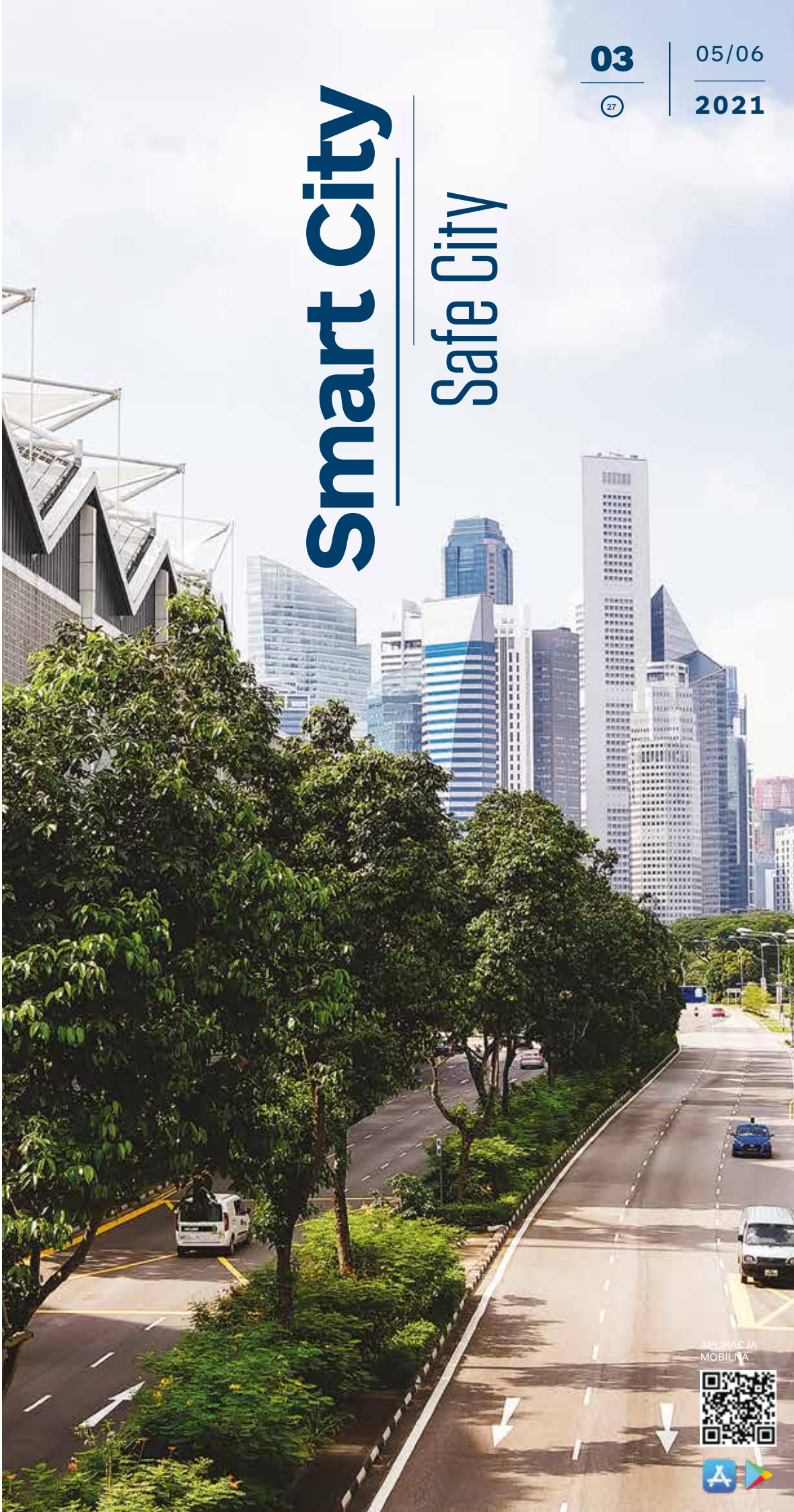
CZASOPISMO RYNKU SECURITY

a&s POLSKA

03 (27) 05/06 2021

Smart City

Safe City



SMART CITY

MIASTA PRZYSZŁOŚCI

Nowoczesna technologia zmienia oblicza miast. Jak będą funkcjonowały w przyszłości? Jedno jest pewne: już dziś trzeba stawiać na inteligentne rozwiązania. Cieszy fakt, że w światowych rankingach miast przyszłości w pierwszej dwudziestce znalazły się Wrocław i Warszawa.

SAFE CITY

ZABEZPIECZENIA W SMART CITY

Ludzie będą chcieli mieszkać w inteligentnych miastach pod warunkiem zapewnienia im bezpieczeństwa. Oferta branży security jest bardzo obszerna: od systemów monitoringu miejskiego po kompleksową ochronę obiektów biurowych.

BEZPIECZEŃSTWO BIZNESU

WYCIEK DANYCH

Publikowane w Internecie wykazy i listy osób mogą nieść duży ładunek ryzyka, co pokazały tegoroczne incydenty wycieku wrażliwych danych osobowych z serwera rządowego. Czy ma tego świadomość biznes, gdzie wykazy uczestników szkoleń i konferencji oraz zestawienia klientów są również zamieszczane online?

APLIKACJA MOBILNA

ISSN 2451-5175

9 772451 517703 05

15 zł (w tym 8% VAT)

www.aspolska.pl

EDYTORIAL

Drodzy Czytelnicy

Powoli wracamy do normalności. Będzie to nowa, bardziej technologiczna normalność. Zapewne każdy z nas zastanawiał się, jak może wyglądać miasto przyszłości. Niektórzy światowi wizjonerzy już zaczynają realizować swoje śmiałe pomysły (s. 14). Ale i polskie miasta nie pozostają w tyle, czego dowodem jest ich wysoka pozycja w globalnych rankingach najlepszych wdrożeń *smart city* (s. 16). Szczególne osiągnięcia w tym zakresie zanotował Wrocław (s. 20).

Czas pandemii przyspieszył wiele zjawisk w dziedzinie innowacyjności, przyczynił się do rozwoju rozwiązań także na styku technologii i bezpieczeństwa. Był to czas powszechnej edukacji publicznej dotyczącej korzystania z nowych usług cyfrowych w codziennym życiu (s. 28). Ujawnione potrzeby wymusiły rewolucję cyfrową, a ta – jak wiadomo – jest jednym z najważniejszych symptomów transformacji miasta w *smart city*. W jaki sposób światowe aglomeracje wykorzystały ten czas? Czy nie stosuje się technologii do zbytniej inwigilacji obywateli? W krajach UE trwa dyskusja nt. większej kontroli nad wdrażanymi technologiami, zwłaszcza sztucznej inteligencji i analityki obrazu, w celu ochrony danych osobowych. Nasza branża powinna wypracować rozwiązania dla własnej oferty mającej służyć bezpieczeństwu (s. 32).

Rozwój mikroelektroniki i technologii informatycznych umożliwił realizację koncepcji inteligentnych miast. Działaniom mającym na celu zapewnienie komfortu pracy i życia musi towarzyszyć gwarancja ochrony ogromnych zasobów informacji przetwarzanych w ramach inteligentnego miasta (s. 36). Tematykę wybranych zagadnień z zakresu cyberbezpieczeństwa danych poszerzamy w artykule na s. 76. Wiemy już, co kryje się pod pojęciem *hardening*, i dlaczego jest tak ważne, że powinno być ostatnim elementem wdrożenia (kamer, systemu VMS) i podlegać ocenie przy odbiorze.

Pandemia zaburzyła nieco przewidywania dotyczące migracji ludności ze wsi do miast. Wiele osób szuka teraz swojego miejsca niekoniecznie w zatłoczonych aglomeracjach, a właśnie w oddalonych od miejskiego zgiełku lokalizacjach wiejskich. Co zatem dla branży security może przynieść ta zmiana? O tych wyzwaniach i szansach piszemy na s. 42.

Prawidłowe funkcjonowanie miasta wymaga sprawnego transportu publicznego. Implementacja analizy zawartości obrazu w tym segmencie przebiegała nieco wolniej ze względu na specyficzne trudności z jej wdrożeniem. Poprosiliśmy ekspertów branżowych, by na podstawie własnych doświadczeń i zgodnie z dobrą praktyką podzielili się radami nt. wyboru odpowiednich rozwiązań (s. 60).

Odmrażamy nasze wydarzenia! Warsaw Security Summit 2021 odbędzie się 6 września. Jeśli pozwolą na to warunki epidemiczne, zorganizujemy konferencję w formie hybrydowej: online i stacjonarnej z zachowaniem wszelkich reżimów sanitarnych. Wydarzenie będzie także transmitowane online. Aby zapewnić uczestnikom bezpieczne warunki, wprowadzimy limit osób obecnych w sali konferencyjnej. Niebawem ogłosimy program konferencji i uruchomimy rejestrację dla uczestników – szczegóły na www.WarsawSecuritySummit.eu.

Marta Dynakowska
REDAKTOR NACZELNA

Jan T. Grusznic
Z-CA REDAKTORA NACZELNEGO

Mariusz Kucharski
PREZES ZARZĄDU

A&S POLSKA REDAKCJA

Wydawca
A&S Polska 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

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

Korekta
Jolanta Kucharska

Projekt graficzny i skład
Kalwala Studio

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

Prenumerata
www.aspolska.pl/prenumerata

a&S POLSKA

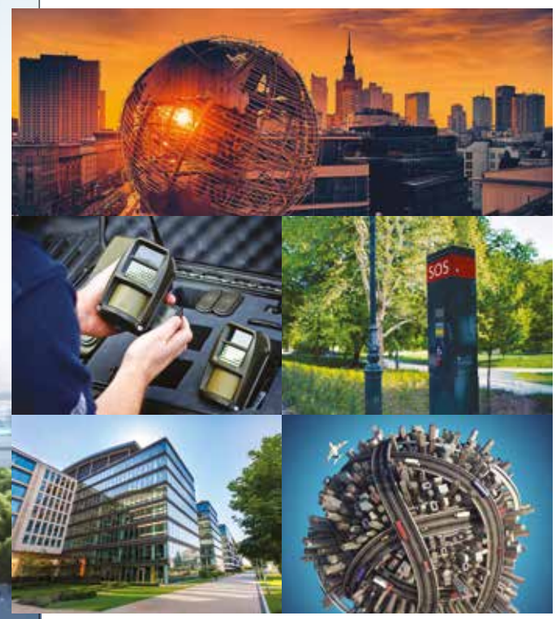
03

27

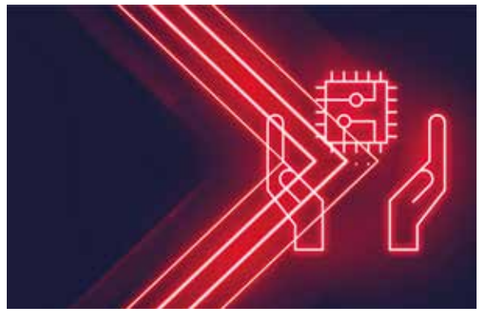
05/06

2021

SPIS TREŚCI



SPIS TREŚCI



AXIS COMMUNICATIONS

www.axis.com/pl

Nowa światłoczuła kamera PTZ firmy Axis

AXIS COMMUNICATIONS WPROWADZA NA RYNEK URZĄDZENIE AXIS Q6315-LE – SZYBKĄ KAMERĘ PTZ Z TRYBEM PODCZERWIENI DO DOZORU W CAŁKOWITEJ CIEMNOŚCI. PROCESOR NOWEJ GENERACJI ZAPEWNIA ULEPSZONĄ OBSŁUGĘ OBRAZU, ROZSZERZONE FUNKCJE ANALIZ I ZNACZNIE EFEKTYWNIEJSZĄ KOMPRESJĘ WIDEO.

Nowa zaawansowana kamera AXIS Q6315-LE udostępnia precyzyjne laserowe ustawianie ostrości (również w ciemności) oraz funkcję Speed Dry, która pozwala uzyskać wyraźny obraz również podczas opadów deszczu.
Ponadto posiada aplikację Autotracking 2 z funkcją „kliknij i śledź" oraz obsługą nakładek dynamicznych, dzięki czemu umożliwia aktywne śledzenie obiektów i szybką orientację. Moduł TPM *(Trusted Platform Module)* z certyfikatem FIPS 140-2 na poziomie 2. zapewnia bezpieczne przechowywanie wszystkich kluczy kryptograficznych i certyfikatów, dzięki czemu nawet w razie naruszenia zabezpieczeń nic im nie grozi.
Kamerę można zamontować na urządzeniu AXIS Q6100-E, zyskując 360-stopniowy obrót ciągły i pełen obraz sytuacji. Korzysta ona z tego samego uchwytu, zasilacza i kabla sieciowego, a to obniża koszty instalacji.

Najważniejsze cechy:

- Przetwornik obrazu 1/2 cala i 31-krotny zoom optyczny.
- Oświetlenie w podczerwieni, tryb pracy dzień/noc.
- Autotracking 2, pomoc w orientacji i AXIS Object Analytics.
- Precyzyjne ustawianie ostrości za pomocą wiązki laserowej i szybki zoom.
- Moduł TPM z certyfikatem FIPS 140-2 poziom 2.
- Efektywna kompresja obrazu.

BCS

www.bcscctv.pl

BCS Manager i kamery ANPR

BCS MANAGER TO AUTORSKA APLIKACJA DO OBSŁUGI WSZYSTKICH SERII PRODUKTÓW BCS. APLIKACJĘ MOŻNA ROZBUDOWAĆ O MODUŁ UMOŻLIWIAJĄCY OBSŁUGĘ KAMER PRZEZNACZONYCH DO ROZPOZNAWANIA NUMERÓW TABLIC REJESTRACYJNYCH. DZIĘKI TAKIEMU ROZWIĄZANIU DOSTĘP DO OBSŁUGI SYSTEMU JEST MOŻLIWY BEZPOŚREDNIO Z APLIKACJI. PO KONFIGURACJI I WSKAZANIU, KTÓRE KAMERY ZAJMUJĄ SIĘ ROZPOZNAWANIEM TABLIC REJESTRACYJNYCH, W APLIKACJI WYŚWIETLANE BĘDĄ INFORMACJE O ZDARZENIACH ORAZ DOSTĘPNE AKCJE.

Aplikacja pozwala na szybką obsługę wjazdu samochodów dzięki przyciskowi uruchamiającemu przekaźnik w kamerze umożliwiający otwarcie szlabanu. W przypadku pojazdu dodanego do białej listy jego przejazd jest zautomatyzowany. Edycja białej listy jest też dostępna bezpośrednio z poziomu BCS Managera, co zdecydowanie ułatwia pracę operatorowi systemu.
Do ustawień ogólnych kamery pracującej w trybie ścieżki lub skanowania można dodać funkcję zbierania metadanych o trzech podstawowych typach obiektów: człowiek, samochód, jednoślad.
Kamera wspiera też tzw. inteligentną detekcję ruchu, z klasyfikacją obiektu. Jakość obrazu zapewniają WDR 120 dB i elektroniczna stabilizacja obrazu.

COMMAX

www.commax.pl

Panele wideodomofonowe z czytnikiem RFID

OPRÓCZ SZEROKIEJ GAMY PANELI JEDNOABONENTOWYCH W OFERCIE FIRMY COMMAX DOSTĘPNE SĄ PANELE DO SYSTEMÓW WIELORODZINNYCH – ZARÓWNO ROZBUDOWANYCH OSIEDLI Z SETKAMI MIESZKAŃ, JAK I DOMÓW WIELORODZINNYCH, KAMIENIC, POJEDYNCZYCH BLOKÓW.

Do tych mniejszych instalacji są dedykowane panele z przyciskami bezpośredniego wyboru odbiorników. Występują one w wersji 2-, 4-, 6-, 8-, 10-przyciskowej, z możliwością rozbudowy o ekspander 24-przyciskowy. Dzięki różnorodności gamy odbiorników każdy z lokatorów może wybrać monitor dostosowany do własnych preferencji – zarówno słuchawkowy, jak i głośnomówiący o przekątnej ekrany od 4,3" do 10,2" lub też prosty unifon.
Każdy z paneli jest dostępny w wersji ze standardową kamerą PAL oraz z kamerą o dużej rozdzielczości HD. Standardowym wyposażeniem jest także czytnik kart/breloków standardu Mifare, umożliwiający lokatorom wejście na posesję bez użycia klucza.
Panele są również wyposażone w dwa wyjścia sterujące, pozwalające na wysterowanie np. furtki i bramy (przy zastosowaniu dedykowanych monitorów). Opisowe tabliczki imienne, a także przyciski wywołania są podświetlane, uławiając odwiedzającym kontakt z lokatorem także w nocy.
Panele wejściowe mogą być instalowane w sposób podtynkowy (dostępne są również dodatkowe daszki) lub natynkowo (w obudowie OS-6/7NB).

PRODUKT NUMERU

GDE

www.gde.pl

IWH-41UIW – kamera MAZi+ z technologią Colour in the Dark

TECHNOLOGIA COLOUR IN THE DARK W KAMERZE IWH-41UIW ZAPEWNIA UZYSKANIE DOBREJ JAKOŚCI KOLOROWEGO OBRAZU NAWET W NOCY. JEST TO MOŻLIWE DZIĘKI ZASTOSOWANIU WYSOKIEJ JAKOŚCI CZUŁEGO PRZETWORNIKA O DUŻEJ PRZEKĄTNEJ 1/1,8", JASNEGO OBIEKTYWU F1,0 ZE SPECJALNĄ POWŁOKĄ ANTYREFLEKSYJNĄ ORAZ OPCJONALNEGO PODŚWIETLENIA ŚWIATŁEM CIEPŁYM BIAŁYM O ZASIĘGU DO 30 M.

Wbudowane oświetlacze o temperaturze barwowej 3000K (barwa ciepła) mogą włączać się w nocy automatycznie lub zostać na stałe wyłączone. Zaletą jest również obsługa przez najnowsze przeglądarki (Edge, Firefox), a także przez Internet Explorer.

To nie koniec możliwości kamery. Oprócz detekcji ruchu dostępne są funkcje VCA (czyli analizy zawartości obrazu): wykrywanie twarzy, wykrywanie zmiany sceny, wtargnięcie w obszar, przekroczenie linii, pozostawienie obiektu i jego zabranie.

Kamera ma rozdzielczość 4 Mpix, obiektyw 2,8 mm (szerokość pola widzenia ok. 109°), dodatkowy trzeci strumień o maks. rozdzielczości 1280 x 720P, WDR o dynamice aż 120 dB, obsługuje kodeki H.264/H.264+/H.265/H.265+.
Dzięki złączu kart mikro SD możliwa jest praca samodzielna bez rejestratora albo z rejestratorem i wykorzystaniem funkcji ANR *(Automatic Network Replenishment)* – w razie przerwy w połączeniu z rejestratorem zapis jest kontynuowany na karcie SD, a po przywróceniu połączenia następuje synchronizacja danych z rejestratorem.
Wyłącznym partnerem MAZi Security Systems jest GDE Polska.

HIKVISION

www.hikvision.com/pl

Stacje bramowe Villa 2. generacji

SYSTEMY WIDEODOMOFONOWE SĄ STOSOWANE W CORAZ WIĘKSZEJ LICZBIE OBIEKTÓW, CO GENERUJE ZAPOTRZEBOWANIE NA RÓŻNORODNE MODELE URZĄDZEŃ. STACJE BRAMOWE TYPU VILLA TO KONSTRUKCJE MAJĄCE WBUDOWANE OD 1 DO 4 PRZYCISKÓW I SĄ DEDYKOWANE DO ZASTOSOWANIA W BUDOWNICTWIE JEDNORODZINNYM.

Stacja bramowa DS-KV-6113-WPE1 to najmniejszy model w ofercie Hikvision. Szerokość 65 mm pozwala na montaż urządzenia na bardzo wąskich słupkach. Duży, efektownie podświetlany przycisk umieszczony w obudowie z tworzywa nie pozostawia wątpliwości, w jaki sposób skorzystać z urządzenia.
Szerokokątna kamera 2 Mpix z doświetleniem IR zapewnia dobrą widoczność i jakość obrazu, a wbudowany czytnik Mifare pozwala mieszkańcom na wejście bez użycia kluczy.
Przy tak dużej funkcjonalności można łatwo zapomnieć, że KV6113 ma tylko jeden przekaźnik. Jeśli konieczne jest sterowanie zarówno furtką, jak i bramą, powinniśmy zastosować wyższy model stacji bramowej wyposażony w dwa przekaźniki: DS-KV8113-WME1. To urządzenie ma wszystkie funkcjonalności niższego modelu, ale jest zamknięte w metalowej obudowie i występuje w wersjach z dwoma i czterema przyciskami wywołania.
W najnowszych wersjach firmware 1-przyciskowe stacje Villa uzyskały możliwość bezpośredniego, bez użycia monitora w lokalu, wdzwaniania się na aplikację Hik-Connect, co pozwala na realizację uproszczonych systemów.
Dalsze szczegóły techniczne i konfiguracyjne można znaleźć na portalu DPP Hikvision, gdzie można obejrzeć nagrania webinarów.

NEDAP SECURITY MANAGEMENT

www.nedapsecurity.com/pl/

Integracja Nedap AEOS z przenośnymi czytnikami kart

INTEGRACJA XPRESSENTRY Z AEOS POZWALA NA WYGODNE WYKORZYSTANIE MOŻLIWOŚCI SYSTEMU KONTROLI DOSTĘPU AEOS W CZYTNIKACH MOBILNYCH, ZAPEWNIAJĄC OGROMNĄ ELASTYCZNOŚĆ I NOWE FUNKCJE W ZAKRESIE BEZPIECZEŃSTWA FIZYCZNEGO.

XPressEntry umożliwia weryfikację tożsamości za pomocą identyfikatorów lub danych biometrycznych, rejestrowanie wejść i wyjść w miejscach, gdzie standardowe czytniki są niepraktyczne, szybkie sprawdzanie pracowników podczas ewakuacji, badania lekarskie w punktach wejściowych i wiele innych.

Czytniki przenośne przechowują wszystkie dane z identyfikatorów oraz informacje o zajętości obiektu i uprawnieniach, by szybko weryfikować informacje z dowolnego miejsca w scenariuszach online lub offline.

Kluczowe cechy:
Weryfikacja identyfikatorów: rejestracja i wyświetlanie w czasie rzeczywistym wejść i wyjść, zapis nowych użytkowników i gości w dowolnym czasie i miejscu;
Ewakuacja w nagłych wypadkach: ciągłe śledzenie zajętości obiektu poprzez monitorowanie bazy danych AEOS. W przypadku ewakuacji uzyskanie raportu ze zdalnych lokalizacji, z weryfikacją czy personel i goście zostali bezpiecznie ewakuowani, a co najważniejsze, identyfikacja zaginionych osób i ich ostatniej zarejestrowanej lokalizacji;
COVID-19 Screening: łatwe sprawdzanie i bezpieczne przechowywanie informacji o aktualnym stanie zdrowia personelu i gości;
Zarządzanie zdarzeniami: dostarczanie biletów wstępu na wydarzenia przy użyciu istniejących identyfikatorów pracowników.

SCHRACK SECONET

www.schrack-seconet.pl

Uniwersalna centrala sygnalizacji pożarowej i sterowania urządzeniami przeciwpożarowymi Integral EvoxX M

INTEGRAL EVOXX M TO FLAGOWY PRODUKT SYSTEMU INTEGRAL EVOXX. CHARAKTERYZUJE SIĘ MODUŁOWĄ BUDOWĄ I MAKS. POZIOMEM BEZPIECZEŃSTWA DZIĘKI ZASTOSOWANIU 100% REDUNDANCJI SPRZĘTOWEJ ORAZ PROGRAMOWEJ.

Nowa platforma sprzętowa centrali (B8) oparta na redundantnych procesorach dwurdzeniowych 5-krotnie zwiększyła wydajność systemu i zoptymalizowała zarządzanie zasobami systemowymi. Dla zapewnienia niezawodności działania systemu funkcje bezpieczeństwa i komfortu są zarządzane przez osobne rdzenie procesora.

Centrala ma certyfikaty i świadectwa dopuszczenia CNBOP-PIB do realizacji następujących funkcji:

- centrala sygnalizacji pożarowej zgodnie z PN-EN54-2,
- zasilacz urządzeń przeciwpożarowych zgodnie EN 54-3,
- centrala sterująca urządzeniami przeciwpożarowymi w systemach kontroli rozprzestrzeniania dymu i ciepła (zgodnie z prEN12101-9) oraz sterowania i nadzorowania w ramach instalacji wodociągowych przeciwpożarowych zgodnie z Krajową Oceną Techniczną (KOT),
- zasilacz urządzeń przeciwpożarowych w systemach kontroli rozprzestrzeniania dymu i ciepła zgodnie z EN 12101-10,
- centrala sterująca stałymi urządzeniami gaśniczymi gazowymi zgodnie z PN-EN12094-1,
- centrala sterująca stałymi urządzeniami gaśniczymi wodnymi, pianowymi i aerozolowymi zgodnie z Krajową Oceną Techniczną (KOT).

Sterowanie bezpośrednie urządzeń przeciwpożarowych odbywa się za pomocą wejść/wyjść centrali oraz modułów wejścia/wyjścia w ramach techniki pętlowej X-LINE. Centrala Integral EvoxX M, realizując jednocześnie wszystkie powyższe funkcje, jest najbardziej uniwersalną centralą na rynku polskim.

TP-LINK

www.tp-link.com.pl

TP-Link VIGI C400P – kopułkowa kamera CCTV typu turret

VIGI C400P TO KAMERA SIECIOWA TYPU TURRET, KTÓRA GENERUJE OBRAZY W ROZDZIELCZOŚCI 3 MPIX. URZĄDZENIE JEST DOSTĘPNE W DWÓCH WERSJACH – Z OBIEKTYWEM O OGNISKOWEJ 2,8 LUB 4 MM. DZIĘKI TEMU ODZNACZA SIĘ UNIWERSALNOŚCIĄ DZIAŁANIA. SPRAWDZI SIĘ ZARÓWNO W DOZORZE WĄSKICH KORYTARZY, JAK I W OTWARTYCH PRZESTRZENIACH.

Zgodność ze standardem 802.3af/at PoE ułatwia instalację i obniża jej koszty. Użytkownik może też skorzystać z opcji zasilania 12 V DC.
Dzięki aplikacji VIGI na urządzenia przenośne z systemem iOS lub Android kamerami można w prosty i kompleksowy sposób zarządzać z poziomu smartfona. Kamera wyśle powiadomienie push za każdym razem, gdy wykryje niepożądany ruch, zaobserwuje przekroczenie wyznaczonej granicy lub gdy ktoś zasłoni jej obiektyw.

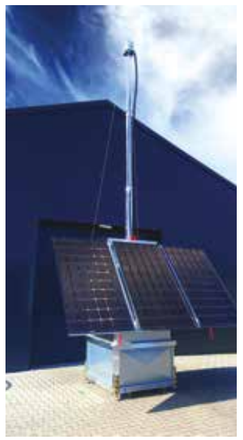
Systemem monitoringu wizyjnego VIGI można też zarządzać z poziomu dedykowanego oprogramowania przeznaczonego dla komputerów lub za pomocą rejestratora VIGI NVR. Ostatnie rozwiązanie pozwala na dostęp do systemu CCTV/VSS bez użycia dodatkowych urządzeń.
Kamera wykorzystuje kompresję obrazu H.264+, co w połączeniu z rejestratorem VIGI NVR1008 umożliwia zarejestrowanie i przechowywanie do 720 dni materiału wizyjnego w wysokiej rozdzielczości na dysku o pojemności 10 TB.

Produkt został objęty 3-letnią gwarancją producenta.

VCS

www.vcs.pl

iTower Tripel Solar – jestem ECO



ZAINTERESOWANIE INSTALACJĄ FOTOWOLTAICZNĄ Z ROKU NA ROK WZRASTA. PROGNOZY POKAZUJĄ, ŻE KONSUMENCI CORAZ CHĘTNIEJ INWESTUJĄ W ODNAWIALNE ŹRÓDŁA ENERGII. DLATEGO NAJNOWSZA GENERACJA WIEŻ ITOWER ZOSTAŁA WYPOSAŻONA W TRZY ZINTEGROWANE PANELE FOTOWOLTAICZNE.

Pomysłowy system składania gwarantuje optymalne pochłanianie energii słonecznej. W połączeniu z systemem akumulatorów zapewnia efektywną autonomię wykorzystania wieży do monitoringu.

Brak infrastruktury, trudno dostępne obszary i częste zmiany lokalizacji dozoru nie stanowią żadnego problemu. Zastosowanie tego rozwiązania przyczyni się do zmniejszenia kosztów zużycia energii, pozytywnie wpłynie na środowisko naturalne, wydłuży bezobsługową pracę systemu.
Wieża iTower Tripel Solar pełni też funkcję mobilnego systemu monitoringu. To połączenie stabilnej konstrukcji, odnawialnego źródła zasilania, transmisji i oświetlenia ze skutecznym systemem zabezpieczeń. Inteligentne oprogramowanie ostrzega o wtargnięciu obiektów na chroniony teren i powiadamia o zagrożeniu Centrum Monitoringu. Wideoweryfikacja ułatwia szybką ocenę sytuacji i podjęcie stosownej decyzji.
Wieża wyposażona w głośnik pozwala natychmiast nadać spersonalizowany komunikat do intruza.

Użyta technologia pozwala na dozór dużych obszarów, takich jak place budowy, farmy fotowoltaiczne, tereny przemysłowe czy miejsca organizacji imprez masowych. To jedno z najbardziej przyjaznych klimatowi rozwiązań do mobilnego monitoringu.

Smart City przyszłości

Prawdziwą rewolucję w życiu miejskim wprowadza Arabia Saudyjska. W mieście NEOM nie będzie samochodów i ulic. Mieszkańcy będą żyli w zgodzie z naturą, a wszystko będzie zasilane zieloną energią.

NEOM to nowa wizja przyszłości. To próba zrobienia czegoś, co nigdy dotąd nie powstało, a nadchodzi w czasie, gdy świat potrzebuje świeżych pomysłów i nowych rozwiązań. Mówiąc prościej, NEOM będzie domem dla ludzi, którzy chcą uczestniczyć w budowaniu nowego modelu zrównoważonego życia.

Zlokalizowany w północno-zachodniej Arabii Saudyjskiej nad Morzem Czerwonym, NEOM będzie domem i miejscem pracy dla ponad miliona mieszkańców z całego świata. Znajdą się w nim osiedla, porty i strefy przedsiębiorczości, ośrodki badawcze, obiekty sportowe i rozrywkowe oraz ośrodki turystyczne. Będzie to centrum innowacji przyciągające przedsiębiorców, liderów biznesu i firmy, którym zależy na tworzeniu przełomowych rozwiązań opartych na nowych technologiach. Mieszkańcy NEOM będą wcielać w życie kulturę poszanowania różnic i otwartość na różnorodność. A wszystko to w sprzyjającym i postępowym otoczeniu, w zgodzie z międzynarodowymi normami, z korzyścią dla wzrostu gospodarczego.

Plany dotyczące NEOM są szeroko zakrojone. Najnowsza wizja skupia się wokół 170-kilometrowego projektu The Line, liniowego miasta połączonego szybkim pociągiem, bez samochodów, którego powstanie zapowiedział w styczniu br. Mohammed ibn Salman, następca tronu Arabii Saudyjskiej i prezes zarządu NEOM. Obszar otaczać mają cztery inne inwestycje – zwane Neom Bay, Aqaba Region, Neom Mountain i Neom Industrial City. Przewiduje się, że NEOM będzie miał 14 sektorów przemysłowych, w tym m.in. energetykę, produkcję żywności i media.

Do 2050 r. czas dojazdów do pracy zwiększy się dwukrotnie. Ponad miliard ludzi będzie musiał przesiedlić się ze względu na rosnącą emisję CO_2 i podnoszący się poziom mórz. Niemal 90% ludności wdycha zanieczyszczone powietrze. Dlaczego mielibyśmy poświęcić przyrodę dla rozwoju? Dlaczego siedem milionów ludzi miałoby umierać co roku z powodu zanieczyszczenia? Czemu mielibyśmy tracić milion osób rocznie z powodu wypadków drogowych? I wreszcie, dlaczego mamy się pogodzić z marnowaniem wielu lat naszego życia na dojazdy do pracy? Z tych powodów konieczne jest przekształcenie koncepcji miasta konwencjonalnego w futurystyczne – powiedział książę Mohammed ibn Salman.

The Line to 170-kilometrowy pas miejski połączony szybkim pociągiem

Fot. NEOM

Projekt zakłada zastosowanie najnowocześniejszych rozwiązań. W tym m.in. latające taksówki, które zagwarantują, że podróżowanie pojazdami nie będzie miało jedynie wymiaru transportowego, ale będzie rozrywką. Nowoczesny system bezpieczeństwa, z dronami i kamerami wyposażonymi w technologię do rozpoznawania twarzy będzie gwarantował bezpieczeństwo obywateli. Przewiduje się również wykorzystanie technologii do tworzenia sztucznych chmur i dzięki temu zwiększenie opadów deszczu, niewystarczających dziś w tych rejonach świata. Po mieście będą poruszać się roboty do różnych zastosowań: informacyjnych, sprzątających czy – jako dinozaury – służących dzieciom do zabawy.

Przestrzeń w The Line będzie zdefiniowana do poruszania się pieszo. Wszystkie niezbędne codzienne usługi: szkoły, ośrodki zdrowia, obiekty rekreacyjne, a także tereny zielone będą znajdować się w zasięgu 5-minutowego spaceru. Osiedla będą bazowały na rozwiązaniach sztucznej inteligencji, które zwiększą poczucie bezpieczeństwa i komfort życia mieszkańców.

Twórcy projektu stawiają na zrównoważony rozwój. Tworzone będą inwestycje miejskie ograniczające emisję dwutlenku węgla, zasilane w 100% czystą energią, zapewniające mieszkańcom wolne od zanieczyszczeń, zdrowsze i bardziej zrównoważone środowisko. To jeden z najbardziej złożonych i wymagających projektów infrastrukturalnych na świecie – stanowi część szeroko zakrojonych prac inwestycyjnych już realizowanych w ramach miasta NEOM. Inwestycja jest częścią portfela Funduszu Inwestycji Publicznych Arabii Saudyjskiej, jednego z największych państwowych funduszy majątkowych na świecie. Przy jej tworzeniu ma powstać bisko 380 tys. miejsc pracy, a do 2030 r. ma zasilić PKB o 48 mld USD.

Polskie miasta w czołówce światowego rankingu Miast Przyszłości

W tegorocznym rankingu Global Cities of the Future 2021/22 na wysokich miejscach znalazły się dwa polskie miasta: Wrocław i Warszawa. Prestiżową listę publikuje co dwa lata należący do grupy „Financial Times" międzynarodowy ośrodek badawczy fDi.

a&s Polska

Liderem najnowszego rankingu Miasta Przyszłości po raz czwarty z rzędu został Singapur, wyprzedzając Londyn i Dubaj. Wśród pierwszych dwudziestu pięciu miast Polska, jako jedyny kraj europejski, ma dwóch reprezentantów. Wrocław, któremu udało się wyprzedzić stolicę, uplasował się na 15. miejscu zestawienia, Warszawa znalazła się na 20.

W tegorocznym rankingu Wrocław zajął pierwsze miejsce w kategorii miast średnich i małych przed Zurychem i Wilnem. Stolica Dolnego Śląska zdecydowanie zwyciężyła w podkategorii „miasto przyjazne dla biznesu", a w podkategorii „efektywność kosztowa" zajęła drugie miejsce. Z kolei Warszawa zajęła 5. miejsce w kategorii dużych miast, ustępując Amsterdamowi, Dublinowi, Abu Zabi i Monachium. Stolica Polski nie zwyciężyła w żadnej podkategorii, a najwyższe 3. miejsce zajęła w podkategorii „efektywność kosztowa".

Autorzy rankingu zauważyli obecność polskich miast, pisząc: „Polska utrzymuje swoją reputację kraju posiadającego dobrze wykształconą siłę roboczą połączoną z zachęcającą opłacalnością biznesową. W kraju działa 14 specjalnych stref ekonomicznych, które umożliwiają inwestorom korzystanie z niższych podatków i innej pomocy publicznej".

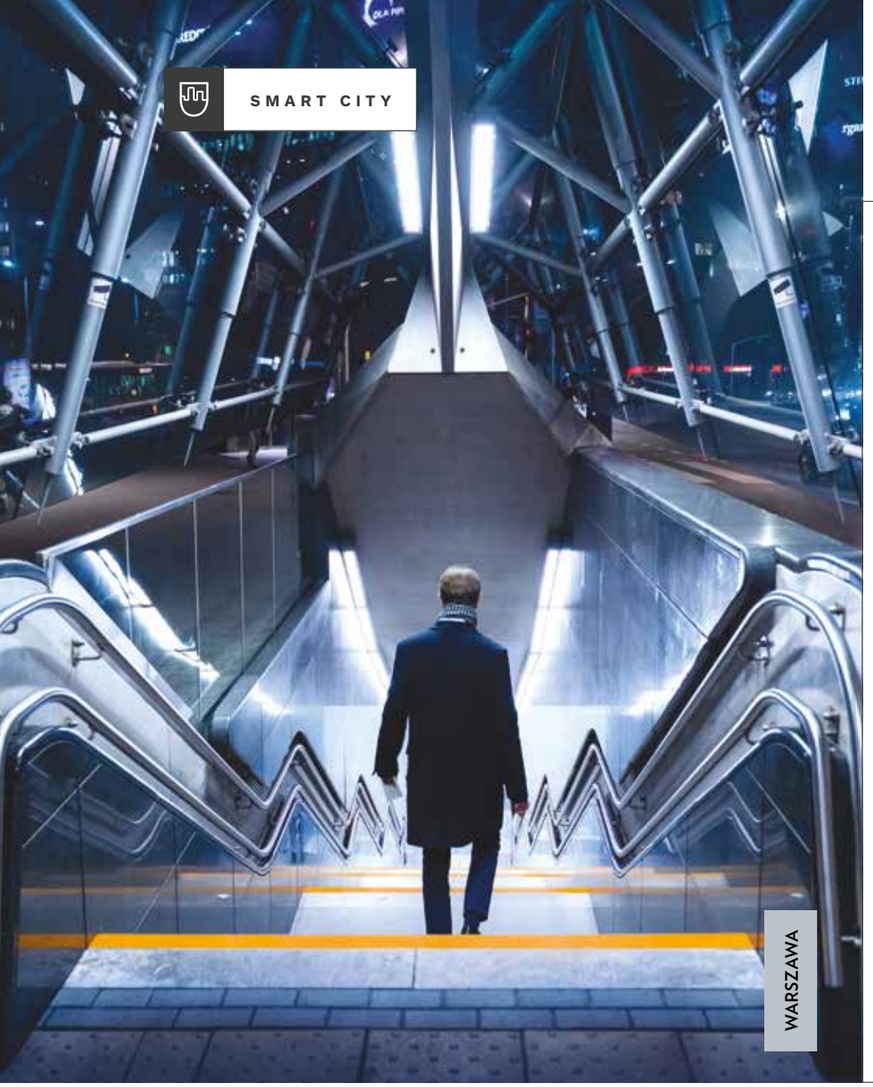
Zwycięzca tegorocznego rankingu – Singapur – triumfował w kategoriach „miasto przyjazne dla biznesu" i „potencjał gospodarczy". Jurorzy docenili niskie stawki podatkowe oraz hojne granty oferowane na cele badawcze. Singapur odnotował najwyższy napływ inwestycji skierowanych na badania i rozwój – w latach 2015–2020 (ocenianych w trzech poprzednich raportach) osiągnęły one 210 mln dolarów. W efekcie to miasto-państwo może się pochwalić kwitnącym ekosystemem badawczo-rozwojowym, obejmującym ponad 150 funduszy VC *(venture capital)*, inkubatory i akceleratory biznesu oraz tysiące start-upów.

Zajmujący drugą pozycję w rankingu Londyn zdeklasował rywali, zwyciężając w czterech spośród pięciu podkategorii. Stolica Wielkiej Brytanii swoją wysoką pozycję zawdzięcza obecności wielu światowej klasy uniwersytetów, tworząc przy tym wraz z Cambridge i Oksfordem tzw. Złoty Trójkąt. W latach 2015–2020 Londyn przyciągnął najwięcej bezpośrednich inwestycji zagranicznych, wyprzedzając nawet Singapur, który w poprzednim rankingu zajął pierwsze miejsce pod tym względem.

Londyn opublikował niedawno swój pięcioletni plan wyjścia z kryzysu po pandemii COVID-19. Władze miasta stawiają na „zielone" ożywienie, szczególnie dzięki nakładom wspomagającym inwestycje ekologiczne i firmy technologiczne *(fintech)*. Obawy budzi jednak niedawny brexit, który stawia sektor finansowy w niepewności. Trudno przewidzieć, czy Londyn zdoła zachować pozycję jednego z czołowych centrów usług finansowych na świecie.

Dubaj zdobył najniższe miejsce na podium, ale wspiął się o trzy pozycje w porównaniu z poprzednim rankingiem. To efekt uruchomionego w 2014 r. planu, którego celem

Miejsce w rankingu	MIASTO	KRAJ
1.	**Singapur**	Singapur
2.	**Londyn**	Wielka Brytania
3.	**Dubaj**	Zjednoczone Emiraty Arabskie
4.	**Amsterdam**	Holandia
5.	**Dublin**	Irlandia
6.	**Hongkong**	Hongkong
7.	**Nowy Jork**	USA
8.	**Szanghaj**	Chiny
9.	**Paryż**	Francja
10.	**Tokio**	Japonia
11.	**Pekin**	Chiny
12.	**Abu Zabi**	Zjednoczone Emiraty Arabskie
13.	**Bangalur**	Indie
14.	**Monachium**	Niemcy
15.	**Wrocław**	Polska
16.	**Zurych**	Szwajcaria
17.	**Toronto**	Kanada
18.	**Seul**	Korea Południowa
19.	**Houston**	USA
20.	**Warszawa**	Polska
21.	**Chicago**	USA
22.	**Moskwa**	Rosja
23.	**San Francisco**	USA
24.	**Wilno**	Litwa
25.	**Montreal**	Kanada



WARSZAWA

Patrząc w przyszłość, pojawienie się i wprowadzenie na masową skalę szczepionek na wirusa SARS-CoV-2 z pewnością jest powodem do optymizmu. Niestety wg Światowej Organizacji Turystyki ONZ miasta utrzymujące się z turystyki na poziom gości porównywalny z wielkością przed pandemią będą musiały poczekać co najmniej do 2023 r.

Ranking Miasta Przyszłości powstaje co dwa lata – ocenie poddawane są ośrodki pod względem ich atrakcyjności dla bezpośrednich inwestycji zagranicznych. Wyjściowa lista rankingowa objęła 129 miast z całego świata. Oceniano potencjał gospodarczy, zasoby siły roboczej i poziom życia, efektywność kosztową, otwartość i zachęty dla biznesu oraz przyjazną komunikację publiczną.
W rankingu głównym zostały podzielone na podkategorie wg wielkości: wielkie miasta (powyżej 10 mln ludności), miasta główne, duże miasta oraz miasta małe i średnie (poniżej 2 mln ludności). Dodatkowa szósta podkategoria dotyczyła strategii miasta mającej na celu pozyskiwanie bezpośrednich inwestycji zagranicznych. Jest to kategoria wyłącznie jakościowa, w której oceny dokonuje zespół siedmiu ekspertów. Warto zauważyć, że w tej kategorii w dwóch podkategoriach pojawiają się inne polskie aglomeracje – Trójmiasto (miasta średnie i małe) oraz miasto Gdynia (miasta rosnące).

było uczynienie miasta kluczowym ośrodkiem gospodarki globalnej. Dubaj zachęca inwestorów korzystnymi stawkami podatkowymi, wolnymi strefami ekonomicznymi i dobrze wykształconą siłą roboczą. Wzorem Singapuru i Londynu władze miasta zadeklarowały transformację gospodarki na model dbający o równowagę środowiska. Jeśli chodzi o inwestycje ekologiczne, strategia czystej energii w Dubaju zakłada, że do 2050 r. 75% energii będzie wytwarzane z czystych źródeł.
W kategorii dużych miast zwyciężył w tym roku Amsterdam, wyprzedzając Dublin. Holenderskie miasto, posiadając jeden z najbardziej ruchliwych portów morskich i port lotniczy – najważniejsze węzły tranzytowe w Europie – konsekwentnie plasuje się w czołówce pod względem połączeń komunikacyjnych. Oba miasta: Amsterdam i Dublin są gotowe, by skorzystać z ewentualnego, związanego z brexitem wyjścia firm z Londynu, ponieważ mają dobrze ugruntowane sektory finansowe. Londyńska Giełda Papierów Wartościowych już pod koniec 2020 r. uruchomiła nowe centrum handlowe w Amsterdamie, aby swoich europejskich klientów ustrzec przed możliwymi zakłóceniami. Według *think tank* New Financial największym beneficjentem relokacji brexitu będzie Dublin.
Wydaje się, że miasta na całym świecie swoje wysiłki koncentrują na naprawie gospodarki po pandemii. Stawiają na rozwój cyfrowy i technologiczny ze szczególnym uwzględnieniem równowagi środowiskowej.

WROCŁAW

Źródło
https://www.fdiintelligence.com/article/79334

Smart Wrocław

Lepszy od Zurychu

O KONCEPCJI SMART CITY ROZMAWIAMY Z **ROBERTEM BEDNARSKIM**, Z-CĄ DYREKTORA DS. SMART CITY W WYDZIALE PROMOCJI MIASTA I TURYSTYKI URZĘDU MIASTA WROCŁAWIA

Gratulujemy zajęcia 15. miejsca w światowym rankingu Global Cities of the Future 2021/22. W kategorii otwartości miast na biznes Wrocław wyprzedził nie tylko Warszawę, ale także Zurych, Seul czy Chicago. Jak dochodzi się do takich wyników?

Bardzo dziękujemy. To ranking bardzo ważny, przygotowany przez grupę należącą do „Financial Times", która cieszy się na świecie dużą renomą. Jest to też ranking ceniony wśród inwestorów, którzy chcą ulokować swoje firmy we Wrocławiu i rzeczywiście korzystać z tego, co oferuje im nasze miasto. Miejsce to traktujemy trochę wtórnie, natomiast bardzo nas cieszy fakt, że zostaliśmy jako miasto dostrzeżeni. To pokazuje potencjał Wrocławia, tego, co zostało tu zbudowane.

Takiego potencjału gospodarczego, takiej tkanki stanowiącej podstawę rozwoju nie buduje się w jeden dzień. To długoterminowa i długofalowa praca wielu instytucji Wrocławia ukierunkowana na przyciąganie biznesu. Wspomnę choćby o ARAW-ie* – spółce, która zajmuje się pozyskiwaniem i obsługą inwestorów. To także działania towarzyszące, które organizuje się wokół biznesu, a więc również promocja miasta jako miejsca przyjaznego do życia i prowadzenia biznesu. Nie możemy też zapominać o tych elementach, które budują tkankę społeczną, dobry klimat, kapitał społeczny. To wszystko co jest związane z kulturą, z bogatą ofertą wydarzeń kulturalnych, jakie proponujemy mieszkańcom. Szczególnie cieszy nas to, że w rankingu zajęliśmy bardzo dobrą 9. pozycję w podkategorii kapitału ludzkiego i 6. miejsce pod względem potencjału gospodarczego. Co jest niezwykle istotne, zajęliśmy 1. miejsce w podkategorii przyjazności dla prowadzenia biznesu. To rzeczywiście pokazuje, że praca, którą wkładamy na co dzień w budowanie gospodarczego Wrocławia, przynosi sukcesy i inwestorzy chcą u nas lokować swoje inwestycje.

* ARAW – Agencja Rozwoju Aglomeracji Wrocławskiej https://araw.pl

Zapewne część inicjatyw gospodarczych jest ulokowana w sektorze smart city?

Oczywiście rozwijamy też koncepcję smart city, a więc rozwiązania innowacyjne, które sprawiają, że Wrocław rzeczywiście staje się miastem bardziej komfortowym do życia. Jak zapewne wszyscy widzimy, za chwilę miasta mogą stać się niewydolne, zwłaszcza że coraz więcej osób chce w nich zamieszkać. Pandemia trochę ten trend odwróciła. Wiele osób pracuje zdalnie i coraz częściej szuka kontaktu z przyrodą. Myślę jednak, że po pandemii znów zaczniemy notować przyrost liczby mieszkańców miast. A miasto, zwłaszcza jego infrastruktura, nie jest z gumy, nie może się rozciągnąć. Tylko wdrożenie rozwiązań inteligentnych, które przede wszystkim pozwolą mieszkańcom oszczędzać czas, tak naprawdę sprawią, że jakość życia w miastach będzie wyższa. I te miasta tak naprawdę będą wygrywały.

Z badań wynika, że najsprawniej działające inteligentne miasta priorytetowo traktują cztery obszary: cyfryzację, zdrowie, infrastrukturę i bezpieczeństwo mieszkańców. Jaką koncepcję rozwoju przyjęto we Wrocławiu?

Postawiliśmy na inwestycje w rozwój wszystkich czterech obszarów. To są bardzo ważne elementy, które w każdym mieście powinny być traktowane priorytetowo. I nie można rozwijać jednego kosztem innego. Cyfryzacja, która zdecydowanie wkracza do miast, jest elementem wiodącym i musimy dostosować funkcjonowanie miasta do nowych realiów. To gromadzone dane są tym paliwem, które napędza nasz rozwój. Dzięki nim możemy oferować różnego rodzaju usługi publiczne, skrojone i dopasowane do potrzeb mieszkańców. Cyfryzacja to też elementy związane z cyberbezpieczeństwem i zabezpieczeniem systemów informatycznych. Bo duża ilość zgromadzonych danych wywołuje potencjalne zagrożenia. Musimy więc pamiętać o dobrym zabezpieczeniu tych elementów.

Drugim ważnym obszarem jest zdrowie. Pandemia pokazała, jak bardzo niewydolny jest system opieki zdrowotnej. We Wrocławiu zdrowie chcemy traktować znacznie szerzej. Mówimy tu o dobrostanie, o tzw. zdrowiu środowiskowym. To nie tylko zdrowie, w podstawowym tego słowa znaczeniu, czyli gdzie i jak się leczymy, ale też profilaktyka. To również sport, który wpływa na ogólną kondycję ludzi, a także środowisko, w jakim przebywamy. Wysoka jakość powietrza, dobry klimat w mieście świadczą o tym, że zdrowie rzeczywiście można traktować wieloaspektowo. Ważne są więc także wszelkie usługi z tym związane, a więc telemedycyna czy teleopieka, które w czasie pandemii zaczęliśmy wprowadzać, i to z sukcesami. Bo widzimy, że ich odbiór jest bardzo dobry. To też pokazuje, że społeczeństwo łączy i akceptuje już te dwa elementy, czyli cyfryzację i zdrowie. Możemy na tym budować ciekawe projekty, które pozytywnie wpłyną na jakość i komfort życia w mieście.

Infrastruktura jest trzecim, równie ważnym elementem, który bodaj w 80% leży w gestii miasta. To są kamienice, jezdnie i chodniki codziennie przemierzane przez tysiące mieszkańców. Bardzo ważne, żeby modernizować tę infrastrukturę, cały czas ją udoskonalając, ponieważ tej starej substancji miasta nie da się powiększyć. Cała zabudowa, cała tkanka miasta została już ukształtowana, więc możemy w nią ingerować tylko w sposób innowacyjny. I tu wracamy do cyfryzacji, która pozwoli nam dostarczyć informacje

i budować tę infrastrukturę w sposób przemyślany, zmierzający w kierunku wygody życia.
Bezpieczeństwo mieszkańców na wielu poziomach to czwarty, bardzo istotny element rozwoju miasta. Bo to jest bezpieczeństwo funkcjonowania infrastruktury na poziomie zarządzania kryzysowego, czyli reagowania na akty wandalizmu, sytuacje nieprzewidziane czy kryzysowe w mieście. To też bezpieczeństwo na poziomie zdrowotnym, klimatycznym i tego, co się dzieje w mieście. Ale bezpieczeństwo mieszkańców to również bezpieczeństwo cyfrowe, związane z wszechobecną cyfryzacją, a więc zataczamy koło i wracamy do cyfryzacji. Wszystkie te cztery obszary są ze sobą ściśle związane i skorelowane. Co istotne, powinny być rozwijane łącznie – nie możemy wybrać jednego, w który będziemy inwestować. To cztery elementy, które musimy traktować priorytetowo i je rozwijać.

Czy przy projekcie smart city korzystaliście z doświadczeń innych miast?
Oczywiście przyglądamy się temu, co jest wdrażane z zakresu innowacyjnych i inteligentnych rozwiązań w różnych miastach. Musimy jednak pamiętać, że każde miasto, patrząc globalnie, jest inne. Każde ma swoje potrzeby, inną strukturę, ich mieszkańcy mają inne zwyczaje. Mieszkańcy Melbourne, Hamburga czy Singapuru mają zupełnie inne potrzeby niż mieszkańcy Wrocławia czy Warszawy lub Gdańska. Nie można kopiować wszystkich rozwiązań i próbować na siłę je wdrażać. Musimy to robić rozsądnie, z głową, bo to jest proces, który zmienia drastycznie sposób funkcjonowania miasta i jego mieszkańców. W tym celu powołaliśmy specjalny program City Lab Wrocław, który pozwala testować innowacyjne rozwiązania i przedstawiać je naszym służbom, a także kolegom z innych wydziałów.
Prezentujemy te technologie również mieszkańcom, aby mogli dotknąć, poczuć, przetestować i podzielić się z nami uwagami, czy rzeczywiście pasują do naszego miasta. Chcemy wiedzieć, jak zaspokajać potrzeby mieszkańców. To ważny proces i musi być gruntownie przemyślany i uzgadniany.

Wróćmy do tematu bezpieczeństwa. Jakie zabezpieczenia techniczne zostały zastosowane, aby podnieść poziom bezpieczeństwa mieszkańców?
Jak już wspominałem, zapewnienie bezpieczeństwa mieszkańcom musimy rozpatrywać na kilku poziomach. Kluczową kwestią jest bezpieczeństwo publiczne. W tym względzie mamy do dyspozycji system kamer, z których obrazy są odbierane w centrum zarządzania kryzysowego. To ciekawa jednostka, ponieważ doszło u nas do centralizacji. Powołaliśmy centrum, w którym operacyjnie wszystkie służby współpracują ze sobą w przypadku sytuacji kryzysowej. W jednym miejscu mamy więc policję, straż miejską, straż pożarną, pogotowie ratunkowe, mamy wszystkie służby odpowiedzialne za to, żeby w mieście było bezpiecznie. W ramach tych działań zamontowaliśmy kamery, które monitorują przestrzeń miasta, przy czym cały czas staramy się system rozbudowywać. Testujemy też różne nowości, różne systemy kamer sieciowych, kamery obrotowe – patrzymy, jak one reagują na sytuacje potencjalnie niebezpieczne.
Współpracujemy również z firmami w zakresie testowania rozwiązań wykorzystujących sztuczną inteligencję w kamerach, np. detekcję pozostawionych pakunków, czyli różnych systemów monitoringu związanych z analizą zachowań mieszkańców. Kamera uczy się najpierw standardowego zachowania, by móc reagować na te niestandardowe. Jeśli np. tłum zaczyna biec, kamera uznaje to za zachowanie niestandardowe i wysyła alarm do centrum monitoringu, żeby operator mógł szybko zareagować.
Kamery mają olbrzymi potencjał, wprowadziliśmy je również w ramach ITS-u. To one obserwują ruch uliczny. Systemy również udoskonalamy, żeby w razie wypadku można było szybko prześledzić trasę przejazdu pojazdu i np. zatrzymać sprawcę. Tutaj oczywiście musimy dokładnie wyważyć elementy związane z ochroną prywatności mieszkańców i wymogami RODO. Zapewnienie bezpieczeństwa i jednocześnie ochrona prywatności osób jest trudnym zadaniem. Ten kompromis jest bardzo ważny dla miasta, ale staramy się tam, gdzie to możliwe, wdrażać takie rozwiązania.
Pandemia sprawiła, że musieliśmy zastosować dodatkowe systemy bezpieczeństwa. W urzędach wprowadziliśmy rozwiązania do pomiaru temperatury osób wchodzących, połączone z dezynfekcją rąk. Bo przecież nie można zamknąć urzędu, sprawy obywatelskie muszą cały czas być realizowane. Nie możemy też wszystkich usług przenieść do sfery wirtualnej, ponieważ ustawodawstwo jeszcze za tym nie nadąża. Nie wszyscy mają profil zaufany, żeby można było realizować zadania cyfrowo. Osobista wizyta w urzędzie jest potrzebna. I tutaj też staramy się zapewnić bezpieczeństwo naszym mieszkańcom.
Pandemia uwidoczniła kolejny element, czyli konieczność pracy zdalnej i zdalnych spotkań. Praca w trybie home office wiązała się u nas z innym problemem – pracownik oddelegowany do takiej pracy nie zawsze może zabrać komputer do domu, pozostawia go w biurze. Musimy więc umożliwić mu na jego prywatnym sprzęcie dostęp do zasobów miejskich, co wymaga utworzenia VPN-ów, które muszą być chronione. Są to dane krytyczne, których ujawnienie może przynieść negatywne skutki. Zapewnienie bezpiecznego połączenia sieciowego jest bardzo ważne. Cały czas stosujemy rozwiązania związane z firewallami, systemami antyspamowymi i antywirusowymi.
Korzystamy też z usług firm zewnętrznych, które przeprowadzają audyty wdrażanych aplikacji. Bardzo ważne jest to, by nie było tam błędów albo luk, którymi osoby nieuprawnione mogą wejść i naruszyć prywatność naszych klientów. Mogę przytoczyć kilka statystyk z 2020 r.

ZAPEWNIENIE BEZPIECZEŃSTWA MIESZKAŃCOM MUSIMY ROZPATRYWAĆ NA KILKU POZIOMACH. KLUCZOWĄ KWESTIĄ JEST BEZPIECZEŃSTWO PUBLICZNE

Wrocław

największe miasto regionu, siedziba władz województwa dolnośląskiego i powiatu wrocławskiego. Miasto dysponuje trzecim w kraju największym budżetem (po Warszawie i Krakowie).

Powierzchnia
292,8 km

Ludność
641,9 tys*

Województwo
dolnośląskie

* stan na 31 XII 2020 r

Liczba zdarzeń ataków DDOS na strony urzędu miasta wyniosła ponad 400, z czego 120 było szczególnie niebezpiecznych. To pokazuje, jak dużo jest ataków na nasze strony po to, żeby przechwycić dane, które w większości są wrażliwe.

Jakim wdrożeniem z sektora smart city szczególnie chcielibyście się pochwalić?
Już wcześniej wspominałem o naszym programie City Lab Wrocław. To ciekawe przedsięwzięcie. W ramach tego programu testujemy różne innowacyjne rozwiązania. Robimy to wspólnie ze start-upami, ale też z firmami globalnymi, uczelniami i inkubatorami. Jako miasto oferujemy takim podmiotom fragment albo całość miasta do testowania danego rozwiązania. Do konkretnego rozwiązania dobieramy miejsce do testu. Czy to będzie jedna ulica, kamienica czy linia autobusowa – tam przeprowadzamy testy, a wynikami dzielimy się z mieszkańcami. Firma, która dostarcza nam takie rozwiązanie, uczy się, jak dany system funkcjonuje w tkance miejskiej, poprawia go, udoskonala, żeby produkt był jeszcze bardziej dopasowany do potrzeb mieszkańców. Z kolei urząd miasta uczy się wprowadzonej innowacji, służby miejskie korzystają z nowych systemów, a mieszkańcy mogą na danym fragmencie zobaczyć, czy ta technologia zwiększa komfort ich życia i czy rzeczywiście jest przydatna.
Mamy ciekawe doświadczenia związane z realizacją takich projektów, bo to one generują innowacyjność, która pojawia się w całym Wrocławiu i sprawia, że jesteśmy wysoko oceniani w rankingach. Innowacyjność w naszym mieście kwitnie, mamy doskonałe warunki, by ją wprowadzać. Chciałbym wspomnieć o jednym z projektów, który był realizowany w ramach wrocławskiego City Lab, a następnie po przeprowadzonym audycie Prezydent Wrocławia zdecydował o jego wdrożeniu w całym mieście. To system detekcji miejsc postojowych dla autokarów turystycznych oraz osób z niepełnosprawnością. W ramach tego projektu w strefach A i B płatnego parkowania na miejscach dla osób z niepełnosprawnością wprowadziliśmy detektory, które informują osobę jadącą na wyznaczone miejsce, czy jest ono wolne, czy zajęte. Nie ma stresu związanego z poszukiwaniem miejsca postojowego czy kilkukrotnym przejazdem wokół. Oferujemy aplikację, która umożliwia sprawdzenie zajętości miejsc.
Ten system zaoferowaliśmy również do usprawnienia ruchu turystycznego, który we Wrocławiu jest bardzo duży. Przed pandemią odwiedzało nas rocznie ok. 5 mln turystów, którzy zazwyczaj autokarami podjeżdżali jak najbliżej atrakcji turystycznych. Tam zawsze były problemy z postojem autokarów. Wprowadziliśmy więc miejsca 15- lub 30-minutowe, aby autokar przyjechał, wysadził wycieczkę i odjechał na miejsce, które nazywamy odstawczym. Tam powinien czekać na turystów. Wcześniej, gdy kierowcy udało się znaleźć miejsce w tym atrakcyjnym sektorze, autokar stał tam cały dzień, blokując możliwość przyjazdu kolejnej wycieczce. Powodowało to również sytuacje niebezpieczne, ponieważ turyści wysiadali na środku ulicy, na której odbywał się ruch. Wprowadziliśmy więc system detekcji miejsc postojowych, dzięki czemu straż miejska widzi, jak długo dany autokar stoi, bo czas 15 minut jest w systemie odnotowany. Mamy więc narzędzie do tego, by kontrolować autokary turystyczne. Z kolei kierowca, dostając informację o wolnych miejscach na parkingach odstawczych, już nie może się tłumaczyć niewiedzą. Aplikacja podpowiada, że to miejsce tam jest i czeka na niego. Takie rozwiązania sprawia również, że jazda dużym pojazdem jest bardziej komfortowa.
W ramach tego systemu dysponujemy platformą, która informuje o wykorzystaniu infrastruktury parkingowej miasta. Widzimy, czy rzeczywiście miejsca postojowe dla osób niepełnosprawnych lub autokarów turystycznych są wykorzystywane i w jakim procencie. Bo być może to miejsce należałoby zlikwidować albo przenieść do innej lokalizacji. Możemy zaproponować bardziej dogodne miejsce, a zwolnione przeznaczyć np. na pas zieleni czy inną usługę. To ciekawy projekt, który został zrealizowany w ramach City Lab, a później przeszedł do fazy realizacyjnej.

ROZWIJAMY KONCEPCJĘ SMART CITY, A WIĘC ROZWIĄZANIA INNOWACYJNE, KTÓRE SPRAWIAJĄ, ŻE WROCŁAW RZECZYWIŚCIE STAJE SIĘ MIASTEM BARDZIEJ KOMFORTOWYM DO ŻYCIA

Wspominał Pan o pandemii COVID-19. Jak ten czas wpłynął na rozwój koncepcji smart city?
Pandemia rzeczywiście spowodowała eksplozję cyfryzacji. Jako miasto byliśmy poniekąd gotowi na to, co się działo, choć część infrastruktury musieliśmy dostosować lub wprowadzić nowe elementy. Natomiast nie było to aż tak trudne, ponieważ już wcześniej korzystaliśmy we Wrocławiu z cyfryzacji i innowacji. I widzimy, że mieszkańcy też zaczęli bardzo aktywnie z tego korzystać. Wprowadziliśmy np. system kolejkowy, w którym przez specjalną stronę internetową można się umówić do urzędu na konkretną godzinę. Nie trzeba już przychodzić i stać w kolejce, okienko otwiera się o danej godzinie. I rzeczywiście mieszkańcy bardzo chętnie z tego korzystają. To przyszłość miast.
Bardzo dobrze sprawdziły się też rozwiązania związane z teleopieką i telemedycyną. Testowaliśmy je wśród naszych starszych mieszkańców, którzy we Wrocławiu mają tzw. karty szmaragdowe, czyli są w wieku 85+. Korzystali z tych usług i pozytywnie je ocenili, pytali też, czy pozostaną po testach na stałe. Gwarantowały im poczucie bezpieczeństwa w miejscu zamieszkania. To były systemy SOS podpięte do centrum ratownictwa medycznego. Osoba potrzebująca pomocy dzięki takiemu systemowi mogła zaalarmować służby, które bardzo szybko podejmowały działania.
Sprawdziły się też rozwiązania telemedyczne związane z urządzeniami kardiologicznymi. Ten projekt również testowaliśmy. Wyposażyliśmy mieszkańców naszego miasta ze zdiagnozowanymi problemami kardiologicznymi lub z objawami chorób kardiologicznych w zdalne urządzenia EKG połączone z centrum telemedycznym. Osoba, która się źle poczuła lub chciała zrobić badania, podpinała urządzenie, które wysyłało informację do centrum ratownictwa medycznego. Tam lekarz kardiolog analizował parametry danej osoby i decydował, czy jest potrzeba zaaplikowania środków farmakologicznych, a może jest czas na wizytę u lekarza lub sytuacja wymaga natychmiastowego wezwania karetki pogotowia ratunkowego. To rozwiązanie bardzo dobrze przyjęły też osoby, które często są określane jako wykluczone cyfrowo. Pandemia pokazała, że nie boją się nowych technologii, wystarczy im pokazać krok po kroku, jak je stosować. Dzięki tym urządzeniom czują się objęte kompleksową opieką.

Nad projektem smart city we Wrocławiu pracowało wiele osób. Na pewno są też już plany na przyszłość. Jakie nowe inwestycje zostaną przeprowadzone w mieście?
Obecnie stawiamy na rozwiązania związane ze sztuczną inteligencją. Skupiamy się na różnych możliwościach, jakie AI oferuje. Ale sztuczna inteligencja nie będzie mogła poprawnie działać bez dużej ilości danych. Dlatego kolejnym celem jest big data, czyli gromadzenie tych danych, ich przetwarzanie i analizowanie, a następnie wykorzystanie do tego, by na ich podstawie móc usprawniać codzienne funkcjonowanie Wrocławia.
Z projektów związanych ze zdrowiem, o których rozmawialiśmy, zamierzamy postawić na usługi w zakresie profilaktyki zdrowotnej, czyli teleopiekę i telemedycynę. Chcemy je zaoferować mieszkańcom po to, aby mogli regularnie dbać o zdrowie. Planujemy też dużo projektów, które będą realizowane w ramach inteligentnego miasta smar. Bo smart city to miasto wielu filarów i wielu kolorów. Będą to punktowe inwestycje zmieniające sposób funkcjonowania miasta. A wszystko po to, żeby mieszkańcom Wrocławia zaoferować najwyższą jakość życia. Będziemy zachęcać inwestorów, żeby do nas przyjeżdżali i inwestowali, bo dzięki temu nasze miasto będzie kwitło. I mamy nadzieję, że w kolejnym rankingu „Financial Times" też nas dostrzeże.

Bezpieczna Warszawa

Czy mieszkańcy Warszawy czują się bezpiecznie? Co roku Urząd Miasta zleca badanie dotyczące wielu aspektów funkcjonowania stolicy, w tym poczucia bezpieczeństwa. Jego wyniki prezentuje w tzw. Barometrze Warszawskim[1].

Ostatnie badanie realizowane na losowej, reprezentatywnej próbie 1100 mieszkańców stolicy w wieku 15 lat i więcej przeprowadzono w listopadzie 2020 r.

OPINIE MIESZKAŃCÓW

Ogólnie rzecz ujmując, warszawiacy czują się w mieście bezpiecznie, tak odpowiedziało 92% ankietowanych. Tylko 7% w swojej okolicy czuje się źle, a 1% nie odniosło się do pytania. Ponad połowa mieszkańców (67%) uważa, że poziom bezpieczeństwa nie zmienił się w ciągu roku, poprawę zauważyło 30% badanych.
Wśród zagrożeń, jakich mieszkańcy stolicy obawiają się najczęściej, wymieniano kierowców jeżdżących brawurowo, niebezpiecznie (34%). Agresji ze strony osób nietrzeźwych, narkomanów boi się 28% ankietowanych, a 24% włamań np. do mieszkań, piwnic lub samochodów. Duża grupa, bo aż 23%, obawia się zaczepiania przez grupy agresywnie zachowującej się młodzieży, a 21% kradzieży i napadów, rozbojów i bójek.
Najpilniejszymi działaniami mogącymi poprawić poziom bezpieczeństwa wg warszawiaków jest m.in. zwiększenie liczby patroli policji (44%) i rozbudowa systemu monitoringu miejskiego – zwiększenie liczby kamer (43%). Wprowadzenie surowszych kar dla przestępców sugeruje 36% badanych, natomiast 20% chce zwiększenia uprawnień policji, a 16% zwiększenia liczby patroli straży miejskiej. Tylko 7% badanych uważa, że poziom bezpieczeństwa jest wystarczający i nic nie trzeba robić.

[1] https://www.um.warszawa.pl/o-warszawie/warszawa-w-liczbach/barometr-warszawski

MONITORING MIEJSKI

Ważnym narzędziem w walce z przestępczością jest system monitoringu wizyjnego. Warszawski system jest sukcesywnie rozwijany od 2001 r. Jego rozbudowę prowadzi się dwutorowo. Po pierwsze, na terenie wszystkich dzielnic stolicy rozbudowuje się sieć światłowodową umożliwiającą podłączanie do systemu kolejnych kamer. Po drugie, rozbudowuje się system monitoringu wizyjnego w środkach komunikacji miejskiej. Kamery nie tylko pozwalają na bieżąco monitorować zagrożenia oraz wykrywać przestępstwa i wykroczenia, ale również spełniają inne, nie mniej ważne funkcje:

- działają prewencyjnie i odstraszają potencjalnych przestępców,
- poprzez dostęp do zarejestrowanego materiału ułatwiają ustalenie sprawców, osób poszukiwanych itd.,
- stanowią efektywne narzędzie operacyjnego wsparcia dla służb i optymalnego dysponowania zasobów w zależności od rodzaju zdarzeń, pozwalając na szybsze usunięcie ich skutków i ograniczenie strat,
- usprawniają zarządzanie bezpieczeństwem miasta (transportu publicznego, wprowadzania ograniczeń w ruchu, działania infrastruktury miejskiej itp.), zwłaszcza podczas zgromadzeń publicznych i imprez masowych oraz sytuacji kryzysowych.

W efekcie pracy operatorów miejskiego systemu monitoringu wizyjnego w 2020 r. zostało zgłoszonych 10 058 zdarzeń – 4858 trafiło do policji, 4132 do straży miejskiej m.st. Warszawy, a 1068 do innych służb.

[2] https://bezpieczna.um.warszawa.pl/bezpieczenstwo-publiczne/monitoring-miejski

KAŻDEGO ROKU WZRASTA LICZBA KAMER MONITORUJĄCYCH PRZESTRZEŃ MIEJSKĄ (NAZIEMNĄ, PODZIEMNĄ I MOBILNĄ). W STYCZNIU 2021 R. FUNKCJONOWAŁO ICH 18 416[2]. NA LICZBĘ TĘ SKŁADAJĄ SIĘ KAMERY:

zintegrowane w miejskiej sieci monitoringu wizyjnego	449	w wagonach tramwajowych	2 484
monitorujące Metro Warszawskie	1 975	w składach Szybkiej Kolei Miejskiej	982
w autobusach miejskich	10 483	w pociągach metra	1 800
należące do ZDM (pracują w Zintegrowanym Systemie Zarządzania Ruchem)	164	dostępne w Centrum Bezpieczeństwa	79

Katowice

Miasto w aplikacji przyszłości Milestone XProtect Corporate

Inteligentne rozwiązania w miastach to niepodważalny dowód na to, że technologia wkroczyła do aglomeracji i stała się nieodzownym elementem ich życia. Kopenhaga, Helsinki czy Chicago wykorzystują zintegrowane systemy nie tylko do zapewnienia bezpieczeństwa mieszkańcom, ale także poprawy warunków ich życia, np. przez dopasowanie transportu publicznego do zmieniającego się przepływu ludzi w miastach. W Polsce jednym z najbardziej zaawansowanych i stale usprawnianych systemów mogą pochwalić się Katowice. W stolicy aglomeracji śląskiej aplikacja Milestone XProtect Corporate pozwala na wykorzystanie wielu rozwiązań w jednym miejscu, a to zarówno zwiększa bezpieczeństwo, jak i ogranicza koszty.

20 LAT MINĘŁO – TROCHĘ HISTORII

Pomysł i pierwsze kamery pojawiły się w Katowicach w 2001 r. – wtedy miasto zainwestowało w 16 urządzeń analogowych, które zostały zainstalowane w centrum miasta i początkowo wysyłały obraz do Komendy Miejskiej Policji. Rozwiązanie to miało być pierwszym krokiem do zbudowania sieci monitoringu wizyjnego i ostrzegania przed niebezpiecznymi wydarzeniami. W latach 2012-2014 pojawił się pomysł na nową inwestycję w zakresie *smart city,* której efektem była realizacja projektu KISMiA, Katowickiego Inteligentnego Systemu Monitoringu i Analizy. Obecnie jest niemal 300 kamer rozsianych po ponad 160 km² miasta liczącego prawie 300 tysięcy mieszkańców. Katowice już na początku tworzenia systemu monitoringu umożliwiły późniejszą jego rozbudowę.

Katowice to miasto innowacyjnych rozwiązań i wdrażania nowych technologii. Stajemy się coraz bardziej smart city w różnych obszarach. To właśnie w naszym mieście powstał pierwszy w Polsce, w tej skali, inteligentny system monitoringu wizyjnego. Bez wątpienia nowoczesne rozwiązania firmy Milestone XProtect Corporate przyczyniają się do podnoszenia poziomu bezpieczeństwa w Katowicach. W 2020 r. Straż Miejska i Policja wykorzystały blisko 2,5 tysiąca nagrań z monitoringu. Wysoka skuteczność systemu KISMiA skłoniła nas do jego systematycznego rozwoju i rozbudowy – mówi Marcin Krupa, prezydent Katowic.

Równolegle z projektem KISMiA powstała sieć światłowodowa łącząca wszystkie miejskie ośrodki. W ten sposób połączono wiele punktów miasta w całość. Prace nad systemem ruszyły intensywnie w 2015 r. Najważniejszymi celami było poprawienie efektywności pracy operatorów monitoringu, skuteczności działania służb oraz ich koordynacji. Zintegrowany system miał zapewnić lepszą orientację co do zdarzenia i sprawniejszą współpracę służb wspierających bezpieczeństwo w mieście. Pełne wdrożenie systemu nastąpiło w roku 2017, obecnie można do niego włączyć monitoring z nowo powstających inwestycji, takich jak centra przesiadkowe.

Dokładanie kolejnych punktów monitoringu spowodowało, że zaczęliśmy myśleć o tym, by efektywnie obsłużyć system, posługując się sztuczną inteligencją, która wspiera pracę operatorów. Centrum monitoringu powstało w 2017 roku i objęło dotychczasowe lokalizacje kamer oraz nowe lokalizacje w śródmieściu i dzielnicach, jak również 16 punktów SAR (Strefy Aktywności Rodzinnej). Dodatkowo w ramach projektu KISMiA uruchomiono 10 punktów nadzoru nad ruchem drogowym usytuowanych na głównych ciągach komunikacyjnych miasta Katowice. System pozwala na rozbudowę nawet do 1024 kamer – mówi Mirosław Cygan, naczelnik Wydziału Zarządzania Kryzysowego Urzędu Miasta, koordynator projektu KISMiA

DATA CENTER NA MIARĘ XXI W.

Proces wdrożenia tego systemu był możliwy dzięki użyciu kilku komponentów. Do tego celu wykorzystano oprogramowanie IBM *Intelligent Operations Center* – służące jako moduł wsparcia operacyjnego oraz IBM *Intelligent Video Analytics* – to moduł analizy rejestrowanych obrazów. Zarządzanie materiałem wizyjnym odbywa się za pomocą aplikacji Milestone XProtect Corporate. Pozwala ona na rejestrację, przechowywanie i udostępnianie materiału wideo oraz płynne zarządzanie kamerami. Kolejnym ważnym elementem KISMiA jest nowoczesne Centrum Przetwarzania Danych, tzw. *Data Center.* To miejsce przechowywania i analizy danych. Ze strony Katowic nad całością projektu czuwały dwa wydziały UM: Informatyki i Zarządzania Kryzysowego. Obecnie nad systemem czuwa ekspercko Marcin Palka.

Moim zdaniem kluczowe i unikatowe na skalę kraju w KISMiA jest to, że system powstawał z myślą o przyszłości. Budowa sieci światłowodowej wraz z kolejnymi punktami monitoringu i data center to był strzał w dziesiątkę – podkreśla Marcin Palka. I dodaje: *– Katowice wyłoniły inżyniera projektu, który pod kątem technologicznym jest wspierany przez Milestone Systems. To ułatwia opracowanie strategii dla miasta na lata.*

System w połączeniu z aplikacją Milestone XProtect działa z pełnym poszanowaniem prywatności. Siatka prywatyzująca, czyli filtr nałożony na obraz z kamer, nie pozwala dostrzec twarzy osób. Do systemu nie ma też swobodnego dostępu nawet dla osób uprawnionych.

UWAGA, ZAGROŻENIE!

W KISMiA zdefiniowano rodzaje sytuacji, które system wykrywa jako zagrożenie i natychmiast alarmuje operatora. To zdecydowanie skraca czas reakcji ze strony odpowiednich służb lub komunikacji głosowej w miejscu zdarzenia. System reaguje m.in. na:

- leżącego człowieka,
- pozostawiony obiekt,
- zwierzęta w Strefach Aktywności Rodzinnej (to m.in. place zabaw, miejskie siłownie w plenerze, parki linowe, miejsca do grillowania itd.),
- zbiegowisko w przestrzeni publicznej (szczególnie ważne w czasie pandemii),
- kolizję pojazdów,
- parkowanie w miejscach niedozwolonych,
- jazdę „pod prąd",
- szkody wywołane np. wiatrem czy podtopieniami.

Każda z tych niebezpiecznych sytuacji jest wykrywana, a następnie trafia do operatora, który decyduje, jak ten incydent rozwiązać. Aplikacja Milestone XProtect w systemie KISMiA alarmuje operatora np. o obiekcie znajdującym się w Strefie Aktywności Rodzinnej w godzinach, gdy SAR nie funkcjonuje. Niepożądany obiekt może pojawić się w nocy i wtedy od operatora zależy, jaką podejmie reakcję na takie zdarzenie. Jeśli obiektem okaże się krążący po okolicy dzik, reakcja będzie inna niż wtedy, gdy zostaną wykryte osoby przebywające w SAR po zmroku. Strefy Aktywności Rodzinnej są nie tylko obserwowane, punkty kamerowe są wyposażone w zestawy głośnikowe, które sprawdzają się, gdy na teren SAR wtargną wandale. Głos operatora skutecznie ich odstrasza i często interwencja na głosowym ostrzeżeniu może się zakończyć.

POLSKIE DROGI

Katowicki Inteligentny System Monitoringu i Analizy wspiera także kontrolę dróg w mieście. Bramownice LPR *(Licence Plate Recognition)* nie monitorują prędkości samochodów w mieście, ale pokazują przepływ ruchu oraz są pomocne w czasie wykrycia incydentu, jakim może być uciekający lub skradziony pojazd. Dzięki bramownicom operator jest w stanie przekazać odpowiednim służbom, w którym kierunku zmierza poszukiwany samochód. Z danych katowickiej policji wynika, że liczba kradzieży samochodów w Katowicach spadła z poziomu 337 w roku 2016 do 79 przypadków w roku 2020! Jednocześnie wzrosła wykrywalność w tej kategorii przestępstw z poziomu 16,4% do 76%.

TROCHĘ STATYSTYKI

O skuteczności systemu świadczy wykrywalność przestępstw ogółem. Z danych katowickiej policji wynika, że od 2017 r. w ciągu roku nie spada ona poniżej 65 proc., zmniejsza się także bezwzględna liczba przestępstw. W 2020 r. wykrywalność przestępczości ogółem w Katowicach osiągnęła poziom 67,4 proc. Rozmieszczenie kamer jest szeroko konsultowane społecznie, a ich rola prewencyjnego odziaływania na przestrzeń publiczną jest nieoceniona.
O kamery monitoringu upominają się sami mieszkańcy stolicy Górnego Śląska, wielu działaczy społecznych składa wnioski do Urzędu Miejskiego, by takie urządzenia zostały zainstalowane i podpięte do systemu KISMiA w najodleglejszych krańcach miasta. Dowodzi to, że system daje mieszkańcom szansę na życie w mieście przyszłości – *smart city.*

Pandemia

czyli poligon doświadczalny nowych technologii

Kilkanaście miesięcy pandemii to wystarczająco długi okres, aby pokusić się o spojrzenie na kilka rozwiązań na styku technologii i bezpieczeństwa, które w tym czasie weszły do użycia lub zostały spopularyzowane. Rozwiązania te zapewne zostaną z nami na dłużej.

Bartosz Dominiak

Pandemia zmieniła nasze życie. Będzie to czynić również w kolejnych latach, niezależnie od tego, kiedy się skończy. Pojęciem, które z dużym prawdopodobieństwem opisze te zmiany w odniesieniu do obszarów miejskich, stanie się *urban resilience,* czyli odporność miast na zjawiska nagłe, nieprzewidziane i zagrażające standardowemu funkcjonowaniu. Do ubiegłego roku ten zwrot był używany raczej w odniesieniu do zmian klimatycznych i gwałtownych zjawisk pogodowych. Pandemia pokazała, że miejska odporność potrzebuje szerszego kontekstu. Jej celem musi być gotowość na kolejne „czarne łabędzie".

Budowanie odporności miast, a szerzej państw na zjawiska nieprzewidywalne będzie opierać się na wykorzystaniu możliwości nowych technologii. Dlatego warto spojrzeć na ostatnich kilkanaście miesięcy jako na ogólnoświatowy poligon, gdzie przetestowano tysiące rozwiązań innowacyjnych. Większość nie wyszła poza fazę koncepcji, a w najlepszym wypadku pierwszych prób. Ale część się sprawdziła i towarzyszy nam w codziennym życiu.
Tak jest z gamą rozwiązań technologicznych zapewniających możliwość bezpiecznej zdalnej pracy i nauki, a także efektywnego i masowego komunikowania się na odległość w celach zawodowych, praktycznie w każdym sektorze gospodarki. Udane rozwiązania można też znaleźć w obszarze bezpośredniej walki z pandemią. Dziś służą jak najszybszemu przywróceniu normalności, choć w przyszłości znajdą również inne zastosowania.

Rok temu w numerze a&s Polska poświęconym *smart city* napisałem, że u progu trzeciej dekady XXI w. żadne miasto inteligentne nie może pomijać nowoczesnych technologii. I nie chodzi tutaj o technologie oraz nowoczesność same w sobie. Należy poszukiwać rozwiązań adekwatnych do potrzeb. Czasami dany problem można rozwiązać bez kosztownych inwestycji w nowoczesny i zaawansowany sprzęt – wystarczą dobry pomysł, drobne zmiany w infrastrukturze, procedurach lub organizacji. I takie są trzy obszary rozwiązań, o których piszę poniżej. Odpowiadają na potrzeby.

APLIKACJE

Zacznijmy od tego, co niemal każdy z nas ma przy sobie, czyli smartfonów. W ostatnim roku pojawiły się dwie rządowe aplikacje, których funkcjonowanie było bezpośrednio i wyłącznie związane z walką z pandemią COVID-19. Pierwsza z nich STOP COVID – ProteGO Safe została udostępniona użytkownikom Androida nieco ponad miesiąc po ogłoszeniu pandemii w Polsce, a kilkanaście dni później również użytkownikom telefonów z system iOS. Założenie jest proste – program ma ostrzegać użytkownika, czy nie był narażony na spotkanie z osobą zakażoną wirusem SARS-CoV-2. Wykorzystując technologię Bluetooth, aplikacja monitoruje otoczenie w poszukiwaniu innych telefonów, na których też jest zainstalowana. Jeśli je znajdzie, a kontakt pomiędzy urządzeniami z odległości mniejszej niż 2 m trwa dłużej niż 15 minut, anonimowe zaszyfrowane informacje o takim spotkaniu zostaną zapamiętane przez smartfony przez 14 dni. Użytkownik, u którego zostanie stwierdzone zakażenie wirusem, otrzymuje unikatowy kod, który wpisuje w aplikacji i w ten sposób wysyła innym telefonom, „spotkanym" w minionych dwóch tygodniach, anonimowe ostrzeżenie o możliwości zakażenia.
Aplikacja STOP COVID nie przesyła żadnych danych osobistych użytkownika. W początkowym okresie jej użytkowania narosło wiele mitów na ten temat, co prawdopodobnie ograniczyło zaufanie potencjalnych użytkowników do tej rządowej usługi. Jej efektywność jest też obarczona wieloma warunkami. Okazuje się pomocna tylko wtedy, gdy jest jednocześnie zainstalowana przy włączonym Bluetooth na „spotykających się" telefonach, a osoba zakażona uzyska i wpisze unikalny kod w aplikacji, aby uruchomić automatyczne powiadomienia. Szansa na wystąpienie łącznie tych warunków jest stosunkowo niewielka przy ograniczonej liczbie pobrań (do lutego 2021 r. – ok. 1,8 miliona).

SZYBKIE WDROŻENIE APLIKACJI ZWIĄZANYCH BEZPOŚREDNIO Z WALKĄ Z PANDEMIĄ PRZEŁAMAŁY NIECHĘĆ UŻYTKOWNIKÓW DO APLIKACJI PODMIOTÓW PUBLICZNYCH

Pozytywem w aplikacji jest jej uzupełnianie na kolejnych etapach pandemii o nowe funkcjonalności: możliwość zapisania się na test czy zgłoszenia chęci zaszczepienia się i uzyskania dostępu do formularza rejestracji na szczepienie. Ciekawym rozwiązaniem jest też współpraca aplikacji z jej odpowiednikami w niektórych krajach członkowskich Unii Europejskiej.
Druga aplikacja – Kwarantanna domowa – jest jedyną w Polsce, której zainstalowanie w określonych przypadkach jest obowiązkowe na mocy przepisów ustawy. Muszą ją instalować wszyscy zobowiązani do poddania się kwarantannie (wyjątek – osoby z dysfunkcją wzroku oraz ci, którzy złożą oświadczenie, że nie posiadają urządzenia mobilnego).
Aplikacja ma wspomóc służby (przede wszystkim policję) przy kontrolowaniu, czy osoby na kwarantannie nie opuszczają miejsca jej odbywania. Założenie jest proste: w momencie rozpoczęcia kwarantanny, znajdując się już w miejscu jej odbywania, instalujemy aplikację na telefonie i wykonujemy selfie. To samo zadanie o losowych porach dnia musimy wykonywać aż do zakończenia kwarantanny. Oprogramowanie kontroluje zgodność twarzy i lokalizacji osoby na kwarantannie. W przypadku braku pozytywnej weryfikacji można spodziewać się wizyty policjanta.
W przeciwieństwie do wcześniejszej aplikacji Kwarantanna domowa korzysta z danych użytkownika (imię, nazwisko, numer telefonu, deklarowany adres odbywania kwarantanny, wykonane aplikacją zdjęcia i lokalizacja użytkownika). Jej niewątpliwą zaletą – jeśli spojrzeć na efektywność całości systemu – jest prawny obowiązek instalacji. Choć niezrozumiały jest brak takiego obowiązku dla osób, które przechodzą z kwarantanny do izolacji, gdy mają już pozytywny wynik testu COVID-19. Takie osoby nie są objęte działaniem tej ani żadnej innej aplikacji.

Z wdrożenia w Polsce obu aplikacji można wyciągnąć kilka wniosków na przyszłość. Po pierwsze, podmiot publiczny (w tym wypadku rząd) jest w stanie szybko (w ciągu kilku tygodni) wdrożyć takie rozwiązanie, co burzy mit budowania tego typu publicznych systemów latami. Po drugie, obie aplikacje, mimo początkowej negatywnej opinii o STOP COVID, w jakimś stopniu przełamały niechęć użytkowników do aplikacji podmiotów publicznych. Może to otworzyć drogę do łatwiejszych wdrożeń kolejnych tego typu rozwiązań, również w innych obszarach niż bezpieczeństwo zdrowotne. Po trzecie, okazało się, że publiczne aplikacje na smartfony nie muszą służyć wyłącznie wymianie informacji z obywatelami, ale mogą stać się realnym narzędziem funkcjonowania państwa, zastępując, w przypadku Kwarantanny domowej, tysiące policjantów.

DRONY

Analizując ostatni rok pod kątem wykorzystania technologii w polskich miastach, nie można pominąć bezzałogowych statków powietrznych (BSP). Popularne drony, wywodzące się z sektora wojskowego, a kojarzące się wielu osobom przede wszystkim z korzystaniem w celach rozrywkowych (niepowtarzalne zdjęcia i filmy), już od wielu lat znajdują zastosowanie w poważnych działaniach cywilnych. W miastach były przede wszystkim używane przez straż miejską do wykrycia źródeł emisji tru-

PANDEMIA ZORGANIZOWAŁA WSZYSTKIM PRZYSPIESZONY KURS KORZYSTANIA Z CYFROWYCH USŁUG PUBLICZNYCH. DLA WIELU POLEK I POLAKÓW INTERNETOWE KONTO PACJENTA (IKP) JEST PIERWSZYM DOŚWIADCZENIEM Z TĄ FORMĄ KORZYSTANIA Z OFERTY USŁUGOWEJ PAŃSTWA

jących substancji do atmosfery. Ostatnie kilkanaście miesięcy pokazało, że drony mogą być pomocne również w innych obszarach.

W początkowych tygodniach pandemii furorę robiły nagrania dronów z całego świata wspierających służby w różnych działaniach w przestrzeni miast: nadawano komunikaty z dronów, kamerami na dronach wyszukiwano osoby nieprzestrzegające reżimu sanitarnego, za pomocą dronów ozonowano ulice i mierzono temperaturę przechodniom. Dron wyprowadzał na spacer psa, prawdopodobnie należącego do osoby znajdującej się na kwarantannie lub w izolacji. Jednak znacznie ciekawsze jest to, co nie było aż tak widowiskowe dla publiczności w mediach społecznościowych. W polskich warunkach ważnym wydarzeniem były testowe loty BSP z towarem realizowane na dłuższą odległość poza zasięgiem wzroku pilota. Historyczny pierwszy tego typu lot odbył się 29 kwietnia 2020 r. na trasie między szpitalem MSWiA przy ul. Wołoskiej a Centralnym Szpitalem Klinicznym przy ul. Banacha w Warszawie. Towarem przeniesionym przez dron były próbki z materiałem do badań na obecność wirusa SARS-CoV-2. Podobne loty techniczne odbyły się również 17 listopada, tym razem na trasie Szpital Narodowy – szpital MSWiA.

Te testy, zapewne przyspieszone pandemią, są dużym krokiem w kierunku uruchomienia w Polsce transportu dronowego. Nietrudno przewidzieć kolejne ładunki do przenoszenia w ten sposób, gdy czas i bezpieczeństwo odgrywają istotną rolę: transport krwi do operacji, organów do przeszczepu czy automatycznego defibrylatora do osoby znajdującej się w sytuacji zagrożenia życia.

WIRTUALNY PACJENT, CZYLI IKP

Na koniec obszar rozwiązań technologicznych, które działały przed pandemią, ale cieszyły się niewielkim zainteresowaniem odbiorców. Internetowe Konto Pacjenta to webowa usługa Ministerstwa Zdrowia ułatwiająca pacjentom korzystanie z usług medycznych – tradycyjnych i cyfrowych. Mimo że IKP posiada każdy obywatel z nadanym numerem PESEL, to usługa do czasu pandemii nie była zbyt popularna. Większość osób wiedziała o niej,, nie miała możliwości zalogowania się (za pośrednictwem profilu zaufanego lub e-dowodu) albo niskie umiejętności cyfrowe uniemożliwiały korzystanie z niej. Pod koniec 2020 r. z IKP korzystało ok. 850 tysięcy osób. Rok później liczba użytkowników wzrosła do 4,7 mln, a w kwietniu 2021 r. przekroczyła 7 mln. Według danych z listopada 2020 r. ok. 20 proc. użytkowników IKP stanowiły osoby powyżej 50. roku życia. Te liczby robią wrażenie.
Okres pandemii przyczynił się do ogromnej dynamiki napływu nowych osób do IKP, choć sama usługa tylko w części dotyczy aktywności związanych z koronawirusem. Od marca ub.r. pacjenci mają utrudniony dostęp do tradycyjnych wizyt w przychodniach, które w wielu wypadkach zastąpiono teleporadami. To zachęca pacjentów do poszukiwania dodatkowych informacji o możliwości leczenia, a tym samym kieruje ich uwagę na IKP. Od roku 2020 trwa proces wdrażania e-recept oraz e-skierowań, które również zachęcają do wypróbowania cyfrowej usługi Ministerstwa Zdrowia.

Na rosnącą popularność IKP można spojrzeć w szerszej perspektywie. Pandemia wymusiła na wszystkich przyspieszony kurs z umiejętności korzystania z cyfrowych usług publicznych. Wydaje się, że dla wielu Polek i Polaków IKP jest pierwszym doświadczeniem z tą formą korzystania z oferty usługowej państwa. Raczej zakładają profil zaufany, aby móc skorzystać z IKP, a nie korzystają z IKP, bo już wcześniej mieli profil zaufany. Taka przyspieszona edukacja cyfrowa zaowocuje w przyszłości zwiększonym korzystaniem z innych usług, które już dziś są dostępne choćby w ramach witryny obywatel.gov.pl.

PRZED NAMI NORMALNOŚĆ BARDZIEJ TECHNOLOGICZNA

Przedstawione w artykule obszary zastosowania nowych technologii stanowią niewielki wycinek innowacyjnych wdrożeń w okresie pandemii. Takich przykładów można podać znacznie więcej. Wymieńmy choćby sztuczną inteligencję wbudowaną w monitoring wizyjny w celu wykrywania dużych skupisk ludzi albo różnego rodzaju urządzenia skanujące zdalnie stan zdrowia osób np. wchodzących do budynku. Kilkanaście ostatnich miesięcy w sposób niezaplanowany przyspieszyło wiele zjawisk w dziedzinie innowacyjności. Ale był to też czas powszechnej, również przyspieszonej edukacji publicznej z korzystania w życiu codziennym z nowych usług cyfrowych.

Dzięki pracy naukowców (szczepionki w niecały rok!) oraz całego środowiska medycznego zaczynamy wracać do normalności. Ale to będzie nowa, bardziej technologiczna normalność.

BARTOSZ DOMINIAK

Autor jest zastępcą burmistrza Dzielnicy Ursynów m.st. Warszawy. Od lat zajmuje się problematyką rozwoju miast inteligentnych w Polsce. Prowadzi zajęcia ze studentami w ramach przedmiotów poruszających tematykę *smart city*.

Covidowe reperkusje

Co pandemia rozwinęła, polityka chce zwinąć – niespodziewane przyspieszenie rozwoju *smart city* i równie niespodziewane czarne chmury na horyzoncie.

Jacek Tyburek

Dla mieszkańców miast pandemia COVID-19 to czas udręki, stresu i ograniczeń. To moment, w którym zdaniem wielu gadżeciarska koncepcja *smart city* miała swoje pięć minut. To był też moment, kiedy miały okazję upaść różne mity dotyczące *smart city.* Jednym z nich było to, że jako koncepcja jest możliwa do zastosowania głównie w nowatorskich projektach miast budowanych od zera, jak Masdar na pustyni czy New Songdo City w Korei. Innym mitem była stawiana często teza, że obszarem wdrożenia technologii *smart city* mogą być jedynie metropolie. W miastach średnich i małych takie inwestycje miały być – zdaniem niektórych komentatorów – nieuzasadnione ekonomicznie. Te właśnie mity zostały skutecznie obalone przez potrzeby wywołane pandemią. Wszyscy nagle musieliśmy się skutecznie komunikować przez Internet, dotyczyło to zakupów, załatwiania spraw zdrowotnych, ale też urzędowych. To nie była sytuacja dobrowolności, tylko konieczność bezalternatywna.

GDZIE JESTEŚMY PO 1,5 ROKU OD PIERWSZYCH DONIESIEŃ O NOWYM ŚMIERCIONOŚNYM WIRUSIE?

Dominika Brodowicz z SGH w kilku swoich publikacjach dokonała interesującego zestawienia konkretnych rozwiązań technologicznych, których rozwój należy powiązać z potrzebami ujawnionymi w trakcie pandemii. To takie aspekty, jak e-urząd czy zakup biletów komunikacji miejskiej za pośrednictwem aplikacji mobilnej, ale nie tylko. Dobrze znane od lat monitorowanie zdrowia seniorów za pomocą bezprzewodowych bransoletek, telemedycyna. Temat wcześniej interesujący wąsko wyspecjalizowanych ekspertów. Technologie, które do tej pory zdawały się mieć rangę zaledwie gadżetów, w dobie epidemii nabierają znaczenia, stają się wręcz niezastąpione. Epidemia doprowadziła do rozwoju takich dziedzin życia nierozerwalnie związanych z inteligentnymi miastami, jak e-handel czy płatności za pomocą e-portfela. Zmiany nastąpiły nie tylko w gospodarce, ale także w kulturze. Wirtualne spektakle teatralne czy muzealne wystawy online przestały dziwić. Wyraźny progres nastąpił także w edukacji. Szkoły musiały szybko wdrożyć w życie nowe formy przekazywania wiedzy.

Epidemia wymusiła rewolucję cyfrową, a ta – jak wiadomo – jest jednym z najważniejszych symptomów transformacji miasta w *smart city.* Pojawiły się takie rozwiązania innowacyjne, jak urzędowe paczkomaty, autonomiczne środki transportu czy drony monitorujące sytuację w mieście. Czujniki implementowane w przestrzeni miejskiej mogą w przyszłości wspomóc systemy wczesnego ostrzegania przed rozprzestrzenianiem się chorób. Wzrosło zainteresowanie automatyzacją w zakładach pracy. Wspomnieć należy też o rozwoju takich rozwiązań, jak system powiadomień SMS o zagrożeniach, e-recepty, systemy monitorujące dystans pomiędzy osobami, internetowe platformy do kontaktu pomiędzy wolontariuszami a osobami potrzebującymi pomocy czy opaski do pomiaru temperatury. Technologia stała się sprzymierzeńcem w walce z pandemią, a rozwiązania, na które dawniej potrzeba było lat, zostały wdrożone w ciągu kilku tygodni. Eksperci są zgodni, że tego typu rozwiązania już z nami pozostaną, co de facto przyspieszy rozwój inteligentnych miast. Wprowadzane w okresie epidemii innowacje z zakresu *smart city* nie tylko zwiększą w przyszłości bezpieczeństwo epidemiczne, ale też pozwolą zrealizować inne cele stawiane przed inteligentnymi miastami, jak chociażby ograniczanie zasobów naturalnych czy poprawa komfortu życia mieszkańców.

Zacznijmy od jednego z liderów szerokiego zastosowania technologii – Seulu. Miasto uruchomiło dedykowaną platformę, uaktualnianą kilkukrotnie w ciągu dnia, która zawiera dane o liczbie nowych przypadków zachorowania, wieku pacjentów, ogniskach zakażeń i dezynfekcjach (z dokładnością do konkretnej restauracji czy kina). System ten ma być wsparciem dla mieszkańców przy podejmowaniu decyzji o wybraniu się do danego miejsca, zachęca też do monitorowania i raportowania symptomów po wizycie w punkcie oznaczonym jako ognisko. Rozwiązanie to – jak wiele innych z zakresu *smart* – wymaga od użytkowników zaufania, że ich personalia są bezpieczne i pozostaną anonimowe, zwłaszcza że na ich podstawie tworzy się komercyjne aplikacje. W Korei Południowej dostępne są np. Corona 100m, Corona NOW oraz Corona Map, które zawierają m.in. dane o wieku pacjentów i miejscach, które ostatnio odwiedzili. W walce z rozprzestrzenianiem się wirusa wykorzystuje się także kamery termowizyjne, inteligentne przystanki czy bezdotykowe kioski (budki). Służą one do wykrywania podwyższonej temperatury u osób chcących skorzystać z transportu miejskiego lub uczestniczyć w imprezach masowych. Dla przykładu, w dzielnicy biznesowej Seongdong w Seulu testowano wiaty autobusowe zasilane energią słoneczną, wyposażone w sterylizatory ultrafioletowe i kamery termowizyjne do mierzenia temperatury osób oczekujących na autobus. Oprócz kamer używa się także opasek do pomiaru temperatury.

Kolejnym przykładem jest Tel Awiw. Poszukując skutecznych rozwiązań do walki z koronawirusem i opracowania odpowiednich rozwiązań technologicznych w celu zapobiegania rozprzestrzenianiu się zachorowań, już na początku pandemii zorganizowano wirtualny hackathon, czyli maraton projektowania dla programistów, służący opracowywaniu określonych aplikacji. Poszukiwano rozwiązań w trzech obszarach:

a) lokalny biznes (narzędzie informujące o tym, które firmy są narażone na bankructwo, a które nie),
b) bezpieczeństwo publiczne (wirtualne i fizyczne narzędzia zachęcające mieszkańców do pomocy służbom miejskim w utrzymaniu porządku),
c) wsparcie mieszkańców (narzędzia organizujące społeczności opiekujące się osobami wymagającymi pomocy).

Co istotne, projekt zrealizowano we współpracy z Global Resilient Cities Network (GRCN), organizacją, która w Tel Awiwie skupia się na działaniach na rzecz zwiększania odporności miasta (ang. *resilience*).

Kwestia odporności miasta w czasach przed pandemią oznaczała raczej to, co łączy się ze zmianami klimatycznymi. W obliczu wyzwania, jakim jest powstrzymanie transmisji wirusa, tworzy się przestrzeń dla biznesu opartego na nowoczesnych technologiach, które można sprzedawać i implementować w wielu miejscach na świecie. W Estonii powstała platforma Zelos, której zadaniem jest wsparcie przez wolontariuszy osób przebywających na kwarantannie. Mediolańska platforma SharingMi z kolei ma na celu skłanianie mieszkańców do odpowiedzialnych zachowań, np. pozostania w domu w zamian za różnego rodzaju nagrody.

Jednakże, będąc odpowiedzialnym za funkcjonowanie miasta, nie można polegać jedynie na dobrej woli i domniemaniu, że wszyscy obywatele dostosują się do wprowadzonych obostrzeń i zasad zachowania w przestrzeni publicznej. Pojawiały się, również na rynku polskim, urządzenia mające ostrzegać o naruszeniu obligatoryjnego dystansu społecznego. Dystans społeczny, który w zależności od rekomendacji danego kraju wynosi od 1,5 do 2 m, stanowi kolejny obszar zastosowania inteligentnych rozwiązań, w tym kamer, czujników i robotów. Specjaliści z DXC Technology podają jako przykład, że przestrzeganie zasad obowiązujących w miejscu pracy znacząco ułatwiałyby noszone osobiste czujniki, emitujące alarmy w momencie niezachowania odległości.

Z kolei w otwartej przestrzeni coraz częściej wykorzystuje się roboty monitorujące skupiska ludzi, dzielący ich dystans i sposób przemieszczania się w ruchu pieszym. W Singapurze tzw. Spot (czyli robot-pies) stworzony przez Boston Dynamics patroluje parki i przypomina osobom w nich obecnym o zachowaniu odpowiedniej odległości od siebie. Tego typu rozwiązania są istotne w czasie łagodzenia restrykcji, gdyż dzięki nim przebywanie w przestrzeni publicznej staje się bezpieczniejsze. Ponadto uruchomiono mapę do monitorowania w czasie rzeczywistym skupisk ludzi w parkach, tak by można było je omijać.

Punktem wspólnym wymiennych projektów jest rozwój nie tylko aplikacji i urządzeń, ale też – a może przede wszystkim – znaczne wzmocnienie zasięgu Internetu. Chodzi o zminimalizowanie wykluczenia społecznego osób, które nie mają do niego dostępu, ale również prozaiczne wzmocnienie dostępności sygnału o wymaganej przepustowości. Wśród licznych wymogów stawianych inteligentnym miastom jednym z najczęściej powielanych jest swobodny, zrównoważony dostęp ich mieszkańców do sieci internetowej i baz danych. Nie jest to jednak możliwe, gdy przesyłanie danych jest zawodne i niestabilne bądź nie jest w stanie obsłużyć dostatecznie dużej liczby urządzeń. W takiej sytuacji ani edukacja na odległość, ani telemedycyna czy zdalne sprawowanie obowiązków służbowych nie są możliwe. Dlatego eksperci z optymizmem patrzą na wprowadzenie nowej generacji sieci bezprzewodowej – 5G, która pozwoli ustabilizować połączenia sieciowe i znieść ich dotychczasowe ograniczenia.

Integralnym elementem funkcjonowania każdego inteligentnego miasta jest wdrożenie i zastosowanie rozwiązań z zakresu tzw. Internetu Rzeczy, w uproszczeniu polegającego na połączonej sieci czujników i inteligentnych urządzeń, które są w stanie zbierać, przechowywać oraz wymieniać pomiędzy sobą zgromadzone dane. W najbardziej rozwiniętej wersji mogą one też odpowiednio reagować w odpowiedzi na otrzymane wiadomości. Wspomniane wcześniej czujniki odległości również należą do zakresu funkcjonowania IoT. Do tego grona można też zaliczyć m.in. autonomiczne pojazdy, zintegrowaną sieć monitoringu w postaci kamer i czujników ruchu, systemy szybkiego ostrzegania czy niezawodne kanały komunikacji i przesyłania danych.

Kolejnymi elementami wchodzącymi w skład IoT są wszelkiego rodzaju kamery i czujniki monitorujące konkretne zjawiska czy sytuacje. Rozbudowana sieć tego typu urządzeń, zaimplementowana na terenach miejskich, znacznie wspomoże systemy wczesnego ostrzegania przed rozprzestrzenianiem się chorób, a ich szybkie wykrywanie pozwoli na skuteczną i szybką reakcję. Przykładem mogą być np. kamery na podczerwień oraz sensory mierzące temperaturę.

W tym miejscu nad koncepcją *smart city* pojawia się pierwsza czarna chmura. Pułapką samą w sobie jest dynamiczny rozwój tej technologii. Oczywiście to nie technologia jest problemem, ale ilość danych, jakich potrzebuje do swojej pełnej funkcjonalności. Koncepcja *smart city* nie ma zwartego modelu rozwoju. Stanowi raczej ideę przybierającą różne formy w zależności od tego, w którym miejscu jest realizowana. To pewnego rodzaju słabość, gdyż brak takiej perspektywy strategicznej nie ułatwia prac inżynierskich, choć z pewnością sprzyja kreatywności.

DROGA CHIN

W ostatnich latach pojawiła się nowa koncepcja, tzw. system kredytu społecznego występujący pod angielską nazwą *social credit system.* Został stworzony w Chinach na potrzeby sprawnego zarządzania w społeczeństwie żyjącym na coraz wyższym poziomie zaawansowania technologicznego. Jego koncepcja i konstrukcja, ciągle testowana i wdrażana w Państwie Środka, jest zgodna z tamtejszym porządkiem prawnym i mentalnością. Jest zupełnie nie do przyjęcia w społeczeństwie obywatelskim na Zachodzie.

Chińczycy są oceniani na podstawie zachowań, które – w przełożeniu na rodzimą płaszczyznę – odnoszą się do różnych gałęzi prawa: cywilnego, karnego czy administracyjnego. Ocena obywatela ma kolosalny wpływ na poziom jego życia. Wysoki wynik nie tylko jest powodem do społecznej nobilitacji, osoby klasyfikowane wysoko wejdą do stref VIP na lotniskach, wypożyczą lepsze auto, pójdą na wymarzone studia bądź poślą dzieci do dobrych szkół. Osoby mające ocenę niską mogą spodziewać się m.in. wolniejszego Internetu, problemów z otrzymaniem kredytu, a nawet zablokowania dostępu do wielu zawodów, np. prawniczych. Co więcej, dostęp do systemu z ocenami obywateli nie jest ograniczony do instytucji rządowych.

Dlaczego wspominamy o tym w artykule na temat *smart city?* Przede wszystkim dlatego, że jedną z bazowych informacji dla systemu są dane z systemów wizyjnych w miastach oraz z biometrycznych systemów kontroli dostępu w różnych instytucjach. Szczególnie monitoring wizyjny, z dynamicznie rozwijającą się warstwą analityki obrazu, jest tutaj punktem stycznym.

OBAWY I OGRANICZENIA W KRAJACH UE

Lęk w świecie zachodnim nie jest zupełnie nieuzasadniony, gdyż niektóre funkcjonalności typowe dla chińskiego ujęcia oceny obywatelskiej są już stosowane na świecie w co najmniej kilku gigantach technologicznych wobec konsumentów. Oczywiście powód takiego rozwoju rozwiązań nie leży w potrzebach inwigilacji politycznej, ma uzasadnienie wyłącznie marketingowe. Nie zmienia to jednak faktu, że zaczynamy poruszać się na cienkiej granicy pomiędzy światami a ich założeniami organizacyjnymi.

Dlatego też w Unii Europejskiej trwa dyskusja nt. większej kontroli nad wdrażanymi technologiami. Jej efektem jest klasyfikacja niektórych systemów AI jako wysokiego ryzyka i co do których mają się pojawić szczególne obowiązki po stronie uczestników cyklu życia tych rozwiązań. Właściwe zrozumienie tej klasyfikacji i dokonanie mapowania własnych rozwiązań ma kluczowe znaczenie dla określenia zakresu naszej odpowiedzialności, a także wyznaczenia kolejnych kroków związanych z marketowaniem systemu wykorzystującego sztuczną inteligencję. Do tej listy zaliczono następujące obszary:

- identyfikacja biometryczna osób (w czasie rzeczywistym i *post factum);*
- zarządzanie ruchem, dostawami wody, paliw czy ogrzewania i elektryczności;
- dostęp osób do instytucji edukacji oraz zawodowych;
- rekrutacja pracowników, awanse lub rozwiązanie stosunku pracy;
- dostęp do benefitów socjalnych i usług;
- ocena zdolności kredytowej lub scoring społeczny;
- awaryjny dostęp do m.in. opieki medycznej (chodzi o ustalanie priorytetów);
- szereg obszarów związanych z egzekwowaniem prawa;
- obszar migracji, udzielania azylu czy kontroli granic – również zawężenie do konkretnych obszarów;
- wymiar sprawiedliwości i procesy demokratyczne – wspieranie w procesie decyzyjnym (np. przy wydawaniu wyroków).

Diabeł tkwi w szczegółach, a właściwie w ich braku. To, z czym musimy się pogodzić, to fakt, że nie ma jasnej i zamkniętej definicji systemu AI wysokiego ryzyka. Można stwierdzić, że jest ona kompilacją art. 6 i art. 7 projektowanego rozporządzenia oraz załącznika III do tego projektu. Projektowane rozporządzenie przyznaje Komisji (UE) prawo do dokonywania zmian w załączniku III. Na szczęście obwarowano to konkretnymi ograniczeniami, KE może bowiem dodać nowe rodzaje systemów klasyfikowanych jako wysokiego ryzyka, jeżeli (łącznie):

1. dany system może nieść ryzyko szkody dla zdrowia lub bezpieczeństwa lub może też mieć negatywny wpływ na realizację praw podstawowych, ale też nie w każdym przypadku, a tylko wtedy, gdy samo ryzyko jest porównywalne z tym, które dostrzegamy w kontekście wspomnianych już systemów z załącznika III;
2. dany system będzie wykorzystywany w obszarach wskazanych w tym załączniku.

Przy tej ocenie Komisja powinna wziąć dodatkowo pod uwagę następujące kryteria:

- zamierzony cel wykorzystania systemu AI;
- prawdopodobieństwo użycia systemu lub fakt jego użycia;
- fakty wskazujące na to, że dany system wcześniej doprowadził do powstania szkody lub istnieją przesłanki, że taka sytuacja może zaistnieć – na bazie stosownej dokumentacji;
- ryzyko dla większej liczby osób – tak ja to rozumiem;
- zależność potencjalnie poszkodowanych osób od wyniku działania systemu – w szczególności czy istnieje opcja rezygnacji z wykorzystania takiego produktu końcowego;
- ocenę, czy potencjalnie poszkodowana osoba jest w nierównej pozycji względem AI ze względu np. na poziom wiedzy czy zależności ekonomiczne;
- ocenę, czy efekt prac systemu jest łatwy do odwrócenia w przypadku pojawienia się szkody;
- stwierdzenie, czy unijne przepisy zapewniają możliwość uzyskania odszkodowania i odpowiednią ochronę w zakresie eliminowania lub minimalizowania ryzyka szkody.

Zmiany te są określane pojęciem *safeguards* i mają stanowić pewnego rodzaju „bezpieczniki" przeciwko nadużyciom w stosowaniu tego prawa. Niemniej kontekst powstawania rozporządzenia może stanowić poważny problem dla branży ochrony.

CO DALEJ?

Wydaje się, że bez uzbrojenia się w transparentnie prezentowaną strategię rozwoju koncepcji *smart city* oraz stworzenia warstwy zarządzania cyberbezpieczeństwem trudno będzie wypracować silną pozycję dla kolejnych etapów rozwoju tych technologii.

Przykład rozwoju koncepcji, jaki w czasach pandemii COVID-19 odegrał pozytywną rolę w poprawie jakości życia obywateli, teraz może zostać przesłonięty niebezpieczeństwami wskazanymi, ale nie do końca jasno zdefiniowanymi. Tutaj jest miejsce dla zorganizowania się branży i uruchomienia kreatywności na polu nie tylko lobbingu, ale zwłaszcza – nomen omen – wypracowania rozwiązań dla własnych produktów mających służyć bezpieczeństwu.

JACEK TYBUREK

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

Bezpieczeństwo w smart city

Jerzy Mikulik

Prof. dr hab. inż.

Rozwój technologii elektronicznych i informatycznych umożliwił najpierw budowę inteligentnych budynków, następnie powstanie koncepcji inteligentnych miast i aglomeracji, a w przyszłości doprowadzi (być może) do powstania inteligentnej planety. Wszystko to ma na celu zapewnienie komfortu pracy i życia w otaczającym nas środowisku.

Piotr Januszewicz

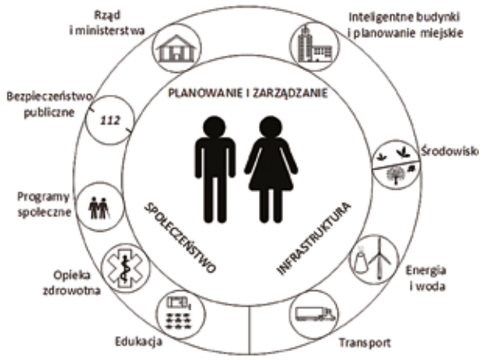
pułkownik rez. WP

Stopień nasycenia obiektów różnego rodzaju systemami jest tak duży, że niezbędna staje się ich integracja i dążenie do obsługi przyjaznej dla użytkownika. Rozwój technologiczny, szczególnie w obszarze mikroelektroniki, urządzeń i sieci mobilnych 4G i 5G, umożliwia odejście od tradycyjnych systemów sterowania funkcjami użytkowymi i korzystania z zasobów informacyjnych. Powstaje kolejna domena zwana Internetem Rzeczy IoT, co sprawia, że przedmioty codziennego użytku, np. pralki, lodówki, a nawet zwykły kubek do kawy mogą stanowić element globalnej wioski. Działania takie niosą jednak zagrożenia mogące się materializować w cyberprzestrzeni. Rozwój cyberprzestępczości, a w niedługim czasie być może realnego cyberterroryzmu sprawia, że te systemy należy projektować w taki sposób, by zapewniały bezpieczeństwo życia i funkcjonowania ludzi. Jest to możliwe tylko wtedy, gdy zostanie zapewnione bezpieczeństwo informacji zawartych w tych systemach.

ZASOBY INFORMACYJNE SMART CITY

W wielu opracowaniach dotyczących koncepcji budowy i funkcjonowania inteligentnych miast zakłada się utworzenie zintegrowanego środowiska obejmującego zasięgiem wszystkie bez wyjątku sfery życia ludzi i funkcjonowania infrastruktury.

Rys. 1. Koncepcja inteligentnego miasta i obszarów funkcjonalnych zarządzania



Źródło: www.smartercomputingblog.com

Na *rys. 1* przedstawiono koncepcję funkcjonowania inteligentnego miasta oraz jego obszary funkcjonalne, które powinny być zarządzane. Można wyróżnić następujące obszary funkcjonalne:

- administracja publiczna i samorządowa,
- planowanie przestrzenne, budownictwo,
- bezpieczeństwo publiczne,
- ochrona środowiska,
- dostęp do energii i wody,
- transport publiczny i indywidualny,
- edukacja,
- ochrona zdrowia,
- aktywność społeczna.

Kompleksowość takiego rozwiązania polega na zarządzaniu w obszarach zarówno infrastruktury, jak i funkcjonowania ludzi. Agregując i odpowiednio analizując – przy wykorzystaniu sztucznej inteligencji – tak potężne zbiory danych, można nie tylko dostarczyć mieszkańcom ważnych dla nich informacji (np. o wolnych miejscach parkingowych, najszybszej drodze do wybranego miejsca, natężeniu ruchu ulicznego itp.), ale także monitorować ich zachowania. To sprawia, że ochrona tych zasobów informacyjnych jest niezwykle istotna. Jak każdy rozwój technologii, można ją wykorzystywać dla pożytku ludzkości albo przeciwko niej. Dysponowanie tak zaawansowanymi technologiami, w razie dostania się informacji wrażliwych w niepowołane ręce, może przyczynić się do stworzenia powszechnego systemu inwigilacji obywateli. Drastycznym przykładem jest jedno z państw, w którym wykorzystywanie informacji z różnych systemów praktycznie wyklucza jakąkolwiek anonimowość lub intymność. Każdy obywatel miasta, w którym wprowadzono taki system, ma tzw. indeks społeczny decydujący o możliwości korzystania np. z transportu publicznego.

ISTOTA ZAPEWNIENIA BEZPIECZEŃSTWA INFORMACJI W INTELIGENTNYCH BUDYNKACH I MIASTACH

Ilość przetwarzanych informacji i ich charakter sprawiają, że właściwie każda dziedzina naszego życia będzie podlegała interakcji z istniejącymi systemami. Uzależnienie to ma bezpośredni związek z bezpieczeństwem obywateli mieszkających i przebywających w takich miastach.
Dokonując analizy potrzeb ludzi, naukowcy potwierdzają znaczenie modelu piramidy potrzeb opracowanej przez amerykańskiego psychologa Abrahama Maslowa. W trakcie badań doszedł on do wniosku, że potrzeby ludzi są uporządkowane hierarchicznie – od podstawowych, jakimi są potrzeby fizjologiczne, po najwyższe, m.in. rozwój osobisty. Oznacza to, że zaspokojenie potrzeb jest realizowane od najważniejszych, leżących u podstawy piramidy, do mniej ważnych, ale istotnych, położonych w kierunku jej szczytu. Z piramidy potrzeb wynika, że najważniejsze jest zaspokojenie potrzeb fizjologicznych, ale tuż po nich są potrzeby bezpieczeństwa (zdrowia, życia, bezpieczeństwa socjalnego itp.). Na tej podstawie można wyciągnąć wniosek, że również oczekiwania w stosunku do inteligentnych budynków i miast będą się koncentrowały wokół bezpieczeństwa. Można też domniemywać, że ludzie poświęcą inne usługi ułatwiające życie, jeśli będą one stały w sprzeczności z zachowaniem bezpieczeństwa.

LUDZIE BĘDĄ CHCIELI MIESZKAĆ W INTELIGENTNYCH MIASTACH POD WARUNKIEM ZAPEWNIENIA IM BEZPIECZEŃSTWA

Bezpieczeństwo natomiast będzie można osiągnąć jedynie w przypadku zapewnienia bezpieczeństwa informacji przetwarzanych w ramach inteligentnych miast.

GŁÓWNE ZAGROŻENIA DLA INFORMACJI W INTELIGENTNYCH BUDYNKACH I MIASTACH

Potrzeba zapewnienia bezpieczeństwa jest wynikiem potencjalnych zagrożeń mogących materializować się wobec infrastruktury i ludzi. Zbiór ten jest oczywiście ogromny i sam w sobie może stanowić oddzielne opracowanie. Podziału dokonano z uwzględnieniem osób i organizacji, które mogą być zainteresowane atakiem na tego typu obiekty. Przyjęto następującą klasyfikację:

1. Organizacje terrorystyczne

Szczególne natężenie w ostatnim dziesięcioleciu działalności terrorystycznej na całym świecie stało się faktem. Organizacje terrorystyczne wykorzystują głównie konwencjonalne kinetyczne środki rażenia: materiały wybuchowe, broń strzelecką. Coraz częściej jednak mamy do czynienia z oddziaływaniem nie kinetycznym, ale polegającym na operacjach psychologicznych z wykorzystaniem mediów internetowych, agitacji, zastraszania (np. pokaz egzekucji jeńców). Można się więc spodziewać, że inteligentne miasta i obiekty będą celem działań tych organizacji, gdyby okazało się, że za pomocą ataków cybernetycznych można wywołać podobne skutki, jak w przypadku ataków kinetycznych. Biorąc pod uwagę fakt automatyzacji funkcji „życiowych" inteligentnych miast, zdarzenia takie mogą się już zmaterializować. Może się okazać, że w niedalekiej przyszłości zagrożenie to stanie się głównym wektorem ataków na infrastrukturę inteligentnych miast i budynków.

2. Hakerzy

Wszelkie formy działań złośliwych wobec systemów teleinformatycznych uważa się za hakerską. Parających się nią można podzielić na dwie podstawowe grupy: hakerzy zawodowi i amatorzy. Do pierwszej należą wysoko wykwalifikowani specjaliści, którzy „zawodowo" prowadzą tego typu działalność. Drugą grupę stanowią amatorzy – ich motywy działania są różne, a skutki oddziaływania czasami nieprzewidywalne. Pierwszą grupę interesują przede wszystkim działania związane z atakami na systemy, głównie bankowe lub handlu elektronicznego, w celu uzyskania korzyści materialnych. W przypadku tego procederu niezbędne są informacje pozyskane np. z mediów społecznościowych czy zasobów państwowych. To tzw. biały wywiad. Inteligentne miasta oferują wszystkie wymienione tu usługi, zatem zapewne staną się celem działań hakerów.
Hakerzy amatorzy atakują bez przemyślenia i strategii, a koncentrują się bardziej na efektach. Ich działania będą więc skierowane na wszystkie elementy infrastruktury miasta i zasobów informacyjnych. Spowodowane przez nich szkody często są większe niż wyrządzone przez hakerów zawodowych, a i walka z nimi jest trudniejsza, ponieważ celem są wszystkie zasoby bez względu na ich krytyczność. Motywem ich działania jest bardziej satysfakcja z pokonania zabezpieczeń niż cel materialny. Biorąc pod uwagę statystyki i rozwój aktywności pojedynczych hakerów i ich grup, zapewne swoją działalność przeniosą na wszystkie elementy decydujące o funkcjonowaniu tych organizacji miejskich.

3. Operacje militarne

Działania militarne mają na celu zdobycie przewagi nad przeciwnikiem i w efekcie osiągnięcie zamierzonych celów, które mogą być różne. Do ich realizacji wykorzystuje się wszystkie prawem dozwolone i dostępne środki oddziaływania, od kinetycznych, poprzez operacje psychologiczne, ekonomiczne itp. Jednym z obszarów zainteresowania sił zbrojnych na całym świecie są działania w cyberprzestrzeni, a inteligentne miasta stanowią jej część. Celem działań militarnych jest paraliż infrastruktury krytycznej przeciwnika oraz osłabienie jego morale przez utratę poczucia bezpieczeństwa obywateli. Można to osiągnąć, oddziałując za pomocą ataków cybernetycznych na inteligentne miasto. Arsenał środków dostępnych dla sił zbrojnych na świecie jest zapewne ogromny, a co za tym idzie stanowi potężne wyzwanie dla obrońców takiego miasta. Przygotowanie systemów na tego typu zagrożenia jest trudne i kosztowne, ale również należy brać je pod uwagę.

ANALIZA MODELI FUNKCJONALNYCH W ASPEKCIE ZAPEWNIENIA BEZPIECZEŃSTWA INFORMACJI

Wyróżniamy kilka typów architektury systemów bezpieczeństwa możliwych do zastosowania przy budowie inteligentnego miasta. Najprostsza jest architektura przedstawiona na *rys. 2,* z sieciami metropolitalnymi i jednym lub dwoma centrami przetwarzania danych. Można w niej wyodrębnić mnogość różnorodnych technologii komunikacji zarówno przewodowych, jak i bezprzewodowych. Zasoby informacyjne takiej metropolii są olbrzymie pod względem ilościowym i różnorodności treści. Można wskazać następujące jej zalety i wady w kontekście bezpieczeństwa i kosztów.

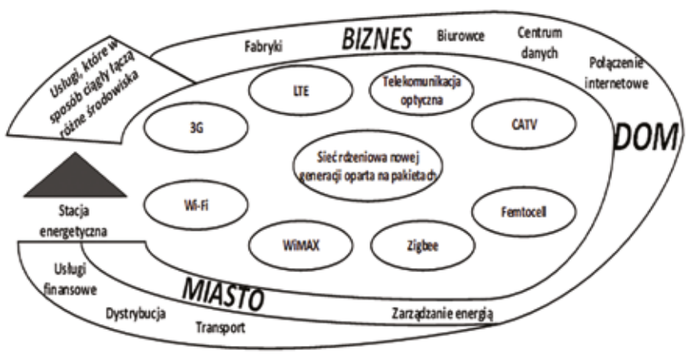
Zalety

- relatywnie niskie koszty budowy (jedno lub dwa centra przetwarzania danych),
- optymalizacja kosztów utrzymania (technologie, ludzie, obiekty),
- łatwość integracji usług,
- łatwość zarządzania na najwyższym poziomie pod względem zarówno bezpieczeństwa informacji, jak i niezawodności eksploatacji.

Wady

- pojedyncze punkty krytyczne (centrum przetwarzania danych),
- trudność w zapewnieniu bezpieczeństwa na poziomie transmisji (różne technologie),
- najczęściej homogeniczna architektura głównych węzłów, co ułatwia wykorzystanie jednej podatności do ataku na wiele zasobów informacyjnych.

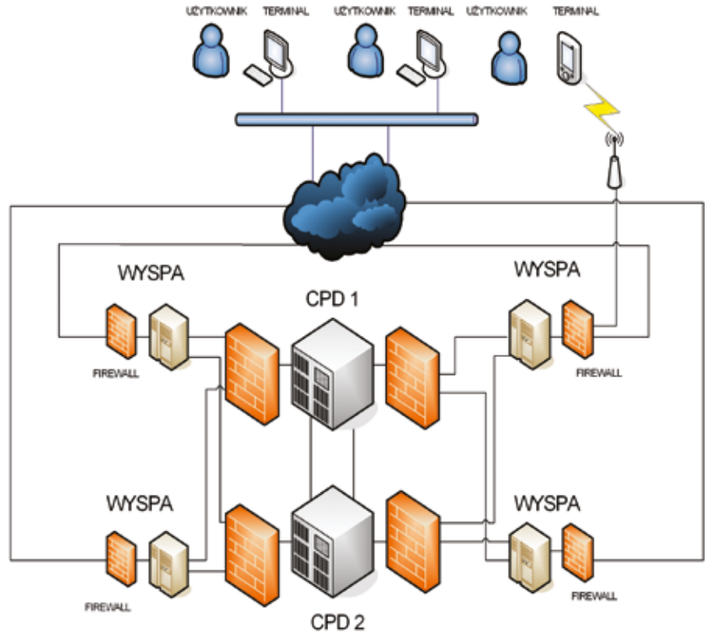
Rys. 2. Architektura systemów inteligentnego miasta



Źródło: www.smartcitiesoftomorrow.com

Przedstawiona koncepcja jest tradycyjnym podejściem do budowy architektury systemów zorientowanych na świadczenie usług *Services Oriented Architecture* (SOA). Zakłada się w niej koncentrację na zdolnościach do integracji różnorodnych platform programowych i sprzętowych w celu świadczenia usług. W tego typu architekturze stosunkowo trudno jest zaimplementować skuteczne środki ochrony. Przyczyną tego stanu jest budowa infrastruktury, która ogranicza lub wręcz uniemożliwia aktywne przeciwdziałanie np. atakom hakerskim, ponieważ nie są zdefiniowane i wyodrębnione obszary poszczególnych usług, a o separacji infrastruktury teletransmisyjnej praktycznie nikt nie myśli. Utworzenie w takim środowisku centrum zajmującego się bezpieczeństwem sieci systemów *Security Operating Center* (SOC) sprawi, że skuteczność jego działania będzie ograniczona ze względu na przedstawione wyżej problemy architektury zasobów. Autorzy artykułu proponują koncepcję architektury systemów zorientowaną na bezpieczeństwo i usługi *Security and Services Oriented Architecture* (SaSOA). Koncepcja ta przewiduje budowę systemów jako zbiór „wysp" (architektura rozproszona z georedundancją) poszczególnych usług, co pokazano na *rys. 3.* Zakłada odseparowanie logiczne (wydzielone kanały komunikacji) lub nawet fizyczne (w zależności od analizy ryzyka) poszczególnych usług i systemów w taki sposób, by w razie ataku na jedną wyspę można było „odłączyć" od niej pozostałe. Pozwala to zmniejszyć ryzyko ataku na pozostałe wyspy oraz dać szansę zespołom bezpieczeństwa w SOC na podjęcie skutecznych środków przeciwdziałania. Takie rozwiązanie ogranicza w trakcie ataku poziom świadczonych usług w zależności od jego siły, umożliwia natomiast zachowanie poprawnego funkcjonowania pozostałych usług oraz przygotowanie ich na znany wektor ataku.
Filozofia takiego rozwiązania jest skutecznie stosowana w walce z epidemiami, kiedy wyznacza się określone kanały przepływu ludzi i miejsca kwarantanny oraz izoluje zainfekowane jednostki. Analogiczna sytuacja występuje w budowie systemów teleinformatycznych inteligentnego miasta, których architektura musi zakładać ograniczoną liczbę łączy dla poszczególnych wysp usług oraz umożliwiać fizyczną izolację wysp lub poszczególnych usług. W stosunku do zasobów, co do których istnieje duże prawdopodobieństwo infekcji złośliwym oprogramowaniem albo istnieniem podatności krytycznej lub ciężkiej dla tej usługi, musi umożliwiać jej izolację i poddanie kwarantannie.

Rys. 3. Architektura systemów zorientowana na bezpieczeństwo i usługi SaSOA



Źródło: opracowanie własne

PODSUMOWANIE

Mając na względzie zapewnienie kompleksowego bezpieczeństwa informacji przy budowie inteligentnych miast usługi cyberbepieczeństwa będą musiały:

- uwzględniać przepisy prawa w zakresie ochrony zasobów informacyjnych prawem chronionych (dane osobowe, informacje medyczne, bankowe, informacje niejawne prawa autorskie itp.),
- uwzględniać przepisy o bezpieczeństwie powszechnym i ludności,
- uwzględniać przepisy w zakresie zarządzania kryzysowego,
- uwzględniać prawo telekomunikacyjne,
- posiadać architekturę systemów zorientowaną na bezpieczeństwo i usługi ***Security and Services Oriented Architecture*** (SaSOA),
- być budowane z uwzględnieniem najlepszych praktyk w dziedzinie bezpieczeństwa informacji.

PŁK REZ. PIOTR JANUSZEWICZ

Absolwent PW (Wydziału Elektroniki i Technik Informacyjnych) oraz Studiów Podyplomowych na Wydziale Cybernetyki WAT. Rzeczoznawca w zakresie Technicznej Ochrony Mienia. Współtwórca i pierwszy Szef Centrum Bezpieczeństwa Cybernetycznego SZ (obecnie Centrum Operacji Cybernetycznych). Były dyr. Departamentu Cyberbezpieczeństwa Ministerstwa Cyfryzacji odpowiedzialny za opracowanie Strategii Cyberbezpieczeństwa Państwa oraz Ustawy o Krajowym Systemie Cyberbezpieczeństwa.

PROF. DR HAB. INŻ. JERZY MIKULIK

Profesor tytularny na Wydziale Zarządzania AGH w Krakowie. Od kilkunastu lat zajmuje się tematyką inteligentnych budynków i miast, a w szczególności zarządzaniem i sterowaniem bezpieczeństwem oraz komfortem fizycznym w dużych obiektach. Kierownik studiów podyplomowych „Cyberbezpieczeństwo i zarządzanie bezpieczeństwem informacji" oraz „Facility management – zarządzanie inteligentnym budynkiem".

Smart City 2021

7 trendów w rozwoju inteligentnych miast

Zainteresowanie rozwiązaniami *smart city* dynamicznie rośnie w związku z postępującą urbanizacją, a także cyfryzacją coraz liczniejszych aspektów życia mieszkańców. Rodzi to wiele nowych wyzwań, stąd zapotrzebowanie na inteligentne rozwiązania, m.in. w obszarach bezpieczeństwa publicznego, mobilności miejskiej czy monitoringu środowiska. W jaki sposób innowacje technologiczne mogą wpłynąć na przyszłość inteligentnych miast? Konrad Badowski, ekspert Axis Communications, przedstawia najważniejsze trendy w rozwoju *smart city*, które mogą najsilniej oddziaływać na nasze aglomeracje w 2021 r.

1

POWSZECHNOŚĆ 5G

Technologia 5G od lat budzi ogromne zainteresowanie, jednak ostatnio jej wdrożenia wyraźnie przyspieszyły. Wkrótce sieci 5G mogą na dobre zadomowić się w miastach i znacznie zwiększyć tempo ich cyfrowej transformacji. Sieci komórkowe nowej generacji zdynamizują ewolucję takich technologii, jak IoT, głębokie uczenie w urządzeniach na brzegu sieci czy szczegółowa analiza danych. Kompatybilność ze znacznie większą liczbą urządzeń 5G pozwoli miastom gromadzić więcej informacji i analizować dane w czasie rzeczywistym, co wpłynie m.in. na efektywność w obszarach bezpieczeństwa publicznego czy mobilności miejskiej.
Przykładem mogą być tzw. inteligentne słupy z zamontowanymi różnymi czujnikami, które dbają o bezpieczeństwo, mierzą jakość powietrza, wspierają zarządzanie parkowaniem itp. Takie rozwiązania są dowodem dla władz miasta, że sieć 5G jest czymś niezbędnym dla prawdziwego *smart city*.

2

POTRZEBA OCHRONY DANYCH

Wraz z popularnością technologii *smart city* rośnie ilość zbieranych danych. Poniekąd przyzwyczailiśmy się już do obecności kamer wspierających bezpieczeństwo w przestrzeni publicznej. Trudno więc dziwić się coraz większym obawom społecznym w kwestii ochrony danych. Uchwalane na całym świecie nowe przepisy z zakresu bezpieczeństwa danych, np. RODO, już sprawiają, że zarówno organy regulacyjne, jak i obywatele uważnie przyglądają się temu, jak przetwarza się, wykorzystuje i chroni dane osobowe.
Miasta wdrażające inteligentne technologie będą zatem musiały spełniać rosnące oczekiwania w zakresie lepszego zabezpieczenia informacji o mieszkańcach, np. stawiając na rozwiązania pozwalające na obrazie automatycznie maskować wizerunek osób przed kamerą.

3

WALKA Z CYBERPRZESTĘPCAMI

Wzmagająca się cyberprzestępczość zmusza miasta do bliższego przyjrzenia się sposobom ochrony miejskich systemów. Ataki cyberprzestępców na firmy i instytucje nieustannie pokazują, że lokalne władze muszą z większą uwagą podejść do kwestii zabezpieczeń cybernetycznych. W wielu miejscach jeszcze nie opracowano planów działań określających sposób reakcji w razie cyberataku na miejskie usługi i infrastrukturę. Tymczasem atak wiążący się z kradzieżą danych może mieć katastrofalne konsekwencje. W przyszłości łagodzenie skutków takich zagrożeń będzie jednym z głównych priorytetów władz miast prawdziwie *smart*.

4

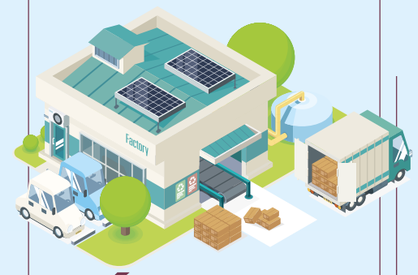
CORAZ BLIŻEJ BRZEGU

Postępująca cyfryzacja miast wzmaga potrzebę przechowywania i analizowania danych zebranych na brzegu sieci, czyli tam, gdzie umiejscowione są czujniki, kamery i inne inteligentne urządzenia. Władze miast już dostrzegły liczne korzyści płynące z takich pogłębionych analiz i chętnie wdrażają nowoczesne rozwiązania z zakresu zarządzania ruchem drogowym, sterowania oświetleniem czy ochrony przeciwpowodziowej. W 2021 roku i kolejnych latach ten trend będzie się nasilał, a podmioty zarówno publiczne, jak i prywatne będą coraz częściej stawiać na systemy, które przetwarzają na brzegu sieci, tym samym zwiększając efektywność inteligentnego miasta.

5

MIEJSKA MOBILNOŚĆ

Wraz ze wzrostem zaludnienia miast rośnie także liczba pojazdów na ulicach. Często katalizatorem dla wdrażania technologii *smart city* jest chęć przezwyciężenia wyzwań związanych właśnie z mobilnością miejską. Tradycyjne metody transportu publicznego, m.in. autobusy, tramwaje czy metro, muszą w ostatnich latach konkurować z nowymi przewoźnikami, takimi jak Uber, oraz mikromobilnością korzystającą z rowerów czy hulajnóg. Władze miast obserwują, że nowi przewoźnicy i nowe środki transportu mimo rosnącej popularności jeszcze wzmagają ruch w centrum, zamiast go rozładowywać.
Samorządy stoją więc przed coraz większymi problemami. W ich rozwiązaniu pomocne będą zautomatyzowane systemy wspierające parkowanie, a także kamery zintegrowane z sygnalizacją świetlną, które pozwolą rozładować ruch w godzinach szczytu.



6

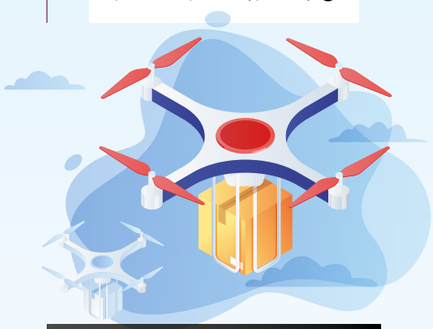
REAKCJA NA ZMIANY KLIMATU

Zmiany klimatu należą do priorytetowych wyzwań, przed którymi stoją dzisiejsze miasta. Wzrost średniej temperatury, ekstremalne zjawiska pogodowe, gwałtowne wezbrania rzek i kurczące się zasoby wód gruntowych w niespotykanym dotąd stopniu odbijają się na obszarach zurbanizowanych. Miasta wręcz uginają się pod ciężarem zanieczyszczania atmosfery, a dotychczasowe mechanizmy ich funkcjonowania są w dłuższej perspektywie nie do utrzymania.
Prawdziwe *smart city* wyznaczają sobie zdecydowanie bardziej ekologiczne cele, chcąc ograniczyć oddziaływanie miasta na środowisko, oraz wdrażają technologie służące do monitorowania zanieczyszczeń i wpływu ekstremalnych czynników pogodowych. Aby sprostać konsekwencjom zmian klimatu, miasta muszą postawić na inteligentne rozwiązania, takie jak analiza i poprawa jakości powietrza, optymalizacja zużycia energii, monitorowanie poziomu wody czy zarządzanie odpadami. Włodarzy miejskich powinny interesować nie tyle rozwiązania IoT, ile „ekologiczny Internet Rzeczy", który wesprze ochronę środowiska i prowadzenie zrównoważonego dozoru.

7

INTELIGENTNE MIASTO PO-COVID-OWE

Pandemia COVID-19 zmieniła priorytety planistów miast, zmusiła wszystkich do ponownego przemyślenia i zrewidowania wielu aspektów życia codziennego. Pojawiły się i są już stosowane inteligentne rozwiązania hamujące rozprzestrzenianie się wirusa. Popularne stały się systemy zdalnego monitorowania temperatury, mechanizmy śledzenia zbiorowisk ludzkich w czasie rzeczywistym czy zintegrowane z inteligentnymi kamerami głośniki, automatycznie emitujące komunikaty przypominające o konieczności zachowania bezpiecznego dystansu.
Władze miast już powinny myśleć o wdrażaniu inteligentnych systemów, które pozwolą przygotować się także na ewentualną, kolejną pandemię, a może wręcz jej zapobiec. W najbliższych miesiącach i latach pierwszorzędne znaczenie zyskają przede wszystkim rozwiązania z zakresu mobilności świadczenia niezbędnych usług, np. telemedycznych, czy też zamówień produktów pierwszej potrzeby.



Smart city, safe city – ten rynek z pewnością jest przyszłościowy, biorąc choćby pod uwagę trendy migracyjne sprzed pandemii, wg których do 2050 r. miasta miały być głównym miejscem zamieszkania powiększającej się liczby mieszkańców naszego globu. Co ciekawe, przewidywania uległy obecnie pewnym korektom, gdyż wiele osób szuka swojego miejsca na Ziemi niekoniecznie w zatłoczonych centrach miast, a właśnie w oddalonych od szumu aglomeracji lokalizacjach wiejskich. Co zatem dla branży security może przynieść ta zmiana?

Wycieczka za miasto

o aspektach systemów smart nie tylko w miastach

Michał Marciniak

Wielkomiejskie rozwiązania *smart city* charakteryzują się najczęściej ogromną kumulacją usług i serwisów na niewielkiej przestrzeni. To nie tylko szybki Internet, sieci 5G, ale również inne inteligentne usługi (np. VOD, wirtualne centrale telefoniczne IP itd.), a także mocno rozwijana koncepcja *smart building,* z jej szlagierem w postaci nadzoru czy też zdalnej kontroli nad własnym domem, mieszkaniem czy biurem (temperatura, kamery, sterowanie urządzeniami). Ale to nie koniec tej listy – bezpieczeństwo stanowi kolejny aspekt, który jednoznacznie wyznacza nowy kierunek związany z *safe city.* Policyjne patrole wyposażone w mobilne kamery, które przekazują obraz do centrali, systemy audio wykrywające potencjalnie groźne dźwięki (strzały, krzyki, wybuchy), kamery lub lidary analizujące zachowania osób i przekazujące do stanowisk operatorów monitorujących podejrzane zdarzenia. Wszystko to – łącznie z systemami drogowymi (inteligentne światła, przejścia dla pieszych) i inteligentnie zarządzaną infrastrukturą transportu miejskiego (przystanki z interaktywną informacją dla pasażerów) – stanowi podstawę, która definiuje pokrótce koncepcję *smart city.*

Czego zatem szukamy poza miastem? Czy trzeba przenosić wielkomiejskie trendy również na obszary mniej zurbanizowane? A może wystarczy modyfikacja lub dostosowanie pewnych rozwiązań, aby spełniały swoje zadanie i twoje potrzeby również w innym środowisku?

Zacznijmy od ograniczeń. Im bliżej „dzikiej natury", tym większa bariera komunikacyjna. Każdy z nas zna ten problem – wyjazd nad jezioro czy do lasu często wiąże się z brakiem zasięgu w telefonie lub modemie. Z punktu widzenia spędzania beztroskiego weekendu ma to sens, ale w przypadku prowadzenia tam biznesu i konieczności zachowania ciągłości nadzoru nad np. infrastrukturą urządzeń, sensorów z obszaru IoT może to być czynnik krytyczny. Kolejnym ograniczeniem jest skala (czy też liczba) wspomnianych urządzeń – nadzór nad stanem wód w rzekach wymaga wielu sensorów rozmieszczonych w różnych punktach koryta rzecznego. Ilość i obszar są tutaj czynnikiem ograniczającym zastosowanie tylko w bardzo rzadkich przypadkach. Częstą przypadłością są przerwy w zasilaniu, co w realiach miejskich jest wręcz nie do pomyślenia. Praktycznie każda miejscowość w Polsce ma dostęp do zasobów energetycznych, jednak jakość tej usługi często pozostawia wiele do życzenia (np. częste i nieplanowane przerwy w dostawach).

Znamy już ograniczenia. Czy zatem można (i czy w ogóle jest sens) korzystać na wsi z dobrodziejstw, jakie oferują inteligentne rozwiązania stworzone dla miast? Zdecydowanie tak, lecz adaptując je do naszych potrzeb. Przykładem mogą być autonomiczne systemy koszenia zbóż lub zbierania plonów rolnych. Pojazdy (traktory) wyposażone m.in. w lokalizatory GPS, systemy kamer czy czujniki położenia efektywnie i bezobsługowo zbiorą plony w najkrótszym możliwym czasie, poruszając się po optymalnie dobranej trasie. Jeśli do tego zastosować rozwiązania zeroemisyjne (pojazdy elektryczne ładowane z systemów solarno-wiatrowych) oraz drony pozwalające na zdalny nadzór wizyjny, mamy pierwszy przykład doskonale użytej inteligentnej technologii w służbie rolnictwa. To nie koniec przykładów z tego obszaru. Farmy, szklarnie czy stodoły korzystają z całej gamy czujników (wilgotność, opady deszczu, temperatura, kwasowość itd.) generujących ogromne ilości danych, które są poddawane analizie i obróbce.

I tutaj przechodzimy do kolejnej kwestii związanej z obsługą tych danych. Obecnie można wyróżnić trzy najpopularniejsze modele przetwarzania: lokalny *(on-site)*, chmurowy i hybrydowy *(on-site + cloud).* Przetwarzając dane lokalnie, wykorzystujemy zasoby serwerowe do przechowywania i pracy nad danymi spływającymi z czujników lub kamer – czynnikiem zaporowym może być konieczność jednorazowego zakupu niezbędnych (często drogich) komponentów serwerowo-sieciowych. Podejście chmurowe gwarantuje nieograniczoną moc i przestrzeń (i tym samym nie wymaga inwestycji w infrastrukturę lokalną), ale wiąże się z koniecznością stałego dostępu do Internetu. Rozwiązanie hybrydowe stanowi pomost pomiędzy dwoma rozwiązaniami – dane mogą być zbierane i wstępnie przetwarzane przez system lokalny, pełna analiza i archiwizacja zaś byłyby wykonywane na poziomie chmury publicznej. Z punktu widzenia łączy internetowych, często niestabilnych i o niskiej przepustowości, proste lokalne repozytorium stanowi bufor i wstępny filtr ogromnej ilości danych, które w skondensowanej postaci trafiają do docelowej bazy w chmurze. Ten model wydaje się obecnie najdoskonalszy i pozwala pokonać ograniczenia technologiczne, zapewniając dostęp do nowoczesnych rozwiązań nawet w oddalonych gospodarstwach.

Farmy fotowoltaiczne i inne obiekty wymagające ciągłego dozoru wizyjnego (ochrona obwodowa, ochrona mienia) są wyzwaniem dla instalatorów ze względu na zdecydowanie większe dystanse, niż ma to miejsce w mia-

stach. W tym przypadku klasyczne połączenia skrętką czteroparową w technologii PoE przy zasięgu 100 m jest kroplą w morzu potrzeb. Odległości do obiektów niejednokrotnie liczone są w kilometrach, więc jedyną opcją jest zastosowanie jednego z trzech głównych rozwiązań: światłowód, Wi-Fi, 3G/4G (o ile jest zasięg). Pierwsze dwa pozwalają na dość swobodne przesyłanie danych, choć praktyka pokazuje, że na dłuższą metę światłowód jest trwalszy i bardziej wydajny niż rozwiązania Wi-Fi (każda dodatkowa kamera dokładana po jakimś czasie powoduje spadek wydajności punktów bezprzewodowych). Punkty Wi-Fi są prostsze w implementacji, ale stabilność i wspomniane już ograniczenia przepustowości oraz wpływ warunków środowiskowych (deszcz, śnieg) sprawiają, że decydujemy się na nie tylko wówczas, gdy instalacja światłowodu jest technicznie niemożliwa. Ostatni wariant – 3G/4G – jest wygodny, ale stanowi wyzwanie pod względem zasięgu i przepustowości. Zasięg samego połączenia można poprawić, stosując kierunkowe anteny o wysokim zysku (dB). Należy przy tym pamiętać o ograniczeniach transferu i danych, jakie najczęściej mają w swoich ofertach dostawcy komórkowi. Warto zatem sprawdzić (zasymulować), ile danych planujemy wysyłać miesięcznie, i przyjąć bezpieczny margines.

Jak zatem zagwarantować działanie tych inteligentnych urządzeń brzegowych w trybie ciągłym, skoro mają one być zainstalowane z dala od jakiejkolwiek infrastruktury energetycznej? Należy dokładnie zbadać planowaną lokalizację: czy teren jest osłonięty, czy nasłoneczniony w ciągu dnia, ile jest statystycznie dni słonecznych w roku, czy często wieje, czy raczej wiatr jest rzadkością, jaki jest dojazd do punktu i czy wymagane są specjalne pozwolenia. Wszystko to ma wpływ na wdrożenie. Najciekawszym (ponownie) rozwiązaniem jest hybryda: zestaw solarno-wiatrowy wraz z akumulatorem o poprawnie dobranej pojemności może stanowić całoroczny element zasilania oddalonej infrastruktury. System monitorowania pojemności i ładowania oraz poprawności działania komponentów jest tutaj kluczowy, a możliwość okresowej kontroli i konserwacji bezpośrednio wpływa na stabilność i sprawność działania całego rozwiązania.
Miasta stanowią zaczątek dla nowych inteligentnych technologii, które później można dostosować i przemodelować na potrzeby innych obszarów i wymagań. Możliwość ich zastosowania i czerpania korzyści wymaga jednak poszukiwania kompromisów i alternatyw, które w zatłoczonych miastach nie stanowią problemu. Dzisiaj wielu producentów urządzeń brzegowych zaczyna zauważać i pilnie analizować potrzeby nie tylko obszarów miejskich, ale również na prowincji. Energooszczędne kamery z 4G dostępne wraz z zestawami solarnymi, switche, mediakonwertery i inne urządzenia aktywne dostępne w wariantach przemysłowych (odporne na kurz i ekstremalne zmiany temperatury) to tylko część oferty. Czujniki BLE (*Bluetooth Low Energy*) wraz z GPS współpracujące z bramą (*gateway*) zainstalowaną np. na farmie przekazują lokalizację zwierząt, obiektów mechanicznych itd. Pozwala to na usprawnienie kanałów komunikacji, badanie zachowań czy wyznaczanie optymalnych tras, poprawiając ogólną wydajność całego gospodarstwa.

Dzisiejsze *smart city* i *safe city* to nieodłączne atrybuty każdej większej aglomeracji, ale również coraz częściej mniejszych miast i miasteczek. Kolejne generacje inteligentnych urządzeń są coraz prostsze w użyciu i wdrożeniu, a jednocześnie ich ceny spadają. Co ważne – kwestie ekologii, takie jak produkcja z materiałów pochodzących z recyklingu czy zmniejszanie zapotrzebowania na energię elektryczną, stanowią podstawę rozwoju tego obszaru. Wypłynięcie na szerokie wody i wdrażanie rozwiązań *smart* poza technologicznie bezpieczną infrastrukturą miejską stanowi duże wyzwanie, ale nie jest niemożliwe. Na ogół odpowiednie dostosowanie strategii może zaowocować ciekawym i nowatorskim wdrożeniem.

MIASTA STANOWIĄ ZACZĄTEK DLA NOWYCH INTELIGENTNYCH TECHNOLOGII, KTÓRE PÓŹNIEJ MOŻNA DOSTOSOWAĆ I PRZEMODELOWAĆ NA POTRZEBY INNYCH OBSZARÓW I WYMAGAŃ. MOŻLIWOŚĆ ICH ZASTOSOWANIA WYMAGA JEDNAK POSZUKIWANIA KOMPROMISÓW

MICHAŁ MARCINIAK

Architekt rozwiązań CCTV, twórca i autor bloga www.10cctv.pl; od 20 lat w branży IT i security – promotor, wdrożeniowiec i pasjonat nowych technologii z pogranicza monitoringu wizyjnego oraz IT.

JAK W DOBIE PANDEMII ZAPEWNIĆ BEZPIECZEŃSTWO MIESZKAŃCOM MIAST, PRACOWNIKOM BIUROWCÓW CZY CHORYM W SZPITALACH? GŁOS ZABIERAJĄ PRZEDSTAWICIELE RÓŻNYCH SEKTORÓW GOSPODARKI.

Głos branży

Leszek Lawera

specjalista ds. wdrażania nowych technologii

Co dała nam pandemia

Ten rok mocno ostudził mój inżynierski entuzjazm. Okazało się, że świat czy też organizacje i przedsiębiorcy poradzili sobie bez zaawansowanych technologii, stosując dużo prostsze rozwiązania.

Pomiar temperatury

Bramki z kamerami termowizyjnymi, które rok temu wydawały się gotowym rozwiązaniem i kupi je prawie każda instytucja, zostały zastąpione ręcznym zdalnym pomiarem temperatury wprawdzie wolniejszym, ale równie skutecznym.

Analityka wideo – automatyczna analiza online streamingu z kamer

Wydawało się, że obostrzenia dotyczące zachowywania odległości w sklepach wielkoprzemysłowych i przy kasach będą impulsem do zakupu systemów lub usług alarmujących przekroczenie bezpiecznych limitów odległości czy też liczby osób na danej powierzchni. Sklepy wielkopowierzchniowe, urzędy, szpitale i inne instytucje zadbały o proste procedury, które były nastawione głównie na bezpieczeństwo prawne tych organizacji. W miejscach, gdzie tworzą się kolejki, oklejono posadzki kółkami, liniami w odstępie 1,5–2 m i wystarczy. Czy ludzie się do tego stosują? To już zupełnie inna sprawa i ich ryzyko. Właściwie słusznie!

A teraz bardziej optymistycznie.

Aplikacje na telefon i automatyka (czujniki i sensory) – przyszłość przed nami

W Polsce z pewnym opóźnieniem, ale została wprowadzona tylko jedna aplikacja rządowa związana z obowiązkową kwarantanną. Są też inne, np. aplikacja firmy kurierskiej umożliwiająca otwarcie paczkomatu bez dotykania jakichkolwiek powierzchni. Kolejnym przykładem jest aplikacja jednej z dużych znanych prywatnych przychodni lekarskich, która nie rezygnując z kontroli na wejściu, rozsyła ankiety w formie linku przed umówioną wizytą.

Kierunek będzie dalej eksploatowany w takich miejscach, jak windy, wejścia czy środki komunikacji zbiorowej. Kody QR, znaczniki RFID, bramki Wi-Fi oraz Bluetooth, w połączeniu z technologią typu MESH, na razie dedykowane do wąskiej grupy automatyków, powoli, ale nieuchronnie znajdą zastosowanie również w security.

Bezdotykowe windy, autoryzowane wejścia, cyfrowe paszporty szczepienia, systemy inteligentnej wentylacji, systemy wykorzystujące wirtualną rzeczywistość do sterowania i zarządzania produkcją, drony i sztuczna inteligencja, rozpoznawanie obrazów itp. już w tej chwili nie są utopią. Przyszłość zależy od ceny i poziomu zagrożenia.

Cyberbezpieczeństwo przede wszystkim

Ten obszar dynamicznie rozwijający się jeszcze przed pandemią wraz z szybkim wzrostem udziału pracy zdalnej nabrał szczególnego znaczenia. Bezpieczeństwo danych, urządzeń i produkcji – ale to osobna informatyczna historia i wiele różnych specjalistycznych narzędzi.

Rafał Batkowski

były komendant wojewódzki mazowieckiej i wielkopolskiej Policji

Bezpieczne miasta w pandemii?

Bezpieczeństwo miasta, poza aspektami zarządzania infrastrukturą, dotyczy przede wszystkim ludzi. Dlatego kluczowym aspektem oceny jakości życia, przedmiotem starań władz samorządowych i policji jest właśnie zapewnienie poczucia bezpieczeństwa mieszkańcom. Próbując krótko odnieść się do 2020 r. i zmienionego przez pandemię środowiska bezpieczeństwa, zauważmy dobrą kontrolę przestępczości wskazaną w policyjnych opracowaniach.

W minionym roku odnotowano 701 714 przestępstw ogółem, przy wysokim poziomie wykrywalności 73,9%. Duże miasta zwykle są najbardziej zagrożone – to będzie stałe wyzwanie, w tym dla przedsiębiorców z branży ochrony. Najbardziej zagrożone wydają się Katowice – wskaźnik zagrożenia przestępczością na 100 tys. mieszkańców o wartości 3454; Wrocław – 2951; Poznań – 2647; Warszawa – 2632; Gdańsk – 2564; Kraków – 2383 i dla przykładu Rzeszów – 1754. Spadek przestępczości o 7,7% w stosunku do 2019 r. to bardzo dobry prognostyk, mimo że niepewny, gdyż badany okres to czas ograniczeń epidemicznych, ale i inne obszary aktywności sprawców wymuszone sytuacją, głównie cyberprzestępczość.

CERT Polska już w 2019 r. zarejestrował rekordową liczbę 6484 incydenty w cyberprzestrzeni, która oznacza wzrost rok do roku aż o 73 proc. Spośród typów ataku phishing stanowił ok. 54,2 proc. wszystkich incydentów, złośliwe oprogramowania ok. 14,9 proc., a incydenty z kategorii „obraźliwe i nielegalne treści" (w tym spam) ok. 12,1 proc. wszystkich zarejestrowanych ataków. Pełnych danych za rok 2020 jeszcze nie znamy, ale poprawy sytuacji nie należy się spodziewać.

Wobec powyższego branża security powinna podążać za trendami zagrożeń i oferować adekwatne usługi – poszukiwać nowych form działań ochronnych dostosowanych do oczekiwań klientów. Spodziewajmy się większego wykorzystania w branży: fotogrametrii i analizy danych pozyskanych przez drony z powietrza, inteligentnego zarządzania infrastrukturą miejską z wykorzystaniem funkcji ochronnych – przyspieszenie implementacji rozwiązań smart city/safe city, subskrybowanych powszechnych rozwiązań chmurowych, które pozwolą niemal każdemu korzystać z zaawansowanych narzędzi ITC, elastycznych form zarządzania zasobami, a także szerszego zastępowania i uzupełniania pracy ludzkiej technologią wykorzystującą uczenie maszynowe machine learning, sztuczną inteligencję i rzeczywistość rozszerzoną. Jestem przekonany, że branża dostrzeże także potrzebę lepszej opieki nad klientem, rzeczywistego wsparcia ludzi – klientów w zakresie poradnictwa związanego z bezpieczeństwem, a nie tylko reagowania na incydenty.

Mam głębokie przekonanie, że przechodzenie wielu branż gospodarki, a nawet wybranych dziedzin życia do sfery cyfrowej będzie rosnąć, w efekcie optymalizując koszty i poprawiając efektywność realizowanych usług. Ten proces nie ominie przedsiębiorców dostarczających usługi ochrony osób i mienia, chyba że branża nie nadąży za światowymi trendami.

Warto na koniec zadać pytanie: Co po pandemii? Bądźmy uważni, obserwując zagrożenia i dostosowując w miastach (i nie tylko) taktykę ich zwalczania. Wydaje się, że wielu przestępców czeka na „odmrożenie" ich branż, np. narkotykowej. Pracownicy ochrony, zaawansowane systemy monitoringu wizyjnego i profesjonalne reakcje na incydenty mogą odegrać swoją rolę obok policji i świadomych mieszkańców, szczególnie w placówkach edukacyjnych, uczelniach, klubach, dyskotekach, miejscach imprez itp. „Wybuchowi" potrzeb spotykania się, wspólnej zabawy, organizacji imprez może towarzyszyć wzmożenie produkcji, handlu, udzielania substancji zmieniających świadomość. Podsumowując, warto podkreślić, że tylko od nas zależy, jak wykorzystamy szanse pojawiające się w kryzysie.

Dagmara Pomirska

Axis Communications

Monitoring wizyjny w służbie zdrowia

Technologia monitoringu wizyjnego odgrywa coraz istotniejszą rolę w sektorze ochrony zdrowia. Inteligentne kamery przestały być jedynie narzędziem do ochrony szpitali przed niepowołanymi gośćmi. Już dziś mogą odpowiadać za analitykę obrazu w dozorze wejść do wyznaczonych stref oraz monitorowaniu stanu pacjentów.

Nowoczesne rozwiązania łączące monitoring wizyjny z dwukierunkowym audio – np. w postaci urządzeń zainstalowanych przy łóżkach pacjentów – wspierają pielęgniarki i lekarzy w monitorowaniu samopoczucia i komunikowaniu się z chorymi na odległość. Analityka wspierająca infrastrukturę kamer może być dostosowana do różnych objawów. Jeśli wymagają one natychmiastowego zaalarmowania personelu, nowoczesne systemy mogą to realizować automatycznie, np. informować o upadkach pacjentów. Co więcej, dostarczają wizualną weryfikację, potwierdzenie alarmów pochodzących z innych urządzeń. Przykładowo, gdy nagle zmieniają się parametry odczytu monitorowanego serca pacjenta, możliwość uzupełnienia wyników urządzenia o obraz pacjenta z kamery może wesprzeć diagnozę lub reakcję lekarzy – pacjent mógł się przewrócić, zadławić czy zdenerwować jakąś sytuacją. Nie mniej ważna pozostaje dla chorych możliwość komunikowania się drogą cyfrową także z rodziną. Nawet gdy parametry zdrowia pacjenta nie są najlepsze, a np. choroba zakaźna nie pozwala na bezpośredni kontakt z najbliższymi, inteligentne systemy monitoringu wizyjnego dają namiastkę bliskości, znacznie pomagając w procesie zdrowienia.

Bardzo ważny jest także aspekt edukacyjny zastosowania monitoringu wizyjnego w służbie zdrowia. Szybka wymiana informacji i szkolenie kolejnych pokoleń personelu medycznego są dziś w medycynie niezbędne. Monitoring wspiera jakość edukacji klinicznej. Daje obraz w czasie rzeczywistym z operacji, możliwość zapoznania z rzadkimi schorzeniami – zarówno procesem diagnozowania, jak i leczenia oraz nauki na realnych przykładach, takich jak procedury opieki nad pacjentami.

Istniejąca infrastruktura monitoringu wizyjnego w szpitalach, wzbogaco-

na lub zintegrowana w systemy spełniające wymagania współczesnej medycyny i opieki nad pacjentem, może zwiększyć poziom bezpieczeństwa w sektorze ochrony zdrowia. Inwestycje w rozwiązania monitoringu poprawiające funkcjonowanie placówek ochrony zdrowia przyniosą prawdziwy zwrot w przyszłości, w której zdalna i zautomatyzowana opieka staną się nową normą.

Łukasz Stępień

ekspert

Rzetelni partnerzy pomogą w kryzysie

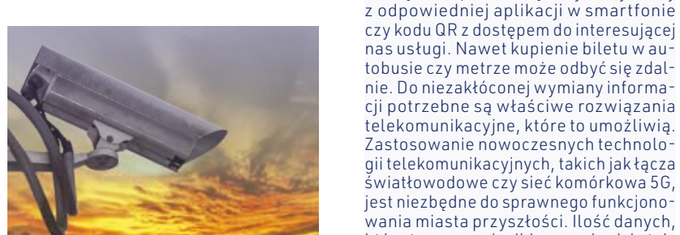
Początek epidemii COVID-19 był dla wszystkich szokiem. Coś nieznanego i niewidocznego gołym okiem wywróciło naszą rzeczywistość, także związaną z zapewnieniem bezpieczeństwa użytkownikom obiektów. Tam, gdzie była możliwość, pracownicy byli delegowani do pracy w trybie zdalnym. Obiekty, które do tej pory tętniły życiem, opustoszały.
W wielu przypadkach pandemia sprawiła, że zarządcy obiektów stanęli przed jeszcze trudniejszym zadaniem. Co można zrobić, aby osoby przebywające wewnątrz budynku czuły się bezpiecznie i były bezpieczne? Wielu zarządców zwróciło się w sposób naturalny do partnerów z branży security. Wybuchło zainteresowanie kamerami termowizyjnymi, urządzeniami sygnalizującymi o braku zachowania dystansu pomiędzy ludźmi czy innymi okołocovidowymi rozwiązaniami, które miały zapewnić bezpieczeństwo i komfort psychiczny osobom przebywającym na terenie obiektów.
W odpowiedzi na ogromne zapotrzebowanie ze strony rynku wiele firm, które do tej pory nie były powiązane z branżą security, postanowiły rozpocząć dostarczanie tego typu usług. Zarządcy obiektów, działający pod presją ze strony swoich klientów, nie zawsze mieli czas oraz kompetencje, aby zweryfikować jakość i realną wartość dostarczanych rozwiązań. Dopiero z czasem się okazywało, że kupiona kamera termowizyjna mierzy temperaturę osób wchodzących do obiektu, ale tylko wtedy, gdy wchodzą one pojedynczo, a temperatura otoczenia jest stabilna. Urządzenia, które miały informować o braku zachowaniu odpowiedniego dystansu, działają, ale trzeba je ładować co trzy godziny. Wystarczy niewłaściwe ułożenie czytnika, aby przestał pełnić swoją funkcję.
Prawdziwymi wygranymi w tej sytuacji były organizacje, którym udało się zbudować wcześniej trwałe relacje z odpowiednimi podmiotami. Jak wiadomo, przyjaciół poznaje się w biedzie, a rzetelnych partnerów biznesowych w kryzysie.

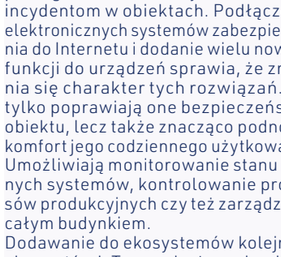
Jakub Sobek

Linc Polska

Zrób sobie prezent...

Zazwyczaj w kontekście poprawy bezpieczeństwa budynków mówi się o zapobieganiu stratom czy ewentualnym incydentom w obiektach. Podłączenie elektronicznych systemów zabezpieczenia do Internetu i dodanie wielu nowych funkcji do urządzeń sprawia, że zmienia się charakter tych rozwiązań. Nie tylko poprawiają one bezpieczeństwo obiektu, lecz także znacząco podnoszą komfort jego codziennego użytkowania. Umożliwiają monitorowanie stanu różnych systemów, kontrolowanie procesów produkcyjnych czy też zarządzanie całym budynkiem.
Dodawanie do ekosystemów kolejnych elementów IoT sprawia, że zacierają się granice pomiędzy systemami inteligentnego budynku a systemami zabezpieczenia technicznego. W kolejnych latach ten trend będzie coraz bardziej zauważalny. Jednym z rozwiązań pozwalających na podniesienie bezpieczeństwa, np. w budynkach użyteczności publicznej, jest system kontroli dostępu. Nie tylko chroni on pomieszczenia przed nieuprawnionym dostępem, ale także ułatwia osobom korzystającym z danych pomieszczeń ich szybkie i łatwe otwieranie, np. za pomocą aplikacji w telefonie komórkowym. Taka koncepcja znacząco poprawia bezpieczeństwo i wpływa na komfort codziennego użytkowania. Ponadto system kontroli dostępu w chmurze zapewnia administratorowi sprawne i zdalne zarządzanie uprawnieniami wszystkich użytkowników z każdego miejsca na świecie.
Również agregacja danych w chmurze pozwala na szybkie tworzenie raportów i analiz wejść do poszczególnych pomieszczeń. Jedną z dodatkowych możliwości jest weryfikacja tras przemieszczania się wybranych osób i ich potencjalnych kontaktów. Opcja ta może okazać się bardzo istotna w przypadku, gdy dowiadujemy się, że jeden z pracowników mógł zarażać inne osoby. Wówczas w systemie zweryfikujemy, z kim w ciągu dnia mógł mieć bliski kontakt. To pozwala na natychmiastowe i bardzo skuteczne reagowanie na potencjalne zagrożenia. Szukając bezpieczeństwa, nie zapominajmy o codziennym komforcie użytkowania. To prezent, jaki robimy sami sobie.





Marcin Walczuk

BCS

Miasta przyszłości już dziś

Nowoczesne miasto to miasto cyfrowe. Żyjemy w świecie informacji, czerpiemy je z całego świata, wiele też generujemy sami. Miasta również muszą nadążać za tym trendem. Zmiany te wymusiła w ostatnim roku pandemia koronawirusa. Aby ograniczyć kontakt fizyczny i nie dotykać miejsc, w których może przenosić się wirus, coraz częściej korzystamy z odpowiedniej aplikacji w smartfonie czy kodu QR z dostępem do interesującej nas usługi. Nawet kupienie biletu w autobusie czy metrze może odbyć się zdalnie. Do niezakłóconej wymiany informacji potrzebne są właściwe rozwiązania telekomunikacyjne, które to umożliwią. Zastosowanie nowoczesnych technologii telekomunikacyjnych, takich jak łącza światłowodowe czy sieć komórkowa 5G, jest niezbędne do sprawnego funkcjonowania miasta przyszłości. Ilość danych, które tworzymy i odbieramy, będzie tylko rosła, dlatego tak ważne są prędkość i przepustowość sieci, do których mamy dostęp. Każdy użytkownik smartfonu korzystający z połączenia z Internetem, przeglądający strony www, media społecznościowe czy uruchamiający zdalnie odkurzacz w swoim domu generuje ruch sieciowy. Do tego dochodzi coraz większa liczba urządzeń IoT, urządzeń inteligentnych czy różnego rodzaju czujników, np. wspomagających systemy monitorowania miejsc parkingowych, zautomatyzowane systemy zarządzania ruchem ulicznym czy system monitoringu miejskiego.
Poprawa i zapewnienie odpowiedniego poziomu bezpieczeństwa mieszkańców powinny być jednym z głównych założeń rozwijającego się miasta. Rosnąca liczba kamer w miejskim systemie monitoringu wizyjnego pozwala na dokładniejszą analizę potencjalnych zagrożeń, ale również przyspiesza reakcję odpowiednich służb na niebezpieczne sytuacje. Dzięki coraz szerszemu wykorzystaniu sztucznej inteligencji w urządzeniach CCTV wykrywanie i wysyłanie powiadomienia o zdarzeniu może odbywać bez udziału operatorów systemu. Oczywiście nie chodzi o całkowite wyeliminowanie człowieka, ale umożliwienie mu skupienia się na zdarzeniach alarmowych, których system nie jest w stanie w jednoznaczny sposób sklasyfikować. W ostatnich latach poprawiła się też jakość obrazu przekazywanego przez kamery. Teraz ich rozdzielczość jest już na tyle wysoka, że nawet z dużej odległości można zidentyfikować numer tablicy rejestracyjnej czy rozpoznać twarz człowieka. Na podstawie dodatkowych informacji, które „dostajemy" z systemu monitoringu wizyjnego, można później w łatwy i zdecydowanie szybszy sposób wyszukać potrzebne nagrania. To przekłada się na skuteczniejsze działanie systemu bezpieczeństwa miasta i mieszkańców jako całości.

Anna Twardowska

Nedap Security Management

Budynki bardziej inteligentne

Nowoczesne budynki to nie tylko nowatorskie rozwiązania w zakresie architektury, designu czy materiałów, z których są zbudowane, ale przede wszystkim technologie, w które są wyposażane. Okres pandemii jest dodatkowym motorem zmian i potrzeb, np. w zakresie ograniczania liczby osób w poszczególnych strefach budynków czy zwiększania reżimu sanitarnego. Wprowadza się nowe rozwiązania, np. systemy łączące autoryzację kartą w systemie kontroli dostępu z koniecznością użycia środka dezynfekującego z dozownika lub urządzenia do sprawdzania temperatury osób wchodzących do obiektu. Technologia pomaga zarządzać miejscami pracy *(hot desk)* tak, aby ułatwić zachowanie dystansu społecznego, przy jednoczesnym umożliwieniu pozostawiania rzeczy osobistych w szafkach, których zamki są sterowane przez system kontroli dostępu.

Ważna jest tutaj rola zintegrowanych systemów, które umożliwią raportowanie aktualnego stanu osób przebywających w budynku, w podziale na pracowników biura, firm wykonujących prace serwisowe i gości. Raporty z wykorzystania poszczególnych stref budynków pozwalają na optymalizowanie przestrzeni biurowej. Coraz częściej pojawiają się systemy, które po przyłożeniu karty do czytnika kontroli dostępu na wejściu do biurowca umożliwiają w pokoju danego pracownika ustawienie odpowiedniej temperatury czy oświetlenia.
Coraz większą popularnością cieszy się też możliwość rezerwowania biurek, sali konferencyjnych czy miejsc parkingowych z poziomu aplikacji mobilnej. Wykorzystywanie kodów QR jako identyfikatorów dla gości czy wysyłanie im regulaminu poruszania się po obiekcie przed spotkaniem to także zauważalny trend. Wszystkie te inteligentne rozwiązania mają wpływ na oszczędność energii elektrycznej oraz poprawę komfortu użytkowników takich przestrzeni. To z pewnością będzie silny motywator do inwestycji w najnowsze technologie budynkowe.
Mnogość oferowanych inteligentnych rozwiązań wpływa także na nowe wyzwania w zakresie bezpieczeństwa. Styk różnych systemów i technologii to potencjalne miejsca, które mogą być podatne na ataki hakerów. Warto podkreślić, że w inteligentnych budynkach nieodzowne są nowoczesne systemy i ich integracje, ale powinno się stosować rozwiązania producentów, którzy mają produkty zapewniające ochronę przed cyberatakami.

Jakub Kozak

Genetec

Co zmieniała pandemia

Pandemia nauczyła nas pracy w trybie hybrydowym, co zmienia podejście do ochrony biurowców. To jednak nie oznacza, że będziemy potrzebować mniej zabezpieczeń.
Często zgłaszali się do nas klienci, którzy szukają nowych rozwiązań do biura. Widzę zainteresowanie modernizacją systemów zabezpieczeń. Trzeba pamiętać, że w czasie, gdy w biurze pozostają tylko niezbędni pracownicy lub osoby zarządzające logistyką, naruszenia bezpieczeństwa mogą zdarzyć się częściej. Jeśli ludzi jest mniej, to więcej jest incydentów niezauważonych, bo odbywają się bez świadków. W pandemii pojawiła się potrzeba zdalnego nadzoru i tutaj widzę wielki potencjał rozwoju systemów zabezpieczeń. Obecnie powinny być one oparte na sieciach TCP/IP. To jest przyszłość.
Widzimy wyraźnie, że systemy powinny być zintegrowane. Alarm można zweryfikować zdalnie, np. przez system monitoringu wizyjnego, i jeśli nie jest fałszywy, właściwie na niego zareagować. Możliwość dołożenia do systemu urządzeń audio IP urządzeń interkomowych to dodatkowy plus. Jeśli mamy zintegrowany system antywłamaniowy z monitoringiem wizyjnym i urządzeniami audio, jesteśmy w stanie zweryfikować alarm i wytworzyć sygnał audio z urządzenia dużej mocy pracujących w sieci TCP/IP.
Nie wszystkie systemy w budynku trzeba integrować. Najlepiej wybrać tylko te części, których połączenie da wymierne korzyści. Podobna sytuacja jest z istniejącą infrastrukturą techniczną. Jej wykorzystanie może zmniejszyć koszty, ale musimy sprawdzić, czy np. istniejące kable nie są za stare.
W pandemii klienci rozumieją, że czasem należy zainwestować więcej, by nie ponosić dodatkowych kosztów w przyszłości. Etapem krytycznym w modernizacji jest przejście ze starego systemu na nowy. Jest to moment, kiedy możemy utracić wiele danych. W przypadku systemu dozoru wizyjnego będziemy mogli utracić materiał wizyjny, w kontroli dostępu będą to raporty kto, gdzie i kiedy wchodził do budynku lub opuszczał go. Te dane muszą mieć kopie, tak by przejście na nowy system nie powodowało ich utraty. Ważne jest też aktualizowanie oprogramowania, a najlepiej zabezpieczenie jego aktualizacji minimum na kilka lat.

System Reconeyez

inteligentny monitoring mobilny dla branży security i miast

ŁATWO O MONITORING, JEŚLI ISTNIEJE INFRASTRUKTURA. CO, JEŚLI JEJ NIE MA?

Zdecydowana większość rozwiązań monitoringu wizyjnego opiera się na istniejącej, nowoczesnej infrastrukturze – szybkim Internecie światłowodowym, stałym zasilaniu i bezpiecznym terenie instalacji. Dla wielu lokalizacji – nawet tych blisko centrum miast – spełnienie takich warunków to pieśń odległej przyszłości. W takich miejscach, jak przedmieścia, parki, skwery, pustostany, tereny nadrzeczne czy zielone obiekty turystyczne zbudowanie odpowiedniej infrastruktury kablowej jest z wielu względów niemożliwe lub bardzo kosztowne. Często dochodzi tam do aktów wandalizmu, kradzieży i niszczenia mienia, tam jak grzyby po deszczu powstają gruzowiska z nielegalnie wyrzucanych odpadów. Miejsca te są solą w oku służb bezpieczeństwa i włodarzy miasta, ponieważ trudno tam zapewnić monitoring wizyjny. Problem dotyczy nie tylko miast – są przecież poligony, żwirownie, pasieki, działki rekreacyjne, place budowy i inne obiekty chronione przez agencje. Wymieniać można długo, a problem trapi wielu klientów komercyjnych z sektora budżetowego, służb mundurowych i specjalnych.

PRZECIEŻ SĄ FOTOPUŁAPKI... PRAWDA?

Nasza firma była jednym z pierwszych dystrybutorów fotopułapek w Polsce i wciąż aktywnie dystrybuuje kilkadziesiąt różnych modeli najbardziej rozpoznawalnych producentów. Pierwsi w kraju dostrzegliśmy zagrożenia związane z ich użytkowaniem po wprowadzeniu RODO, na co odpowiedzią było wprowadzenie do oferty fotopułapek z szyfrowaniem danych. Jednak nawet najbardziej zaawansowane fotopułapki nie mają zalet, jakie ma system Reconeyez.

PO PIERWSZE – DETEKTOR

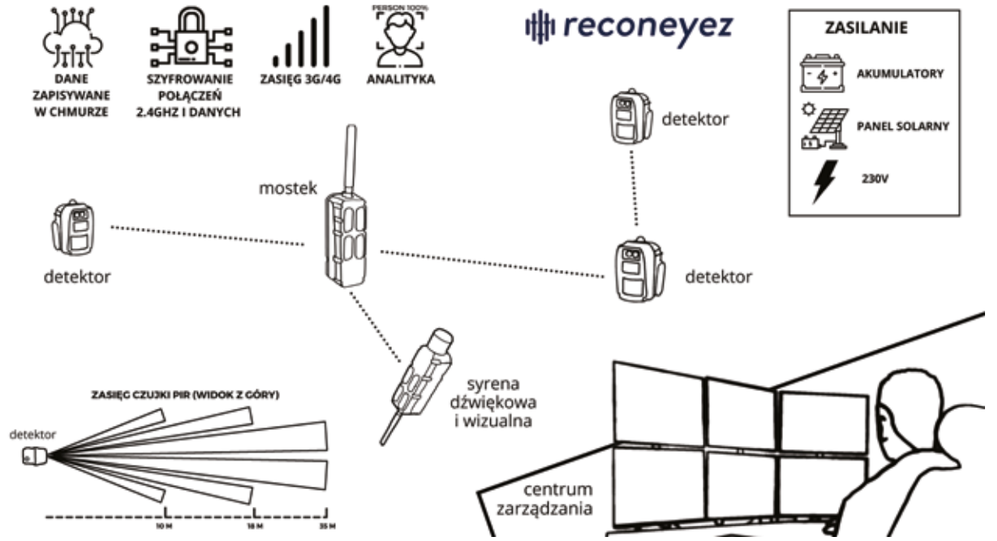
Reconeyez jest połączeniem bezprzewodowych kamer z oprogramowaniem online do zarządzania materiałem i samymi kamerami. Wszystkie urządzenia są produkowane w Estonii, a sam system istnieje od 12 lat i jest sprawdzony przez setki użytkowników w ponad 35 krajach. Najważniejszym jego elementem jest detektor, czyli kamera z dwoma obiektywami (do pracy dziennej i nocnej) i diodami podczerwieni. Czujka PIR wykrywa ruch z 30 m, po czym wykonywane są zdjęcia. Minimalny dopuszczalny interwał między nimi to 100 ms, co oznacza, że w ciągu jednej sekundy detektor Reconeyez może wykonać 10 zdjęć! Ma to bardzo duże znaczenie w trakcie fotografowania szybko poruszających się osób i pojazdów, by uchwycić najważniejsze klatki – np. z widocznymi numerami tablicy rejestracyjnej lub detalami twarzy.

PO DRUGIE – MOSTEK

Za wysyłkę zdjęć odpowiada mostek – osobny nadajnik, który łączy się z detektorami drogą radiową 2,4 GHz. Jeden mostek może pracować w zestawie z maks. 8 detektorami jednocześnie i może być ustawiony w odległości do 500 m od detektora. Dowolna przy tym jest możliwość konfiguracji ułożenia detektorów i mostków, ponieważ detektory mogą pełnić funkcję repeaterów i przekazywać zdjęcia również z innych urządzeń, które znajdują się w sieci, ale które nie mają komunikacji radiowej bezpośrednio z mostkiem. Można więc rozwiesić detektory tak, by były w podobnej odległości od mostka, lub ustawić system w linii. Następnie zdjęcia są przesyłane przez mostek na serwer z analityką obrazu przez moduł GSM (2G/3G/4G). Mostek Reconeyez pracuje z kartami SIM każdego polskiego operatora komórkowego – wystarczy raz przeprowadzić konfigurację sieci.

PO TRZECIE – OPROGRAMOWANIE Z ANALITYKĄ OBRAZU, KTÓRA MINIMALIZUJE FAŁSZYWE ALARMY

Jedną z kluczowych zalet systemu Reconeyez jest aplikacja do obsługi systemu. Domyślnie odbywa się przez konto użytkownika założone na serwerze producenta, ale istnieje też możliwość kupna serwera i oprogramowania *on-site* (u klienta). Aplikacja służy do przeglądania zdjęć, monitorowania statusu detektorów i mostków oraz do ich konfiguracji. Użytkownik otrzymuje dostęp jako administrator i ma pełne możliwości w tworzeniu subkont dla kolejnych użytkowników. Mogą



mieć oni różny stopień dostępu, a także przypisane konkretne urządzenia – możliwe jest więc rozdzielenie zadań i obowiązków nawet w bardzo dużych strukturach pracowniczych. Kluczową funkcjonalnością Reconeyez jest analityka obrazu, która przebiega automatycznie na każdym przesłanym zdjęciu. Wszystkie zdjęcia, na których zostaje wykryta osoba lub pojazd, będą automatycznie oznaczone jako alarm. Analityka obrazu znacznie minimalizuje liczbę fałszywych alarmów, oszczędza czas i podnosi skuteczność systemu.

POJEMNE AKUMULATORY = WYGODNA I BEZPIECZNA OBSŁUGA

Dlaczego wygodna? Pojemne akumulatory oznaczają rzadsze wizyty w miejscu instalacji, co oszczędza czas i pieniądze potrzebne na dojazdy. Dlaczego bezpieczna? Częste wizyty przy urządzeniach mogą zwrócić niepotrzebną uwagę osób postronnych.
Akumulatory Li-Ion stosowane w systemie Reconeyez to ogniwa o pojemności 10 200 mAh, które pozwalają na wykonanie aż 50 000 zdjęć lub pracę przez 400 dni w trybie *stand-by*. Są to wartości nieosiągalne dla innych kamer mobilnych. Detektor mieści jeden akumulator, a mostek aż cztery. Wymiana akumulatora jest niezwykle prosta i zajmuje kilkanaście sekund. Dla dodatkowego zabezpieczenia można zainstalować syrenę, która w trakcie wykrycia intruza w pobliżu nada odstraszający sygnał audiowizualny. Wszystkie urządzenia – mostki, detektory i syreny można podpiąć pod panel solarny, dodatkowy zestaw baterii lub nawet zasilanie z sieci.

INSTALACJA? DZIECINNIE PROSTA

Sama instalacja detektorów i mostków jest łatwa i opiera się na uniwersalnym uchwycie montażowym, który ma otwory do montażu na śruby lub kołki rozporowe oraz wejścia na parciane paski montażowe. Od strony, gdzie uchwyt łączy się z urządzeniem, mamy do dyspozycji okrągłą głowicę do regulacji położenia i kąta nachylenia detektorów i mostków.

INTEGRACJA? OCZYWIŚCIE

Reconeyez można integrować z innymi systemami bezpieczeństwa – m.in. z systemami wykorzystywanymi przez agencje ochrony i centra monitoringu miejskiego.

BEZPIECZEŃSTWO TO PODSTAWA

System Reconeyez korzysta z AES128 i ECC. Wszelkie połączenia między detektorem a mostkiem i między mostkiem a serwerem są szyfrowane, a zdjęcia zapisywane w pamięci wewnętrznej detektorów.

NIE DOTYKAJ MNIE!

Urządzenia monitoringu mobilnego są zazwyczaj pozostawiane w miejscu obserwacji bez nadzoru. Na szczęście potrafią się „bronić” – wbudowany akcelerometr reaguje na poruszenie i przesyła alarm do użytkowników i syreny alarmowej. Detektory w momencie poruszenia robią zdjęcie, co zwiększa szansę na rozpoznanie złodzieja. Akcelerometr można w dużym zakresie regulować (w każdym urządzeniu z osobna), co pozwala wykluczyć fałszywe alarmy czujnika antykradzieżowego.

I DO OGRÓDKA, I DO OGRODU... NP. BOTANICZNEGO?

Reconeyez jest w pełni skalowalny – mogą to być trzy detektory do ochrony parku miejskiego czy trzydzieści detektorów do ochrony parku narodowego. Dzięki temu sprawdzi się wszędzie tam, gdzie monitoring jest potrzebny, a nie ma odpowiedniej infrastruktury dla kamer CCTV. System Reconeyez jest ciągle rozwijany, zarówno na poziomie sprzętowym, jak i programowym, co zapewni w przyszłości wiele nowych funkcji.
Obecnie rozbudowujemy sieć partnerów, w związku z czym zapraszamy do nawiązania z nami kontaktu i rozpoczęcia współpracy – wszystkim partnerom oferujemy szerokie wsparcie techniczno-handlowe, szkolenia i atrakcyjne warunki projektowe.
Charakter produktu umożliwia nie tylko jego sprzedaż, ale również najem krótko- i długoterminowy – chętnie przedstawimy szczegóły tego rozwiązania partnerom i klientom końcowym.

O FIRMIE

Firma TVprzemyslowa od 2007 r. prowadzi dystrybucję systemów telewizji dozorowej, a także innych rozwiązań z zakresu zabezpieczeń technicznych. Od wielu lat specjalizuje się w monitoringu mobilnym, dostarczając unikatowe rozwiązania wyposażone we własne zasilanie i moduły bezprzewodowej komunikacji danych. Pracownicy kierują się wartościami rzetelnej i uczciwej współpracy z partnerami, stawiając przy tym na ochronę projektową i wsparcie przy realizacji wspólnych działań.

TVPRZEMYSLOWA
ul. Kórnicka 30, 61-141, Poznań
tel: +48 61 875 04 76
www.TVprzemyslowa.pl
www.reconeyez.pl

System monitoringu wizyjnego miasta

wspierany sztuczną inteligencją gwarancją skutecznej reakcji na zdarzenia

Wykrywanie i szybka reakcja na zdarzenia w miejskim systemie monitoringu wizyjnego to dla operatorów centrum monitorowania odpowiedzialne i wyczerpujące zadanie. Stres z tym związany może powodować częste błędy personelu i opóźniać jego reakcję. Pomocna w tym przypadku jest sztuczna inteligencja *(Artificial Intelligence, AI).* Dzięki niej zdarzenia są sprawniej zarządzane, a w efekcie zwiększa się ich wykrywalność.

System monitoringu miasta jest stosowany do śledzenia podejrzanych zdarzeń i przeciwdziałania zagrożeniom na danym obszarze. Dotychczas to operatorzy systemu musieli uważnie obserwować obrazy z wielu kamer na monitorach i reagować na zdarzenia wymagające podjęcia interwencji. Wbudowana sztuczna inteligencja wyręcza ich w uciążliwej obserwacji monitorów i wspiera w szybszym i dokładniejszym rozpoznawaniu zdarzeń. Bez pomocy AI operatorom jest znacznie trudniej szybko zareagować na dany incydent; również czas niezbędny na ręczne przeszukanie materiału zarejestrowanego z wielu kamer w celu np. zlokalizowania podejrzanej osoby niebezpiecznie się wydłuża. A czas jest w takich sytuacjach parametrem niezmiernie istotnym.

Miejski system bezpieczeństwa stoi przed wyjątkowymi wyzwaniami. Fakt, że system często składa się z tysięcy kamer, które transmitują ogromne ilości danych, może stwarzać problemy w zakresie przestrzeni dyskowej, nie wspominając już o przeciążeniu operatorów. Sztuczna inteligencja sprawia, że dozór jest znacznie efektywniejszy. Analizuje błyskawicznie ogromne ilości danych w całej sieci, a jednocześnie odciąża operatorów, optymalizuje bezpieczeństwo, usprawnia zarządzanie zdarzeniami i znacząco zwiększa wydajność pracy.

AI TWORZY INTELIGENTNY SYSTEM DOZORU WIZYJNEGO MIASTA

Zastosowanie sztucznej inteligencji znacznie zwiększa wygodę użytkowania systemu przez operatora. Automatyczne i szybkie wykrycie podejrzanego zdarzenia ułatwia identyfikację zagrożeń, zwiększając w ten sposób efektywność i skracając czas reakcji. Sztuczną inteligencję można zaprogramować tak, aby wykrywała nietypowe zachowania (niespełniające określonych kryteriów) i natychmiast ostrzegała o nich operatora. Dzięki AI szybciej sygnalizowane są krytyczne zdarzenia, a to umożliwia operatorowi natychmiastowe podjęcie wymaganego w danej sytuacji działania.
Wykorzystanie AI w aplikacjach obejmujących całe miasto jest szczególnie korzystne ze względu na dużą liczbę kamer. Operatorzy mogą być bardziej skuteczni w zarządzaniu wieloma kamerami, jeśli otrzymają ostrzeżenia i alarmy dotyczące potencjalnych incydentów. Przykładem może być np. pozostawienie pakunku na środku zatłoczonego placu miejskiego. System dozoru wizyjnego wspomagany sztuczną inteligencją został skonfigurowany tak, aby rozpoznawać/wykrywać nietypowe obiekty stacjonarne i wysyłać ostrzeżenie do operatora stacji roboczej, gdy zdarzenie wymaga interwencji człowieka. Widząc, że przedmiot został pozostawiony przez jakiś czas, operator może powiadomić odpowiednie służby i jednocześnie, korzystając z funkcji AI wyszukiwania (rozpoznawania) twarzy, łatwo może uzyskać obraz osoby, która pakunek pozostawiła. Oprogramowanie do rozpoznawania twarzy może przeszukać zapisany materiał z miejskiej sieci kamer w celu wskazania osoby, a następnie prześledzić jej zachowanie przed pozostawieniem pakunku i po tym fakcie. Ten automatyczny proces wyszukiwania przeprowadzany przez technologię AI pozwala zaoszczędzić cenny czas reakcji na zdarzenia alarmowe.

INCYDENTY W CZASACH PANDEMII

Wraz z nastaniem ery COVID-19 zmieniła się liczba incydentów, na które operator musi reagować. Mogą nimi być np. zgromadzenia, brak maseczki, niezachowanie dystansu a także podwyższona temperatura ciała, mierzona za pomocą specjalistycznych kamer termowizyjnych skalibrowanych do jak najdokładniejszego ustalenia temperatury ciała człowieka.

IMPLIKACJE DLA SYSTEMÓW MONITORINGU MIEJSKIEGO

Miasta, które mogą się pochwalić wysoką skutecznością/efektywnością miejskiego systemu monitoringu, w których mieszkańcy czują się bezpiecznie, mają większą szansę na przyciągnięcie turystów i inwestorów. Dlaczego? Choćby dlatego, że zmniejszenie liczby incydentów w danym mieście i uczynienie z niego bezpieczniejszego miejsca do życia i pracy wspiera jego długoterminowy rozwój i sukces. Zatem korzyści płynące z zastosowania AI w monitoringu miejskim są bardzo atrakcyjne dla miast na całym świecie. Już dziś wiele z nich rozważa wykorzystanie dostępnych opcji technologicznych.

WYKORZYSTANIE NOWOCZESNYCH KAMER CCTV ZGODNYCH Z NDAA

Nowatorskie kamery dozorowe mogą objąć swoim zasięgiem dużo większy obszar obserwowanej sceny. W przypadku rozległych systemów miejskich ma to znaczenie szczególne. Jeśli jedna kamera może zarejestrować obraz, który wcześniej rejestrowały cztery niezależne kamery, jest to bez wątpienia rozwiązanie bardziej ekonomiczne i funkcjonalne. A przecież na takich właśnie oszczędnościach włodarzom miast zależy. Przykładem takiego rozwiązania jest wieloprzetwornikowa kamera firmy IndigoVision, idealna choćby do obserwacji skrzyżowań ulic, a posiadająca:

- Cztery indywidualnie regulowane przetworniki obrazu (moduły wizyjne z własnymi obiektywami) patrzące w czterech różnych kierunkach jednocześnie, generujące obraz wysokiej rozdzielczości łącznie 20 Mpix.
- Kompresję H.265 i H.264 z technologią SmartCodec, co zapewnia maksymalizację przepustowości i zmniejszenie zapotrzebowania na przestrzeń dyskową bez pogorszenia jakości obrazu.
- True Wide Dynamic Range pozwalające wychwycić szczegóły w scenach o różnych warunkach oświetleniowych, dostosowując się zarówno do jasnych, jak i ciemnych obszarów. Ponadto adaptacyjne oświetlenie promiennika podczerwieni umożliwia kamerom regulację szerokości wiązki IR. Zapobiega to prześwietleniu obiektów znajdujących się bliżej promiennika i źródeł światła.
- 5-letnią gwarancję producenta.

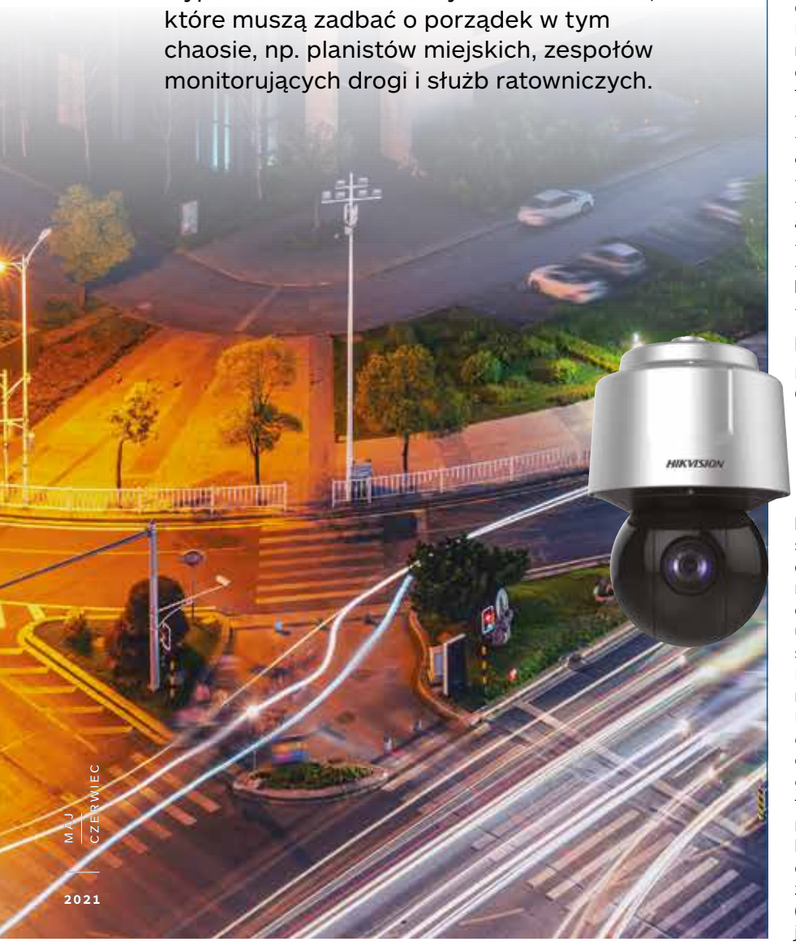
Dzięki widokowi panoramicznemu 360° wieloprzetwornikowa kamera IndigoVision umożliwia obserwację dużych obszarów za pomocą jednego urządzenia. Poszczególne przetworniki obrazu (moduły wizyjne) można ustawić tak, aby monitorować praktycznie osobno każdy obszar, co ułatwia późniejsze odszukiwanie odpowiednich nagrań ze zgłoszonych incydentów, a w efekcie zwiększa wydajność pracy operatora. Zastosowanie w systemie IndigoVision technologii rozproszonej architektury sieci DNA zapewnia bezawaryjność podglądu na żywo przez operatorów. Strumień wideo z kamery do stacji operatora nie jest zależny od centralnego serwera, a opóźnienia są minimalne.

Wszystkie wprowadzone do oferty w 2021 roku kamery IndigoVision mają zgodność z NDAA *(National Defense Authorization Act),* dzięki czemu mogą być stosowane w obiektach infrastruktury krytycznej, takich jak obiekty militarne, szpitale, lotniska, obiekty rządowe, systemy monitoringu miejskiego i inne.

Rozwiązania Hikvision

usprawniające ruch drogowy

Wraz ze wzrostem liczby samochodów infrastruktura drogowa staje się coraz bardziej obciążona. Większa liczba pojazdów przekłada się na korki, frustracje i opóźnienia, co z kolei może prowadzić do łamania przepisów ruchu drogowego, a nawet do wyższych wskaźników wypadków. To złożone wyzwania dla służb, które muszą zadbać o porządek w tym chaosie, np. planistów miejskich, zespołów monitorujących drogi i służb ratowniczych.



Kluczowym celem pozostaje utrzymanie i egzekwowanie bezpiecznego i odpowiedzialnego poruszania się po drodze, optymalizacja wykorzystania dostępnych zasobów transportowych oraz jak najszybsze reagowanie na zdarzenia drogowe. Inteligentny system zarządzania ruchem drogowym firmy Hikvision całkowicie rozwiązuje wszystkie te problemy, usuwając utrudnienia dla użytkowników dróg oraz wąskie gardła, które od dawna stanowiły wyzwanie dla władz miasta, chcących utrzymać płynność ruchu i pomóc ludziom dotrzeć do celu bezpiecznie i na czas. Hikvision stale rozwija systemy analityczne, które, oprócz numerów tablic rejestracyjnych, potrafią również rozpoznać nietypowe zachowania na drodze:

→ niewłaściwy kierunek ruchu pojazdu,
→ pieszego w miejscu, w którym nie powinien się on znajdować,
→ korek uliczny,
→ przekroczenie dozwolonej szybkości,

a także – oprócz nietypowych zachowań – potrafią:

→ sklasyfikować markę i kolor pojazdu,
→ sprawdzić, czy użytkownicy mają zapięte pasy lub założony kask,
→ policzyć użytkowników jednośladów.

MIASTO CHORZÓW

Doskonałym przykładem może być miasto Chorzów. Chorzowski System Zarządzania Ruchem wykorzystujący inteligentne kamery ANPR Hikvision został zainstalowany w 2019 roku. Do budowy systemu wykorzystano kamery DarkFighter Network Speed Dome PTZ (DS-2DF6A236X-AEL), którą zainstalowano w newralgicznych obszarach miasta i na drogach kluczowych dla komunikacji miejskiej. Ten model kamery wyróżnia wysoka czułość przy słabym oświetleniu, stabilizacja obrazu i szybkie ustawianie ostrości, dzięki czemu idealnie sprawdza się w tym scenariuszu.
Na ruchliwych skrzyżowaniach wykorzystano również kamery 4-Directional Multi-sensor Network PanoVu (DS-2CD-6D24FWD), których celem jest uchwycenia widoku 360° na wszystkie drogi dojazdowe do skrzyżowania. Dało to również pewne oszczędności, ponieważ ten model łączy cztery moduły kamerowe. Wartość dodana to świetny design! Do rejestracji obrazu z kamer zastosowano 5 rejestratorów 4K NVR (DS-9632NI-I16), a całość zarządzana jest z platformy HikCentral.

Za „prawdziwego bohatera" systemu można uznać technologię ANPR (rozpoznawania numerów tablic rejestracyjnych). Dane ANPR z jednostki przechwytywania punktu kontrolnego ANPR (iDS--TCV300) dostarczyły kluczowych informacji, które spełniają wszystkie potrzeby projektu. Rozpoznawanie numerów rejestracyjnych pojazdów poruszających się (do prędkości 250 km/h), klasyfikacja pojazdów z podziałem na kategorie (osobowy, van, bus, ciężarowy itd.) to ważne funkcje tego systemu.
System został również zaprojektowany do integracji z wbudowanymi w jezdnię pętlami indukcyjnymi, które rejestrują przejeżdżające po nich pojazdy i przekazują zbierane informacje. Dzięki wdrożonemu systemowi Chorzów ma możliwość monitorowania ruchu miejskiego w jednym centrum monitoringu. Przyniosło to wiele korzyści, takich jak automatyczne wykrywanie wykroczeń drogowych i umożliwienie wydziałowi priorytetowego traktowania transportu publicznego w celu zapewnienia mieszkańcom szybszej podróży środkami komunikacji miejskiej. Pozwoliło to również policji na śledzenie podejrzanych pojazdów, dzięki integracji z platformą Smart City.

SYSTEM PARKINGOWY

Zarządcy parkingów i kierowcy mają wspólną potrzebę: chcą, aby parkowanie było łatwe, bezpieczne i efektywne. W praktyce jednak znalezienie wolnego miejsca po wjeździe na parking może być trudne. Wielu kierowców wie, że jest to bardzo frustrujące.
Hikvision oferuje sposób na szybkie prowadzenie kierowców do wolnego miejsca dzięki produktom, które można łatwo łączyć i integrować w celu uzyskania prostego i wydajnego rozwiązania. Usprawnienie parkowania, zarówno przy wjazdach/wyjazdach, jak i na całym parkingu, sprawia, że operacje stają się znacznie bardziej efektywne, przyspieszając proces i potencjalnie zwalniając miejsca szybciej do dalszego wykorzystania. Oznacza to też maksymalizację osiąganych zysków z przestrzeni. Zapewnia również dodatkowe warstwy bezpieczeństwa i spokój ducha zarówno kierowcom, jak i operatorom.

Wszystkie funkcje oferowane w rozwiązaniach Hikvision mogą służyć nie tylko zwiększeniu płynności i bezpieczeństwa ruchu, ale także wygodzie kierowców. Przykładowo, kierowcy będą mogli otrzymywać użyteczne informacje z systemu, który zostanie uzupełniony rozwiązaniami nadzorującymi miejsca parkingowe w mieście, a całość połączona z aplikacją informującą o wolnych miejscach.
Wykorzystując zespoły kamerowe serii iDS do nadzorowania miejsc parkingowych, operator systemu może:

→ otrzymać informacje o zajętości,
→ uzyskać wsparcie w procesie poboru opłat za parkowanie lub weryfikować, czy opłata została uiszczona,
→ kontrolować sposób parkowania pojazdów,
→ dostarczyć na urządzenie mobilne kierowcy informacje o wolnych miejscach.

Korzyścią dla kierowcy jest możliwość zidentyfikowania miejsca postoju pojazdu na mapie względem jego pozycji na parkingu. W skali mikro tego typu rozwiązania są stosowane na parkingach zamkniętych, gdyż często właściciel auta zapomina, na którym poziomie zostawił swój pojazd. System kamer nadzorujących miejsca parkingowe może dostarczyć informacje o miejscu postoju na terminal lub urządzenie mobilne. Dynamicznie rosnąca liczba różnego rodzaju inteligentnych urządzeń w naszym otoczeniu będzie z jednej strony powodowała obawy o możliwość inwigilacji, z drugiej zaś – podobnie jak smartfony – zmieni nasz styl życia. Dookoła nas są gromadzone ogromne ilości danych, które skorelowane ze sobą udostępnią kolejne użyteczne funkcje. I tylko wyobraźnia użytkownika oraz finanse mogą ograniczyć dostęp do najnowszych technologicznie rozwiązań.

HIKVISION POLAND

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

Inteligentne algorytmy

wspierają bezpieczeństwo polskich miast

Jednym z rozwiązań umożliwiających rozwój inteligentnych bezpiecznych miast są platformy bazujące na algorytmach sztucznej inteligencji. Wspierają one pracę operatorów systemu monitoringu wizyjnego poprzez automatyczną detekcję zdarzeń. Algorytmy te na bieżąco analizują obrazy z kamer i w razie wykrycia uprzednio zdefiniowanych zdarzeń natychmiast wysyłają powiadomienie do operatora. Możliwość szybkiej reakcji przyczynia się do zwiększenia skuteczności monitoringu w wykrywaniu oraz zapobieganiu zdarzeniom niepożądanym. Dzieje się tak m.in. w wielkopolskim Lesznie.

INTELIGENTNY MONITORING W LESZNIE

Miejski system monitoringu z inteligentną analizą obrazu funkcjonuje w Lesznie od 2014 r. i nieustannie jest rozbudowywany o kolejne rozwiązania. Obecnie w mieście zainstalowano ponad 60 kamer, które stale monitorują kluczowe dla bezpieczeństwa mieszkańców lokalizacje. Wszystkie są podłączone do serwerów i obsługiwane z centrum monitoringu znajdującego się w siedzibie Straży Miejskiej. Stamtąd koordynowana jest praca całego systemu wizyjnego w mieście.

EKOLOGICZNY SYSTEM OŚWIETLENIA W PRZEJŚCIU PODZIEMNYM

W Lesznie firma C&C Partners dostarczyła także ekologiczny system oświetlenia LED do remontowanego przejścia podziemnego. Jego unikatowość polega na tym, że oprócz równomiernego rozświetlenia, w oprawy ma wbudowane głośniki, z których w razie potrzeby rozgłaszane są komunikaty przez osoby sprawujące nadzór nad bezpieczeństwem w mieście.

POLSKIE MIASTA INWESTUJĄ W ZAAWANSOWANE BEZPIECZEŃSTWO

Wśród polskich miast, które zainwestowały w takie rozwiązania, jak Leszno, są m.in. Częstochowa, Łódź czy Zielona Góra. W Częstochowie na istniejącym serwerze Straży Miejskiej zainstalowano platformę analizującą obraz. Dzięki temu wdrożeniu miasto może korzystać z dotychczasowych kamer, a także wykorzystać nowe możliwości oferowane przez technologię, np. rozpoznawanie numerów rejestracyjnych samochodów. Do tej pory w ramach budżetu obywatelskiego zainstalowano dwa dodatkowe serwery oraz zakupiono 47 licencji na kanały wizyjne.

STACJE INTERKOMOWE SOS

W Łodzi z kolei jest wykorzystywany system komunikacji interkomowej do wewnętrznej łączności pomiędzy 18 jednostkami operacyjnymi, które realizują monitoring miejski. Dodatkowo cały system jest wspierany przez stację interkomową SOS przy ul. Piotrkowskiej oraz wolno stojące kolumny SOS zainstalowane w parkach miejskich, z których – w sytuacjach awaryjnych – bezpośrednio mogą korzystać mieszkańcy miasta i turyści. Na terenie objętym monitoringiem miejskim zostały także zainstalowane urządzenia nagłaśniające oraz tuba umożliwiająca przekazywanie komunikatów za pośrednictwem sieci interkomowej.
Zielona Góra natomiast zainwestowała w ponad 100 kamer wieloprzetwornikowych. Dzięki zastosowaniu zaawansowanych urządzeń pozyskano dodatkowo 328 obrazów z 82 newralgicznych punktów miasta. W systemie monitoringu wizyjnego zastosowano platformę z analityką obrazu, która realizuje funkcje rozpoznawania tablic rejestracyjnych i koloru samochodu, a także rozpoznawania twarzy, wieku i płci kierowcy. Znacznie poprawia to poziom bezpieczeństwa w polskich miastach.

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

Securitas smartIN

zadania i funkcjonalności nowoczesnych e-recepcji

Zaskocz gości komfortem, wygodą i możliwością automatycznej obsługi spotkań. Securitas smartIN pozwala na zaplanowanie wizyt i zarządzanie nimi od momentu wysłania zaproszenia po ich zakończenie. Intuicyjna obsługa minimalizuje liczbę czynności potrzebnych do umówienia spotkania i systematyzuje cały proces. W zaproszeniu możesz pozwolić gościom na wjazd, udostępnić miejsce parkingowe i nadać dostęp do określonych części biura. Goście korzystający z zaproszeń systemowych Securitas smartIN zyskują dużą wygodę i komfort, a zarządcy –bezpieczeństwo, prestiż i bezobsługową realizację wizyt.

Securitas smartIN to usługa wspierająca proces umawiania spotkań i automatyzująca pracę recepcji. Wysyła zaproszenia, powiadamia o przybyciu gości, przydziela i rezerwuje miejsca parkingowe oraz przyznaje unikalne kody, które po aktywacji stanowią czasowe identyfikatory dostępu do określonych wcześniej części obiektu.

Zaprojektowaliśmy Securitas smartIN tak, aby proces rejestracji przebiegał sprawnie i szybko, a poziom bezpieczeństwa w budynku wzrastał. Łącząc przemyślane oprogramowanie, mobilność i urządzenia IoT, sprawiliśmy, że goście oceniają wizyty jako komfortowe i nieskomplikowane, a gospodarze cieszą się z prostego zdalnego procesu rejestracji – mówi Radomir Dębek, inżynier produktu w Securitas Polska.

Komfort i sprawne zarządzanie procesem awizacji to zasługa integracji w czasie rzeczywistym wielu systemów i pożądanych funkcjonalności. Połączone zostały system KD, zarządzanie pozwoleniami na wjazd, czytniki kodów QR, kalendarze Google czy MS Outlook oraz iCal, a dopełnieniem jest usługa powiadomień. Dane spotkania, m.in. adres i termin oraz kod dostępu, gość otrzymuje automatycznie drogą mailową lub SMS-em w postaci kodu QR, a system synchronizuje terminy w kalendarzach. Dbając o bezpieczeństwo, Securitas smartIN nadaje uprawnienia ważne tylko w określonym czasie spotkania. Podanie w zaproszeniu numerów rejestracyjnych pojazdu gościa pozwala na automatyczny wjazd i rezerwację miejsca parkingowego na czas trwania spotkania. Ta funkcjonalność optymalizuje zarządzanie miejscami parkingowymi. Numery rejestracyjne gość może zmienić w dowolnym momencie, może też anulować spotkanie, wybierając taką opcję w zaproszeniu.

W trakcie tworzenia usługi przyświecała nam zasada secure by design i zgodność z wymogami RODO. Mamy pewność, że na każdym etapie nasze rozwiązanie chroni wprowadzone dane osobowe gości – dodaje Radomir Dębek.
Gość awizuje swoje przybycie za pomocą kodu QR, korzystając z bezobsługowego stanowiska Securitas smartIN. W tym momencie osoba zapraszająca otrzymuje przez aplikację mobilną powiadomienie o jego przybyciu. Moment awizacji jest też równoznaczny z wpisaniem gościa na budynkową listę ewakuacji – to funkcjonalność istotna dla firmy ochrony. Po zakończeniu spotkania ponowne zeskanowanie kodu w terminalu Securitas smartIN skutkuje wypisaniem gościa z listy ewakuacyjnej i automatycznym unieważnieniem przypisanych wcześniej uprawnień.
Securitas smartIN daje możliwość zarządzania większą liczbą recepcji za pomocą jednej centralnej platformy. Możliwe jest śledzenie ruchu osób odwiedzających budynek i uzyskanie wglądu w listę gości aktualnie znajdujących się w budynku.

- Securitas smartIN to szybka i samodzielna rejestracja wizyty poprzez zeskanowanie kodu QR.
- Securitas smartIN pozwala na rejestrację i zarządzanie wizyt nie tylko gości indywidualnych, ale też na rejestrowanie stałych dostawców.
- Securitas smartIN przydziela uprawnienia do poruszania się po określonych strefach budynku za pomocą cyfrowych kart dostępu. Możliwe jest tworzenie stałych przepustek dla określonych gości / dostawców.
- Securitas smartIN poprawia jakość obsługi, przyspiesza proces awizacji oraz zmniejsza koszty działania firmy.

Securitas smartIN działa w oparciu o rozwiązania chmurowe, aplikacje mobilne i urządzenia IoT. A to oznacza, że oprócz usprawnienia procesu awizacji i zwiększenia wygody usługa pozwala na szybkie wdrożenie i optymalizację kosztów.

SECURITAS POLSKA
Postępu 6
02-676 Warszawa
securitas@securitas.pl

Kompleksowa ochrona obiektów biurowych

Zabezpieczenie obiektów biurowych przez wzgląd na ich intensywne użytkowanie jest wyzwaniem dla administratorów i służb dozorujących. Chcąc zapewnić ochronę na wysokim poziomie, jednocześnie ułatwiając proces zarządzania bezpieczeństwem, warto sięgnąć po dostępne na rynku rozwiązania, które można dopasować do potrzeb danego przedsięwzięcia. Czy są wśród nich produkty, które sprawdzą się w instytucjach wielooddziałowych?

W budynkach biurowych stosuje się elektroniczne systemy zabezpieczenia technicznego, takie jak: sygnalizacji włamania i napadu (SSWiN), kontroli dostępu (SKD) oraz sygnalizacji pożarowej (SSP). Firma SATEL produkuje urządzenia umożliwiające budowę każdego z ww. systemów, jednocześnie oferując integrację części z nich.

SSWIN I ICH INTEGRACJA

Zaawansowane centrale alarmowe z rodziny INTEGRA i INTEGRA Plus umożliwiają budowę systemów sygnalizacji włamania i napadu łączących funkcje bezpieczeństwa, kontroli dostępu, monitoringu zdarzeń i automatyki budynkowej. Do zdalnego zarządzania warto wykorzystać INTEGRUM – narzędzie umożliwiające wygodny i przejrzysty nadzór nad bezpieczeństwem pojedynczych obiektów lub nawet całych ich sieci (także rozproszonych terytorialnie). Rozwiązanie to ułatwia i usprawnia procesy administracyjne, w tym zarządzanie globalną bazą użytkowników i nadzorowanie stanu wszystkich zintegrowanych instalacji alarmowych. Informacje zbierane są na bieżąco, dzięki czemu reakcja np. na alarmy czy awarie może mieć miejsce zaraz po ich wystąpieniu. Istotną cechą INTEGRUM jest skalowalność – w każdej chwili do systemu można dołączać kolejne centrale alarmowe.

ZAAWANSOWANA KONTROLA DOSTĘPU

ACCO NET to rozwiązanie przeznaczone zarówno dla podmiotów o zwartej strukturze (pojedynczy obiekt), jak i rozproszonych terytorialnie organizacji wielooddziałowych. System można wygodnie obsługiwać, wykorzystując aplikację ACCO Web dostępną poprzez przeglądarkę internetową, zarówno z urządzeń stacjonarnych, jak i mobilnych, z dowolnego miejsca na świecie. Rozbudowana funkcjonalność, zaawansowane metody kontroli dostępu oraz możliwość elastycznego budowania i rozbudowywania struktury systemu to niewątpliwe zalety ACCO NET.

INTEGRACJA SKD Z SSWIN

Główną zaletą integracji ACCO NET z centralami serii INTEGRA i INTEGRA Plus jest możliwość efektywnego i wygodnego jednoczesnego sterowania obydwoma systemami (ich powiązanymi strefami). Przykładowo użytkownik, uzyskując dostęp do pomieszczenia, rozbroi czuwający tam system alarmowy. Analogicznie, załączając czuwanie SSWiN, można zablokować przejścia (zaryglować drzwi) przypisane do zintegrowanej strefy SKD. W ramach integracji operator systemu ACCO NET zyskuje dostęp do wspólnej listy zdarzeń, ma też wgląd w stan wejść i wyjść central alarmowych. W efekcie obsługa i nadzór nad współpracującymi ze sobą instalacjami zabezpieczeń są wygodniejsze, bardziej przejrzyste, a przede wszystkim niezwykle wydajne (również ekonomicznie).

SYGNALIZACJA ZAGROŻENIA POŻAROWEGO

W budynkach biurowych o nieskomplikowanym układzie pomieszczeń można wykorzystać CSP – konwencjonalny system sygnalizacji pożarowej spełniający wymagania europejskich norm EN 54. Do central serii CSP-100 i CSP-200 można podłączyć szereg urządzeń sygnalizacji zagrożenia pożarowego, dzięki czemu system ten zapewnia skuteczne ostrzeganie o niebezpieczeństwie. Dostępne są także inne urządzenia niezbędne w SSP, takie jak ręczne ostrzegacze pożarowe (wewnętrzne i zewnętrzne), czujki dymu, ciepła oraz wielosensorowe.

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

Analiza wizji w transporcie publicznym

Praktyczne wskazówki dotyczące poprawnego wdrożenia

a&s Polska

Analiza zawartości obrazu (VCA) stała się już integralną częścią systemów dozoru wizyjnego stosowanych w różnych branżach. W transporcie zbiorowym jej implementacja przebiegała nieco wolniej ze względu na specyficzne trudności z wdrożeniem. Obecnie coraz więcej menedżerów zarządzających tą gałęzią gospodarki rozważa możliwość wykorzystania analizy wizyjnej do proaktywnego zapewniania bezpieczeństwa pasażerom i załodze, a także uzyskania dodatkowych korzyści biznesowych płynących z analizy przetworzonych danych.

Czym się należy kierować, aby wybrać odpowiednie rozwiązanie? Poprosiliśmy ekspertów branżowych o podzielenie się swoją wiedzą na temat najlepszych praktyk zastosowania automatycznej analizy wizyjnej w transporcie publicznym.

KLUCZOWA JEST JAKOŚĆ OBRAZU

Wybór odpowiedniego rozwiązania dostosowanego do pracy w środku transportu publicznego nie jest zadaniem łatwym. Powodem tego są m.in. szybko zmieniające się sceny i warunki oświetlenia, będące naturalną konsekwencją ruchu pojazdów. Ostre światło pojawia się na przemian z cieniami. Dla algorytmów analizujących obrazy z kamer są to warunki ekstremalnie trudne, co w efekcie wpływa na dużą liczbę zdarzeń alarmowych błędnie zaliczanych jako pozytywne.

Szybki postęp w dziedzinie przetwarzania obrazu zapewnił w ostatnim czasie sporo nowych rozwiązań, które wykazują większą odporność na zmienne warunki oświetlenia. Poprawia się jakość uzyskiwanych obrazów, zatem i dane dostarczane do analizy są lepszej jakości. – *Kamery muszą zapewniać wyraźny obraz, być w stanie generować wiele strumieni wideo jednocześnie, aby materiał mógł być efektywnie wykorzystany przez algorytmy analizy wizyjnej* – zaznacza Jakub Kozak z Genetec. I dodaje: – *Oprócz wyboru właściwego modelu kamery, bardzo ważny jest też wybór odpowiedniego miejsca montażu.*

Na istotny aspekt – miejsce montażu – zwraca również uwagę Piotr Świder z Hikvision Poland: *Należy też sprawdzić, jakie są wymogi względem pola widzenia kamery, aby ograniczyć tzw. martwe strefy. Wtedy zastosowana analityka obejmie cały pojazd i będzie bardziej skuteczna.*

Aby wyniki analizy były zgodne z potrzebami i oczekiwaniami, ważne jest uzyskanie szczegółowego i ostrego obrazu. Istnieje poważne ryzyko, że na obrazach z kamer zamontowanych w pojazdach obiekty w ruchu będą rozmyte, co osłabi skuteczność analizy. Kluczowe w tym przypadku są możliwości kamer i ich prawidłowa konfiguracja, m.in. parametryzacja kompresji obrazu czy ustawień naświetlania, zapewniające utrzymanie wysokiej jakości obrazu. Jednak zazwyczaj te dane nie są podawane w kartach katalogowych produktów.
– *Dlatego zawsze zalecamy testy porównawcze różnych technologii w rzeczywistych warunkach pracy. Dopiero na podstawie takich testów można wychwycić różnice pomiędzy urządzeniami i wskazać te, które rzeczywiście odpowiadają naszym potrzebom* – podkreśla Karol Dominiczak z Axis Communications.

PARAMETRY TECHNICZNE I WYBÓR TECHNOLOGII

Kamery stosowane w taborze są narażone na ciągłe silne wibracje. Urządzenia zamontowane na zewnątrz pojazdów wystawione są ponadto na działanie deszczu lub mrozu, śniegu i soli w zimie. Powinny być to specjalnie zaprojektowane konstrukcje, które poradzą sobie z tak trudnymi warunkami pracy. Na przykład kamery instalowane w taborze kolejowym powinny być wykonane zgodnie z rygorystycznymi wymaganiami normy PN-EN 50155, co będzie gwarancją, że spełniają najwyższe standardy i zostały przetestowane w trudnych warunkach wibracji i przeciążeń, a użytkowanie w pojazdach nie obniży ich trwałości.

Przykładem zachodzących zmian w urządzeniach stosowanych w transporcie są kamery z mechanicznym filtrem, które pojawiły się stosunkowo niedawno, gdy technologia pozwoliła na zagwarantowanie odporności na udary. Innym przykładem jest wykorzystanie urządzeń pracujących w paśmie średniej podczerwieni.

Jak mówi Jakub Sobek z Linc Polska: – *Technologia termowizyjna pozwala na skuteczną detekcję obiektów zarówno w ciągu dnia, jak i nocy, niezależnie od warunków oświetlenia. Trudne warunki atmosferyczne, takie jak mgła czy deszcz, nie stanowią dla niej problemu. Termowizja w połączeniu z analizą wizyjną może ostrzegać kierowców np. o osobie znajdującej się na poboczu lub zwierzętach przy drodze. Dzięki temu mogą dostosować prędkość pojazdu do sytuacji. Ponieważ obraz z kamery termowizyjnej pozwala na lepsze odseparowanie obiektów od tła, zaimplementowana analiza wizyjna osiąga znacznie wyższą dokładność i skuteczność.*

CORAZ WIĘCEJ MENEDŻERÓW ROZWAŻA MOŻLIWOŚĆ WYKORZYSTANIA ANALIZY WIZYJNEJ NIE TYLKO DO PROAKTYWNEGO ZAPEWNIANIA BEZPIECZEŃSTWA PASAŻEROM I ZAŁODZE, ALE TAKŻE DO UZYSKANIA DODATKOWYCH KORZYŚCI BIZNESOWYCH PŁYNĄCYCH Z ANALIZY PRZETWORZONYCH DANYCH

Jakub Sobek wskazuje również na wpływ technologii rozwijanej w branży transportowej na branżę zabezpieczeń technicznych. – *Zastosowanie radarów w transporcie wpłynęło na obniżenie cen ich produkcji. Rynek motoryzacyjny także pozwolił na zebranie wielu nowych doświadczeń, które umożliwiły znaczne udoskonalenia wielu rozwiązań To w efekcie spopularyzowało rozwiązania radarowe w ochronie obiektów stacjonarnych* – podkreślił.

OKREŚLENIE CELU ANALIZY

Liczba potencjalnych rozwiązań jest duża, a właściwy dobór technologii i urządzeń znacząco wpływa na wyniki analizy. Marcin Walczuk z firmy BCS zdradza pewien klucz, którym należy się posługiwać przy wyborze: – *Należy dobierać urządzenia zaprojektowane do konkretnego celu. Jeśli kamera ma zliczać pasażerów, to najlepiej sprawdzi się model do tego celu przeznaczony.*

Zdefiniowanie typów wykrywanych incydentów oraz warunków środowiskowych będzie determinowało wybór konkretnego rozwiązania. To z kolei wpłynie na sposób obróbki materiału wizyjnego oraz wynikające z tego zapotrzebowanie na moc obliczeniową i pamięć. Analiza wymagająca dużej mocy obliczeniowej będzie potrzebowała wydajnych jednostek serwerowych, na które trzeba znaleźć miejsce i którym trzeba zapewnić odpowiednie zasilanie w pojeździe. Może to stanowić wyzwanie – konieczność stosowania urządzeń odpornych na wibracje oznacza dodatkowe koszty.

Z kolei, jeśli analiza materiału wizyjnego ma się odbywać np. w chmurze, należy zapewnić sprawny transfer materiału wideo z pojazdu. Kluczowe stają się odpowiednia przepustowość i stabilność łącza, a to wszystko przekłada się na większe koszty systemu. Sposobem na ich obniżenie może być skuteczna kompresja obrazu oraz docelowa lub częściowa analiza materiału realizowana w kamerach, na co wskazuje Karol Dominiczak: – *Jeśli analizujemy obraz lokalnie, system będzie wydajniejszy, nie będzie wymagał nakładów na duże transfery danych i centralną moc obliczenio-*

wą. Warto więc zainwestować nieco więcej w kamery o wyższej mocy obliczeniowej, by zaoszczędzić w innych miejscach. Takie rozwiązanie będzie też mniej narażone na zerwanie połączenia, niespójność danych itp., bo cała praca jest wykonana lokalnie. Wadą takiego podejścia jest wciąż ograniczona moc obliczeniowa pojedynczej kamery, choć pojawiają się już bardzo wydajne urządzenia, zdolne obsłużyć nawet algorytmy sztucznej inteligencji.
I, jak zaznacza, zakres wybranych rozwiązań będzie zdeterminowany przez cel analizy materiału. – *Drogę do podjęcia decyzji, które rozwiązanie będzie dla nas najlepsze, rozpocząłbym od analizy wyzwań, wyznaczenia celów i odpowiedzi na pytanie: ile mogłoby kosztować nierozwiązanie naszego problemu* – radzi Karol Dominiczak.

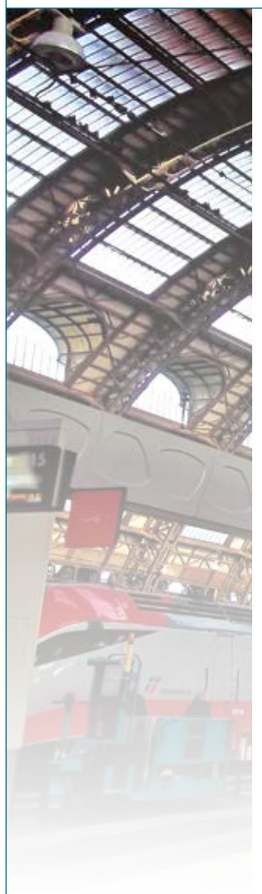
A Marcin Walczuk dopowiada: – *Powinniśmy się zastanowić, czy ma być to analiza statystyczna, np. zliczanie pasażerów w pojeździe, podróżnych na danej trasie. Czy może zależy nam na analizie bardziej ukierunkowanej na bezpieczeństwo pasażerów, zabezpieczenie samego środka transportu.*

Na korzyści z wykorzystania VCA zwraca uwagę Jakub Sobek, który zgadza się, że jednym z najważniejszych czynników powinna być skuteczność działania samej analizy wizyjnej. – *Niestety, nie zawsze informacje podawane przez producentów są obiektywne. Warto więc zwracać uwagę na łatwość adaptacji danego rozwiązania w określonym środku transportu i możliwość jego integracji z innymi systemami w pojeździe. Prawidłowa współpraca kilku różnych systemów daje najlepsze rezultaty.*

PRYWATNOŚĆ

W latach 2017-2030 europejski rynek IoT ma wzrosnąć o ponad 18%, a największą część tego rynku (23%) stanowi segment transportu i logistyki*. Urządzenia Internetu Rzeczy oferują niezrównane możliwości, zapewniając bezpieczeństwo pasażerom, efektywniejsze monitorowanie np. sieci kolejowych oraz znalezienie nowych obszarów optymalizacji usług i kosztów. Wszystko to dzięki skuteczniejszej analizie danych, w tym danych wizyjnych.

Jakub Kozak zwraca w tym miejscu uwagę na konieczność poszanowania prywatności osób: – *Bardzo ważne jest, aby wybrany dostawca funkcji analitycznych zapewnił ochronę sfery prywatności obywateli i zagwarantował tylko uprawniony dostęp do ich danych osobowych*. Piotr Świder precyzuje, że większość wdrożeń analizy w transporcie publicznym dotyczy prostych algorytmów, takich jak detekcja ruchu czy wykrycie manipulacji lub zasłonięcia kamery i nie narusza prywatności pasażerów lub pracowników. – *Często potrzeby firm transportowych są bardziej złożone. Przykładowo oczekują analizy zachowania kierowcy czy detekcji rozmów przez telefon* – przyznaje.



OTWARTOŚĆ

Przy wyborze odpowiedniego rozwiązania kluczowe znaczenie ma elastyczność w podejściu, ponieważ rozwijające się technologie, takie jak Internet Rzeczy i sztuczna inteligencja ewoluują i wymuszają współpracę urządzeń z wykorzystaniem ustandaryzowanych protokołów komunikacyjnych. – *Rozwiązania technologiczne bez wymaganej elastyczności umożliwiającej uwzględnienie pojawiających się nowości mogą stanowić problem, dlatego staramy się pomagać naszym klientom, zapewniając im prawdziwie otwartą platformę do zarządzania danymi z systemu dozoru wizyjnego i innych czujników. Ponieważ platforma jest otwarta, można do niej dodawać kolejne aplikacje w miarę pojawiania się nowych rozwiązań* – zwraca uwagę Borislava Kenarova z Milestone Systems.

Z kolei Jakub Kozak doradza: – *Wybór ujednoliconej otwartej platformy do zarządzania materiałem wizyjnym z całej floty pojazdów, przystanków, stacji i zajezdni, która połączy potrzeby agencji i operatorów transportowych*. Możliwość przetworzenia wyników analizy wideo i korelacja ich z danymi z innych czujników zapewni pełny wgląd operacyjny i wesprze podejmowanie właściwych decyzji przez menedżerów branży. Na korzyści z takiego podejścia wskazuje Karol Dominiczak: – *Jeżeli potrafimy skutecznie policzyć podróżujących, a do tego jeszcze określić, gdzie wsiedli, gdzie wysiedli, możemy bardzo precyzyjnie reagować na sytuacje nadzwyczajne, a także dopasować częstotliwość kursowania środków komunikacji do faktycznych potrzeb pasażerów. A to szybko przełoży się na ich zadowolenie oraz obniżenie kosztów eksploatacyjnych i zużycie paliw.*

* „Bezpieczeństwo transportu publicznego w erze smart city", Milestone Systems, 2021

RACS 5 v2.0

Nowa odsłona polskiego systemu kontroli dostępu klasy Enterprise

W ramach ciągłego rozwoju oferty i podążania za oczekiwaniami rynku firma Roger wprowadza do oferty kolejną wersję systemu kontroli dostępu i automatyki budynkowej RACS 5 v2.0. W tej wersji możliwości systemu zostały rozbudowane m.in. o bezpieczną obsługę systemów rozproszonych terytorialnie, integracje z systemami serwerowych systemów windowych, a także z kolejnymi systemami zarządzania bezpieczeństwem obiektów (SMS/PSIM/VMS) i platformami zarządzania biurowcem.

W wersji 2.0 wprowadzono ponadto długo wyczekiwaną przez klientów funkcję globalnego *anti-passback* oraz rozbudowano moduł monitorowania graficznego na planach obiektu (tzw. mapy). Nowa wersja systemu oferuje integrację z usługami katalogowymi (LDAP), dzięki której możliwe jest automatyczne synchronizowanie użytkowników systemu z zewnętrzną bazą danych użytkowników, w tym za pośrednictwem usługi Active Directory.

OBSŁUGA SYSTEMÓW ROZPROSZONYCH TERYTORIALNIE

System RACS 5 v2.0 umożliwia obsługę systemów kontroli dostępu złożonych z wielu rozproszonych terytorialnie podsystemów. W tym scenariuszu instalacji lokalne podsystemy są wyposażane we własny serwer komunikacyjny, który korzystając z bezpiecznego połączenia transmisji danych (TLS), komunikuje się przez sieć WAN z centralnym serwerem systemu. W przypadku utraty komunikacji lokalnego serwera komunikacyjnego z serwerem centralnym praca systemu jest kontynuowana zgodnie z konfiguracją, a zdarzenia są buforowane w pamięci kontrolerów. Po powrocie komunikacji pomiędzy serwerem lokalnym a serwerem centralnym zbuforowane w kontrolerach zdarzenia są automatycznie pobierane na serwer centralny.

WSPÓŁPRACA Z SYSTEMAMI WINDOWYMI

Nowa wersja systemu oferuje pełną programową integrację z wiodącymi dostawcami systemów windowych, w tym KONE Access i Schindler Port. Integracja ta pozwala zarządzać uprawnieniami użytkowników do poruszania się pomiędzy wybranymi piętrami budynku z poziomu oprogramowania systemu kontroli dostępu, a także określać zasady przydziału wind specjalnych, gdy takie windy są stosowane w budynku. W obiektach korzystających z wind klasycznych bazujących na panelu przycisków wyboru piętra możliwa jest integracja sprzętowa.

WIZUALIZACJA NA MAPACH OBIEKTU

W systemie RACS 5 v2.0 został ulepszony i rozbudowany moduł Map, który umożliwia wizualizację i nadzorowanie pracy systemu w trybie graficznym. Moduł rozbudowano o możliwość powiększania, pomniejszania i przesuwania obrazu, możliwa jest konfiguracja elementów mapy, obsługa wybranych grafik wektorowych oraz definiowanie zestawu map w układzie hierarchicznym. Nową wersję uzupełniono o możliwość wyświetlania w czasie rzeczywistym liczby osób znajdujących się w kontrolowanych strefach. Wizualizacja obejmuje zarówno system kontroli dostępu, jak i zintegrowane z nim systemy CCTV (Dahua, Hikvision, BCS, ONVIF) oraz SSWiN (INTEGRA, Galaxy).
Moduł Map jest jednym z ciągle rozwijanych elementów systemu i dlatego w niedalekiej przyszłości zostanie on poszerzony o wizualizację wiodących systemów sygnalizacji pożarowej.

INTEGRACJE Z SYSTEMAMI ZARZĄDZANIA BEZPIECZEŃSTWEM

W przypadku obiektów wymagających szerszego zakresu integracji system RACS 5 v2.0 oferuje możliwość współpracy ze zintegrowanymi systemami zarządzania bezpieczeństwem (SMS i PSIM), systemami zarządzania wideo (VMS) oraz systemami zarządzania budynkiem (BMS).
W ramach zrealizowanych projektów została wdrożona współpraca m.in. z systemami: WinGuard (Advancis), Axxon Intellect Enterprise (AxxonSoft), XProtect (Milestone), ARGUS RV (Telbud), NetStation Enterprise (Alnet Systems), GANZ CORTROL (CBC), Luxriot EVO (Luxriot), VIZAN SMS (Sprint), Nazca (APA Group). Powyższe integracje zostały zrealizowane za pośrednictwem tzw. Serwera Integracji, który umożliwia dostęp do bazy danych systemu oraz wykonywanie czynności związanych z bieżącą obsługą systemu, a w szczególności zarządzanie użytkownikami oraz wydawanie zdalnych poleceń.
Wykorzystanie Serwera Integracji umożliwia współpracę systemu kontroli dostępu z dowolnym zewnętrznym systemem informatycznym (np. system ERP, system zarządzania budynkiem, system hotelowy itp.).

INTEGRACJA Z DEPOZYTORAMI KLUCZY RKD32

System kontroli obiegu kluczy, w którego skład wchodzą elektroniczne depozytory kluczy RKD32, pozwala na ograniczenie dostępu osób do kluczy oraz zapewnia pełną rejestrację zdarzeń związanych z ich obiegiem. Depozytory RKD32 mogą pracować w trybie autonomicznym, niezależnie od innych systemów zainstalowanych w obiekcie. Decydując się na zastosowanie systemu kontroli obiegu kluczy, warto rozważyć jego integrację z obecnymi w obiekcie systemami bezpieczeństwa, w szczególności z systemem kontroli dostępu.
System RACS 5 v2.0 oferuje pełną bazodanową integrację z depozytorami kluczy RKD32, co pozwala na zarządzanie systemem kontroli dostępu i depozytorami z poziomu jednego programu nadzorczego (VISO). Integracja umożliwia tworzenie różnych raportów i wykorzystanie wartościowych funkcji. Jedną z takich funkcji jest możliwość zablokowania wyjścia z obiektu użytkownikowi, który nie zwrócił klucza pobranego wcześniej z depozytora.

INTEGRACJE Z PLATFORMAMI DO OBSŁUGI BIUROWCÓW

Przy użyciu wspomnianego wcześniej Serwera Integracji zrealizowano również integracje z platformami dostarczającymi zaawansowane rozwiązania dla biurowców. Nawiązanie współpracy firmy Roger z dostawcami tego typu rozwiązań (IU Technology, Zonifero) pozwoliło na wykorzystanie bazy danych systemu kontroli dostępu RACS 5 v2.0 na potrzeby obsługi wirtualnej recepcji, systemu rezerwacji sal, rezerwacji biurek czy systemu do zarządzania podwykonawcami.
System RACS 5 v2.0 pozwala na identyfikację użytkowników korzystających z urządzeń mobilnych (Android, iOS), która może być realizowana w technologii NFC *(Near Field Communication)*, BLE *(Bluetooth Low Energy)* oraz QR Code. W ramach nawiązanej współpracy firma Roger udostępniła możliwość stosowania identyfikatorów mobilnych w aplikacjach do obsługi biurowców. W praktyce oznacza to, że użytkownicy korzystający z tych platform mogą uzyskiwać dostęp do pomieszczeń z poziomu mobilnej aplikacji budynkowej wykorzystywanej w danym obiekcie.

UPROSZCZONY INTERFEJS DODAWANIA UŻYTKOWNIKÓW I SZYBSZA KONFIGURACJA

Aby maksymalnie usprawnić codzienną obsługę systemu, w nowej wersji dodawanie nowego użytkownika jest wykonywane z poziomu jednego okna, które zawiera wszystkie wymagane do tego celu dane. Dzięki wprowadzonej optymalizacji procesu przesyłania ustawień do kontrolerów czas synchronizacji systemu został znacznie skrócony. Nowe oprogramowanie będzie dostępne w wersji 64-bit., co przyczyni się do znacznej poprawy komfortu pracy z aplikacją VISO.

PODSUMOWANIE

Rosnące potrzeby rynku projektowego są wyznacznikiem kierunków rozwoju systemu RACS 5. Mając na uwadze wymagania stawiane przez inwestorów, inżynierowie firmy Roger starają się im sprostać i dostarczyć produkt realizujący ich oczekiwania. Zachęcamy do wizyty na stronę www.roger.pl, gdzie na bieżąco udostępniane są informacje o nowych funkcjonalnościach pojawiających się w systemie.

ROGER
Gościszewo 59, 82-400
Sztum
www.roger.pl

Rozszerzanie funkcjonalności kamer

ponad aplikacje security

W ciągu ostatniej dekady kamery z urządzeń służących do rejestracji obrazu przeistoczyły się w kompletne sensory. Generowane przez nie dane mogą być wykorzystywane w wielu aplikacjach, dzięki czemu użytkownik może czerpać znacznie większe korzyści w porównaniu do klasycznego systemu monitoringu wizyjnego.

Michał Małek

Regionalny kierownik sprzedaży systemów wideo

Firma Bosch rozwija zaawansowane algorytmy analizy obrazu od wielu lat, a od 2016 roku wprowadza je jako standard do wszystkich modeli kamer IP. Klient końcowy może dzięki temu mieć pewność, że skuteczność detekcji wykroczeń jest na najwyższym poziomie. Jednocześnie te same urządzenia biorą udział w zbieraniu metadanych wspierających działania biznesowe i redukcję kosztów przedsiębiorstwa oraz w zarządzaniu przestrzenią. Dzięki możliwości jednoczesnego zbierana danych z wielu kamer instalacja zaczyna pełnić funkcję ekosystemu dbającego nie tylko o bezpieczeństwo, ale też o komercyjną stronę inwestycji.

Zaawansowane algorytmy analizy obrazu pozwalają operatorowi systemu skupić się na najważniejszych zdarzeniach. Umożliwiają również tworzenie własnych reguł i akcji, które sprawiają, że system wymaga znacznie ograniczonej obsługi osób ochrony. Najnowsze modele kamer Bosch zapewniają kombinację odpowiednio skonfigurowanych reguł. W połączeniu z uczeniem głębokim (sieci neuronowe) urządzenia „uczą się" sceny, oferując wiele możliwości, np. mierzenie odległości pomiędzy ludźmi, detekcję maseczek czy kasków ochronnych. Potencjalnych aplikacji z zastosowaniem analizy obrazu jest bardzo dużo, a ograniczenia techniczne powoli przestają być problemem.

Kiedy mówimy o przyszłości i ciekawych obszarach zastosowań dla inteligentnych kamer, wydaje się oczywiste, że producenci urządzeń nie powinni być osamotnieni w rozwoju nowych aplikacji. Wręcz przeciwnie, bardziej zasadne jest tworzenie bezpiecznego środowiska dla zewnętrznych deweloperów, którzy wykorzystując platformy sprzętowe najwyższej klasy, mogą rozwiązywać nieskończoną ilość problemów życia codziennego.

Świetnym przykładem jest rynek smartfonów. Czołowi producenci udostępniają szereg narzędzi programistycznych, dzięki czemu użytkownicy za pośrednictwem dedykowanych sklepów są w stanie instalować aplikacje mobilne, tworzące z nich urządzenia potężne do pracy i rozrywki.

W roku 2018 Bosch zdecydował się na utworzenie start-upu o nazwie OSSA (Open Security & Safety Alliance), który zrzesza dziś już ponad 40 producentów technologii, w tym czołowych dostawców kamer. W ramach organizacji udało się zbudować pierwsze „otwarte" urządzenia oraz API *(Application Programming Interface)*, dzięki

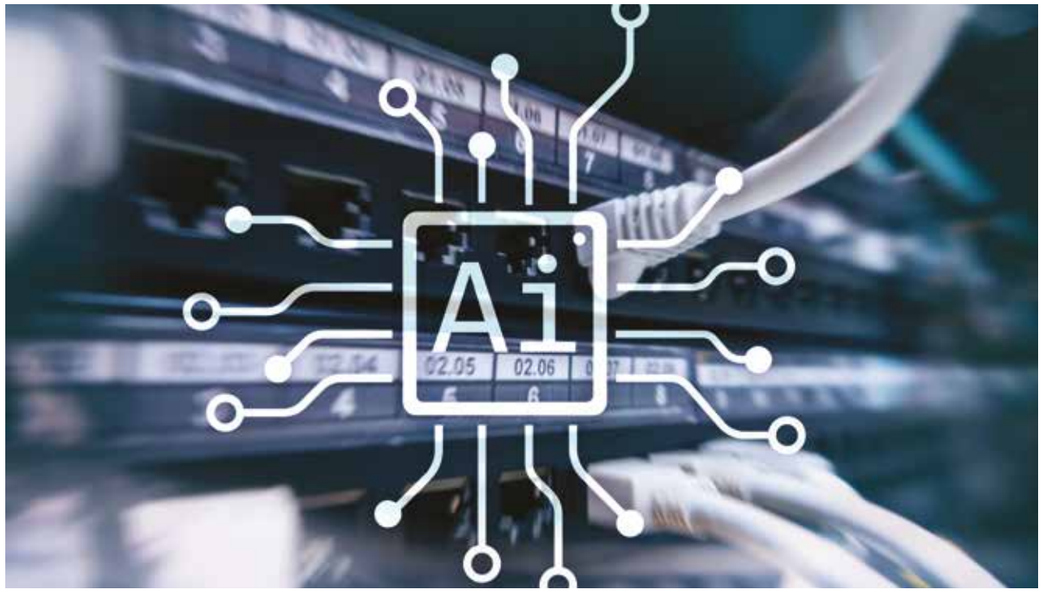
czemu deweloperzy są w stanie tworzyć aplikacje współpracujące z zaawansowanymi kamerami. Dodatkowo klient – podobnie jak w przypadku rynku smartfonów – ma dostęp do internetowego sklepu, w którym może wybierać spośród wielu aplikacji, tworząc ze swoich kamer sensory IoT wykraczające poza klasyczne aplikacje bezpieczeństwa.

W tym roku Bosch wprowadza na rynek kilka modeli kamer z platformą INTEOX, która umożliwia deweloperom aplikacji i integratorom systemów zabezpieczeń korzystanie z wbudowanej inteligencji oraz tworzenie nieograniczonej liczby aplikacji opartych na powszechnie używanym języku programowania. Równocześnie integratorzy systemów mogą personalizować systemy, aby dostosować je do potrzeb klienta poprzez dodawanie aplikacji oraz instalowanie ich w kamerach INTEOX.

Co więcej, wszystkie kamery zapewniają najwyższy poziom bezpieczeństwa danych. Oznacza to, że nie jest możliwe zainstalowanie oprogramowania, które nie zostało przetestowane, ani użycie kamer w nieodpowiedni sposób. Również wyciek wrażliwych danych został ograniczony do minimum.

BOSCH SECURITY AND SAFETY SYSTEMS

www.boschsecurity.com/pl/pl/



Nowe możliwości

dla branży ochrony z zasilaczem Ajax

Według raportu firmy Grand View Research Inc. globalny rynek usług związanych z bezpieczeństwem przekroczy do 2025 r. wartość 167 mld dolarów. Setki tysięcy agencji ochrony i instalatorów poszukują niszy rynkowej.

Konkurencja wymusza poszukiwanie nowych segmentów rynku, a jednym z nich może być ochrona w pomieszczeniach, gdzie zasilanie jest słabe, niestabilne lub w ogóle go brakuje. Domy na kółkach, vany i jachty potrzebują ochrony nie mniej niż inne posesje. Puste domy są wystawione na łup szabrowników i dzikich lokatorów, a przecież zdarzają się też włamania, pożary czy wycieki gazu.
Moduły zasilające Ajax 12V PSU i Ajax 6V PSU umożliwiają podłączenie centrali alarmowej (CPU) do źródła zasilania o niskim napięciu, zapewniając ochronę posesji na wiele lat – brak dostępu do sieci elektroenergetycznej nie stanowi już problemu. Otwiera to nowe możliwości w zakresie świadczenia usług ochrony.

DO CZEGO SŁUŻY SYSTEM ALARMOWY?

System alarmowy Ajax odstrasza złodziei, wykrywa pożar, zapobiega zalaniu i steruje urządzeniami AGD. Mobilna aplikacja natychmiast informuje użytkownika i agencję ochrony o zagrożeniu, a weryfikacja fotograficzna pokazuje, co się stało. Wykrywa próby zagłuszenia transmisji i jest odporny na zakłócenia oraz hakowanie. Wystarczy smartfon, aby kontrolować zarówno małe pomieszczenia, jak i obszary wielkości kilku boisk do piłki nożnej.

DO CZEGO SŁUŻĄ MODUŁY ZASILANIA 12V PSU I 6V PSU?

Dzięki nim funkcje systemu Ajax są dostępne w miejscach, w których nie doprowadzono elektryczności lub gdzie zasilanie jest niestabilne.
Moduły 12V PSU i 6V PSU umożliwiają podłączenie huba, czyli centrali alarmowej systemu, do źródła zasilania o niskim napięciu (4,2–16 V dla 6V PSU; 8–20 V dla 12V PSU) i korzystanie z zewnętrznych źródeł zasilania. Moduł zasilający instaluje się w obudowie centrali zamiast fabrycznego zasilacza 110/230 V.

PUSTE POSESJE

Niezamieszkane nieruchomości w posiadaniu klienta. Dom letni bez elektryczności, zamknięty na zimę. Wstrzymana budowa. Czynny plac budowy bez najemców, który już wymaga ochrony obszaru, materiałów budowlanych i sprzętu. Puste domy zajęte przez dzikich lokatorów – tego rodzaju posesje przyciągają uwagę wandali, włamywaczy i włóczęgów.
Grabieże, pożary i wandalizm to niejedyne problemy, które mogą się zdarzyć. Wycieki gazu prowadzą do ogromnych kosztów i zniszczeń na skutek eksplozji czy zalania podczas gaszenia.
Instalacja systemu Ajax może ochronić nieruchomość i zaoszczędzić właścicielom wielu problemów. Po podłączeniu do zewnętrznej baterii za pośrednictwem modułu 6V PSU hub zgłosi zagrożenia. Czujka ruchu MotionCam z fotograficzną weryfikacją alarmów wykonuje serię zdjęć, które umożliwiają właściwą ocenę sytuacji. Z kolei czujka LeaksProtect wykrywa i zgłasza wycieki. Fabrycznie zainstalowane baterie zasilają urządzenie do 7 lat (w zależności od typu urządzenia i ustawień).
Dzięki Ajax właściciel przy minimalnym wysiłku zyskuje ciągłe monitorowanie obiektu na wiele lat.

MAGAZYNY

Moduły zasilania umożliwiają podłączenie huba i podwajaczy zasięgu ReX do źródeł zasilania o niskim napięciu lub zasilania bateryjnego. Podłączając pięć urządzeń ReX do systemu, zasięg radiowy można zwiększyć do 35 km² – to więcej niż dwa lotniska Heathrow. Utrzymanie kontroli nad magazynami tej wielkości staje się proste, nawet jeśli na miejscu nie ma dostępu do zasilania.

DOMY NA KÓŁKACH

Rynek kamperów i sprzętu kempingowego rośnie w odpowiedzi na mobilny styl życia. Oczekuje się, że rozwinie się jeszcze bardziej, zwłaszcza biorąc pod uwagę boom na turystykę przygodową. Przewiduje się wzrost o 12% do 2025 r.
Vany i przyczepy rozszerzają listę usług możliwych do zaoferowania dzięki modułom zasilania 12V PSU i 6V PSU. Wystarczy, że instalator podłączy hub do akumulatora samochodowego, a system alarmowy wyruszy w podróż razem z kierowcą. Zazwyczaj hub zużywa mniej niż 100 mA, co oznacza, że standardowy akumulator samochodowy może zasilać go przez 1–2 miesiące bez konieczności doładowania. Możliwość konfiguracji scenariuszy daje zupełnie nowy poziom ochrony.

W reakcji na zdarzenie (np. włamanie) odpowiednie polecenie natychmiast uruchomi generator mgły.

JACHTY

Wystarczy włożyć kartę SIM i podłączyć hub do instalacji pokładowej lub baterii, aby system Ajax zapewnił ochronę cumującego jachtu.
Zagrożenie związane z nieproszonymi gośćmi dotyczy nie tylko ryzyka dla osób na pokładzie, ale również drogiej elektroniki, sprzętu i łodzi. Ubezpieczenia to świetna inwestycja, ale niejedyna. Profesjonalny system alarmowy jest lepszy i tańszy.

WNIOSKI

Inteligentne systemy alarmowe reagują na zagrożenia, a inteligentne agencje ochrony reagują na zmiany rynkowe i poszukują możliwości wyjścia na pozycję lidera na niezwykle konkurencyjnym rynku. Moduły zasilania Ajax 12V PSU i 6V PSU są nie tylko łatwe w użyciu, ale otwierają również nowe perspektywy biznesowe dla sprzedawców i instalatorów systemów alarmowych.

FPM+ Centrala sterująca

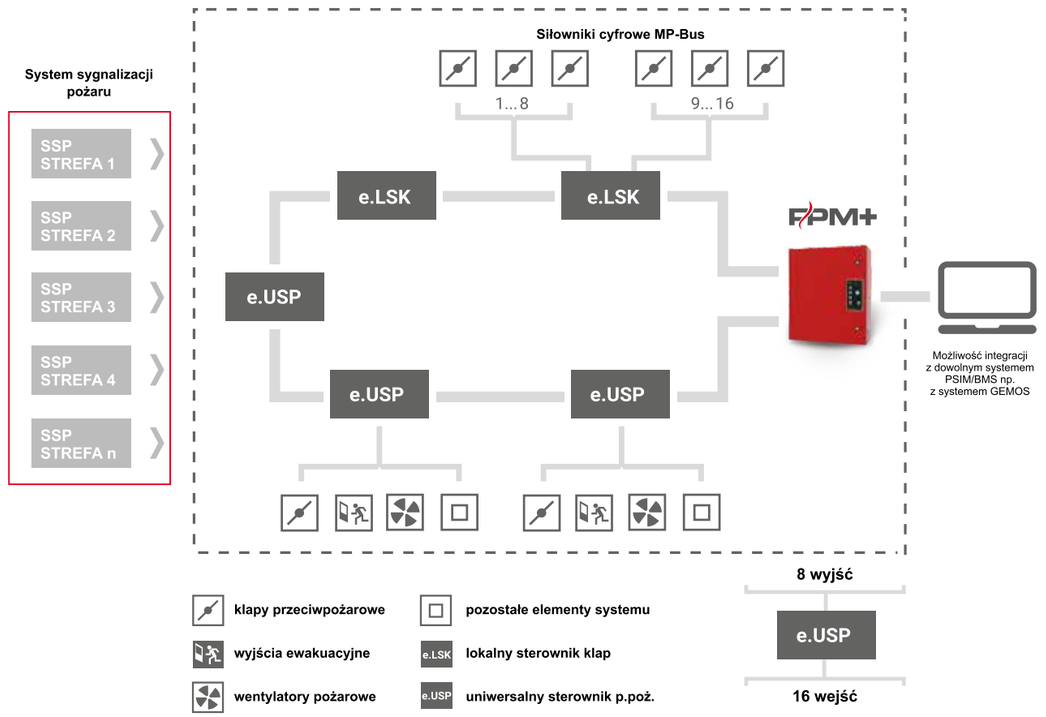
urządzeniami przeciwpożarowymi

W obszarze przeciwpożarowym branża zabezpieczeń spotyka się z wieloma wyzwaniami. Zmiany w prawie budowlanym, brak wzajemnej interakcji pomiędzy systemami, rosnące koszty ochrony fizycznej to tylko niektóre z nich. Wielu zarządców obiektów boryka się ze zbyt długim czasem reakcji na zagrożenia, odstępstwami w projektach budowlanych czy koniecznością adaptacji scenariusza pożarowego.

W trakcie eksploatacji obiektu rzeczą oczywistą jest gromadzenie wszelkich informacji o stanie zintegrowanych, sterowanych i monitorowanych systemów, a także analiza potencjalnych słabych punktów i natychmiastowa informacja o wykrytych awariach i usterkach. Gromadzone dane można przetwarzać na wiele sposobów i przedstawiać je w najbardziej czytelnej formie. Dlatego w Ela-compil powstał i jest rozwijany FPM+, czyli *Fire Protection Manager* – nowoczesne środowisko zapewniające sterowanie wszystkimi urządzeniami przeciwpożarowymi, a także pozostałymi urządzeniami uwzględnianymi w scenariuszu pożarowym.
Elementami składowymi FPM+ są modułowa centrala sterująca, której zadaniem jest przejęcie sygnału alarmowego z systemu sygnalizacji pożarowej i wykonanie zaprogramowanych algorytmów sterowania, oraz program FireMATRIX, za pomocą którego można dowolnie konfigurować centralę FPM+. Program ten, oprócz konfigurowania centrali sterującej, umożliwia przeprowadzenie testów na dowolnym etapie instalacji. Jedną z wielu innowacji FireMATRIX jest funkcja generowania gotowych protokołów z przeprowadzonych testów.
Oprogramowanie FireMATRIX ułatwia instalowanie, uruchamianie i testowanie urządzeń ppoż. W trakcie eksploatacji obiektu często zdarza się, że konieczne są zmiany w matrycy sterowań (czyli pliku wykonawczym, w którym zapisano algorytmy sterowania). Taka potrzeba zachodzi, gdy np. pojawia się nowy najemca lub obiekt podlega zmianom architektonicznym. Dzięki zastosowaniu FPM+ wszystkie zmiany są dużo łatwiejsze, zwykle wystarczy zmiana parametrów w oprogramowaniu.
Ogromną zaletą jest fakt, że cały czas mamy aktualną dokumentację, w której znajdują się wyspecyfikowane wszystkie urządzenia przeciwpożarowe (w wielu obiektach do dzisiaj nie można się doliczyć takich urządzeń), ich stan w trakcie eksploatacji, a także podczas pożaru.

- FPM+ zapewnia kontrolę nad wszystkimi urządzeniami ze scenariusza pożarowego, zwiększając tym samym poziom bezpieczeństwa przeciwpożarowego budynku.
- FPM+ działa niezależnie od systemu wykrywania pożaru, co nie tylko poprawia bezpieczeństwo, ale zapewnia też szybki i tani odbiór całego systemu ppoż. Przy dużej liczbie urządzeń FPM+ odciąża centrale sygnalizacji pożaru, zapewniając bezpieczeństwo w dużych obiektach.
- FPM+ jest urządzeniem modułowym, przeznaczonym do sterowania i nadzorowania pracy urządzeń i systemów w obiekcie budowlanym, które będą uruchomione w razie zagrożenia pożarem. Umożliwia zbudowanie w krótkim czasie instalacji rozproszonej oraz łatwą rozbudowę systemu.
- FPM+ pozwala na zintegrowane zarządzanie urządzeniami różnych producentów, biorącymi udział w akcji ratowniczo-gaśniczej, takimi jak systemy wentylacji ppoż., systemy odcięć pożarowych, systemy wspomagające ewakuację itp.
- System FPM+, oprócz pełnej automatycznej pracy, umożliwia ręczne sterowanie scenariuszami.

Topologia Centrali FPM+



Centrala FPM+ jako jedna z pierwszych w Polsce została z powodzeniem przebadana i certyfikowana przez CNBOP-PIB i legitymuje się następującymi certyfikatami:

- Krajowa Deklaracja Właściwości Użytkowych nr 2020/B/FMP/01
- Krajowa Ocena Techniczna CNBOP-PIB nr CNBOP-PIB-KOT-2017/0028-1009 wydanie 4
- Krajowy Certyfikat Stałości Właściwości Użytkowych nr 063-UWB-0075
- Świadectwo Dopuszczenia 2088/2017

Zgodnie z Krajową Oceną Techniczną nr CNBOP-PIB-KOT-2017/0028-1009 wydanie 4 z dnia 14.V.2020 – centrala FPM+ nosi oficjalną nazwę „Urządzenie sterujące i sygnalizujące w systemach kontroli rozprzestrzeniania dymu i ciepła oraz sterowania gaszeniem – Centrala sterująca urządzeniami przeciwpożarowymi typu FPM plus (FPM+)". Jej funkcjonalność została powiększona o możliwość pracy sieciowej oraz o sterowanie gaszeniem, co zostało potwierdzone w dokumentach certyfikacyjnych.
Centrala sterowania urządzeniami przeciwpożarowymi FPM+ jest urządzeniem modułowym, przeznaczonym do nadzorowania stanu pracy oraz sterowania wszelkimi urządzeniami uruchamianymi podczas pożaru. Mogą to być systemy dedykowane do zastosowań ppoż., m.in.:

- systemy wentylacji pożarowej,
- systemy odcięć przeciwpożarowych,
- systemy gaszenia wodą,
- inne systemy budynkowe, które wskutek wystąpienia pożaru wykonują jakiekolwiek działanie.

Innymi systemami, które może nadzorować FPM+ są:

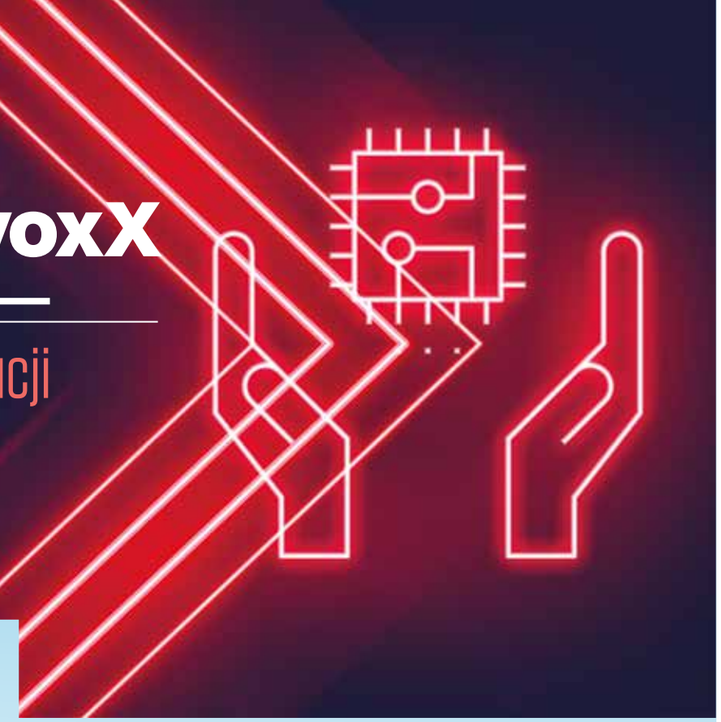
- system kontroli dostępu,
- system sygnalizacji włamania i napadu,
- schody ruchome,
- windy,
- systemy kontroli (odcięcia) mediów,
- pompy ciepła i systemy wentylacji i klimatyzacji.

FPM+ pozwala na stworzenie najbardziej skomplikowanych scenariuszy za pomocą jednej, wspólnej matrycy sterowań. Takie podejście pozwala wykluczyć większość błędów już na etapie projektowania, instalowania, a następnie uruchamiania instalacji bezpieczeństwa.
Modułowość systemu sprawia, że instalacja może zostać wykonana ponad dwukrotnie szybciej niż do tej pory. Dodatkowo centrala sterująca FPM+ jest kompatybilna z dowolnymi systemami SSP i BMS (w tym z systemem zarządzania obiektem GEMOS), może więc być bez obaw stosowana we wszelkiego rodzaju budynkach, w których systemy te są odpowiedzialne za komfort i bezpieczeństwo.
Centrala FPM+ dzięki stałemu nadzorowaniu funkcji obiektu znacznie ułatwia kontrolę nad wszelkimi urządzeniami i systemami przeciwpożarowymi, zwiększając tym samym poziom bezpieczeństwa budynków użyteczności publicznej oraz dużych obiektów. Rozwiązanie to perfekcyjnie sprawdzi się zatem we wszelkiego rodzaju obiektach. Tam, gdzie w grę wchodzi ochrona życia ludzkiego, nie może być mowy o kompromisowych rozwiązaniach.

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

Integral EvoxX

kolejny etap (r)ewolucji



Integral EvoxX to kolejny etap ewolucji systemu sygnalizacji pożarowej Integral oferowanego przez Schrack Seconet od 1996 r. Na każdym etapie jego rozwoju wprowadzane są nowe rozwiązania konstrukcyjne i funkcjonalne oraz kolejne udoskonalenia w zakresie niezawodności działania, funkcjonalności i elastyczności, oparte na nowościach technologicznych, a także zgodnie z obowiązującymi przepisami i wytycznymi.

Celem i misją Schrack Seconet jest zapewnienie maksymalnego poziomu bezpieczeństwa pożarowego we wszystkich rodzajach obiektów budowlanych. System Integral EvoxX to najnowsza platforma sprzętowa i programowa wspierająca rozwiązania chmurowe, przygotowana na dalszy rozwój systemu, szczególnie w zakresie technologii cyfrowych i współdziałania z innymi systemami bezpieczeństwa w obiekcie.

W RAMACH SYSTEMU INTEGRAL EVOXX DOSTĘPNE SĄ NASTĘPUJĄCE TYPY CENTRAL

- **Integral EvoxX M** – uniwersalna modułowa redundantna centrala:
  - sygnalizacji pożarowej,
  - sterująca urządzeniami przeciwpożarowymi, w tym sterowania urządzeniami w systemach kontroli rozprzestrzeniania dymu i ciepła,
  - sterująca stałymi urządzeniami gaśniczymi obejmującymi takie środki gaśnicze jak gaz, woda, piana, mgła i aerozole,
- **Integral EvoxX C** – 2(4) pętlowa kompaktowa centrala sygnalizacji pożarowej i jednostrefowa centrala sterująca stałymi urządzeniami gaśniczymi,
- **Integral EvoxX B** – jednopętlowa centrala sygnalizacji pożarowej.

UNIWERSALNA CENTRALA SYGNALIZACJI POŻAROWEJ I STEROWANIA URZĄDZENIAMI PPOŻ.

Flagowym produktem systemu jest centrala Integral EvoxX M, skonstruowana z naciskiem na maksymalne bezpieczeństwo, funkcjonalność i elastyczność, aby umożliwić realizację nawet najbardziej skomplikowanych zadań w zakresie sygnalizacji pożarowej i sterowania urządzeniami przeciwpożarowymi w obiekcie. Dla potwierdzenia najwyższych standardów bezpieczeństwa w CNBOP-PIB zostały wykonane dodatkowe badania w zakresie sterowania urządzeniami przeciwpożarowymi. Potwierdziły one w 100% spełnianie wymagań technicznych i formalnych, które są kluczowe dla bezpiecznego wdrożenia systemu w obiekcie, późniejszego formalnego odbioru instalacji i bezpiecznej eksploatacji. Centrala ma certyfikaty i świadectwa dopuszczenia CNBOP-PIB do realizacji następujących funkcji:

- centrala sygnalizacji pożarowej zgodnie z PN-EN 54-2,
- zasilacz urządzeń przeciwpożarowych zgodnie PN-EN 54-3,
- centrala sterująca urządzeniami przeciwpożarowymi w systemach kontroli rozprzestrzeniania dymu i ciepła (zgodnie z prEN 12101-9), centrala sterująca oddzieleniami przeciwpożarowymi oraz przeznaczona do sterowania i nadzorowania w ramach instalacji wodociągowych przeciwpożarowych zgodnie z Krajową Oceną Techniczną (KOT),
- zasilacz urządzeń przeciwpożarowych w systemach kontroli rozprzestrzeniania dymu i ciepła zgodnie z PN-EN 12101-10,
- centrala sterująca stałymi urządzeniami gaśniczymi gazowymi zgodnie z PN-EN 12094-1,
- centrala sterująca stałymi urządzeniami gaśniczymi wodnymi, pianowymi i aerozolowymi zgodnie z KOT.

Sterowanie bezpośrednie urządzeń przeciwpożarowych odbywa się za pomocą wejść/wyjść central oraz modułów wejścia/wyjścia w ramach techniki pętlowej X-LINE. **Centrala Integral EvoxX M, realizując wszystkie powyższe funkcje jednocześnie, staje się najbardziej uniwersalną centralą na rynku polskim.**
Architektura i elastyczność Integral EvoxX M umożliwiają realizację funkcji systemu sygnalizacji pożarowej (SSP) i sterowania urządzeniami ppoż. przez jedną centralę lub centrale pracujące w sieci. W ramach systemu sieciowego istnieje możliwość rozdzielania funkcji sygnalizacji pożarowej i sterowania na poszczególne centrale lub wyodrębnienia niezależnych podsystemów dla łatwiejszego zarządzania i eksploatacji, co jest praktykowane np. w zakresie systemu detekcji i sterowania SUG.

MAKSYMALNA SZYBKOŚĆ I NIEZAWODNOŚĆ DZIAŁANIA

Centrale Integral EvoxX są oparte na platformach sprzętowych nowej generacji (B8, B9, B10), zapewniających kolejne, znaczne zwiększenie wydajności systemu oraz wprowadzających nowe interfejsy wejścia/wyjścia, które ułatwiają obsługę, konfigurację i serwis, a także współdziałanie z systemami zewnętrznymi. Zastosowanie nowych bardzo wydajnych platform sprzętowych to realizacja długofalowej strategii Schrack Seconet budowy niezawodnych systemów bezpieczeństwa pożarowego o możliwościach wykraczających poza obowiązujące obecnie wymagania i standardy. Unowocześniona platforma jest przygotowana na nowe wyzwania w zakresie rozwoju technologicznego, przy zapewnieniu maksymalnego poziomu bezpieczeństwa.

W PORÓWNANIU Z SYSTEMEM POPRZEDNIEJ GENERACJI, INTEGRAL EVOXX MA:

- ponad 5-krotnie większą moc obliczeniową dzięki zastosowaniu nowych redundantnych procesorów dwurdzeniowych,
- ponad 32-krotnie większą pamięć operacyjną/programową,
- interfejs techniki bezprzewodowej Bluetooth dla łatwiejszej komunikacji z użytkownikiem,
- nowy interfejs dla kart pamięci SD HC i SD XC (standard 3.0),
- Interfejs serwisowy USB v 2.0.

Podobnie jak w systemach poprzedniej generacji, zapewniono maksymalny poziom bezpieczeństwa – system Integral EvoxX M ma pełną redundancję sprzętową i programową, a centrale Integral EvoxX C i B redundancję programową.

Integral EvoxX M

NOWOCZESNY CYFROWY SYSTEM BEZPIECZEŃSTWA POŻAROWEGO WSPIERAJĄCY SYSTEMY ZEWNĘTRZNE

Dzięki zastosowaniu nowej, znacznie wydajniejszej platformy sprzętowej oraz nowego oprogramowania systemowego V8.4, Integral EvoxX jest jeszcze lepiej przygotowany do bezpiecznego współdziałania z innymi systemami bezpieczeństwa oraz wdrożenia specjalnych narzędzi do zarządzania całym cyklem życia projektu systemu bezpieczeństwa. Oferowane przez Schrack Seconet narzędzia z pakietu Integral Remote oraz przygotowana specjalna Platforma Serwisowa oparta na chmurze pozwalają na pełne wsparcie w zakresie projektowania, uruchamiania, konserwacji, serwisu i modernizacji systemu.
Integral EvoxX jest przystosowany do integracji z systemami zewnętrznymi, ma możliwość elastycznego dostosowywania funkcji w zakresie wizualizacji i sterowania w zależności od wymagań danego projektu oraz obowiązujących norm i wytycznych. Stale szczegółowo monitoruje i przetwarza wartości chwilowe stanów pracy całej instalacji i może je udostępniać (w wersji przetworzonej lub w postaci wartości analogowych) do zewnętrznych urządzeń. Dzięki temu, w ramach funkcji bezpieczeństwa, system wcześniej sygnalizuje odbiegające od wymagań projektowych nieprawidłowe stany pracy (takie jak niebezpieczne zabrudzenie układów detekcyjnych czujek pożarowych, zmiana rezystancji linii dozorowych i sterujących spowodowana starzeniem się instalacji, rozszczelnienia w układach pneumatycznych czujek zasysających dymu i liniowych czujek ciepła dzięki dokładnemu monitorowaniu przepływu powietrza). Pozwala to na wcześniejszą reakcję służb ochrony na rozwijające się uszkodzenie, zanim dojdzie do poważniejszej awarii w systemie. W ramach funkcji detekcji pożaru interaktywne czujki wielokryteriowe serii CUBUS stale analizują wartości chwilowe takich parametrów, jak temperatura, zadymienie czy stężenie tlenku węgla.
Integral EvoxX umożliwia przekazanie tych danych do systemu integrującego urządzenia przeciwpożarowe SIS-FIRE oraz, fakultatywnie, do zewnętrznych systemów zarządzania budynkiem (BMS/BAS) w celu realizacji funkcji bezpieczeństwa i komfortu. W systemie BMS dane mogą być wykorzystane do sygnalizacji różnych nieprawidłowości w obiekcie – np. wykrycie podwyższonej temperatury w serwerowni może świadczyć o uszkodzeniu układu wentylacji i klimatyzacji. Jednocześnie, dzięki stałemu odczytowi wartości chwilowych, informacje o aktualnej temperaturze czy stężeniu CO mogą być w niektórych obiektach wykorzystywane do sterowania i regulacji innych urządzeń, np. w zakresie klimatyzacji i wentylacji.
Realizując takie funkcje, SSP wspomaga aktywnie inne systemy bezpieczeństwa w obiekcie. Aby zapewnić maksymalną wydajność i niezawodność działania central, funkcje podstawowe systemu związane z bezpieczeństwem pożarowym oraz funkcje fakultatywne zostały rozdzielone i są zarządzane przez osobne rdzenie procesorów systemowych. Dzięki temu w razie ewentualnych zakłóceń w zakresie funkcji dodatkowych zapewniona jest niezakłócona praca w zakresie funkcji bezpieczeństwa.

ŚCISŁA WSPÓŁPRACA Z SYSTEMEM INTEGRUJĄCYM SIS-FIRE

Zapewnienie maksymalnego poziomu bezpieczeństwa z puntu widzenia nadzoru i obsługi systemów i urządzeń przeciwpożarowych, w tym przede wszystkim aktywnego zarządzania ewakuacją osób w przypadku alarmu pożarowego, wymaga zastosowania systemu integrującego urządzenia ppoż. (SIUP). Oferowany przez Schrack Seconet system zarządzania bezpieczeństwem pożarowym SIS-FIRE współpracuje z Integral EvoxX,

korzystając z protokołu systemowego ISP-IP, pozwalającego na realizację wszystkich funkcji systemowych w zakresie bezpieczeństwa i komfortu. SIS-FIRE wraz z Integral EvoxX oraz innymi zintegrowanymi systemami (m.in. KD, CCTV/VMS) mającymi wpływ na bezpieczeństwo obiektu tworzą jeden spójny, w pełni kompatybilny system zarządzania bezpieczeństwem pożarowym obiektu.

BEZPIECZNA KOMPATYBILNOŚĆ W PRZÓD I WSTECZ

Jedną z głównych zalet systemu Integral EvoxX jest pełna kompatybilność „wstecz" oraz „w przód" w zakresie komponentów sprzętowych (*hardware*) oraz oprogramowania (*software*). Pod tym pojęciem należy rozumieć możliwość współpracy wszystkich urządzeń i systemów, które były oferowane przez firmę Schrack Seconet w celu zapewnienia bezpiecznej modernizacji i rozbudowy instalacji w całym cyklu życia obiektu.
Kompatybilność wsteczna oznacza możliwość rozbudowy systemów o nowe urządzenia systemu Integral z zapewnieniem ich współpracy z urządzeniami istniejącymi w danej instalacji. Dotyczy to szczególnie elementów peryferyjnych opartych na starszej technologii, które mogą współpracować z centralami najnowszej generacji oferowanymi przez Schrack Seconet. W zakresie komponentów sprzętowych centrali oznacza to współpracę z kartami rozszerzeń central poprzednich generacji – Integral EvoxX jest kompatybilny z Integral IP, Integral Evolution i BMZ Integral. W praktyce możliwe jest zastosowanie w jednej centrali modułowej Integral EvoxX M komponentów sprzętowych platform B3, B5, B5A oraz platformy najnowszej generacji B8.
Jako kompatybilność „w przód" należy rozumieć możliwość, na poziomie sprzętowym i oprogramowania, rozbudowy i współpracy istniejącej instalacji z urządzeniami, które zostaną wprowadzone w przyszłości. W zakresie urządzeń oznacza to możliwość rozbudowy istniejących central o nowe komponenty w ramach danej platformy sprzętowej lub upgrade'u tylko niektórych podzespołów systemu przy wprowadzaniu nowej platformy sprzętowej. Dodatkowo współpraca pomiędzy centralami różnych generacji (np. wdrażanych na różnych etapach cyklu życia obiektu) jest zapewniona w ramach spójnego systemu sieciowego. Oferowana sieć central Integral WAN może zintegrować sieci SecoNET, Integral LAN i „pętlę podcentral Integral".

BEZPIECZNA I PRAKTYCZNIE NIEOGRANICZONA MOŻLIWOŚĆ PRACY W SIECI

Centrale Integral EvoxX mogą być połączone w sieć o dowolnej topologii (pierścień, magistrala, sieć kratowa) z wykorzystaniem różnych mediów transmisji (połączenia miedziane i światłowodowe) i różnego stopnia zabezpieczenia (redundancji) połączeń. Pozwala to na elastyczność w budowaniu systemu sieciowego, z optymalnym dostosowaniem do wymagań danego obiektu i wdrożenie wymaganego poziomu bezpieczeństwa. Standardowo centrale pracują w sieci o topologii podwójnego pierścienia, a więc system jest odporny na trzy uszkodzenia połączeń, ale poziom bezpieczeństwa może być jeszcze wyższy, ponieważ przy zastosowaniu sieci kratowej (*mesh network)* system jest odporny nawet na siedem uszkodzeń łączy sieciowych.
System Integral EvoxX wprowadza nowe możliwości w zakresie sieciowania central z wykorzystaniem sieci Intranet/Internet. Dzięki wprowadzeniu funkcji Integral WAN Bridge możliwe jest wykonanie bezpiecznych szyfrowanych połączeń VPN między dowolnymi centralami, niezależnie od ich lokalizacji – jedynym warunkiem jest to, aby były one podłączone do sieci Internet o wymaganej przepustowości.

Integral EvoxX C

Integral EvoxX B

Ta nowa funkcjonalność pozwala na nieograniczone łączenie central w sieć, w celu realizacji funkcji nadzoru i serwisu nad rozproszonymi systemami sygnalizacji pożarowej i sterowania urządzeniami przeciwpożarowymi.

ELASTYCZNE INTERAKTYWNE OPROGRAMOWANIE SYSTEMOWE

System Integral EvoxX, podobnie jak centrale poprzedniej generacji Integral, charakteryzuje się elastycznym oprogramowaniem pozwalającym na wdrożenie w obiekcie praktycznie dowolnego scenariusza pożarowego. Funkcje i kryteria dotyczące sterowania i obsługi mogą być dowolnie programowane z wykorzystaniem operatorów logicznych Boole'a – dzięki temu można zdefiniować różne kryteria sterowania i wdrożyć alternatywne sposoby sterowania w zależności od rozwoju pożaru w obiekcie. Dzięki oprogramowaniu pracującemu w trybie dynamicznym można zastosować specjalne blokady międzystrefowe oraz bezpieczne procedury sterowania *„fail-safe"* uwzględniające sterowanie urządzeniami przeciwpożarowymi w sytuacji wystąpienia różnego typu uszkodzeń w instalacji.

PODSUMOWANIE

System Integral EvoxX jest kolejnym ważnym etapem rozwoju systemu bezpieczeństwa pożarowego Schrack Seconet. Dzięki swojej niezawodnej i elastycznej architekturze pozwala zrealizować kompleksową ochronę w zakresie sygnalizacji pożarowej i sterowania urządzeniami przeciwpożarowymi. Platforma sprzętowa i programowa systemu została opracowana pod kątem zapewnienia maksymalnego poziomu bezpieczeństwa oraz wsparcia dla nowych rozwiązań technologicznych związanych z rozwojem cyfryzacji w dobie Przemysłu 4.0.

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

Cyberzagrożenia a bezpieczeństwo fizyczne Cz. 2

Poprzednia część artykułu traktowała o wybranych zagadnieniach z zakresu cyberbezpieczeństwa w kontekście użyteczności w elektronicznych systemach zabezpieczeń, które *de facto* są niczym innym, jak często rozbudowanymi systemami teleinformatycznymi.
Jak się okazuje ze świata IT można czerpać dobre wzorce, takie jak analiza ryzyka, hardening czy triada CIA i stosować je z powodzeniem w naszych codziennych obowiązkach. Druga część artykułu kontynuuje tę tematykę.

Tomasz Dacka

THE KILL CHAIN

Modus operandi cyberprzestępców jest opisany przez tzw. *The Kill Chain*. To schemat, który kreśli krok po kroku działania podjęte przez intruza w celu uzyskania nieuprawnionego dostępu do chronionych zasobów informatycznych. Najczęściej dzieli się na następujące etapy:

PLANOWANIE *(Planning)* – atakujący wybiera cel ataku, analizuje sposób, w jaki chce się dostać do chronionych zasobów, wybiera sposób działania (np. atak typu DDoS przez sieć botnet, którą mogą tworzyć skompromitowane kamery).

REKONESANS *(Reconnaissance/discovery)* – atakujący poznaje organizację w sposób aktywny bądź pasywny, na tym etapie zależy mu na pozostaniu anonimowym (może zatem wykorzystywać tzw. OSINT). Ta faza kończy się wypracowaniem tzw. exploitów – wykrytych podatności, które można wykorzystać w celu materializacji ataku.

UZBRAJANIE *(Weaponization)* – atakujący, wykorzystując exploit, dostaje się do systemu informatycznego. Skompromitowany komputer lub konto, które to umożliwiło, to tzw. *pivot point* – punkt, z którego będą dokonywane dalsze penetracje systemu. W tym momencie atakujący jest już w pełni uzbrojony (może uruchomić złośliwe oprogramowanie), najczęściej jego obecność jest wciąż niewykryta.

DZIAŁANIA NA ZASOBACH *(Lateral movement)* – uzbrojony w *pivot point* atakujący penetruje dalej system informatyczny, szuka eskalacji uprawnień aplikacji, aż trafia na zasób, który go interesuje, i dokonuje kopii, skasowania bądź zaszyfrowania danych w celu wyłudzenia okupu. Bardzo często intruz tworzy ukryty kanał komunikacji z tzw. *Command & Control* (C2) – zewnętrzną siecią, którą w pełni zarządza.

WYCOFANIE SIĘ *(Retreat)* – atakujący osiągnął cel, w tym momencie zaciera ślady swojej obecności w systemach, aby po wykryciu ataku (co średnio następuje w okresie ok. 6 miesięcy od momentu ataku) utrudnić zbieranie danych na temat działań i jego osoby.

Skoro celem ataku zazwyczaj nie są dane związane bezpośrednio z systemami zabezpieczenia (technicznego), po co nam ta wiedza? Opisałem *The Kill Chain*, aby uzmysłowić, że „nasze systemy" mogą stać się drogą do celu (tzw. *pivot point*). Atakujący zdają sobie świetnie sprawę z tego, że bezpieczeństwo IT systemów z obszaru *physical security* stoi zazwyczaj na niższym poziomie, co czyni je świetnym początkowym celem, od którego można zacząć eksplorację sieci. Pierwszym krokiem może być pozyskanie uprawnień administratora takich systemów, a następnie próba wykorzystania ich w innych systemach (dlatego tak często mówi się o tym, aby generować unikalne loginy do systemów). Ponadto atakujący, który ma dostęp do sieci kamer, może łatwo, za pomocą DDoS, sparaliżować ruch w sieci i tak obciążyć serwer, że przestanie działać, a z nim cały system CCTV.
Każdy poważny incydent jest rozpatrywany przez informatykę śledczą, tzw. *computer forensics*. Wyniki jej pracy nie przysporzą nam chwały, kiedy dowiemy się, że staliśmy się szeroko otwartą bramą dla działań intruza.

AKTUALIZACJE, SYSTEMY LEGACY

Problem na pierwszy rzut oka wydaje się prosty i jednoznaczny, jednak z doświadczenia wiem, że niestety często jest pomijany w naszej branży. Bezpieczeństwo, zarówno fizyczne, jak i teleinformatyczne, nigdy nie przyjmuje wartości stałej, jest zmienne w czasie. Wymaga to od nas pewnego rodzaju ubezpieczenia się, zminimalizowania prawdopodobieństwa wystąpienia incydentu. Taką właśnie formą jest zapewnienie aktualizacji wykorzystywanego oprogramowania oraz przeprowadzanie tych aktualizacji w momencie, gdy:

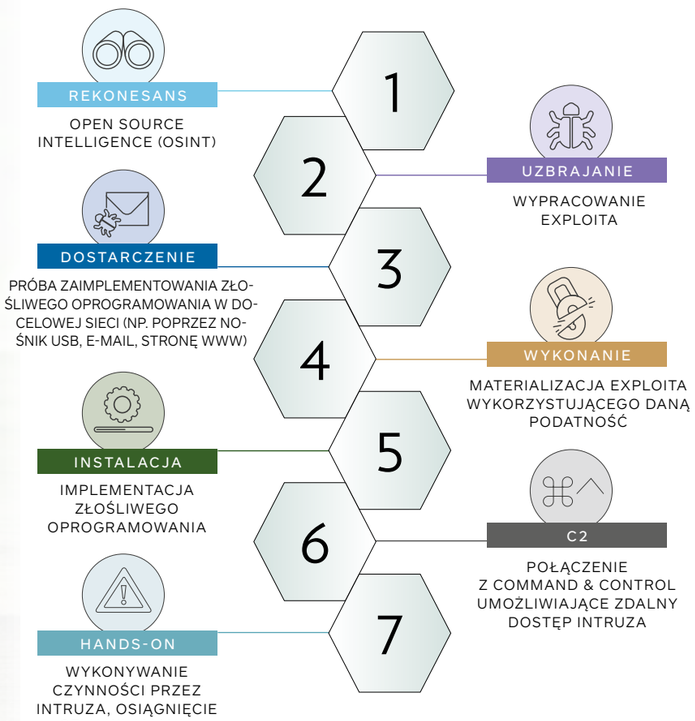
- producent wydał nową funkcjonalność, której wdrożeniem jesteśmy zainteresowani,
- został wykryty błąd w kodzie umożliwiający wykorzystanie go w nieuprawniony sposób.

Drugim ciekawym aspektem są tzw. systemy *legacy*, czyli nieaktualizowane, pozostawione bez wsparcia producenta. Takie systemy powinny podlegać analizie ryzyka w celu jego mitygacji. System operacyjny, oprogramowanie, urządzenie należy regularnie aktualizować, modernizować. Dzisiaj twój *soft* może być „szczelny", jutro przeciwnie: ktoś znalazł podatność, potrafi ją wykorzystać i nie zawaha się spróbować, jeśli nie zostanie odstraszony. Należy też pamiętać o sprawdzonym łańcuchu dostaw w przypadku pobierania aktualizacji, aby w dobrej wierze nie wprowadzić złośliwego oprogramowania razem z aktualizacją systemu. Służą temu *hashe* podawane przez producentów oprogramowania, zapewniające zachowanie integralności informacji.

ARCHITEKTURA

Zapewne każdy słyszał, że system jest bezpieczny, bo działa w wydzielonej podsieci i nie ma dostępu do Inter-

Rys. The Kill Chain



NOWOCZESNY „BEZPIECZNIK" POWINIEN WIEDZIEĆ, JAKIE ROZWIĄZANIA ISTNIEJĄ I ZNAĆ ICH GŁÓWNE ZADANIA, ABY DZIĘKI TEJ ŚWIADOMOŚCI MÓC W POROZUMIENIU Z OBSZAREM SEC IT WSPÓLNIE MITYGOWAĆ RYZYKA I KORZYSTAĆ Z DZIAŁAJĄCEJ JUŻ INFRASTRUKTURY IT

netu. Sieć rzeczywiście można wydzielić fizycznie (tzw. *air gap)* lub logicznie (np. za pomocą VLAN-ów). I jest to jak najbardziej słuszna droga, z tym że to jeszcze nie wszystko. Wydzielając sieć logicznie, trzeba pamiętać, że podsieć konfigurujemy np. na switchach warstwy 3. czy routerach. Musimy zatem udrożnić odpowiedni ruch, a zablokować ten, który jest nam niepotrzebny. W przeciwnym razie przenosimy się z hali głównej co prawda do dedykowanego pokoju, ale nadal z otwartymi drzwiami i oknami.

Wydzielenie fizyczne jest zazwyczaj trudne do osiągnięcia w rozwiązaniach biznesowych, ponieważ poniekąd kłóci się z atrybutem dostępności informacji. Jednak nawet takie wydzielenie nie chroni np. przed wpięciem przez uprawnionego pracownika do takiego systemu skompromitowanego urządzenia (np. pamięci USB), podsłuchu elektromagnetycznego, zagrożeniem wewnętrznym (tzw. *insider threat),* wrogim przejęciem telefonu komórkowego połączonego z tym systemem czy innymi atakami socjotechnicznymi.

Wracając do pytania, czy „bezpiecznik" musi znać się na bezpieczeństwie architektury systemu informatycznego, uważam, że nie potrzebuje wiedzy nt. konfiguracji portów na switchu, nie potrzebuje wiedzy nt. zarządzania ruchem na *load balancerze,* konfiguracji WAF-ów, wydzielania DMZ-ów. Jednak jestem zdania, że nowoczesny „bezpiecznik" powinien wiedzieć, że takie rozwiązania istnieją, i znać ich główne zadania, aby dzięki tej świadomości móc w porozumieniu z obszarem Sec IT wspólnie mitygować ryzyka i korzystać z działającej już infrastruktury IT. To trochę tak, jak umieścić serwer np. z oprogramowaniem PSIM w serwerowni zarządzanej przez dział infrastruktury. Nie musimy sami martwić się o temperaturę, wilgotność, środowisko wirtualne czy redundancję, to zazwyczaj dostarczą nam działy IT. Musimy jednak wiedzieć, że taka możliwość istnieje, i rozumieć plusy i minusy z jej skorzystania.

AAA

To kolejna złota zasada prosto ze świata IT. Właściwie ten zapis powinien brzmieć IAAA, co należy rozumieć następująco:

IDENTIFICATION (identyfikacja) – proces zakładania konta, numeru ID użytkownika, urządzenia lub procesu w sieci.

AUTHENTICATION (autentykacja) – proces, w którym dane konto musi udowodnić, że jest tym, za jakie się podaje w momencie żądania dostępu do zasobów.

AUTHORIZATION (autoryzacja) – przypisanie uprawnień do konkretnych zasobów.

ACCOUNTING (rozliczalność) – śledzenie autoryzowanego ruchu, wykrywanie nieuprawnionych prób oraz dostępów do zasobów.

Czy to nie opisuje wielu procesów z naszej branży? Zakładamy konto użytkownika w systemie kontroli dostępu, którego tożsamość potwierdzamy np. dowodem osobistym (identyfikacja), następnie użytkownik, chcąc dostać się do przydzielonego obszaru, przykłada kartę KD do czytnika (autentykacja), porusza się tylko po tym obszarze, do którego ma uprawnienia (autoryzacja). System KD zapamiętuje ścieżki ruchu oraz alarmuje o próbie forsowania drzwi lub wejścia do zabronionej strefy (rozliczalność). To ogólny przykład, brakuje w nim wielu kwestii, z którymi musimy mierzyć się co dzień (np. *tailgating* czy *piggy backing).* Innym przykładem jest możliwość kopiowania kart dostępu czy procedury tworzenia konta bez sprawdzenia tożsamości użytkownika.

CYKL ŻYCIA BITA

Elektroniczne systemy zabezpieczeń przetwarzają bardzo dużą ilość danych, kluczowych ze względów bezpieczeństwa. Dane te w pewnym momencie, z perspektywy Sec IT, mogą przyjmować trzy różne stany wymagające od nas trzech różnych analiz pod kątem zachowania trzech głównych atrybutów informacji (CIA):

Dane w spoczynku *(data at rest)* – mogą to być nasze archiwa nagrań wideo, bazy danych użytkowników, repozytoria procedur, polityk czy kopie zapasowe. Zaleca się, aby te dane chronić poprzez szyfrowanie oraz utworzenie odpowiednich ACL (list dostępowych).

Dane w ruchu *(data in transit)* – stan, w którym nasze cenne bity są transmitowane przez sieć. Może to być np. sygnał wizyjny z kamery czy proces autentykacji/autoryzacji użytkownika na przejściu kontrolowanym przez system KD. Tutaj zaleca się również szyfrowanie danych z wykorzystaniem takich protokołów, jak TLS, IPSec i efemerycznych kluczy sesji.

Dane w użyciu *(data in use)* – stanowi największe wyzwanie, w tym aspekcie jesteśmy niejako zdani na dostawców technologii. Dane w tym stanie są przetwarzane w pamięciach ulotnych, np. pamięć RAM, rejestry CPU czy pamięć cache. Przykładami mogą być: modyfikowanie danych użytkownika w bazie danych czy generowanie logów zdarzeń w systemie SKD. Jest to stan, w którym dane są najczęściej deszyfrowane (co naraża je na nieuprawniony dostęp), przechodząc ze stanu w spoczynku do stanu w użyciu.

PODSUMOWANIE

Czy rzeczywiście nasza branża jest realnie zagrożona atakami ze strony cyberprzestępców? Polecam zaznajomić się ze sprawą botnetu Mirai (sieci przejętych przez intruzów urządzeń, często zwanych zombie), gdzie wykorzystano m.in. kamery CCTV do potężnego ataku DDoS *(Distributed Denial of Service)* w USA w październiku 2016 r. Motywacje i cele intruzów są różne, nie ma też idealnych systemów, które w pełni zabezpieczą nas przed zagrożeniem.

„Utwardzając" urządzenia systemów zabezpieczeń, tak naprawdę kupujemy sobie czas, jaki atakujący musi poświęcić, aby dostać się do naszych zasobów. Liczy się właśnie ten czas, który podczas ataku działa na naszą korzyść. Chroni nas dokładnie w ten sam sposób, co ogrodzenie czy solidne drzwi antywłamaniowe. Przestępcy natomiast mogą zamienić wytrychy i łomy na exploity, złośliwe oprogramowanie.

Czy twój system kontroli dostępu jest odporny na cyberataki?

Dzisiejsza kontrola fizycznego dostępu to znacznie więcej niż nadawanie uprawnień dostępu do poszczególnych pomieszczeń. Wiele nowoczesnych systemów kontroli dostępu fizycznego jest opartych na protokole IP i obsługiwanych przez inteligentne oprogramowanie, umożliwiając przetwarzanie ogromnych ilości danych. Zapewnia to większą funkcjonalność, elastyczność i skalowalność oraz możliwości integracji z innymi systemami (interoperacyjność). Oznacza to również, że systemy KD stanowią część firmowej sieci IT, więc należy je chronić i aktualizować – tak jak pozostałe systemy infrastruktury IT.

O cyberbezpieczeństwie rozmawiamy z **Wesleyem Keegstrą, kierownikiem ds. integracji w firmie Nedap Security Management**. Wyjaśniamy także, dlaczego cyberbezpieczeństwo stanowi istotną, choć często nieuświadamianą potrzebę ochrony systemów kontroli dostępu fizycznego.

Wiele przedsiębiorstw wciąż nie zadbało o cyberbezpieczeństwo swoich systemów kontroli dostępu fizycznego opartych na IP. Co pana zdaniem jest przyczyną takiego stanu?

Myślę, że dużą rolę odgrywa tu brak świadomości. Bezpieczeństwo fizycznego dostępu dotyczy czegoś, co można zobaczyć i dotknąć, a więc łatwiej je zrozumieć czy uzasadnić. Cyberbezpieczeństwo jest równie ważne, a cyberataki są bardziej wyrafinowane. Brak cyberzabezpieczeń systemu KD opartego na IP jest jak pozostawienie szeroko otwartych drzwi. A jeśli zostawiamy otwarte tylne drzwi, inwestowanie czasu i pieniędzy w fizyczne zabezpieczenia obiektu nie ma sensu.

W jaki sposób cyberprzestępcy mogą naruszyć systemy kontroli dostępu fizycznego?

Cyberprzestępczość ma wiele postaci. Może polegać np. na nieuprawnionym pobieraniu danych lub manipulowaniu danymi przesyłanymi pomiędzy urządzeniami systemu kontroli dostępu, m.in. w celu ujawnienia, które osoby mają dostęp i w jakim miejscu. Może to być także gromadzenie danych z kart dostępu, a następnie ich kopiowanie lub klonowanie. Idąc krok dalej, cyberprzestępcy mogą ukraść czyjeś dane uwierzytelniające, aby zalogować się do oprogramowania systemu KD. Po zalogowaniu mogą udzielić nieautoryzowanego dostępu do wszelkiego rodzaju drzwi i pomieszczeń. Uzyskując dostęp do firmowej bazy danych, mogą manipulować zapisami zdarzeń lub nawet usunąć zapisy świadczące o działaniach wykonanych przez nich samych lub przez inne osoby.
Urządzenia systemu kontroli dostępu oparte na sieci IP współpracują z różnymi urządzeniami sieciowymi innych systemów, zatem ważne, aby każde z nich było chronione przed cyberatakami – chodzi tu zarówno o czytniki, sterowniki, kamery, jak i wiele innych urządzeń.

Jakie mogą być konsekwencje cyberataku?

Skutki mogą być różne. Najbardziej oczywistym jest możliwość uzyskania fizycznego dostępu do mienia i dokonanie jego kradzieży lub nawet aktów terroryzmu. Cyberprzestępca może też – zdalnie lub uzyskując dostęp do obiektu – wykraść gromadzone i przetwarzane dane. Mogą to być informacje niejawne, takie jak dane dotyczące produktu, które w przypadku wycieku mogą zapewnić przewagę konkurentom. Cyberprzestępca może również wykraść dane osobowe lub finansowe, a to narazi administratora danych na wysokie, w zależności od branży i kraju, kary.
Naprawa skutków cyberataku i przywrócenie funkcjonalności systemów często wiąże się z kosztami. Jeśli przedsiębiorstwo nie może funkcjonować wskutek awarii systemu informatycznego, trzeba się liczyć z dodatkowymi kosztami. Cyberataki mogą również zaszkodzić reputacji firmy, a to prowadzi do strat finansowych i wpływa na rozwój i stabilność działalności. Podsumowując, w kwestii cyberbezpieczeństwa należy dmuchać na zimne.

W jaki sposób firmy mogą chronić swoje systemy kontroli dostępu fizycznego przed cyberprzestępcami?

Nikt nie może powiedzieć, że coś jest cyberbezpieczne w 100%, ale zdecydowanie lepiej zapobiegać, niż leczyć. Najważniejsze kwestie to zapewnienie cyberochrony zarówno urządzeń i oprogramowania do kontroli dostępu, jak i nośników danych oraz sposobu uzyskiwania dostępu do przesyłanych informacji – nie tylko w obrębie jednego budynku, lecz także całego kraju czy na poziomie międzynarodowym.
Bardzo istotne jest wprowadzenie jasnych zasad bezpiecznego korzystania z systemów kontroli dostępu fizycznego i bezpiecznego zarządzania nimi. Powinny one obejmować elementy cyberbezpieczeństwa i wymagać korzystania z silnych haseł, zmienianych po upływie określonej liczby dni. Należy także opracować politykę bezpieczeństwa dotyczącą innych urządzeń bazujących na IP, takich jak kamery, pamiętając, że o wytrzymałości całego łańcucha decyduje jego najsłabsze ogniwo.
Pracownicy powinni zostać przeszkoleni w zakresie cyberbezpieczeństwa, aby zastosowane środki nie okazały się nieskuteczne w wyniku braku wiedzy i nieodpowiedzialnego zachowania ludzi.

Czy każda organizacja potrzebuje takiego samego poziomu cyberbezpieczeństwa?

Wymagania w zakresie cyberbezpieczeństwa mogą różnić się w zależności od branży i konkretnego przedsiębiorstwa lub organizacji. Cyberbezpieczeństwo wymaga zasobów i inwestycji, więc ważne jest to, aby odpowiednio je dopasować do sytuacji firmy.
Oferowany przez firmę Nedap system kontroli dostępu AEOS zapewnia użytkownikowi kontrolę nad cyberbezpieczeństwem, umożliwiając podejmowanie decyzji, co należy zabezpieczyć i na jakim poziomie. Można zabezpieczyć np. karty, czytniki kart, kontrolery (centrale systemu KD) i bazy danych. Możliwe jest także zabezpieczenie dostępu do interfejsu użytkownika AEOS i szyfrowanie komunikacji między poszczególnymi komponentami systemu – to, co zabezpieczysz, zależy wyłącznie od ciebie. Gdy cyberbezpieczeństwo stanie się coraz ważniejsze dla organizacji, będziesz w stanie podnieść poziom ochrony w systemie AEOS.

Więcej o cyberbezpieczeństwie i systemie AEOS znajdziesz na www.nedapsecurity.com/pl/.

Jakie lekcje z wycieków danych powinien wyciągnąć biznes

Kwiecień 2021 r. przyniósł poważny incydent, jakim był duży wyciek danych osobowych z jednego z serwerów rządowych. W sieci znalazł się plik Excel, który zawierał informacje identyfikujące funkcjonariuszy policji, służby celno-skarbowej, Służby Ochrony Państwa, administracji skarbowej, Straży Granicznej, Straży Pożarnej (w tym strażaków ochotniczych straży pożarnych), Inspekcji Transportu Drogowego, straży miejskiej, straży ochrony kolei czy służby więziennej. Ujawnieniu uległy takie dane, jak imiona, nazwiska, numery PESEL, adres miejsca pracy, pełna nazwa jednostki pełnienia służby, numery telefonów i adresy e-mail. Zakres danych był więc znaczny, a ich liczba przekraczała 20 tysięcy.

Jacek Grzechowiak

Wszystkie te informacje dotyczyły osób, które zostały zgłoszone do programu szczepień, stąd tak szeroki zakres instytucji, w których są one zatrudnione lub pełnią służbę. To było również powodem utworzenia tego zbioru danych z wykorzystaniem popularnej aplikacji biurowej. Mamy więc do czynienia z procesem spotykanym powszechnie w wielu organizacjach biznesowych, gdzie różnego rodzaju wykazy osób szkolonych, uczestników konferencji czy zestawienia klientów są tworzone właśnie w ten sam sposób. Wkrótce dojdzie kolejny wykaz, co do zasady identyczny. Umożliwienie przedsiębiorcom samodzielnej realizacji szczepień jest bowiem obwarowane wymogiem zgromadzenia 300 chętnych, a więc w naturalny sposób wymagające tego typu wykazów. Z dużym prawdopodobieństwem one również będą tworzone w arkuszu Excel, a przynajmniej w części przedsiębiorstwa będą zapewne opracowywane na platformach współdzielonych, co będzie związane z ryzykiem nieuprawnionego dostępu.

Wyciek już sam w sobie stwarza szereg zagrożeń, jednak, jak twierdzi Biuro Rzecznika Praw Obywatelskich: *W przypadku funkcjonariuszy publicznych jeszcze większe zagrożenie wiąże się z możliwością wkroczenia w życie prywatne poprzez niechciane telefony czy korespondencję, a nawet wykorzystanie możliwości kontaktu do wywierania wpływu lub podejmowanie działań w celu pozbawienia ich zaufania publicznego...*[1]. Mimo że w biznesie nie będziemy raczej mieli do czynienia z funkcjonariuszami publicznymi (choć nie należy tego wykluczać, wszak znane są przypadki, że funkcjonariusze publiczni „dorabiają" w firmach prywatnych), to jednak ich dane zapewne nie znajdą się w tych wykazach, bo ta grupa została już zaszczepiona. Tym niemniej nie oznacza to, że wykaz biznesowy nie będzie zawierał danych wrażliwych. Co do zasady będą w nim przecież dane osobowe, a przez identyfikowanie stanowisk służbowych czy działów firmy może wchodzić w grę tajemnica przedsiębiorstwa. Jest więc powód do zastanowienia się, co w praktyce może powodować nieuprawnione ujawnienie takich danych.

A jak widać z praktyki, jest o czym myśleć, bo to nie pierwszy taki przypadek, choć patrząc z perspektywy ilości danych oraz profilu osób, których dotyczą, wydaje się najpoważniejszy. W jaki sposób tego typu zagrożenie może się zmaterializować, pokazuje historia innego wycieku, do jakiego doszło w styczniu tego roku z Platformy Szkoleniowej Krajowej Szkoły Sądownictwa i Prokuratury. W jego wyniku uzyskano w sposób nieautoryzowany dostęp do danych ponad 400 osób, wchodząc w posiadanie numerów telefonów oraz prywatnych adresów poczty elektronicznej. Informacje te zostały wykorzystane do skierowania wobec adresatów spersonalizowanych gróźb, m.in. pozbawienia życia.

DANE, KTÓRE WYCIEKŁY, ZOSTAŁY WYKORZYSTANE DO SKIEROWANIA WOBEC ADRESATÓW SPERSONALIZOWANYCH GRÓŹB, M.IN. POZBAWIENIA ŻYCIA

Tego typu incydenty zdarzają się wszędzie, a nasz 20-tysięczny zbiór danych w konfrontacji z – mającym miejsce także w tym roku – wyciekiem w Brazylii[2], kiedy to do sieci wyciekły 223 mln danych, czyli więcej niż liczy populacja tego kraju, wydaje się niewielki. Pozostawiając kwestie cyberbezpieczeństwa oraz RODO specjalistom w tym zakresie, chciałbym skupić się na innych potencjalnych problemach, jakich tego typu incydenty mogą przysporzyć biznesowi. A sprawa jest istotna i jak najbardziej „na czasie", w obecnej sytuacji epidemiologicznej bowiem różnego rodzaju wykazy już stały się powszechne, a możliwość tworzenia przez przedsiębiorstwa własnych punktów szczepień sprawia naturalną okazję do tworzenia kolejnego wykazu. W ten sposób niektóre organizacje biznesowe będą przygotowywały analogiczne wykazy do tego, który wyciekł do sieci w kwietniu.

Jednym ze sposobów zbierania informacji jest metoda mozaikowa, dlatego poszczególne wycieki danych powinny być rozpatrywane nie tylko jako pojedyncze zdarzenia, ale też jako przesłanki do wystąpienia kolejnych incydentów, do których może dojść w przypadku połączenia danych uzyskanych w trakcie różnych wycieków. Wzorem innych działalności przestępczych czy działań służb specjalnych, w których ramach dochodzi do sprzedaży lub wymiany informacji i know-how, także i tutaj może zdarzyć się tego typu sytuacja, dlatego niezbędne jest rozważenie zagrożeń już zidentyfikowanych oraz potencjalnych – jeszcze niewystępujących, choć pewnie bezpieczniej będzie powiedzieć: takich, o których wystąpieniu nie wiadomo publicznie.

POSZCZEGÓLNE WYCIEKI DANYCH POWINNY BYĆ ROZPATRYWANE NIE TYLKO JAKO POJEDYNCZE ZDARZENIA, ALE TAKŻE JAKO PRZESŁANKI DO WYSTĄPIENIA KOLEJNYCH INCYDENTÓW

Skoro więc mieliśmy już przypadki targetowania (obierania za cel) w odniesieniu do pracowników wymiaru sprawiedliwości, należy przyjąć, że takie samo działanie może być skierowane do biznesu, a jego celem będą przede wszystkim osoby decyzyjne i mające szczególne znaczenie dla ciągłości działania przedsiębiorstwa. Lista tworzona na potrzeby realizacji programu szczepień w zakładzie pracy z pewnością stanie się gotowym materiałem z precyzyjnie zdefiniowaną grupą odbiorców. Tym samym będzie to materiał wrażliwy, którego nieuprawnione ujawnienie może prowadzić do wielu zagrożeń, poczynając od kierowania do tych pracowników informacji dyskredytujących pracodawcę, poprzez wszelkiego rodzaju próby docierania z produktami, usługami i propozycjami korupcyjnymi, po agresywną ingerencję w życie prywatne pracowników, a nawet różne formy zastraszania, zmuszając ich do skupienia uwagi na rozwiązywaniu osobistych problemów, przez co pośrednio zostanie zmniejszona ich wydajność w pracy.

Zagrożenie może pójść dalej. Coraz częściej pojawiają się informacje wskazujące na agresywne kampanie fake newsów wobec różnych firm czy ich produktów.

I tak np. posiadanie wiarygodnej bazy danych pracowników pozwala na podjęcie tego typu działań w sposób jeszcze bardziej sprofilowany, odnoszący się nie tylko do firmy, ale także do poszczególnych jej działów czy wręcz konkretnych pracowników i w ten sposób oddziałujący jeszcze bardziej destrukcyjnie. Takie dane pozwalają bowiem na kierowanie fałszywych wiadomości w sposób selektywny, np. poprzez przesyłanie destrukcyjnych komunikatów do wybranej grupy pracowników, tylko z jednego działu lub o jednej specjalności. To swego rodzaju broń precyzyjnego rażenia pozwalająca nawet na wywołanie kryzysu wewnątrz konkurencyjnego przedsiębiorstwa.

Czy to *science fiction?* Nie sądzę. Tego typu przypadki miały już miejsce i to w czasach, gdy wycieki danych nie były jeszcze w ogóle w polu naszego widzenia. Wyobraźmy sobie następującą sytuację: firma modernizuje linię produkcyjną, kupuje nową innowacyjną maszynę, szkoli zespół pracowników do jej obsługi, a w tym samym czasie ta właśnie grupa pracowników zostaje „zaatakowana" informacją np. o problemach z płynnością finansową swojego pracodawcy, która wzbudza u nich obawy o stabilność zatrudnienia, a tym samym zdolność pokrycia zobowiązań finansowych. Rodzi się pytanie, skąd atakujący wiedzieli, jakich informacji użyć.

Tu właśnie przychodzi im z pomocą metoda mozaikowa, za pomocą której dane z różnych wycieków mogą „skleić" i w ten sposób stworzyć spójny obraz i adekwatny model działania. Dzięki temu w tym samym czasie „atakowani" pracownicy zaczynają otrzymywać ciekawe oferty pracy, spersonalizowane, kierowane przez osoby, które najwyraźniej dokładnie znają ich kompetencje i je „doceniają"... Tak przeprowadzona operacja, nawet gdyby bazowała na fałszywych ofertach pracy, może zaburzyć projekt, a jeśli osoby poddane takiemu działaniu odczują niepewność, potrzeba poszukiwania pracy pojawi się u nich w sposób naturalny, co może doprowadzić do problemu z wdrożeniem tej przykładowej modernizacji linii produkcyjnej. Modernizacja linii produkcyjnej jest tu oczywiście tylko przykładem.

Kolejnym zagrożeniem jest precyzyjne niszczenie reputacji – zarówno przedsiębiorstwa, jak i jego pracowników. Niedawno mieliśmy okazję obserwować, w jaki sposób, dzięki posiadanym numerom telefonów oraz danych ich użytkowników, Aleksiej Nawalny był w stanie pozyskać dużą ilość informacji o zamachu na jego życie, dzwoniąc bezpośrednio do osób zaangażowanych w tę sprawę. To uzmysławia nam, że skoro w służbach specjalnych telefonicznie można uzyskać wrażliwe informacje, tym bardziej będzie to możliwe w organizacjach, w których poufność nie ma tak wysokiego priorytetu. Tak więc wyciek danych z telefonami daje możliwość kontaktu z osobami, od których analogicznymi metodami można pozyskać wrażliwe informacje biznesowe, i nie tylko. To obszar szczególnie ryzykowny, w ten sposób bowiem można pozyskać nie tylko tajemnice firmowe, ale także informacje budujące wiedzę o sprawach wewnętrznych, relacjach, atmosferze panującej w infiltrowanym przedsiębiorstwie. A stąd już jest bardzo blisko do zagrożeń dużo poważniejszych, łącznie z działaniami w zakresie szantażu i niszczenia reputacji.

Wreszcie możliwość bezpośredniego bądź pośredniego wywierania presji. Wyciek danych, zwłaszcza z numerami telefonów, pozwala na bezpośredni kontakt z wybranymi pracownikami. W ten sposób pracownik będzie angażowany w niepożądaną komunikację, niosącą jeszcze większy ładunek emocjonalny niż komunikacja e-mailowa, a przy dużym natężeniu niechcianych telefonów i wiadomości tekstowych czy multimedialnych może wystąpić potrzeba zmiany numeru telefonu, co powoduje kolejne problemy natury organizacyjnej.

Jak wiadomo, wyciek danych z platformy szkoleniowej KSSiP zmaterializował się wysyłaniem wiadomości z bramki internetowej, ale każdy SMS sprawca zaczynał od poprawnego imienia adresata. Dlaczego więc nie miałoby tak stać się w przypadku biznesu? Kluczowy jest motyw. Jeśli będzie, działanie takie jest w biznesie równie prawdopodobne, jak w sektorze publicznym. A walka konkurencyjna takim motywem bezsprzecznie może być, bo przecież wiadomo, że nie wszyscy konkurenci zachowują się etycznie, tym bardziej środowisko przestępcze.

Jak więc widać, wykazy i listy przygotowywane w różnych celach mogą nieść duży ładunek ryzyka, dlatego każde tego typu działanie należy rozpatrywać z różnych perspektyw, także szukając zagrożeń pozornie z nimi niezwiązanych. Stąd kolejny wniosek, że świadomość ciągle jest sprawą kluczową, zarówno na etapie tworzenia baz danych, nawet tych „chwilowych", jak wykazy osób szczepionych, jak i na etapie zarządzania systemami informatycznymi i w zakresie zasad pozyskiwania, a zwłaszcza przekazywania informacji.

Świadomość bezpieczeństwa informacji gromadzonych w systemach IT w obecnych czasach jest widoczna niemal na każdym kroku. Jednak (jak pokazują przykładowe incydenty) pomyłki zdarzają się wszędzie, a więc niezbędne jest tworzenie procedur reagowania zarówno na incydent, jak i incydenty wtórne. W ten sposób RODO pomaga zarządzać ryzykiem przedsiębiorstwa, ale postrzeganie tych regulacji tylko przez pryzmat wysokich kar jest błędne.

Drugim ważnym ogniwem tego systemu jest bezpieczeństwo informacji posiadanych przez nas. Tematowi temu poświęcony był artykuł „*Bezpieczeństwo informacji z perspektywy praktyka*"[3]. W przypadkach zagrożenia wyciekiem informacji – kiedy to każdy z nas może być nie tylko celem ataku, ale także elementem ataku, z reguły nieświadomym – umiejętność właściwego dysponowania posiadanymi informacjami, zachowanie zasady wiedzy koniecznej w rozmowach i komunikacji e-mailowej jest tak samo ważne, jak cały kompleks bezpieczeństwa cybernetycznego. Stąd tak duża rola kształtowania świadomości bezpieczeństwa informacyjnego.

Wreszcie aspekt łączący nasze życie osobiste z biznesowym. Numery telefonów, adresy poczty elektronicznej, a przed wszystkim dane jeszcze bardziej wrażliwe, takie jak numer PESEL, łączą nasze bezpieczeństwo osobiste z bezpieczeństwem przedsiębiorstwa, w którym pracujemy. Dane te pozwalają nam autoryzować osobiste transakcje i decyzje, ale także funkcjonują w autoryzowaniu decyzji podejmowanych w imieniu pracodawcy. Stąd obie strony powinny zapewnić ochronę tych danych, a jej sposób musi być przemyślany jeszcze przed rozpoczęciem ich przetwarzania.

1) https://www.cyberdefence24.pl/wyciek-danych-z-rcb-co-zrobiono-by-chronic-funkcjonariuszy (dostęp: 5.05.2021).
2) https://gdpr.pl/prawdopodobnie-najwiekszy-dotychczas-wyciek-danych-osobowych (dostęp: 5.05.2021).
3) https://aspolska.pl/bezpieczenstwo-informacji-perspektywy-praktyka/ (dostęp: 5.05.2021).

JACEK GRZECHOWIAK

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

Kamera pokładowa

pomoc w identyfikacji usterek w środkach transportu

Axis Communications prezentuje urządzenie AXIS P3925-LRE – nową, solidną i kompaktową kamerę pokładową do zastosowań zewnętrznych.

Kamera została skonstruowana z myślą o potrzebach branży transportowej i jest zgodna z normami branżowymi, w tym EN50155 i EN45545-2. Urządzenie jest zaprojektowane do monitorowania scen z boku autobusów, pociągów i innych pojazdów. Kamera może również pomagać w identyfikacji koniecznych napraw eksploatacyjnych, a więc w utrzymaniu taboru. Przykładowo, może monitorować zużycie taśmy kolektora pantografu. Dzięki funkcji Forensic WDR kamera oferuje doskonałą jakość obrazu o rozdzielczości HDTV 1080p, nawet gdy w obserwowanej scenie występują zarówno ciemne, jak i jasne obszary. Ostre kolorowe obrazy, również w słabych warunkach oświetleniowych, zapewnia ponadto technologia Lightfinder. Dzięki wbudowanym diodom podczerwieni urządzenie może dozorować w całkowitej ciemności.

Model AXIS P3925-LRE oferuje ulepszone funkcje bezpieczeństwa, takie jak podpisane oprogramowanie sprzętowe i funkcja bezpieczny start, które pozwalają zapobiec nieautoryzowanemu dostępowi i zabezpieczają system. Z kolei funkcja detekcji wstrząsów wysyła automatyczne powiadomienie o sabotażu w przypadku naruszenia obudowy kamery. Najważniejsze cechy kamery:

- zgodność z EN50155 i EN45545-2,
- oświetlenie IR oraz elektroniczna stabilizacja obrazu (EIS),
- technologie Lightfinder i Forensic WDR,
- podpisane oprogramowanie i bezpieczny start.

Więcej na: www.axis.com/pl

Sztuczna inteligencja i mechanizmy głębokiego uczenia

w nowej kamerze Axis

Axis Communications prezentuje nową kamerę P3255-LVE, która ma funkcje analizy obrazu wsparte algorytmami sztucznej inteligencji i mechanizmami głębokiego uczenia. Ta wszechstronna stałopozycyjna kamera kopułkowa zawiera innowacyjny podwójny chipset, umożliwiający szczegółową klasyfikację obiektów.

Wspomniany chipset – łączący procesor Axis ARTPEC-7 oraz jednostkę przetwarzania głębokiego uczenia – to klucz do udostępnianych przez kamerę funkcji klasyfikacji obiektów. Tak zaawansowane elementy sprzętowe umożliwiają użytkownikom korzystanie ze specjalnie opracowanych aplikacji zewnętrznych opartych na funkcjach AI.

Ponadto, dzięki podwójnemu chipsetowi, fabrycznie zainstalowana aplikacja analityczna AXIS Object Detector może wykrywać oraz klasyfikować osoby i obiekty, a także rozróżniać takie typy pojazdów, jak samochody osobowe, autobusy, samochody ciężarowe oraz jednoślady (motocykle i rowery).

Wyposażenie urządzenia w podwójny chipset sprawia też, że analizy mogą być wykonywane bezpośrednio w kamerze (na brzegu sieci), co zwiększa szybkość działania i skalowalność systemu. Inne korzyści obejmują: przetwarzanie w czasie rzeczywistym, redukcję kosztów i obniżenie stopnia złożoności systemu. Ponadto przez sieć przesyłany jest tylko niezbędny materiał wizyjny, co ogranicza zapotrzebowanie na pamięć masową i przepustowość oraz zmniejsza obawy dotyczące prywatności.

Ta gotowa do montażu zewnętrzna kamera o klasie ochrony obudowy IK10 zawiera szereg funkcji bezpieczeństwa, które zapobiegają nieautoryzowanemu dostępowi. Urządzenie oferuje znakomitą jakość obrazu o rozdzielczości HDTV 1080p. Technologie Axis Lightfinder 2.0 i Axis Forensic WDR zapewniają realistyczne kolory i wierne odwzorowanie szczegółów, nawet w trudnych warunkach oświetleniowych.

Dodatkowo technologia OptimizedIR pozwala uzyskiwać wyraźny, pozbawiony odbić materiał wizyjny w całkowitej ciemności bez stosowania dodatkowego oświetlenia.

Najważniejsze cechy kamery:

- zaawansowane funkcje AI z mechanizmami głębokiego uczenia,
- szczegółowa klasyfikacja obiektów,
- obsługa aplikacji AI innych firm,
- przetwarzanie na brzegu sieci — łatwa skalowalność,
- Lightfinder 2.0, Forensic WDR, OptimizedIR.

Więcej na: www.axis.com/pl

Nowe kamery Wisenet P z AI

Hanwha Techwin poszerza swoją ofertę sprzętową o 5 nowych kamer full HD z serii Wisenet P, które uzupełniają modele o rozdzielczości 4K wprowadzone na rynek w 2020 r. Dzięki temu kamery z algorytmami sztucznej inteligencji stają się bardziej przystępne cenowo dla użytkowników o ograniczonym budżecie.

Wszystkie modele Wisenet P mają funkcję analizy treści obrazu wspieraną sztuczną inteligencją i głębokim uczeniem. Zapewnia to wysoką precyzję wykrywania obiektów, przy jednoczesnym zmniejszeniu liczby fałszywych alarmów.

Algorytmy Wisenet AI określają, na podstawie rozpoznanych cech (wiek, płeć, kolor ubrania, czy dana osoba nosi okulary, trzyma torbę), atrybuty osób i zapisują je jako metadane wraz z obrazami, co umożliwia użytkownikom szybkie wyszukiwanie określonych obiektów lub incydentów w zarejestrowanym materiale wizyjnym. W tym celu operatorzy systemów mogą korzystać z oprogramowania VMS wiodących producentów, np. Genetec i Milestone, a także z pakietów Wisenet WAVE i Wisenet SSM.

Kamery mają wbudowaną aplikację firmy Hanwha Techwin do określania liczby osób przebywających na wyznaczonym obszarze. Można ją wykorzystać do sterowania automatycznie otwieranymi drzwiami lub sygnalizatorami drogowymi, a także do wyświetlania komunikatów typu: „czekaj"' lub „wejdź", gdy przekroczony zostanie dopuszczalny limit. Użytkownicy nie muszą ponosić kosztów zakupu licencji, aby korzystać z wyrafinowanych funkcji realizowanych przez te aplikacje.

Nowe kamery korzystają z funkcji WiseStream III optymalizującej proces kompresji obrazu. Obrazy obiektów wykrywanych i śledzonych przez algorytmy AI są słabiej kompresowane, przy jednoczesnym zastosowaniu silnej kompresji pozostałych fragmentów kadru. W połączeniu z kompresją H.265 poprawia to wykorzystanie pasma sieciowego nawet o 80% w porównaniu z H.264. Aby jeszcze lepiej wykorzystać przepustowość sieci i zmniejszyć wymagania dotyczące pamięci masowej, a także ułatwić pracę operatorów systemu, kamery mają wbudowaną funkcję BestShot, która wybiera najlepsze z uchwyconych zdjęć osób lub obiektów i wysyła je wraz z powiązanymi metadanymi do serwera zapisującego materiał wizyjny.

Nowe, przystępne cenowo kamery z serii Wisenet P udowodnią, że systemy monitoringu wizyjnego wykorzystujące sztuczną inteligencję nadają się nie tylko do kosztownych zastosowań o znaczeniu krytycznym – powiedział Uri Guterman, dyrektor ds. produktów i marketingu w Hanwha Techwin Europe. – *Istniejące liczne aplikacje, w których informacje biznesowe są pozyskiwane drogą inteligentnej analizy treści obrazu, zapewnią wysoką stopę zwrotu z inwestycji, niezależnie od tego, gdzie zostaną wdrożone.*

Więcej na www.hanwha-security-eu

Integracja systemu RACS 5

z oprogramowaniem Milestone VMS XProtect

System kontroli dostępu i automatyki budynkowej RACS 5 oferuje możliwość integracji z oprogramowaniem VMS XProtect firmy Milestone Systems A/S. Możliwe są dwa scenariusze integracji, przy czym mogą one być wykorzystywane współbieżnie.

W pierwszym z nich zdarzenia z systemu KD są przekazywane do oprogramowania VMS, gdzie podlegają prezentacji i przetwarzaniu na identycznych zasadach, jak zdarzenia pochodzące z innych systemów bezpieczeństwa budynku, m.in. mogą być prezentowane na zaawansowanych graficznie i funkcjonalnie mapach obiektu. W scenariuszu tym możliwe jest też wydawanie poleceń sterujących przejściami i monitorowanie ich statusu. Kolejną możliwością jest zdalna autoryzacja dostępu i prezentacja alarmów z systemu KD. W drugiej z dostępnych form integracji oprogramowanie systemu KD może pobierać zdjęcia i wideo z systemu VMS na podobnych zasadach, jak z rejestratorów telewizji dozorowej.

Integracja systemu RACS 5 z oprogramowaniem VMS XProtect umożliwia jego wykorzystanie w obiektach wymagających zaawansowanych form dozoru i monitorowania pracy systemu z udziałem służb ochrony prowadzącej ciągły lub interwencyjny dozór wizyjny budynku, a także w tych systemach, gdzie wymagana jest wizualizacja pracy całego systemu bezpieczeństwa w zintegrowanym środowisku wideo.

Więcej na www.roger.pl

Incedo Business firmy ASSA ABLOY

Skuteczna ochrona budynków wielkopowierzchniowych to dziś szczególne wyzwanie. Administratorzy i menedżerowie obiektów coraz częściej poszukują elastycznych i skalowalnych rozwiązań zapewniających bezpieczeństwo podczas pracy zdalnej, umożliwiających skuteczne zarządzanie dostępami dla pracujących w systemie hybrydowym oraz gwarantujących wyeliminowanie obecności osób nieuprawnionych. Wiąże się to także z wyzwaniami dla instalatorów i integratorów, którzy muszą sprostać oczekiwaniom swoich klientów. Ważne dla wszystkich jest, aby system KD był łatwy i wygodny w początkowej fazie instalacji, a także umożliwiał wprowadzanie późniejszych modyfikacji.

Przykładem takiego rozwiązania jest Incedo Business firmy ASSA ABLOY. Łączy on niezbędny osprzęt i oprogramowanie, jest rozwiązaniem bogatym w funkcje i nie wymaga dedykowanego komputera PC.
Umożliwia także administrowanie z dowolnego miejsca w dowolnym momencie, dlatego zarządzanie systemami klientów odbywa się szybciej – bez konieczności dojazdu na miejsce. Takie rozwiązanie sprawia, że integratorzy mogą sprawnie modernizować połączone technologie i systemy, aby spełniać rosnące oczekiwania klientów wobec nowoczesnych technologii. Instalatorzy zaś nie muszą już zmagać się z niekompatybilnymi systemami, co eliminuje opóźnienia i niepotrzebne komplikacje.
Z kolei użytkownicy systemów KD oczekują wygody i dopasowania do codziennych potrzeb. Dlatego należy wybrać sprzęt zabezpieczający i dane uwierzytelniające dostosowane do ich wymagań oraz odpowiednią opcję systemu zarządzania.
Ważnym udogodnieniem jest prosty w obsłudze interfejs użytkownika, do którego administrator ma szybki dostęp. Coraz częściej spotykane w nowoczesnych rozwiązaniach z obszaru KD są też klucze mobilne, umożliwiające otwieranie drzwi za pomocą smartfona.
Optymalnym rozwiązaniem są systemy, które można w razie potrzeby skalować w górę (rozbudowywać) i w dół (likwidacja przejścia KD), co maksymalizuje zwrot z inwestycji.
– *Nasza firma postanowiła wprowadzić na rynek globalne rozwiązanie zapewniające integrację produktów związanych z kontrolą dostępu z portfolio ASSA ABLOY i firm będących w naszej grupie. Dostępna będzie też platforma integracyjna zapewniająca współpracę systemu KD z innymi systemami security: SSWIN, CCTV, wideodomofony, czytniki biometryczne, depozytory kluczy i system „Master Key". W planach jest integracja z systemami sterowania windami i automatyką budynkową. Jednocześnie możliwa będzie integracja po API dowolnie wybranych przez klientów systemów firm trzecich* – mówi Beata Idziak, Business Development Manager DAS z firmy ASSA ABLOY Opening Solutions Poland.

www.assaabloyopeningsolutions.pl/pl/

Telbud zmodernizuje system zabezpieczeń technicznych

w oddziałach PGE Energia Odnawialna

Postępowanie przetargowe w trybie negocjacji z ogłoszeniem na „Modernizację systemu zabezpieczeń technicznych w oddziałach PGE Energia Odnawialna" zostało ogłoszone 25 stycznia 2019 r. Procedura przetargowa obejmowała składanie wniosków, ofertę wstępną, negocjacje oraz ofertę ostateczną. Wynik postępowania przetargowego ogłoszono 7 kwietnia 2021 r. Najkorzystniejszą ofertę przedstawiła firma Telbud.

Modernizacja, której celem jest zwiększenie poziomu bezpieczeństwa obiektów, będzie dotyczyła czterech oddziałów PGE EO SA: ZEW Porąbka Żar w Międzybrodziu Bialskim, ZEW Dychów w Bobrowicach, EW Żarnowiec w Czymanowie i ZEW Solina Myczkowce w Solinie.
Telbud zrealizuje takie prace, jak:

- budowa rozwiązań korelujących działania zintegrowanych systemów ochrony i automatyzację pracy tych systemów,
- wdrożenie technologii identyfikujących awarie, zagrożenia i sytuacje alarmowe,
- wdrożenie mechanizmów analizy zdarzeń i zagrożeń, wspomagających podejmowanie decyzji,
- zautomatyzowanie raportowania o stanie bezpieczeństwa obiektów dla wsparcia operatorów, administratorów i nadzoru,
- uruchomienie zaawansowanych mechanizmów bezpieczeństwa cyfrowego,
- modernizacja systemów analizy obrazu,
- zastosowanie rozwiązań rejestrujących działania operatorów,
- wdrożenie innowacyjnych technik radarowych dla procesu szybkiej identyfikacji zagrożeń.

Więcej informacji na: www.telbud.pl

Wykryj pożar, póki NIE jest za późno!

Pożary, które nie zostaną wcześnie wykryte i szybko ugaszone, mogą mieć tragiczne konsekwencje – spowodować utratę życia bądź zdrowia, a także przyczynić się do poważnych strat finansowych oraz negatywnie wpłynąć na środowisko naturalne, a w efekcie zaburzyć ciągłość działania firmy.

W niektórych przedsiębiorstwach ryzyko wystąpienia pożaru jest tak duże, że wczesna jego detekcja musi być traktowana priorytetowo. Niestety większość systemów przeciwpożarowych została zaprojektowana w taki sposób, że sygnalizuje pożar już po jego pojawieniu się. Takie działanie nie jest najskuteczniejszym rozwiązaniem, szczególnie w miejscach, gdzie do rozprzestrzeniania się ognia może dojść bardzo szybko.
System, który pozwala zapobiec pożarom, zanim jeszcze wystąpią, ratuje życie i zapobiega stratom finansowym, jest rozwiązaniem optymalnym. Wczesna detekcja jest możliwa dzięki kamerom termowizyjnym FLIR A400/A700. Ogień pojawia się na skutek wzrostu temperatury. Kamera termowizyjna monitorująca wybrany obszar bardzo sprawnie lokalizuje miejsca o podwyższonej temperaturze. Odczyty pomiarowe mogą być aktualizowane do 60 razy na sekundę, co gwarantuje imponującą szybkość detekcji zagrożenia. Dane są w czasie rzeczywistym analizowane przez kamerę, co przyspiesza sygnalizację sytuacji alarmowych.
Kamery FLIR A400/A700 mogą być także zintegrowane ze sterownikami PLC w celu np. natychmiastowego zatrzymania produkcji lub zmiany wybranych parametrów procesów. Te modele kamer FLIR mają zakres pomiarowy od -40°C do +2000°C. Możliwość dokładnego pomiaru temperatury pozwala na szybką i skuteczną detekcję miejsc będących źródłem/zarzewiem pożaru lub w których dochodzi do przegrzewania pewnych elementów infrastruktury technicznej. Dzięki temu można uruchomić procedurę alarmową, jeszcze zanim pożar się rozwinie.

Więcej na www.linc.pl

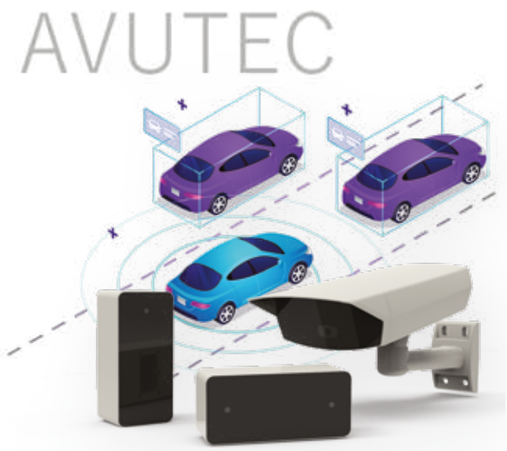
AVUTEC Gatekeeper-X

otwarty na przyszłość

AVUTEC jest producentem kamer z wbudowanymi algorytmami sztucznej inteligencji (AI) oferującymi ekonomiczne i praktyczne aplikacje analityczne. Nowe technologie zastosowane w urządzeniach i oprogramowaniu przekładają się na produkty, które odzwierciedlają zalety sztucznej inteligencji.

Dzięki inteligentnym kamerom Gatekeeper z serii X firma AVUTEC wybiega w przyszłość. Zwiększona moc obliczeniowa i wysokiej jakości analiza obrazu oparta na algorytmach AI zmieniają kamery w szybkie i dokładne urządzenia ze sztuczną inteligencją.
Kamery Gatekeeper-X są wyposażone w przetwornik obrazu czuły na promieniowanie z zakresu podczerwieni, diody (oświetlacze) podczerwieni oraz filtr światła dziennego, co sprawia, że doskonale sprawdzają się w zastosowaniach ARTR (Automatyczne Rozpoznawanie Tablic Rejestracyjnych). Zaimplementowane aplikacje analityczne klasyfikują obiekty i śledzą ruch samochodów, a procesory o dużej mocy obliczeniowej wspierane mechanizmami uczenia maszynowego pozwalają na równoległe działanie funkcji ARTR.
Kamery zostały zaprojektowane zarówno do pracy samodzielnej, jak i integracji z innymi systemami. Kamera oferuje technologię identyfikacji do zastosowań, których podstawowym celem są dokładność, szybkość i automatyzacja.
Gatekeeper X znajduje zastosowanie m.in. w systemach parkingowych, *smart city,* logistyce oraz wielu innych, zwiększając bezpieczeństwo, wygodę lub usprawniając zarządzanie ruchem osób i pojazdów.
Kamery z serii X można spotkać również w myjniach samochodowych, przemyśle motoryzacyjnym i hotelarskim, gdzie zapewniają bezobsługową, szybką i zaawansowaną technologicznie obsługę klienta.

Więcej na: www.smart-i.pl



Europejski rynek chmury

Francuski oddział firmy KPMG na zlecenie liderów branży – InfraNum, Talan, OVHcloud oraz Linkt – opracował raport analizujący główne wyzwania związane z usługami w chmurze w Europie w nadchodzących latach oraz prognozujący pięć scenariuszy do roku 2027 (2030).

W latach 2017–2019 rynek przetwarzania danych w chmurze (zogniskowany wokół trzech modeli usług: SaaS – oprogramowanie jako usługa, PaaS – platforma jako usługa, IaaS – infrastruktura jako usługa) rósł w Europie o 27 proc. rocznie. Szacuje się, że wartość ta ma osiągnąć od 300 do 500 mld euro do roku 2027 (2030). Pandemia COVID-19 przyśpieszyła przechodzenie na usługi chmurowe, co dowiodło ich strategicznej roli jako kluczowego składnika infrastruktury i czynnika odporności. Aż 82 proc. ankietowanych zaczęło w szerszym zakresie korzystać z chmury w bezpośredniej reakcji na pandemię.

Pięć scenariuszy dla europejskiego rynku:

- Chmura rozumiana jako dobro wspólne.
- Wzrost znaczenia graczy europejskich.
- Wprowadzenie daleko idących regulacji.
- Europeizacja działalności głównych nieeuropejskich graczy.
- Funkcjonalne lub strukturalne oddzielenie działalności chmurowej od innych rodzajów działalności operatorów chmurowych.

Europejski rynek chmury jest zdominowany przez trzech głównych graczy („hiperskalerów"), którzy mają aż 70 proc. udziału w rynku IaaS: Amazon AWS (53 proc.), Microsoft Azure (9 proc.) i Google Cloud (8 proc.). Jednak europejscy dostawcy usług chmurowych i operatorzy telekomunikacyjni wciąż zyskują na znaczeniu na swoich macierzystych rynkach. Przykładowo OVHcloud i Deutsche Telekom zajmują odpowiednio trzecie i czwarte miejsce w swoich krajach na rynku infrastrukturalnym i platformowym.
Raport pokazuje, że przyszłość europejskiej chmury może łączyć kilka scenariuszy z różnym horyzontem czasowym. Przy braku znaczących zmian w porównaniu z obecną sytuacją, gdyby dominacja „hiperskalerów" miała się umocnić, Europa może stracić od 20 do 50 proc. szacowanych korzyści gospodarczych z rynku przetwarzania danych w chmurze.

Kluczowe wnioski

- Pandemia COVID-19 zdynamizowała wdrażanie usług chmurowych w firmach. Migracja motywowana jest optymalizacją operacyjną i finansową.
- Europejski rynek chmury czekają wyzwania: szacuje się, że do 2027 roku powstanie tu ponad 500 tys. miejsc pracy, a skumulowane inwestycje wyniosą około 200 mld euro.
- Rośnie rola europejskich ekspertów na lokalnych rynkach w sektorze uprzednio zdominowanym już przez trzech amerykańskich graczy.
- Bez podjęcia strategicznych decyzji Europa może stracić nawet połowę zarówno ekonomicznych, jak i społecznych korzyści wynikających z rozwoju rynku technologii chmurowych.

Nowe ataki ransomware

Ransomware, phishing, uszkodzenie plików i socjotechniki – tych ataków obawiamy się najbardziej. Cyberprzestępczość kosztuje rocznie ponad 1 bilion dolarów, z czego tylko ataki szyfrujące generują straty w wysokości 20 miliardów USD. Takie statystyki płyną z raportu „Cyberzagrożenia: cyberpułapki i jak nie paść ofiarą hakerów" opracowanego przez Xopero Software przy współpracy z ekspertami z siedmiu firm, m.in. QNAP, CERT Orange Polska, Sophos, WatchGuard czy TestArmy.

Ransomware to rodzaj oprogramowania, ale też technika ataku polegająca na blokadzie dostępu do danych lub całego systemu komputerowego. Celem jest wymuszenie zapłaty okupu za jego odblokowanie lub odszyfrowanie danych. Stąd też nazwa tego typu programów – ransom, czyli okup, oraz software – oprogramowanie.
Według badań ankietowych Xopero Software ataków ransomware obawia się najwięcej, bo blisko 80 proc. przedsiębiorców. Niewątpliwie wpływ mają na to koszty tych ataków i ich częstotliwość. Na początku 2016 r. ransomware uderzał co 2 minuty, trzy lata później mówiono o 14 sekundach, a w tym roku czas ten skróci się do 11 sekund! W trakcie czytania tego akapitu ktoś właśnie padł jego ofiarą.

Według danych Cybersecurity Ventures wartość globalnych szkód spowodowanych przez ransomware jeszcze w 2019 r. szacowano na 11,5 miliarda dolarów (dla porównania, w 2015 było to 325 milionów!). To samo źródło podaje, że w tym roku straty te wyniosą nawet 20 miliardów dolarów, czyli blisko dwukrotnie więcej.

W tym roku mamy rekordową wysokość żądanego okupu. 50 milionów dolarów – takiej kwoty oczekuje grupa REvil od firmy Acer, która padła ofiarą ransomware w marcu tego roku. Przestępcy grożą upublicznieniem skradzionych informacji w przypadku braku uzyskania płatności.

www.xopero.com/pl/

Gdy ochrona jest sztuką

Wykrywanie włamania

Bezpieczeństwo przeciwpożarowe

Zapobieganie zalaniu

Automatyka domu

Weryfikacja fotograficzna alarmów

Miłego oglądania

Darmowe aplikacje dla instalatorów i użytkowników końcowych

www.ajax.systems

macOS Windows iOS Android