CZASOPISMO RYNKU SECURITY

ASPOLSKA

04 (34) 07/08 2022

Czas na zmiany?

BEZPIECZEŃSTWO BIZNESU

USTAWA O OBRONIE OJCZYZNY

Obowiązująca od kwietnia ustawa liczy 824 artykuły ujęte w 26 działach – w sumie aż 248 stron! Wiele przepisów ma ogromny wpływ na prowadzenie biznesu w branży safety i security. Kontynuujemy omawianie najistotniejszych z nich.

NOWA RZECZYWISTOŚĆ

PRZYKAZANIA WSPÓŁCZESNEGO „BEZPIECZNIKA”

Organizacje stawiają dziś przed działami bezpieczeństwa inne oczekiwania, co zmusza menedżerów do zmiany strategii, by sprostać współczesnym wyzwaniom. Jak przygotować się na przyszłe (nieznane jeszcze) scenariusze?

RYNEK SECURITY

JAK DZIAŁA SZTUCZNA INTELIGENCJA

Nadchodzi kolejny etap ewolucji systemów zabezpieczeń zasilanych przez AI. Korzystanie z narzędzi analitycznych operujących na *Big Data* umożliwia przekształcanie „gór danych” w użyteczne informacje.

APLIKACJA MOBILNA

www.aspolska.pl

ISSN 2451-5175

9 772451 517703 05

15 zł (w tym 8% VAT)

EDYTORIAL

Drodzy Czytelnicy

Możliwy nawrót pandemii, wojna w Ukrainie, wzmożona dezinformacja i infiltracja, ataki hakerskie i wyrafinowane techniki manipulacji skutkujące utratą danych i stratami finansowymi... Jak radzić sobie z zagrożeniami, zwłaszcza tymi nowymi? Zdolność do przygotowania się na przyszłe scenariusze zdarzeń jest tym, czego dziś oczekuje się od komórek bezpieczeństwa.

Publikujemy „dekalog współczesnego bezpiecznika", by każda osoba odpowiedzialna za tworzenie strategii bezpieczeństwa nie tylko mogła sprostać dzisiejszym wyzwaniom, ale dała się poznać jako profesjonalny partner, z którego głosem warto się liczyć (s. 22).

Nowe zagrożenia są groźne szczególnie dla organizacji działających w obszarze usług finansowych. Zwłaszcza banki i ich klienci są poddawani ciągłej presji różnego rodzaju transformacji. To efekt zmian na rynku, nowych regulacji, a przede wszystkim nowych zachowań konsumentów. Jednym z głównych czynników wspierających i umożliwiających głęboką transformację organizacji jest adaptacja technologiczna i chmurowa (s. 26 oraz 38).

Mocno dotknięty ostatnimi wydarzeniamijest rynek hotelarski (s. 34). By sprostać obecnym wyzwaniom hotelarze podnieśli poziom bezpieczeństwa świadczonych usług, szczególnie w obszarach związanych z realizacją procedur i wyposażenia obiektów w dodatkowy sprzęt. Kładą także większy nacisk na ochronę gości przed cyberatakami i zagrożeniami informacyjnymi.

Sztuczna inteligencja rewolucjonizuje obszar bezpieczeństwa fizycznego. Technologie AI – oparte na uczeniu maszynowym i sieciach neuronowych – wspomagają pracę operatorów, działając predykcyjnie. Polecamy szczególnej uwadze dwa artykuły w tym zakresie – jeden systematyzujący tematykę sztucznej inteligencji (uczenie maszynowe i głębokie uczenie), drugi odnoszący się do możliwości wykorzystania analityki big data w biznesie (s. 42 oraz 44).

W tym wydaniu kontynuujemy przegląd istotnych dla branży postanowień Ustawy o obronie Ojczyzny. Lektura obu części artykułu powinna skłonić branżowych przedsiębiorców i zatrudnianych przez nich prawników do uważnej obserwacji rozwoju legislacji – jest to niewątpliwie jest w interesie całego rynku bezpieczeństwa (s. 70).

***

Po pandemicznej przerwie gościliśmy szefów bezpieczeństwa i security menedżerów na kolejnej edycji konferencji Warsaw Security Summit. W Centrum Praskim KONESER w Warszawie spotkało się 6 czerwca blisko 600 osób związanych profesjonalnie z branżą safety i security (s. 16). Relacja oraz zapis całej konferencji jest dostępny na profilu a&s Polska na YouTubie

Sukcesem było też trzecie szkolenie dla security menedżerów – Security BootCamp. W warunkach terenowych uczestnicy rozwiązywali wyzwania przygotowane przez Partnerów technologicznych (s. 76). Ogromne zainteresowanie ze strony uczestników sprawiło, że na jesieni zorganizujemy kolejną edycję wydarzenia.

Marta Dynakowska
REDAKTOR NACZELNA

Jan T. Grusznic
Z-CA REDAKTORA NACZELNEGO

Mariusz Kucharski
PREZES ZARZĄDU

A&S POLSKA REDAKCJA

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

Prezes Zarządu
Mariusz Kucharski

Redaktor naczelna
Marta Dynakowska

Z-ca redaktora naczelnego
Jan T. Grusznic

Dział reklamy i marketingu
Iwona Krawiec

Dział projektów specjalnych
Jolanta A. Kucharska
Aleksandra Czapska
Michalina Nowak

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

Korekta
Jolanta Kucharska

Projekt graficzny i skład
Kalwala Studio

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

Prenumerata
www.aspolska.pl/prenumerata

a&S POLSKA

04

34

07/08

2022

SPIS TREŚCI

HOTELE I INSTYTUCJE FINANSOWE

SPIS TREŚCI

RYNEK SECURITY

BEZPIECZEŃSTWO POŻAROWE

BEZPIECZEŃSTWO BIZNESU

SERWIS INFORMACYJNY

AXIS COMMUNICATIONS

www.axis.com/pl

Cztery nowe kamery typu box od Axis Communications

AXIS M11 TO PRZYSTĘPNA CENOWO, ŁATWA W UŻYTKOWANIU SERIA KAMER DO ZAAWANSOWANEGO MONITORINGU WIZYJNEGO WYPOSAŻONYCH W NAJNOWSZE TECHNOLOGIE. OFERUJĄ DOSKONAŁĄ JAKOŚĆ OBRAZU I OBSŁUGĘ STANDARDU POE, WYBRANE MODELE MOŻNA MONTOWAĆ TAKŻE NA ZEWNĄTRZ.

W skład AXIS M11 Camera Series wchodzą cztery urządzenia typu box. AXIS M1135 Mk II i AXIS M1135-E Mk II oferują rozdzielczość 2 Mpix, natomiast modele przeznaczone do użytku zewnętrznego AXIS M1137 Mk II i AXIS M1137-E Mk II Box Camera – rozdzielczość 5 Mpix. Kamery zapewniają niezakłóconą jakość obrazu w każdych warunkach atmosferycznych, a mocowanie CS z obsługą obiektywów i-CS umożliwia zdalne ustawianie zoomu. Wszystkie modele mają wbudowany mikrofon pozwalający na detekcję dźwięków na określonym obszarze.
Urządzenia wyposażono w najnowsze technologie Axis: Axis Lightfinder Axis Forensic WDR, co pozwala na wierne odwzorowywanie barw i szczegółów przy słabym oświetleniu lub niemal w ciemności. Z kolei dzięki technologii Axis Zipstream kamery mają zmniejszone zapotrzebowanie na przepustowość, a Axis Object Analitycs umożliwia prowadzenie zaawansowanej analityki wideo na brzegu sieci.
Kamery serii M11 mają stały kąt widzenia, są dobrze widoczne w przestrzeni, więc można łatwo stwierdzić, na jaki obszar są skierowane. Ponadto dzięki obudowie o klasie ochrony IP66, odporności mechanicznej IK10 i NEMA 4X modele przystosowane do zastosowań zewnętrznych są wodo- i pyłoszczelne oraz odporne na uderzenia.

BCS

www.bcscctv.pl

BCS-NVR3204-P-4K-AI

DO TEJ PORY, ŻEBY MOŻNA BYŁO KORZYSTAĆ Z FUNKCJI ZAAWANSOWANEJ ANALIZY OBRAZU W SYSTEMACH IP, TRZEBA BYŁO PRECYZYJNIE DOBRAĆ KAMERY, ABY DOPASOWAĆ JE DO WYMAGAŃ KLIENTA. I TAK W PRZYPADKU BARDZIEJ WYMAGAJĄCYCH ROZWIĄZAŃ JEDNA KAMERA BYŁA ODPOWIEDZIALNA ZA IDENTYFIKACJĘ TABLIC REJESTRACYJNYCH, INNA ZA ROZPOZNAWANIE I PORÓWNYWANIE TWARZY, KOLEJNA ZA LICZENIE OSÓB WCHODZĄCYCH DO OBIEKTU I WYCHODZĄCYCH Z NIEGO, A JESZCZE INNA ZA OCHRONĘ OBWODOWĄ.

Z pomocą przychodzą rejestratory AI serii BCS Line. Mają one zaimplementowaną w oprogramowaniu systemowym obsługę funkcji zaawansowanej analizy obrazu. Na 16 kanałach rejestrator może obsługiwać funkcje związane z ochroną obwodową, np. przekroczenie linii czy wtargnięcie w strefę, przy czym można dodatkowo wybrać typ obiektu uruchamiającego alarm.
Natomiast na 4 kanałach potrafi pokazać pełnię swoich możliwości, oferując dostęp do takich funkcji, jak rozpoznawanie i identyfikacja twarzy czy gromadzenie metadanych, w których skład wchodzi rozpoznawanie obiektów i informacji o nich.
Rejestrator zbiera metadane z otrzymanego obrazu, dzięki czemu wyszukiwanie odpowiednich zdarzeń staje się wyjątkowo łatwe i skuteczne. Nie ma już potrzeby przeglądania godzin nagrań. Wystarczy określić dodatkowe parametry nagrania, by po chwili mieć do niego dostęp. Kryteriami wyszukiwania mogą być m.in. przedział wiekowy, płeć, kolor i typ ubrania w przypadku ludzi czy numer tablicy rejestracyjnej, kolor, marka dla samochodów.

CC PARTNERS

www.ccpartners.pl

Nowoczesna platforma parkingowa w biurowcach

W OPARCIU O WIELOLETNIE DOŚWIADCZENIE INTEGRACYJNE POWSTAŁO NOWOCZESNE ROZWIĄZANIE BĘDĄCE ODPOWIEDZIĄ NA STALE ROSNĄCE ZAPOTRZEBOWANIE NA MIEJSCA PARKINGOWE. AUTONOMICZNY SYSTEM ZARZĄDZANIA PARKINGIEM DOSKONALE SPRAWDZI SIĘ NIE TYLKO W BIUROWCACH, ALE TAKŻE ZNAJDZIE SWOJE ZASTOSOWANIE NA PARKINGACH FIRMOWYCH CZY SPÓŁDZIELNI MIESZKANIOWYCH.

System przydziela dostęp do parkingu na podstawie analizy tablic rejestracyjnych CarR VDG Sense oraz integracji z czytnikami systemu kontroli dostępu iProtect . Rozwiązanie umożliwia podział odpowiedniej liczby miejsc parkingowych pomiędzy wiele firm.
System może być zintegrowany z pylonem wskazującym aktualną liczbę miejsc oraz wyświetlającym inne komunikaty, np. „Brak miejsca dla Twojej firmy" lub cykliczne informacje dotyczące m.in. promocji.
Rozwiązanie zapewnia dynamiczną zmianę liczby miejsc w panelu administracyjnym oraz wizualizację miejsc przydzielonych danym firmom w interfejsie operatora. System działa autonomicznie, natomiast w przypadku firm z rozproszonymi oddziałami, możliwe jest centralne zarządzanie wieloma parkingami. Pomaga zoptymalizować, usprawnić i obniżyć koszty pracy.

HANWHA TECHWIN

www.hanwha-security.eu/pl/

Nowe kamery Wisenet z serii X z wbudowanymi funkcjami AI

NOWA LINIA PRODUKTÓW, W KTÓREJ SKŁAD WCHODZI 28 MODELI KAMER, OFERUJE FUNKCJE PRZYDATNE DLA OPERATORÓW WIZYJNYCH SYSTEMÓW DOZOROWYCH OPARTE NA SZTUCZNEJ INTELIGENCJI I GŁĘBOKIM UCZENIU MASZYNOWYM. ZMNIEJSZAJĄ ONE LICZBĘ FAŁSZYWYCH ALARMÓW I USPRAWNIAJĄ PRACĘ TYCH SYSTEMÓW.

Realizacja inteligentnych funkcji analitycznych w urządzeniach brzegowych pozwala na skuteczniejsze niż dotychczas wykrywanie i rozpoznawanie obiektów, takich jak ludzie i pojazdy. Umożliwia to operatorom systemów dozorowych szybką identyfikację osób i pojazdów, co przekłada się na lepsze rozeznanie w sytuacji z uwzględnieniem kontekstu zachodzących wydarzeń. Nieistotne ruchome elementy tła, takie jak gałęzie drzew, poruszające się cienie czy przebiegające zwierzęta, są ignorowane. Operatorzy systemów dozorowych mogą skoncentrować się na przebiegu rzeczywistych incydentów i sytuacji awaryjnych. Zaawansowana detekcja ruchu dzięki możliwości rozpoznawania ludzi i pojazdów zmniejsza liczbę fałszywych alarmów, a przeszukiwanie nagrań jest dużo łatwiejsze i szybsze.
Analiza treści obrazów wsparta sztuczną inteligencją służy nie tylko bezpieczeństwu. Dostarcza również wielu danych przydatnych dla działów marketingu i sprzedaży. Dzięki algorytmom AI firmy mogą np. dokładnie zliczać klientów, pozyskiwać dane ułatwiające zarządzanie kolejkami czy tworzyć mapy cieplne szczegółowo dokumentujące wzorce zachowań klientów.
Nowe kamery mają wandaloodporne metalowe obudowy kopułowe, tubowe lub kompaktowe typu box. Urządzenia mogą być zasilane prądem stałym o napięciu 12 V lub metodą PoE przez sieć Ethernet. Pozwala to na redundantne zasilanie kamer z różnych źródeł w przypadku awarii podstawowej instalacji zasilającej.

HIKVISION

www.hikvision.com/pl

Kamery panoramiczne z ColorVu

DUŻE OBSZARY MOGĄ BYĆ BARDZO TRUDNE DO ZABEZPIECZENIA. CZĘSTO, ABY ZAPEWNIĆ PEŁNE POKRYCIE ZASIĘGIEM, TRZEBA ZASTOSOWAĆ WIELE KAMER. W PRZYPADKU TRADYCYJNYCH MODELI MONITOROWANIE TEGO TYPU OBSZARÓW MOŻE BYĆ RÓWNIEŻ TRUDNE LUB WRĘCZ NIEMOŻLIWE W WARUNKACH SŁABEGO OŚWIETLENIA LUB W NOCY.

Chcąc sprostać tym wszystkim wyzwaniom, firma Hikvision zintegrowała technologię ColorVu z wiodącymi kamerami panoramicznymi, które wykorzystują technologię fuzji obrazu do połączenia obrazów z dwóch obiektywów stałoogniskowych 4 mm umieszczonych obok siebie. Pozwala to na uzyskanie płynnego, 180-stopniowego widoku w rozdzielczości 8 Mpix.
Rezultatem są zmniejszone wymagania sprzętowe (mniejsza liczba kamer potrzebnych do pokrycia dużych obszarów) oraz lepsza świadomość sytuacyjna oparta na pojedynczym szerokokątnym obrazie bez martwych punktów, a także możliwość uchwycenia każdego szczegółu w pełnym kolorze – nawet w ciemności. Ponadto w kamerach zastosowano technologię WDR 130 dB, zapewniającą wyraźne obrazowanie i kompensację światła tylnego oraz kompresję obrazu H.265+, dzięki której możliwe jest zoptymalizowane kodowanie wideo o wysokiej wydajności.

Dostępne modele: DS-2CD2T87G-2P-LSU/SL – kamera sieciowa typu bullet oraz DS-2CD2387G-2P-LSU/SL – kamera sieciowa typu turret.

NEDAP SECURITY MANAGEMENT

www.nedapsecurity.com/pl/

Nedap AEOS Locker Management

W CZASACH, GDY NOWĄ NORMĄ JEST PRACA HYBRYDOWA, PRACOWNICY, WYKONAWCY I GOŚCIE POTRZEBUJĄ PRZESTRZENI DO PRACY W OGRANICZONYM WYMIARZE. NIE MAJĄC STAŁEGO BIURKA, MUSZĄ MIEĆ BEZPIECZNE MIEJSCE DO PRZECHOWYWANIA SWOICH RZECZY. TO OZNACZA, ŻE SZAFKI STAJĄ SIĘ NIEZBĘDNĄ I CENNĄ INWESTYCJĄ DLA WIELU FIRM.

Zarządzanie szafkami AEOS to inteligentna odpowiedź na te wymagania. Umożliwia przypisywanie szafek do poszczególnych osób lub grup, zezwala na korzystanie z nich przez określony czas lub bez limitu, blokowanie i odblokowywanie za pomocą dowolnego identyfikatora – karty, telefonu komórkowego, cechy biometrycznej lub kodu QR.
Dashboard AEOS ułatwia zarządzanie tysiącami szafek. Terminal w postaci tabletu zapewnia użytkownikom prostotę użytkowania, a aplikacja mobilna – otwieranie i zamykanie skrytek za pomocą telefonu.

Z kolei połączenie zarządzania szafkami z fizyczną kontrolą dostępu umożliwia szybki dostęp do danych i zaawansowanego systemu raportowania. Połączenie z systemem KD zapewnia ponadto dostęp do wielu integracji, m.in. z systemami HR.

AEOS Locker Management można wykorzystać, gdy towary lub urządzenia muszą zostać nadane lub odebrane. Rozwiązanie jest często stosowane m.in. przez:

- Działy IT – pracownicy mogą np. bezpiecznie zostawić uszkodzonego laptopa i odebrać go po naprawie.
- Sklepy z narzędziami – instalatorzy mogą odbierać materiały po godzinach pracy.
- Kurierzy – paczki można zostawić w bezpiecznym miejscu, gotowe do odbioru w późniejszym czasie.

SCHRACK SECONET

www.schrack-seconet.pl

APS®-APROSYS: dźwiękowy system ostrzegawczy

DŹWIĘKOWY SYSTEM OSTRZEGAWCZY APS®-APROSYS (PRODUKCJI G+M ELEKTRONIK AG) TO PRZEWODOWY, MODUŁOWY SYSTEM SŁUŻĄCY PRZEDE WSZYSTKIM DO POWIADAMIANIA OSÓB ZNAJDUJĄCYCH SIĘ W ZAGROŻONYCH OBSZARACH O EWAKUACJI LUB ZMOBILIZOWANIA ICH DO INNEGO DZIAŁANIA.

Dzięki wykorzystaniu technologii warstw i priorytetów może też służyć jako system rozgłaszania komercyjnego (PA – *public address)*, system zegarowy czy system dystrybuujący tło muzyczne w obiekcie (BGM – *background music)* w tym samym czasie.
Rozwiązaniem wyróżniającym system APS®-APROSYS jest m.in. możliwość optymalizacji instalacji DSO dzięki zastosowaniu elastycznego rozdziału mocy wzmacniaczy.
Zaawansowane kontrolery linii głośnikowych APS-178.1-XX--EV z wbudowanymi selektorami stref pozwalają na pełne wykorzystanie zakresów mocy oferowanych przez odpowiednio dobrane wzmacniacze.
Gdy w obiekcie występuje wiele stref nagłośnienia małej lub średniej mocy obsługiwanych przez jedną lub kilka par linii głośnikowych, można tu zastosować tylko jedną końcówkę wzmacniacza! Ponadto każda pożądana funkcja fakultatywna systemu to zaledwie jedna lub dwie karty systemowe dołożone do ramy montażowej MC-03 systemu.
Projektując dźwiękowy system ostrzegawczy z użyciem kontrolerów linii głośnikowych z selektorami stref, można znacznie zredukować liczbę wzmacniaczy, a co za tym idzie wymaganą pojemność akumulatorów zasilania rezerwowego, okablowanie systemowe, rozmiar i liczbę szaf typu RACK 19", bez zbędnego przewymiarowania systemu.

SMART-I

https://smart-i.pl

Praca hybrydowa napędza popyt na kontrolę dostępu w chmurze

WSPÓŁCZESNE ORGANIZACJE INWESTUJĄ W HYBRYDOWE MIEJSCA PRACY. W EFEKCIE FIRMY OCZEKUJĄ, ŻE SYSTEMY KD BĘDĄ DOSTARCZAĆ INFORMACJI BIZNESOWYCH, POZWALAĆ NA ZROZUMIENIE ZACHOWAŃ UŻYTKOWNIKÓW, DOKUMENTOWAĆ TRENDY. TE INFORMACJE POMOGĄ ORGANIZACJOM W PODEJMOWANIU LEPSZYCH DECYZJI BIZNESOWYCH W TAKICH OBSZARACH, JAK PODRÓŻE SŁUŻBOWE, NEGOCJACJE NAJMU CZY INWESTYCJE KAPITAŁOWE W TECHNOLOGIĘ.

Wraz z postępującą transformacją cyfrową, która unowocześnia wszystkie aspekty działalności biznesowej, korzyści płynące z KD opartej na chmurze stają się coraz bardziej widoczne, w szczególności niższy całkowity koszt posiadania.
Rozwiązania mobilne umożliwiają użytkownikom otwieranie drzwi, bram i innych systemów wejściowych za pomocą smartfonu. Pandemia przyspieszyła rozwój aplikacji mobilnych z powodu zapotrzebowania na bezdotykowy sposób rejestrowania nowych osób.
Ponadto, w przeciwieństwie do fizycznych kart czy breloków, smartfony są bezpieczniejsze, łatwiejsze w zarządzaniu i bardziej opłacalne. Kontrola dostępu oparta na chmurze ułatwia integrację z innymi aplikacjami działającymi w chmurze. Oznacza to, że rozwiązania mogą działać szybciej już od pierwszego dnia.
Pakiet bezpieczeństwa Brivo zbudowany na solidnej, opartej na chmurze platformie kontroli dostępu umożliwia i optymalizuje hybrydowe modele pracy, modernizuje operacje i dostarcza dane, które zamieniają praktyczne wnioski w decyzje oparte na danych w całym ekosystemie przedsiębiorstwa.

TELBUD

www.telbud.pl

System kontroli dostępu ARGUS KD

ARGUS KD JEST OPARTY NA NAJNOWSZYCH TECHNOLOGIACH INFORMATYCZNYCH Z PROSTYM INTERFEJSEM UŻYTKOWNIKA. NAPISANY JEST Z WYKORZYSTANIEM .NET CORE 6.0, KTÓRY ZAPEWNIA WIELOPLATFORMOWOŚĆ. SYSTEM MOŻNA URUCHOMIĆ Z TRYBU WEB (PRZEGLĄDARKA) LUB APLIKACJI PREINSTALOWANEJ NA DYSKU STANOWISKA OPERATORSKIEGO/ADMINISTRACYJNEGO.

Jest w pełni kompatybilny z innymi systemami z rodziny ARGUS. Stany systemu są wizualizowane w systemach klasy PSIM – ARGUS WEB oraz ARGUS RV, skąd można też wysyłać sterowania do serwera ARGUS KD, umożliwiające zamknięcie lub otwarcie drzwi na zworze elektromagnetycznej. Przejścia są powiązane z systemem wizualizacji kamer ARGUS CCTV, które w razie naruszenia pokazują przejścia w czasie rzeczywistym na ekranie alarmowym.
System umożliwia zbudowanie drzewa administracyjnego przedsiębiorstwa, które ułatwia zarządzanie uprawnieniami, użytkownikami i przejściami. Nadawanie i odbieranie uprawnień do przejść może odbywać się za pomocą grupowania, co przyspiesza dodawanie nowych użytkowników i zarządzanie nimi. Grupa uprawnień to zbiór przejść, które po przypisaniu do użytkownika umożliwiają mu przejście przez drzwi po identyfikacji kartą. System współpracuje z kartami HID Elite zwiększającymi bezpieczeństwo przedsiębiorstwa.
ARGUS KD można zintegrować z systemem wycieczkowym zliczającym ludzi na trasie wycieczki wewnątrz organizacji. System nadzoruje, czy któraś z osób nie zgubiła się na terenie obiektu i nie stwarza zagrożenia dla obiektu lub siebie samej.

TP-LINK

www.tp-link.com.pl

TP-Link EAP670 – nowy punkt dostępowy WiFi 6 z serii Omada EAP

EAP670 JEST PRZEZNACZONY DO BUDOWY CENTRALNIE ZARZĄDZANEJ SIECI BEZPRZEWODOWEJ NA DUŻYCH POWIERZCHNIACH. ZNAJDZIE ZASTOSOWANIE W MIEJSCACH, W KTÓRYCH Z BEZPRZEWODOWEJ SIECI KORZYSTA WIELU UŻYTKOWNIKÓW JEDNOCZEŚNIE. DZIĘKI INTEGRACJI Z PLATFORMĄ OMADA SDN MOŻE BYĆ CENTRALNIE ZARZĄDZANY PRZEZ CHMURĘ.

Nowe technologie standardu 802.11ax (modulacja 1024QAM, długi symbol OFDM) i wykorzystanie kanałów 160 MHz HE160 umożliwiają osiąganie bardzo wysokich prędkości – do 5378 Mb/s (do 574 Mb/s w paśmie 2,4 GHz i do 4804 Mb/s w paśmie 5 GHz). Port 2,5 Gb/s zapewnia bardzo dużą przepustowość. Instalacja EAP670 jest niezwykle prosta, obsługa zasilania PoE w standardzie 802.3at eliminuje dodatkowe okablowanie.
W modelu zastosowano technologie MU-MIMO i OFDMA. EAP670 gwarantuje też płynny roaming, dzięki czemu transmisje wideo i połączenia głosowe nie są przerywane, gdy użytkownicy zmieniają lokalizację. Obsługa technologii Omada Mesh pozwalającej łączyć punkty dostępowe bezprzewodowo w sieć kratową umożliwia ich montaż w miejscach, gdzie nie można doprowadzić kabla sieciowego.
EAP670 pozwala utworzyć aż 16 niezależnych sieci Wi-Fi (SSID) – z możliwością autoryzacji dostępu z uwierzytelnianiem przez Facebook albo SMS i logowaniem za pomocą strony powitalnej – jednorazowych haseł dostępu lub voucherów. Razem z szyfrowaniem WPA3-Enterprise znacząco zwiększa to bezpieczeństwo całej sieci i wrażliwych danych. Produkt jest objęty 5-letnią gwarancją producenta.

W2

www.w2.com.pl

Nowy pożarowy zewnętrzny sygnalizator głosowo-optyczny SGO-Pgz3

URZĄDZENIE SŁUŻY DO ALARMOWANIA ZAGROŻENIA POŻAROWEGO SYGNAŁEM OSTRZEGAWCZYM, KOMUNIKATEM SŁOWNYM I BŁYSKOWYM SYGNAŁEM OPTYCZNYM. SYGNALIZATOR JEST ZGODNY Z WYMAGANIAMI NORM ZHARMONIZOWANYCH EN 54-3 ORAZ EN 54-23. NA WYRÓB ZOSTAŁY WYDANE PRZEZ CNBOP-PIB CERTYFIKAT STAŁOŚCI WŁAŚCIWOŚCI UŻYTKOWYCH ORAZ ŚWIADECTWO DOPUSZCZENIA (WAŻNE TYLKO DLA ODMIANY SGO-PGZ3).

Urządzenie jest wyposażone w całkiem nowy człon optyczny, zbudowany na 4 diodach LED o wysokiej jasności. Sygnalizator występuje w trzech odmianach, które różnią się między sobą konstrukcją członu optycznego:

- **SGO-Pgz3** – światło czerwone (4 diody), klosz lampy w kolorze czerwonym
- **SGO-Pgz3/śb** – światło białe (2 diody), klosz lampy w kolorze białym
- **SGO-Pgz3/śbcz** – światło białe i czerwone naprzemiennie (2 czerwone i 2 białe diody), klosz lampy w kolorze białym.

W członie akustycznym zastosowano głośnik 4 Ω o wysokiej efektywności >90 dB (1 W/1 m) w szerokim paśmie oraz wzmacniacz audio pracujący w klasie D z układem wyciszenia stuknięć w głośniku o mocy wyjściowej ok. 20 W RMS 1 kHz.
Nowa konstrukcja poprawiła nie tylko poziom dźwięku sygnału alarmowego czy komunikatu słownego, lecz także ich jakość. Sygnalizator ma wiele funkcjonalności: płynna regulacja poziomu dźwięku, blokada podnapięciowa, autoaktualizacja, autoadresowanie, możliwość synchronizacji, złącze microUSB, magistrala komunikacyjna CAN, ogranicznik prądu rozruchowego czy autodiagnostyka akustyczna i optyczna.

ZKTeco

www.zkteco.eu

TRÓJRAMIENNE BRAMKI OBROTOWE SERII mTS1000 FIRMY ZKTeco

FIRMA ZKTECO DO SWOJEJ SZEROKIEJ KOLEKCJI BRAMEK OBROTOWYCH DODAŁA KOLEJNE MODELE SERII MTS1000. CHARAKTERYZUJE JE WYRAFINOWANA KOMPAKTOWA KONSTRUKCJA UMOŻLIWIAJĄCA ICH OPTYMALNY MONTAŻ, PRZY JEDNOCZESNEJ OSZCZĘDNOŚCI ZAJMOWANEGO MIEJSCA.

Zarówno kołowrót, jak i obudowa są wykonane z wysokoudarowej stali nierdzewnej SU304 (opcjonalnie SU316) przykrytej trwałą płytą akrylową. Bramki są oferowane w różnych wersjach, zależnie od wyposażenia:

- mTS1000 – bramka standardowa,
- mTS1011 – bramka z kontrolerem i czytnikiem kontroli dostępu RFID,
- mTS1022 – bramka z kontrolerem oraz kombinacją czytników RFID i linii papilarnych.

Wszystkie bramki mogą pracować dwukierunkowo. Wbudowane intuicyjne piktogramy LED zapewniają użytkownikom jasne wskazówki dotyczące zezwolenia przejścia i kierunku ruchu. Charakteryzuje je wysoka przepustowość przejścia oraz identyfikacji kontroli dostępu.
Są też łatwe w instalacji. Mogą pracować zarówno wewnątrz, jak i na zewnątrz obiektów.
W sytuacjach awaryjnych dla zapewnienia swobodnego przejścia ramiona kołowrotu można skutecznie opuścić za pomocą pilota zdalnego sterowania. Ramiona opuszczają się też automatycznie w przypadku braku zasilania. Integrując wiele funkcji, bramki te zapewniają szerokie i optymalne finansowo rozwiązanie w wielu miejscach.

Doskonale sprawdzają się m.in. w biurach korporacyjnych, obiektach targowych czy parkach rozrywki.

Warsaw Security Summit to nie tylko konferencja, ale także konsultacje na stoiskach wystawienniczych, rozmowy w kuluarach oraz nowe wartościowe kontakty.

Mariusz Kucharski

pomysłodawca konferencji, wydawca czasopisma „a&s Polska”

Warsaw Security Summit 2022

a&s POLSKA

Bardzo szeroki zakres tematyczny – od bezpieczeństwa fizycznego po cyberbezpieczeństwo – oraz odpowiedzi na pytania, jak sobie radzić z nowymi wyzwaniami, jakie stawia nowa rzeczywistość. Mnóstwo wiedzy oraz wielu specjalistów i praktyków.

Marcin Prokop

Za nami szósta edycja konferencji Warsaw Security Summit. Po pandemicznej przerwie szefowie bezpieczeństwa i security menedżerowie spotkali się 6 czerwca w Centrum Praskim KONESER w Warszawie. Wydarzenie przyciągnęło do stolicy prawie 600 osób z całego kraju związanych profesjonalnie z branżą bezpieczeństwa.

Konferencję zdominowały tematy dotyczące zapewnienia szeroko pojętego bezpieczeństwa w obliczu wojny w Ukrainie. Duże wrażenie na uczestnikach wywarł wykład inauguracyjny pod tytułem: „Nigdy nie zakładam, że coś jest niemożliwe tylko dlatego, że nie mieści się to w mojej głowie. Czyli dlaczego wojsko ćwiczy na serio obronę przed atakiem z Kosmosu”. Generał Roman Polko tłumaczył żywiołowo, jak przygotować się na nieoczekiwane sytuacje kryzysowe, co ilustrował przykładami ze służby wojskowej.

O ważności systemów kontroli dostępu w dużych zakładach produkcyjnych nie trzeba przypominać. W czasie Warsaw Security Summit specjaliści od kontroli dostępu wskazywali, jak dopasować system do konkretnych wymagań użytkownika, który nie utrudniałby pracy. Zapewnienie bezpieczeństwa w zakładzie produkcyjnym z wykorzystaniem nowych możliwości platformy kontroli dostępu zademonstrowali Anna Twardowska i Błażej Ożga z firmy Nedap Security Management.

Tematy konferencji nie ograniczały się do trendów technologicznych w przemyśle czy energetyce. Jak po dwóch latach pandemii zmieniło się podejście do idei *smart city* i co nowego dzieje się w obszarze bezpieczeństwa polskich miast? Wiceburmistrz warszawskiej dzielnicy Ursynów Bartosz Dominiak mówił o tym, jak wykorzystanie dronów może zaspokoić potrzeby mieszkańców i władz miasta w sferze poprawy bezpieczeństwa transportu czy zarządzania miastem.

Tematykę *smart city* uzupełniła prezentacja Michała Swobody z Hikvision, który przybliżył zastosowania analizy wizyjnej wspartej technologią *deep learning* w rozwiązaniach ITS/Traffic. Uczestnicy konferencji mogli też się dowiedzieć na przykładzie Tarnowa i Bielska-Białej, jak skutecznie poprawić bezpieczeństwo w ruchu miejskim. Ten temat omówił Dominik Weder z firmy Sprint. Z kolei Kazimierz Liver (Wasko) przedstawił system nadzoru i monitorowania zdarzeń na przykładzie tunelu pod Ursynowem w południowej obwodnicy Warszawy.

W trakcie Warsaw Security Summit dużo miejsca poświęcono rozwojowi technologicznemu, dlatego nie mogło zabraknąć wystąpień z zakresu cybersecurity. Marcin Maj z niebezpiecznik.pl wskazał na zagrożenia i najczęściej popełniane błędy, zwracając uwagę na dobre praktyki w zapewnieniach bezpieczeństwa świata wirtualnego firm i instytucji. Do tego tematu nawiązał też Piotr Rogalewski z Hikvision, omawiając bezpieczeństwo cybernetyczne systemów zabezpieczeń technicznych. Konferencję zakończyło wystąpienie Tomasza Olejniczaka (Hikvision), który przedstawił zalety zastosowania inteligentnego systemu wspomagania decyzji (IDSS).

Zapis konferencji jest dostępny na profilu a&s Polska na YouTube.

gen. Roman Polko

były dowódca GROM

Warsaw Security Summit to doskonałe miejsce do wymiany myśli. To budowa sieci *good guys*, czyli ludzi, którzy zajmują się podobnymi problemami, ale z inną perspektywą, i dzięki temu wspólnie szukają najlepszych rozwiązań. Takie kontakty pomagają w podejmowaniu dobrych decyzji o naszym wspólnym bezpieczeństwie.

Łukasz Lik

Hikvision Poland

Bardzo się cieszymy, że byliśmy głównym partnerem tej merytorycznej konferencji. W swojej prezentacji przedstawiłem najnowsze trendy technologiczne, które oddziałują na branżę w 2022 roku. Są to m.in. cyberbezpieczeństwo, sztuczna inteligencja oraz IoT.

Anna Twardowska

Nedap Security Management

Podczas prelekcji pokazaliśmy problemy, z jakimi zmagali się nasi klienci. Opowiedzieliśmy przy tym, jakim wyzwaniom może sprostać nasz system i jak jesteśmy w stanie go dostosować do indywidualnych potrzeb klientów.

Jarosław Stelmach

Safety Project

Jest tu zjawiskowo i prestiżowo. To także dobry czas na takie spotkanie, dlatego że trwa wojna w Ukrainie i mamy stopień BRAVO wprowadzony w całym kraju. Pochylmy się po prostu nad metodą, nad narzędziem i zastanówmy się, jakie miejsca mogą zostać zaatakowane. Zbudujmy bezpieczeństwo metodą scenariuszową, uwzględniając najgorsze scenariusze. Wówczas znajdziemy adekwatne rozwiązania.

Bartosz Dominiak

wiceburmistrz Dzielnicy Ursynów m.st. Warszawy

Jestem wielkim fanem konferencji, na których specjaliści z różnych branż, ale z danego obszaru tematycznego mogą wymieniać się swoimi przemyśleniami i doświadczeniami. W dzisiejszych czasach postpandemicznych z jednej strony, z drugiej – w czasach realnej wojny, która się dzieje tuż za naszą granicą oraz wojny hybrydowej, która ma miejsce w Polsce, takie konferencje są bezcenne.

Marcin Maj

Niebezpiecznik.pl

Moja prelekcja dotyczyła takich tematów z zakresu bezpieczeństwa, które nie są może najbardziej efektowne, jeśli chodzi o wartość teoretyczną, natomiast występują najczęściej. My jesteśmy ludźmi, którzy nie tyle tworzą fajne produkty, ile starają się sprawdzić, jak można je zepsuć. I stąd wiemy, że najczęściej różne rzeczy zawodzą właśnie u podstawy.

Wielka Gala Security

Wieczorem zaproszeni goście uczestniczyli w uroczystej gali, na której wystąpił Krzysztof Cugowski z Zespołem Mistrzów.

Jacek Tołżewski

Przedsiębiorstwo Państwowe „Porty Lotnicze”

Wrażenia bardzo dobre, konferencja merytoryczna, dużo osób z branży. To daje możliwość nawiązania nowych kontaktów i przeprowadzania ciekawych rozmów.

Tomasz Grzelak

DPD Polska

To już kolejna konferencja Warsaw Security Summit, w której uczestniczę. Jak zawsze świetna organizacja, świetni prelegenci, tematy idealnie dobrane do wyzwań obecnych czasów.

Hubert Żak

Accor Hotels

Wszystko to, co tu zobaczyliśmy i usłyszeliśmy, daje nam kolejną możliwość do uzupełniania wiedzy, bardzo dziś potrzebnej, byśmy mogli dobrze przygotować użytkowników sektora bezpieczeństwa do tych trudnych czasów. Dotyczy to tak naprawdę nas wszystkich.

Tomasz Guzikowski

CIECH

Takie konferencje są bardzo potrzebne, ponieważ umożliwiają wymianę doświadczeń i konsultacje ze specjalistami z różnych dziedzin. Nikt nie jest alfą i omegą we wszystkich specjalizacjach, więc na pewno zyskuje się dużo szerszy pogląd na to, co jest dostępne na rynku i co można wykorzystać w swojej pracy.

Echa zmiany paradygmatu w bezpieczeństwie

– przykazania współczesnego bezpiecznika

Artykuł stanowi z jednej strony próbę zwrócenia uwagi na przyczynę obecnej sytuacji wielu komórek bezpieczeństwa, z drugiej – wskazania popartej nie tylko własnym doświadczeniem drogi (i kierunku), którą współczesny bezpiecznik powinien podążać. Oczywiście przekazywana treść jest subiektywna i nie stanowi jedynie słusznej prawdy objawionej.

Jan Kapusta

Co za tym idzie, nie oczekuję od nikogo pełnej czy nawet jakiejkolwiek zgody z wyrażanymi w artykule poglądami. Jeżeli natomiast jego lektura skłoni do refleksji, a może nawet konstruktywnych wniosków, to mój cel został osiągnięty. Choć treść jest umieszczona w dziale poświęconym bankom – w środowisku tym spędziłem sporą część swojego zawodowego życia – to mam nadzieję, że coś wartościowego znajdzie tu każdy „bezpiecznik", niezależnie od sektora, w jakim pracuje.

W szeroko rozumianym świecie bezpieczeństwa (głównie w przestrzeni akademickiej) funkcjonuje termin *paradigm shift*, co oznacza „zmiana paradygmatu". Bez zagłębiania się w tłumaczenie znaczenia tego terminu obejmuje on niemal każdy aspekt bezpieczeństwa, w jakim kiedyś myśleliśmy inaczej, niż powinniśmy myśleć obecnie. I tak mówimy o zmianie paradygmatu w stosunkach międzynarodowych, obronności kraju i innych obszarach. W literaturze przedmiotu można znaleźć informacje, które w kontekście bezpieczeństwa mówią, że stare podejście było oparte na negatywnych przesłankach – wszędzie był wróg i przestępca myślący o tym, jak nas skrzywdzić. Współczesne podejście ma być pozytywne i konstruktywne – nie ma wroga czy bandyty, jest natomiast przeciwnik, a nasze działania są skoncentrowane raczej na budowaniu niż destrukcji. Być może da się wyczuć w tej wypowiedzi odrobinę sarkazmu, nasuwa się też pytanie, jakie ma to przełożenie na „bezpiecznika" (fizycznego) czy to w banku, czy w innej organizacji.

Niektórzy z łezką w oku wspominają czasy, gdy w większości banków funkcjonowały silne i w dużym stopniu niezależne Departamenty Bezpieczeństwa. Każdy liczył się z ich zdaniem, a ilość wszelkiego rodzaju zasobów zapewniała spokojną pracę. Wystarczyło słowo „nie", by jego adresat nie podejmował zbędnej polemiki z naszym doświadczeniem i wiedzą ekspercką. Tak… To właśnie z chwilą, kiedy te sielskie czasy komórek bezpieczeństwa się skończyły, doświadczyliśmy zmiany paradygmatu. Z tym, że doświadczyliśmy tej zmiany, nie będąc w pełni świadomi tego faktu czy rozumiejąc, co się dzieje. Zostaliśmy „pozbawioną władzy grupą" kompletnie nieprzygotowaną na zmiany – postawieni przed faktem dokonanym. Niektórzy do dziś nie potrafią sobie z tym poradzić.
W mojej ocenie stan, kiedy komórki bezpieczeństwa zostały sprowadzone do roli pasywnego narzędzia mającego zapewnić względną zgodność z wymaganiami formalnoprawnymi danej organizacji, zawdzięczamy poniekąd sami sobie. Frustracja wynikająca z niewiedzy i braku zrozumienia tego, co się dzieje, zastąpiła konstruktywną analizę i proaktywne wytyczanie ścieżek przez nową rzeczywistość. Zresztą przewidywanie i przygotowanie się na kryzys przed katastrofą, a nie po jej wystąpieniu jest również elementem zmiany paradygmatu. Z tego właśnie powodu poruszam kilka aspektów wspomnianej zmiany, których zrozumienie może pomóc w ustawieniu komórki bezpieczeństwa ponownie na właściwe tory, choć tory te trzeba wcześniej samemu cierpliwie budować. Mam świadomość różnego rodzaju ograniczeń, ale o tym będzie trochę później.

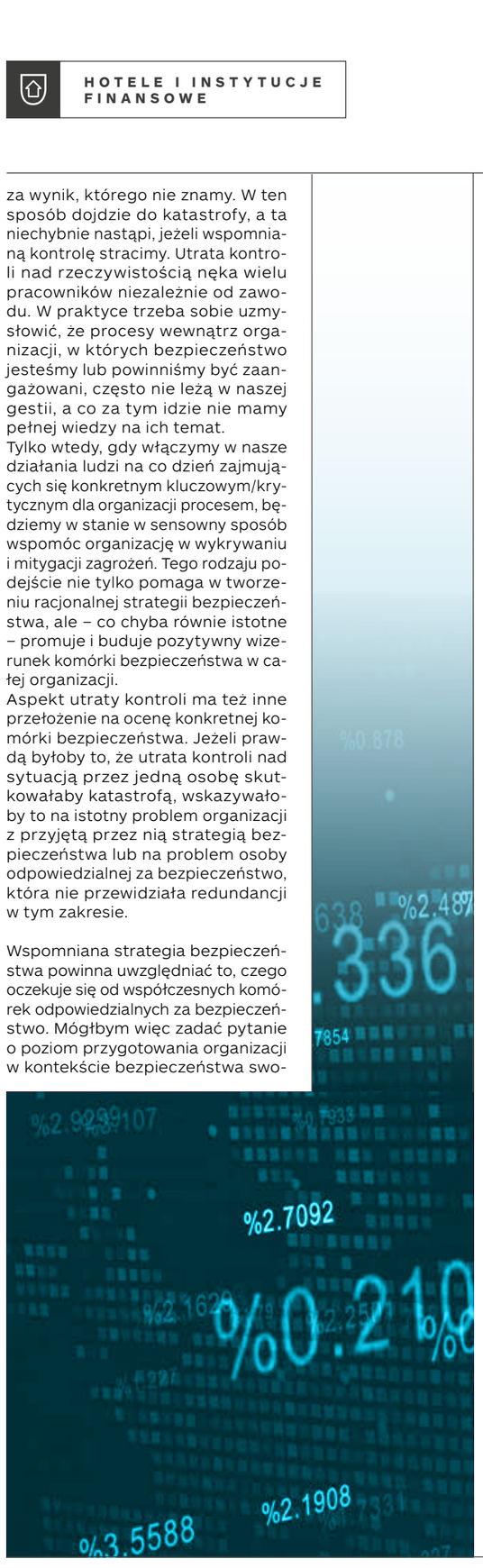
Punktem wyjścia niech będzie fakt, że celem komórki bezpieczeństwa nie jest blokowanie inicjatyw podejmowanych przez organizację poprzez wskazywanie związanego z daną inicjatywą ryzyka (ryzyk). Celem jest pomoc organizacji w „dowiezieniu" tej inicjatywy w możliwie bezpieczny i sensowny sposób. Innymi słowy, nie mówimy tylko o tym, co złego może się przytrafić, a raczej koncentrujemy się na tym, co zrobić, by tego „złego" uniknąć w racjonalny sposób. Co gorsza, musimy wiedzieć, jak to powiedzieć – i tu dotykamy kolejnego strategicznego punktu, którego wielu z nas musi się nauczyć, jeżeli chce dobrze funkcjonować w organizacji.

Musimy używać języka biznesu. Nie jest niczym odkrywczym, że komórki bezpieczeństwa nie generują przychodu, tylko konsumują pieniądze zarobione przez innych. I nie ma znaczenia, czy są to pieniądze zarobione przez tych, którzy sprzedają produkty i usługi dostarczane przez organizację, czy mówimy o pieniądzach dostarczanych przez podatnika do Skarbu Państwa. Musimy umieć pokazać w liczbach (najlepiej wyrażonych w konkretnej walucie), że pieniądze wydajemy w niezbędnej ilości na konieczne i efektywne rozwiązania przynoszące wymierną korzyść organizacji.
Z pomocą przychodzą narzędzia, m.in. różnego rodzaju metodologie i narzędzia programowe wspomagające nas niemal na każdym etapie pracy „bezpiecznika" (przynajmniej stworzone z myślą o jego wspomożeniu). Z wielu już potrafimy korzystać, ale mam przekonanie graniczące z pewnością, że istnieje spora grupa narzędzi, z których nie korzystamy, bo często nawet nie wiemy o ich istnieniu. Zacznijmy zatem od samodzielnego poszukania i zrozumienia idei ALARP *(As Low As Reasonably Possible)*, następnie poszukajmy narzędzi oceny efektywności rozwiązań, z których zamierzamy skorzystać, zestawmy to z oceną ryzyka, oceną zagrożeń i oceną podatności – i dopiero na tym spróbujmy oprzeć strategię komunikacji z tymi, od których zależy nasz budżet. Nic nowego. Czy aby na pewno?

Często żartuję, że jedyną cechą wspólną wszystkich „bezpieczników" jest posiadanie jedynej słusznej i obiektywnie objawionej prawdy. Zawsze mamy rację i tylko my tę rację posiadamy. Mówiąc poważnie, zapewne przez specyfikę naszego zawodu mamy tendencję do rozumowania, że jeżeli sami czegoś nie zrobimy, to stracimy nad tym kontrolę i trudno nam będzie odpowiadać

za wynik, którego nie znamy. W ten sposób dojdzie do katastrofy, a ta niechybnie nastąpi, jeżeli wspomnianą kontrolę stracimy. Utrata kontroli nad rzeczywistością nęka wielu pracowników niezależnie od zawodu. W praktyce trzeba sobie uzmysłowić, że procesy wewnątrz organizacji, w których bezpieczeństwo jesteśmy lub powinniśmy być zaangażowani, często nie leżą w naszej gestii, a co za tym idzie nie mamy pełnej wiedzy na ich temat.
Tylko wtedy, gdy włączymy w nasze działania ludzi na co dzień zajmujących się konkretnym kluczowym/krytycznym dla organizacji procesem, będziemy w stanie w sensowny sposób wspomóc organizację w wykrywaniu i mitygacji zagrożeń. Tego rodzaju podejście nie tylko pomaga w tworzeniu racjonalnej strategii bezpieczeństwa, ale – co chyba równie istotne – promuje i buduje pozytywny wizerunek komórki bezpieczeństwa w całej organizacji.
Aspekt utraty kontroli ma też inne przełożenie na ocenę konkretnej komórki bezpieczeństwa. Jeżeli prawdą byłoby to, że utrata kontroli nad sytuacją przez jedną osobę skutkowałaby katastrofą, wskazywałoby to na istotny problem organizacji z przyjętą przez nią strategią bezpieczeństwa lub na problem osoby odpowiedzialnej za bezpieczeństwo, która nie przewidziała redundancji w tym zakresie.

Wspomniana strategia bezpieczeństwa powinna uwzględniać to, czego oczekuje się od współczesnych komórek odpowiedzialnych za bezpieczeństwo. Mógłbym więc zadać pytanie o poziom przygotowania organizacji w kontekście bezpieczeństwa swoich zasobów na dzień wybuchu wojny w Ukrainie. Mógłbym również zapytać o przygotowanie banków na zmianę w statystykach dotyczących liczby napadów rabunkowych w porównaniu z liczbą ataków na bankomaty. Każdy może sobie sam odpowiedzieć, jak to wyglądało w jego organizacji. Zapytam natomiast, czy można było to wszystko przewidzieć? Odpowiedź jest prosta – można było. Co więcej, można było i należało się do tego przygotować.



Zdolność do monitorowania, analizowania i przygotowywania przyszłych i niekoniecznie dobrze znanych scenariuszy zdarzeń jest tym, czego oczekuje się od współczesnych komórek bezpieczeństwa. Oczywiście mowa tu o scenariuszach tworzonych na bazie oceny faktów i odpowiednio silnych przesłanek oraz ich pragmatycznej oceny w kontekście konsekwencji, jakie niosą. Jeżeli nauczyłeś się, jak używać języka liczb i pieniądza, masz już nawiązane dobre relacje z decyzyjnymi właścicielami procesów krytycznych i innymi kluczowymi funkcjami, wtedy przedyskutowanie i ocena konkretnego scenariusza nie będzie stanowić problemu, a tym bardziej przygotowanie się na ten scenariusz. Problemem nie są dobrze znane, powtarzające się zdarzenia niechciane (napady, włamania itp.). Nie zapominamy o nich i troszczymy się o to, by sobie z nimi radzić, ale te, jak wspomniałem, już dobrze znamy.
Problemem jest to, co może się wydarzyć, a jest dla nas względnie nowe z perspektywy statystycznych danych historycznych czy wynikających z nich trendów. Monitoring i analiza danych z bieżących wydarzeń i przygotowanie na nowe istotne zdarzenia jest tym, czego powinniśmy szukać. Zanim ktoś po raz pierwszy wysadził bankomat, dane historyczne nie wskazywały na to, że do takiego ataku dojdzie, a jednak doszło. Nim ten atak stał się popularny i urósł do skali istotnego problemu, minęło kilka lat, które prawdopodobnie można było lepiej wykorzystać. W całościowym bilansie przygotowanie się na możliwy do przewidzenia scenariusz wychodzi taniej niż reaktywne podejście *post factum*. To właśnie działania proaktywne są tym, czego potrzebujemy obecnie bardziej. Z przyczyn oczywistych z dobrze znanych działań reaktywnych nie możemy i nie powinniśmy zrezygnować, ale bez koncentracji na metodach przewidywania trudno będzie komukolwiek zbudować silny wizerunek komórki bezpieczeństwa. Pragnę podkreślić, że za działania reaktywne uznaję również te, które zabezpieczają nas przed przyszłym wystąpieniem zdarzeń, które dobrze znamy. W tym kontekście planowanie zabezpieczenia na okoliczność potencjalnego, dobrze znanego zjawiska, jakim jest napad rabunkowy, to również działanie reaktywne.

Mówi się, że łatwiej powiedzieć, niż zrobić. Przecież jest tyle problemów i barier. Owszem, nie jest to łatwe, co nie znaczy jednak, że nie można sobie z nimi radzić. Warto by zacząć od zrozumienia, z jakimi przeszkodami mamy do czynienia, i spróbować znaleźć na nie sposób. Generalnie świat zna problemy, z którymi trzeba się zmierzyć podczas tworzenia współczesnej strategii bezpieczeństwa. Co więcej, można znaleźć opracowania, które je grupują i nazywają. Przychylam się do osób wskazujących na następujące ograniczenia, z którymi należy się zmierzyć:

- **POZNAWCZE** (sensoryczne) – łatwiej zauważyć i reagować na to, co znamy i czego doświadczyliśmy „na własnej skórze". Nasze zmysły już to znają, więc jesteśmy na to bardziej wyczuleni. Trudno zrozumieć i dostrzec zagrożenie, którego nie doświadczyliśmy. Niewiele dzieci (organizacji) uwierzy na słowo, że coś jest gorące i może się poparzyć. Sytuacja się zmienia po pierwszym doświadczeniu bólu wynikającego z poparzenia, a przecież chcemy, by dziecko uniknęło bólu lub przynajmniej było przygotowane na ten scenariusz.
- **PSYCHOLOGICZNE I KIEROWNICZE** – zarówno my, jak i nasi przełożeni (różnego szczebla) mamy tendencję do unikania wszystkiego, co może narazić naszą/ich pozycję na ryzyko. *Status quo* to ważna rzecz i może lepiej nie tworzyć wizji czegoś, co może się nie sprawdzić, i wtedy narazimy na szwank swoją reputację? Tylko że nam chodzi o to, by powiedzieć, że przewidzieliśmy i byliśmy przygotowani na konkretny scenariusz.
- **ORGANIZACYJNE** – organizacja działa w obrębie ustalonego porządku, który narzuca określone ramy działania. Co za tym idzie, każda zmiana, która niesie konieczność poszerzenia tych ram o elementy nowe, jest trudna do przeprowadzenia. Może lepiej nie rozmawiać o ryzyku wystąpienia konkretnego nowego zdarzenia, bo i tak nikt nie da pieniędzy na wróżenie z fusów, przecież do tej pory nikt nie wysadził w powietrze bankomatu...
- **POLITYCZNE** – choć chodzi tu o politykę w ujęciu relacji międzynarodowych, to zależności „polityczne" wewnątrz organizacji nie zawsze sprzyjają określonym zmianom. Może lepiej nie podnosić konkretnego tematu, bo nie wpisuje się w wizję szefa? Ale jak się to coś wydarzy, to czy wpisze się lepiej i pomoże organizacji?

Zasadniczo wszystkie wymienione bariery sprowadzają się z jednej strony do psychologicznych atrybutów określonych ludzi w organizacji i „naturalnej" chęci utrzymania *status quo*, z drugiej – do tego, jak dobrze organizację i tworzących ją ludzi znamy oraz jaką mamy zdolność do zbudowania z nimi odpowiednich relacji.

Biorąc pod uwagę wszystko powyższe i nieco więcej, przygotowałem swego rodzaju dekalog współczesnego „bezpiecznika". Jestem głęboko przekonany, że kierując się tymi zasadami (choć nie uważam ich za katalog zamknięty), każdy „bezpiecznik", a zwłaszcza osoba odpowiedzialna za tworzenie strategii bezpieczeństwa nie tylko sprosta współczesnym wyzwaniom bezpieczeństwa, ale także da się poznać jako wartościowy i profesjonalny partner do rozmów wewnątrz organizacji, z którego głosem warto się liczyć.

TE ZASADY SĄ NASTĘPUJĄCE:

1. Konstruktywnie pomagaj organizacji w bezpiecznej realizacji jej celów.
2. Skup się na proaktywnym przewidywaniu, lecz nie zapominaj o obowiązkach reaktywnych.
3. Pracuj na faktach i wynikających z nich mocnych przesłankach.
4. Korzystaj ze sprawdzonych narzędzi wspomagających ocenę stosowanych rozwiązań.
5. Proponuj rozwiązania problemów w miejsce jedynie wskazywania zagrożeń.
6. Szukaj wartości dodanej dla organizacji przy każdym planowanym elemencie bezpieczeństwa.
7. Posługuj się językiem liczb i pieniądza zrozumiałym dla tych, którzy o pieniądzu decydują.
8. Buduj relacje wewnątrz organizacji i poza nią.
9. Angażuj i korzystaj z wiedzy tych, którzy znają proces lepiej od ciebie, oraz tych, którzy są decyzyjni.
10. Poznaj ograniczenia i uwzględnij ich pokonywanie w budowanej strategii bezpieczeństwa.

JAN KAPUSTA

mgr inż., Dip. CSMP®, M.ISMI®. Praktyk i wykładowca, od ponad 20 lat związany z branżą security i zarządzaniem bezpieczeństwem. Współtwórca i były przewodniczący Forum Bezpieczeństwa Fizycznego przy Radzie Bezpieczeństwa ZBP. Obecnie zarządza bezpieczeństwem operacyjnym z obszarem działania obejmującym Europę Środkową i Wschodnią, Rosję i Wspólnotę Niepodległych Państw.

Chmura z efektem biznesowym

Organizacje działające w obszarze rynków i usług finansowych, a zwłaszcza banki, są poddawane ciągłej presji różnego rodzaju transformacji. To efekt zmian na rynku, nowych regulacji, nowego spojrzenia na rynek pracy przez pracowników banków, a przede wszystkim nowych zachowań konsumentów. Nowe oczekiwania klientów są kluczem do zrozumienia tych zjawisk dotykających banki, a które implikują konieczność modyfikacji usług finalnie dostarczanych właśnie klientom oraz bardzo często modelu ich oferowania czy zupełnie innych ich parametrów.

Przemysław Galiński

Pojawiają się obszary wpływu i konieczność zmian, które historycznie nigdy wcześniej nie miały miejsca, np. pandemia, która zmieniła postrzeganie i oczekiwania stawiane instytucjom finansowym, w tym choćby prawdziwej omnikanałowości, czyli w pełni cyfrowej bankowości świadczonej niezależnie od miejsca i czasu. Ponadto zwiększył się poziom wymagań klientów. Wynika to z aktywnego działania konkurencyjnego klasycznych instytucji finansowych, a więc m.in. innych banków, ale też fintechów, które bardzo szybko potrafią zaadresować oczekiwania klientów. Wychodząc na rynek z komunikatem, że potrafią z większą lub mniejszą skutecznością przewidywać trendy i obszary, które wkrótce pojawią się na rynku, a już dziś są w domenie zainteresowań konsumentów, a więc klientów.

Polski rynek finansowy jest na poziomie technologii jednym z dynamicznie rozwijających się. Sprawia to, że mamy do czynienia z dość dobrze działającą rozpędzoną maszyną, której zmiana lub modyfikacja nie jest łatwa, a przy tym potencjalnie kosztowna. Na szczęście menedżerowie banków, obserwując bardziej dojrzałe rynki, mają świadomość konieczności zmiany. Przed nami jeden z większych historycznie przełomów, który porównałbym choćby do przejścia z dokumentów papierowych na elektroniczne.

TECHNOLOGIA

Technologia staje się imperatywem każdej organizacji, a *cloud* imperatywem strategii technologicznej. Idąc tym tropem, analizując i obserwując dojrzalsze rynki, można przyjąć, że adaptacja technologiczna i chmurowa stanowią jeden z głównych czynników wspierających i umożliwiających głęboką transformację organizacji. Tak dzieje się już w instytucjach finansowych na naszym rynku. Każdy, kto działa z instytucjami finansowymi, może potwierdzić, że właściwie nie pozostał żaden bank, który by obecnie nie testował, nie wdrażał i w mniejszym lub większym zakresie nie używał chmury obliczeniowej lub nie korzystał z rozwiązań klasy *software as a service (SaaS)*. Pracując na rynku nowych technologii przez kilkanaście lat, nigdy wcześniej nie zaobserwowałem takiej liczby ambitnych, a przy tym bardzo ciekawych projektów digitalizacyjnych, jak ma to miejsce teraz. Jako eksperta od chmury i równocześnie klienta banków napawa mnie to uzasadnionym optymizmem.

ADAPTACJA CHMURY

Oczywiście jeden projekt adaptacji chmury nie jest równy drugiemu. Zanim banki globalnie zaczną masowo przenosić swoje systemy centralne do chmury (choć zaczyna się to powoli dziać) albo zastąpią je rozwiązaniami, które bazując technologicznie na chmurze, będą miały inną logikę działania (choć podobną funkcję biznesową), minie jeszcze trochę czasu. Jednak już teraz takie prace trwają, także na rynku polskim.

Z punktu widzenia PwC można zaobserwować kilka rodzajów aktywności. Są to m.in. testowanie rozwiązań opartych na chmurze (w obszarze usług dostępnych na platformach PaaS i SaaS dostawców *cloud*), implementacja rozwiązań chmurowych stanowiących systemy istotne, ale nie kluczowe dla banków, np. implementacja narzędzi typu *modern workplace* (narzędzi do pracy biurowej, komunikacji IM itp.) oraz podejście do „ciężkich" systemów bankowych w celu ich ewentualnej modernizacji lub zmiany w kierunku migracji do chmury lub szerokiej w zakresie transformacji. To tylko przykłady stanowiące wycinek tego, co można obserwować w bankowości w zakresie chmury, jednak oddające charakterystykę trwających aktywności. W większym lub mniejszym stopniu takie działania są prowadzone we wszystkich bez wyjątku polskich bankach, na coraz większą skalę.

CZY SAMA PLATFORMA CHMUROWA TO WSZYSTKO, CO JEST NIEZBĘDNE DO IMPLEMENTACJI *CLOUD*?

Na tak zadane pytanie można odpowiedzieć jednoznacznie – nie. Chmura (jako sama technologia) jest składnikiem koniecznym, ale tylko jednym z wielu w procesie transformacji. Często też jest katalizatorem większych zmian następujących w obszarze biznesu. Jako PwC dostrzegliśmy w projektach chmurowych wiele wyzwań, a ich część wynika z czynników innych niż stricte IT, choć te są dominujące. Dlatego też jako jedna z nielicznych firm na świecie potrafimy dostrzec, a także zaadresować proces adaptacji uwzględniający wszystkie takie elementy bez wyjątku.

W naszej unikalnej metodyce adaptacji chmury uwzględniamy WSZYSTKIE czynniki wpływające na projekt. Mieszczą się one w zakresie trzech obszarów:

1. Technologia
2. Regulacje/prawo
3. Biznes

Komentarz PwC do raportu Związku Banków Polskich oraz Centrum Prawa Bankowego i Informacji „Transformacja banku do chmury" (https://www.pwc.pl/pl/artykuly/transformacja-banku-do-chmury-raport-zwiazku-bankow-polskich-z-insightem-pwc.html (dostęp: 12.01.2022)

Technologia

Powinna być wystarczająco wydajna, bezpieczna, optymalna kosztowo i najlepiej dopasowana do SPECYFICZNYCH wymagań danej organizacji. Zarówno zespoły wewnętrzne, jak i dostawcy, partnerzy wdrożeniowi powinni cechować się możliwie najwyższymi umiejętnościami interdyscyplinarnymi (w obszarze technologii IT i *cloud*), aby móc wykorzystać cały potencjał chmury.
W tym (oraz biznesowym) zakresie możemy mieć do czynienia także z ewentualnym opracowaniem lub dostosowaniem istniejącego Modelu Operacyjnego do funkcjonowania z zupełnie innym modelem korzystania z usług charakteryzowanych jako *as a service* (usług, których odbiorcami jest biznes banku, a potem klienci końcowi). Bez zaadresowania tego elementu potencjalne wdrożenie będzie mieć o wiele niższy wpływ na naszą organizację, zatem przyniesie o wiele mniejsze korzyści i uzysk.

Regulacje/prawo

To krytyczny obszar w projektach implementacji chmury. Ze względu na wysokie wymagania regulacyjne charakterystyczne nie tylko dla Polski, specyfikę branży oraz obowiązki spoczywające na organizacji wdrażającej tę technologię, jest to sfera, która powinna być uwzględniona w kontekście wsparcia już od samego początku projektu i/lub programu chmurowego. Jego rozszerzeniem jest *cloud security* – a więc obszar odpowiadający za technologiczne bezpieczeństwo, ale również to wynikające z wymagań właśnie regulacyjnych.

Biznes

Stanowi kolejny krytyczny czynnik w implementacji *cloud*. Chmura sama w sobie nie stanowi wystarczającej wartości, a nabywa ją dopiero wtedy, gdy przynosi wartość biznesową samej organizacji (a następnie klientom). To tu następuje uwzględnienie wszystkich wymagań biznesowych, to tutaj można przewidzieć i określić, czy i w jaki sposób chmura wpłynie na naszą organizację w przyszłości oraz to, w jaki sposób może wzmocnić np. naszą przewagę konkurencyjną, wpłynąć na zyski czy np. wycenę giełdową. Tu widzimy (albo przynajmniej staramy się dostrzec) przyszłość naszej organizacji i jej miejsce względem choćby konkurencji.

Te wszystkie trzy obszary są przez zespół ekspertów PwC określane jako „DNA projektu chmurowego" i w tym zakresie każdy projekt wdrożeniowo-implementacyjny powinien być sparametryzowany, a potem wspar-

ty, żeby na końcu móc ocenić jego efektywność. Bazując na projektach, które realizowaliśmy, to właśnie zaadresowanie czy uwzględnienie tych trzech elementów wyraźnie zwiększa prawdopodobieństwo sukcesu projektu, implementacji, modernizacji lub migracji do chmury.
Naszym doświadczeniem rekomendujemy wprost takie budowanie projektów chmurowych, aby obejmowało każdy z nich, choć oczywiście zarówno nakłady pracy, jak i koszty nie są rozłożone proporcjonalnie. Często charakteryzuje się to tym, że np. technologia z punktu widzenia wielkości projektu, jego skali i kosztów angażuje 60% zasobów (i kosztów), regulacje i bezpieczeństwo 30%, a część biznesowa kolejne 10%. Wszystko zależy od wymagań stawianych projektowi i sytuacji w samej organizacji.

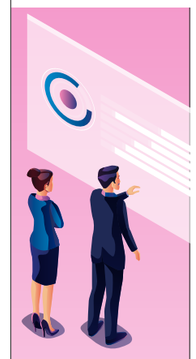
JAK ZACZĄĆ? CO JESZCZE JEST WAŻNE?

Z punktu widzenia rozpoczęcia projektu chmurowego jednym z pierwszych kroków jest opracowanie i przedstawienie strategii technologicznej organizacji (często strategii *cloud)* będącej rozwinięciem lub kontynuacją strategii biznesowej organizacji. Powinny one mieć zbliżone, a często tożsame fundamenty i na pewno nie być przeciwstawne. Nadrzędne i wspólne cele są kluczem do powodzenia. Następnie konieczne jest przeanalizowanie organizacji w zakresie posiadanych kompetencji i ewentualnie dojrzałości organizacyjnej w kontekście adaptacji chmury. Ciekawym podejściem jest analiza dojrzałości organizacyjnej uwzględniająca kilka obszarów.
Istotne z punktu widzenia technologii chmurowej jest także zbudowanie tzw. *Cloud Competency Center,* czyli centrum kompetencji chmurowych. Jest to obszar w organizacji (wykraczający poza silosy kompetencyjne IT), który zbierze posiadane kompetencje *cloud*, zinwentaryzuje je, a następnie będzie gotowy do opracowania i pozyskiwania nowej, specyficznej wiedzy, która umożliwi IT (przede wszystkim) operowanie w nowym modelu usługowym. Jest to także istotne z punktu widzenia zaadresowania szeroko pojętego HR, czyli pozyskania talentów (co w obecnej sytuacji na rynku pracy nie jest zadaniem łatwym), utrzymania posiadanych i modernizacji istniejących już kompetencji ludzi i zespołów. Tutaj także powinno nastąpić zaadresowanie obaw ludzi związanych z nadchodzącą, niewątpliwie dużą zmianą organizacyjną.

NAJLEPSZE PRAKTYKI, CZYLI DLACZEGO ZEWNĘTRZNE WSPARCIE JEST CZĘSTO NIEZBĘDNE

Z punktu widzenia banku i jego celów jako organizacji finansowej mamy do czynienia ze świadczeniem usług finansowych (i nie tylko) dla klientów. Jest to nadrzędny cel organizacji (stawiany wprost przez właścicieli, np. giełdę) – oczywiście nie bez znaczenia pozostają wymagania, takie jak wzmacnianie stabilności systemu finansowego danego kraju i/lub krytyczna rola organizacji zaufania publicznego. Upraszczając, z perspektywy biznesowej organizacja ma świadczyć usługi finansowe w sposób bezpieczny i pewny, a w zamian za to otrzymuje stosowne wynagrodzenie (od swoich klientów czy rynku), generując zysk dla właścicieli.
Do funkcjonowania tak złożonego przedsiębiorstwa potrzeba różnego rodzaju kompetencji i zasobów, także informatycznych. Bez wątpienia wiedza i kompetencje dotyczące chmury są niezbędne do wykonywania w obecnych czasach usług, które świadczą nowoczesne działy IT, ale każda organizacja powinna odpowiedzieć sobie na pytanie, czy lepiej pozyskać, nabywać i budować kompetencje, które będą potrzebne w danym momencie. Może też warto utrwalić te, które pomogą organizacji funkcjonować w nowym chmurowym modelu, a dla ograniczenia czasu, w którym następuje transformacja (migracja do chmury), posiłkować się zasobami zewnętrznymi, które w przyszłości nie będą już wykorzystywane w takim zakresie.
W PwC ze względu na specyficzną rolę niezależnego, agnostycznego (z punktu widzenia technologii i vendorów) dostawcy rozwiązań i usług profesjonalnych koncentruję się przede wszystkim na celu biznesowym organizacji. Dlatego uzasadnione pozostaje stwierdzenie, że migracja banku jako dużej, złożonej organizacji do chmury, która dzieje się prawdopodobnie raz na wiele lat, powinna być realizowana przede wszystkim najlepszymi zasobami, jakie są możliwe do pozyskania, z wykorzystaniem najlepszych specjalistów. Tutaj konieczne jest ograniczenie do minimum ryzyka, np. niedostępności systemów dla klientów czy utrata danych. Idąc dalej, zasoby (specjaliści, eksperci) posiadający specyficzną, często też unikalną wiedzę i co najważniejsze doświadczenie, niezbędne np. do przystosowania aplikacji do migracji (niezależnie, czy mówimy o migracji typu *lift & shift,* czy o głębokiej zmianie w samej strukturze aplikacji lub architekturze, czyli o reengineeringu), są wykorzystywane tylko raz w danym momencie albo projekcie.
Sama chmura, bez kontekstu i uzasadnienia biznesowego, nie niesie większej wartości. Natomiast chmura z efektem biznesowym może podnieść naszą organizację do poziomu, jakiego konkurencja nie będzie mogła osiągnąć, a na pewno nie tak szybko.
Pozyskanie najlepszych specjalistów, ekspertów z rynku jest obecnie wyjątkowo kosztowne i trudne. Następnie taki zasób potencjalnie nie będzie już wykorzystywany w pełnym zakresie swoich specyficznych kompetencji. Dlatego też najrozsądniejsze kosztowo, ale także technologicznie, pozostaje korzystanie z zewnętrznych zasobów firm specjalizujących się w takich pracach, a następnie zdobycie niezbędnej wiedzy przez zespoły banku. Równie istotne jest wykorzystanie specyficznych, gotowych i unikalnych metodyk stosowanych choćby przez PwC, które zostały wypracowane przez lata doświadczeń oraz często setki zrealizowanych z sukcesem projektów. To kolejny element, który przynosi wymierne korzyści – czas i bezpieczeństwo. Model ten jest zarówno optymalny kosztowo (w dłuższej perspektywie), jak i potencjalnie najszybszy w implementacji. To stanowi ogromną zaletę zwłaszcza w czasie niewątpliwego wyścigu technologicznego, jaki trwa na rynku, i konkurencji realizującej podobne działania prawdopodobnie w tym samym czasie, pozyskującej ekspertów z tego samego rynku co my.
Nie bez znaczenia jest fakt posiadania choćby takich zasobów, jak zespół ekspertów i praktyków PwC, mających pełne spektrum kompetencji – począwszy od budowania strategii, poprzez technologie, a skończywszy na obszarach bezpieczeństwa i regulacji prawnych.

Chmura (jako sama technologia) jest składnikiem koniecznym, ale tylko jednym z wielu w procesie transformacji. Często też jest katalizatorem większych zmian następujących w obszarze biznesu



Podsumowując, chmura stała się krytycznym filarem projektów informatycznych każdego banku. Rozwiązania chmury prywatnej (uruchomionej w data center banku lub dedykowanych, wydzielonych galwanicznie lub logicznie zasobów u dostawcy chmurowego), a zwłaszcza chmury publicznej (realizowanej także coraz częściej w modelu *multicloud*, w którym wykorzystywani są określeni dostawcy do określonych zastosowań) stały się odpowiedzią na większość wymagań technicznych stawianych zespołom IT przez biznes.

Zdezaktualizowały się dyskusje dotyczące tego, czy chmura jest mniej bezpieczna niż rozwiązania *on-premises.* Uprawniona i nadal w mocy pozostaje polemika dotycząca zarządzania bezpieczeństwem w chmurze i zabezpieczania zgodności regulacyjnej dla implementacji chmury. Równie ważne są dyskusje dotyczące tzw. *cloud economy.* U podstaw stoi przede wszystkim wymaganie biznesowe, które determinuje działania i bardzo często alokuje zasoby finansowe w dany projekt.

Dlatego tak ważne pozostają pryncypia, które powinny wskazywać chmurę nie jako projekt, ale PROGRAM. To coś znacznie szerszego i większego, dotyczące i wpływające na każdy bez wyjątku obszar firmy. Dlatego tym bardziej warto go realizować z najlepszymi specjalistami, cechującymi się przede wszystkim agnostycznością, doświadczeniem, praktyką i gotowymi metodykami. Tylko zespół mający takie atuty może zagwarantować, że wdrożenie będzie szybkie, efektywne kosztowo i technologicznie, a przede wszystkim zapewni oczekiwany efekt biznesowy.

Raport „Transformacja banku do chmury" jest dostępny stronach miesięcznika „BANK", https://alebank.pl/banki-z-glowa-w-chmurach-ale-nogami-twardo-na-ziemi/?id=393352&catid=630&cat2id=361

Chmura hybrydowa pomoże dużym bankom

zwiększyć bezpieczeństwo, obniżyć koszty i poprawić funkcjonowanie

Dla dużych banków mających lokalne oddziały w różnych częściach kraju lub świata zarządzanie rozproszonymi, starszymi systemami zabezpieczeń staje się coraz bardziej problematyczne. Do najważniejszych wyzwań należą stale zmieniające się zagrożenia, brak zasobów informatycznych i kurczące się budżety. Chcąc temu zaradzić, coraz więcej instytucji finansowych rozważa migrację systemu monitoringu wizyjnego do chmury hybrydowej.

Duże banki mają do czynienia z inwestycjami, przychodami i oszczędnościami o bardzo dużej wartości. Zarządzają również ogromnymi ilościami informacji prywatnych, w tym danymi przechwytywanymi przez ich fizyczne systemy zabezpieczeń. Obecnie stoją też przed wyzwaniami związanymi z ewoluującymi cyberzagrożeniami, rosnącymi kosztami IT i zarządzaniem ogromną ilością danych. Wyzwania te są często jeszcze większe, gdyż banki borykają się z problemem współpracy różnych technologii i procesów.
Wiele banków nadal korzysta z rozproszonych, starszych narzędzi zaprojektowanych z myślą o specyficznych potrzebach różnych działów. Niektóre z nich mają nawet 1000 różnych aplikacji w swoich sieciach. Te starsze narzędzia i tworzone przez nie silosy utrudniają bankom ochronę przed rosnącymi zagrożeniami cybernetycznymi, redukcję kosztów IT, a także wykorzystanie danych i analityki w celu usprawnienia pracy.

POSTĘPUJĄCE CYBERZAGROŻENIA

Sektor bankowy jest obecnie głównym celem ataków cybernetycznych. Prawdopodobieństwo, że stanie się celem cyberprzestępców, jest 300 razy większe niż w przypadku jakiejkolwiek innej branży. W 2020 r. banki doświadczyły ponad 3400[1] udanych ataków. Według IBM i Ponemon Institute, średni koszt naruszenia danych w sektorze finansowym w 2021 r. wyniósł 5,72 mln USD[2].

Jest to również branża najbardziej dotknięta przez oprogramowanie ransomware. W porównaniu z pierwszą połową 2020 r., w analogicznym okresie 2021 r. banki na całym świecie doświadczyły znacznego wzrostu ataków ransomware o 1318%[3] rok do roku. W 2021 r. usuwanie skutków oprogramowania ransomware kosztowało świat 20 mld dolarów[4]. Przewiduje się, że do 2031 r. kwota ta wzrośnie do 265 mld dolarów[5].
Należy pamiętać, że chociaż ataki te prowadzą do natychmiastowej utraty przychodów, mogą także być przyczyną strat w przyszłości. Negatywny wpływ udanego ataku na reputację banku może zagrozić zaufaniu klientów, wartościom akcjonariuszy i potencjalnym przyszłym zyskom. Ograniczanie tego ryzyka może być również kosztowne. Szacuje się, że do 2027 r. wydatki na szkolenia z zakresu cyberbezpieczeństwa osiągną poziom 10 mld dolarów[6]. Aby nadążyć za stale zmieniającymi się zagrożeniami i ryzykiem, banki muszą wdrażać innowacyjne rozwiązania, które pomogą im chronić swoje dane i planować przyszłe potrzeby.

OBNIŻANIE KOSZTÓW IT

W czasach, gdy duże banki wprowadzają bankowość cyfrową i stają w obliczu coraz częstszych ataków cybernetycznych, od działów bezpieczeństwa oczekuje się bardziej inteligentnej pracy przy zmniejszonym budżecie. Cięcie kosztów stało się priorytetem, ponieważ banki starają się modernizować swoje systemy.
Jednym z głównych problemów, z jakimi borykają się działy bezpieczeństwa i IT, jest fakt, że ich dotychczasowe systemy są zarówno nieefektywne, jak i kosztowne w utrzymaniu. Banki wydają zazwyczaj około 75% swoich budżetów informatycznych na utrzymanie starszej architektury, a zespoły informatyków tracą czas i pieniądze na utrzymanie i modernizację równoległych systemów. Modernizacja do nowoczesnego systemu zabezpieczeń może pomóc w obniżeniu kosztów utrzymania, jednak bez solidnej strategii banki ryzykują wprowadzenie nowych luk w zabezpieczeniach. Wykorzystanie nowych technologii, które usprawniają działania i zwiększają wydajność, może pomóc w obniżeniu kosztów IT, ale tylko wtedy, gdy sieci nie są narażone na zwiększone ryzyko. Mając to na względzie, należy szukać skalowalnych rozwiązań, które oferują możliwość bezpiecznego integrowania najnowszych technologii w miarę pojawiających się potrzeb.

SENSOWNE WYKORZYSTANIE DANYCH

Dla dużych banków wyprzedzanie konkurencji oznacza wykorzystywanie danych do badania incydentów, dostarczania informacji o klientach i usprawniania działalności oddziałów. Również w tym przypadku starsze narzędzia i wynikające z nich silosy mogą stwarzać niepotrzebne i kosztowne wyzwania. Po pierwsze utrudniają one dostęp do niezbędnych danych z systemów bezpieczeństwa i ich pozyskiwanie. Po drugie wyszukanie dowodów incydentów może stać się logistycznym koszmarem.
Gdy w oddziale dochodzi do incydentu, pracownicy ochrony muszą przeszukiwać godziny nagrań wideo z wielu kamer, aby zidentyfikować i zebrać potrzebny materiał. Proces ten może być jeszcze trudniejszy i bardziej czasochłonny, jeśli dochodzenie wymaga skorelowania danych z różnych systemów, w tym telewizji dozorowej i kontroli dostępu lub przejrzenia danych z wielu oddziałów.
W przypadku rozbieżności systemów wyodrębnianie nagrań wideo na potrzeby śledztwa jest zarówno pracochłonne, jak i podatne na błędy ludzkie. Aby obniżyć koszty, bankom potrzebne są narzędzia, które zautomatyzują i usprawnią procesy, dzięki czemu zespoły ds. bezpieczeństwa będą mogły szybciej zamykać dochodzenia.
Szybsze zamykanie dochodzeń usprawnia działalność operacyjną, ale te same dane dotyczące bezpieczeństwa mogą być też wykorzystane do pomocy klientom. W ramach swoich nowych ofert banki starają się podnieść jakość obsługi klienta. W tym celu potrzebują łatwego dostępu do danych, aby lepiej zrozumieć potrzeby swoich klientów i efektywnie świadczyć usługi. Dalsze stosowanie podejścia silosowego utrudnia dostęp do różnych danych i ich korelację. W ostatecznym rozrachunku może to mieć negatywny wpływ na zdolność banku do świadczenia konkurencyjnych usług.

CZAS NA MODERNIZACJĘ

Duże banki zdają sobie sprawę z wyzwań, jakie stawiają przed nimi silosowe, starsze systemy. Wiedzą też, że nadszedł czas na modernizację. Chcąc sprostać wymaganiom związanym z coraz bardziej złożonymi zagrożeniami i osiągnąć większą wydajność operacyjną, wiele z nich sięga po narzędzia przeznaczone do jednego celu, aby rozwiązać konkretne, krótkoterminowe problemy. Niestety rezultatem takiego podejścia jest często zbiór systemów, które nie zostały zaprojektowane do wspólnej pracy.
Zamiast wdrażać rozwiązania krótkoterminowe, aby stawić czoła obecnym i przyszłym wyzwaniom, banki muszą zastanowić się nad fundamentami swojego systemu zabezpieczeń. Muszą także rozważyć zdolność systemu do ewolucji w celu spełnienia przyszłych potrzeb w zakresie bezpieczeństwa i działalności operacyjnej. Przede wszystkim system zabezpieczeń powinien pomagać w przełamywaniu silosów, a nie ich powielaniu. Zwykła integracja nowych narzędzi nie rozwiązuje silosowego podejścia, ponieważ zespoły ds. bezpieczeństwa nadal muszą przeskakiwać między wieloma systemami, które nie zostały zaprojektowane z myślą o tej funkcjonalności.
Odejście od silosów będzie wymagało od dużych banków przyjęcia podejścia hybrydowego, obejmującego ujednolicenie systemów i przejście do chmury. Ujednolicona platforma zapewni spójny poziom ochrony cybernetycznej we wszystkich oddziałach, usprawni działalność operacyjną poprzez centralne zarządzanie bezpieczeństwem oraz zwiększy efektywność poprzez obniżenie kosztów aktualizacji i konserwacji, które są nieodłącznym elementem zintegrowanych narzędzi. Ponadto dzięki wdrożeniu w chmurze rozwiązań z wbudowaną analityką banki będą mogły lepiej chronić swoje dane przed uszkodzeniami sprzętu i kradzieżą, a także uzyskiwać użyteczne informacje, które pomogą utrzymać sprawne funkcjonowanie oddziałów.

WDRAŻANIE UJEDNOLICONEJ INFRASTRUKTURY HYBRYDOWEJ CHMURY OBLICZENIOWEJ

Infrastruktura sieciowa stanowi kręgosłup każdego systemu zabezpieczeń i pomaga chronić przed zagrożeniami zewnętrznymi. Bez jej starannego planowania dążenie

[1] https://www.genetec.com/industries/banking
[2] https://www.ibm.com/security/data-breach
[3] https://newsroom.trendmicro.com/2021-09-14-Attacks-Surge-in-1H-2021-as-Trend-Micro-Blocks-41-Billion-Cyber-Threats
[4] https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/
[5] https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/
[6] https://fortunly.com/statistics/data-breach-statistics/#gref

do modernizacji infrastruktury sieciowej może narazić banki na nowe zagrożenia. Gdy są gotowe do migracji do ujednoliconego systemu bezpieczeństwa, konieczne jest opracowanie kompleksowego planu.

Samo dodanie nowych urządzeń do systemu zabezpieczeń może sprawić, że duże banki staną się bardziej podatne na ataki cybernetyczne. Z tego powodu niezbędne są rozwiązania opracowane specjalnie z myślą o bezpieczeństwie typu end-to-end i ochronie prywatności w fazie projektowania. Ponadto banki powinny poszukiwać rozwiązań, które można wdrożyć w chmurze. W przypadku korzystania z ujednoliconej platformy przejście do chmury ułatwia dostęp do danych dotyczących bezpieczeństwa, ich zabezpieczanie i zarządzanie nimi. Pomaga to obniżyć koszty fizycznego przechowywania danych w małych oddziałach i zwiększyć zarówno wydajność, jak i inteligencję.

ZNACZENIE UJEDNOLICENIA

Naruszenie bezpieczeństwa wynikające z niewłaściwego zabezpieczenia urządzenia lub nadużycia uprzywilejowanego dostępu może kosztować miliony dolarów i bezpośrednio wpłynąć na reputację marki. Duże banki potrzebują rozwiązań, które oferują scentralizowany monitoring, zapewniający większą kontrolę nad zarządzaniem systemami zabezpieczeń w całej organizacji.

Dzięki ujednoliconej platformie bezpieczeństwa, obejmującej kontrolę dostępu, dozór wizyjny, automatyczne rozpoznawanie tablic rejestracyjnych, wykrywanie włamań i analitykę w ramach jednego intuicyjnego interfejsu banki mogą monitorować urządzenia i uzyskać pełną „widoczność" oddziałów bez zakłócania działalności. Pracownicy ochrony mogą odbierać na żywo alarmy wraz z obrazem wideo z miejsca alarmu i szybko weryfikować, czy incydent wymaga reakcji – bez konieczności przełączania między wieloma systemami. Zapewnione jest również spójne, szybkie i skuteczne reagowanie na zagrożenia dzięki standardowym procedurom operacyjnym (SOP), które prowadzą zespoły bezpieczeństwa przez incydenty w czasie rzeczywistym.

Ujednolicona platforma bezpieczeństwa z wbudowanymi narzędziami do automatyzacji pozwala również zachować czujność wobec słabych punktów systemu dzięki monitorowaniu jego stanu i automatycznej konserwacji. Narzędzia te działają bezgłośnie w tle, monitorując stan i kondycję poszczególnych komponentów systemu. Wysyłają też powiadomienia o nowych aktualizacjach produktów oraz umożliwiają automatyczne pobieranie i instalowanie aktualizacji zgodnie z harmonogramem lub wtedy, gdy pozwala na to czas.

WYKORZYSTANIE CHMURY HYBRYDOWEJ DO POPRAWY JAKOŚCI DANYCH

W przypadku dużych banków sztuczna inteligencja oparta na danych ma kluczowe znaczenie dla usprawnienia dochodzeń i poprawy obsługi klienta. Praca z infrastrukturą hybrydową i rozwiązaniami opartymi na chmurze z wbudowaną analityką ułatwia dostęp do danych z wielu systemów i ich korelację. A to oznacza większe bezpieczeństwo i lepszy wgląd w sytuację.

Ujednolicona platforma może automatycznie łączyć strumienie wizyjne z kamer i inne dane, m.in. z systemu kontroli dostępu, co skraca czas potrzebny na znalezienie i skorelowanie informacji oraz eliminuje błędy ludzkie. Następnie wraz z opartym na chmurze rozwiązaniem do zarządzania dowodami ujednolicona platforma może wspomóc pracowników ochrony i organy ścigania podczas prac dochodzeniowych po zdarzeniu, zapewniając centralny punkt kontaktowy.

Oprócz uproszczenia dochodzeń rozwiązanie do zarządzania dowodami, ułatwiające zarządzanie i przeglądanie nagrań wideo oraz udostępnianie zaszyfrowanych plików organom ścigania, pozwala również zmniejszyć koszty związane z kopiowaniem dowodów na płyty DVD. Ponieważ system ten może przeszukiwać i korelować strumienie wizyjne i inne dane ze wszystkich oddziałów i placówek korporacyjnych, banki mogą korzystać z systemu zarządzania dowodami w chmurze, aby uprościć proces dowodowy w przypadku zaangażowania wielu lokalizacji.

Kolejną zaletą migracji do infrastruktury chmury hybrydowej jest uzyskiwanie informacji, które usprawniają obsługę klienta. Analityka może obejmować sprawdzanie liczby osób odwiedzających daną placówkę w danym czasie, określanie, jak długo klienci czekają w kolejce czy w jaki sposób odbywa się ruch pieszych w różnych miejscach. Gdy duże banki mają dostęp do swoich danych dotyczących bezpieczeństwa, mogą wdrażać strategie organizacyjne i kadrowe, które skracają czas oczekiwania i ułatwiają przepływ osób w oddziałach. W ostatecznym rozrachunku odblokowanie tych informacji pomaga bankom wyprzedzić konkurencję.

OCHRONA BANKÓW TERAZ I W PRZYSZŁOŚCI

Duże banki muszą spojrzeć na swoje systemy zabezpieczeń jak na coś więcej niż tylko zbiór narzędzi. Zamiast tego muszą postrzegać je jako sposób na usprawnienie operacji i uzyskanie większego wglądu w sytuację. Osiągnięcie tego celu wymaga starannego przemyślenia i podejścia hybrydowego, które obejmuje ujednolicenie systemów i przejście do chmury.

Więcej informacji o tym, jak Genetec może pomóc dużym bankom we wdrożeniu hybrydowej infrastruktury chmurowej dla ich systemów zabezpieczeń, można znaleźć w ofercie rozwiązań Genetec dla sektora bankowego[7] oraz na dedykowanej stronie internetowej[8] poświęconej temu sektorowi.

[7] https://www.genetec.com/industries/banking/portfolio
[8] https://www.genetec.com/industries/banking

GENETEC

2280 Alfred-Nobel Blvd.
Montreal, Canada H4S 2A4
www.genetec.com
jkozak@genetec.com

Hotel po pandemii

Hubert Żak

Sektor HoReCa[1] jest jednym z najmocniej dotkniętych zmianami, jakie przyniosła pandemia koronawirusa dla gospodarki. Straty poniesione z tytułu spadku przychodów, wzrost kosztów operacyjnych oraz brak amortyzacji zapewne jeszcze długo będą spędzać sen z powiek zarządzającym.

Aby znaleźć odpowiedź na pytanie, jak bardzo zmiany wpłynęły na poziom bezpieczeństwa obiektów hotelowych, należy spojrzeć na ten obszar z zupełnie innej perspektywy niż przed okresem pandemii COVID-19 oraz wojną w Ukrainie.

Bezpieczeństwo w hotelach znacznie zmieniło się w wielu podobszarach – przeobrażeniu uległa struktura bezpieczeństwa, zmienił się sprzęt oraz instrukcje i procedury opracowane lub zmodyfikowane w odpowiedzi na nową sytuację gospodarczą. Rynek hotelarski został zmuszony do szybkiej adaptacji do nowego rodzaju zagrożeń. Potencjalna utrata przychodu wymusiła zmianę podejścia do wdrożenia często autorskich rozwiązań w zakresie paneli kryzysowych i nowych procedur już w pierwszym okresie pandemii.

Wraz z postępującymi zmianami gospodarczymi aktualizacjom podlegały także rozwiązania proceduralne. Proces ich dostosowywania uwzględniał najnowsze informacje dotyczące stale zwiększającego się wymaganego poziomu zabezpieczeń, publikowanego przez instytucje rządowe. Nieco więcej czasu zajęła odpowiednia implementacja sprzętu niezbędnego do sprostania nowym wymogom, w tym instalacja kamer termowizyjnych, analityki, urządzeń i systemów dezynfekcyjnych czy punktów kontroli zabezpieczeń stref wydzielonych. W kolejnych okresach widoczne były coraz większe zmiany w zakresie hotelowych systemów dedykowanych bezpieczeństwu w obszarach pandemicznych.
Aby ograniczyć ryzyko całkowitego lub czasowego zamknięcia obiektu hotelowego w okresie pandemii, zwrócono się do ekspertów i producentów zabezpieczeń z pytaniem, w jaki sposób zoptymalizować koszty związane z bezpieczeństwem, by sprostać nowym wyzwaniom, w pełni przestrzegając wymogów dotyczących ograniczenia liczby gości oraz przepisów sanitarnych i innych wymogów epidemiologicznych.

Zaproponowane rozwiązania, zwłaszcza w pierwszym okresie pandemii, koncentrowały się na wsparciu technicznym i proceduralnym. Oferowane usprawnienia wiązały się z koniecznością poniesienia niemałych kosztów, co w okresie pandemicznym było dla hoteli sporym wyzwaniem. Aby temu sprostać, skupiono się na doposażeniu obiektów w urządzenia niezbędne, w tym rozwiązania techniczne m.in. w zakresie pomiaru temperatury oraz dostosowania i uszczegółowienia procedur dezynfekcyjno-epidemiologicznych. Najważniejszą rzeczą stało się właściwe wdrożenie procedur wspierających codzienną pracę obiektu, spośród których należy wymienić spersonalizowane instrukcje dla następujących obszarów:

- dział F&B,
- dział obsługi i recepcji,
- dział housekeepingu,
- dział maintenance & service,
- dział techniczny.

Konieczne było również wypracowanie zasad współpracy z gośćmi hotelowymi, a także dostawcami wszelkich niezbędnych dla hoteli produktów. Nowe podejście do wykonywanych działań i pracy operacyjnej okazało się konieczne do utrzymania właściwego funkcjonowania obiektów hotelowych.
Po okresie stabilizacji cen oraz dopasowania dedykowanych rozwiązań technicznych doposażono obiekty hotelowe w urządzenia zwiększające i zapewniające wystarczające standardy do właściwego funkcjonowania i dostosowania w okresie pandemii. Wśród głównych systemów zainstalowanych lub zmodyfikowanych na potrzeby postpandemicznych przepisów znalazły się następujące:

- analityka systemowa CCTV, szczególnie dotycząca zliczania osób w poszczególnych strefach, uwzględniająca konieczność limitowania liczby osób w danym obszarze;
- pełna analiza danych polegająca na stałym, reaktywnym pomiarze temperatury obiektów oraz przemieszczaniu się w wyznaczonych, monitorowanych obszarach;
- wyznaczenie dodatkowych punktów kontroli systemowej, opartych m.in. na wirtualnych barierach, analizie ruchu czy przydziale obiektu do poszczególnych stref;
- analiza otagowanych obiektów w zakresie wykonania wszystkich etapów kontrolnych w poszczególnych strefach.

Zmiany te zostały dopasowane w sposób autorski i indywidualny w zależności od obiektu hotelowego. Na ich formę miały wpływ możliwości sprzętowe oraz uwarunkowania architektoniczne, pod uwagę wzięto także części wspólne hotelu oraz obiektowe ciągi komunikacyjne. Część hoteli wdrożyła pełen zakres rozwiązań umożliwiających w pełni bezpieczną i zgodną w przepisami pracę operacyjną. Inne ograniczyły się do spełnienia niezbędnych wymogów sanitarnych, wprowadzając rozwiązania proceduralne wspomagane dodatkowymi zabezpieczeniami, takimi jak mobilny pomiar temperatury.

W okresie pandemii i po jej zakończeniu hotele podchodziły do zakresu zmian jednostkowo, opierając się na zaleceniach ekspertów i doradców ds. bezpieczeństwa oraz rekomendacjach rządowych w zakresie ustaw, przepisów i rozporządzeń. Brak zunifikowanych rozwiązań wpłynął na jakość i wielkość zastosowanych zmian. Bezpośredni wpływ miały przy tym ogromne koszty poniesione z tytułu braku przychodów w okresie całkowitego lub częściowego zamknięcia.
Po ustaniu pandemii koronawirusa w części sektora hotelarskiego można zauważyć znaczące zmiany. Niektóre hotele zostały dostosowane w maksymalny możliwy i dostępny rynkowo sposób zarówno w obszarze zakupu i wprowadzenia do użytku wskazanych powyżej rozwiązań sprzętowych, jak i nowych spójnych procedur pozwalających na wyeliminowanie zagrożenia dla prawidłowego funkcjonowania obiektu.

Część hoteli dostosowała model swojej pracy do ogólnych procedur i rekomendacji – trudno wskazać, które z tych rozwiązań było lepsze. Fakt braku zamknięcia obiektów dużych sieci nasuwa wnioski, że każde z tych rozwiązań było dobre, o ile było zaimplementowane oraz realizowane w sposób właściwy.
Analizując dane rynkowe, można z przekonaniem powiedzieć, że poziom bezpieczeństwa w sektorze hotelarskim podniósł się, szczególnie w obszarach związanych z realizacją procedur oraz doposażenia obiektów w dodatkowy sprzęt, który można wykorzystać nie tylko w czasie pandemii, ale także w codziennej rzeczywistości, w której jest kolejnym elementem zapewniającym pełne bezpieczeństwo usług.

[1] HoReCa – hotele, restauracje, kawiarnie

HUBERT ŻAK

Ekspert ds. bezpieczeństwa i techniki zabezpieczeń, menedżer projektów. Wieloletni pracownik służb, od kilkunastu lat związany z bezpieczeństwem biznesu, szczególnie z zarządzaniem kryzysowym, prewencją, zapobieganiem zagrożeniom i bezpieczeństwem publicznym. Współpracuje z korporacjami międzynarodowymi i instytucjami rządowymi, gdzie odpowiada za nowe rozwiązania w systemach bezpieczeństwa oraz specjalistyczne szkolenia.

Recepta na sprawne funkcjonowanie hotelu

Branża turystyczna i powiązana z nią branża hotelarska są jednymi z najszybciej rozwijających się w naszym kraju. Niestety należą jednocześnie do najbardziej narażonych na skutki globalnych zmian, kryzysów czy niepokojów. Początek pandemii w Polsce drastycznie dotknął właścicieli hoteli, którzy musieli na pewien czas zamknąć lub w znacznym stopniu ograniczyć działanie swoich biznesów. Poskutkowało to zamrożeniem często jedynych źródeł dochodów dla wielu pracujących i ucieczką siły roboczej do innych branż.

Krzysztof Mika

Początek 2022 r., w związku z kończącą się pandemią COVID-19, pozwalał patrzeć z optymizmem na szansę odbudowania branży, tymczasem dzień rozpoczęcia wojny w Ukrainie zmusił wszystkie osoby działające w branży turystycznej do ponownej weryfikacji planów. Oprócz krajów bezpośrednio zaangażowanych w wojnę, największy niepokój pojawił się w państwach bezpośrednio graniczących z obszarem działań wojennych, takich jak Polska. Skutki agresji Federacji Rosyjskiej w lutym wymusiły całkowitą zmianę podejścia zwłaszcza właścicieli hoteli, którzy po raz kolejny musieli się dostosować do nowych warunków, by móc świadczyć swoje usługi w sposób bezpieczny dla gości i pracowników.

Okres pandemii wymusił wiele nowych inwestycji umożliwiających dalsze korzystanie z tak ważnych dla wszystkich usług noclegowych, w tym zakup środków dezynfekujących, zachowanie dystansu w kontaktach międzyludzkich czy też sprawny i zautomatyzowany pomiar temperatury ciała, np. z wykorzystaniem dedykowanej do tego kamery. Obecne wyzwania wymagają znacznie szerszego spojrzenia na bezpieczeństwo i komfort gości. Obawa turystów przed przyjazdem do krajów bezpośrednio graniczących z Ukrainą jest spora, przez co perspektywy dla branży w obecnym sezonie nie są najlepsze.

Obywatele Ukrainy bardzo chętnie odwiedzali nasz kraj w celach turystycznych, będąc najliczniejszą grupą po obywatelach Niemiec. Powstałej luki z tym związanej nie da się łatwo wypełnić, a jedną z metod jest zadbanie o najwyższe standardy dla gości hotelowych. W tym na szczęście przychodzi z pomocą technologia, która szybko dostosowuje się do aktualnych wymagań.

Systemy monitoringu wizyjnego zawsze odgrywały w hotelach duże znaczenie. Kamery od początku potrafiły „patrzeć” na to, co się dzieje w hotelu, odpowiednio reagować na zagrożenia czy nietypowe sytuacje wymagające interwencji obsługi lub ochrony. Przez lata producenci koncentrowali się na poprawie jakości przetwarzanego obrazu, co ułatwia ich obsługę i weryfikację nagrań. Zmieniający się świat sprawił, że kamery nauczyły się nie tylko „patrzeć”, ale również „widzieć i rozumieć” obraz znajdujący się w ich zasięgu.

Największy wpływ na obecne możliwości ma rozwój tzw. sztucznej inteligencji, dzięki której producent jest w stanie nauczyć kamerę, np. rozróżniać postać człowieka od samochodu lub innych obiektów i reagować tylko na określone zdarzenia, na których nam zależy. To ogromne odciążenie pracy operatorów, ograniczające liczbę fałszywych alarmów do minimum. Dzięki temu jest im łatwiej zareagować na zdarzenia wymagające natychmiastowej interwencji lub wyszukania potrzebnego nagrania.

Zaawansowana analiza obrazu dostępna we współczesnych kamerach pozwala na wiele więcej. W branży hotelowej świetnie przyjęła się możliwość odczytu przez kamery tablic rejestracyjnych pojazdów. Klient, podając numer rejestracyjny w momencie dokonywania rezerwacji, bez problemów wjedzie na teren hotelowy oraz wyjedzie bez ograniczeń pod względem liczby w okresie wykupionego pobytu. To bardzo wygodne rozwiązanie, które nie wymaga pobierania karty parkingowej i pozostawia pozytywne wrażenie już w chwili przyjazdu.

Ponadto współczesne systemy dozoru wizyjnego bez problemu monitorują liczbę wolnych miejsc na parkingach (zewnętrznych i wewnętrznych), oferując dodatkowe możliwości, np. wyświetlenie informacji o miejscu zaparkowania pojazdu. Obraz z kamer systemu parkingowego jest rejestrowany w sposób ciągły i może być ważnym dowodem w sytuacji zarysowania lub innego uszkodzenia pojazdu.

Kolejną chwaloną technologią, która jeszcze do niedawna nie była często spotykana, jest możliwość obserwacji obrazu w kolorze już nie tylko w dzień, ale również w nocy, niezależnie od panujących warunków atmosferycznych czy oświetleniowych. Wprowadzenie przez firmę Hikvision technologii ColorVu zrewolucjonizowało rynek CCTV na świecie. Standardowe kamery, używając podczerwieni do oświetlania sceny w nocy, mogły przetwarzać jedynie obraz czarno-biały, przez co uzyskanie wyraźnego obrazu i dostrzeżenie szczegółów zwłaszcza podczas opadów czy też mgły było bardzo trudne. Obecne kamery dzięki zastosowaniu przetworników 1/1,2’’ o bardzo wysokiej czułości, a przede wszystkim dzięki aperturze F1.0 dostarczają kolorowy obraz przez całą dobę.

Dzisiaj hotele wykorzystują technologię również do wielu innych działań. Przykładem może być automatyczna kontrola kolejki informująca menedżera, gdy liczba osób oczekujących przekroczy ustalony limit i potrzebna jest dodatkowa osoba do wsparcia w recepcji. Innym rozwiązaniem ułatwiającym pracę hotelu są kamery liczące liczbę przebywających w nich osób, co pozwala mieć wiedzę nie tylko o zameldowanych gościach, ale również o liczbie wszystkich osób przebywających w budynku (np. w razie konieczności ewakuacji).

Dla pracowników ochrony, oprócz wspomnianej technologii AcuSense zmniejszającej liczbę fałszywych alarmów do minimum, ważne są takie funkcjonalności, np. alarm w sytuacji pozostawienia bagażu bez opieki przez określony czas, alarm reagujący na wejście osoby niepowołanej w strefę tylko dla obsługi czy też funkcje ochrony perymetrycznej z użyciem np. termowizji. Pozwala ona bezbłędnie zareagować na nieuprawnione wtargnięcie na teren. Kamery z funkcją rozpoznawania twarzy wiedzą, że osoba będąca pracownikiem ma prawo przebywać w danej strefie, co nie powoduje reakcji systemu. Wejście do pomieszczenia ochrony jest zabezpieczone systemem kontroli dostępu nie tylko na standardową kartę (którą można zgubić), ale również poprzez potwierdzenie jej zgodności z odciskiem palca i kodem dostępu lub porównanie rysów twarzy z zapisanym wzorcem. Gwarantuje to, iż w pomieszczeniu lub obiekcie przebywają tylko osoby posiadające do tego uprawnienia.

Współczesny system dozorowy dostarcza również nieocenione dla zarządcy hotelu dane statystyczne, np. informacje, w których częściach obiektu goście przebywają najczęściej, z jakich atrakcji najchętniej korzystają, nawet z podziałem na płeć i wiek. Wiele danych można również uzyskać nt. pracowników oraz sposobu wykonywanej przez nich pracy. Otrzymane statystyki pozwalają na ciągłe usprawnienia w działaniu hotelu, powiązane z łańcuchem dostaw i zarządzaniem kompetencjami pracowników.

Branża hotelowa przeżywa trudny okres, pojawiające się przed nią wyzwania zmuszają do częstego dostosowywania się do aktualnej sytuacji na rynku rodzimym oraz globalnym. Hikvision, światowy lider branży zabezpieczeń, jest pionierem w rozwoju technologii, dzięki którym hotele, ale również inne branże, są w stanie zagwarantować najwyższe standardy bezpieczeństwa i zaskakiwać swoich gości coraz nowszymi rozwiązaniami obsługi. Naszym zdaniem ogromne znaczenie ma szerzenie wiedzy o możliwościach współczesnych systemów, co staramy się czynić, publikując od lat artykuły w czasopiśmie „a&s Polska” oraz organizując liczne szkolenia prowadzone na terenie całej Polski, na które serdecznie zapraszamy.

Głos branży

MENEDŻEROWIE SECURITY W TAKICH OBIEKTACH, JAK HOTELE, INSTYTUCJE FINANSOWE CZY SZKOŁY STOJĄ DZIŚ PRZED NIE LADA WYZWANIAMI. DO ZADAŃ ZWIĄZANYCH Z ZAPEWNIENIEM BEZPIECZEŃSTWA GOŚCIOM, KLIENTOM CZY UCZNIOM DOSZŁY TEŻ TE ZWIĄZANE Z ZAGROŻENIAMI CYBERNETYCZNYMI.

Tomasz Smoczyk

C&C Partners

Sztuczna inteligencja podnosi poziom bezpieczeństwa

Zainstalowane systemy zabezpieczeń cechują się często dużym zróżnicowaniem ze względu na wykorzystanie różnych technologii pojawiających się na przestrzeni lat i adekwatnie do możliwości danego etapu rozbudowy obiektu. Czy właściciel, chcąc zwiększyć bezpieczeństwo i przenieść system na wyższy poziom, jest zmuszony wymienić wszystkie jego elementy? Nie, jeżeli skorzysta z nowoczesnego systemu zarządzania wideo VDG Sense, który jest otwarty na rozwiązaniach wielu producentów i łączy różne technologie. W ten sposób zapewnia wykorzystanie już funkcjonujących urządzeń, jednocześnie umożliwiając rozbudowę o nowoczesne elementy.

Tak elastyczne i ekonomiczne podejście pozwala na wzbogacenie funkcjonalne najstarszych systemów, w tym kamer analogowych czy funkcjonujących od wielu lat kamer IP. Algorytmy sztucznej inteligencji (AI) pozwalają m.in. zwielokrotnić wykładniczo wizyjną ochronę obwodową obiektów, odsiewając wiele fałszywych alarmów wywołanych np. przez opady atmosferyczne czy poruszające się cienie. W połączeniu z kamerami termowizyjnymi o zasięgu detekcji w granicach 200–1000 metrów taka ochrona obwodowa staje się efektywna i łatwa w zarządzaniu. Wynika to z tego, że operator wspomagany algorytmami AI obsługuje zdarzenia wyłącznie z kilku kamer, które zastąpiły kilkadziesiąt kamer wizyjnych, a z których obrazów i tak nie byłby w stanie obserwować.

Kolejna możliwość AI to m.in. wizyjna detekcja nietypowych zdarzeń. System umożliwia kategoryzację zdarzeń i obiektów w czasie rzeczywistym oraz szybkie filtrowanie materiału wideo na podstawie cech charakterystycznych. Rozwiązanie jest przeznaczone dla służb pracujących w obiektach szczególnie wrażliwych, takich jak lotniska, jednostki wojskowe, zakłady penitencjarne, stadiony, dworce itp. o ograniczonym dostępie.

Kluczowe są integracja i zarządzanie systemami bezpieczeństwa za pomocą platformy integracyjnej PSIM z certyfikacją CNBOP pozwalającą na sterowanie systemami przeciwpożarowymi SIUP. Dzięki powiązaniu systemu PSIM z innymi systemami zaimplementowanymi w obiekcie, takimi jak system sygnalizacji pożarowej czy system zarządzania produkcją, z systemem CCTV, system telewizji dozorowej staje się oczami operatora, a on sam w znormalizowanym interfejsie otrzymuje do wykonania krok po kroku zadania wg ustalonych procedur – bez szkodliwej uznaniowości. Tym samym bezpieczeństwo osób i obiektu osiąga niespotykanie wysoki poziom.

Barbara Podwysocka

PIH

Najważniejsze zadania w sektorze hotelowym

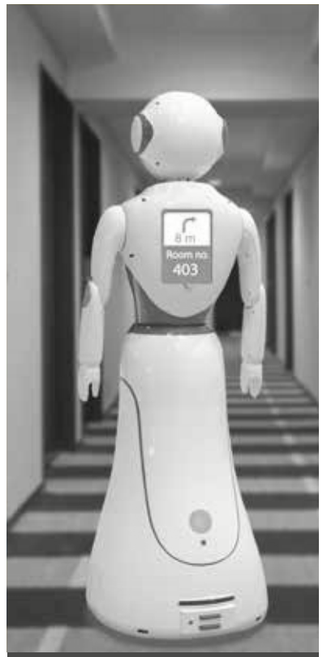
Działalność hotelowa jest branżą szczególnie podatną na czynniki rynkowe. Wszelkie zmiany zachodzące w sytuacji społecznej i gospodarczej na rynku zarówno krajowym, jak i międzynarodowym wpływają na popyt na usługi hotelowe i turystyczne.

Po bardzo dobrym roku 2019 kolejne lata i trwająca pandemia wpłynęły negatywnie na sytuację na rynku hotelarskim. Rok 2022 przy wyciszającej się pandemii miał być okresem ponownego ożywienia w turystyce i hotelarstwie. Niestety czynniki zewnętrzne, w tym m.in. wybuch wojny na Ukrainie, spowodowały, że nasze społeczeństwo zauważa inne zagrożenia, m.in. zagrożenie cybernetyczne i informacyjne.

Obecnie w grupie Polskiego Holdingu Hotelowego bardzo duży nacisk kładziemy na ochronę przed cyberatakami i zagrożeniami informacyjnymi. Goście hotelowi chcą czuć się bezpiecznie pod względem zarówno epidemicznym, jak i fizycznym czy cybernetycznym. Chcą mieć pewność, że załoga jest przygotowana na różne scenariusze kryzysowe, i potrafi udzielić szeroko rozumianej pomocy, dbając o ochronę danych osobowych z jednoczesnym zachowaniem prywatności.

Załoga w naszych hotelach i obiektach jest odpowiednio przeszkolona i wyczulona na każde nienaturalne zachowania bądź sytuacje odbiegające od standardowych. Szybko podejmuje odpowiednie działania, zachowując wszelkie środki bezpieczeństwa i pamiętając jednocześnie o trwającym zagrożeniu COVID-19. Wszystko po to, aby podczas pobytu gość mógł się czuć bezpiecznie.

Dla nas, hotelarzy, wartością nadrzędną jest dbałość o to, by każdy nasz gość mógł w pełni cieszyć się z jakości usług świadczonych przez hotel bez niepotrzebnego martwienia się o względy bezpieczeństwa czy zdrowia. Dlatego też dokładamy wszelkich starań, aby zapewnić odpowiedni komfort i bezpieczeństwo wszystkim osobom przebywającym w naszych obiektach.



Emil Zarzecki

mBank

Wyzwania sektora bankowego

Przed wybuchem wojny w Ukrainie wielu z nas nie wierzyło, że drastyczny scenariusz wojenny w Europie jest możliwy w XXI wieku. Mimo wysiłków dyplomatycznych ze strony państw Zachodu konfliktu nie udało się uniknąć, a w wyniku toczącej się wojny za naszą wschodnią granicą mapa zagrożeń dla naszego kraju zmieniła się diametralnie. Sektor finansowy także odczuwa skutki wojny w wielu wymiarach, w tym również w obszarze bezpieczeństwa. W wyniku toczącego się konfliktu pośrednio instytucje i firmy w naszym kraju oraz ich klienci coraz częściej stają się celem ataków hakerskich.

Ponadto obserwujemy znaczny wzrost oszustw z wykorzystaniem wyrafinowanych technik manipulacji, tzw. socjotechnik. Grupy przestępcze, które stoją za takimi działaniami, bardzo często wykorzystują umiejętności skutecznego oddziaływania na ludzką

psychikę, posługując się różnymi technikami manipulacji. Powtarzającymi się mechanizmami stosowanymi przy atakach socjotechnicznych jest powoływanie się na autorytet lub znajomości, wywołanie uczucia pilności tematu lub stresu u swojej ofiary, a czasem nawet jej zastraszanie. Potencjalne skutki skutecznych ataków socjotechnicznych na klientów to przede wszystkim straty finansowe, skompromitowane konta, wycieki danych, jak również możliwe straty wizerunkowe dla firmy, której ofiara jest klientem. Niemal codziennie w mediach pojawiają się informacje o wyłudzeniach metodami „na wnuczka", „na policjanta", „na pana z banku".
Taki obraz dzisiejszego świata powoduje, że menedżerowie uruchamiają programy szkoleniowe dla pracowników i klientów mające na celu podniesienie świadomości zagrożeń, tzw. *security awareness*. Odporność na ataki socjotechniczne zależy od poziomu świadomości każdego z nas. Dlatego skuteczny program szkoleń uświadamiających o tematyce rozpoznawania i reagowania na próby ataków socjotechnicznych skierowany do szerokiego grona adresatów jest moim zdaniem niezbędny.
Zauważalny jest także wzrost klasycznych środków operacyjnych do pozyskiwania informacji. W sferze cyberbezpieczeństwa wiele przedsiębiorstw jest bardzo dobrze zabezpieczonych, ale jeśli chodzi o kwestie kontrinwigilacyjne temat ten jest często ignorowany. Na popularnych portalach aukcyjnych można kupić w przystępnych cenach środki techniki inwigilacyjnej, które stanowią bardzo duże zagrożenie bezpieczeństwa informacji. I ten aspekt będzie się dynamicznie rozwijał w najbliższym czasie.

Bogumił Szymanek

Axis Communications

Bezpieczeństwo gości hotelowych

Systemy zabezpieczeń technicznych różnych obiektów zależą od ich charakterystyki w kwestiach przeznaczenia i rodzaju prowadzonej działalności. Dobór tego typu systemów zawsze powinien być poprzedzony oceną ryzyka. Zastosowane środki bezpieczeństwa muszą być adekwatne do zagrożeń.
Szczególnie interesujące jest zapewnienie odpowiednich systemów do obiektów hotelowych. Są to miejsca z natury otwarte na gości, ale istnieje też ryzyko pojawienia się osób niepożądanych.

Oczywiście należy zadbać o ogólne bezpieczeństwo obiektu, ale konieczne jest też połączenie działania wielu systemów – kamer, kontroli dostępu, systemu parkingowego, systemu rezerwacji, systemów oświetlenia i nagłośnienia. Oprócz typowych zagrożeń związanych z utratą mienia właściciel musi zapobiegać zdarzeniom, które mogą zmniejszyć wiarygodność hotelu i oceny gości. Skutki utraty wizerunku mogą być katastrofalne dla prowadzonego biznesu.
Wiele z tych potrzeb można zaspokoić za pomocą rozwiązań technicznych Axis Communications. W ramach spójnego interfejsu możliwe jest połączenie kamer i systemu kontroli dostępu, łatwo więc zarządzać dostępem do pomieszczeń i wyszukiwać zdarzenia na obrazie z kamer. Ponadto agregowane są również metadane pochodzące z kamer, takie jak rozpoznane tablice rejestracyjne, wykryte osoby czy pojazdy. Dzięki temu wyszukanie zapisu wideo konkretnego pojazdu albo osoby w ubraniu o określonej kolorystyce zajmuje kilka minut.
Kamery mogą pomagać w optymalizacji działania hotelu i przeciwdziałać zakłóceniom w pracy. Oprócz wykrywania podejrzanego zachowania osób, które np. zbyt długo przebywają w danej przestrzeni, możliwe jest automatyczne reagowanie na wiele innych zdarzeń. Obsługę dostaw na zapleczu usprawni wideodomofon z kontrolą dostępu. Za pomocą urządzeń audio lub syreny można dźwiękowo i wizualnie ostrzegać kierowców o osobach na drodze wewnętrznej. Ostrzeżemy też pieszych, jeśli przebywają w strefie ruchu pojazdów.
Blokowanie podjazdów przez zbyt długi postój może również zostać wykryte za pomocą kamery. Możliwe jest też wykrywanie zdarzeń dźwiękowych, np. krzyku czy dźwięku tłuczonego szkła.
Hotel to miejsce, gdzie liczą się estetyka i poczucie komfortu gości. Kamery Axis są dyskretne i łatwo wtopią się w architekturę obiektu. Systemy IP Audio zapewnią odpowiedni klimat muzyką w tle, jednocześnie umożliwiając przekazywanie komunikatów. Obsługa będzie też szybko poinformowana, że ktoś zbyt długo oczekuje w recepcji. Wymienione integracje systemów Axis zwiększają bezpieczeństwo oraz komfort gości i personelu. Zachowujemy nadal dużą elastyczność i otwartość na nowe potrzeby i pomysły. Działania te przekładają się na zwiększenie zadowolenia klientów i budują renomę hotelu na rynku.

Marcin Walczuk

BCS

Monitoring w szkole

Dzieci to nasza przyszłość i oczko w głowie każdego rodzica. Chcielibyśmy o nie dbać i chronić je na każdym kroku, co z oczywistych względów jest niemożliwe. W przedszkolu, szkole czy po zajęciach chcemy, aby w każdej sytuacji były bezpieczne.
Placówki edukacyjne, rozumiejąc potrzeby rodziców i chcąc zapewnić swoim podopiecznym możliwie najwyższy poziom bezpieczeństwa, od lat wykorzystują w tym celu elektroniczne systemy zabezpieczeń. Najbardziej użyteczne będą tutaj systemy kontroli dostępu, dzięki którym ograniczamy dostęp osobom postronnym, ale też mamy kontrolę nad tym, czy uczeń jest w szkole lub kiedy ją opuścił. Drugim systemem dbającym o bezpieczeństwo podczas pobytu uczniów w szkole będzie oczywiście monitoring wizyjny. Kamery wysokiej rozdzielczości zadbają o najwyższej jakości obraz, a rejestratory – o bezpieczne przechowywanie nagrań.
W ostatnich latach główną rolę w systemach CCTV zaczęła odgrywać analiza wideo, dzięki której możemy wskazać niepożądane zachowania, których chcemy na terenie placówki unikać i odpowiednio szybko być o nich informowani. Urządzenia BCS wyposażone w szereg funkcji zaawansowanej analizy wideo będą znakomitym narzędziem podnoszącym poziom bezpieczeństwa tych, którzy są dla nas najważniejsi, naszych dzieci.

Należy też wspomnieć o funkcji identyfikacji twarzy weryfikującej, czy dane dziecko jest uprawnione do wejścia na teren szkoły, a w połączeniu ze wspomnianym wcześniej systemem kontroli dostępu zapewnia możliwość podwójnej weryfikacji na wypadek „pożyczenia" sobie karty dostępu. Funkcja liczenia osób może dać informacje statystyczne o liczbie uczniów przebywających na terenie szkoły, a także pozwoli sprawdzić, np. w przypadku alarmu pożarowego, czy na pewno wszyscy opuścili strefę zagrożenia.
Funkcje określane jako ochrona obwodowa pozwolą zabezpieczyć teren przed dostępem osób z zewnątrz, np. w godzinach wieczornych, a jednocześnie poinformują odpowiednie osoby w przypadku wyjścia uczniów z placówki w godzinach lekcyjnych. Analiza zachowań z kolei pozwoli zawczasu wykryć niepokojące zachowania, np. gromadzenie tłumu, co może zapowiadać bójkę wśród uczniów.
Dzięki wykorzystaniu możliwości nowoczesnych systemów monitoringu wizyjnego można w dodatkowy sposób zadbać o bezpieczeństwo wszystkich osób przebywających na terenie placówek oświaty, zarówno uczniów, jak i grona pedagogicznego.

Krzysztof Mika

Hikvision Poland

Bezpieczeństwo i niezawodność

Zdecydowana większość ludzi odczuła skutki pandemii, z jakimi przyszło nam żyć już od ponad dwóch lat. Jedną z branż najbardziej dotkniętych jest hotelarstwo, którego ogromne nadzieje na odbudowanie po pandemii COVID-19 zostały mocno nadszarpnięte przez wojnę w Ukrainie. Polska, jako jeden z krajów w bezpośrednim sąsiedztwie i mocno zaangażowana we wsparcie, stała się dla wielu turystów z zagranicy krajem podwyższonego ryzyka, co negatywnie wpłynęło na plany wypoczynku w naszym kraju.
Ograniczona liczba gości oznacza, iż trzeba zrobić wszystko, aby to właśnie nasz hotel został wybrany. Jednym ze sposobów jest maksymalne zwiększenie bezpieczeństwa i komfortu, na co pozwala postęp technologiczny m.in. w dziedzinie telewizji dozorowej (CCTV). Systemy monitoringu wizyjnego musiały nauczyć się nie tylko patrzeć, ale także widzieć i – co najważniejsze – rozumieć to, co widzą. Dynamiczny rozwój licznych funkcji analitycznych, jakie można obecnie zaobserwować w kamerach, umożliwia automatyczne wykrycie, przeanalizowanie zagrożeń i poinformowanie ochrony tylko w sytuacji, gdy rzeczywiście dzieje się coś, co wymaga reakcji. Obecnie spotykane rozwiązania rozróżniają pojawiającą się ludzką sylwetkę czy też pojazd od innych obiektów, minimalizując tym samym fałszywe alarmy.
Otrzymany wyraźny obraz w kolorze, także w warunkach słabego oświetlenia, gwarantuje rejestrację szczegółów. Kamery termowizyjne natomiast pozwalają z dużej odległości wykryć intruza przeskakującego przez ogrodzenie niezależnie od warunków atmosferycznych.
Funkcja rozpoznawania twarzy zapewnia płynna analizę, czy np. w części obiektu przeznaczonej tylko dla pracowników nie znajdują się osoby nieupoważnione. Do tego dochodzą technologie znane już wcześniej, np. reakcja na wałęsające się osoby lub pozostawiony bez opieki bagaż i wiele innych. Bardzo ważna jest indywidualna analiza wymogów i cech każdego z obiektów, aby dobrane rozwiązanie spełniło swoje oczekiwania.

Daniel Kamiński

Smart-i

Obsługa gości hotelowych w chmurze

Większości osób wizyta w hotelu kojarzy się z szeregiem formalności oraz próbą cierpliwości. Na początku czekasz na zameldowanie. Otrzymujesz kartę dostępu, która może, ale nie musi działać z zamkiem drzwi do pokoju. W takiej sytuacji dostajesz drugą kartę i sugestię, abyś nie nosił jej z telefonem, bo się „rozkoduje". Dodatkowa wycieczka do recepcji, gdy zapomnisz zabrać karty z pokoju. Na koniec czekasz na wymeldowanie.
Doświadczam podobnych uciążliwości, jeżdżąc po Polsce w celu odwiedzenia klientów. Ale ostatnio zacząłem stawiać na wygodę i oszczędność czasu. Szukam hoteli lub apartamentów, które umożliwiają bezobsługowe zameldowanie oraz wymeldowanie, i mogę w nich korzystać z mobilnych poświadczeń, nie martwiąc się, że zapomniałem karty.
Takich gości musi być więcej, ponieważ tego typu usługi stają się modne. Za pomocą aplikacji można dokonać rezerwacji, uzyskać poświadczenia mobilne do systemu kontroli dostępu oraz rozliczyć się za pobyt. Klient, który ma już nadane poświadczenia, będzie szukał tej samej sieci hoteli w innych lokalizacjach. Tak poprzez wygodę buduje się lojalność klienta.
Jak to jest możliwe? Główną rolę odgrywa system kontroli dostępu pracujący w chmurze i obsługujący mobilne poświadczenia. Klienci identyfikują się za pomocą swoich telefonów i dzięki temu mają zawsze karty kontroli dostępu przy sobie. Wprowadza to spore oszczędności eksploatacyjne, bo każdy klient ma swoją kartę dostępu w telefonie.
Połączenie z systemem awizacji i rezerwacji odbywa się dzięki otwartemu API. Podobnie ma się rzecz, jeśli chodzi o integrację z systemami płatności, nawet Apple Pay. Dzięki usługom chmurowym wymiana danych jest szybka i pewna. Co więcej, podobnie działa integracja kamer nagrywających obraz w chmurze. Dzięki funkcjom centralnego zarządzania autoryzowani użytkownicy mogą przedłużać ważność poświadczeń w telefonach lub je anulować. Ponadto mogą uzyskać dostęp do wszystkich swoich kamer w różnych lokalizacjach przy użyciu tych samych danych uwierzytelniających. A gdy przydarzy się kradzież, szybko zidentyfikować, czy był to gość, czy pracownik.

Jak działa sztuczna inteligencja?

Sztuczna inteligencja rewolucjonizuje obszar bezpieczeństwa fizycznego: inteligentne, autonomiczne systemy zabezpieczeń, które zapobiegają potencjalnym incydentom. Nadchodzi kolejny etap ewolucji systemów gwarantujących szybsze, wydajniejsze i sprawniejsze działanie. Technologia bezpieczeństwa zasilona AI będzie działać predykcyjnie, głęboko zintegrowana z systemami obiektu.

Choć nadal obiekty są wyposażane w standardowe rozwiązania wspomagające bezpieczeństwo (niestety często wdrażane w silosach technologicznych bez połączenia z pozostałymi systemami), to już nowe produkty wyposażone w silniki sztucznej inteligencji (AI) oferują lepszą analizę danych, dzięki czemu mogą działać wydajniej i efektywniej wykorzystywać posiadane zasoby. Ewolucja techniki zapewniła uruchomienie automatycznych reakcji, które nie tylko przyspieszają operacje związane z bezpieczeństwem, ale także poprawiają wydajność operacyjną.

Kolejny etap związany z rozwiązaniami autonomicznymi wspomaganymi AI uwolnią personel od żmudnych, powtarzalnych czynności, realizując jednocześnie inne zadania. Mogą np. aktywować protokoły bezpieczeństwa i umożliwiać urządzeniom komunikowanie się ze sobą, co pozwala przechwycić więcej informacji, aby zapewnić utrzymanie bezpieczeństwa bez interwencji człowieka. Autonomia pozwoli personelowi skupić się na strategii oraz podjęciu właściwej decyzji.

Ale czy wszyscy jednakowo rozumiemy pojęcie sztucznej inteligencji? Firma Gartner pokusiła się o przybliżenie tematu[1].

[1] https://www.gartner.com/en/topics/artificial-intelligence

DEFINICJE

Definicji sztucznej inteligencji (AI) jest wiele. Gartner określa ją jako zastosowanie zaawansowanych technik analitycznych i logicznych, w tym uczenia maszynowego (ML) do interpretowania zdarzeń, wspierania i automatyzacji decyzji oraz podejmowania działań. Definicja ta jest zgodna z obecnym i przewidywanym stanem technologii i możliwości AI. Potwierdza, że wiąże się z analizą probabilistyczną (łączącą prawdopodobieństwo i logikę, aby nieokreśloności przypisać wartość).

Sztuczna inteligencja może wspierać, rozszerzać i automatyzować ludzkie działania na wiele sposobów, uczyć się i działać niezależnie, toteż jej definicje mogą być różne. Aby organizacja mogła wykorzystać jej możliwości, należy jednak sformułować i uzgodnić ogólnie przyjętą definicję określającą, co AI ma osiągnąć. Trzeba zostawić przestrzeń na różnicę zdań, ale upewnić się, że między biznesem, liderami IT (informatykami) oraz ds. danych i analityki nie ma zasadniczych rozbieżności w kwestii znaczenia AI dla organizacji, w przeciwnym razie nie będzie można opracować strategii, która przyniesie korzyści.

Dostawcy technologii AI prawdopodobnie również będą mieli własne definicje tego terminu. Należy poprosić o wyjaśnienie, czy ich oferta wychodzi naprzeciw naszym oczekiwaniom dotyczącym sposobu, w jaki AI będzie dostarczać pożądany efekt.

CO TO JEST UCZENIE MASZYNOWE I UCZENIE GŁĘBOKIE?

Jak podaje Gartner, uczenie maszynowe (*machine learning,* ML) jest przełomową techniką, która sztucznej inteligencji umożliwia rozwiązywanie problemów. Wbrew powszechnym, błędnym wyobrażeniom (i błędnym potocznym określeniom) maszyny się nie uczą. One gromadzą dane, przetwarzają i obliczają co prawda w coraz bardziej skomplikowany sposób.

Uczenie maszynowe jest dyscypliną analityczną. Stosuje modele matematyczne do danych w celu wydobycia z nich wiedzy, rozpoznania prawidłowości i znalezienia wzorców, które człowiek prawdopodobnie by przeoczył. ML zaleca również działania, ale nie kieruje systemami, aby reagowały bez interwencji człowieka.

Mówiąc precyzyjniej, uczenie maszynowe tworzy algorytm lub formułę statystyczną (zwaną modelem), która przekształca serię punktów danych w pojedynczy wynik. Algorytmy ML „uczą się" poprzez „trening", podczas którego identyfikują wzorce i korelacje między danymi oraz wykorzystują je do tworzenia nowych wniosków i przewidywań bez konieczności wyraźnego zaprogramowania ich do tego.

Głębokie uczenie *(deep learning,* DL), odmiana algorytmów uczenia maszynowego, wykorzystuje wiele (coraz głębszych) warstw sztucznych neutronów – algorytmów do rozwiązywania problemów poprzez wydobywanie wiedzy z danych pierwotnych i przetwarzanie ich na każdym poziomie. Głębokie uczenie przewyższa tradycyjne ML (lub techniki płytkiego uczenia) w pracy ze złożonymi i często wielowymiarowymi danymi, takimi jak obrazy, mowa i tekst. Mimo to sztuczna inteligencja oparta na regułach lub tradycyjne ML zapewniają skuteczne rozwiązanie wielu problemów związanych z AI.

W większości organizacji rozwiązania oparte na głębokim uczeniu nie stanowią jeszcze istotnej części mapy drogowej produktów (systemy ML oparte na regułach lub tradycyjne ML potrafią dziś skutecznie wspierać większość przypadków użycia AI), ale ich zastosowanie szybko rośnie wraz z postępem w przetwarzaniu danych i przełomowymi technikami obliczeniowymi.

Wykorzystanie ML, w tym głębokiego uczenia, do przewidywania umożliwia procesowi napędzanemu przez sztuczną inteligencję zautomatyzowanie wyboru najkorzystniejszego wyniku, co eliminuje potrzebę udziału człowieka w podejmowaniu decyzji.

PRZYSZŁOŚĆ SZTUCZNEJ INTELIGENCJI I TECHNOLOGII AI

Dziedzina sztucznej inteligencji szybko się rozwija dzięki nowym technikom, dedykowanej infrastrukturze i zaawansowanemu sprzętowi. Firma Gartner prognozuje, że w ciągu najbliższych pięciu lat organizacje zaadaptują najnowocześniejsze techniki do inteligentniejszych i bardziej niezawodnych, odpowiedzialnych i zrównoważonych środowiskowo zastosowań AI. Trajektoria rozwoju AI jest obecnie bardziej zbliżona do trajektorii poprzedzających ją technologii. Dla firm i rządów AI staje się bardziej:

- familiarna (oswojona): narzędzia, wiedza i umiejętności informatyczne sprzyjają teraz AI,
- skalowalna: AI jest tańsza, a sukces łatwiejszy do osiągnięcia niż kiedykolwiek wcześniej,
- użyteczna: liderzy IT i biznesowi częściej rozważają AI jako sposób na ulepszenie aplikacji.

W przyszłości organizacje będą nadal podążać tropem AI, by wzmocnić swoje procesy decyzyjne. Te, które szybko zaadaptują te metody, zwiększą swoją konkurencyjność, staną się bardziej elastyczne i będą lepiej reagować na zmiany w ekosystemie.

Wdrażanie strategii AI pozostaje wyzwaniem dla zespołów zajmujących się infrastrukturą i operacjami. Rozpoczęcie działalności w siedzibie firmy oznacza inwestowanie w infrastrukturę i architekturę, kadry i finansowanie, co może być trudne do przewidzenia i oszacowania. To sprawia, że opcja chmury staje się atrakcyjna, chociaż w miarę wzrostu zapotrzebowania na sztuczną inteligencję i wymagane inwestycje chmura może okazać się zbyt kosztowna (a zobowiązania wobec dostawców chmury bardziej problematyczne). Dlatego tak atrakcyjne jest pojawienie się strategii, które równoważą inwestycje w funkcje chmury z inwestycjami w infrastrukturę (tzw. strategie hybrydowe chmura/*on-premises).*

W zakresie planowania strategicznego w zakresie AI specjaliści Gartnera wskazali, że do 2025 r.

- 50% przedsiębiorstw będzie miało opracowane platformy wdrażania AI w porównaniu z ok. 10% w 2020 r.,
- AI będzie główną kategorią wpływającą na decyzje dotyczące infrastruktury ze względu na rozwój rynku AI, co spowoduje dziesięciokrotny wzrost wymagań na moc obliczeniową,
- 10% rządów będzie wykorzystywać syntetyczną (całościową) populację z realistycznymi wzorcami zachowania do szkolenia AI, unikając jednocześnie obaw związanych z prywatnością i bezpieczeństwem.

CZY PRZEDSIĘBIORSTWA MOGĄ UFAĆ SZTUCZNEJ INTELIGENCJI?

Większość organizacji biznesowych nie zna i nie rozumie wewnętrznych mechanizmów działania sztucznej inteligencji, co stwarza potencjalne obawy dotyczące uczciwości, bezpieczeństwa i prywatności. Nie może ona jednak się rozwijać, gdy firma nie ma zaufania do technik AI, dlatego organizacje potrzebują mechanizmów kontroli i równowagi, aby oceniać i reagować na zagrożenia i szkody oraz zapewniać integralność AI. Gartner określa ramy zarządzania ryzykiem AI mianem MOST. Składają się one z następujących filarów:

- ***M**odel **O**perations* – wspieranie niezawodności, przewidywalności i dokładności AI,
- ***S**ecurity* – bezpieczeństwo (uniemożliwienie hakerom i złośliwym osobom wewnątrz firmy manipulowanie danymi wejściowymi, aplikacjami i wynikami AI)
- ***T**rustworthiness* – wiarygodność (wspieranie uczciwości, etyki, dobrobytu społecznego i „odpowiedzialności SI").

Wraz z upowszechnianiem się AI w przedsiębiorstwie nieuchronnie pojawią się zagrożenia, które spowodują poważne ryzyko organizacyjne. Organizacje muszą proaktywnie je oceniać. W ten sposób mogą zwiększyć zaufanie interesariuszy do AI. Gartner przewiduje, że do 2025 r. regulacje prawne będą wymagały skupienia się na etyce, przejrzystości i prywatności AI, co będzie stymulować, a nie tłumić zaufanie, wzrost i lepsze funkcjonowanie AI na całym świecie.

Zarządzanie danymi i wykorzystanie analityki

Cz. 1.

Szacuje się, że każdego dnia elektroniczne systemy zabezpieczeń produkują 413 petabajtów (PB) danych[1]. Ponad 99% tego zbioru stanowi materiał wideo. Spośród setek milionów godzin nagrań z kamer dozoru wizyjnego, miesięcy zapisów danych ze zdarzeń systemów kontroli dostępu, alarmowych i sygnalizacji pożarowej analizie są poddawane tylko te dotyczące incydentów – zaledwie kilka procent.

Resztę rzadko kiedy poddaje się jakiemukolwiek przeglądowi. Tymczasem zestawienie danych z wielu źródeł – w tym z systemów zabezpieczeń – pozwala na analizę trendów i uzyskanie informacji dotyczących szeroko rozumianego bezpieczeństwem.
Wspólna analiza różnorodnych danych może wskazać anomalie sugerujące wzrost zagrożenia. Czy pracownik odwiedza obszar poza swoim zwykłym środowiskiem pracy? Czy ktoś zjawia się kilka godzin wcześniej na swoją zmianę i dokąd zmierza?

Analiza dużych zbiorów danych w zakresie systemów bezpieczeństwa pozwala obniżyć koszty utrzymania i serwisu.
Narzędzia analityczne są szczególnie przydatne dla rozwiązań o dużej skali – im więcej danych, tym są bardziej użyteczne. Ręczna analiza danych stanów z 2000 przejść, statusu 10 tys. posiadaczy kart i zdarzeń 300 tys. odczytów kart dziennie jest niewykonalna, natomiast analiza automatyczna wraz ze wzrostem liczby danych staje się dokładniejsza. Korzystanie z narzędzi analitycznych operujących na *Big Data* umożliwia użytkownikom przekształcanie „gór danych" w „stosy informacji", a te w „obszary użytecznych spostrzeżeń".

Co na ten temat sądzą eksperci? Przyjrzyjmy się opracowaniu firmy Gartner[2]. Według niej termin „dane i analityka" *(Data and Analytics* – D&A) odnosi się do sposobów zarządzania danymi w celu wspierania każdego ich zastosowania oraz analizy danych, pozwalającej usprawnić podejmowanie decyzji biznesowych, zapewnić firmie rozwój i poprawić wyniki ekonomiczne, a także odkrywać nowe zagrożenia i możliwości.

ROLA DANYCH I ANALITYKI W BIZNESIE

Dane i analityka są szczególnie ważne dla współczesnych przedsiębiorstw, ponieważ mają ogromny wpływ na poprawę wyników wszelkich decyzji (makro- i mikroekonomicznych, podejmowanych w czasie rzeczywistym, cyklicznych, strategicznych, taktycznych i operacyjnych). Równocześnie dzięki D&A można odkrywać nowe, innowacyjne rozwiązania i możliwości, których liderzy biznesowi nawet nie brali pod uwagę. Organizacje idące za postępem wykorzystują dane na wiele sposobów i często muszą je pozyskiwać spoza swojego obszaru kontroli, aby podejmować mądrzejsze decyzje biznesowe.
Dane i analityka są również katalizatorem cyfrowej strategii i transformacji, umożliwiając szybsze, dokładniejsze i trafniejsze decyzje w złożonych i szybko zmieniających się realiach biznesowych. Decyzje podejmują zarówno pojedyncze osoby (np. gdy rozważają, czy kupić produkt lub usługę), jak i zespoły organizacyjne (np. kiedy decydują, jak najlepiej obsłużyć klienta).
Podejmowanie decyzji wspomagane danymi oznacza sposób, w jaki dane są wykorzystywane do usprawnienia procesów decyzyjnych. Prowadzi to do koncepcji modelu decyzyjnego, który może obejmować techniki analityczne o charakterze normatywnym, generujące dane wyjściowe, które są w stanie określić, jakie działania należy podjąć. Inne modele analityczne – opisowe, diagnostyczne lub predykcyjne – są pomocne w podejmowaniu innych rodzajów decyzji. I co istotne, decyzje nie tylko są motorem działania, ale mogą też rozstrzygać o tym, kiedy działania nie należy podejmować.
Postępowe organizacje wprowadzają dane i analitykę do swojej strategii biznesowej i transformacji cyfrowej, tworząc wizję przedsiębiorstwa opartego na danych, kwantyfikując (określając ilościowo) i komunikując wyniki ekonomiczne oraz wspierając zmiany w działalności biznesowej oparte na danych. Coraz częściej wykorzystują zaawansowaną analitykę do rozwiązywania problemów biznesowych, przy czym charakter i złożoność problemu determinuje wybór, czy i w jaki sposób wykorzystywać predykcję[3] *(prediction)*, prognozowanie[4] *(forecasting)* lub symulację/modelowanie w komponencie analizy predykcyjnej. Skalowanie biznesu cyfrowego (zarządzanie coraz większymi ilościami danych cyfrowych) szczególnie komplikuje podejmowanie decyzji i wymaga miksu wiedzy o danych i bardziej zaawansowanych technik. Łącząc możliwości predykcyjne i normatywne, organizacje mogą szybciej reagować na zmieniające się wymagania i ograniczenia. Przykładem takich złożonych możliwości może być prognozowanie napływających zamówień na produkty, połączone z optymalizacją w celu proaktywnego reagowania na zmieniający się popyt w całym łańcuchu dostaw, ale bez opierania się na danych historycznych, które mogą być niekompletne lub zafałszowane.

KLUCZOWE ELEMENTY STRATEGII W ZAKRESIE DANYCH I ANALITYKI

Eksperci Gartner polecają, aby każda organizacja sprecyzowała, czym są dla niej dane i analityka, a także jakie inicjatywy (projekty) i budżety są niezbędne, by móc wykorzystać wszystkie możliwości. Można wskazać kilka kluczowych kroków w strategicznym planowaniu analityki danych, które mają na celu:

- zdefiniowanie misji i celów organizacji,
- określenie strategicznego wpływu danych i analityki na te cele,
- określenie priorytetów działań zmierzających do realizacji celów biznesowych z wykorzystaniem danych i celów analityki,
- opracowanie strategicznej mapy drogowej w zakresie analityki danych,
- wdrożenie tej mapy (tj. projektów, programów i produktów) przy użyciu spójnego i nowoczesnego modelu operacyjnego,
- komunikowanie nt. strategii w zakresie danych i analityki oraz jej wpływu i wyników, by zdobyć wsparcie dla jej realizacji.

Model operacyjny przedsiębiorstwa w tym zakresie musi również eliminować luki w ekosystemie danych, ich strukturach i podejściu organizacyjnym niezbędnych do realizacji strategii analityki danych.

UMIEJĘTNOŚĆ KORZYSTANIA Z DANYCH

Gartner definiuje umiejętność korzystania z danych *(data literacy)* jako zdolność do kontekstowego odczytywania, zapisywania i przekazywania danych. Wymaga to zrozumienia źródeł i struktury danych, stosowanych metod i technik analitycznych oraz umiejętności opisania przykładowego użycia i wynikającej z tego wartości. Niech to nie zabrzmi jak argument za szkoleniem każdego pracownika na naukowca/specjalistę w zakresie danych, bo tak nie jest. Z perspektywy biznesowej umiejętność posłu-

[1] Statista.com, solink.com (dostęp: 26/06/2022)

[2] https://www.gartner.com/en/topics/data-and-analytics

[3] predykcja – statystyczny proces wnioskowania o przyszłych wielkościach zmiennych losowych w określonym przyszłym momencie (okresie), gdy nie jest znana wielkość wyjściowa; wynikiem predykcji jest prognoza; termin „predykcja" jest często używany jako synonim prognozowania

[4] prognoza – przewidywanie czegoś oparte na określonych danych, obliczeniach

giwania się danymi można po prostu podsumować jako program wspomagający liderów biznesowych w nauce zadawania dobrych pytań dotyczących danych.
Budowanie umiejętności korzystania z danych w organizacji jest wyzwaniem związanym nie z technologią, ale także ze zmianą kulturową i zarządzaniem tą zmianą. Dane są coraz bardziej wszechobecne we wszystkich aspektach działalności biznesowej, w społecznościach, a nawet w naszym życiu osobistym. Umiejętność komunikowania się w tym skojarzeniowym języku – umiejętność korzystania z danych – ma coraz większe znaczenie dla sukcesu organizacji. Tego rodzaju trwała, znacząca zmiana wymaga jednak od ludzi nauczenia się nowych umiejętności i zachowań.
Zgodnie z najlepszymi praktykami organizacje kładą znacznie większy nacisk, energię i wysiłek na zarządzanie zmianą w ramach strategii D&A, wykorzystanie przywództwa i czynników zmiany, zajęcie się zarówno umiejętnością wykorzystania danych („wprawa" – określana również jako predyspozycja), jak i kulturą („chęć"/„wola" – określana alternatywnie jako nastawienie).
Umiejętność korzystania z danych musi zaczynać się od zajęcia stanowiska przez kierownictwo. Przykładowo, dyrektor ds. informatyki lub dyrektor ds. danych wraz z liderami ds. finansów (zwykle business intelligence, BI) i HR (rozwój i szkolenia) mogą wprowadzić programy w zakresie zdobywania umiejętności korzystania z danych, zapewniając swoim współpracownikom narzędzia do adaptacji i przyjęcia RODO w ich działach.
Opowieść o danych, jako część ogólnego programu wiedzy o danych, może przyczynić się do pozytywnego i skutecznego zaangażowania interesariuszy. Stosuje się w niej przemyślane techniki, by ująć dane i spostrzeżenia w historie, w których centrum są dane. Ułatwia to interpretację, zrozumienie i działanie na podstawie udostępnianych danych.

CZYM JEST ZARZĄDZANIE DANYMI I ANALITYKĄ?

Według Gartnera zarządzanie danymi i analityką (co wiele organizacji nazywa „zarządzaniem informacją") określa prawa decyzyjne i odpowiedzialność, mające zapewnić właściwe zachowania organizacji w zakresie wartości, tworzenia, przechowywania, dostępu, analizowania, użytkowania, przechowywania aktywów informacyjnych i dysponowania nimi. Kluczowe znaczenie ma powiązanie zarządzania informacją z ogólną strategią biznesową oraz jego zakotwiczenie w tych

zasobach danych i analiz, które interesariusze organizacji uważają za krytyczne.
Zarządzanie danymi i analityką obejmuje:

- osoby (m.in. odpowiedzialne za wyznaczanie kierunków polityki, podejmujące decyzje oraz odpowiedzialne za zarządzanie i administrowanie danymi w biznesie),
- procesy (takie jak architektura i inżynieria zarządzania i administracji oraz procesy decyzyjne),
- technologie (np. zarządzanie danymi podstawowymi),

które zapewniają zaufane i wiarygodne dane o znaczeniu krytycznym w całym przedsiębiorstwie.
Początkowo zarządzanie danymi koncentrowało się wyłącznie na zapewnieniu zgodności z przepisami. Obecnie ewoluuje i rozszerza się w kierunku zarządzania możliwie najmniejszą ilością danych pozwalającą na uzyskanie jak największego wpływu na działalność biznesową. Innymi słowy, zarządzanie danymi i analityką rozwinęło się w taki sposób, że obejmuje zarówno funkcje ofensywne zwiększające wartość biznesową, jak i funkcje obronne, które chronią organizację.
Efektywne zarządzanie danymi i analityką musi też równoważyć zarządzanie na poziomie całego przedsiębiorstwa i na poziomie obszarów biznesowych, ale wymaga to znormalizowanego/ujednoliconego podejścia korporacyjnego. Zarządzanie informacją nie funkcjonuje w próżni, musi czerpać inspirację ze strategii D&A. Należy odnosić się do określonych wyników biznesowych, wprowadzając konkretne, wymierne mierniki (np. odsetek utrzymania klientów w danym segmencie rynku czy procent przychodów uzyskiwanych dzięki partnerom), które łączą zasoby i inicjatywy D&A z wartością biznesową.
W kolejnej części artykułu przedstawimy prognozy ekspertów Gartnera dotyczące przyszłości technologii danych i analityki oraz *big data*.

DAHUA TECHNOLOGY

www.xxxxxx.pl

Kamery z funkcjami AI w ofercie Dahua Technology

Maciej Pietrzak

Technologia analizy obrazu przy użyciu algorytmów sztucznej inteligencji zadomowiła się w systemach zabezpieczeń. Algorytmy AI *(Artifical Intelligence)* stosowane w elementach systemów wizyjnych pozwalają na skuteczną detekcję uwzględniającą typ wykrywanego obiektu, jego pozycję oraz zachowanie. To dopiero początek możliwości, jakie otwiera uczenie maszynowe *i głębokie uczenie się*.

Dahua Technology, lider w dziedzinie dostarczania systemów zabezpieczeń, kładzie nacisk na rozwój nowych technologii, czego efektem są kolejne generacje kamer, rejestratorów i oprogramowania dające użytkownikowi coraz więcej możliwości. Najnowsze modele kamer Lite AI, Pro AI oraz Ultra AI łączą ostatnie osiągnięcia z zakresu optyki (wykorzystanie technologii Full Color 2.0) oraz analizy obrazu bazującej na algorytmach sztucznej inteligencji.

W serii Lite AI zastosowano SMD Plus, czyli inteligentną detekcję ruchu umożliwiającą filtrowanie wykrywanych obiektów, dzięki czemu kamera reaguje wyłącznie na pojawienie się w scenie człowieka lub pojazdu. Wprowadzenie tej funkcji pozwoliło osiągać detekcję intruza na wysokim, niespotykanym do tej pory poziomie przy wyeliminowaniu fałszywych alarmów do minimum, co było największą wadą tego typu funkcji. Dzięki możliwości wyznaczania wirtualnych stref lub linii, których naruszenie powoduje wyzwolenie alarmu, seria kamer Lite AI doskonale sprawdza się w ochronie obwodowej.

Za pomocą kamer Pro AI można korzystać z bardziej zaawansowanych funkcjonalności. Ta seria doskonale sprawdza się jako element systemu zabezpieczeń, ale dostarczając informacje z zakresu *Business Intelligence,* może również wspomagać menedżerów z różnych sektorów gospodarki, np. handlu detalicznego dzięki możliwości zliczania zarówno wejść lub wyjść osób, jak i liczby przebywających w wirtualnej strefie. Ponadto użytkownik ma możliwość analizy klientów na podstawie informacji zaszytych w metadanych, takich jak płeć czy wiek, co pozwala na jeszcze lepsze profilowanie działań sprzedażowych.

Ultra AI to najbardziej zaawansowana seria kamer w ofercie Dahua Technology. Oprócz wspomnianych funkcjonalności do dyspozycji są kolejne: rozpoznawanie twarzy, przetwarzanie 20 typów metadanych, m.in. kolor ubioru, bagaż, nakrycie głowy, typ, kolor i marka pojazdu, a nawet automatyczne czytanie numerów tablic rejestracyjnych. Funkcja rozpoznawania twarzy umożliwia tworzenie bazy nawet 200 tys. wizerunków. Kamera może zaalarmować w przypadku wykrycia w scenie osoby, której wizerunek został wcześniej umieszczony w bazie.

Kamera z serii Ultra AI zarządzana z poziomu flagowego oprogramowania DSS Pro w wersji 8. pozwala na śledzenie trasy, jaką poruszała się określona osoba lub pojazd, dzięki wspomnianym wcześniej metadanym. Detekcja braku kasku ochronnego czy kamizelki odblaskowej to funkcjonalności, których zastosowanie znajdą zastosowanie w takich obiektach, jak magazyny, zakłady produkcyjne lub obiekty budowlane. Unikalną funkcjonalnością jest dynamiczna maska prywatności, która anonimizuje, rozmazując twarz lub sylwetkę osób znajdujących się w kadrze. Co więcej, administrator w każdej chwili może zadecydować, kiedy maska prywatności jest widoczna lub nie, również na nagraniach.
Nowością w kamerach PTZ jest wykorzystanie algorytmów AI w celu jeszcze skuteczniejszego śledzenia obiektów w ramach funkcjonalności Auto Tracking 3.0.

Więcej informacji na https://dahuasecurity.com oraz profilu firmy na Facebooku.

AXIS COMMUNICATIONS

www.axis.com/pl

Kopułkowa kamera 8 Mpix z funkcjami OptimizedIR i głębokiego uczenia

KAMERA AXIS P3268-LV ZAPEWNIA WYJĄTKOWĄ JAKOŚĆ OBRAZU I SZCZEGÓŁY NA POTRZEBY POSTĘPOWAŃ WYJAŚNIAJĄCYCH W DOSKONAŁEJ ROZDZIELCZOŚCI 4K Z PRĘDKOŚCIĄ DO 60 KL./S. JEST WYPOSAŻONA W ZMIENNOOGNISKOWY OBIEKTYW 9 MM DO PROWADZENIA DOZORU NA DUŻYM OBSZARZE I MA KĄT WIDZENIA 100–53 STOPNI. DZIĘKI FUNKCJOM LIGHTFINDER 2.0 I FORENSIC WDR KAMERA ZAPEWNIA WIERNE ODWZOROWANIE BARW I DUŻĄ SZCZEGÓŁOWOŚĆ PRZY SŁABYM OŚWIETLENIU LUB NIEMAL W CIEMNOŚCI.

Technologia OptimizedIR gwarantuje ostre i wyraźne nagrania w całkowitej ciemności na odległość do 40 m bez konieczności stosowania dodatkowego oświetlenia. Z kolei funkcja Axis Zipstream (z obsługą kompresji H.264 i H.265) znacząco ogranicza zapotrzebowanie na przepustowość i pamięć masową bez negatywnego wpływu na jakość obrazu.
Platforma Incedo™ jest na tyle otwarta, że można dostosować się do najnowszych zmian technologicznych, łącząc bezpieczne punkty dostępu z inteligentnymi technologiami identyfikacji, np. uwierzytelnieniami mobilnymi *(mobile access)* i biometrycznymi. Ponadto umożliwia współpracę z innymi systemami zabezpieczeń, takimi jak telewizja dozorowa, sygnalizacja włamania, VSM czy interkomy, w celu stworzenia uniwersalnego, niezwodnego systemu zarządzania bezpieczeństwem obiektu.
Kamera wykorzystuje ARTPEC-8, najnowszy procesor SoC Axis i moduł przetwarzania danych z funkcją głębokiego uczenia (DLPU). Umożliwia to lepsze przetwarzanie, gromadzenie, przechowywanie i analizowanie jeszcze większej ilości danych niż wcześniej – na brzegu sieci. AXIS Object Analytics wykrywa i klasyfikuje osoby, pojazdy i typy pojazdów – wszystkie te funkcje są dostosowane do konkretnych potrzeb. Co więcej, dzięki obsłudze ACAP w wersji 4. można zwiększyć wartość systemu poprzez wykorzystanie wyspecjalizowanych aplikacji opartych na głębokim uczeniu w urządzeniu brzegowym.
Łatwa w instalacji kamera kopułkowa została zaprojektowana tak, że wpasowuje się w każde otoczenie. Ma zmiennoogniskowy obiektyw z opcją zdalnego zbliżania i ustawiania ostrości, więc może dostarczać widok ogólny i zbliżenia bez konieczności ręcznego dostrajania. Kanał fonii oraz wejścia/wyjścia umożliwiają integrację urządzeń peryferyjnych, takich jak mikrofon, co znacząco podnosi wartość całego systemu.
Wydajna kamera kopułkowa ma wiele zintegrowanych funkcji związanych z cyberbezpieczeństwem, które zapobiegają nieautoryzowanemu dostępowi i chronią system.

ROBERT BOSCH

www.bosch.pl

Nowa kamera Dinion Inteox OC: NBE-7604-AL-OC

W OFERCIE SYSTEMÓW WIZYJNYCH ROBERT BOSCH POJAWIŁA SIĘ NOWA KAMERA WYPOSAŻONA W SZEREG ZAIMPLEMENTOWANYCH ALGORYTMÓW SZTUCZNEJ INTELIGENCJI ORAZ MOŻLIWOŚCI PERSONALIZACJI FUNKCJI KAMERY DZIĘKI OTWARTEJ PLATFORMIE INTEOX.

Wbudowana w kamerę analityka danych wizyjnych bazuje na mechanizmie Intelligent Video Analytics, który pozwala na zastosowanie do 16 różnego rodzaju reguł analitycznych jednocześnie. Dla lepszej świadomości sytuacyjnej algorytm ten umożliwia klasyfikację obiektów na osoby, samochody, motocykle/rowery oraz samochody ciężarowe/autobusy.
NBE-7604-AL-OC ma zaimplementowaną także funkcję uczenia maszynowego *(Camera Trainer)*, dającą możliwość „douczenia" przez integratora nawet do 16 dodatkowych klas obiektów/detektorów. Funkcja ta idealnie uzupełnia algorytm IVA dzięki elastyczności działania oraz możliwości „mieszania" obu technologii w tym samym czasie.
Do zastosowań w załoczonych miejscach – instalacje ITS (Inteligentny System Transportowy), miejskie systemy monitoringu, lotniska, kolej itp. – w kamerze zaimplementowano sztuczną sieć neuronową (algorytmy głębokiego uczenia) zdolną do klasyfikowania jednocześnie wielu różnych obiektów. Są wśród nich osoby, rowery/motory, samochody osobowe, ciężarówki i autobusy.
Wychodząc naprzeciw wymaganiom klientów oczekujących niestandardowych analityk, kamerę wyposażono w otwartą platformę Inteox. Umożliwia ona (podobnie jak smartfony) instalację zewnętrznych aplikacji dostępnych na serwisie zakupowym azena.com. Z racji ustandaryzowania rozwiązania Intoex/azena.com klient dodatkowo uzyskuje narzędzia, dzięki którym (posiadając odpowiednie zaplecze) jest w stanie sam utworzyć odpowiednią dla siebie aplikację.
Wszystkie zaimplementowane mechanizmy dostarczają dane, które mogą być wykorzystane już na poziomie kamery (statystyki na żywo) lub dane te mogą być zaimplementowane do zewnętrznego narzędzia, dając praktycznie nieograniczone możliwości ich interpretacji w każdym środowisku biznesowym.

I-PRO

https://i-pro.com/

i-PRO z szeroką ofertą kamer wspieranych sztuczną inteligencją

NIEGDYŚ PANASONIC BUSINESS – OD PAŹDZIERNIKA UB.R. JUŻ OFICJALNIE I-PRO EMEA – STAWIA SOBIE ZA CEL ZBUDOWANIE ROZPOZNAWALNOŚCI JAKO ZAUFANY DOSTAWCA KAMER NOWEJ GENERACJI WSPOMAGANYCH SZTUCZNĄ INTELIGENCJĄ (AI). JEDNYM Z FLAGOWYCH CELÓW STRATEGII I-PRO JEST WZBOGACANIE BRANŻY ZABEZPIECZEŃ O ROZWIĄZANIA OPARTE NA AI, DLATEGO TEŻ WSZYSTKIE PRODUKTY WYPOSAŻA W TE MECHANIZMY.

W lutym br. i-PRO wprowadziła na rynek nową serię kamer wielosensorowych o rozdzielczości 4K, 6 Mpix i 4 Mpix. Mają wbudowany procesor sztucznej inteligencji, który obsługuje analitykę opartą na głębokim uczeniu się. Urządzenia są także wyposażone w zestaw SDK ułatwiający integrację aplikacji innych producentów. Oferują szerszy zasięg i większy zakres pochylenia niż inne porównywalne produkty na rynku, a także doświetlenie IR LED w wybranych modelach. Są wyposażone w wiodące w branży szyfrowanie FIPS 140-2 na poziomie 3. Nadają się do szerokiej gamy zastosowań wymagających wysokiego poziomu bezpieczeństwa w monitoringu miast i budynków, logistyce, przemyśle i transporcie.
Firma ma w ofercie również 34 nowe modele kamer serii S o rozdzielczościach 4K, 6 Mpix i 5 Mpix, w wersjach do zastosowań wewnętrznych i zewnętrznych oraz jako kamery typu bullet i kopułkowe.
Modele serii S również mają wbudowany procesor AI i zestaw SDK, linia jest kompatybilna z wtyczką i-PRO Active Guard opracowaną w celu łatwego, intuicyjnego zarządzania alarmami. W ofercie i-PRO jest też dodatek do serii S – model mini – kamera sieciowa o kieszonkowej obudowie (10 x 5 x 2 cm) i pełnej funkcjonalności analityki wspieranej sztuczną inteligencją.
W obliczu globalnych niedoborów chipsetów i półprzewodników i-PRO wprowadziła usługę szybkiej dostawy wszystkich kluczowych modeli z dostępnością w ciągu 2-4 dni z magazynu europejskiego i 2-4 tygodni z fabryki. Ponadto firma zobowiązała się do utrzymania cen swoich kamer, w tym modeli z obsługą sztucznej inteligencji, pomimo globalnej inflacji.

Najnowsze funkcje analizy wizyjnej

Analiza obrazu stale się rozwija, otwierając więcej możliwości wykorzystania kamer sieciowych – na innych obszarach i w całkiem nowy sposób. Axis pozostaje liderem w tej dziedzinie, tworząc unikalną własną strategię rozwoju produktów, w której ważnym elementem jest standaryzacja w kierunku *Deep Learning*.

Specjalistyczny procesor SoC *(system-on-chip)* najnowszej generacji przeznaczony do sieciowych systemów wizyjnych – ARPTEC-8 – został opracowany z myślą o obsłudze aplikacji do analiz brzegowych opartych na głębokim uczeniu (DL). Kamera dysponuje dzięki niemu mocą obliczeniową niezbędną do lokalnego analizowania danych. Pozwala to na bardzo szczegółową detekcję i klasyfikację obiektów w czasie rzeczywistym oraz projektowanie wydajnych aplikacji analitycznych przeznaczonych do rozróżniania obiektów, np. rodzajów pojazdów – co jest podstawą aplikacji AXIS Object Analytics.
Otwiera ona również drzwi do innych rodzajów analityki opartych na głębokim uczeniu się, które dostarczają użytecznych informacji na potrzeby ochrony, bezpieczeństwa i celów operacyjnych.

Dzięki analizowaniu danych na brzegu sieci – czyli w kamerze – nie dochodzi do ich utraty na skutek kompresji czy transmisji, co zwiększa wiarygodność wyników. Należy jednak pamiętać, że procesor ARTPEC-8 nie daje gotowej, całościowej analizy obrazu, tylko otwartą platformę, która może być wykorzystywana w dowolny sposób przez partnerów w zależności od potrzeb i celów, które ma realizować system dozorowy.

Rozwiązania oparte na najnowszym procesorze oferują szereg możliwości analityki wizyjnej, która znacznie wpływa na zwiększenie bezpieczeństwa w obiekcie. Przykładem mogą być systemy wykrywania pożaru na najwcześniejszym jego etapie. Jest to możliwe dzięki aplikacji, która nie potrzebuje fizycznego kontaktu z dymem, ale poprzez obraz, na którym natychmiast „dostrzega” niebezpieczeństwo w chwili jego wystąpienia. Zaawansowane algorytmy programowe zainstalowane w wysokorozdzielczej kamerze bezpieczeństwa pożarowego skanują otoczenie i stale, w czasie rzeczywistym je analizują, aby precyzyjnie lokalizować różne zdarzenia pożarowe. Obsługa czterech zdarzeń alarmowych za pośrednictwem sieci sprawia, że ich detekcja może spowodować zarejestrowanie materiału wizyjnego, wyemitowanie alarmu dźwiękowego, wysłanie e-maila lub ostrzeżenie operatora w inny sposób.
Funkcja ta może być stosowana jako uzupełnienie obowiązkowych detektorów dymu w obiekcie, a także w miejscach, które nie są objęte obowiązkową detekcją pożarów lub tam, gdzie nie można zainstalować innego rodzaju detektorów dymu, np. na rozległych obszarach zewnętrznych.
W jaki sposób działa system ostrzegania o dymie w kamerach Axis? Analizuje on materiał wizyjny w czasie rzeczywistym pod kątem sygnałów wskazujących na obecność dymu lub płomieni. Funkcja ostrzeżenia o dymie

aktywuje się w ciągu pięciu sekund (przy domyślnym ustawieniu czułości) od pojawienia się dymu w polu widzenia kamery. Umożliwia to sprawną reakcję i szybkie podjęcie interwencji w ciągu pierwszych minut, kiedy pożar wciąż łatwo ugasić. W chwili detekcji funkcja ostrzeżenia o dymie generuje alarm, który może być umieszczony na ekranie w postaci etykiety tekstowej i strefy z dynamicznym obramowaniem, wskazując miejsce alarmu.
Dodatkowo funkcja Forensic Search 2 umożliwia szybkie pozyskiwanie z kamery konkretnych danych. Analityka pozwala na wyszukiwanie obrazu wg wielu zmiennych, np. kierunku ruchu, rejonu, prędkości poruszania się obiektu, kolorystyki ubioru czy typu pojazdu. Wyniki wyszukiwania i nagrania wideo można łatwo wyodrębnić i nimi zarządzać. System umożliwia automatyczne tworzenie zdarzeń i wypełnianie ich odpowiednimi nagraniami oraz cyfrowymi dowodami z innych źródeł.
Do analizy wybranego materiału wideo można ponadto wykorzystać system map ciepła, czyli linii ruchu obiektów wg ich typów, np. ludzie, pojazdy. Możliwe jest także wygenerowanie graficznej wizualizacji danych w formie wykresów. Takie rozwiązania, dzięki zastosowaniu odpowiednich filtrów wyszukiwania, pozwalają na jak najszybszą weryfikację wybranego zdarzenia.

W połączeniu z aplikacją AXIS Object Analitycs możliwa jest też dokładna klasyfikacja typów pojazdów. Dzięki algorytmom opartym na sztucznej inteligencji aplikacja analizuje scenę i zachowanie obiektów w przestrzeni, ignorując typowe, nieistotne źródła niepożądanych zdarzeń. Aplikacja wie, co ma wykrywać, więc można skupić się tylko na obiektach zainteresowania i zdarzeniach wymagających uwagi, a to sprawia, że dozorowanie jest bardziej efektywne.
Analityka zainstalowana w urządzeniu przetwarza i analizuje obraz wideo na żywo bezpośrednio w kamerze, eliminując potrzebę stosowania kosztownych serwerów. Dodatkowe korzyści obejmują wydajniejsze przetwarzanie danych, zminimalizowane wymagania dotyczące pamięci masowej i przepustowości oraz lepszą skalowalność.

W rozwiązaniach Axis dostępne są także nowe funkcjonalności zachowania prywatności. Aplikacja Live Privacy Shield umożliwia analizę obrazu wideo pod tym kątem – maskowanie ludzi pozwala na utajnienie ich tożsamości. Dynamiczne maskowanie z szybkością 10 kl./s ma zastosowanie do scen bliskiego zasięgu w pomieszczeniach i na zewnątrz, w miejscach takich jak zakłady produkcyjne, szpitale, domy opieki nad osobami starszymi, hotele, szkoły, biura czy sklepy. Analityka w kamerze pozwala także na maskowanie np. tylko twarzy lub tablic rejestracyjnych, w zależności od potrzeb operatora.
Ponadto do wyboru pozostają dwie techniki maskowania: kolorem lub poprzez mozaikę. Metoda kolorystyczna sprawdza się w sytuacjach, kiedy najważniejsze jest dokładne obserwowanie ruchu monitorowanego obiektu. Mozaika natomiast pokazuje poruszające się osoby w bardzo niskiej rozdzielczości (rozpikselowanie), dzięki czemu możliwa jest lepsza detekcja barw obserwowanego obiektu. Maski można dowolnie skonfigurować, tak aby obejmowały całe pole widzenia kamery bądź wybrany obszar. Wykonywanie analizy nie wymaga posiadania kosztownych serwerów centralnych, a sama konfiguracja aplikacji została znacznie uproszczona.

Dynamiczne maskowanie z szybkością

10 kl./s

ma zastosowanie do scen bliskiego zasięgu w pomieszczeniach i na zewnątrz, w miejscach takich jak zakłady produkcyjne, szpitale, domy opieki nad osobami starszymi, hotele, szkoły, biura czy sklepy

Analityka w kamerach wyposażonych w procesor DLPU może przynieść również szereg niestandardowych zastosowań, specyficznych dla danej branży, zwiększających zarówno bezpieczeństwo, jak i wydajność operacyjną zakładu produkcyjnego, sklepu bądź punktu usługowego. W zakładach przemysłowych systemy analityczne są pomocne przy weryfikacji, czy pracownicy stosują odpowiednie zabezpieczenia podczas przebywania na terenie zakładu, np. prawidłowo noszą kaski. Kamera potrafi wychwycić osobę, która nie stosuje należytych środków ochrony osobistej, a następnie przekazać tę informację do systemu powiadomień audio.
Ponadto mogą wspierać standardowe procedury kontroli dostępu, co jest istotne zwłaszcza na tak dużych przestrzeniach, jak obiekty przemysłowe. Kamery przystosowane do wykrywania podejrzanych zachowań i podążania za obiektem w ruchu są w stanie wykryć niepowołaną osobę. Dzięki zainstalowanym w urządzeniu funkcjom analitycznym kamera może wysłać odpowiedni komunikat pracownikom ochrony budynku.
Z kolei w sektorze handlu detalicznego właściciel może wprowadzić do swojego sklepu wiele udogodnień, nie tylko skierowanych do klientów, ale także znacznie ułatwiających pracę personelu. Rozwiązania analityczne analizujące obraz z kamery można wykorzystać do zliczania osób przechodzących pod kamerą w czasie rzeczywistym. Uzyskane dane będą przydatne do podejmowania kluczowych decyzji biznesowych, np. o konieczności zwiększenia personelu w godzinach szczytu. Monitorowanie kolejek może znacznie poprawić poziom zadowolenia klientów dokonujących zakupy w sklepie. Dodatkowo informacje o średnim czasie oczekiwania i wskaźnikach rezygnacji przyspieszą wprowadzenie zmian.

Wyższy poziom bezpieczeństwa w PWPW

AEOS spełnia surowe kryteria światowej klasy dostawcy druku zabezpieczonego

PWPW (Polska Wytwórnia Papierów Wartościowych) to jedna z najbardziej zaawansowanych europejskich firm z sektora druku zabezpieczonego. W jej portfolio znajduje się szereg wysoce zabezpieczonych dokumentów, np. paszporty i wizy, a także banknoty i karty płatnicze. W związku z tym potrzebuje systemu kontroli dostępu, na którym może polegać. Po dogłębnej analizie PWPW zdecydowała, że najlepszym rozwiązaniem będzie system AEOS.

PODSTAWOWE INFORMACJE:

- Ponad 3000 kart
- 470 drzwi
- Dwie lokalizacje (kolejne wkrótce)
- Integracja z systemami biometrycznymi 3D

KOMPLEKSOWE WYMAGANIA ZWIĄZANE Z NOWYM SYSTEMEM

Dotychczasowy system kontroli dostępu PWPW przestał być wspierany przez producenta, dlatego organizacja rozpoczęła poszukiwania zamiennika oferującego wysoki poziom zabezpieczeń. Jednak PWPW nie jest placówką, którą można zabezpieczyć w prosty sposób. To kompleks jedenastu budynków zbudowanych w różnych latach, ze skomplikowanym układem różnego rodzaju przejść i klatek schodowych. Oznaczało to, że PWPW nie mogła czerpać inspiracji z podobnych do niej placówek. Zespół musiał postawić na innowacyjność i opracować nową koncepcję zabezpieczeń, która spełniałaby standardy obowiązujące w światowej klasy przedsiębiorstwach zajmujących się drukiem.

STABILNOŚĆ PRODUCENTA JAKO KLUCZOWY WYMÓG

Ponieważ producent istniejącego systemu kontroli dostępu w PWPW zakończył swoje wsparcie, oczywiste było, że jednym z najważniejszych kryteriów wyboru nowego systemu była stabilność nowego dostawcy. Istotną kwestią było również jego podejście do długoterminowego wsparcia dla oferowanego systemu.

– Działamy na bardzo trudnym i skomplikowanym rynku. Często zdarza się, że niedawno zakupiony system przestaje być wspierany, bo jego producent został wykupiony przez inną firmę. Może to stwarzać poważne problemy. Aby ich uniknąć, przeprowadziliśmy wnikliwy proces analizy producentów oferujących rozwiązania z zakresu kontroli dostępu – mówi Piotr Sitko, zastępca dyrektora ds. bezpieczeństwa w PWPW.

RYGORYSTYCZNE POSZUKIWANIA WŁAŚCIWEGO ROZWIĄZANIA

Z tego względu PWPW dokonała szczegółowej analizy, poszukując nowego rozwiązania. Zespół odwiedził krajowe i międzynarodowe targi oraz spotkał się z co najmniej 12 producentami. Złożył również wizyty u wybranych użytkowników końcowych, aby zobaczyć, jak poszczególne systemy sprawdzają się w praktyce. Oprócz rozważenia „wschodzących innowacji" i portfolio produktów zespół sprawdził również historię działalności potencjalnych dostawców oraz ich plany na przyszłość.
Ostatecznie PWPW zdecydowała, że to właśnie firma Nedap spełnia jej najsurowsze kryteria, a oferowany przez nią system kontroli dostępu AEOS oferuje zabezpieczenia, których potrzebuje.

KRYTERIA WYBORU

W odniesieniu do nowego systemu kontroli dostępu PWPW przyjęła następujące kryteria:

1. Niezawodność o bardzo wysokim poziomie bezpieczeństwa

To główny priorytet dla PWPW. Ponieważ organizacja dostarcza papiery wartościowe wymagające wysokiego poziomu bezpieczeństwa, musi polegać na systemie kontroli dostępu, który gwarantuje odpowiednią ochronę.

Implementacja AEOS pozwoliła PWPW zdobyć certyfikat INTERGRAF (ISO 14298). Stanowi on poświadczenie najwyższego poziomu bezpieczeństwa procesu produkcji i pozwala wyróżnić się na tle konkurencyjnych przedsiębiorstw w tym sektorze.

2. Nowoczesny system wysokiej klasy

PWPW poszukiwała systemu kontroli dostępu, który wykorzystuje najnowsze technologie i spełnia surowe standardy bezpieczeństwa.

3. Otwartość na integracje

Dla PWPW bardzo ważne było wybranie systemu bazującego na otwartej platformie, którą będzie można połączyć z pozostałymi technologiami. Zespołowi zależało przede wszystkim na zintegrowaniu czytników biometrycznych umożliwiających obsługę śluz powietrznych.

4. Optymalizacja pod kątem przyszłych rozwiązań

PWPW poszukiwała systemu, który będzie można z łatwością dostosować do przyszłych zmian i rozwiązań, gdy np. zmienią się regulacje prawne i zajdzie konieczność poszerzenia instalacji o dodatkowe zabezpieczenia, np. system liczenia osób w pomieszczeniu. PWPW chciała mieć pewność, że będzie to możliwe.

5. Brak uzależnienia od dostawcy

PWPW nie chciała uzależniać się od producenta systemu kontroli dostępu ani od konkretnych firm świadczących powiązane usługi i serwis.

CEL OSTATECZNY – SCENTRALIZOWANY I ZUNIFIKOWANY SYSTEM

System kontroli dostępu AEOS spełnia wszystkie powyższe kryteria i nie tylko. Dlatego właśnie PWPW powierzyła instalację systemu AEOS firmie Team Systems – zarówno w siedzibie głównej przy ulicy Sanguszki, jak i w placówce przy alei Niepodległości. W nadchodzących latach przedsiębiorstwo planuje instalację systemu AEOS w pozostałych budynkach. Celem jest umożliwienie pracownikom dostępu do wszystkich placówek PWPW za pomocą pojedynczej karty.

– Po tak dogłębnym zbadaniu rynku mamy pewność, że podjęliśmy słuszną decyzję, wybierając firmę Nedap i jej system kontroli dostępu AEOS. Zapewnia on wszystko, czego aktualnie potrzebujemy, a oprócz tego daje nam możliwość rozbudowy i dostosowania do przyszłych zmian. Co więcej, doceniamy swobodę korzystania z usług różnych instalatorów, co pozwala nam wybrać właściwą firmę do każdego projektu i lokalizacji. Mamy możliwość korzystania z konkurencyjnych stawek za usługi i serwis – wyjaśnia Piotr Sitko.

– Jesteśmy dumni, że system AEOS sprostał rygorystycznym wymaganiom PWPW i pozwolił firmie przezwyciężyć trudności związane z kompleksowym zabezpieczeniem. Właśnie takie projekty unaoczniają elastyczność systemu AEOS – mówi Anna Twardowska, Regional Sales Manager Poland and Eastern Europe w Nedap.

Firma Nedap została założona w 1929 r. w Holandii, a od 1949 r. jest spółką notowaną na giełdzie Euronext. Od 1980 r. jest liderem w projektowaniu i produkcji elektronicznych systemów kontroli dostępu, ma certyfikację ISO 9001. Firma ma 7 biur na całym świecie, zatrudnia ponad 100 specjalistów ds. bezpieczeństwa. Rozwiązania Nedap działają w ponad 5,5 tys. przedsiębiorstw w 83 krajach.

Politechnika Wrocławska ze zintegrowanym systemem kontroli dostępu

Politechnika Wrocławska może cieszyć się najwyższym stopniem bezpieczeństwa dzięki rozwiązaniom dostarczanym przez firmę C&C Partners. W ramach zastosowanego rozwiązania zintegrowano systemy: KD, SSWiN, monitoringu wizyjnego i komunikacji interkomowej. System zarządzania obiektami rozproszonymi zastosowany na terenie uczelni pozwoli objąć ochroną elektroniczną zarówno kompleks budynków uczelni, jak i parkingi uczelniane.

Kontrola przepływu osób niepożądanych w strefach administracyjnych, bibliotecznych, archiwalnych, a także niedopuszczanie do miejsc newralgicznych, takich jak serwerownie i informatyczne punkty węzłowe to kluczowe wyzwania stawiane przed wdrożeniowcami z C&C Partners. Celem było maksymalne ułatwienie zarządzania bezpieczeństwem w obiekcie oraz przejrzysty i szybki sposób nadawania uprawnień i dostępów dla ponad 50 tys. użytkowników.

– *Głównym założeniem realizowanego projektu było poszerzenie funkcjonalności legitymacji studenckiej i karty pracowniczej. Dzięki zastosowaniu naszych systemów i zintegrowaniu ich z bazą uczelnianą stają się one kartami dostępu do różnych miejsc. Dzięki tak globalnemu połączeniu zaproponowanych rozwiązań użytkownik może z jednego miejsca zarządzać nie tylko uczelnianym parkingiem, lecz także całą uczelnią. Zastosowane rozwiązanie stawia Politechnikę Wrocławską w czołówce najbezpieczniejszych uczelni w Polsce* – mówi Leszek Schmidt, kierownik Działu Wsparcia Technicznego w C&C Partners.

INWESTYCJA NA LATA

Do najważniejszych korzyści płynących z zastosowanych technologii można zaliczyć weryfikację uprawnień dostępu do określonych miejsc, wprowadzenie modułu automatycznego rozpoznawania tablic rejestracyjnych, kontrolę przepływu niepożądanych osób w poszczególnych pomieszczeniach, włączenie do systemu bezpieczeństwa parkingów uczelnianych czy kompatybilność systemu z uczelnianą bazą studentów i pracowników.
Modułowość projektu umożliwia rozbudowę systemu w czasie i poszerzanie go o kolejne funkcjonalności wg potrzeb inwestora. Ogromne znaczenie ma cykliczna aktualizacja, która gwarantuje poprawę funkcjonalności oprogramowania. Przekłada się także na wyższy poziom bezpieczeństwa IT uczelni.

LEGITYMACJA JAKO KARTA DOSTĘPU ORAZ MONITORING WIZYJNY

Legitymacja studencka czy karta pracownicza stanowią jednocześnie kartę dostępu do różnych miejsc. System sygnalizacji włamania i napadu jest aktywowany w godzinach nocnych, a generowane alarmy zbiegają się w centrum nadzoru, gdzie podejmuje się decyzje co do dalszych kroków. System monitoringu wizyjnego weryfikuje niepożądane zdarzenia, a także wspomaga decyzje podejmowane przez pracowników ochrony obiektów. Monitorowane są miejsca newralgiczne, ciągi komunikacyjne i teren zewnętrzny.

– *Ciekawym rozwiązaniem jest włączenie do systemu bezpieczeństwa parkingów uczelnianych, które z punktu widzenia systemu stają się strefami chronionymi, a dostęp do nich następuje po weryfikacji uprawnień. Przy wjeździe na parking odczytywane są tablice rejestracyjne pojazdu. Jeżeli dany numer znajduje się w bazie i pojazd ma uprawnienia do wjazdu na parking, zostaje automatycznie wpuszczony* – podkreśla Leszek Schmidt.

W przypadku zabrudzenia tablicy bądź przyjazdu innym samochodem użytkownik może użyć legitymacji studenckiej lub pracowniczej jako karty kontroli dostępu. Kierowcy samochodów niezarejestrowanych w bazie (np. dostawy kurierskie, goście) mogą użyć interkomu. Ochrona weryfikuje ich uprawnienia wjazdowe. System podaje też liczbę dostępnych miejsc parkingowych.
Co ważne, baza systemu wymienia informacje z uczelnianą bazą studentów i pracowników, a także portalem uczelni. Nadanie uprawnień danej osobie w systemie uczelnianym automatycznie umożliwia dostęp do określonych zasobów w systemie bezpieczeństwa.

C&C PARTNERS

ul. 17 Stycznia 119, 121
64-100 Leszno
www.ccpartners.pl
l.schmidt@ccpartners.pl

Cztery tryby WaveKey
Jak działają i gdzie z nich korzystać

WaveKey to opatentowana technologia dostępu mobilnego z telefonu komórkowego. Jest najszybsza na rynku, z najlepszą w swojej klasie niezawodnością i „pancernym" bezpieczeństwem.

Oferuje użytkownikom cztery tryby użytkowania różniące się głównie pod względem wygody i związanego z tym poziomu bezpieczeństwa. Dlatego należy się zastanowić, jaki tryb wybrać dla danych drzwi. Oczywiście, można również włączyć kilka trybów dla pojedynczych drzwi i pozostawić decyzję użytkownikowi, z których będzie korzystał.

DOTKNIJ W TRYBIE APLIKACJI

JAK TO DZIAŁA?

Użytkownik otwiera drzwi, dotykając wirtualnego przycisku w aplikacji 2N® Mobile Key. Ponieważ każdy telefon jest zwykle zabezpieczony hasłem, gestem, odciskiem palca albo funkcją rozpoznawania twarzy, ten tryb jest uważany za możliwie najbezpieczniejszy. Jeszcze wyższy poziom bezpieczeństwa można uzyskać dzięki uwierzytelnianiu dwuskładnikowemu, który można włączyć do tego trybu. Aby otworzyć drzwi, po naciśnięciu przycisku w aplikacji użytkownik musi wprowadzić swój kod PIN.

GDZIE JEJ UŻYWAĆ?

- Wejścia do budynków biurowych
- Wejścia do stref zabezpieczonych (dział finansowy, serwerownia, laboratoria)
- Drzwi garażowe, bariery parkingowe (większy zasięg otwierania bezpośrednio z samochodu)

BEZPIECZEŃSTWO A WYGODA

Maksymalna ochrona

TRYB KARTY

JAK TO DZIAŁA?

Tryb karty to coś więcej niż pełnowartościowy zamiennik technologii NFC *(Near Field Communication),* ponieważ działa na urządzeniach z systemem zarówno Android, jak i iOS. Użytkownik przykłada telefon do czytnika Bluetooth tak jak tradycyjną kartę. Tryb karty jest zalecany w instalacjach o dużym przepływie osób. Chociaż nie ma potrzeby odblokowywania telefonu, odblokowuje on tylko z bardzo niewielkiej odległości.

GDZIE JEJ UŻYWAĆ?

- Ruchliwe biura i bramki obrotowe (gdzie pracownicy przybywają do pracy)

BEZPIECZEŃSTWO A WYGODA

75% bezpieczeństwa

TRYB DOTYKOWY

JAK TO DZIAŁA?

Dzięki temu wyjątkowemu trybowi użytkownik nie musi wyjmować telefonu z kieszeni ani torebki, kiedy zbliża się do drzwi. Lekko dotyka czytnika Bluetooth ręką lub łokciem i jeśli jest uprawniony do wejścia, drzwi otwierają się natychmiast po dotknięciu czytnika (średnio w ciągu 0,3 s).

GDZIE JEJ UŻYWAĆ?

- Budynki mieszkalne – drzwi frontowe, wspólne obszary
- Budynki biurowe – biura, sale konferencyjne, przejścia pomiędzy kondygnacjami
- W windzie – odblokowanie piętra

Uwaga! Tryb dotykowy jest mniej odpowiedni w miejscach, gdzie wiele osób regularnie się przemieszcza lub gromadzi w odległości kilku metrów od drzwi.

BEZPIECZEŃSTWO A WYGODA

50% : 50%

TRYB RUCHU

JAK TO DZIAŁA?

Bezdotykowy sposób otwierania drzwi, który podnosi wygodę trybu dotykowego na wyższy poziom. Kamera w interkomie uruchamia proces uwierzytelniania oparty na wykrywaniu ruchu. Ważne, aby dobrze ustawić reagowanie kamery.

- Reaguje na machnięcie dłonią przed obiektywem, czyli na znaczącą zmianę obrazu w jej pobliżu.
- Wychwytuje również sylwetkę zbliżającej się osoby, więc wystarczy niewielka zmiana w otoczeniu. Oznacza to płynne przechodzenie przez drzwi, jednak czułość ruchu musi być idealnie dostrojona.
- Tryb ten ma zastosowanie tylko do interkomów wyposażonych w kamerę, licencję konfiguracji kamery oraz czytnik Bluetooth (2N® IP Style, 2N® IP Verso i 2N® LTE Verso).

GDZIE JEJ UŻYWAĆ?

- Wejścia do budynków mieszkalnych lub biurowych

Nie zalecamy stosowania tego trybu w miejscach o dużym natężeniu ruchu. Istnieje ryzyko, że drzwi mogą zostać niezamierzenie otwarte przez osobę trzecią.

BEZPIECZEŃSTWO A WYGODA

Maksymalny komfort

2N TELEKOMUNIKACE

Pod Vinicí 20
143 01 Praha 4
Czech Republic
www.2n.com

Sprawna ewakuacja niepełnosprawnych

O tym, że interesuje mnie tematyka ewakuacji, uważni czytelnicy moich artykułów doskonale wiedzą. Nie powinno więc być zaskoczeniem, że znowu poruszam tę kwestię. Mam nadzieję, że i tym razem podzielę się swoimi przemyśleniami w tej kwestii w sposób pozytywnie kontrowersyjny, by sprowokować czytelnika do własnej analizy tematu, poszukiwania odpowiedzi na zasygnalizowane przeze mnie problemy, a może wypłyną też kolejne.

Chciałbym odnieść się bardziej szczegółowo do problematyki ewakuacji (ale także do skutecznego powiadamiania o konieczności ewakuacji) osób niepełnosprawnych w szerokim tego słowa znaczeniu. Do jej poruszenia częściowo zmobilizowała mnie lektura artykułu Bogdana Leszko „Strategia ewakuacji ludzi lub ich uratowania w inny sposób" z poprzedniego numeru „a&s". Doskonały artykuł, wyraźnie przypominający, że osoba wymagająca specjalnej strategii ewakuacji to nie tylko osoba na wózku, ale także np. ludzie starsi czy cierpiący na astmę (która nasila się w sytuacjach stresowych). Autor bardzo dokładnie opisuje ideę „platform ewakuacyjnych", konieczności lokalizacji ich w sposób niezabierający światła drogi ewakuacyjnej, a także wyposażenia miejsc oczekiwania na ewakuację w interkomy pożarowe.

I tutaj pojawiają się moje przemyślenia inżynierskie dotyczące opisywanych rozwiązań. Kilka obiektów udało mi się wyposażyć w takie urządzenia, zostały one zrealizowane według zasad podobnych dla innych systemów zabezpieczeń mimo braku uregulowań formalnych w tej sprawie. Moja pierwsza refleksja dotyczy urządzeń. Oprócz dwukierunkowej komunikacji, o której wspomina B. Leszko, oraz identyfikacji lokalizacji stacji wywoławczej należy zapewnić kilka innych warunków.

Kolejkowanie połączeń: nie można pozwolić, by połączenie z ochroną z jednego miejsca blokowało inne połączenia. Operator musi widzieć w trakcie rozmowy, czy nie przychodzą inne wywołania z innych miejsc w budynku, od tego może i musi uzależnić swoje działania, musi więc mieć na ten temat pełną wiedzę.

Michał Zalewski

Bardzo ważnym aspektem jest również konieczność rejestracji rozmów i wszystkich zdarzeń systemowych (wywołania, czas trwania itp.). Nie ma to bezpośredniego znaczenia na sposób ewakuacji, ale powinno być wymagane przez operatorów tych systemów w interesie ich bezpieczeństwa. Skoro oczekujemy od nich, że biorą na siebie odpowiedzialność za odpowiednią obsługę tych urządzeń, musi być możliwość oceny prawidłowości ich działań – i to zarówno podczas rzeczywistej ewakuacji, jak i szkoleń.

Kolejnym aspektem jest wymóg, by instalacja tego systemu była wykonywana zespołem kablowych wg zasad określonych w § 187 Rozporządzenia o Warunkach Technicznych. Wymagałbym tutaj najwyższej możliwej odporności, czyli PH90. Projektant powinien rozważyć również, czy magistrala komunikacyjna systemu mogłaby być w architekturze ringu w celu podniesienia odporności systemu na pojedyncze uszkodzenia, urządzenia zaś powinny być wyposażone w izolatory zwarć.

Jako projektant rozważyłbym również instalację kamer CCTV monitorujących obszary platform. Nie wprowadzimy do instalacji CCTV wymagań odporności ogniowej instalacji, ale lepiej mieć obraz z tych kamer na początku pożaru niż wcale. Tyle na temat samej instalacji. Jako inżynier uruchomieniowy nie byłbym sobą, gdybym nie poruszył kwestii uruchomieniowych: po zakończeniu instalacji szczegółowo kontrolujemy spełnienie wszystkich wymienionych parametrów instalacji, planując i przeprowadzając odpowiednie testy funkcjonalne, które szczegółowo dokumentujemy. Jest jeszcze kwestia obsługi. Zacznę od liczby osób pełniących funkcję obsługującego systemy bezpieczeństwa pożarowego. Zdarza się, że właściciele/zarządcy budynków, optymalizując koszty obsługi, zapominają o wymogach technicznych. Wprowadzając takie systemy do obiektu, trzeba pamiętać o zapewnieniu odpowiedniej liczby osób do ich obsługi – SSP, DSO oraz interkom ewakuacyjny… Nie zapominajmy o tym, podobnie jak nie można zapominać o cyklicznych szkoleniach oraz ćwiczeniach sprawdzających i przypominających zasady pracy i procedury w stanach zagrożenia.

Kolejny temat to skuteczne powiadomienia o alarmie. Pojawienie się systemów DSO spowodowało usunięcie prawie całkowicie z obszaru budynków sygnalizatorów optycznych, a to błąd. Powszechnie instaluje się je w pomieszczeniach głośnych (agregat, maszynownia wentylacji pożarowej), ale już np. o zainstalowaniu na dachu budynku zdarza się projektantom zapominać. A jeżeli dach jest wielką maszynownią, w której może pracować wiele ekip technicznych? Ale to nie wszystko. Są miejsca w budynku, o których musimy pamiętać i wyposażyć je w sygnalizację optyczną: to toalety oraz tzw. pokoje dla matek karmiących. Zahaczamy tutaj właśnie o osoby niepełnosprawne, a dokładniej osoby z upośledzeniem słuchu. One też mają prawo zostać poinformowane o konieczności ewakuacji natychmiast w II stopniu alarmu. Znam inwestora, który kilka lat temu wprowadził taki wymóg w swoich obiektach, polecam to rozwiązanie innym, a projektantów systemów SSP zachęcam, by dopytywali się o te rozwiązania w trakcie planowania inwestycji.

Innymi obiektami, dość specyficznymi z tej perspektywy, są hotele i akademiki. Mało mówi się o zapewnieniu skutecznego powiadamiania o alarmach również osób z upośledzeniem słuchu przebywających w takich obiektach. Osoba niedosłysząca ma prawo zostać natychmiast powiadomiona o ewakuacji.

W trakcie pracy nad artykułem przeprowadziłem małe dochodzenie dziennikarskie. Zadzwoniłem z pytaniami o te kwestie do kilku hoteli w centrum Warszawy. To, co ustaliłem, nie napawa optymizmem. Tylko w jednym hotelu na wyposażeniu było alarmowe przenośne urządzenie wibrujące, które jest pożyczane na życzenie osoby niesłyszącej, ale tylko jedne. A urządzenie jest dość łatwo dostępne i niedrogie, jak udało mi się ustalić. W innym hotelu zapewniono mnie, że obsługa w razie alarmu powiadomi o tym, jest do tego przeszkolona i gotowa. Jednak co do skuteczności takiej realizacji obowiązku właściciela mam wątpliwości.

Nie wykluczam, że mój sprawdzian nie był pełny, wiem również z doświadczenia, że pewna sieć hotelowa ma takie urządzenia w standardzie, tymczasem jeden ze sprawdzanych obiektów należący do tej sieci nie miał ich na stanie. Poruszam ten problem na łamach czasopisma branżowego, by go uświadomić projektantom i instalatorom systemu DSO, gdyż jeżeli jest taki standard w budynku, to musimy o tym wiedzieć i uwzględnić go w projektowaniu (urządzenia te działają przy określonym poziomie SPL alarmu).

Chciałbym zasygnalizować temat ujęty z nieco innej strony. NIK w 2018 r. sporządziła raport w tej sprawie, jest on dostępny na stronach NIK[1], polecam jego lekturę: **„Miejsca powszechnie dostępne – wciąż niedostępne. NIK o dostępności przestrzeni publicznej dla osób starszych i niepełnosprawnych".**

Zapoznając się z nim i analizując, co się wydarzyło w tej sprawie od dnia opublikowania, odnoszę wrażenie, że zbyt mało się o tym mówi. Dlatego poruszam ten temat, starając się poszerzać grono osób świadomych, i zachęcam do lektury zarówno artykułu B. Leszko, o którym wspomniałem, raportu NIK w tej sprawie, jak i do własnych przemyśleń i analiz tej kwestii. Wszak zgodnie z prawem musimy projektować i budować budynki bezpieczne dla wszystkich bez wyjątku.

[1] https://www.nik.gov.pl/aktualnosci/miejsca-powszechnie-dostepne-wciaz-niedostepne.html

MICHAŁ ZALEWSKI

Absolwent Politechniki Gdańskiej i studiów podyplomowych Zarządzania Projektami Politechniki Warszawskiej. W branży od 25 lat, od 13 lat niezależny konsultant, inżynier uruchomieniowy.

Ochrona uniwersytetów i kampusów za pomocą systemu SSP ZETTLER

Wymagania dotyczące instalacji odpowiedniego systemu sygnalizacji pożarowej w obiektach uniwersyteckich zwykle łączą wyzwania związane z ochroną budynków uczelni, audytoriów i budynków zakwaterowania studentów (domów akademickich), które są zbliżone do hoteli. Uniwersytety różnią się wielkością w zależności od liczby studentów, która może wahać się od kilkuset do wielu tysięcy, a wymagania dotyczące automatycznego wykrywania pożaru zależą od wielkości obiektu i liczby mogących przebywać w nim osób.

Uczelnie są bardzo zróżnicowane liczebnie, wybrana technologia wykrywania pożaru powinna odpowiadać środowisku, m.in. salom wykładowym, bibliotekom, laboratoriom i terenom badawczym, obiektom rekreacyjnym i budynkom mieszkalnym dla studentów. Ze względu na zmienny cykl powstawania potencjalnych zagrożeń w niektórych obszarach mogą obowiązywać inne zasady ochrony ppoż., a system SSP będzie musiał się dostosowywać do zmiennego zagrożenia.

UNIKANIE FAŁSZYWYCH ALARMÓW MA KLUCZOWE ZNACZENIE

Zakłócenia dnia pracy spowodowane niechcianymi alarmami mogą być uciążliwe (zwłaszcza podczas egzaminów), dlatego czynnik niezawodności jest niezwykle ważny przy wyborze odpowiedniego systemu. Kompleksowy system sygnalizacji pożarowej ZETTLER został zaprojektowany z myślą o zapewnieniu optymalnej wydajności/skuteczności przez cały czas.

Uczelnia może zmieniać układ pomieszczeń w obiekcie w związku z jego modernizacją lub rozbudową, dlatego przy zmianie warunków ochrony ppoż. również system SSP powinien zostać zmodernizowany i dostosowany do nowych warunków pracy. Często jednak ten fakt jest ignorowany, a to zwiększa ryzyko niepożądanych alarmów. Ten problem rozwiązuje zainstalowanie czujek wielosensorowych 850PC. Czujka ma sześć trybów detekcji i wykorzystuje trzy kanały wykrywania: ciepło, dym i tlenek węgla. Kanały te są połączone w oprogramowaniu, zapewniając optymalną detekcję adekwatną do danego ryzyka. Jeśli jeden lub dwa z nich zmienią się, tryb wykrywania można odpowiednio dostosować. Zmiana trybów może być tak prosta, jak naciśnięcie przycisku na centrali, a jeśli wymagana jest trwała zmiana, łatwo jej dokonać w oprogramowaniu.
Czujkę 850PC można skonfigurować jako wysokowydajny detektor optyczny, detektor z kompensacją tlenku węgla (pożar), czujnik tlenku węgla (gaz toksyczny), detektor ciepła lub jako elastyczny lub uniwersalny (wysoka czułość) detektor optyczny. Czujki z serii 850 są dostępne z wbudowanym izolatorem zwarć i wykorzystują zaawansowaną sygnalizację cyfrową, zapewniającą niezawodną komunikację z centralą SSP ZETTLER. Technologia MZX gwarantuje niezawodność przez cały okres eksploatacji.

SYSTEM MOŻNA ROZBUDOWYWAĆ WRAZ ZE WZROSTEM WYMAGAŃ

Uniwersytety muszą nadążać za rozwojem, a zwiększenie liczby studentów będzie wymagało dodatkowych zasobów i infrastruktury. Z czasem kampus będzie się rozrastał, potrzebne będą nowe budynki z nową detekcją pożaru. Asortyment central PROFILE Flexible jest wysoce skalowalny i może się powiększać wraz ze zmianą wymagań. Dzięki mechanizmowi kart rozszerzeń centrale PROFILE Flexible można łatwo rozbudowywać i dostosować do specyficznych nowych wymagań realizacji, jeśli obiekt zmieni charakter lub zostanie rozbudowany. Centrala została specjalnie zaprojektowana, aby oferować zwiększoną wydajność pętli i opcję współdzielenia pętli, co zapewnia jeszcze większą elastyczność w projektowaniu systemów i niższe koszty instalacji.
Urządzenia systemu sygnalizacji pożarowej ZETTLER oferują szeroką gamę rozwiązań, dzięki którym obiekt uniwersytecki będzie zawsze bezpieczny.

Więcej informacji na stronie: www.zettlerfire.com

JOHNSON CONTROLS INTERNATIONAL

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

Pomieszczenia obsługi urządzeń ppoż.

i kasety straży pożarnej

mł. bryg. mgr inż. Grzegorz Mroczko

Wyposażenie budynków w niezbędne urządzenia przeciwpożarowe ma na celu zapewnienie bezpiecznego użytkowania budynków, m.in. ze względu na ograniczenie powstawania pożaru i kontroli jego rozwoju, jeżeli do pożaru dojdzie. Istotna jest również możliwość ich wykorzystania w trakcie eksploatacji obiektu, a przede wszystkim podczas działań ratowniczo-gaśniczych w razie wystąpienia pożaru lub innego miejscowego zagrożenia.

Po przyjeździe na miejsce zdarzenia strażacy muszą dokonać rozpoznania i ustalić, co i gdzie się dzieje, czy są poszkodowani, jakie działania podjąć itp. Do przeprowadzenia rozpoznania niezbędne jest wejście do budynku i odnalezienie miejsca, w którym wystąpiło zagrożenie. Kiedy nie ma zewnętrznych oznak pożaru (dymu, ognia), ustalenie miejsca i skutków wystąpienia zagrożenia wymaga czasu i poszukiwań, aby potwierdzić lub wykluczyć jego wystąpienie.

W przypadku budynków wyposażonych w adresowalny system sygnalizacji pożarowej poszukiwania ułatwia i przyspiesza odczytanie na centrali SSP informacji, która czujka, w której strefie weszła w stan alarmowania. Rzut oka na inne urządzenia pozwoli na ustalenie, w jakim stanie pracy się znajdują np. system oddymiania budynku czy system gaszenia. W obiektach, w których personel jest obecny przez całą dobę (np. hotele, placówki medyczne), informacji udzieli także personel. W przypadku budynków, które po godzinach funkcjonowania są zamknięte i nie ma w nich personelu (placówki banku, urzędy, ośrodki zdrowia, szkoły, hotele bez całodobowej recepcji itp.), wyzwaniem dla służb ratowniczych jest już uzyskanie dostępu do niego. Ratownicy mierzą się wówczas z decyzją, czy dokonywać siłowego wejścia, czy czekać na przyjazd osoby posiadającej klucze, której dostępność i mobilność w czasie wolnym od pracy jest ograniczona.
Przy projektowaniu i lokalizacji urządzeń ppoż. w budynku należy brać pod uwagę nie tylko korzyści inwestorskie (możliwość wznoszenia większych, wyższych, bardziej rozległych obiektów), ale także zagadnienie dostępności urządzeń ppoż. dla służb ratowniczych – elementy związane z pracą i sterowaniem urządzeniami ppoż. powinny być szybko i łatwo dostępne dla służb ratowniczych.
Oznacza to m.in. odpowiednią lokalizację tych urządzeń, odpowiednie oznakowanie miejsca ich instalacji oraz odpowiednie warunki w pobliżu urządzeń umożliwiające odczytanie informacji, zatrzymanie pracy, uruchomienie, zmianę sposobu działania urządzeń przez strażaków ratowników, którzy będą prowadzić działania ratowniczo-gaśnicze w budynku.
Należy też zapewnić, aby informacje przesyłane z systemu sygnalizacji pożarowej w budynku do komendy miejskiej lub powiatowej PSP zawierały informację, którym wejściem strażacy powinni dostać się do budynku, aby jak najszybciej ustalić i zlokalizować zagrożenie.
W przypadku budynków bez całodobowej obecności personelu należy rozważyć instalację systemu Kasety Straży Pożarnej (KSP), w której znajdują się klucze umożliwiające bezinwazyjne, sprawne wejście strażaków do obiektu i przeprowadzenie rozpoznania. Kaseta straży pożarnej jest instalowana w elewacji zewnętrznej budynku i zawiera podwójne drzwi.
Drzwi zewnętrzne są zwalniane przez system sygnalizacji pożarowej w chwili wejścia systemu w II stopień alarmowania. Drugie drzwi (wewnętrzne) są otwierane za pomocą kodu wpisywanego przez strażaków, a sam kod jest generowany przez dyspozytora na stanowisku kierowania i przekazywany strażakom przez radiostację. Kod jest aktywny tylko kilka minut.
Po otwarciu wewnętrznych drzwi można z kaset pobrać klucze do drzwi wejściowych do budynku. Po zakończeniu akcji klucze ponownie deponuje się w KSP i zamyka podwójne drzwi.

Fot. 1. Kaseta Straży Pożarnej
Źródło: https://kruse-sicherheit.de/produkte/objektzutritt-und-orientierung (dostęp: 24.06.2022 r.)

Projektowanie budynków pod względem jak najlepszej dostępności dla służb ratowniczych nie jest szczegółowo opisane w przepisach techniczno-budowlanych. Można powiedzieć, że mieści się w zbiorze dobrych praktyk i wiedzy technicznej. Wsparcie dla inwestorów, projektantów, wykonawców, instalatorów i zarządców budynków w tym obszarze stanowią dostępne wytyczne CNBOP-PIB:

- W-0001 Wydanie 2:2016 – Pomieszczenia i miejsca obsługi urządzeń przeciwpożarowych w budynkach – lokalizacja, warunki wykonania, wyposażenie,
- W-0002 Wydanie 2:2021 – Wytyczne wyposażania budynków w Kasety Straży Pożarnej.

WYTYCZNE CNBOP-PIB W-0001

W wytycznych W-0001 wprowadzono pojęcia pomieszczenia obsługi urządzeń przeciwpożarowych (POUP), pomieszczenia technicznego urządzeń przeciwpożarowych (PTUP) oraz wskazano wymagania dotyczące lokalizacji, wyposażenia i oznakowania tych pomieszczeń.

POMIESZCZENIE OBSŁUGI URZĄDZEŃ PRZECIWPOŻAROWYCH (POUP)

Pomieszczenie, w którym są zlokalizowane elementy obsługowe urządzeń przeciwpożarowych (centrala sygnalizacji pożarowej, urządzenie zdalnej sygnalizacji i obsługi, centrala dźwiękowego systemu ostrzegawczego, mikrofon alarmowy lub tylko konsola z mikrofonem dla straży pożarnej). W tym pomieszczeniu przebywają pracownicy obsługujący urządzenia przeciwpożarowe, np. portier, personel firmy świadczącej usługi ochrony itp.

POMIESZCZENIE TECHNICZNE URZĄDZEŃ PRZECIWPOŻAROWYCH (PTUP)

Pomieszczenie, w którym – ze względu na specyficzne wymagania w zakresie warunków środowiskowych (np. konieczność klimatyzowania pomieszczenia) lub warunki pracy urządzeń (szum wentylatorów) – można zlokalizować elementy centralne urządzeń ppoż. (np. centrala dźwiękowego systemu ostrzegawczego bez mikrofonu alarmowego, centrala systemu kontroli rozprzestrzeniania dymu i ciepła). Do tego pomieszczenia posiada dostęp personel dokonujący czynności obsługowych i serwisowych/konserwacyjnych jedynie w czasie wykonywania wymienionych czynności.

WYBRANE WYMAGANIA DOTYCZĄCE POMIESZCZENIA OBSŁUGI URZĄDZEŃ PPOŻ. (POUP)

POUP powinno być zlokalizowane w sposób zapewniający szybkie dotarcie ratowników:

- na kondygnacji budynku, na której znajduje się wejście przewidziane i oznaczone jako wejście dla ekip ratowniczych,
- w pobliżu wejścia dla ekip ratowniczych,
- drzwi wejściowe do POUP powinny znajdować się w odległości nie większej niż 10 m od wejścia dla ekip ratowniczych.

POUP powinno mieć odpowiednie wymiary i być wydzielone pożarowo:

- ściany i stropy pomieszczenia w klasie odporności ogniowej REI 60,
- drzwi wejściowe w klasie odporności ogniowej EI 30,
- minimalna szerokość drzwi w świetle powinna wynosić 0,9 m,
- wymiary pomieszczenia powinny wynosić co najmniej 4 m x 4 m. Wielkość pomieszczenia powinna być dostosowana do liczby i wielkości zainstalowanych w nim urządzeń oraz umożliwiać ich konserwację. Wejście oraz poruszanie się ratownika wyposażonego w środki ochrony indywidualnej (m.in. aparat ochrony dróg oddechowych, rękawice ochronne) powinno być swobodne i zapewniać łatwy dostęp do urządzeń, otwarcie obudów czy drzwiczek od urządzeń).

POUP powinno być odpowiednio wyposażone:

- monitorowane poprzez czujki automatyczne systemu sygnalizacji pożarowej,
- w pomieszczeniu lub w bezpośrednim jego sąsiedztwie należy zainstalować ręczny ostrzegacz pożarowy (ROP),
- centrale i urządzenia zdalnej obsługi urządzeń ppoż. powinny być umieszczone w sposób umożliwiający dostęp

i obsługę przez ratownika wyposażonego w środki ochrony indywidualnej oraz odczyt informacji prezentowanych na wyświetlaczach (nie na jasnym tle, np. okna, bez refleksów sztucznego i naturalnego oświetlenia na wyświetlaczu),
- centrale i urządzenia zdalnej obsługi urządzeń ppoż. przewidziane do montażu na ścianie powinny być zamontowane na wysokości od 1,4 do 1,8 m,
- w razie potrzeby dopuszcza się umiejscowienie central urządzeń ppoż. w pomieszczeniu technicznym PTUP, wówczas w pomieszczeniu obsługi POUP należy zlokalizować urządzenia zdalnej obsługi urządzeń ppoż.

POUP powinno być odpowiednio oznakowane *(rys. 1)*:
- w sposób widoczny po wejściu do budynku wejściem przewidzianym dla ekip ratowniczych,
- w przypadku lokalizacji POUP innej niż 10 m od wyjścia dla ekip ratowniczych należy zastosować dodatkowe oznakowanie wskazujące miejsce jego lokalizacji i kierunek dojścia.

POMIESZCZENIE OBSŁUGI URZĄDZEŃ PRZECIWPOŻAROWYCH

Rys. 1. Wzór oznakowania POUP
Źródło: Wytyczne CNBOP-PIB W-0001

Oznaczenie w części graficznej IBP
- Instrukcja Bezpieczeństwa Pożarowego (IBP) w części graficznej oraz na planach ewakuacyjnych budynku powinna zawierać oznakowanie i lokalizację POUP. Oznaczenie na planach ewakuacyjnych powinno być opisane pełną nazwą.

W POUP powinna znajdować się dokumentacja bądź być zapewniona możliwość dostępu do wersji elektronicznej dokumentacji:
1. Instrukcja postępowania w przypadku alarmów pożarowych i uszkodzeniowych
2. Plan ewakuacyjny budynku
3. Instrukcja Bezpieczeństwa Pożarowego
4. Dokumentacja dla urządzeń ppoż., w które jest wyposażony budynek
   a. instrukcja obsługi i konserwacji,
   b. książka pracy,
   c. dokumentacja zawierającą opis działania, rozmieszczenie i identyfikację elementów,
   d. protokoły z przeglądów.
5. Dane kontaktowe do zarządcy budynku, firm wykonujących konserwacje i naprawy systemów, firm świadczących usługę monitoringu pożarowego (kontakt do firmy świadczącej usługę obsługi SSP powinien być naklejony na centrali) i przeciwwłamaniowego.

WYBRANE WYMAGANIA DOTYCZĄCE POMIESZCZENIA TECHNICZNEGO URZĄDZEŃ PPOŻ. (PTUP)

PTUP powinno być zlokalizowane w pobliżu POUP:
- Wyjście z PTUP powinno znajdować się w odległości nie większej niż 10 m od wyjścia z POUP, może znajdować się w POUP.

PTUP powinno mieć odpowiednie wymiary i być wydzielone pożarowo:
- ściany i stropy pomieszczenia w klasie odporności ogniowej REI 60,
- drzwi wejściowe w klasie odporności ogniowej EI 30,
- minimalna szerokość drzwi w świetle powinna wynosić 0,9 m,
- szerokość dojścia do pomieszczenia powinna wynosić co najmniej 1,5 m,
- wymiary pomieszczenia powinny zapewnić odpowiedni dostęp do urządzeń przez strażaka w pełnym ekwipunku np. z aparatem ochrony dróg oddechowych.

PTUP powinno być odpowiednio wyposażone:
- monitorowane przez czujki automatyczne SSP,
- wyposażone w instalacje i urządzenia elektryczne dostosowane do ich przeznaczenia zgodnie z wymaganiami Polskich Norm dotyczących tych instalacji i urządzeń,
- zapewnione oświetlenie o natężeniu od 300 do 500 lx,
- wyposażone w awaryjne oświetlenie ewakuacyjne.

Wyposażenie w urządzenia ppoż.:
- W razie potrzeby dopuszcza się umiejscowienie central urządzeń ppoż. w PTUP, wówczas w POUP należy zlokalizować urządzenia zdalnej obsługi urządzeń ppoż. połączone z centralami za pomocą nadzorowanego redundantnego połączenia (panel wyniesiony obsługi do centrali sygnalizacji pożarowej, mikrofon alarmowy, ręczny przycisk oddymiania, ręczny ostrzegacz pożarowy).

PTUP powinno być odpowiednio oznakowane *(rys. 2)*:

POMIESZCZENIE TECHNICZNE URZĄDZEŃ PRZECIWPOŻAROWYCH

Rys. 2. Wzór oznakowania PTUP
Źródło: Wytyczne CNBOP-PIB W-0001

Oznaczenie w części graficznej IBP
- W Instrukcji Bezpieczeństwa Pożarowego w części graficznej i na planach ewakuacyjnych budynku niezbędne jest zastosowanie oznaczenia wraz z dokładną lokalizacją pomieszczenia.

W PTUP nie powinna być przechowywana dokumentacja, natomiast:
- powinien obowiązywać zakaz magazynowania i przechowywania rzeczy niezwiązanych z funkcjami pomieszczenia.
- powinien być utrzymywany stały porządek.

Dostęp do PTUP powinien być ograniczony tylko do osób uprawnionych i służb ratowniczych. Dopuszcza się zamykanie drzwi na klucz z zastrzeżeniem, że klucz znajduje się w odpowiednio oznaczonej skrzynce ze zbijaną szybą, przymocowanej do ściany w bezpośrednim sąsiedztwie drzwi do pomieszczenia.
Wytyczne określają także wymagania dotyczące lokalizacji Panelu Obsługi dla Straży Pożarnej (POSP).
POSP powinien być łatwo dostępny:
- zlokalizowany na kondygnacji budynku, na której znajduje się wejście, przewidziane i oznaczone jako wejście dla ekip ratowniczych,
- zlokalizowany w pobliżu wejścia dla ekip ratowniczych, w odległości nie większej niż 5 m od wejścia,
- POSP powinien być zamontowany na ścianie na wys. od 1,4 do 1,8 m,
- dostęp i obsługa POSP powinna być możliwa przez ratownika wyposażonego w środki ochrony indywidualnej.

Miejsce instalacji POSP powinno być oznakowane *(rys. 3)*:
- w sposób widoczny po wejściu do budynku wejściem przewidzianym dla ekip ratowniczych.

PANEL OBSŁUGI DLA STRAŻY POŻARNEJ

Rys. 3. Wzór oznakowania POSP
Źródło: Wytyczne CNBOP-PIB W-0001

Oznaczenie w części graficznej IBP
- Instrukcja Bezpieczeństwa Pożarowego w części graficznej oraz na planach ewakuacyjnych budynku powinna zawierać oznakowanie i lokalizację POSP.

WYTYCZNE CNBOP-PIB W-0002 (dotyczące wyposażania budynków w Kasety Straży Pożarnej)

Drugie z omawianych wytycznych opisuje wymagania techniczne i organizacyjne związane ze stosowaniem systemu Kasety Straży Pożarnej, w tym m.in.:
- koncepcje rozwiązań technicznych kasety straży pożarnej,
- wymagania techniczne stosowania kasety,
- wymagania organizacyjne stosowania kasety,
- wymagania dotyczące oceny poprawności działania urządzeń i ich funkcjonalności,
- podczas przekazywania systemu kaset straży pożarnej do użytkowania,
- wymagania dotyczące oceny poprawności działania urządzeń i ich funkcjonalności,
- przez straż pożarną, listy kontrolne warunki, zalecenia dot. odbiorów,
- zalecenia obsługi i użytkowania zainstalowanych systemów,
- wytyczne dla użytkownika budynku.

Poniżej przedstawiono wybrane wymagania tych wytycznych.
Lokalizacja Kasety Straży Pożarnej (KSP) powinna być:
- uzgodniona z właściwym miejscowo komendantem powiatowym/miejskim PSP,
- zapewniająca swobodny dostęp po utwardzonym podłożu,
- zabezpieczona przed negatywnym wpływem warunków atmosferycznych,
- monitorowana antysabotażowo przez system sygnalizacji włamania i napadu,
- instalowana na ścianie zewnętrznej budynku, murowanej lub betonowej,
- instalowana w odległości nie większej niż 5 m od wejścia dla straży pożarnej albo wejścia głównego, jeżeli stanowi jednocześnie wejście dla straży pożarnej do budynku,
- drzwi zewnętrzne KSP powinny być w jednej płaszczyźnie z zewnętrzną powierzchnią ściany (zlicowane),
- dolna krawędź KSP powinna znajdować się na wys. od 1,0 m do 1,5 m.

KSP nie powinna być oznakowana ze względu na ewentualne działania sabotażowe.
Drzwi wejściowe do budynku, otwierane kluczami przechowywanymi w KSP, powinny być oznakowane w sposób jednoznaczny, trwały i czytelny *(rys. 4)*:

KSP 1

Rys. 4. Wzór oznakowania drzwi otwieranych kluczem przechowywanym w KSP

SZAFKA NA KLUCZE DO POMIESZCZEŃ

Wewnątrz budynku może być zainstalowana zamykana i nadzorowana szafka na klucze do pomieszczeń wewnętrznych budynku. Zamek szafki powinien być otwierany kluczem do drzwi zewnętrznych do budynku zdeponowanym w KSP. Szafka taka powinna być oznakowana w następujący sposób:

Klucze do pomieszczeń

Rys. 5. Wzór oznakowania szafki na klucze

PODSUMOWANIE

Dostępność budynku oraz lokalizacja i dostępność urządzeń przeciwpożarowych w budynku mają kluczowe znaczenie dla jego bezpiecznej eksploatacji oraz sprawności prowadzonych działań ratowniczo-gaśniczych. Służby ratownicze po przybyciu na miejsce zdarzenia mogą, dzięki zastosowaniu systemu KSP, szybko i sprawnie dostać się do budynku.
Odpowiednio wyposażone i zlokalizowane pomieszczenie, w którym znajdują się wszystkie elementy sygnalizacyjno-obsługowe urządzeń ppoż., pozwala służbom odczytać informacje z działających w budynku systemów i podjąć adekwatne działania, w tym także z wykorzystaniem tych systemów. Umożliwi to sprawne przeprowadzenie działań i szybsze udzielenie pomocy poszkodowanym oraz zmniejszy skutki wystąpienia pożaru lub innego zdarzenia.
Cel ten może być zrealizowany poprzez przyjęcie odpowiednich założeń projektowych i stosowanie dostępnych wytycznych, które stanowią uzupełnienie wymagań zawartych w przepisach techniczno-budowlanych, a ich stosowanie jest zalecane.

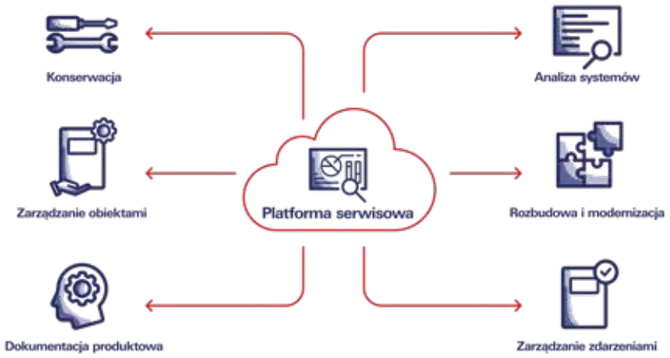
Omawiane w artykule wytyczne CNBOP-PIB są dostępne pod adresem https://www.cnbop.pl/pl/wydawnictwa/wytyczne.

MŁ. BRYG. MGR INŻ. GRZEGORZ MROCZKO

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

Integral Remote – narzędzia zdalnego dostępu do systemu Integral EvoxX

Firma Schrack Seconet szczególnie dba o ciągły rozwój systemu Integral EvoxX, rozbudowę o innowacyjne rozwiązania służące poprawie bezpieczeństwa i zwiększenie jego funkcjonalności.



Fot. 1. S2Service

Prężnie rozwijane są produkty dedykowane do zdalnego dostępu należące do pakietu Integral Remote. Jego zalety dostrzegają wszyscy interesariusze rynku systemów bezpieczeństwa pożarowego – inwestorzy, zarządcy i integratorzy oraz osoby obsługujące i serwisujące instalacje sygnalizacji pożarowej. W skład pakietu wchodzą:

1. Platforma serwisowa S2Service *(fot. 1)*

– platforma informatyczna pracująca w chmurze spełniającej najwyższe standardy bezpieczeństwa. Ma szereg innowacyjnych funkcjonalności poprawiających jakość usług na każdym etapie procesów wdrożeniowych i serwisowych:

- **Dokumentacja projektowa** – pełny dostęp do najnowszej dokumentacji produktowej, projektowej i informacji serwisowych. Szybkie wyszukiwanie elementów (zeskanowanie kodu QR).
- **Zarządzanie obiektami** – platforma serwisowa umożliwia zapisanie plików konfiguracyjnych dla danego obiektu w chmurze, co, oprócz bezpiecznego przechowywania i pewności pracy na najnowszej wersji programu daje możliwość analizy plików pod kątem poprawności zaprogramowania systemu.
- **Analiza systemu** – wbudowane algorytmy do szczegółowej analizy oprogramowania dla danego systemu pod kątem poprawności oprogramowania, przyjętych rozwiązań i ich wzajemnej kompatybilności.
- **Rozbudowa i modernizacja** – automatyczna analiza obłożenia systemu. Szczegółowa informacja o możliwościach rozbudowy, elementów zarówno wyposażenia central, jak i peryferyjnych.
- **Konserwacja** – wsparcie procesu konserwacji systemu na każdym etapie. Automatyczne generowanie protokołów serwisowych, list przetestowanych elementów i list nieprawidłowości. Możliwość szybkiego dodania dokumentacji fotograficznej ewentualnych nieprawidłowości bezpośrednio do raportu z przeglądu.
- **Zarządzanie zdarzeniami** – platforma serwisowa, wykorzystując bezpieczne połączenie poprzez routery S2Service, ma dostęp do wszystkich zdarzeń mających miejsce w systemie w czasie rzeczywistym. Można też łatwo przypisać dane zdarzenie jako zgłoszenie serwisowe do konkretnego użytkownika platformy.

2. Integral Application Center

– pakiet dla programistów i instalatorów systemu Integral EvoxX. Dzięki technologii IP obecnej w każdej centrali z rodziny Integral EvoxX wszystkie urządzenia mogą być zdalnie zarządzane w pełnym zakresie funkcji. Operacje związane z wdrażaniem systemu, dotychczas wykonywane wyłącznie lokalnie w obiekcie, obecnie w coraz większym zakresie mogą być też realizowane zdalnie dzięki komunikacji za pomocą protokołu TCP/IP z wykorzystaniem dedykowanych sieci LAN/WAN lub w ramach Internetu. Oprogramowanie IAC może być wykorzystywane do następujących celów:

- zdalnej diagnostyki – odpytywanie systemu i analiza aktualnych stanów pracy SSP w ramach uzupełnienia do standardowo prowadzonego serwisu i przeglądu instalacji sygnalizacji pożarowej,
- zdalnego wsparcia technicznego podczas procesu uruchamiania systemu (np. analiza i rozwiązywanie problemów przez inżynierów wsparcia technicznego producenta),
- odbierania informacji o stanach systemowych w obiektach bezzałogowych, np. uszkodzenia, informacje serwisowe (poziom zabrudzenia czujek, stan wysterowań),
- zdalnej obsługi SSP z poziomu stacji roboczej PC przez inżyniera serwisu technicznego itp.

3. INTEGRAL DESKTOP

– przeznaczony do obsługi i nadzorowania instalacji na komputerach stacjonarnych. Program wyświetla odwzorowany 1:1 panel obsługi centrali sygnalizacji pożarowej Integral EvoxX, oferując tym samym narzędzie do wygodnej obsługi w czasie rzeczywistym. Wersja językowa interfejsu może być dostosowana do operatora i dowolnie zmieniana nawet podczas pracy oprogramowania.
Bezpieczeństwo korzystania z oprogramowania Integral Desktop zapewnia wdrożona wielopoziomowa koncepcja bezpieczeństwa. Aplikacja jest chroniona kluczem sprzętowym, a użytkownik na etapie logowania się aplikacji do systemu Integral EvoxX musi podać użytkownika uprawnionego do zdalnego dostępu oraz hasło. Następnie po wybraniu kodu dostępu, operator wchodzi na odpowiedni poziom dostępu na panelu obsługi w taki sam sposób, jak w przypadku standardowego panelu obsługi MAP centrali Integral EvoxX.

4. INTEGRAL MOBILE/ /INTEGRAL BROWSER

– przeznaczone do zdalnego nadzorowania i obsługi instalacji sygnalizacji pożarowej z wykorzystaniem urządzeń mobilnych. Aplikacja odwzorowuje panel centrali Integral EvoxX w celu podglądu zdarzeń i wykonywania ewentualnych operacji serwisowych przez uprawnionych użytkowników. Ponadto wspiera technologię aktywnych powiadomień *(push notification),* dzięki czemu operator zostanie powiadomiony o wszystkich krytycznych zdarzeniach, które wystąpią w nadzorowanym SSP.
Atutem w kwestii bezpieczeństwa, na który producent kładzie duży nacisk, jest możliwość zdefiniowania koordynat GPS do określenia dozwolonego obszaru, z którego może być wykonywana zdalna obsługa. W skład pakietu wchodzi też aplikacja Integral Browser, która umożliwia nadzorowanie i obsługę SSP z poziomu panelu obsługi prezentowanego w przeglądarce internetowej.

5. INTEGRAL MESSAGE

– przeznaczony do zdalnego nadzorowania wielu niezależnych instalacji sygnalizacji pożarowej Integral EvoxX podłączonych do serwera systemu, który wraz ze stanowiskami operatorskimi stanowi centrum nadzoru. Główne zadania oprogramowania: informowanie o zdarzeniach występujących w nadzorowanych systemach, zapisywanie ich w bazie danych oraz wyświetlanie na stacjach klienckich, które można swobodnie konfigurować zarówno w zakresie wysyłanych komunikatów, jak i obsługiwanych instalacji (projektów). Wszystkie komunikaty są przedstawiane w formie tabelarycznej, z określeniem rodzaju zdarzenia (alarm, uszkodzenie itp.), nazwy obiektu i szczegółowego opisu zdarzenia. Podczas każdego zdarzenia na ekranie komputera są wyświetlane powiadomienia typu pop-up, dzięki którym operator nie pominie kluczowych informacji z nadzorowanych systemów. Ponadto z daną instalacją można się łatwo i szybko połączyć za pomocą aplikacji Integral Desktop, która jest nieodłączną częścią oprogramowania Integral Message. Wszystkie operacje użytkowników są rejestrowane w systemie.

6. INTEGRAL MAIL

– umożliwia wysyłanie e-maili bezpośrednio z centrali SSP, która łącząc się z dedykowanym serwerem pocztowym, wysyła informacje o najważniejszych zdarzeniach w systemie Integral EvoxX (alarm, uszkodzenie itp.) na zdefiniowane adresy e-mailowe użytkowników. Zakres wysyłanych komunikatów można dowolnie konfigurować w zależności od tego, kto jest ich odbiorcą i jakie informacje są dla niego kluczowe. Wymienione rozwiązania mogą być oparte na certyfikowanej (pod względem bezpieczeństwa) platformie chmurowej producenta S2Service, która umożliwia zestawienie bezpiecznych połączeń z wykorzystaniem tuneli VPN pomiędzy aplikacjami a nadzorowanymi obiektami. Wszystkie routery pracują w chmurze S2Service i są zarządzane przez producenta, co gwarantuje najwyższy poziom bezpieczeństwa.
W pakiecie zdalnego dostępu zaimplementowano zaawansowane rozwiązania w zakresie bezpieczeństwa połączenia aplikacji z SSP, zapewniające ochronę przed nieautoryzowanym dostępem i przypadkowym wpływem na sposób działania krytycznych elementów instalacji. Przyjęta koncepcja bezpieczeństwa uwzględnia kryteria obowiązujących norm i wytycznych. Zależnie od wymagań można tworzyć dowolną liczbę użytkowników zdalnych i przypisywać im określone funkcje i sposoby autoryzacji. Poziom bezpieczeństwa można indywidualnie ustawić dla każdego użytkownika, a jego dane i hasłach są zapisane w sposób zaszyfrowany w CSP – ich zmiana wymaga przeprogramowania systemu przez autoryzowany personel.
W celu zwiększenia poziomu bezpieczeństwa można zastosować autoryzację dwustopniową w razie potrzeby wykonywania zdalnych operacji na elementach SSP. Funkcjonuje to następująco: po zalogowaniu się do systemu poprzez wpisanie nazwy użytkownika i hasła zdalny operator ma dostęp tylko do informacji o aktualnym stanie systemu. Aby móc obsługiwać system, musi uzyskać pozwolenie od personelu ochrony obiektu, który zdalnie autoryzuje połączenie z poziomu panelu obsługi centrali Integral EvoxX.

System Zarządzania Ciągłością Działania (BCMS)

Cz. 5. Kolejne kroki – Etap 2. (analiza ryzyka)

Tomasz Guzikowski

Zarządzający przedsiębiorstwem muszą dbać o rozwój firmy. Zabezpieczenie nieprzerwanego jej funkcjonowania zapewnia system zarządzania ciągłością działania. Oto kolejny etap – analiza ryzyka.

Na tym poziomie odbywa się identyfikacja kluczowych zagrożeń dla ciągłości działania krytycznych procesów realizowanych w organizacji. Norma europejska ISO 22301 wymaga, aby organizacja wdrożyła i utrzymywała formalny proces oceny ryzyka, który systematycznie identyfikuje, analizuje i ocenia nie tylko ryzyko zakłócenia priorytetowych działań i procesów, ale także systemów, informacji, ludzi, aktywów, dostawców oraz innych zasobów, które je wspierają.

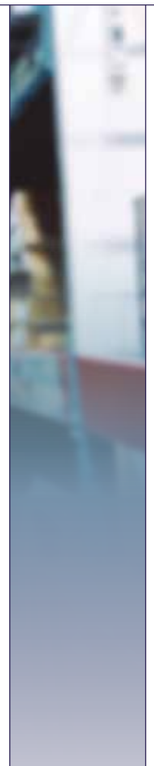
Proces ten powinien uwzględniać kontekst organizacji oraz potrzeby i oczekiwania zainteresowanych stron. Realizując go, należy mieć świadomość zagrożeń i podatności istotnych dla zasobów wymaganych przez działania organizacji, w szczególności:

- wykorzystanie zasobów wymaganych podczas działań priorytetowych,
- czas działań związanych z danym zasobem – czy nie jest dłuższy niż cel czasu odtworzenia danego działania.

Należy również wybrać odpowiednią metodę identyfikacji, analizy i oceny ryzyka, które może prowadzić do zakłóceń w funkcjonowaniu. Rekomendowana jest w tym przypadku norma ISO 31000 – Zarządzanie ryzykiem. Zasady i wytyczne.

Aby zrealizować cel niniejszego kroku, należy przeprowadzić następujące działania:

- Identyfikacja kluczowych zagrożeń mogących doprowadzić do zatrzymania produkcji, przerwy w dostawie surowca lub innych negatywnych skutków dla kluczowych procesów zidentyfikowanych w poprzednim kroku.
- Identyfikacja stosowanych zabezpieczeń wpływających na zapewnienie ciągłości działania, w tym analiza funkcjonującej w organizacji dokumentacji dotyczącej ciągłości działania.
- Przeprowadzenie szacowania ryzyka z wykorzystaniem wybranej metodyki obowiązującej w organizacji oraz listy zidentyfikowanych zagrożeń w celu określenia prawdopodobieństwa wystąpienia każdego z nich, a także wpływu ich wystąpienia na ciągłość działania i związane z tym konsekwencje.
- Wybór kluczowych zagrożeń dla ciągłości działania poprzedzony potwierdzeniem, jakie poziomy ryzyka są akceptowalne na podstawie przyjętego w metodyce poziomu akceptowania ryzyka.



- Opracowanie strategii zapewnienia ciągłości funkcjonowania dla wybranych, kluczowych zagrożeń/zakłóceń obejmujących działania zmierzające do:
  - zabezpieczenia kluczowych zasobów przed ryzykiem sytuacji awaryjnych,
  - ustabilizowania, zapewnienia ciągłości oraz odtworzenia kluczowych procesów w przypadku materializacji ryzyka,
  - zapewnienia odpowiedniego stanu zasobów magazynowych, personelu utrzymania oraz alternatywnych źródeł zaopatrzenia,
  - zabezpieczenia uszkodzonych elementów infrastruktury.
  - Opracowanie raportu stanowiącego podsumowanie zidentyfikowanych zagrożeń/incydentów/zakłóceń oraz rekomendacji postępowania (plan postępowania z ryzykiem).

Z punktu widzenia organizacji ważne jest sklasyfikowanie rodzajów zagrożeń i oszacowanie ryzyka, aby w następstwie ich wystąpienia można było odpowiednio wdrożyć opracowane scenariusze działań awaryjnych. Przykładowy podział może być zawarty w następujących grupach, które mają realny wpływ na utrzymanie ciągłości działania:

- zarządzanie zasobami ludzkimi,
- zarządzanie finansami,
- infrastruktura,
- zakupy,
- logistyka i sprzedaż.

Zagrożenia można również podzielić na techniczne i nietechniczne. Przykładowo mogą to być m.in.:

- zły stan techniczny i awarie urządzeń i budynków,
- zakłócenia w funkcjonowaniu sieci i systemów informatycznych,
- awarie systemów i urządzeń IT,
- przerwy w zasilaniu,
- susza i niedobór wody,
- brak podstawowych surowców produkcyjnych,
- niedostępność pracowników,
- zmiana regulacji prawnych,
- ryzyka środowiskowe,
- epidemia,
- protesty społeczne (związki zawodowe),
- zagrożenie terrorystyczne i cyberterroryzm,
- inne zakłócenia:
  - kradzież, wandalizm, sabotaż,
  - pożar,
  - śnieżyca/mróz/upały,
  - siła wyższa/decyzje administracyjne.

Scenariusze działań, które organizacja będzie mogła wykorzystać zarówno w razie przewidzianych, jak i nieprzewidzianych incydentów, powinny ponadto zawierać następujące istotne elementy:

- komunikacja kryzysowa w celu utrzymania swoich klientów,
- utrzymanie wyższych stanów zapasów produktów/surowców na okres utraty ciągłości działania,
- zdefiniowanie, jeśli to możliwe, alternatywnych sposobów realizacji krytycznych procesów biznesowych,
- opracowanie i wdrożenie planu odbudowy obszaru IT w celu jak najszybszego odzyskania dostępu do danych i systemów/aplikacji,
- wymiana lub naprawa uszkodzonych maszyn i urządzeń,
- ponowne zamówienie zniszczonych czy utraconych zapasów i materiałów,
- przeniesienie lub zabezpieczenie uszkodzonej infrastruktury/instalacji,
- zapewnienie alternatywnych źródeł zaopatrzenia.

Dalsze kroki w kolejnych artykułach.

TOMASZ GUZIKOWSKI

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

Ustawa o obronie Ojczyzny

i wpływ jej postanowień na branżę safety&security. Cz. 2.

Sejm i Senat RP uchwaliły – podobno przez aklamację – a Prezydent RP podpisał w trybie *cito* ustawę z dnia 11 marca 2022 r. o obronie Ojczyzny. Rządowe Centrum Legislacji opublikowało ją, chyba też w trybie *cito*, już 23 marca 2022 r. w Dzienniku Ustaw RP z br. pod pozycją 655. Ustawa weszła w życie z dniem 23 kwietnia 2022 r. przy czym jej art. 288 ust. 2 i art. 777 ust. 4 już z dniem 24 marca 2022 r.; natomiast art. 439 ust. 1 pkt 4 – wejdzie dopiero 1 stycznia 2023 roku. Generalnie *vacatio legis* tej ustawy (poza wymienionym fragmentem art. 439) nie trwało długo, biorąc pod uwagę fakt, że liczy ona 824 artykuły ujęte w 26 działach tematycznych. Jej wydruk papierowy czcionką i w formacie jak w Dz.U. RP liczy 248 stron A4.

Marek Ryszkowski

W poprzednim numerze „a&s" przedstawiłem wybrane przepisy Ustawy o obronie Ojczyzny zawarte w Działach XX. Militaryzacja i ochrona obiektów szczególnie ważnych dla bezpieczeństwa lub obronności państwa oraz XXI. Świadczenia na rzecz obrony. Obecnie odniosę się do przepisów znajdujących się w Działach XXII i XXV, które są istotne dla przedsiębiorców z branży security & safety.

DZIAŁ XXII. ORGANIZOWANIE ZADAŃ REALIZOWANYCH PRZEZ PRZEDSIĘBIORCÓW NA RZECZ SIŁ ZBROJNYCH

W tym obszernym Dziale liczącym 6 rozdziałów ustawodawcy zawarli wiele przepisów, które przede wszystkim będą miały wpływ na warunki prowadzenia biznesu przez te podmioty prawa handlowego (PPH) branży safety & security (dalej s&s), które zostaną zmilitaryzowane. Zatem z przepisami tego Działu powinien szczególnie dokładnie zapoznać się Zarząd każdego z nich. Dwa pierwsze rozdziały tego Działu określają *...zadania na rzecz Sił Zbrojnych realizowane przez przedsiębiorców (R.1) i plan zabezpieczenia potrzeb Sił Zbrojnych realizowanych przez przedsiębiorców* (R.2). Warto zwrócić uwagę na cytowane niżej przepisy:

- *art. 649 – Zadania przedsiębiorcy (...) obejmują uzupełnienie jego potrzeb kadrowych, sprzętowych i materiałowych wynikających ze struktury jednostki przewidzianej do militaryzacji albo zmilitaryzowanej oraz inne (pogrubienia w cytatach – MR) przedsięwzięcia w zakresie przygotowań organizacyjno-mobilizacyjnych. Wykonanie tego zadania przedsiębiorca ma sfinansować własnymi środkami (art. 603 ust. 2 w Dziale XX „Militaryzacja i ochrona obiektów szczególnie ważnych dla bezpieczeństwa lub obronności państwa").*
- *art. 650 – Zadania przedsiębiorców w zakresie ochrony obiektów szczególnie ważnych dla bezpieczeństwa lub obronności państwa stanowią zadania, o których mowa w art. 613 ust. 2 i 3 oraz w: 1) art. 5 ustawy z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz.U. z 2021 r. poz. 1995) w zakresie obiektów, w tym: obiektów budowlanych, urządzeń, instalacji, usług ujętych w jednolitym wykazie obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej; 2) przepisach wydanych na podstawie art. 6 ust. 7 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2022 r. poz. 261 i 583), w zakresie zadań z obszaru ochrony infrastruktury krytycznej.*

Dokumentem planistycznym w zakresie realizacji zadań wykonywanych przez przedsiębiorców jest *Plan zabezpieczenia potrzeb Sił Zbrojnych realizowanych przez przedsiębiorców*, który opracowuje Minister Obrony Narodowej na okres 5 lat (art. 651). Podlega on aktualizacji w formie aneksu do istniejącego Planu. Minister Obrony Narodowej, w drodze rozporządzenia, określa *sposób i tryb opracowywania Planu i aneksu do Planu oraz załączników do Planu lub aneksu do Planu, a także zawartość oraz strukturę tych dokumentów...* (art. 653). Natomiast Prezes Rady Ministrów na wniosek *Ministra Obrony Narodowej podejmuje decyzję o uruchomieniu planu w drodze rozporządzenia* (art. 654).

Wymagania wobec przedsiębiorców będących osobami fizycznymi zawarli ustawodawcy w art. 657, który liczy 10 punktów. Istotny jest pkt 2), podzielony na litery od a) do j), w którym określono wymagania prawne (przede wszystkim niekaralność za przestępstwa w nich wyszczególnione). Przepisy znajdujące się w tym punkcie obejmują nie tylko przedsiębiorców, ale także członków zarządu i osoby zatrudnione przez przedsiębiorcę (np. współwłaściciele) oraz inne osoby wskazane w przepisach tego punktu. Istotne dla przedsiębiorców są również przepisy punktów 9) i 10) tego artykułu. Zawarto w nich wymagania dotyczące posiadania przez przedsiębiorców *koncesji, licencji* [i] *zezwoleń do prowadzenia działalności gospodarczej* (pkt 9) oraz *zdolność do przetwarzania informacji niejawnych* (pkt 10), jeśli jest to określone przez Ministra Obrony Narodowej jako wymóg przy wykonywaniu zadań.

Art. 658 zawiera (w ust. 1 i 2) przepisy administracyjne dotyczące obowiązków przedsiębiorcy dot. zgłaszania zmian w statusie prawnym, organizacji, lokalizacji przedsiębiorstwa itd., znane dobrze przedsiębiorcom branży s&s. Artykuły 659 i 660 dotyczą *zasad finansowania zadań na rzecz Sił Zbrojnych*. Przepisy w nich zawarte są z pewnością istotne dla przedsiębiorców branży s&s,

zatrudniają oni jednak specjalistów z tego zakresu, którzy najlepiej wskażą im ewentualne niejasności lub nawet pułapki znajdujące się w przepisach tych artykułów. Zdaniem autora piszącego ten tekst brzmienie art. 660 może stanowić jedną z tych pułapek, gdyż przewiduje się w nim, co następuje: *Koszty realizacji zadań na rzecz Sił Zbrojnych oraz służb specjalnych (...) poniesione przez przedsiębiorcę, zostaną temu przedsiębiorcy pomniejszone o wartość otrzymanych w ramach rezerw strategicznych surowców i materiałów niezbędnych do zabezpieczenia ich realizacji. Nie ma delegacji dla Rady Ministrów do określenia zasad i trybu określania ww. wartości, zatem i wielkości pomniejszenia wspomnianych kosztów.*

Końcowe przepisy Działu XXII (artykuły 661, 662, 663 i 664) określają ogólne zasady nadzoru i kontroli nad realizacją zadań na rzecz Sił Zbrojnych (i nie tylko) oraz wskazują, że je sprawuje Minister Obrony Narodowej. Krytyczne omówienie tych przepisów wykracza poza ramy artykułu, gdyż musiałoby być obszerne ze względu na bogatą w RP bibliotekę przepisów o sprawowaniu nadzoru i kontroli przez organy władzy publicznej. Nadzór i kontrola sprawowane przez Ministra Obrony Narodowej nad realizacją ww. zadań poddane będą zatem nie tylko przepisom tych czterech artykułów Ustawy o obronie Ojczyzny.

DZIAŁ XXV. PRZEPISY KARNE

W skład tego Działu wchodzą artykuły od 681 do 697 omawianej ustawy, których przepisy mogą mieć istotny wpływ na działalność biznesową tych podmiotów prawa handlowego branży s&s, które zmilitaryzowano i/lub tych, którym powierzono wykonywanie zadań na rzecz Sił Zbrojnych i na zasadach określonych w tejże ustawie. Oto co o tych przepisach sądzi autor tego tekstu.

- *art. 681 – Kto wbrew obowiązkom wynikającym z ustawy: (...) – podlega karze ograniczenia wolności albo grzywny. W miejscu wykropkowanym wyszczególniono enumeratywnie rodzaje czynności lub zaniechań, które ustawodawcy ocenili jako naruszenie jakiegoś przepisu omawianej ustawy. Nie określono w tym art., który(e) organ(y) władzy publicznej i w jakim trybie upoważnia się do oceniania zaistnienia naruszenia i określania wymiaru kar albo grzywien, o których mowa w tym artykule.*
- *art. 682 – Kto bez usprawiedliwionej przyczyny: (...) – podlega karze aresztu albo grzywny. Uwaga jw., z zastrzeżeniem, że w tym art. chodzi niemal wyłącznie o zaniechania wykonania jakiejś czynności (zadania) przez obywatela zobowiązanego do jej (jego) wykonania, nałożonej (nałożonego) nań prawomocnie na podstawie przepisów tej ustawy.*
- *art. 683 – Kto wbrew obowiązkom wynikającym z ustawy: (...) – podlega karze aresztu albo grzywny. Uwaga jw., z zastrzeżeniem, że w tym art. chodzi wyłącznie o zaniechania nałożonych prawomocnie na obywatela obowiązku świadczeń osobistych i/lub rzeczowych.*
- *art. 684 – Dopiero w tym art. zapisano, że orzekanie w ww. sprawach następuje na podstawie przepisów ustawy z dnia 24 sierpnia 2001 r. – Kodeks postępowania w sprawach o wykroczenia.*
- *art. od 685 do 689 określają liczne rodzaje czynów, za których popełnienie sprawcom grożą kary pozbawienia wolności orzekane w większości przez sądy wojskowe, co wynika z przepisu art. 692. I tak: do roku pozbawienia wolności – art. 686, do 2 lat pozbawienia wolności – art. 685, do 3 lat pozbawienia wolności – art. 687 i 689, do 5 lat pozbawienia wolności – art. 688.*
- *art. 690 i 691 precyzują, na czym polegają czyny, o których mowa w art. od 681 do 689.*
- *art. 693 i 694 odnoszą się wprost do przedsiębiorców, którym za popełnienie niektórych, szczególnego rodzaju czynów, o których mowa w tych artykułach, grożą kary pozbawienia od roku do 5 lat pozbawienia wolności. Przedsiębiorcy branży s&s, którzy często zatrudniają byłych żołnierzy zawodowych, powinni – wraz ze swoimi doradcami prawnymi – dogłębnie przestudiować te i inne przepisy tego Działu.*
- *art. 695 – Przedsiębiorca, który nie realizuje nałożonego zadania na rzecz Sił Zbrojnych lub służb specjalnych, (...), odmówi poddania się kontroli lub będzie ją utrudniać, podlega karze pieniężnej. Kary te, w wysokości od 10- do 30-krotności przeciętnego miesięcznego wynagrodzenia w sektorze przedsiębiorstw bez wypłat nagród z zysku w czwartym kwartale roku poprzedniego, ogłoszonego przez Prezesa Głównego Urzędu Statystycznego w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski" nakłada Minister Obrony Narodowej, w drodze decyzji administracyjnej (art. 696). Kary mogą być dotkliwe dla wielu przedsiębiorców branży s&s, gdyż ich minimalna wysokość to obecnie ok. 60 tys. zł, a maksymalna – ok. 180 tys. zł). Nakładane są w trybie decyzji administracyjnej, zatem w procesie ich nakładania stosuje się odpowiednio przepisy działu IVa ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (art. art. 697).*

Prezentowany w artykule przegląd wybranych przepisów Ustawy o obronie Ojczyzny nie jest ich analizą prawną sensu stricte. Analizy prawa o obronie Ojczyzny będą mogli dokonać prawnicy dysponujący nie tylko tekstem ustawy, ale też rozporządzeniami i innymi aktami wykonawczymi, które ukażą się w ciągu najbliższych 18 miesięcy na podstawie zawartych w tej ustawie delegacji – a więc kompletem przepisów niezbędnych do takiej analizy.
Jeżeli lektura obu części artykułu skłoni przedsiębiorców branży security & safety i zatrudnianych przez nich prawników do uważnej obserwacji rozwoju legislacji w dziedzinie obrony Ojczyzny, co niewątpliwie będzie w ich interesie, to spełni on swoje zadanie.

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.

Nowe technologie przyszłością sektora ochrony

30 lat PZP Ochrona

Zastosowania nowych technologii i zagrożenia dla prowadzenia biznesu w branży ochrony to tematy, które zdominowały Walne Zgromadzenie Polskiego Związku Pracodawców Ochrona. Wydarzenie, które odbyło się 6 czerwca 2022 r. w Jachrance pod Warszawą, połączono z uroczystymi obchodami 30-lecia organizacji.

OTOCZENIE BIZNESOWE BRANŻY OCHRONY

Zagrożeń dla prowadzenia biznesu w branży ochrony nie brakuje, o czym otwarcie mówiono podczas Walnego Zgromadzenia. Są to zarówno zmiany w przepisach prawa, nieuwzględniające specyfiki branży (omawiała je Grażyna Spytek-Bandurska z Federacji Przedsiębiorców Polskich), zapowiedź Krajowego Planu Odbudowy i jego wpływ na „oskładkowanie" wszystkich umów zleceń, które w sektorze ochrony są stosowane dość powszechnie, jak i coroczne podwyżki płacy minimalnej mające realny wpływ na rentowność i rozwój firm.

Ważnym zagadnieniem poruszonym przez Jakuba Dzika, eksperta PZPO, był wpływ inflacji na sytuację w branży. Zwrócił on uwagę, że w ciągu roku koszty prowadzenia działalności w sektorze ochrony wzrosły o ok. 100%, jednocześnie niskie bezrobocie przyczynia się do coraz większych problemów z pozyskaniem nowych pracowników. To wszystko w połączeniu z wysoką inflacją stanowi mocny argument za podniesieniem cen usług świadczonych przez sektor ochrony. Zwrócono też uwagę, że zgodnie z założeniami Ministerstwa Finansów od 1 stycznia 2023 r. obligatoryjne stanie się wystawianie faktur za pośrednictwem Krajowego Systemu e-Faktury. Problemy, korzyści i zagrożenia z tego wynikające omawiał doradca podatkowy Piotr Litwin. W jaki sposób poświęcać mniej zasobów firmy na administrację, a więcej na rozwój biznesu, podpowiadał natomiast Michał Zębala.

Gościem Walnego Zgromadzenia była przedstawicielka Państwowej Inspekcji Pracy (PIP), która omawiała zakres kontroli przedsiębiorstw branży ochrony osób i mienia w ub. roku. Wiele zarzutów dotyczyło podejrzenia o zaniżanie cen przez przedsiębiorców, co stanowi znamiona nieuczciwej konkurencji. W sumie w 2021 r. PIP przyjął 68 zgłoszeń dotyczących różnych spraw, wszczęto 18 postępowań, z czego 6 zrealizowano (w tym 5 postępowań wyjaśniających). Urząd skierował jedno zawiadomienie o przeprowadzenie kontroli do NIK.

Ważnym partnerem dla Związku jest policja, która co roku gości na wydarzeniach organizowanych przez PZPO, niezmiennie zwracając uwagę na wymagania stawiane przed firmami z sektora ochrony oraz dotyczące kontroli Specjalistycznych Uzbrojonych Formacji Ochronnych (SUFO). Delegaci postulowali o udostępnienie branży ochrony systemu umożliwiającego sprawdzenie uprawnień pracowników, co ułatwiłoby pracę firm ochrony lub przynajmniej dostęp do bazy danych Krajowego Rejestru Karnego (KRK) w celu weryfikacji poprawności oświadczeń o niekaralności. W pierwszym przypadku policja nie dysponuje uprawnieniami do udostępnienia bazy, a stworzenie nowego systemu wykracza poza jej możliwości finansowe. W przypadku KRK sprawa będzie konsultowana.

OKRĄGŁA ROCZNICA POWSTANIA PZPO

– W tym roku mija 30 lat od powstania Związku, a to dłużej niż obowiązuje ustawa o ochronie osób i mienia – mówi Tomasz Wojak, prezes PZPO.

Obchody tak znaczącej rocznicy musiały odbyć się w sposób wyjątkowy, tym bardziej że miały miejsce po długiej przerwie spowodowanej pandemią. Przygotowane z dbałością o każdy szczegół Walne Zgromadzenie zorganizowano w hotelu Warszawianka w Jachrance, który zapewnił komfort, wygodę oraz odpowiednią oprawę do świętowania. Oprócz części formalnej nie mogło zabraknąć uroczystej gali, podczas której nagrodzono, wyróżniono i doceniono zasłużonych pracodawców branży ochrony osób i mienia, którzy działają na rynku od 10, 20, a nawet 30 lat, a w tym roku obchodzili własne jubileusze.

PRZYSZŁOŚĆ BRANŻY OCHRONY

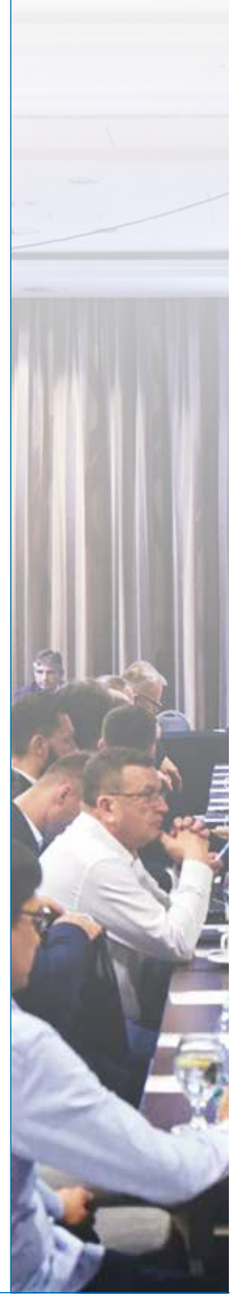
Ważną rolą Walnego Zgromadzenia było wskazanie kierunku rozwoju branży ochrony, a tym bez wątpienia jest rozwój technologiczny. Jak podkreśla Jarosław Kur, podczas spotkania zostały przekazane ważne kwestie merytoryczne dotyczące chociażby wygaśnięcia nadawania sieci w systemie 2G/3G, które czekają nas już niebawem, i przejście na systemy 4G, które będą wymagały nowej generacji urządzeń do monitoringu sygnałów alarmowych. Problem omówili Krzysztof Kołtun i Piotr Smuniewski.

Na co jeszcze zwrócono uwagę? Kwestie techniczne dotyczące wykorzystania kamer, zmiany znaczenia centrów monitorowania oraz liczba prelegentów, którzy o tym mówili, jasno wskazują, w jakim kierunku będzie zmierzać branża. Tadeusz Glita zwrócił uwagę, że ochrona techniczna, która przed 2016 rokiem miała szczątkowy udział w ochronie mienia, na koniec 2020 r. uzyskała poziom 40–50% rynku ochrony fizycznej, a planowany udział ochrony technicznej na koniec 2025 r. znacząco przewyższy udział klasycznej ochrony fizycznej. Dlatego tak ważne jest inwestowanie w rozwój zwiększający potencjał centrum monitorowania.

O sprawdzonych technologiach w nowoczesnych usługach wideomonitoringu mówił Arkadiusz Seta, podkreślając wpływ analityki AI (sztucznej inteligencji) w zakresie security i safety, która znalazła zastosowanie w nowoczesnym urządzeniu AIBOX – inteligentnym nadajniku wideoalarmów oraz funkcjonowaniu kamer z wbudowanym nadajnikiem.

Zastosowanie sztucznej inteligencji w innowacyjnych rozwiązaniach omawiał na przykładzie technologii AcuSense także Rafał Rubik. AI pozwala na klasyfikację ruchomych obiektów człowiek/pojazd oraz filtrację fałszywych alarmów pochodzących od obiektów innego typu (np. ruchome gałęzie, liście, zwierzęta, nagłe zmiany poziomu oświetlenia, cienie, opady atmosferyczne itp.).

Prelegenci starali się również odpowiedzieć na pytanie, co przyniesie przyszłość. Zdaniem Daniela Kamińskiego ta będzie zdominowana przez usługę kontroli dostępu, serwer zarządzający w chmurze, analizę wideo ze wsparciem sztucznej inteligencji czy mechanizmy „głębokiego uczenia się".



Temat korzystania z chmury, jako jednego z filarów transformacji cyfrowej branży ochrony, pojawił się podczas wystąpień kilkukrotnie. W Polsce w 2021 r. 29% firm deklarowało korzystanie z rozwiązań chmurowych przy średniej unijnej ponad 40%. Ważne zatem, co podkreślał podczas prezentacji Krzysztof Ciesielski, aby z chmury zaczęły także korzystać firmy branży ochrony w zakresie np. komunikacji marketingowej i obsługi klienta, usług ochrony fizycznej czy jako wsparcie grup i patroli interwencyjnych. To nowoczesne i bezpieczne narzędzie może mieć wiele zastosowań. Jednym z możliwych jest np. korzystanie z systemu wsparcia pn. NASA (Nowa Automatyzacja Systemów i Aplikacji), o którym opowiadał Piotr Małecki. To aplikacja automatyzująca pracę poprzez samoczynne wypełnianie dokumentów.

Dużym zainteresowaniem zgromadzonych cieszył się temat dotyczący wykorzystania dronów przybliżony przez Urszulę Mróz. Proponowane rozwiązania umożliwiają patrolowanie terenu i weryfikację fałszywych alarmów, ograniczając przy tym koszty operacyjne. Jakub Sobek podczas prezentacji nt. technologii bezprzewodowych w zabezpieczeniach technicznych zaznaczył, że aby lepiej przygotować się na przyszłe zagrożenia, już teraz trzeba poszukiwać innowacyjnych technologii, które pozwolą stworzyć skuteczne systemy zabezpieczenia technicznego.

Walne Zgromadzenie PZPO było ważnym wydarzeniem dla całego sektora w Polsce. Oprócz możliwości wymiany poglądów dotyczących kluczowych wyzwań stojących przed branżą w najbliższym czasie uczestnicy mogli zapoznać się z nowoczesnymi rozwiązaniami technologicznymi, które znajdą zastosowanie w firmach obszaru security, a w niedalekiej przyszłości będą mieć realny wpływ na ich kształt i rozwój.

Doświadczenie w terenie
Security BootCamp

Trzeci raz zorganizowaliśmy wyjątkowe szkolenie dla security menedżerów – Security BootCamp. Tym razem na terenie szkockiego rancza Highland w Naruszewie uczestnicy rozwiązywali szereg problemów z zakresu bezpieczeństwa. Każde ze stanowisk partnerskich dotyczyło innego segmentu branży. Goście mogli zmierzyć się z zadaniami z zakresu kontroli dostępu, monitoringu wizyjnego, platform integrujących systemy zabezpieczeń, systemów sygnalizacji pożarowej oraz planowania procesów logistycznych.

PARTNERZY WYDARZENIA:

Axis Communications, Genetec, Nedap Security Management, Schrack-Seconet oraz Securitas Polska.

Tomasz Grzelak

DPD Polska

Możemy sprawdzić zastosowanie nowego sprzętu i nowych rozwiązań rynkowych w terenie. Możliwość przetestowania nowości w świecie szybko zmieniających się technologii bardzo pomaga security menedżerom.

Patryk Polit

Straż Miejska w Łodzi

Takie szkolenia pozwalają poznać najnowsze zdobycze technologii z zakresu security. To pomaga w pracy i może bezpośrednio wpływać na bezpieczeństwo naszych mieszkańców.

Grzegorz Klamut

Port Lotniczy Lublin

Bardzo dobre szkolenie. Największą wartością była możliwość praktycznego przetestowania scenariuszy w realnych warunkach, co w codziennej pracy trudno osiągnąć. Dyskusja z innymi fachowcami pozwala z kolei wyciągnąć wiele merytorycznych wniosków.

Oskar Małecki

Dino Market

Powiem krotko: bardzo polecam takie szkolenia! Zobaczyć rozwiązania security w praktyce – bezcenne doświadczenie!

Piotr Kiliszek

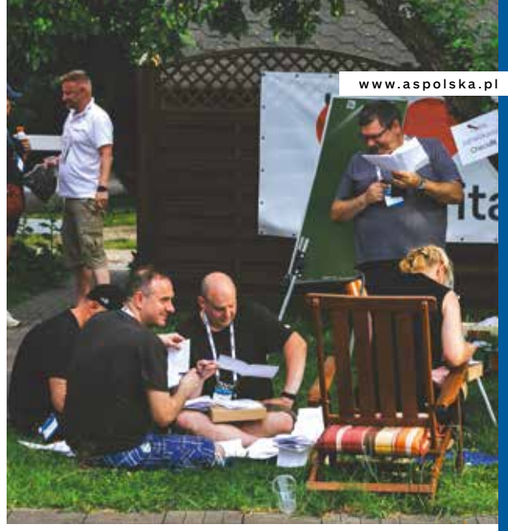
Polskie Porty Lotnicze

To kolejna szansa na spotkanie się w gronie specjalistów. Wymiana doświadczeń jest tak samo cenna, jak spojrzenie na nowe technologie w praktyce. Podzielenie się case study z innymi security menedżerami wzbogaca wiedzę i pomaga w codziennej pracy.

Mariusz Kucharski

a&s Polska

Konwencja takich spotkań spotkała się z bardzo dużym zainteresowaniem i już mamy kolejne zgłoszenia od następnych chętnych uczestników. W związku z tym zorganizujemy w tym roku drugą (jesienną) edycję Security Bootcamp.



www.aspolska.pl

Axis IP Piknik

Wśród natury, z dala od zatłoczonego stołecznego miasta, na początku czerwca br. Axis Communications zorganizował dla swoich partnerów biznesowych Piknik Techniczny, by zaprezentować nowości produktowe. Zespół porzucił koncepcję tradycyjnej formuły spotkań „przy PowerPoincie", umożliwiając przetestowanie wybranych rozwiązań w rzeczywistych scenariuszach na przygotowanych wcześniej stoiskach.

Zanim uczestnicy wydarzenia poddali urządzenia Axis serii prób i testów, otrzymali porządną dawkę wiedzy od Martina Jensena, Global Product Managera, który przedstawił plan wprowadzania produktów bazujących na najnowszym chipsecie ARTPEC-8 i spodziewanych rozwiązań technicznych. Poruszono również trudny w dzisiejszych czasach temat dostępności produktów, który podjęła Agata Majkucińska, Distribution Account Manager. Wskazała na ciągłą poprawę czasu dostawy oraz podkreśliła nieprzerwane prace Axis nad nowymi produktami.

Na stoiskach uczestnicy pikniku mogli sprawdzić:

- możliwości integracyjne różnych rozwiązań z zakresu systemów VSS, KD i audio za pomocą wspólnej platformy Axis Camera Station,
- najnowsze funkcje i usprawnienia interfejsu użytkownika wprowadzone ostatnio do Axis Camera Station,
- rozwiązania łączące kamerę PTZ i radar jako narzędzia dozoru dużych przestrzeni,
- Axis Speed Monitor jako integrację kamery, radaru i sygnalizatora optyczno-akustycznego,
- oprogramowanie Axis Object Analytics – bezpłatną zaawansowaną analizę obrazu opartą na algorytmach Machine i Deep Learning, dostępną w najnowszych kamerach Axis.

Tradycją spotkań z Partnerami są wyróżnienia przyznawane przez Axis Communications w kilku kategoriach. W tym roku polski zespół nagrodził firmy:

- mvb, squareTec, DG Elpro i Elstech za najwyższy poziom sprzedaży w 2021,
- Mikronika za najwyższy wzrost obrotów w 2021,
- Sprint za największy projekt 2021 Smart City,
- Alto Computers za największy projekt 2021 Transport,
- API Smart za największy projekt 2021 Infrastruktura Krytyczna,
- Elecom za najciekawszy projekt E2E w 2021,
- Securitas za najciekawszy projekt audio w 2021.

JTG

Jubileuszowy piknik CBC Poland

Z okazji 25-lecia działalności w Polsce firma CBC Poland zorganizowała dla klientów i partnerów jubileuszowy piknik. Impreza, która miała miejsce na początku czerwca br., była też okazją do zaprezentowania nowej siedziby firmy.

Gratulacje z okazji rocznicy składano na ręce Krzysztofa Skowrońskiego, dyrektora zarządzającego oddziału w Polsce.

– Od dwudziestu pięciu lat jesteśmy obecni na polskim rynku, oferując naszym klientom doskonałe rozwiązania, bezpośrednie wsparcie przed- i posprzedażowe oraz fachowe doradztwo techniczne. Nasz polski zespół stanowią doświadczeni profesjonaliści, a warszawski oddział firmy jest jednym z siedmiu europejskich oddziałów grupy CBC. Dzięki zaufaniu i zadowoleniu klientów jesteśmy liczącym się dostawcą rozwiązań CCTV na polskim rynku – powiedział Krzysztof Skowroński.

Przy wspaniałej pogodzie świętowano, delektując się piknikowym menu i podziwiając atrakcje przygotowane przez organizatora.

Ogólnopolskie warsztaty Reagowanie na Zamachy – Dobre Praktyki i Rekomendacje

24-25 maja odbyła się druga edycja ogólnopolskich warsztatów Reagowanie na Zamachy – Dobre Praktyki i Rekomendacje. To kolejna impreza organizowana przez Aritech i Safety Project. Współpraca między firmami ma na celu promocję świadomości o zagrożeniach oraz szerzenie wiedzy nt. metod prewencji i usuwania skutków zdarzeń o charakterze terrorystycznym czy skutków katastrof naturalnych.

Głównymi tematami warsztatów były zagadnienia przygotowania obiektów i organizacji do skutecznego reagowania na zdarzenia z szerokiego spektrum zagrożeń, np. komunikaty o zagrożeniu, masowym zabójcy czy materiałach wybuchowych. Testowano też pierwszą pomoc oraz omawiano wykorzystanie zabezpieczeń technicznych.

Dwa dni szkolenia, ćwiczeń praktycznych, dyskusji i wymiany doświadczeń pomiędzy uczestnikami i zaproszonymi ekspertami pozwoliły poczuć namiastkę realnych zdarzeń w trakcie przygotowanych symulacji i ćwiczeń.

Możliwość spotkania i wymiany doświadczeń praktyków odpowiedzialnych za przygotowanie obiektów z ratownikami i specjalistami weteranami służb antyterrorystycznych pozwoliła na nowe spojrzenie na tematykę warsztatów, bez konieczności zdobywania własnego doświadczenia w traumatycznych okolicznościach.

Już dzisiaj zapraszamy na kongres Safe Place, który odbędzie się 17-19 października 2022 r., oraz kolejne edycje warsztatów.

Więcej na stronie pl.firesecurityproducts.com

Katowice: Smart City

W czerwcu 2022 r. w Katowicach odbyła się konferencja „Smart City Katowice – Historia Sukcesu". Uczestnicy wydarzenia dowiedzieli się, jak działa modelowy system *smart city* w tym mieście oraz z jakimi problemami musieli zmierzyć się jego projektanci oraz Urząd Miasta jako właściciel i użytkownik rozwiązania. KISMIA (Katowicki Inteligentny System Monitoringu i Analiz) to „dziecko" stolicy Górnego Śląska i firmy Milestone Systems.

Konferencję otworzyli ambasador Królestwa Danii Ole Toft oraz I zastępca prezydenta Katowic Bogumił Sobula. Zgromadzeni w kinoteatrze Rialto dyskutowali o nowych wdrożeniach nowoczesnych rozwiązań, które przybliżają polskie miasta do bycia *smart*. Swoimi doświadczeniami podzielili się ojcowie systemu KISMIA: I zastępca prezydenta Katowic Bogumił Sobula, Maciej Stachura sekretarz miasta, Tomasz Kępa, zastępca naczelnika Wydziału Zarządzania Kryzysowego Katowic i Marcin Palka, inżynier wykonawczy systemu, Interiority. Jak działają systemy *smart city* na świecie i jakie dają korzyści – nie tylko związane z bezpieczeństwem, ale m.in. poprawiające komfort życia w mieście – mówił Bjorn Bergqvist, senior Vertical Marketing Manager Milestone Systems.

– W Katowicach radykalnie zmniejszyło się prawdopodobieństwo, by niechciane zdarzenie w obrębie systemu monitoringu zostało niezauważone. To przełożyło się na komfort życia w mieście. Ten system nie tylko wpływa na poziom bezpieczeństwa, obecnie jest rozbudowywany o inteligentny system zarządzania transportem miejskim czy monitorowaniem czystości powietrza – mówił w czasie swojego wystąpienia wiceprezydent Katowic.

– Dzielimy się naszymi doświadczeniami z uczestnikami. Jesteśmy dumni, że firma Milestone wybrała Katowice, które ma swoje doświadczenia i może się pochwalić innowacyjnym, sprawnie działającym systemem – powiedział Maciej Stachura, sekretarz miasta Katowice.

Katowice przeżywają renesans, jeśli chodzi o rozbudowę miasta i bezpieczeństwo mieszkańców. Katowicki Inteligentny System Monitoringu i Analiz to krok w stronę technologicznego rozwoju miasta, który widać w statystykach.

Nowy terminal dostępu

systemie RACS 5

Oferta terminali dostępu przeznaczonych do bezpiecznej identyfikacji użytkowników w systemie kontroli dostępu RACS 5 została poszerzona o czytnik MCT84M-BK-QB.

Nowy terminal umożliwia identyfikację użytkowników w systemie poprzez odczyt:.

- kodu QR
- identyfikatora mobilnego BLE/NFC
- karty zbliżeniowej MIFARE Ultralight®, MIFARE® Classic, MIFARE® DESFire®, MIFARE Plus®

Czytnik obsługuje kody QR szyfrowane zgodnie z standardem Roger lub kody nieszyfrowane. Szyfrowane kody QR są generowane z poziomu oprogramowania zarządzającego systemem kontroli dostępu. Mogą być udostępniane w formie wydrukowanego obrazu (etykieta) lub wyświetlane na ekranie telefonu.
W przypadku podłączenia do kontrolera MC16 czytnik MCT84M-BK-QB może funkcjonować jako terminal kontroli dostępu i/lub rejestracji czasu pracy, stanowiąc jednocześnie punkt sterowania automatyką budynkową w ramach funkcji dostępnych w systemie RACS 5. Opcjonalnie czytnik można skonfigurować do pracy z otwartym protokołem komunikacyjnym i wykorzystać poza systemem RACS 5 (np. w systemach automatyki czy aplikacjach do zarządzania biurem).
Obudowa czytnika ma neutralny wzorniczo wygląd, dzięki czemu dobrze wkomponowuje się we wnętrza zarówno tradycyjne, jak i nowoczesne. Terminal może być wykorzystywany z powodzeniem wszędzie tam, gdzie trzeba zapewnić bezpieczną – mobilną lub zbliżeniową – identyfikację użytkowników.
Znajduje zatem zastosowanie w biurowcach i różnych obiektach komercyjnych, placówkach sektora publicznego, fabrykach, obiektach przemysłowych i innych korzystających z systemów kontroli dostępu, rejestracji czasu pracy czy automatyki budynkowej.

Więcej na: www.roger.pl

Cloud Link Roadrunner

Firma Genetec wprowadziła na rynek rozwiązanie do zdalnego zarządzania dostępem do skrzynek rozdzielczych. Zarządzający ruchem drogowym i inżynierowie mogą teraz zdalnie zarządzać skrzynkami rozdzielczymi i innymi urządzeniami sterowania ruchem, a także monitorować je i zabezpieczać.

Cloud Link Roadrunner to pierwsze w branży, bezpieczne pod względem cybernetycznym i odporne mechanicznie urządzenie IoT, stanowiące część zunifikowanego systemu zarządzania ruchem firmy Genetec. Osoby zarządzające mogą bez obaw wdrażać w swoich skrzynkach rozdzielczych funkcje kontroli dostępu, które można rozbudowywać. W połączeniu z najnowszym oprogramowaniem do zarządzania dostępem, nowe urządzenie (zgodne z normą NEMA TS2 – *National Electrical Manufacturer Association)* zastępuje tradycyjne zamki mechaniczne i umożliwia klientom kontrolę nad tym kto, jak i kiedy ma dostęp do ich zdalnych obudów.

Dzięki połączeniu rozwiązań do zarządzania dostępem i monitoringu wizyjnego pracownicy odpowiedzialni za zarządzanie ruchem drogowym mogą natychmiast zweryfikować zdarzenie bez konieczności wysyłania ekip i w razie potrzeby szybko zareagować. Dostęp do skrzynek może być przyznawany zdalnie oraz dostosowany do charakteru wykonywanej pracy i roli wykonawcy lub pracownika.
– *Tradycyjnie obudowy skrzynek rozdzielczych z urządzeniami do zarządzania ruchem są chronione zamkami mechanicznymi, które można otworzyć zwykłymi kluczami. To sprawia, że są one podatne na ataki fizyczne* – wyjaśnia Jordan Burnsed, dyrektor działu wprowadzania nowych produktów w firmie Genetec Inc. – *Nasze nowe rozwiązanie jest bezpieczne i pomaga zarządzającym ruchem zmniejszyć koszty, poprawić wydajność i zwiększyć bezpieczeństwo.*
Oprócz kontroli dostępu użytkowników w czasie rzeczywistym i weryfikacji wizyjnej Cloud Link Roadrunner™ umożliwia kontrolę i rozliczanie wykonawców i pracowników. Użytkownicy mogą tworzyć niestandardowe pulpity i raporty, analizować dane i wzorce aktywności oraz śledzić prace kontraktowe w celu uzgodnienia rozliczeń z wykonawcami. Mogą też określać trendy, przeszukiwać dane i prowadzić dochodzenia w przypadku wymuszonych otwarć lub innych nieprawidłowości w użytkowaniu.

Więcej na:
https://www.genetec.com/a/enclosure-management

Poprzeczka w górę!

Hanwha Techwin wprowadza na rynek nową przeglądarkę obrazów typu Wisenet Viewer 1.0, która upraszcza zarządzanie wieloma strumieniami wizyjnymi za pomocą pojedynczego interfejsu. Aplikacja Wisenet Viewer 1.0 współpracuje ze wszystkimi rejestratorami Wisenet i eliminuje potrzebę posiadania osobnego serwera do zarządzania źródłami strumieni wizyjnych.

Przeglądanie wielu obrazów jednocześnie. Dzięki przeglądarce Wisenet Viewer 1.0 operatorzy systemów mogą uruchamiać wiele aplikacji jednocześnie (otwierać strony internetowe, obserwować bieżące obrazy z wybranych kamer czy wyszukiwać i odtwarzać fragmenty nagrań archiwalnych, definiować reguły obsługi zdarzeń wykrywanych przez aplikacje analizujące treść obrazów). Oprogramowanie jest zgodne z systemami operacyjnymi Windows iOS.

Łatwa adaptacja. Dzięki niestandardowym kompozycjom obrazów, które mogą zawierać wiele kart i okien, operatorzy mogą łatwo dostosować nową przeglądarkę do swoich potrzeb. Poszczególne obrazy można łatwo przekształcać, zmieniać ich rozmiar i położenie za pomocą kilku kliknięć. Można też nadawać i usuwać uprawnienia poszczególnym użytkownikom systemu.

Uri Guterman, dyrektor ds. produktów i marketingu w Hanwha Techwin Europe, powiedział: – *Naszym celem jest ciągłe podnoszenie poprzeczki w dziedzinie wizyjnych systemów dozorowych i wprowadzanie innowacyjnych rozwiązań wspierających działania naszych klientów. Aplikacja Wisenet Viewer 1.0 realizuje te cele, ułatwiając użytkownikom zarządzanie wieloma strumieniami wizyjnymi jednocześnie, reagowanie na zachodzące w terenie wydarzenia, które zostały wykryte przez inteligentne aplikacje do analizy treści obrazów.*
Aplikacja Wisenet Viewer 1.0 jest łatwa w konfiguracji, oszczędza czas i koszty utrzymania systemów wizyjnych. Jest bezpłatna dla nabywców rejestratorów Wisenet.

Więcej na:
https://bit.ly/3q9BTln

Nowe radary

do szlabanów firmy ZKTeco

VR10 Pro to druga generacja radarów firmy ZKTeco opracowanych do wykrywania i identyfikacji pojazdów (motocykli, samochodów, ciężarówek itp.) i pieszych przemieszczających się przez wjazd wyposażony w szlaban. Cechą szczególną radarów jest możliwość zdalnego ustawienia ich parametrów przez łącze Bluetooth.

Dzięki połączeniu z płytą główną sterownika szlabanu, VR10 Pro może zapobiec zderzeniu pojazdów z przeszkodami oraz uszkodzeniu obiektów i przechodniów, umożliwiając jednocześnie automatyczne opuszczenie wysięgnika szlabanu. W porównaniu do detektora w postaci pętli indukcyjnej oferuje on bardziej elastyczną i prostą instalację oraz niższe koszty pracy.

Ponadto użytkownik może ustawić parametry VR10 Pro za pomocą aplikacji mobilnej *(Radar Assistant)* po połączeniu jej z radarem przez Bluetooth.

Podstawowe zalety radaru:

- Szybkie wykrywanie pojazdów i pieszych;
- Komunikacja przez Bluetooth, umożliwiająca aktualizację i debugowanie za pomocą aplikacji mobilnej *(Radar Assistant);*
- Komunikacja przez interfejs RS-485, umożliwiająca aktualizację i debugowanie za pomocą komputera;
- Prosta i elastyczna instalacja;
- Normalne działanie w trudnych warunkach zewnętrznych (IP67);
- Regulowany zasięg wykrywania poruszających się obiektów od 1 do 6 m;
- Obsługa wysięgnika szlabanu.

Aplikacja *Radar Assistant* obsługuje systemy Android i iOS.

Zasięg komunikacji Bluetooth wynosi od 3 do 5 m. Połączenie z radarem następuje po kliknięciu na ikonkę w telefonie. Aplikacja umożliwia zdalne ustawienie zasięgu wykrywania urządzenia, nagrywanie w tle, pokazanie stanu radaru, ponowne jego uruchomienie oraz ustawianie innych parametrów. Za pomocą aplikacji można dokonać również aktualizacji oprogramowania sprzętowego.

Więcej na: www.zkteco.eu/

Honeywell

Inteligentna analityka IntrusionTrace ciągle na szczycie!

Analityka IntrusionTrace marki Honeywell jest kompatybilna z większością popularnych na rynku kamer (IP, termowizyjnych i analogowych). Oznacza to, że można ją zastosować zarówno w istniejących, jak i nowych systemach monitoringu wizyjnego. Detekcja intruza może być zainstalowana na inteligentnym rejestratorze (bramce wideo) z rodziny FastTrace marki ADPRO by Honeywell.

Analityka IntrusionTrace wykrywa obiekty, ich wielkość i prędkość poruszania się oraz przebyty dystans. Te cechy sprawiają, że nie jesteśmy uzależnieni od rozpoznania typu obiektu (człowiek czy pojazd), a jedynie od jego wielkości. Taka koncepcja wymaga mniejszej liczby pikseli na cel niż w przypadku konieczności rozpoznania/identyfikacji obiektu. Pozwala to na realne zwiększenie dystansu działania analityki przy identycznych warunkach środowiskowych w porównaniu do analityk opartych na klasyfikacji/identyfikacji np. wbudowanych w kamerach. W praktyce oznacza to, że potrzebujemy mniej kamer do zabezpieczenia danego obiektu, czyli generujemy oszczędności.

Ponadto analitykę IntrusionTrace można skonfigurować pod kątem danego obiektu i/lub zmieniające się warunki, co przekłada się na zwiększenie skuteczności działania i zminimalizowanie liczby fałszywych alarmów.

Analityka IntrusionTrace jest wykorzystywana do zdalnej wideoweryfikacji zdarzeń alarmowych w Centrach Monitoringu. W przypadku zidentyfikowania zagrożenia to operator może decydować o dalszych działaniach, podejmując ostateczną decyzję. To rozwiązanie sprawdza się w praktyce.

Więcej na: www.linc.pl

OMTECH

SMF

SYSTEM MONITOROWANIA FLOT

Szukamy nowych
Dystrybutorów w całej Polsce!
Zadzwoń, rozwijaj się i zarabiaj z nami!
+48 798 466 606

System Monitorowania Flot SMF:

- lokalizowanie położenia pojazdu w czasie rzeczywistym
- historia tras przejazdu i postojów
- wyznaczanie geostref pracy kierowcy
- analiza stylu jazdy kierowcy
- rozbudowany system raportowania
- kontrola gospodarki paliwowej
- powiadamianie o zaistniałych sytuacjach alarmowych
- zdalne pobieranie plików DDD z tachografów
- funkcja Eco-Driving - monitorowanie stylu jazdy kierowcy
- monitoring Sent Geo
- e-TOLL - obsługa systemu poboru opłat elektronicznych
- i wiele innych

SMF to kompleksowe narzędzie w postaci nowoczesnej aplikacji, służącej do monitorowania i zarządzania flotą pojazdów jak również pracownikami mobilnymi. Aplikacja umożliwia podgląd położenia naszych pojazdów w czasie rzeczywistym oraz uzyskanie wszystkich niezbędnych informacji dotyczących eksploatacji pojazdów i maszyn. Dodatkowo, aplikacja wyposażona jest w funkcje, dzięki którym mamy możliwość zredukowania wydatków na paliwo oraz szybką reakcję w przypadku kradzieży auta. Inżynierowie i programiści grupy OMTECH stworzyli przyjazny i łatwy w obsłudze interfejs, który dzięki swojej prostocie pozwala użytkownikowi już od pierwszej chwili po zalogowaniu rozpocząć skuteczne użytkowanie aplikacji, bez konieczności przeprowadzania czasochłonnych szkoleń.

POLSKI PRODUKT
OMTECH

www.omtech.pl
www.smfonline.pl