Zanim zaprojektujemy, zamontujemy kamerę, musimy wiedzieć, jakie

cele i zadania dany punkt kamerowy ma realizować (np. obserwację czy inspekcję zgodnie z normą PN EN 62676-4 *Systemy dozoru wizyjnego stosowane w zabezpieczeniach: Wytyczne stosowania*). Identyfikacja aktywów, podatności, zagrożeń, a następnie ocena ryzyka i sposobu postępowania z nim (tzw. mitygacja) są sprawą kluczową na początkowych etapach wdrażania, późniejszej modernizacji czy wymiany systemów. Zachęcam do przeprowadzania analiz, które nie muszą być rozbudowanym dokumentem, można je wykonać np. w sposób graficzny (analiza typu Bow – Tie). Schemat tego typu analizy przedstawiono na *rys. 1*.

CIA

Nie mam zamiaru wprowadzać czytelnika w tajniki pracy operacyjnej jednej z najbardziej znanych agencji na świecie. CIA to również skrót od *Confidentiality, Integrity, Availability* i odnosi się do trzech głównych atrybutów informacji i danych: poufność, integralność, dostępność *(rys. 2)*. Systemy VSS czy KD przetwarzają ogromne ilości danych (w tym dane osobowe), które ze względu na ogólnie pojęte bezpieczeństwo są szczególnie narażone na utratę wymienionych atrybutów. Do tego dochodzą zapisy RODO wymuszające ochronę danych osobowych w sposób adekwatny do celu ich przetwarzania.

POUFNOŚĆ – informacje są przeznaczone tylko dla uprawnionych osób. Nasze nagrania wideo czy możliwość nadawania uprawnień nie mogą być dostępne dla każdego użytkownika.

INTEGRALNOŚĆ – zapewniona jest spójność danych, które nie mogą być w żaden sposób modyfikowane bez naszej wiedzy. Najlepszym przykładem jest atak typu Man in the Middle, kiedy atakujący jest w stanie przechwycić uprawnienia administratora systemu SKD i dobrowolnie nadawać prawo dostępu do zabezpieczonych stref. Innym przykładem są nagrania wideo, które mogą stanowić dowody wystąpienia incydentu, tutaj również musimy być pewni, że materiał nie był modyfikowany.

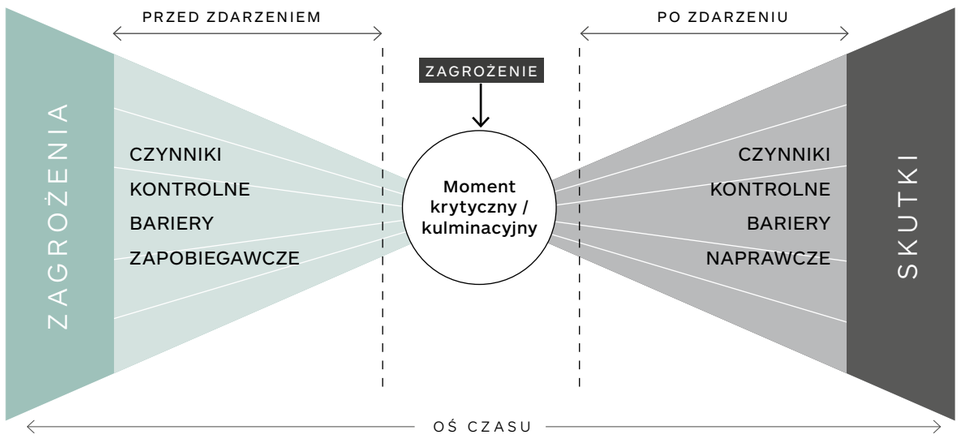
Rys. 2. Triada CIA

DOSTĘPNOŚĆ – informacja jest osiągalna dla osób uprawnionych, poufność zapewnia nam uprawnienie do zapoznania się z nią, a dostępność to, że w każdym momencie możemy to zrobić. Zapewniamy tym samym pełną rozliczalność systemów bezpieczeństwa w momencie śledztwa w obszarze wystąpienia incydentu, czy zasilamy danymi systemy analityczne. To również atrybut, który zapewnia dostęp do kopii zapasowych.

W jaki zatem sposób triada CIA przekłada się na codzienne obowiązki specjalisty ds. bezpieczeństwa? Czy poufność, integralność i dostępność odgrywają ważną rolę w codziennych obowiązkach? Zachęcam do przeanalizowania wybranych kwestii:

- Jaki system operacyjny pracuje w danej kamerze i czy np. nie jest to stara dystrybucja Linuxa z dosyć długą listą dobrze wszystkim znanych podatności?
- Czy dana kamera zawiera moduł TPM *(Trusted Platform Module)*, aby w sposób bezpieczny przechowywać poświadczenia (klucze kryptograficzne, certyfikaty)? I czy mamy pomysł na to, jak z tych poświadczeń korzystać?

Rys. 1. Scenariusz ryzyka Bow-TIE



- Czy nasze urządzenia pozwalają nam na wdrożenie uwierzytelniania zgodnie ze standardem 802.1x? Dzięki temu eliminujemy ryzyko wpięcia do naszej sieci urządzeń, które nie będą w stanie się uwierzytelnić zgodnie z wdrożonymi przez nas zasadami.
- Jaką technologię RFID wykorzystują nasze karty i czytniki SKD? Czy jest bezpieczna, czy jednak łatwa do skompromitowania, a skopiowanie karty nie nastręcza problemów?
- Jakie protokoły komunikacyjne wykorzystują nasze systemy i czy gwarantują poufność oraz integralność przetwarzanych informacji?
- Czy szyfrujemy dane? A jeśli tak, to za pomocą jakiego algorytmu i czy jest on na tyle „silny", by w akceptowalny sposób „obudować" nasze dane?
- Czy jest sens tworzenia kopii zapasowych i budowania środowiska redundantnego na wypadek awarii serwera i błędów bazy danych (dostępność informacji)? Czy mamy wdrożone plany backupowe oraz disaster recovery dla naszego obszaru?
- Czy jesteśmy zabezpieczeni odpowiednimi umowami aktualizacji systemów w momencie wykrycia błędów w oprogramowaniu?
- Czy sprawdziliśmy łańcuch dostaw urządzeń i oprogramowania, czy jest on dla nas akceptowalny?
- Czy zapewniliśmy unikatowe loginy do urządzeń, a może nadal działają na domyślnym użytkowniku i haśle? Czy wprowadziliśmy politykę dotyczącą haseł?

HARDENING

Pojęcie to, niestety nieznane jeszcze w branży zabezpieczeń (security), wywodzące się ze świata IT, tłumaczy się jako „utwardzanie" urządzeń. Co oznacza i dlaczego jest tak ważne? Wyjmując kamerę z pudełka czy instalując oprogramowanie VMS od dostawcy, mamy produkt skonfigurowany domyślnie pod kątem łatwości użytkowania (tzw. *plug and play*). Kamerze należy tylko nadać adres IP, wyregulować optykę i już działa (zachęcam do głębszych konfiguracji każdego punktu kamerowego).
Patrząc jednak przez pryzmat sposobu, w jaki kamera się komunikuje, sprawa nie jest taka prosta. Domyślna konfiguracja zazwyczaj nie zapewnia odpowiedniego poziomu bezpieczeństwa w warstwach aplikacyjnych i komunikacyjnych. Jak to w życiu często bywa, to, co ułatwia pracę (np. protokoły typu *discovery* usprawniające wyszukiwanie kamer w sieci po adresach MAC) stanowi duże zagrożenie od strony cyberbezpieczeństwa.
Wiodący producenci wydają wytyczne w tym zakresie, tzw. hardening guide, krok po kroku opisujące czynności, jakie należy wykonać, aby utrudnić potencjalnym intruzom „dostęp" do systemu (np. zamykać porty niepotrzebne do codziennej pracy kamery, jakie usługi systemu VMS, OS należy wyłączyć, jeśli nie są wykorzystywane). Uważam, że *hardening* systemów zabezpieczeń powinien być ostatnim elementem wdrożenia i podlegać ocenie przy odbiorze.

LEAST PRIVILEGE

Termin ten odnosi się do wyspecyfikowania uprawnień do urządzeń i aplikacji w taki sposób, aby użytkownik posiadał tylko te poświadczenia i dostępy, które są mu potrzebne do wykonywania swoich obowiązków. Operator centrum nadzoru ma dostęp do obrazu na żywo, może przeglądać materiał archiwalny, ale nie ma uprawnień do jego kasowania czy kopiowania. Jeśli jest to konieczne, wymaga poświadczeń kierownictwa, które tym samym autoryzuje taką czynność (tzw. zasada *two-man rule*). Ma to również odniesienie do wymagań RODO, w ten sposób zapewniamy wymóg tzw. minimalizacji danych.

CERTYFIKATY

Certyfikat dla urządzenia (np. kamery) potwierdza jego tożsamość. Powinien być wydany przez jednostkę certyfikującą *(Certificate Authority – CA)*. Nie wchodząc w strukturę działania CA, załóżmy, że mamy w organizacji swój wewnętrzny CA wystawiający odpowiednie certyfikaty dla naszych urządzeń. Wtedy jesteśmy pewni, że w sieci działają tylko autoryzowane przez nas urządzenia (odnosząc się dodatkowo do wspomnianego wcześniej standardu uwierzytelniania 802.1x).
Ryzyko podmiany kamery czy jej demontażu, by w ten sposób dostać się do sieci, jest raczej niewielkie, natomiast ryzyko nieuprawnionego wejścia do sieci za pomocą stacji interkomowej wyniesionej do strefy ogólnodostępnej gwałtownie wzrasta. To jedna strona medalu. Drugą jest sposób działania intruzów, który przedstawię w drugiej części artykułu.
W kolejnej części postaram się też wyjaśnić na czym polega *modus operandi* cyberprzestępców opisany przez tzw. *The Kill Chain, rozszyfruję znaczenie skrótu AAA oraz przedstawię cykl „życia" bita w elektronicznych systemach zabezpieczeń.*

TOMASZ DACKA

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

Cyberbezpieczeństwo w firmach branży S&S

CZ. 2

W części pierwszej artykułu, która ukazała się w nr. 1/2021 „a&s Polska”, przywołano Dyrektywę Parlamentu Europejskiego i Rady (UE) w sprawie cyberbezpieczeństwa w unijnej cyberprzestrzeni oraz polską ustawę i sześć rozporządzeń wydanych na podstawie jej delegacji, stanowiących łącznie z ustawą bazę normatywno-prawną Krajowego Systemu Cyberbezpieczeństwa (KSC).

Marek Ryszkowski

Wspomniano w niej także o metodyce audytowania stanu cyberbezpieczeństwa, opracowanej i wdrożonej przez Urząd Dozoru Technicznego (UDT), która została nazwana przez jej twórców metodyką **Framework UDTCyber.** Audytorzy **UDTCert** zapewne już ją stosują do audytowania stanu cyberbezpieczeństwa w podmiotach prawa handlowego lub podmiotach o innym statusie prawnym, które są – w rozumieniu ustawy o krajowym systemie cyberbezpieczeństwa (w cz. I artykułu pod lp. 1) – operatorami usług kluczowych lub dostawcami usług cyfrowych. Przywołano również ustawowe definicje terminów: cyberbezpieczeństwo, usługa kluczowa, operator usługi kluczowej i dostawca usługi cyfrowej.
Wspomniano w pierwszej części artykułu także o tym, że zastosowanie niektórych metod teorii systemów może być użyteczne w rozważaniu przez kierownitwo podmiotów decyzji – budować system cyberbezpieczeństwa w zarządzanym podmiocie czy nie budować go. Jeżeli z analizy i syntezy problemu wyłoni się decyzja (wniosek decyzyjny): budować, w dalszych działaniach kierownictwa będzie niezbędna dogłębna znajomość nie tylko ustawy i rozporządzeń, o których wspomniano wyżej, lecz także metodyki Framework UDT-Cyber. Zapewnienie bezpieczeństwa danych (aktywom informacyjnym) podlegających obligatoryjnej lub fakultatywnej ochronie w polskim systemie prawnym, przetwarzanych w systemach i sieciach teleinformatycznych jest obowiązkiem nie tylko decydentów unijnych i krajowych, lecz także zarządców podmiotów prawa handlowego i podmiotów o innym statusie prawnym, działających w polskiej, zatem także unijnej przestrzeni prawnej.
Zobaczmy zatem najpierw, czym jest owa metodyka UDT-u, nazwana Framework UDTCyber. Oto, co na jej temat można przeczytać na stronie internetowej UDT-u oraz w numerze 2/2020 biuletynu UDT-u – INSPEKTOR, TECHNIKA i BEZPIECZEŃSTWO.

Metodyka oceny Framework UDTCyber opracowana została przez Urząd Dozoru Technicznego na potrzeby przeprowadzania audytu (wszystkie podkreślenia i wstawki w nawiasach [...] – MR) organizacji [podmiotów] w obszarze cyberbezpieczeństwa. Jest ona oparta na międzynarodowych metodykach, tj. NIST Cybersecurity Framework i ISO/IEC 27001, wytycznych i wymaganiach norm: PN-ISO/IEC 27002 i PN-EN ISO 22301 oraz na wymaganiach Ustawy o Krajowym Systemie Cyberbezpieczeństwa – UoKSC (Dz. U. 2018 poz. 1560). Metodyka [ta] to struktura ramowa systemu oceny stanowiąca jednocześnie podstawę do budowania programu [chyba systemu] cyberbezpieczeństwa w organizacji. Konieczność stworzenia niniejszej metodyki i opracowania na jej podstawie systemu oceny, stosowanego podczas audytu cyberbezpieczeństwa wynikała z potrzeby wiedzy jak dobrze zbudować oraz ocenić wdrożony program [lokalny lub ponadlokalny system] cyberbezpieczeństwa[1].

1) www.udt.gov.pl
2) Mowa o Rozporządzeniu Ministra Cyfryzacji z 4 grudnia 2019 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo. Rozporządzenie ogłoszono w DzU z 23.XII.2019 r. poz. 2479, z 14-dniowym vacatio legis, czyli weszło ono w życie 7 stycznia 2020 r.

Warto zastanowić się nad znaczeniem wiedzy dla kierownictwa podmiotów, także tych z branży S&S, co się kryje pod podkreślonymi fragmentami powyższego tekstu, który opublikowany został na stronie internetowej UDT-u. Instytucja ta, z mocy przepisów ww. ustawy i rozporządzeń wykonawczych, uzyskała niemałe kompetencje i znaczącą pozycję w Krajowym Systemie Cyberbezpieczeństwa (KSC). Kompetencje te wymieniono poniżej, bo wiedza o nich może być ważna dla niektórych czytelników.

UDTCERT W OBSZARZE CYBERBEZPIECZEŃSTWA REALIZUJE AUDYT CYBERBEZPIECZEŃSTWA NA ZGODNOŚĆ Z WYMAGANIAMI USTAWY O KSC Z DNIA 5 LIPCA 2018 R. ORAZ:

1. certyfikuje system zarządzania bezpieczeństwem funkcjonalnym (FSM – Functional Safety Management);
2. certyfikuje system zarządzania bezpieczeństwem informacji wg wymagań PN-EN ISO/IEC 27001;
3. certyfikuje system zarządzania ciągłością działania wg wymagań PN-EN ISO 22301;
4. prowadzi szkolenia w obszarze audytu, certyfikacji i analizy zagrożeń w obszarze cyberbezpieczeństwa.

Zamierzałem przedstawić najważniejsze z przedsięwzięć, które zamieścili autorzy UDT-u w swojej metodyce audytowania stanu cyberbezpieczeństwa w podmiotach – operatorach usług kluczowych lub dostawcach usług elektronicznych. Jednakże próby pozyskania tekstu tej metodyki z UDT-u okazały się bezowocne. Także przyczyn tego stanu rzeczy nie zdołałem dociec. Postanowiłem zatem w tej sytuacji skoncentrować się na dyspozycjach rozporządzenia ministra cyfryzacji, wyszczególnionego w pierwszej części tego artykułu pod. lp. 7[2]. Określa ono warunki organizacyjno-prawne i techniczne wpisania określonego podmiotu przez uprawniony ***organ właściwy do spraw cyberbezpieczeństwa***[3] do rejestru ww. operatorów i dostawców[4]. Niżej przywołane zostaną tylko te warunki i wymagania, które mogą być najistotniejsze dla zarządców podmiotów prawa handlowego z branży S&S, gdyż katalog wspomnianych wymagań i warunków, technicznych i organizacyjno-prawnych jest imponująco obszerny.

3) Organami właściwymi do spraw cyberbezpieczeństwa są: 1) dla sektora energii – minister właściwy do spraw energii; 2) dla sektora transportu z wyłączeniem podsektora transportu wodnego – minister właściwy ds. transportu; 3) dla podsektora transportu wodnego – minister właściwy ds. gospodarki morskiej i minister właściwy ds. żeglugi śródlądowej; 4) dla sektora bankowego i infrastruktury rynków finansowych – Komisja Nadzoru Finansowego; 5) dla sektora ochrony zdrowia z wyłączeniem podmiotów, o których mowa w art. 26 ust. 5 – minister właściwy ds. zdrowia; 6) dla sektora ochrony zdrowia obejmującego podmioty, o których mowa w art. 26 ust. 5 – Minister Obrony Narodowej; 7) dla sektora zaopatrzenia w wodę pitną i jej dystrybucji – minister właściwy ds. gospodarki wodnej; 8) dla sektora infrastruktury cyfrowej z wyłączeniem podmiotów, o których mowa w art. 26 ust. 5 – minister właściwy ds. informatyzacji; 9) dla sektora infrastruktury cyfrowej obejmującego podmioty, o których mowa w art. 26 ust. 5 – Minister Obrony Narodowej; 10) dla dostawców usług cyfrowych z wyłączeniem podmiotów, o których mowa w art. 26 ust. 5 – minister właściwy ds. informatyzacji; 11) dla dostawców usług cyfrowych obejmujących podmioty, o których mowa w art. 26 ust. 5 – Minister Obrony Narodowej (art. 41 ustawy).
4) Rejestr ten prowadzi minister cyfryzacji (art. 7 ust.1 ustawy).
5) Art. 8. Operator usługi kluczowej wdraża system zarządzania bezpieczeństwem w systemie informacyjnym wykorzystywanym do świadczenia usługi kluczowej, zapewniający: 4) zarządzanie incydentami; 6) stosowanie środków łączności umożliwiających prawidłową i bezpieczną komunikację w ramach krajowego systemu cyberbezpieczeństwa. Art. 11. 1. Operator usługi kluczowej: 1) zapewnia obsługę incydentu; zapewnia dostęp do informacji o rejestrowanych incydentach właściwemu CSIRT MON, CSIRT NASK lub CSIRT GOV w zakresie niezbędnym do realizacji jego zadań; 3) klasyfikuje incydent jako poważny na podstawie progów uznawania incydentu za poważny; 4) zgłasza incydent poważny niezwłocznie, nie później niż w ciągu 24 godzin od momentu jego wykrycia, do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV; 5) współdziała podczas obsługi incydentu poważnego i incydentu krytycznego z właściwym CSIRT MON, CSIRT NASK lub CSIRT GOV, przekazując niezbędne dane, w tym dane osobowe. Art. 12. 1. Określa, co powinno zawierać głoszenie, o którym mowa w art. 11 ust. 1 pkt 4. Natomiast Art. 13. Stanowi, że operator usługi kluczowej może przekazywać do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV informacje: 1) o innych incydentach; 2) o zagrożeniach cyberbezpieczeństwa; 3) dotyczące szacowania ryzyka; 4) o podatnościach; 5) o wykorzystywanych technologiach.

Paragraf pierwszy rozporządzenia określa warunki organizacyjne, których spełnienie jest niezbędne do uzyskania uprawnień podmiotu świadczącego usługi z zakresu cyberbezpieczeństwa. Natomiast jego paragraf drugi określa warunki techniczne, jakie obowiązane są spełniać podmioty świadczące usługi z zakresu cyberbezpieczeństwa, oraz wewnętrzne struktury organizacyjne operatorów usług kluczowych odpowiedzialne za cyberbezpieczeństwo. Z mojego doświadczenia wynika, że warunki techniczne bardziej powinny interesować kierownictwo firm branży S&S, bowiem ich spełnienie jest znacznie kosztowniejsze, od spełnienia warunków organizacyjnych, zapewnienia bezpieczeństwa cyberbezpieczeństwa. Utrzymanie tych warunków w czasie na wymaganym poziomie także generuje niemałe koszty. Oto wybrane postanowienia § 2 ust. 2 ww. rozporządzenia. Część znaczną tych postanowień przedstawiono niżej w formie cytatów.

Podmioty świadczące usługi z zakresu cyberbezpieczeństwa oraz wewnętrzne struktury organizacyjne operatorów usług kluczowych odpowiedzialne za cyberbezpieczeństwo, które wykonują czynności związane z realizacją obowiązków, o których mowa w art. 8 pkt 4 i 6, art. 11 ust. 1 pkt 1–5, art. 12 i art. 13[5] *[podkr. MR] ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, są obowiązane stosować następujące zabezpieczenia pomieszczenia lub zespołu pomieszczeń adekwatne do przeprowadzonego szacowania ryzyka (...).*

Metody szacowania ryzyka i zarządzania nim mogą być zapewne takie same lub podobne, jak w wypadku szacowania ryzyka dla bezpieczeństwa informacji niejawnych, tj. opatrywanych klauzulami tajności ŚCIŚLE TAJNE, TAJNE, POUFNE I ZASTRZEZONE.

DLA ZAPEWNIENIA CYBERBEZPIECZEŃSTWA W DANYM PODMIOCIE SĄ TO M.IN. WYSZCZEGÓLNIONE NIŻEJ ZABEZPIECZENIA:

1) ściany i stropy pomieszczenia lub zespołu pomieszczeń, w których będą świadczone usługi z zakresu cyberbezpieczeństwa, powinny mieć klasę odporności ogniowej co najmniej EI 60, określoną w Polskiej Normie PN-EN 1350-1[6]*, a budynek, w którym będą świadczone usługi z zakresu cyberbezpieczeństwa, powinien mieć klasę odporności pożarowej nie niższą niż klasa B, określoną w przepisach wydanych na podstawie art. 7 ust. 2 pkt 1 ustawy z 7 lipca 1994 r. – Prawo budowlane (Dz.U. z 2019 r. poz. 1186, z późn. zm.);*

2) drzwi do pomieszczenia lub zespołu pomieszczeń spełniające co najmniej wymagania klasy 2 określone w Polskiej Normie PN-EN 1627, wyposażone w zamek spełniający co najmniej wymagania klasy 4 określone w Polskiej Normie PN-EN 12209, o ile na podstawie przeprowadzonego szacowania ryzyka do-stęp do nich rodziłby nieakceptowane ryzyko nieuprawnionego wejścia do [tego] pomieszczenia lub zespołu [tych] pomieszczeń;

3) konstrukcję pomieszczenia lub zespołu pomieszczeń zapewniającą odporność na próbę nieuprawnionego dostępu;

4) okna spełniające co najmniej wymagania klasy 2 określone w Polskiej Normie PN-EN 1627, o ile na podstawie przeprowadzonego szacowania ryzyka dostęp do nich niesie nieakceptowalne ryzyko nieuprawnionego wejścia do pomieszczenia lub zespołu pomieszczeń;

5) szafy o podwyższonej odporności ogniowej, zabezpieczające przed próbami włamań oraz pożarami, odpowiednio do wartości danych oraz ewentualnych innych zagrożeń, na podstawie przeprowadzonego szacowanego ryzyka, służące do przechowywania dokumentacji papierowej oraz informatycznych nośników danych mających istotne znaczenie dla prowadzonej działalności;

6) system kontroli dostępu obejmujący wszystkie wejścia i wyjścia kontrolowanego obszaru, w którym co najmniej rozpoznanie osoby uprawnionej następuje w wyniku odczytu identyfikatora lub odczytu cech biometrycznych, oraz rejestrujący zdarzenia;

7) stały nadzór osoby uprawnionej nad osobami niewykonującymi czynności związanych z realizacją obowiązków, o których mowa w art. 8 pkt 4 i 6, art. 11 ust. 1 pkt 1–5, art. 12 i art. 13 ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa, przebywającymi w pomieszczeniu lub zespole pomieszczeń, w których wykonywane są te czynności;

8) system sygnalizacji napadu i włamania spełniający co najmniej wymagania systemu stopnia 2 określone w Polskiej Normie PN-EN 50131-1, stale monitorowany przez personel bezpieczeństwa oraz wyposażony w rezerwowe źródło zasilania i obejmujący ochroną wejścia i wyjścia kontrolowanego obszaru oraz sygnalizujący co najmniej: a) otwarcie drzwi, okien i innych zamknięć chronionego obszaru, b) poruszanie się w chronionym obszarze, c) stan systemu, w tym generujący ostrzeżenia i alarmy;

9) system sygnalizacji pożarowej obejmujący urządzenia sygnalizacyjno-alarmowe, służące do samoczynnego wykrywania i przekazywania informacji o pożarze, a także urządzenia odbiorcze alarmów pożarowych i urządzenia odbiorcze sygnałów uszkodzeniowych, przy czym obiekty wyposażone w stałe urządzenia gaśnicze i objęte całodobowym nadzorem co najmniej jednej osoby nie muszą być wyposażone w system sygnalizacji pożarowej.

Zarządców firm branży S&S zainteresować powinny także dyspozycje §3 cytowanego rozporządzenia. Stanowi on bowiem, że podmioty i struktury, o których mowa wyżej, realizujące inne obowiązki, niż wymienione w przypisie 5, zobowiązane są: *wprowadzić zabezpieczenia adekwatne do [wartości lub znaczenia dla podmiotu] przetwarzanych informacji na podstawie przeprowadzonego szacowanego ryzyka, a także z wykorzystaniem dobrych praktyk.*

CYTOWANE PRZEPISY STANOWIĄ TYLKO CZĘŚĆ WYMAGAŃ, KTÓRE SĄ NIEZBĘDNE DO SPEŁNIENIA PRZEZ DANY PODMIOT, BY MIAŁ ON SZANSĘ NA UZYSKANIE STATUSU OPERATORA USŁUGI KRYTYCZNEJ LUB DOSTAWCY USŁUGI CYFROWEJ

Celem tych działań ma być m.in. skuteczne:
1) monitorowanie i wykrywanie incydentów bezpieczeństwa informacji;
2) reagowanie na incydenty bezpieczeństwa;
3) zapobieganie incydentom bezpieczeństwa informacji;
4) zarządzanie jakością zabezpieczeń systemów, informacji i powierzonych aktywów;
5) aktualizowanie [oceny] ryzyk w przypadku zmiany struktury organizacyjnej, procesów i technologii, które mogą wpływać na reakcję na incydent.

Cytowane przepisy stanowią tylko część wymagań organizacyjno-prawnych i technicznych, które są niezbędne do spełnienia przez dany podmiot, by miał on szansę na uzyskanie statusu operatora usługi krytycznej lub dostawcy usługi cyfrowej. Zarządcy podmiotów ubiegających się o taki status powinni o tym wiedzieć.
Natomiast kierownictwo podmiotów, które w § 5 rozporządzenia określono jako świadczące usługi z zakresu cyberbezpieczeństwa oraz wewnętrzne struktury organizacyjne operatorów usług kluczowych odpowiedzialne za cyberbezpieczeństwo zobowiązano do dostosowania pomieszczenia lub zespołu pomieszczeń, w którym/których te usługi są świadczone, do wymogów określonych w przepisach przywołanego w tym tekście rozporządzenia, w terminie do 6 miesięcy od dnia jego wejścia w życie. Termin ten minął w lipcu 2020 r.

MAREK RYSZKOWSKI

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

6) Nie wątpię, że kierownictwu firm z branży S&S są doskonale znane przepisy norm i aktów prawnych przywołanych w tekście cytowanego wyżej artykułu ustawy o Krajowym Systemie Cyberbezpieczeństwa, zatem nie uważam za potrzebne omawianie ich w tym artykule. Przepisy te dotyczą bowiem dobrze znanych zasad dobierania środków budowlano-mechanicznych, elektronicznych i ochrony czynnej (liczby, organizacji i wyszkolenia personelu bezpieczeństwa) do globalnych i lokalnych zagrożeń cennych aktywów niematerialnych (intelektualnych) i materialnych podmiotów, które takie aktywa posiadają. Zwłaszcza takich aktywów, których utrata może grozić bankructwem lub zachwianiem rynkowej pozycji danego podmiotu albo narazić jego management na konsekwencje prawne z powodu niezapewnienia należytej ochrony takim aktywom.

Cybersecurity

E2E w systemach KD i innych

Piotr Oleksiewicz

Pojęcie End to End (E2E) Security ma swój rodowód w systemach teleinformatycznych i dotyczy bezpieczeństwa wymiany informacji cyfrowej na różnych warstwach interakcji między człowiekiem a systemem oraz między podsystemami/elementami systemu.

Komunikacja szyfrowana jest domeną nie tylko połączeń TCP/IP. W systemach zabezpieczeń stosuje się połączenia zarówno kablowe, jak i bezprzewodowe (radiowe), którymi wymieniane są istotne z punktu widzenia bezpieczeństwa dane. Niestety nie zawsze są to połączenia szyfrowane. Na etapie projektowania czy wyboru rozwiązania warto dokonać analizy, pomiędzy którymi elementami systemu zabezpieczeń będzie zachodzić wymiana informacji. W systemach SSWiN np. najbardziej pierwotnym sposobem zabezpieczenia komunikacji między centralami/rozszerzeniami a elementami peryferyjnymi jest parametryzacja linii, informująca o tym, czy sam element bądź okablowanie nie zostało zmienione, by dostarczać fałszywe sygnały lub, częściej, nie informować o naruszeniu.

W systemach kontroli dostępu, oprócz transmisji informacji z elementów peryferyjnych, jest wiele innych transmisji danych, które są podatne na cyberataki i muszą być zabezpieczone.

1. komunikacja między kartą a czytnikiem,
2. komunikacja między czytnikiem a kontrolerem,
3. komunikacja między kontrolerem a ekspanderem,
4. komunikacja między kontrolerem a jednostką zarządzającą,
5. komunikacja między jednostką zarządzającą a stacjami operatorskimi,
6. komunikacja między stacją operatorską a jej urządzeniami.

To tylko część elementów wymagających zabezpieczenia. System zabezpieczeń jest zazwyczaj aplikacją, do której loguje się operator, i już sam ten proces można łatwo i skutecznie zaatakować. Aplikacje coraz częściej oferują możliwość zastosowania standardów logowania wieloskładnikowego, co w połączeniu z możliwością wymuszenia na operatorach polityki częstych zmian złożonych haseł pozwala uznać warstwę aplikacji za relatywnie bezpieczną.
Wróćmy jednak do systemów kontroli dostępu. Każdy użytkownik systemu KD posiada kartę lub inny nośnik informacji, który go identyfikuje w systemie. Karta jest najbardziej podatnym na manipulację elementem systemu, głównie dlatego, że zgubiona lub skradziona może zostać użyta przez osobę, która nie jest jej właścicielem. Tutaj z odsieczą przychodzą mechanizmy weryfikacji wspierające identyfikację – np. informacja zapamiętana (PIN) lub trudniejsze do kradzieży dane biometryczne, które potwierdzą tożsamość posiadacza karty.
Kradzież karty należy niezwłocznie zgłosić, by skrócić do minimum okres, w którym może zostać użyta przez niepowołaną osobę. Co jednak w sytuacji, gdy zostanie skradziona nie fizyczna karta, a jedynie informacje na niej zawarte? Dużo można opowiadać o używaniu do identyfikacji seryjnych numerów kart, słabościach metod szyfrowania informacji na kartach czy technologiach kartowych, które łatwo skopiować (np. urządzeniem dostępnym na portalach aukcyjnych już od kilkudziesięciu złotych).
Ograniczę się do stwierdzenia, że karta stosowana w naszym systemie KD powinna być dobrze zabezpieczona – technologia kartowa używana w naszym systemie KD powinna być nieskompromitowana oraz powinna wykorzystywać mechanizm szyfrowania asymetrycznego przy wymianie informacji między czytnikiem a nośnikiem informacji identyfikującej. Warto też pomyśleć o bezpieczeństwie warstwy fizycznej E2E i rozważyć, np. czy na karcie powinno się drukować informacje mogące nakierować jej „znalazcę" do odpowiednich drzwi. Może należałoby pozostać przy zdjęciu i numerze identyfikacyjnym, jeśli w ogóle nadruk jest konieczny?

Innym elementem, w aspekcie bezpieczeństwa kart oraz czytników KD, jest ich podatność na popularne ataki typu „relay" (przekaźnik). Gdy już uda się nam bezpiecznie dostarczyć informację do czytnika KD, ten musi w bezpieczny sposób przekazać ją do kontrolera. Większość czytników kontroli dostępu komunikuje się z kontrolerem za pomocą protokołu komunikacyjnego Wiegand – „wiecznie żywego", a przecież archaicznego sposobu przezroczystej wymiany informacji w formie impulsów o określonej amplitudzie i częstotliwości. Łatwej do podsłuchu i replikacji. Wychodząc naprzeciw potrzebie szyfrowania tego kanału komunikacji, we współczesnych systemach stosuje się czytniki komunikujące się po szyfrowanym protokole RS485, niekiedy przybierającym formę otwartych standardów (np. OSDP v2).
Niektórzy producenci idą o krok dalej i stosują klucze odczytu kart w taki sposób, by przechowywane były po zabezpieczonej stronie – na kontrolerze. Dzięki temu sam czytnik, który znajduje się po niechronionej stronie, jest mniej podatny na ataki, np. metodami wstecznej inżynierii. W którym momencie zaczyna się E2E w aspekcie bezpieczeństwa w przypadku czytników, pozostawiam Państwa ocenie.

Kontroler/centrala/kamera to najczęściej komputer z systemem operacyjnym i ma wszystkie te same podatności co system na nich pracujący. Najważniejszą rzeczą, o której należy wspomnieć w aspekcie bezpieczeństwa urządzeń, jest konieczność zmiany domyślnych haseł producenta. Jeśli pozostaną domyślne, może to spowodować, że do urządzenia będą mogły uzyskać dostęp osoby nieupoważnione. Istnieją metody autoryzacji poszczególnych urządzeń („namaszczenia" do pracy w danej instalacji), które, abstrahując od zarządzania hasłami, uniemożliwiają ich fizyczną podmianę. Kontroler wymienia dane z jednostką centralną – najczęściej z serwerem aplikacyjnym. Komunikacja ta zazwyczaj

jest realizowana po sieci TCP/IP i może być zabezpieczona zgodnie ze standardami szyfrowania TLS. Nieszyfrowana komunikacja może być podsłuchana i przechwycona. Same certyfikaty często są dostarczane przez producenta oprogramowania do zabezpieczeń i są domyślne. Aby zabezpieczyć się na tym odcinku, należy użyć własnych certyfikatów.
Podobnie zabezpieczona jest komunikacja serwera ze stacjami operatorskimi. Jednak powszechna zielona kłódka w oknie przeglądarki może dawać jedynie złudzenie bezpiecznej komunikacji, jeśli pozostaniemy przy domyślnych certyfikatach aplikacji. Tylko wymiana ich na prywatne zapewni, że nikt nie podsłucha nas na drogach między kontrolerem/serwerem/stacją operatorską.
Kontrolery rzadko występują jako samodzielne urządzenia. Zazwyczaj są do nich podłączane rozszerzenia, do których można podłączać kolejne i następne drzwi. Połączenie między kontrolerem a rozszerzeniem to najczęściej połączenie RS485 lub CAN. Rozpatrując mechanizm E2E w naszym systemie KD, musimy zastanowić się, czy taka architektura umożliwia szyfrowanie każdego połączenia, również magistralowego.
Gdy, jak sądzimy, zaszyfrujemy już całą drogę komunikacji, to spokojnie zasiadamy do stacji operatorskiej (autoryzowanej na warstwie sieciowej do użycia tylko z tego gniazda przełącznika sieciowego na adresie IP, z którego jedynie operator „Jan Kowalski" może połączyć się z aplikacją KD) oraz wpisujemy swoją nazwę użytkownika i hasło. Nie wiemy natomiast tego, że wieczorem anonimowa osoba z serwisu sprzątającego, posługująca się przepustką KD „serwis sprzątający 2" założyła na naszą klawiaturę podsłuch USB, który przechwycił nasze dane logowania. Następnego dnia okazuje się, że w tajemniczy sposób operator Jan Kowalski po godzinie 22:00 udzielił dostępu z poziomu aplikacji do pomieszczenia „Główna Serwerownia" zakapturzonemu pracownikowi serwisu sprzątającego, posługującego się wcześniej kartą obecną w systemie jako „serwis sprzątający 1"...

Według koncepcji E2E – od początku do końca – w aspekcie bezpieczeństwa mamy wrażenie, że system zrobi za nas wszystko i nie musimy się o nic martwić. Jednak nic nie dzieje się samo i oprócz bezpieczeństwa elektroniki, której zasad można się na bieżąco uczyć (często na błędach) są jeszcze warstwy fizyczna i ludzka, których nie można pomijać. I na jednym, i na drugim końcu E2E Security znajdują się ludzie.

PIOTR BARNABA OLEKSIEWICZ

Od początku zawodowej kariery związany z branżą kontroli dostępu oraz systemów zabezpieczeń. Obecnie w Nedap Security Management.

Strategia bezpieczeństwa w monitoringu wizyjnym

Cyberbezpieczeństwo w inteligentnych miastach

Systemy infrastruktury miejskiej oparte na technologiach IT coraz mocniej się integrują i obejmują coraz więcej nowo podłączanych urządzeń i czujników IoT. W ślad za rozrastającą się nieuchronnie technologią powiększa się pole do ataków hakerskich, a cyberbezpieczeństwo staje się kluczową dziedziną ochrony płynności i sprawności działania zarówno inteligentnych miast, jak i branż wykorzystujących IoT.

Wizja inteligentnego miasta opiera się na połączonym ekosystemie usług, systemów i przedsiębiorstw, w którym ich współpraca pozwala na podnoszenie jakości życia mieszkańców. Korzyści wynikające z digitalizacji i rosnącego poziomu inteligencji organizacji wiążą się obecnie z podwyższonym ryzykiem hakerskim, wpływającym na efektywność stosowanych technologii. Dlatego cyberbezpieczeństwo jest krytyczną funkcją bezpieczeństwa użytkowników i mieszkańców.

IOT A CYBERATAKI

W miarę podłączania kolejnych urządzeń do już funkcjonujących systemów, w tym miejskich, rośnie ryzyko zagrożeń. Tylko w 2019 r. liczba cyberataków na urządzenia IoT wzrosła o 300% r/r i spodziewamy się, że podobnie było także w 2020 r. Przyczyny są jasne. Cyberprzestępcy stale poszukują wrażliwych punktów wejścia do sieci, a podłączane do niej urządzenia – gdy są niezabezpieczone – stanowią punkty dostępu, przez które przestępcy sięgają głębiej.
Odpowiedzialni za fizyczne bezpieczeństwo muszą mieć pewność, że mogą polegać na technologiach obsługujących ich działania operacyjne. Jednocześnie powinni także przestrzegać polityki bezpieczeństwa IT, żeby fizyczne urządzenia nie stały się tylnymi drzwiami wejścia do sieci danej organizacji.

JAK SIĘ BRONIĆ?

Podstawą jest zapewnienie maksymalnego bezpieczeństwa wszystkich urządzeń IoT i punktów końcowych sieci. Nie jest to jednorazowe działanie, lecz stały proces zrozumienia nowych i wykrywania kolejnych, ale też potencjalnych zagrożeń. Wymaga proaktywnej postawy, współpracy całego ekosystemu interesariuszy i planowania bezpieczeństwa systemu przed dołączeniem do niego kolejnych urządzeń – tak, aby istniała możliwość łatania luk i aktualizowania do najnowszych światowych wymagań bezpieczeństwa. Szereg wbudowanych funkcji cyberbezpieczeństwa zawierają rozwiązania sieciowe Axis.

ZABEZPIECZENIA PRZED MANIPULACJAMI

Bezpieczne systemy i urządzenia funkcjonujące w fizycznej i sieciowej tkance miasta czy organizacji powinny dziś mieć wbudowane funkcje do wykrywania manipulacji oprogramowaniem sprzętowym, aby zapobiegać nieautoryzowanej wymianie urządzenia czy dostępowi do jego cyfrowego wnętrza. Dopiero wtedy będą wspierać zarządzających, mieszkańców i użytkowników w redukowaniu ryzyka cyberataku.
Przestępcy mogą próbować oszukać właścicieli systemu, aby zainstalowali zmienione oprogramowanie sprzętowe, które może zawierać złośliwy kod. Zapobiega temu podpisane oprogramowanie sprzętowe. Można zweryfikować integralność oprogramowania sprzętowego przed zainstalowaniem nowych urządzeń lub aktualizacją istniejących.
Oprogramowanie sprzętowe Axis jest oznaczane przy użyciu podpisu cyfrowego. Ten proces opiera się na metodzie szyfrowania RSA, w której klucz publiczny jest osadzony w urządzeniu Axis, natomiast klucz prywatny przechowywany w bezpiecznym miejscu w firmie Axis. Urządzenia z podpisanym oprogramowaniem sprzętowym mogą zweryfikować poprawność oprogramowania przed zezwoleniem na instalację. Gwarantuje to, że oprogramowanie sprzętowe rzeczywiście pochodzi od producenta i nie zostało naruszone.
Istotne jest również regularne aktualizowanie oprogramowania, by uchronić się przed sytuacją, w której hakerzy wbudowują złośliwy kod do nieautoryzowanego oprogramowania, uzyskując tą drogą „wejście" do dowolnych systemów, w których urządzenia mogą funkcjonować.

CERTYFIKATY BEZPIECZEŃSTWA – IDENTYFIKACJA URZĄDZENIA IOT W SIECI

Rozwiązania Axis Communications zbudowane są także zgodnie z najnowszymi standardami, gwarantującymi pewność bezpiecznego komunikowania. Zgodnie z najnowszym międzynarodowym standardem bezpiecznej identyfikacji urządzenia (IEEE 802.1AR) kompatybilne urządzenia Axis automatyzują i zabezpieczają identyfikację urządzenia w sieci. Dodatkowym zabezpieczeniem może być także technologia Axis Edge Vault. Ten element chroni identyfikator urządzenia, zbiór certyfikatów, w tym podpisaną cyfrowo wersję unikatowego w skali globalnej numeru seryjnego sprzętu. Identyfikator urządzenia Axis upraszcza autoryzację produktów w sieci, zapewniając ekonomiczną konfigurację, która oszczędza czas i pieniądze.

SZYFROWANIE – CERTYFIKATY IOT

Rozwiązania Certyfikowanego Magazynu Kluczy zapewniają bezpieczeństwo kluczy kryptograficznych i certyfikatów – przykładem może być stosowany w rozwiązaniach Axis komponent Trusted Platform Module (TPM). Takie wbudowane, fizyczne elementy urządzeń zabezpieczają klucze kryptograficzne i certyfikaty wykorzystywane w komunikowaniu, nawet w przypadku gdy dojdzie już do ataku. Moduł TPM w produktach Axis ma certyfikat zgodności z certyfikatem FIPS 140-2 na poziomie 2 i obejmuje uwierzytelnianie operatora oparte na pełnionej funkcji i dowodach ataku.

SECURE BOOT

Niezwykle istotną funkcją bezpiecznych urządzeń może się też okazać – powiązana z autorskim, wbudowanym oprogramowaniem – funkcja bezpiecznego ponownego uruchamiania *(secure boot)* w dowolnym przypadku przerwania pracy. Wbudowana w rozwiązania Axis zapewnia, że gdy dojdzie do próby ataku, nieuwierzytelniony naruszony kod jest blokowany i odrzucany podczas procesu uruchamiania, zanim będzie mógł zaatakować lub zainfekować cały system. Dla przykładu – kamery monitoringu odpowiadające za dozór terenu miasta powinny bezpiecznie uruchamiać się ponownie po próbie ich zhakowania. Zapewni to ciągłość funkcjonowania całego zorganizowanego systemu, do którego celów system monitoringu został zainstalowany i przygotowany po stronie IT.

Wybór urządzeń spełniających kolejne funkcje w zastosowaniach *smart city* staje się wymagający – królujące dotychczas kryterium ceny i nieśmiało wprowadzane praktyczne testy sprawdzające deklarowane parametry już nie wystarczą. Włodarze i odpowiedzialni za bezpieczeństwo powinni priorytetowo brać pod uwagę kwestie cyberbezpieczeństwa. Nawet najwyższej jakości urządzenie IoT może być bowiem niewystarczająco zabezpieczone przed atakami hakerskimi. Ryzyko utraty bezpieczeństwa funkcji pełnionych przez wprowadzane dla podnoszenia inteligencji organizacji IoT znacznie przewyższa już dziś koszty napraw czy wymian urządzeń. Warto mieć to na względzie, decydując się na wybór systemu.

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

Skuteczność potwierdzona

Telbud z pozytywnym wynikiem audytu

W lutym 2021 r. w firmie Telbud S.A. został przeprowadzony audyt nadzoru systemu zarządzania bezpieczeństwem informacji wg ISO 27001:2017. Jednostką audytującą było Centrum Certyfikacji Jakości. Audytor nie stwierdził żadnych niezgodności i potwierdził skuteczność działania systemu.

ISO/IEC 27001 to międzynarodowa norma, która standaryzuje systemy zarządzania bezpieczeństwem informacji. Celem jej opracowania było dostarczenie wymagań dotyczących ustanawiania, wdrażania, utrzymania i doskonalenia systemu zarządzania bezpieczeństwem informacji. W Polsce weszła w życie 4 stycznia 2007 r. jako PN-ISO/IEC 27001:2007. Aktualna norma PN-ISO/IEC 27001:2017-06 odnosi się m.in. do polityki bezpieczeństwa, organizacji bezpieczeństwa informacji, bezpieczeństwa zasobów ludzkich, zarządzania systemami i sieciami, kontroli dostępu, zarządzania ciągłością działania czy bezpieczeństwa fizycznego i środowiskowego.
Bezpieczeństwo posiadanych informacji dotyczy ochrony przetwarzanych danych (m.in. handlowych, osobowych, technicznych, rozwojowych, finansowych) w systemach zarówno informatycznych, jak i tradycyjnych z wykorzystaniem papieru. Ważnymi korzyściami wynikającymi z wdrożenia ISO 27001 są m.in.:

- poufność, integralność i dostępność informacji przetwarzanych przez organizację,
- monitoring przetwarzania informacji,
- poprawa zarządzania czynnikami ryzyka (identyfikacja zagrożeń i zmniejszenie ich skutków),
- wzrost zaufania klientów,
- nadzór nad spełnianiem wymagań prawnych dot. przedsiębiorstwa,
- zwiększenie świadomości pracowników,
- wyższa jakość wykonywanych usług.

Pozytywny wynik audytu potwierdził, że Telbud S.A. zapewnia właściwą poufność, integralność i dostępność informacji na każdym etapie procesów projektowania, wykonawstwa i serwisu oraz we wszystkich procesach towarzyszących.

Więcej na www.telbud.pl

AI oraz mechanizmy deep learning

w nowej kamerze Axis

Firma Axis Communications zaprezentowała nową kamerę P3255-LVE, która dokonuje analiz zawartości obrazu, wykorzystując sztuczną inteligencję i mechanizmy głębokiego uczenia. Ta stałopozycyjna kamera kopułkowa zawiera innowacyjny podwójny chipset, który umożliwia niezwykle szczegółową klasyfikację obiektów.

Kluczem do funkcji klasyfikacji obiektów jest chipset, łączący procesor Axis ARTPEC-7 oraz procesor głębokiego uczenia. Tak zaawansowane elementy sprzętowe dają użytkownikom możliwość korzystania ze specjalnie opracowanych aplikacji zewnętrznych opartych na funkcjach AI. Fabrycznie zainstalowana aplikacja analityczna AXIS Object Detector wykrywa i klasyfikuje osoby i obiekty/pojazdy, rozróżniając przy tym samochody osobowe, autobusy, samochody ciężarowe oraz jednoślady (motocykle i rowery).
Kamera z podwójnym chipsetem dokonuje analiz bezpośrednio w urządzeniu, co zwiększa szybkość działania i skalowalność systemu. Przetwarzanie w czasie rzeczywistym redukuje koszty i obniża złożoność systemu. Przez sieć przesyłany jest tylko niezbędny materiał wizyjny, co ogranicza zapotrzebowanie na pamięć masową i przepustowość oraz zmniejsza obawy dotyczące prywatności.
Ta gotowa do montażu, zewnętrzna kamera o rozdzielczości HDTV 1080p w odpornej obudowie (IK10) zawiera szereg funkcji bezpieczeństwa zapobiegających nieautoryzowanemu dostępowi.

Więcej na www.axis.com/pl

Współpraca RACS 5

z systemami SMS/PSIM/ VMS/BMS

Moduł Map systemu kontroli dostępu i automatyki budynkowej RACS 5 firmy Roger umożliwia wizualizację i nadzorowanie pracy systemu w trybie graficznym. Wizualizacja obejmuje system KD i zintegrowane z nim systemy CCTV (Dahua, Hikvision, BCS, ONVIF) oraz SSWiN (INTEGRA, Galaxy). W niedalekiej przyszłości moduł Map zostanie poszerzony o wizualizację systemów sygnalizacji pożarowej.

W obiektach wymagających szerszego zakresu integracji RACS 5 oferuje możliwość współpracy ze zintegrowanymi systemami zarządzania bezpieczeństwem (SMS i PSIM), systemami zarządzania wideo (VMS) oraz systemami zarządzania budynkiem (BMS).
W ramach zrealizowanych projektów wdrożono współpracę m.in. z systemami: WinGuard (Advancis), Axxon Intellect Enterprise (AxxonSoft), XProtect (Milestone Systems), ARGUS RV (Telbud), NetStation Enterprise (ALNET SYSTEMS), GANZ Cortrol (CBC Group), Luxriot EVO (Luxriot), Nazca (APA Group).
Integracje te zrealizowano za pośrednictwem tzw. serwera integracji, który umożliwia dostęp do bazy danych systemu i wykonywanie czynności związanych z bieżącą jego obsługą, m.in. zarządzanie użytkownikami oraz wydawanie zdalnych poleceń. Wykorzystanie serwera integracji umożliwia współpracę systemu KD z dowolnym zewnętrznym systemem informatycznym (np. system ERP, system zarządzania budynkiem itp.).

Więcej na www.roger.pl

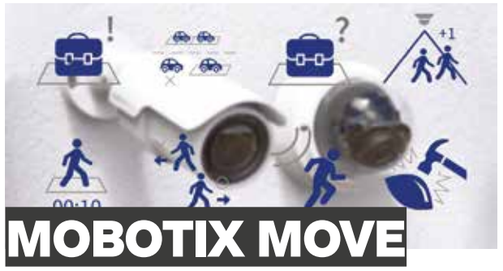
Nowa kamera Wisenet 5 Mpix

do montażu narożnego

Nowa kamera Wisenet TNV-8010C została skonstruowana tak, aby uniemożliwić akty wandalizmu. Zasadniczo jest produkowana z myślą o instalacji w zakładach karnych i instytucjach zdrowia psychicznego w celu zapobiegania samookaleczaniu się osadzonych i pacjentów.

Opływowa, wandaloodporna i wodoodporna konstrukcja (IP66, IP6K9K i IK10+) pozwoli na jej wykorzystanie również w kioskach bankomatowych czy windach. Obrazy o rozdzielczości 5 Mpix w proporcjach 3:4 i o rozdzielczości 2 Mpix w proporcjach 9:16, czyli w formatach korytarzowych, są przydatne do obserwacji wąskich i wysokich przestrzeni.
Kamera TNV-8010C pracuje w trybie dzień/noc i odznacza się wysoką czułością. Dostarcza kolorowe obrazy, gdy poziom oświetlenia przekroczy zaledwie 0,1 lx. Ma funkcję rozszerzania zakresu dynamiki do 120 dB, dzięki temu pozwala na wyraźne odwzorowanie szczegółów obrazu w partiach bardzo jasnych i bardzo ciemnych.
Zasilanie PoE eliminuje potrzebę instalowania zasilacza i oddzielnego okablowania zasilającego.
Zestaw wbudowanych inteligentnych funkcji analitycznych (IVA) obejmuje: wykrywanie braku ostrości oraz zmiany pola widzenia, wykrywanie ruchu, w tym wejścia/wyjścia z wyznaczonego obszaru, przekroczenie wirtualnej linii, analizę dźwięku, a także wykrywanie prób oderwania kamery od podłoża.

Więcej na www.hanwha-security.eu



MOBOTIX MOVE

kamery z wbudowaną analizą obrazu

Portfolio MOBOTIX MOVE poszerza się o nowe kamery z rozdzielczością obrazu 2 Mpix lub 5 Mpix, obiektywem o zmiennej ogniskowej oraz klasą odporności IK 10.

Po raz pierwszy zaawansowane algorytmy przetwarzania obrazu do inteligentnej analizy wideo są dostępne bezpośrednio w oprogramowaniu kamer bez dodatkowych opłat.
Jednym z narzędzi analizy obrazu jest wykrycie pozostawionych lub usuniętych przedmiotów w strefie zdefiniowanej przez użytkownika. Kamery mogą też wykrywać i śledzić intruza w określonym obszarze. Aplikacje mogą pracować zarówno wewnątrz, jak i na zewnątrz obiektu.
Algorytmy dostosowują się do zmian monitorowanego środowiska (śnieg, deszcz, mgła). Każda próba sabotażu przez zakrycie lub zamalowanie obiektywu natychmiast uruchomi alarm. System wyzwala też ostrzeżenie, gdy osoba lub obiekt porusza się w przeciwnym do dozwolonego kierunku. Identyfikuje osoby lub pojazdy, które pozostają w określonej strefie dłużej niż zdefiniowany przez użytkownika czas.
Kamera wysyła powiadomienia o podejrzanych incydentach w czasie rzeczywistym. Zlicza obiekty wchodzące do strefy zdefiniowanej przez użytkownika.
Wszystkie nowe kamery z serii MOBOTIX MOVE zawierają bezpłatną analitykę bez dodatkowych kosztów licencji, warto ją przetestować!

Więcej na www.linc.pl

Eagle Eye Networks

monitoring wizyjny w chmurze

Organizacje coraz częściej chcą wykorzystywać kamery do wspierania procesów biznesowych, zbierania informacji statystycznych, kontroli swoich obiektów i weryfikacji standardów firmowych.

Pełna obsługa kamer analogowych i IP, ciągła analiza obrazów, podgląd wielu lokalizacji i historii nagrań czy zdalny dostęp przez przeglądarkę internetową to tylko niektóre korzyści z zastosowania platformy do nadzoru opartej na chmurze firmy Eagle Eye Networks.
Przerwy i ograniczenia w dostępie do Internetu nie stanowią problemu. Urządzenia sieciowe Eagle Eye przy braku połączenia buforują lokalnie nagrania i nadzorują status kamer. Odpowiadają też za automatyzację konfiguracji kamer i szyfrowanie połączeń z chmurą. Wielowarstwowa technologia zarządzania pasmem umożliwia aktualizację danych w momentach małego obciążenia sieci, np. w nocy. Dzięki temu system współpracuje zarówno z małymi, jak i dużymi instalacjami kamer.
Właściciele starych systemów CCTV/VSS mogą w prosty sposób korzystać z funkcjonalności chmury. Dodanie urządzeń sieciowych Eagle Eye do istniejących systemów umożliwia bezpieczny podgląd oraz kopię zapasową w chmurze. Rozbudowa systemu jest łatwa i może postępować wraz ze zmianą oczekiwań klienta, czyli przejdźmy na chmurę!

Więcej na www.smart-i.pl

Profesjonalny bezprzewodowy system bezpieczeństwa

Wykrywanie włamania

Bezpieczeństwo przeciwpożarowe

Zapobieganie zalaniu

Automatyka domu

Weryfikacja fotograficzna alarmów

Miłego oglądania

Darmowe aplikacje dla instalatorów i użytkowników końcowych

www.ajax.systems

macOS | Windows | iOS | Android