CZASOPISMO RYNKU SECURITY

a&s POLSKA

04 (28) 07/08 2021

Przyszłość security

Redefinicja

NOWOCZESNE TECHNOLOGIE

WSZYSTKO ZDEFINIOWANE PROGRAMOWO

Wkroczyliśmy w erę, kiedy wartość zdecydowanie przesuwa się ze sprzętu na oprogramowanie. Także w naszej branży pojawia się coraz więcej aplikacji umożliwiających dostosowanie pracy kamer do różnych wymagań użytkownika.

RYNEK SECURITY

TRENDY W KONTROLI DOSTĘPU

Pandemia wpłynęła na rozwój systemów KD zarówno w zakresie zastosowania nowoczesnych technologii, jak i poszerzenia ich funkcjonalności. Wybór rozwiązania jest trudny, musi uwzględniać spełnienie potrzeb wszystkich interesariuszy.

TEMAT NUMERU

BEZPIECZNE HOTELE I INSTYTUCJE FINANSOWE

Ze względu na specyfikę i przeznaczenie obiektów wymagany stopień zabezpieczenia w obu sektorach jest wyraźnie różny. Branża security oferuje rozwiązania spełniające wszystkie kryteria – od wygody obsługi po cyberbezpieczeństwo.

APLIKACJA MOBILNA

www.aspolska.pl

ISSN 2451-5175

9 772451 517703 05

15 zł (w tym 8% VAT)

EDYTORIAL

Drodzy Czytelnicy

To wydanie otwieramy ciekawym wywiadem – osoba spoza branży security, propagator wprowadzania nowych technologii, dzieli się z pozycji użytkownika spostrzeżeniami, doświadczeniami i odczuciami dotyczącymi ich wdrażania w elektronicznych systemach zabezpieczeń (s. 16). Dostrzega przy tym granice, ale racjonalne, związane z ochroną prywatności, ochroną danych osobowych. Czy nasza branża jest otwarta na nowe technologie, potrafi w pełni wykorzystać ich ogromny potencjał? Jak promować rozwiązania polskich start-upów technologicznych wdrażane w branży security, by je pokazać w sposób atrakcyjniejszy? Nasz rozmówca kończy swe rozważania z przekonaniem, że przyszłość należy do sztucznej inteligencji i nie widzi jej w czarnych barwach...

Kontynuując wątek technologiczny, wiele popularnych terminów funkcjonujących w dzisiejszym świecie technologii IT staje się częścią szerszego trendu, zwanego Wszystko Zdefiniowane Programowo. Wkroczyliśmy w erę, kiedy wartość zdecydowanie przenosi się ze sprzętu na oprogramowanie. Ta zmiana zaczyna dotykać także naszą branżę, a coraz większa liczba dostawców kamer zajmuje się promowaniem aplikacji dla różnych scenariuszy bezpieczeństwa. Kamera definiowana programowo – co to oznacza dla użytkowników systemów zabezpieczeń, wyjaśniamy na s. 24.

Gdy w poddanej dozorowi CCTV celi (stale obserwowanej przez operatora) ginie kolejny osadzony, skuteczność monitoringu jest kwestionowana. Podstawowym celem wieloletnich badań i analiz prowadzonych przez autorów jest przeciwdziałanie samobójstwom i alarmowanie presuicydalne. Koncepcja ich zaawansowanych prac projektowych obejmuje zastosowanie inteligentnej analizy obrazu oraz uczenia maszynowego (s. 32).

W świecie zagrożonym kolejnymi falami pandemii systemy kontroli dostępu oferują coraz więcej. Analitycy portalu asmag.com wskazują kilka trendów technologicznych, które będą kształtować światowy rynek KD w 2021 r. (s. 44). Czy są one zbieżne z potrzebami użytkowników? Zapytaliśmy o to przedstawicieli firm oferujących te rozwiązania na rynku polskim (s. 48). Skutki pandemii szczególnie mocno odczuły branże hotelarska i finansowa. Opinię ekspertów nt. sytuacji w obu sektorach rynku przedstawiamy na s. 66.

W tym wydaniu rozpoczynamy dyskusję o Health-Safety--Environment. Czym HSE różni się od BHP, wyjaśniamy na s. 70. Tematykę kontynuuje artykuł o problemach projektowych i uruchomieniowym w obiektach szpitalnych (s. 74).

Zapewnienie bezpieczeństwa cybernetycznego jest cały czas poważnym wyzwaniem. Wprawdzie budujemy zaawansowany system zabezpieczeń i uważamy, że mamy „szczelny" system ochrony, tymczasem okazuje się, że praktycznie sami wpuszczamy intruza... (s. 76).

Mamy nadzieję, że po kilkunastu miesiącach pandemicznych restrykcji spotkamy się wszyscy 6 września na kolejnej edycji Warsaw Security Summit. Tym razem konferencję organizujemy w formule hybrydowej: stacjonarnej (w hotelu Sheraton w Warszawie) oraz online (transmisja live). Zapraszamy do rejestracji na WarsawSecuritySummit.eu Do zobaczenia!

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

04

28

07/08

2021

SPIS TREŚCI

RYNEK SECURITY

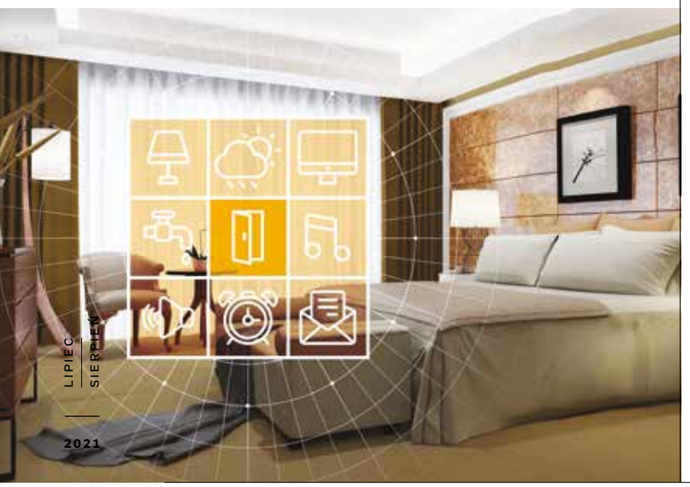
SPIS TREŚCI

HOTELE I INSTYTUCJE FINANSOWE

HEALTH, SAFETY, ENVIRONMENT

CYBERBEZPIECZEŃSTWO

SERWIS INFORMACYJNY



ASCS

www.ascs.pl

Uzupełnienie systemu CCTV o funkcje głosowe

W CELU ZAPEWNIENIA BEZPIECZEŃSTWA PRZESTRZEŃ PUBLICZNA JEST STALE OBSERWOWANA PRZEZ KAMERY CCTV/VSS. JEDNAK SAMA OBSERWACJA JEST TYLKO PASYWNĄ FORMĄ OCHRONY. ZWIĘKSZENIE POZIOMU BEZPIECZEŃSTWA WYMAGA INTERAKCJI Z OBSERWOWANYM OBSZAREM.

Taką interakcję, a dzięki temu aktywną ochronę, zapewniają głośniki IP. Operatorzy systemu monitoringu w momencie zauważenia incydentu mają możliwość zdalnego nadania komunikatu do uczestników zdarzenia, zapewniając w ten sposób skuteczne działanie prewencyjne zanim jeszcze dojdzie do powstania szkody.

ASCS Sp. z o.o. posiada w swojej ofercie portfolio głośników IP zarówno wewnętrznych, jak i zewnętrznych. Mają one możliwość nadawania komunikatów na pojedynczy głośnik IP lub grupę takich głośników.
Komunikaty mogą być nadawane „na żywo" przez operatora lub odtwarzane z pliku przechowywanego w pamięci głośnika. Głośnik tubowy IP VCLH3002 ma moc 30 W i maks. głośność 125 dB. Jest wyposażony w dwa porty Ethernet, 16 wejść, do których można podłączyć zewnętrzne sygnały, dwa przekaźniki umożliwiające wysterowanie sygnalizatora czy otwarcie wejścia oraz jedno wyjście.
Ponadto, dzięki możliwości podłączenia mikrofonu i przycisku, głośnik może pełnić funkcję punktu Info/SOS.

Głośnik obsługuje protokół SIP i może pracować w trybie bezserwerowym P2P lub zostać podłączony do serwera VoIP.

AXIS COMMUNICATIONS

www.axis.com/pl

Nowa panoramiczna kamera wieloprzetwornikowa Axis

FIRMA AXIS COMMUNICATIONS WPROWADZIŁA NA RYNEK AXIS Q3819-PVE – WIELOPRZETWORNIKOWĄ KAMERĘ O ROZDZIELCZOŚCI 14 MPIX, OFERUJĄCĄ PŁYNNY, 180-STOPNIOWY WIDOK PANORAMICZNY, WYSOKĄ JAKOŚĆ OBRAZU I POKLATKOWOŚĆ NA POZIOMIE 30 KL./S. DZIĘKI PŁYNNEMU SCALANIU CZTERECH WIDOKÓW KAMERA W POJEDYNCZYM STRUMIENIU WIZJI DOSTARCZA SPÓJNIE WYGLĄDAJĄCY OBRAZ BEZ JAKICHKOLWIEK ŚLADÓW ŁĄCZENIA.

Poza bezszwowym łączeniem obrazu nowa kamera wieloprzetwornikowa udostępnia także funkcję inteligentnego parowania z głośnikami sieciowymi Axis przy użyciu technologii *edge-to-edge*. Dzięki temu można np. emitować ostrzeżenia skierowane do intruzów.
Ponadto aplikacja AXIS Object Analytics umożliwia detekcję oraz klasyfikację ludzi i pojazdów. Funkcja Axis Edge Vault chroni identyfikator urządzenia Axis i upraszcza ich autoryzację w sieci. Natomiast moduł TPM *(Trusted Platform Module)* z certyfikatem FIPS 140-2 na poziomie 2. zapewnia bezpieczne przechowywanie wszystkich kluczy kryptograficznych i certyfikatów, nawet w razie naruszenia zabezpieczeń.
Nowe urządzenie można montować na wiele sposobów – na płaszczyźnie, we wnęce, w pozycji wiszącej, a nawet tyłem do drugiego egzemplarza. Kamera ma też wbudowane silniki, które umożliwiają zdalne sterowanie funkcjami obrotu, pochylenia i przechylenia *(pan/tilt/roll)*.

BCS

www.bcscctv.pl

TEGO LATA W OFERCIE BCS POJAWIŁA SIĘ NOWA SERIA KAMER NIGHTCOLOR, A W NIEJ KLASYCZNE MODELE TUBOWE I WANDALOODPORNE KOPUŁOWE Z KLOSZEM Z POLIWĘGLANU IK10. KAMERY O ROZDZIELCZOŚCIACH 2 ORAZ 4 MPIX Z OBIEKTYWAMI O STAŁEJ OGNISKOWEJ SĄ W KATALOGU LINII PRODUKTOWEJ BCS LINE OZNACZONE NOWYMI SYMBOLAMI: BCS-L-DMIP1-2MWSC-F-A-AI2 (KOPUŁA 2 MPIX) ORAZ BCS-L-TIP4-2MWSC-F-A-AI2 (TUBA 2 MPIX).

Noc w kolorach tęczy

Co wyróżnia serię NightColor? Kamery nie wymagają zastosowania promiennika podczerwieni. Superczuły przetwornik obrazu pozwala na uzyskanie w kolorze czułości na poziomie 0,001 lx, a więc na pracę w trybie kolorowym przez 24 h/dobę. Ponieważ w kamerach BCS NightColor nie ma promiennika IR, nie ma też refleksów od powierzchni klosza powodujących efekt „mgły" czy rozmycia obrazu. Brak żarzących się diod IR to również brak lgnących do nich owadów wywołujących fałszywe alarmy.
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.
W ofercie kamer BCS NightColor są też modele tubowe BCS-L-TIP4-2MWSCL4RBS-F-M-A-AI1 dostępne w rozdzielczościach 2 i 5 Mpix, w których diody IR zastąpiono diodami LED światła białego. Ich zadaniem jest oświetlenie obserwowanego terenu. Kamera ma też diody w kolorach czerwonym i niebieskim oraz wbudowany głośnik. Zestaw taki pozwala na aktywne odstraszanie/ostrzeganie po wykryciu zdarzenia alarmowego. Emitowany jest wtedy sygnał dźwiękowy (jeden z 10 predefiniowanych lub wgrany własny) oraz sygnalizacja optyczna kolorowymi LED-ami.
Oba typy kamer wspierają funkcje zaawansowanej analizy wizji oraz inteligentnej detekcji ruchu.

C&C PARTNERS

www.ccpartners.pl

Nowa centrala alarmowa UNii – innowacja w systemach sygnalizacji włamania i kontroli dostępu

UNii TO KOMPLETNA OFERTA SYSTEMU ALARMOWEGO – CENTRALI, KLAWIATURY, KOMPONENTÓW MAGISTRALI I DETEKTORÓW. CHARAKTERYZUJE SIĘ BUDOWĄ MODUŁOWĄ. JEDNA PLATFORMA SPRZĘTOWA UMOŻLIWIA DOSTOSOWANIE SYSTEMU ALARMOWEGO DO AKTUALNYCH I PRZYSZŁYCH OCZEKIWAŃ KLIENTA.

Liczbę wejść/linii dostępnych w centrali można łatwo powiększyć z 32 do 128 lub 512. Rozszerzenie jest aktywowane za pomocą licencji online, nie wymaga wymiany płyty głównej centrali.
Centrala ma dodatkowe moduły rozszerzeń: dodatkowe wejścia, wyjścia OC i przekaźnikowe, expandery czytników KD, moduły do komunikacji urządzeń bezprzewodowych Pyronix, PowerG, Elite, moduł integracji automatyki KNX i moduł monitorujący GPRS. System jest dostępny w wersji z centralą redundantną, co zapewnia 100 proc. dostępność przez 24 h/7. Za pomocą magistrali RS-485 można łączyć kilka central alarmowych w klastry, tworząc jeden system z maks. 4096 wejściami linii!
Dostępne wersje central:
– 32 wejścia (od 8 do 32 linii przewodowych i/lub 32 bezprzewodowych),
– 128 wejść (od 8 do 128 linii przewodowych i/lub 32 bezprzewodowych),
– 512 wejść (od 8 do 512 linii przewodowych i/lub 64 bezprzewodowych).
Manipulator jest łatwy w użyciu. Podświetlane klawisze nawigacyjne są intuicyjne w obsłudze i dobrze widoczne w ciemnych pomieszczeniach. Czytnik DESFire EV2 pozwala zarządzać systemem za pomocą kart zbliżeniowych DESFire.

D+H POLSKA

www.dhpolska.pl

Ochrona przed pożarem obiektów hotelowych

NIEZAWODNY SYSTEM SYGNALIZACJI POŻAROWEJ, KTÓRY ZAPEWNI WCZESNE WYKRYCIE POŻARU I ZAALARMUJE O ZAGROŻENIU, JEST WAŻNYM ELEMENTEM WYPOSAŻENIA KAŻDEGO OBIEKTU HOTELOWEGO. SYSTEM PROTEC CHARAKTERYZUJE SIĘ WYSOKĄ ODPORNOŚCIĄ NA FAŁSZYWE ALARMY, PRECYZYJNĄ LOKALIZACJĄ ZDARZENIA POŻAROWEGO I DUŻĄ ELASTYCZNOŚCIĄ W ZAKRESIE PODŁĄCZENIA ELEMENTÓW PĘTLOWYCH.

System Protec, oferowany przez firmę D+H Polska, składa się z interaktywnej, cyfrowej i adresowalnej centrali sygnalizacji pożarowej oraz szerokiej gamy urządzeń peryferyjnych – czujek ciepła, optyczno-termicznych, z dodatkowym sensorem CO, zasysających i samokalibrujących się czujek liniowych.
W budynkach o małej i średniej kubaturze stosuje się łatwą w instalacji i eksploatacji centralę Protec 6100, w dużych obiektach – centralę Protec 6500 charakteryzującą się łatwością adresowania i konfiguracji, precyzją lokalizacji zdarzenia pożarowego i pełną kontrolą obiektu z dowolnego miejsca.
Centralę można zaprogramować wg różnych trybów pracy uwzględniających funkcję obiektu i specyficzne warunki środowiskowe.

Ważnym aspektem w przypadku obiektów hotelowych jest możliwość wystąpienia fałszywych alarmów wywołanych wilgocią i parą wodną wydobywającą się ze stref saun i pomieszczeń basenowych. Czujki Protec rozpoznają czynniki kwalifikujące się jako zdarzenie pożarowe i odróżniają je od powodujących fałszywe alarm.

HANWHA TECHWIN

www.hanwha-security.eu/pl/

Nowe rejestratory NVR obsługujące kamery Wisenet ze sztuczną inteligencją

WPROWADZENIE NA RYNEK 8- I 16-KANAŁOWYCH REJESTRATORÓW NVR WISENET Z SERII X SPRAWIA, ŻE KORZYSTANIE Z BEZPŁATNEJ FUNKCJI ANALIZY TREŚCI OBRAZU WBUDOWANEJ W KAMERY WISENET AI JEST DOSTĘPNE NAWET DLA MAŁYCH FIRM.

Funkcja analizy treści obrazu, bazująca na sztucznej inteligencji i głębokim uczeniu, wykrywa i klasyfikuje obiekty różnego typu (m.in. ludzi, twarze, pojazdy i tablice rejestracyjne). Jest obsługiwana przez algorytmy Wisenet AI Hanwha Techwin. Rozróżniają one cechy osób (wiek, płeć lub kolor odzieży, którą dana osoba ma na sobie), a także kształty i kolorystykę przedmiotów. Algorytmy są nawet w stanie rozpoznać, czy dana osoba nosi okulary lub trzyma torbę.
Dzięki obróbce metadanych wytwarzanych przez kamery Wisenet AI nowe rejestratory NVR ułatwiają użytkownikom szybkie i precyzyjne wyszukiwanie właściwych fragmentów w zarejestrowanym materiale wizyjnym na zasadzie rozpoznawania obiektów na podstawie powiązanych z nimi atrybutów.
Atrybuty są zapisywane jako metadane w rejestratorach NVR wraz z obrazami wytworzonymi przez kamery. Umożliwiają użytkownikom szybkie wyszukiwanie określonych obiektów lub incydentów.
Konfigurację rejestratorów NVR można łatwo przeprowadzić za pomocą intuicyjnego interfejsu i kreatora instalacji. Rejestratory NVR są zaprogramowane tak, aby automatycznie usuwały zawartość materiału wizyjnego po określonym czasie z tzw. zakładek, co zapewnia zgodność z wymaganiami RODO.

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.
Szczegóły techniczne i konfiguracyjne są dostępne na portalu DPP Hikvision, gdzie można obejrzeć nagrania webinarów.

IMPAKT

www.impakt.com.pl

Nowa generacja zasilaczy awaryjnych PowerWalker

OD 1999 R. INTERNET RZECZY ROZWIJA SIĘ BARDZO PRĘŻNIE. INTELIGENTNE URZĄDZENIA I NAJNOWOCZEŚNIEJSZE MASZYNY, KTÓRE WYKORZYSTUJĄ TECHNOLOGIĘ BEZPRZEWODOWĄ, ABY KOMUNIKOWAĆ SIĘ ZE SOBĄ (I Z NAMI), ROZWIJAJĄ SIĘ W ZAPIERAJĄCYM DECH W PIERSIACH TEMPIE – OD 2 MLD URZĄDZEŃ W 2006 R. DO PRZEWIDYWANYCH 100 MLD W 2022 R. LAPTOPY, SMARTWATCHE, ROBOTY, SYGNALIZACJA ŚWIETLNA, AUTONOMICZNE SAMOCHODY, BEZPIECZEŃSTWO I DOSTĘPNOŚĆ DANYCH CZY WRESZCIE SMART HOME. INTERNET RZECZY TO PRZYSZŁOŚĆ.

Do tej wizji przyszłości wchodzi również PowerWalker z nową serią UPS IOT w wersjach ICT (tower) i ICR (rack). Są to profesjonalne, wszechstronne UPS-y online z technologią podwójnej konwersji.
Ich funkcja IoT pozwala na wysyłanie ważnych informacji do zabezpieczonej chmury Microsoft Azure po podłączeniu do Internetu.
Urządzenia są monitorowane w czasie rzeczywistym za pomocą aplikacji WinPower View, która jest dostępna dla systemów Android i iOS. Dzięki niej możliwy jest dostęp do wielu funkcji IoT, których sam UPS nie może zaoferować, takich jak szybka i prosta konfiguracja, monitoring podłączonych urządzeń, harmonogram działań czy dziennik zdarzeń krytycznych.
Możliwość nadania uprawnień innym użytkownikom sprawia, że można szybko reagować na wszelkie niebezpieczne sytuacje spowodowane utratą zasilania, a co za tym idzie – chronić przed ryzykiem ingerencji w bezpieczeństwo struktury firmy.

LINC POLSKA

www.linc.pl

FLIR A500f/A700f – nowa kamera termowizyjna FLIR do monitorowania procesów i wczesnej detekcji pożarów

INNOWACYJNE KAMERY TERMOWIZYJNE FLIR A500F I A700F Z ZAAWANSOWANYMI FUNKCJAMI ANALITYCZNYMI SĄ IDEALNE DLA UŻYTKOWNIKÓW, KTÓRZY POTRZEBUJĄ WBUDOWANYCH FUNKCJI POMIAROWYCH I ALARMOWYCH DO MONITOROWANIA NP. PROCESÓW PRODUKCYJNYCH LUB WCZESNEGO WYKRYWANIA POŻARÓW.

Dzięki rozdzielczości przetwornika termowizyjnego do 640 × 480 pix, zdalnej możliwości zmiany ogniskowej czy technologii MSX® *(Multi-Spectral Dynamic Imaging)* kamery zapewniają niezawodne pomiary. Mogą pomóc firmom chronić własne zasoby, poprawić bezpieczeństwo, zmaksymalizować czas pracy bez przestojów i zminimalizować koszty konserwacji. Są wyposażone w obudowę ochronną zaprojektowaną tak, aby wytrzymała trudne warunki środowiska pracy (od -30 do +50°C).
Kamery FLIR A500f/A700f łączą wysokiej jakości obraz termowizyjny z jego przetwarzaniem już w samej kamerze i funkcjami urządzeń IIoT. Wszystko w celu uproszczenia integracji z nowymi lub istniejącymi sieciami.
W przypadku integracji z oprogramowaniem VMS strumień termowizyjny i wizyjny można oglądać niezależnie lub jednocześnie.
Kamery można dodawać, konfigurować i obsługiwać w systemach HMI/SCADA, co zapewnia dostawcom rozwiązań systemów automatyki możliwość uruchomienia zaawansowanych funkcji monitorujących.
Wiele opcji komunikacji i sterowania umożliwia łatwą integrację ze standardowymi rozwiązaniami zabezpieczenia technicznego oraz przemysłowym internetem rzeczy (IIoT), w tym m.in. z ONVIF, Modbus, MQTT i REST API.

PRODUKT NUMERU

NEDAP SECURITY MANAGEMENT

www.nedapsecurity.com/pl/

Obudowy z zasilaczami do kontrolerów dostępu

Z POCZĄTKIEM 2021 ROKU FIRMY NEDAP ORAZ PULSAR ROZSZERZYŁY WZAJEMNĄ WSPÓŁPRACĘ, CZEGO EFEKTEM JEST WPROWADZENIE PRZEZ FIRMĘ PULSAR DEDYKOWANYCH OBUDÓW WRAZ Z ZASILACZAMI DO KONTROLERÓW DOSTĘPU, MODUŁÓW DRZWIOWYCH ORAZ MODUŁÓW WEJŚĆ/WYJŚĆ Z SERII BLUE.

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.

- **Nedap Power 1M** umożliwia montaż jednego kontrolera drzwiowego Nedap oraz jednego akumulatora 7 Ah lub 17 Ah. Wymiary: 230 x 372 x 80 [+/-2 mm], dystans od podłoża: 8 mm.
- **Nedap Power 4M** pozwala na montaż czterech kontrolerów oraz dwóch akumulatorów 7 Ah lub 17 Ah. Wymiary: 340 x 550 x 170 [+/-2 mm], dystans od podłoża: 14 mm.

Obie obudowy zostały wykonanie w klasie szczelności IP20 oraz wyposażone w styk antysabotażowy.

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 EAP660 HD – punkt dostępowy Wi-Fi 6 do najbardziej obciążonych środowisk

OMADA EAP265 HD ZOSTAŁ ZAPROJEKTOWANY DO PRACY W BARDZO OBCIĄŻONYCH ŚRODOWISKACH (SALE KONFERENCYJNE, POWIERZCHNIE TARGOWE). PRACUJĄCY W STANDARDZIE AX3600 ACCESS POINT MOŻE OBSŁUŻYĆ KILKASET URZĄDZEŃ KLIENCKICH JEDNOCZEŚNIE.

NAJWAŻNIEJSZE CECHY PRODUKTU:

- **prędkość transmisji** do 2402 Mb/s w paśmie 5 GHz oraz do 1128 Mb/s w paśmie 2,4 GHz;
- **port Ethernet 2,5 Gb/s**
- **technologie MU-MIMO** UL/DL oraz OFDMA zwiększają przepustowość w obciążonych sieciach, pozwalając na łączenie się wielu urządzeń jednocześnie;
- **scentralizowane zarządzanie**: dostęp w chmurze i aplikacja Omada lub sprzętowy kontroler OC200/OC300 dla wygody i łatwości zarządzania;
- **płynny roaming**: urządzenia tworzą jednolitą sieć Wi-Fi w całym budynku. Smartfon użytkownika zawsze połączy się z API, który oferuje mu najlepsze połączenie, bez przerywania transferu;
- **wsparcie PoE**: obsługa standardu 802.3at

Instalacja i połączenie EAP660 HD do istniejącej sieci odbywa się za pomocą jednego przewodu. Dzięki PoE można zasilać i zintegrować urządzenie z siecią LAN. To znacznie ogranicza koszty założenia instalacji.

Punkty dostępowe z serii EAP pozwalają na stworzenie wydajnej i bezpiecznej sieci Wi-Fi. Oprócz podstawowych funkcji bezpieczeństwa istnieje możliwość autoryzacji dostępu z uwierzytelnianiem przez SMS, Facebooka oraz logowaniem za pomocą strony powitalnej, voucherów lub jednorazowych haseł dostępu. Produkt objęty jest 5-letnią gwarancją producenta.

Na temat nowych technologii w zastosowaniach elektronicznych systemów zabezpieczeń wypowiadają się u nas security menedżerowie z różnych sektorów gospodarki. Przedstawiamy opinię **dr. Macieja Kaweckiego**, który o swoich doświadczeniach z zabezpieczeniami opowie z perspektywy zarówno użytkownika końcowego, jak i propagatora wdrażania najnowszych technologii.

Branża security widziana oczami propagatora najnowszych technologii

MACIEJ KAWECKI , DOKTOR NAUK PRAWNYCH, NAUCZYCIEL AKADEMICKI, URZĘDNIK PAŃSTWOWY, OD 2019 R. DZIEKAN WYDZIAŁU INNOWACJI I PRZEDSIĘBIORCZOŚCI WYŻSZEJ SZKOŁY BANKOWEJ W WARSZAWIE, PREZES INSTYTUTU LEMA

Czy jako użytkownik spotyka się pan na co dzień z najnowszą technologią w systemach zabezpieczeń?
Patrząc na systemy zabezpieczeń czy systemy bezpieczeństwa, większą wagę przykładam do bezpieczeństwa danych, bezpieczeństwa w Internecie, bezpieczeństwa aplikacji mobilnych, z których korzystam, oraz bezpieczeństwa cyfrowego w takiej przestrzeni analogowej. Poznałem wyniki badania, które opublikowała fundacja Panoptykon na temat monitoringu wizyjnego miasta. Próbowano podjąć zmiany prawne w tym zakresie. Wyrażana jest opinia, że monitoring miejski w takim samym stopniu pomaga i szkodzi, ponieważ w dłuższej perspektywie pogłębiony monitoring buduje w mieszkańcach postawę konformizmu. Czyli fakt, że cały czas jesteśmy obserwowani – co wpływa w określony sposób na nasze zachowania, na nasze emocje – powoduje wzrost poczucia bezpieczeństwa w rozumieniu bezpieczeństwa osobistego, ale ma negatywny wpływ na nasze zachowania, prowadząc do bierności. Dlatego postulują – z czym prywatnie też się zgadzam – bardziej racjonalne korzystanie z rozwiązań monitoringu miejskiego, zdecydowanie w kierunku zachodnim niż wschodnim czy azjatyckim.
Uważam, że w Polsce potrafimy korzystać z zalet monitoringu wizyjnego, że jego forma jest racjonalna, właściwa, nie nadmiarowa. Co do tego nie mam żadnych wątpliwości. Większy problem mam z bezpieczeństwem przestrzeni cyfrowej i infrastruktury jako takiej.
Jeśli chodzi o rozwiązania w zakresie bezpieczeństwa i monitoringu przestrzeni miejskiej, to zwracam uwagę na rozwiązania oferowane przez start-upy. Jakiś czas temu miałem okazję spotkać się ze start-upem z Wrocławia, który wdraża rozwiązania wykorzystujące system monitoringu miejskiego do badania rozprzestrzeniania się COVID-19. Za pomocą odpowiednich algorytmów, w tym również tych do rozpoznawania temperatury ciała, określają prawdopodobieństwo pojawienia się ogniska choroby na danym obszarze miasta. Kamera ma wbudowany system termowizyjny do mierzenia temperatury ciała człowieka. Można przypuszczać z większym prawdopodobieństwem, że w trakcie pandemii osoba mająca podwyższoną temperaturę, która przemieszcza się po ulicy, jest nosicielem wirusa.
Opracowane algorytmy potrafią rozpoznać odległości pomiędzy ludźmi, którzy z zainfekowaną osobą miały styczność, i określić z dużym prawdopodobieństwem, ile z nich mogło się zarazić. W ten sposób bardzo skutecznie – oczywiście przy pewnej skali masowości – są w stanie określić prawdopodobieństwo zwiększenia zachorowań na COVID-19 w wybranych częściach miasta. Jednak jest to ingerencja w prywatność. Nie wiem, czy chciałbym, żeby tego typu rozwiązania były stosowane w Polsce. Ale z takimi rozwiązaniami już się spotykałem.

Mówiliśmy o systemach monitoringu wizyjnego w przestrzeni miejskiej, a jak pan postrzega nowości w kontroli dostępu? Czy ułatwiają życie?
Byłem pierwszym orędownikiem wprowadzania biometrii, jeszcze w trakcie projektowania przepisów wdrażających RODO. Odpowiadałem za część wprowadzenia do kodeksu pracy przepisów dotyczących biometrycznej weryfikacji tożsamości. Przepis pojawił się z wielkim trudem, był chyba najtrudniejszy do wprowadzenia ze wszystkich w kodeksie pracy. Pamiętam gorący apel najpierw GIODO, potem przekształconego Prezesa Urzędu Ochrony Danych Osobowych, że to jest zbyt duża ingerencja w prywatność. Próbowano w tych przepisach wprowadzić pewną furtkę, że można korzystać z biometrii do weryfikacji tożsamości tylko w niektórych rodzajach obiektów, np. w bankach przy kontroli jakości znaków pieniężnych czy tam, gdzie liczy się pieniądze, lub w obszarach medycznych. To się nie udało i według mnie bardzo dobrze, że ten przepis pozostał otwarty, gdyż dzisiaj widzimy, że jest on wykorzystywany racjonalnie. Pandemia nadała mu nowy wymiar, bo stał się podstawą prawną do tego, aby zakłady pracy mogły wykorzystywać biometrię do mierzenia temperatury pracowników w walce z COVID-19.
Jestem więc wielkim zwolennikiem korzystania z rozwiązań biometrycznych. Uważam, że dzisiaj znajdujemy się już na kolejnym etapie. Przypomnę, że pierwsza fala wdrażania przepisów polegała na tym, że przedsiębiorcy musieli zapewniać pracownikom również tradycyjną formę dostępu, czyli obok bramki biometrycznej musiała być bramka zwykła. W Ministerstwie Cyfryzacji pierwsze takie bramki zastosowano 5 czy 6 lat temu. Dzisiaj wydaje mi się, że wchodzimy w fazę, w której można przy dużej świadomości pracowników myśleć o tym, czy tego przepisu nie zrewidować jeszcze bardziej. Po prostu go dopuścić, ponieważ zawiera pewne zawężenie – mówi o tym, że można identyfikację biometryczną stosować, o ile jest to niezbędne do zapewnienia bezpieczeństwa zakładu pracy i eliminacji szkód. Uważam, że moglibyśmy otworzyć ten przepis, w całości dopuszczając korzystanie z rozwiązań biometrycznych do weryfikacji tożsamości.

Czy nie ma pan problemu z systemami rozpoznawania twarzy? Godzi się na przechwytywanie swojego wizerunku i zapisywanie go w bazach danych?
Nie do końca pochwalam te rozwiązania, ale nie ze względu na poczucie intymności czy ingerencji w moją prywatność, ale dlatego że systemy te są bardzo łatwe do oszukania. Pół roku temu przeprowadziłem eksperyment, z którego reportaż był emitowany w programie „Dzień dobry TVN". Polegał on na tym, że wydrukowałem na drukarce 3D twarz określonej osoby, a następnie poszedłem do sklepu w telefonami komórkowymi i z wykorzystaniem tej twarzy otworzyłem wszystkie modele telefonów z systemem Android z 2019 i 2020 r. Następnie wydrukowałem w bardzo dobrej jakości twarz w normalnych rozmiarach i na podstawie tego zwykłego cyfrowego wydruku udało mi się otworzyć dwa telefony. To oznacza, że te systemy jeszcze nie mają sensora do pomiaru głębi. Wystarczy wydruk, żeby uwierzytelnić użytkownika. W związku z tym dzisiaj nie jest to rekomendowana forma weryfikacji tożsamości, łatwo bowiem system oszukać.
Wszystko oczywiście zależy od zaawansowania systemu. Próbowałem tej metody z telefonami z systemem iOS, których nie udało mi się oszukać, mimo że próbowałem podgrzać maskę lampą UV, symulując temperaturę ciała człowieka. Jednak dziś, przy pewnej masowości i skali stosowania, gdy nie mamy gwarancji, że każda technologia rozpoznawania twarzy

WSZYSCY MUSIMY ROZUMIEĆ TECHNOLOGIĘ, MUSIMY UMIEĆ DANE ROZWIĄZANIE UMIEJSCOWIĆ W PEWNYM EKOSYSTEMIE, ALE NIE MUSIMY WIEDZIEĆ, JAK TO TECHNICZNIE DZIAŁA OD STRONY INŻYNIERYJNEJ

jest ograniczona tylko do identyfikacji zewnętrznych cech fizycznych, powoduje, że dla mnie to nie jest rekomendowane rozwiązanie. A przynajmniej nie jako jednoelementowa metoda potwierdzania tożsamości. Przy autoryzacji wieloelementowej, jako jedna z nich, już jak najbardziej. I to się dzieje w telefonach komórkowych. Uzyskujesz dostęp za pomocą dwustopniowego uwierzytelnienia. W moim przekonaniu to jest akceptowalne.

Czy korzysta pan z systemu zabezpieczeń, np. włamaniowego?

Tak, ale z bardzo prostego. Dużo lepiej zabezpieczałbym nieruchomość, gdyby była oderwana od czynnika ludzkiego, jakim są sąsiedzi, jakim jest poczucie bezpieczeństwa miejsca, historia związana z włamaniami. Do zabezpieczenia nie podchodzę zerojedynkowo. Każde miejsce, każda nieruchomość i każde dobro, które mam, musi być chronione. Do wyboru rozwiązania podchodzę indywidualnie. Na nieruchomość patrzę w szerszym ekosystemie miejsca, w którym się znajduje.

Podam też inny przykład. Kilka miesięcy temu ukradziono mi spod domu samochód. I dzisiaj, decydując się na zakup czy wynajem auta, pierwszym moim pytaniem, zaraz po tym, ile spala na 100 km, jest pytanie o dwuskładnikowe zabezpieczenie samochodu. Czyli o specjalny token, który mam przy kluczykach, który zawsze musi znajdować się wewnątrz pojazdu, żeby go uruchomić. Decyzja o wyborze sposobu zabezpieczenia ma według mnie wymiar empiryczny. Wszystko zależy od naszych doświadczeń.

Są to pana doświadczenia jako użytkownika końcowego. A jak – z punktu widzenia propagatora nowych technologii – ocenia pan umiejętność producentów elektronicznych systemów zabezpieczeń do wprowadzania najnowszych technologii w swoich produktach, rozwiązaniach?

Umiejętność ta jest zdeterminowana świadomością i oczekiwaniami klientów. Wydaje mi się, że wchodzimy w taką fazę personalizacji produktów – nie tylko w rozumieniu odpowiedzi na oczekiwania konkretnych użytkowników, ale też regionalizacji, czyli dostosowywania produktów do pewnych cech populacyjnych. I rzeczywiście tak jest.

Ostatnio rozmawiałem z Motorolą, że ten sam model telefonu różni się wbudowanymi domyślnie zabezpieczeniami czy funkcjonalnościami w zależności od kraju. Inne są np. w USA, inne w Europie, a jeszcze inne w Azji. Mamy inne preferencje populacyjne, inne oczekiwania. My – Europejczycy – cenimy sobie prywatność, ale jednocześnie szybkość, komfort i łatwość obsługi. A to niestety

nie do końca idzie w parze z zabezpieczeniami. Produkty, które są oferowane – i nie mówię tylko o urządzeniach czy aplikacjach mobilnych, komunikatorach, które również powstają w Polsce – domyślnie nie mają najwyższego możliwego poziomu zabezpieczenia. Dają techniczną możliwość korzystania z nich, ale – jako użytkownicy – nie oczekujemy, nie wymagamy takich ustawień domyślnych. I to jest moje „wysokopoziomowe" spostrzeżenie w tym obszarze.

To znaczy, że my sami nie zabezpieczamy naszych urządzeń?

Absolutnie tak jest. Z jednej strony słyszymy o zagrożeniach, o cyberbezpieczeństwie, z drugiej zaś – poświęcenie 5 sekund na to, aby wzmocnić dostęp do naszego telefonu, to dla nas za dużo. Dokładnie tak samo jest – moim zdaniem – z systemami zabezpieczeń. Nie mam w tym temacie aż tak pogłębionej wiedzy, ale ostatnio spędziłem sporo czasu na analizie trendów związanych z urządzeniami mobilnymi, dlatego posłużyłem się ich przykładem.

Jak pan ocenia potencjał technologiczny branży elektronicznych systemów zabezpieczeń na tle innych branż?

Uważam, że potencjał jest ogromny. Liczba polskich firm w tym obszarze jest gigantyczna. Od dłuższego czasu zajmuję się promowaniem polskich start-upów technologicznych, m.in. na LinkedIn. Branża zabezpieczeń ma ten problem, że nie jest ławo ją pokazać w sposób interesujący. Ona nie jest spektakularna w rozumieniu całych rozwiązań. Tu nie ma fajerwerków, a firmy bardzo na tym cierpią. Niedawno spotkałem się ze start-upem, który wdrożył fantastyczny system informowania o pożarze. Są w stanie, za pomocą algorytmów, wykryć pożar jeszcze w jego początkowej fazie, kiedy ugaszenie nie powoduje dużych szkód. Rzeczywiście długo zastanawiałem się, w jaki sposób to pokazać, żeby było atrakcyjne dla odbiorcy. W zasadzie dzisiaj nie jest to możliwe. I to wydaje mi się jest problemem tej branży.

To smutne...

Tak, jestem po prostu szczery. Jeśli spojrzy się na segmenty rozwoju technologii, to widać takie, o których się mówi bardzo często, np. o automatyzacji, robotyzacji, sztucznej inteligencji, bo je bardzo łatwo pokazać. Natomiast w branży zabezpieczeń jest to dużo trudniejsze. To powoduje, że niestety branża, jeżeli chodzi o dotarcie z nowymi rozwiązaniami, bardziej kuleje.

W takim razie w jaki sposób dostawcy technologii powinni przekonywać użytkowników do stosowania ich rozwiązań opartych na najnowszych technologiach?

Pokazując korzyści bezpośrednio po stronie użytkownika. Schodząc z takiego piedestału uniwersalnych wartości, mówić o bardzo konkretnych korzyściach. Pokazując historię, która najlepiej sprzeda rozwiązanie. Ludzie lubią się uczyć na błędach. Pokazując negatywne konsekwencje wynikające z braku wykorzystania tego typu systemów, jesteśmy w stanie przekonać użytkownika końcowego do tego, że musi z nich korzystać, by uniknąć błędów czy zagrożeń. Negatywne konsekwencje mogą się wiązać z naruszeniem tajemnicy przedsiębiorstwa, wyciekiem danych osobowych, naruszeniem prywatności, intymności, a to może wpłynąć na spadek wartości firmy, pociąga też skutki dla pracowników. Tylko w ten sposób, pokazując konkretne historie ludzi, które naprawdę się wydarzyły.

A czy zamiast podkreślać błędy, nie lepiej chwalić się rozwiązaniami, które zostały zrealizowane z sukcesem?

Powiem szczerze, że jeśli chodzi o pokazywanie technologii, jedną z form, jaką często stosuję, jest akcentowanie polskości, czyli pokazywanie polskiej myśli innowacyjnej – że u nas mogło coś powstać, że to jest kreatywne. Bo my mamy kompleks narodowy, nam się wydaje, że jako Polacy jesteśmy w ogonie rozwoju świata, co wcale nie jest prawdą. My będziemy to komentować, możemy być z tego dumni, ale niestety nie idzie to w parze z decyzją zakupową. Natomiast kiedy pokazuję konkretną historię ludzką, ktoś sobie ją spersonalizuje i dojdzie do wniosku, że sam też mógł paść ofiarą tego typu zjawiska. Kiedy pokazuję konkretną negatywną konsekwencję, dużo łatwiej jest namówić decydenta do zakupu rozwiązania.

Ale czy klient zgodzi się na upublicznienie tego typu przypadku?

Przykłady można zanonimizować. Można też, wychodząc od negatywnego skutku, pokazać, jak rozwiązanie wpłynęło na korzyść firmy. Najlepsze efekty osiąga się, pokazując historię na konkretnym przykładzie. Oczywiście nie należy ujawniać wszystkich zabezpieczeń, ale można pokazać, jaką technologię zastosowaliśmy, bez szczegółów dotyczących działania algorytmów. Nie wolno ujawniać kodów, ale można pochwalić się, że zastosowaliśmy sztuczną inteligencję. Możemy powiedzieć, jakie kamery zastosowaliśmy, ale nie ujawniać ich lokalizacji.

Ludzi nie interesują szczegóły techniczne, ich interesuje praktyczny aspekt wykorzystywania technologii. Coraz częściej wchodzimy w fazę rozwoju technologii, gdzie od pracowników oczekuje się wiedzy technologicznej, a nie wiedzy inżynieryjnej. Czyli wszyscy musimy rozumieć technologię, rozumieć, w jaki sposób określone rozwiązanie mieści się w ekosystemie technologicznym, czym jest rzeczywistość rozszerzona, wirtualna, technologia *blockchain*, sztuczna inteligencja, uczenie maszynowe. Musimy wiedzieć, co to znaczy, umieć dane rozwiązanie umiejscowić w pewnym ekosystemie, ale nie musimy wiedzieć, jak to technicznie działa od strony inżynieryjnej. Nikt od nas tego nie oczekuje. Skupmy się na pokazaniu rozwiązania i skutków jego stosowania dla konkretnych użytkowników. Bez ujawniania kuluarów, czyli wiedzy inżynieryjnej.

Wspomniał pan o najnowszych technologiach. Czy przyszłość branży elektronicznych systemów zabezpieczeń należy do sztucznej inteligencji?

Wiem, że to jest stwierdzenie sztampowe, ale naprawdę przyszłość zależy od sztucznej inteligencji. Uważam, że przeceniamy ją, tzn. wizje, które mówią o tym, że sztuczna inteligencja nas zastąpi, czy sieci neuronowe zastąpią proces myślenia, to jest oczywiście bzdura. Dzisiaj nie potrafimy stworzyć sieci neuronowej, która jest w stanie symulować ruchy muchy, a co dopiero mózgu człowieka, którego działania do końca jeszcze nie poznaliśmy.

Przyszłość automatyzacji procesów natomiast należy do algorytmów. To nie ulega żadnej wątpliwości. One w jakiś sposób uniwersalizują i obiektywizują, czyli odrywają proces decyzyjny od tego, co subiektywne. Są w stanie w jednej chwili podjąć decyzję, wykorzystując tysiące podobnych stanów faktycznych, i w pewien sposób uniwersalizują odpowiedź, czyli ją obiektywizują. I to jest największa wartość algorytmów. Uważam, że tak rzeczywiście będzie, że to jest przyszłość rozwoju technologii.

O sztucznej inteligencji tak naprawdę mówi się od roku 1958. Potem przez 60 lat się rozwijała, najpierw na poziomie teoretycznym, później praktycznym. To jest jedyna technologia, która swój rozwój rozpoczęła nie od praktyki, tylko od teorii. Bo gdy mówimy o technologiach *blockchain, big data*, o Internecie rzeczy, zaczęliśmy tworzyć konkretne rozwiązania. Sztuczna inteligencja natomiast rozpoczęła swój rozwój od teorii, od filozoficznego ujęcia jej mechanizmów. A później podążaliśmy w kierunku tworzenia konkretnych rozwiązań. Jest to technologia nieprawdopodobnie dopasowana do naszych potrzeb, więc wydaje mi się, że jest absolutnie kierunkiem rozwoju.

Czy świat będzie wyglądał tak jak w wizji filmu „Raport mniejszości"?

Nie, myślę, że tak nie będzie wyglądał. Jest taka teoria w rozwoju nowych technologii, która nazywa się „doliną niesamowitości". Wskazuje ona granice rozwoju technologii, której my, jako ludzie, nie chcemy przekraczać. I tą granicą jesteśmy my sami – tzn. wszystko to, co w jakiś sposób konkuruje z nami, ten proces decyzyjny, który jest dla nas konkurencyjny, który wypiera człowieka. Stąd Boston Dynamics wycofał się z tworzenia robotów humanoidalnych na rzecz robotów psów, które są w stanie pomóc człowiekowi dokładnie tak samo, ale jednocześnie nie tworzą poczucia zagrożenia. I dlatego ten robot, który nazywa się Spot, fantastycznie się sprzedaje. Bo sylwetka psa nie powoduje u nas poczucia zagrożenia, gdyż utożsamia się ze zwierzęciem uległym, miłym i sympatycznym. W przeciwieństwie do robotów humanoidalnych, które mogą wywołać negatywne emocje.

I dokładnie tak jest z każdą technologią. Wszędzie tam, gdzie widzimy konkurencję, niechętnie z niej korzystamy. Z kolei tam, gdzie rozwiązanie technologiczne jest w pew rozwiązania stosujemy. Oczywiście powstają cuda technologiczne, które próbują zastąpić człowieka, ale na tym etapie pozostają one w sferze gadżetów.

Ja nie widzę przyszłości świata w czarnych barwach, wręcz przeciwnie.

Z dr. Maciejem Kaweckim rozmawiali Iwona Krawiec i Jan T. Grusznic

Sztuczna inteligencja w Polsce

raport Fundacji Digital Poland

Polska zajmuje 7. miejsce w Unii Europejskiej pod względem liczby ekspertów pracujących nad rozwojem lub wdrożeniem sztucznej inteligencji *(artificial intelligence, AI)* i jednocześnie 1. miejsce w regionie krajów Europy Środkowo-Wschodniej (CEE). Pozostałe dane dotyczące ekosystemu AI nie są już tak optymistyczne, mimo że polskie firmy udowadniają, że zastosowanie sztucznej inteligencji to nie jest odległa wizja, ale realny scenariusz biznesowy.

Fundacja Digital Poland w swoim najnowszym raporcie *State of Polish AI 2021* przedstawiła stan rozwoju sztucznej inteligencji w Polsce oraz rekomendacje, które pozwolą dotrzymać kroku najlepszym gospodarkom świata. Raport dostępny jest na stronie fundacji: https://www.digitalpoland.org/publikacje.

Zdaniem KPRM skuteczne zaimplementowanie rozwiązań bazujących na AI do polskiej gospodarki może podnieść dynamikę wzrostu PKB o 2,65% rocznie. Wzrost napędzany sztuczną inteligencją jest celem uchwalonej przez rząd polityki rozwoju AI w Polsce. Efektywna realizacja wszystkich celów nie będzie możliwa jednak bez dogłębnej analizy rynku, dlatego fundacja Digital Poland postanowiła sprawdzić kondycję krajowego ekosystemu sztucznej inteligencji. Badanie jest pierwszym na rynku, które tak kompleksowo przedstawia wdrożenia i zainteresowanie rodzimych spółek sztuczną inteligencją.

EKOSYSTEM AI W POLSCE

Z przeprowadzonych przez Fundację Digital Poland badań wynika, że polskie spółki zajmujące się sztuczną inteligencją zwykle działają w małych zespołach, od pięciu do dziesięciu pracowników. Największy kapitał ludzki gromadzą korporacje, które stać na sfinansowanie zespołów liczących ponad 40 osób. Ponad połowa firm rozwijających produkty i usługi AI osiąga siedmiocyfrowe zyski, a 8% notuje przychody powyżej 50 mln zł.

Sztuczna inteligencja niewątpliwie pozostaje domeną dużych aglomeracji. To globalny trend ze względu na dostęp do środowiska akademickiego oraz do przemysłu z wystarczającymi funduszami na wsparcie procesów R&D. Pierwsze miejsce na mapie polskiego AI od lat zajmuje Warszawa. Stolica skupia blisko 45% firm rozwijających produkty i usługi oparte na narzędziach AI. Jest to możliwe dzięki zagranicznym korporacjom, które lokują tu swoje centrale. Na kolejnych miejscach plasują się Kraków, Trójmiasto, Wrocław, Poznań i Katowice.

UTRUDNIONA WSPÓŁPRACA FIRM I NAUKI

Polska wciąż jest na wczesnym etapie wdrożenia rozwiązań opartych na AI. Jednym z powodów jest brak efektywnej współpracy firm i jednostek naukowych. Najczęściej przybiera ona formę zatrudniania pojedynczych badaczy z uczelni, a nie współpracy z instytucją.
Chociaż 47% badanych organizacji zatrudnia naukowców, zaledwie 13% z nich wymienia dane z ośrodkami akademickimi.

ROZWIĄZANIA AI W BRANŻY SECURITY

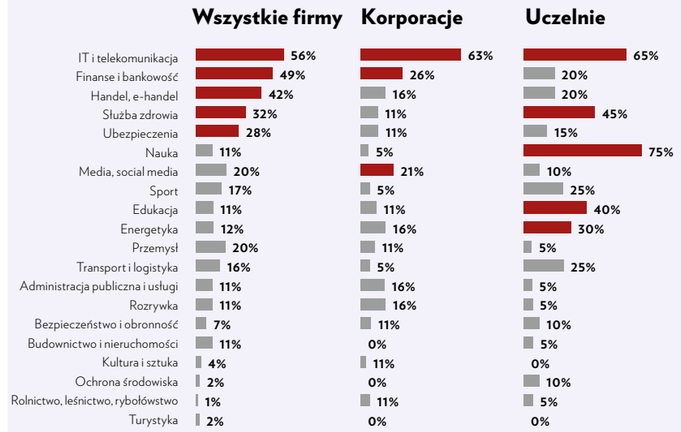
Firmy AI świadczą usługi głównie w takich sektorach, jak IT i telekomunikacja (58%), finanse i bankowość (41%) czy handel, w tym e-commerce (34%). Wydaje się jednocześnie, że kilka sektorów jest mało zainteresowanych inwestycjami w rozwiązania sztucznej inteligencji, m.in. turystyka (2%), rolnictwo, leśnictwo i rybołówstwo (3%), ochrona środowiska (3%), bezpieczeństwo i obrona (8%). Należy jednak podkreślić, że oferta dla tych sektorów gospodarki nie jest zbyt duża *(rys. 1)*.

Większość firm AI świadczy usługi dla sektorów finansowo-bankowego (49%) i ubezpieczeniowego (28%), handlu (42%) i ochrony zdrowia (32%).
Zespoły naukowe zajmujące się sztuczną inteligencją są skoncentrowane na pracy naukowej (75%) oraz na rzecz sektora IT i telekomunikacji (65%). Ponadto 45% pracuje nad rozwiązaniami dla służby zdrowia i 40% dla sektora edukacji. Tylko 7% zajmuje się rozwiązaniami dla branży security.
Korporacje najczęściej współpracują z firmami IT i telekomunikacyjnymi – 63% oraz w sektorze finansowo-bankowym 26% i mediach 21% *(rys. 2)*.

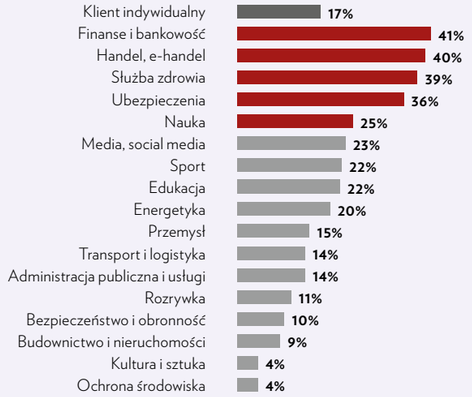
Usługodawcy AI koncentrują się na potrzebach korporacji, tylko 17% zespołów pracuje nad usługami lub produktami dla klientów B2C.
W przypadku odbiorców B2B usługi świadczone są zazwyczaj dla takich działów, jak R&D (41%), IT i rozwój oprogramowania (40%), BI i analityki danych (39%) oraz innowacji (36%).
Tylko niewielu klientów spośród producentów (15%), z działu logistyki (14%), sektora security (14%) czy inżynierów jest odbiorcami rozwiązań AI *(rys. 3)*.

Rys. 1. W jakich sektorach biznesowych organizacja wygenerowała przychody lub zastosowała sztuczną inteligencję w ciągu ostatnich 18 m-cy?

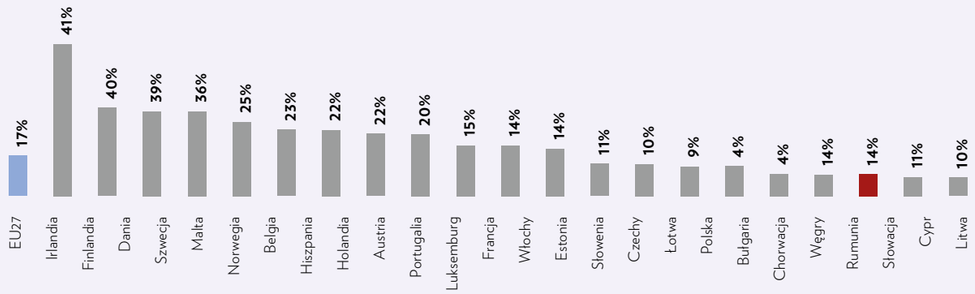
Rys. 2. Z kim współpracowaliście przy wdrażaniu sztucznej inteligencji w ciągu ostatnich 18 miesięcy?



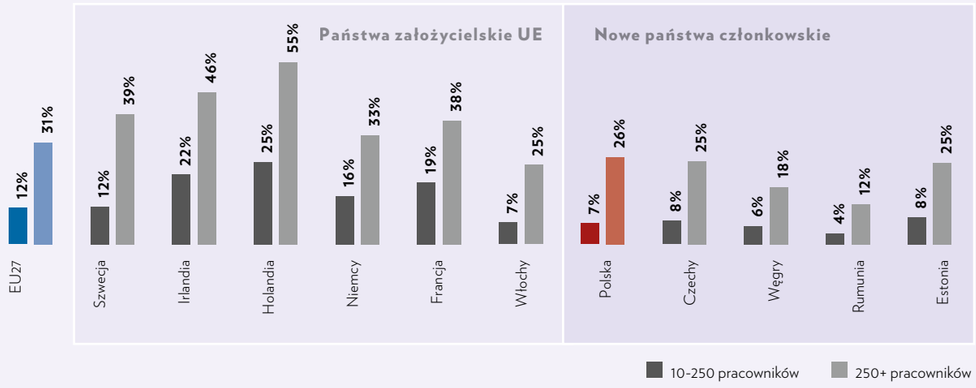
Rys. 3. Jacy klienci korzystali z twoich rozwiązań sztucznej inteligencji wdrożonej w produktach, usługach, działaniach w ciągu ostatnich 18 miesięcy?



Rys. 4. Duże firmy (250+ pracowników) analizujące duże zbiory danych *(big data)* z wykorzystaniem uczenia maszynowego



Rys. 5. Firmy, które analizują duże zbiory danych *(big data)* z dowolnego źródła danych



Tylko 6% polskich dużych firm korzysta z uczenia maszynowego. To jedna z najniższych wartości, poniżej średniej w UE. Jest to jednak wynik zbliżony do innych krajów regionu CEE (średnia w całej UE wynosi 11%) *(rys. 4)*.

W Polsce duże zbiory danych *(big data)* analizuje 26% dużych firm. To nieco mniej niż średnia dla UE (31%), ale to niezły wynik w porównaniu do innych krajów Europy Środkowo-Wschodniej. Zauważalna jest różnica w porównaniu z Niemcami (33%) czy Francją (38%), ale nie jest ona duża *(rys. 5)*.

Duże zbiory danych *(big data)* z inteligentnych urządzeń lub czujników analizuje 26% dużych (powyżej 250 pracowników) polskich firm. To tylko 5 punktów proc. poniżej średniej w całej UE (31%) i najlepszy wynik w grupie nowych członków UE, co może być postrzegane jako niezły wynik, biorąc pod uwagę mniejsze budżety IT w Polsce.

Tylko 7% małych i średnich polskich przedsiębiorstw (10-250 pracowników) korzysta z własnych analiz *big data*. W rozwiniętych krajach starej UE korzystanie z tego typu analiz w mniejszych firmach jest jednak również dużo niższe – średnia dla całej Unii wynosi 12%.

*Raport **„State of Polish AI 2021”** przedstawia stan rozwoju rynku sztucznej inteligencji w Polsce oraz zalecenia, które pozwolą polskim przedsiębiorcom dotrzymać kroku najlepszym gospodarkom świata. W trakcie tegorocznej, trzeciej już edycji Digital Festivalu poświęcimy temu zagadnieniu sporo miejsca. Chcemy uświadomić uczestnikom, że od sztucznej inteligencji nie ma ucieczki*
– Paulina Szkoła, Project Manager w Fundacji Digital Poland.

Przyszłość VSS

Kamera Zdefiniowana Programowo

Jan T. Grusznic

Wkroczyliśmy w erę, w której wartość zdecydowanie przesuwa się ze sprzętu na oprogramowanie. Dla użytkowników komputerów oznacza to, że sprzęt – serwer, pamięć masowa lub sieć – nie jest już dostarczany fizycznie przez personel IT.

Wiele popularnych terminów funkcjonujących w dzisiejszym świecie technologii IT, np. sieci zdefiniowane programowo (SDN – *Software Defined Network)*, pamięć masowa zdefiniowana programowo (SDS – *Software Defined Storage)* i centrum danych zdefiniowane programowo (SDDC – *Software Defined Data Center),* jest częścią szerszego trendu, który równie dobrze można nazwać Wszystko Zdefiniowane Programowo (SDE lub SDx – *Software Defined Everything*)[1]. Fizyczne przedmioty i funkcje z naszego codziennego życia również stają się zdefiniowane przez oprogramowanie. To przeniesienie wartości na oprogramowanie ma konsekwencje znacznie wykraczające poza branżę IT i zaczyna dotykać nas – branżę elektronicznych systemów zabezpieczeń.

1) https://www.sdxcentral.com/cloud/definitions/software-defined-everything-sdx-part-1-definition/ (dostęp: 3.02.2016).

INTELIGENTA KAMERA

W roku 2018 prawie wszystkie analizy głębokiego uczenia się były przetwarzane na serwerze lub w chmurze, a nie w urządzeniu końcowym. Obecnie, dzięki układom scalonym z dedykowanym akceleratorem sprzętowym dla algorytmów opartych na sieciach neuronowych, podstawowe wykrywanie i klasyfikacja obiektów stały się standardową funkcją także w kamerach. Nie dziwi zatem fakt, że coraz większa liczba sprzedawców zajmuje się marketingiem aplikacji do kamer dozoru wizyjnego. Jest to kolejny przejaw zwiększonej mocy przetwarzania w urządzeniach końcowych i korzyści z wdrożeń zdecentralizowanej architektury. Aplikacje do kamer dozorowych nie są nową koncepcją. Odrodzenie ekosystemów opartych na aplikacjach wynikło z ponownego zainteresowania się analityką wizji napędzanej postępami technologicznymi w zakresie sieci neuronowych. Wiele nowych aplikacji dostępnych u przedstawicieli producentów naszej branży opiera się na analizie obrazu opartej właśnie na głębokim uczeniu. Wśród znanych ekosystemów aplikacji do kamer dozoru wizyjnego są:

- Software Defined Camera firmy Huawei,
- Stowarzyszenie SAST (Security and Safety Things) wspierane przez firmę Bosch i związane z nią stowarzyszenie Open Security and Safety Alliance,
- AXIS Camera Application Platform
- Hanwha Open Platform Application,
- MOBOTIX Certified Apps.

Wymienione platformy oferują aplikacje do pobrania do kompatybilnych kamer sieciowych za pośrednictwem „sklepu" z aplikacjami. Takie podejście potencjalnie oferuje możliwość zdalnej zmiany możliwości kamery za pomocą uruchomienia na niej pobranego oprogramowania. Zapożyczony przez Huawei termin ze świata IT (zdefiniowane oprogramowaniem) w odniesieniu do kamer dozoru wizyjnego idealnie wiąże się z kolejnym etapem rozwoju tych kamer. Obecnie jednak oprogramowanie stosowane w kamerach jest sprzężone ze sprzętem, co stanowi ograniczenie[2]. Dopiero oderwanie części sprzętowej od programowej umożliwia zrównoważony rozwój algorytmów przez cały cykl życia kamery, wymagając tylko jednorazowej inwestycji w sprzęt[3].

KAMERA ZDEFINIOWANA PROGRAMOWO (SDC – SOFTWARE DEFINED CAMERA)

Gdy w 2018 r. SAST ogłosił wizję rewolucyjnej platformy z globalnym ekosystem do rozwoju innowacyjnych aplikacji kamer stosowanych w systemach dozoru wizyjnego, pojawiło się wielu sceptyków wskazujących na małe prawdopodobieństwo zmiany pola widzenia kamer w taki sposób, aby można je było uwzględnić w innych zastosowaniach, zwłaszcza że po zakończeniu konfiguracji systemu rzadko zmienia się funkcja kamery. Dzisiaj SAST oferuje 95 różnych aplikacji 29 deweloperów dla 15 urządzeń pochodzących od sześciu producentów[4]. Ciągła praca nad ulepszeniem tradycyjnych kamer dozoru wizyjnego zmieniła te urządzenia z pojedynczego źródła danych do wielowymiarowej ich integracji. Dostępne dzisiaj nawet najprostsze sieciowe kamery dozoru wizyjnego pełnią wielorakie funkcje: przechwytują strumienie wizji wysokiej rozdzielczości, kodują obraz i zarządzają jego transmisją, przechowują dane wideo czy analizują gromadzone dane. Dostawcy kamer natomiast próbują stworzyć szeroką gamę aplikacji dla różnych scenariuszy bezpieczeństwa, takich jak świadomość sytuacyjna, punkty kontroli oparte na biometrii, inteligentny nadzór transportu (ITS) i punkty kontroli pojazdów.
Nie oznacza to jeszcze, że mamy do czynienia z kamerami definiowanymi programowo. U podstaw SDC bowiem leżą ciągła ewolucja i rozwój algorytmów sztucznej inteligencji (AI), otwartość umożliwiająca integrację i wdrażanie sztucznej inteligencji w różnych scenariuszach bezpieczeństwa oraz cyberbezpieczeństwo na kilku poziomach: sprzętu, aplikacji i danych.

Rys. 1. Transformacja kamer do SDC oparta na trzech kluczowych trendach

(źródło: Software-Defined Cameras for Edge Computing of the Future, a Presentation from Arm, 30.05.2021)

REKOMENDACJA ITU

Aby jasno określić, czym jest kamera zdefiniowana programowo oraz jakie musi spełniać kryteria, Międzynarodowa Jednostka Telekomunikacyjna (ITU) w lipcu 2020 r. wprowadziła, pod numerem rekomendacji ITU-T F.735.1, pierwszy międzynarodowy standard kamer definiowanych programowo. W preambule dokumentu normatywnego autorzy wskazują na fakt, że wraz z rozwojem urządzeń i metod analizy zawartości obrazu są opracowywane różne algorytmy oparte na sieciach neuronowych dla dużej liczby scenariuszy. Aby spełnić stawiane przed nimi wymagania, niezbędne jest stworzenie kamer zdefiniowanych programowo, które zapewnią techniczne podejście do rozdzielenia sprzętu od oprogramowania, umożliwiając realizację następujących wymagań:

Wdrażanie algorytmów na żądanie i aktualizacja online
Kamery definiowane programowo obsługują różne aplikacje dzięki jednoczesnej obsłudze wielu algorytmów i aktualizowaniu ich na żądanie. W tradycyjnych systemach dozoru wizyjnego wdrożenie nowej funkcji lub uaktualnienie działającego już algorytmu na ogół wymaga ponownego uruchomienia systemu operacyjnego kamery lub restartu aplikacji. W systemach z kamerami SDC administrator może wdrożyć nowe algorytmy, wysyłając polecenie wdrożenia lub aktualizacji do kamer, które następnie zastosują tę nową funkcję bez ponownego uruchamiania systemu lub innych przerw w działaniu usług.

Wieloalgorytmowe obliczenia równoległe
Kamera SDC obsługuje wieloalgorytmowe obliczenia równoległe. Oznacza to, że może pracować poprawnie z równocześnie działającymi różnymi algorytmami analizy obrazu, np. rozpoznawaniem pojazdów, analizą ruchu/ruchu pieszych, wyodrębnianiem atrybutów ludzkiego ciała itp. Kombinacja algorytmów może działać jako określony tryb pracy urządzenia, zatem będzie się liczyć nie tylko samo wykrycie, lecz również sekwencja detekcji (dla wielu aplikacji). Użytkownicy systemu VSS mogą przełączać się między różnymi trybami, aby dostosować różne scenariusze pracy.

Umiejętność ciągłego uczenia się
Bodaj najbardziej oczekiwana opcja – kamera SDC – wspiera ciągłą naukę sieci neuronowych online. Automatycznie zbiera, czyści i oznacza dane wideo lub obrazy zarejestrowane w rzeczywistej scenie jako zestaw szkoleniowy. Następnie używa go do trenowania oryginalnego modelu szkoleniowego sieci neuronowych, który jest już osadzony wewnątrz urządzenia i dostosowuje parametry tego modelu, aby zakończyć proces jego ostateczną optymalizacją. Dzięki temu model uczenia się staje się odpowiedni dla rzeczywistej sceny, a także poprawia dokładność wyniku analizy.
W ramach rekomendacji znalazł się też opis ogólnej 3-warstwowej architektury funkcjonalnej, którą przedstawiono na *rys. 2:*

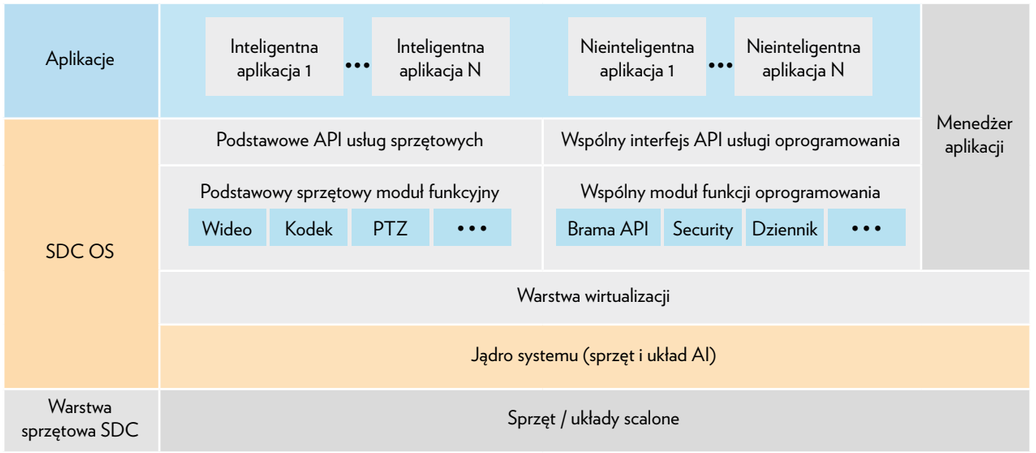
I. warstwa sprzętowa SDC – zapewnia odpowiednie zasoby sprzętowe i chipy AI dla warstwy górnej;

II. warstwa SDC OS – składa się z podstawowego interfejsu API usługi sprzętowej, wspólnego interfejsu API usługi oprogramowania, wspólnego modułu funkcji oprogramowania, podstawowego modułu funkcji sprzętu, warstwy wirtualizacji, menedżera aplikacji i jądra systemu.

1. Jądro jest sterownikiem sprzętu i układów AI.
2. Podstawowy sprzętowy moduł funkcyjny obsługuje najważniejsze usługi związane z kamerą takie jak przetwarzanie obrazu, kodowanie, generowanie strumienia, sterowanie PTZ itp.
3. Podstawowe API usług sprzętowych to API usługowe podstawowego modułu funkcyjnego sprzętu.
4. Wspólny moduł funkcji oprogramowania służy do zapewnienia wspólnych funkcji oprogramowania kamery, które obejmują interfejs bramy API, zarządzanie zdarzeniami, zabezpieczenia, rejestr itp.
5. Wspólny interfejs API usługi oprogramowania służy do udostępniania interfejsów usług, działa jako brama API dla kamery; wszystkie dane wynikowe z uruchomionych aplikacji są dostarczane za pośrednictwem tego wspólnego interfejsu API usługi oprogramowania.
6. Menedżer aplikacji to menedżer kontenerów, który obsługuje zarządzanie cyklem życia aplikacji – instalację, aktywację, dezaktywację, deinstalację, aktualizację, zarządzanie licencjami itp.

2) Takim ograniczeniem jest np. liczba symultanicznie pracujących różnych aplikacji lub wymóg stosowania API i/lub SDK danego producenta (które same w sobie też wprowadzają ograniczenia).
3) https://e.huawei.com/gr/products/intelligent-vision/cameras/software-defined-camera (dostęp: 23.07.2021).
4) https://www.securityandsafetythings.com (dostęp: 27.07.2021).

Rys. 2. Architektura funkcjonalna SDC



(źródło: ITU-T F.735.1)

7. Warstwa wirtualizacji służy do izolacji zasobów aplikacji i obsługi aktualizacji oraz wdrażania online bez przerw w działaniu usług; główną technologią stosowaną w tym przypadku jest technologia kontenerowa.

III. Warstwa aplikacji – aplikacja łączy się w tym miejscu z systemem operacyjnym używanym w kamerze. Warstwa aplikacji składa się z aplikacji „inteligentnych" i „nieinteligentnych". „Inteligentne" obejmują rozpoznawanie twarzy, rozpoznawanie tablic rejestracyjnych itp. „Nieinteligentne" aplikacje mogą być stosowane do przesyłania strumieniowego wideo, przekształcania, zarządzaniem sygnałami z czujników powiązanych itp[5].

TRENDY STOJĄ TWARDO ZA SDC

Postęp technologiczny, powiększająca się populacja i coraz większe obawy dotyczące bezpieczeństwa, wzrost liczby przestępstw i wykroczeń drogowych to tylko niektóre z głównych czynników napędzających globalny rynek kamer zdefiniowanych programowo. Kwestia dzisiejszej wielowymiarowości kamer jest adresowana do wielu użytkowników tego samego systemu dozoru wizyjnego, przez co cele stawiane zarówno kamerom, jak i systemom stają się różne. Przykładem może być jednoczesna potrzeba zbierania informacji statystycznych związanych z ruchem pojazdów i klasyfikacja zdarzeń drogowych wraz z identyfikacją wszystkich pojazdów tych zdarzeń.
Jednocześnie jest wiele różnych czynników związanych z kamerami SDC, które działają hamująco na rozwój tego rynku, np. zmienność warunków pogodowych (wpływających negatywnie na poziom jakości analizy obrazu), wysokie początkowe koszty wdrożenia, stosunkowo wysoki koszt utrzymania czy brak narzędzi do zarządzania urządzeniami i aplikacjami. Co więcej, trudności w instalacji i ciągle utrzymujący się niski wskaźnik udanych wdrożeń stanowią wyzwania stojące przed dostawcami takich kamer.

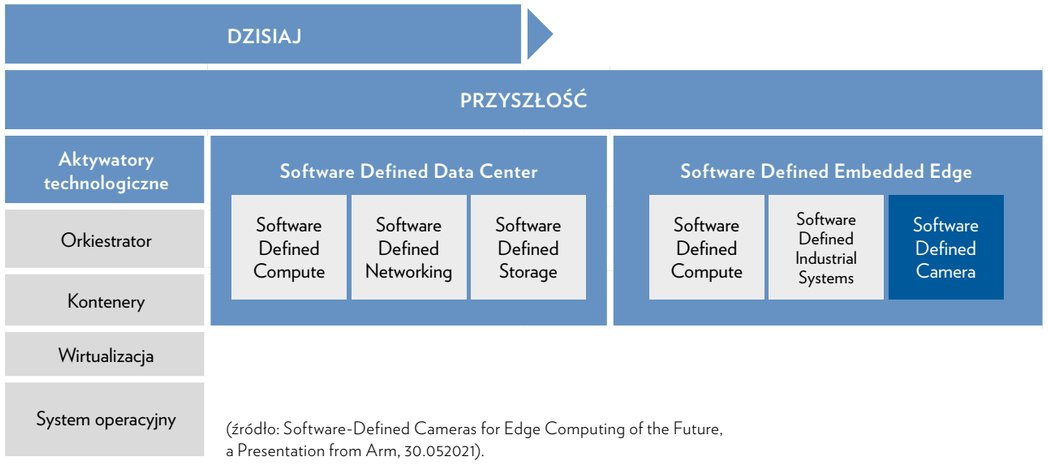
Tymczasem postęp w technologiach, takich jak sztuczna inteligencja, Internet rzeczy i uczenie maszynowe, stwarzają lukratywne możliwości dla globalnego rynku kamer SDC. Według globalnej firmy doradczej ds. rynku technologii, ABI Research, światowa baza inteligentnych kamer z chipsetem sztucznej inteligencji osiągnie w 2025 r. ponad 350 mln sztuk. Włączenie chipsetów AI do kamer dozoru wizyjnego stanie się normą, przy czym ponad 65% kamer dostarczonych w 2025 r. ma być wyposażonych w co najmniej jeden chipset AI. Kamery te będą zawierały modele głębokiego uczenia, które zautomatyzują i usprawnią podejmowanie decyzji w takich zastosowaniach, jak inteligentne zarządzanie ruchem drogowym, autonomiczne urządzenia, monitorowanie i zarządzanie ruchem pieszych, bezpieczeństwo fizyczne i obwodowe oraz zapobiegawcze wykrywanie zagrożeń[6].
Przyspieszenie wynika z istniejącego trendu SDx. Postęp technologiczny utorował drogę do prawdziwego zdefiniowania centrum danych jako zdefiniowanego programowo. Sieci zdefiniowane programowo i pamięć masowa zdefiniowana programowo stały się normą. Według przedstawicieli firmy ARM[7] widoczne inicjatywy SDx w różnych branżach, np. motoryzacyjnej, pozwalają optymistycznie myśleć również o branży elektronicznych systemów zabezpieczeń[8]. W przypadku wielu produktów do przechwytywania obrazu, w tym w kamerach, zachodzi ogromna transformacja, której podstawą są przede wszystkim trzy kluczowe trendy (rys. 1):

1. przejście na obliczenia brzegowe,
2. bezpieczeństwo – ze względu na charakter danych,
3. naturalna praca w chmurze, co daje kamerom ogromny potencjał do uruchamiania aplikacji, które mogą być wdrażane z biegiem czasu. Takie podejście również wydłuża znacząco czas życia produktu.

PODSUMOWANIE

Posiadanie otwartego standardu i jednego systemu operacyjnego dla urządzeń elektronicznych systemów zabezpieczeń oznacza, że różni dostawcy sprzętu i oprogramowania mogą korzystać z tej samej platformy. Teoretycznie ułatwia to implementację najlepszych w swojej klasie rozwiązań, zwiększa elastyczność do wprowadzania zmian i jednocześnie zapewnia ściślejszą kontrolę cyberbezpieczeństwa w porównaniu z dotychczasowymi protokołami interpretacyjnymi. Może to również oznaczać, że konfiguracje systemów i aplikacje kamer mogą zmieniać się częściej ze względu na łatwiejszy model dostarczania zapewniany przez ekosystem aplikacji, nieskrępowany obecnymi, bardziej ręcznymi i czasochłonnymi procesami. Ekosystem, umożliwiając zdalną i bezpośrednią sprzedaż oprogramowania, a nawet instalację, będzie wymagać od każdego dewelopera aplikacji znacznych inwestycji w odpowiednie wsparcie techniczne i konfiguracyjne, zwłaszcza gdy mają zbudować skuteczną i wysoko ocenianą aplikację dla urządzeń elektronicznych systemów zabezpieczeń.
Model „sklepu z aplikacjami" może jednocześnie znacząco zakłócić tradycyjny kanał sprzedaży i model licencjonowania oprogramowania w branży dozoru wizyjnego. Gdy różne urządzenia IoT (zatem nie tylko kamery) również znajdą się na tej samej platformie, zwiększy się wymóg wymiany danych i konwergencji urządzeń.
Chociaż ekosystem aplikacji nie jest koncepcją nową, istnieje ryzyko, że może być siłą zakłócającą porządek nie tylko w branży, ale także w dziedzinach bezpieczeństwa i IoT. I może stać się „nową normalnością" dla branży.

Rys. 3. Trendy rozwoju SDx wg ARM



(źródło: Software-Defined Cameras for Edge Computing of the Future, a Presentation from Arm, 30.052021).

WG RAPORTU TRANSPARENCY MARKET RESEARCH PRZEWIDUJE SIĘ, ŻE W NAJBLIŻSZEJ PRZYSZŁOŚCI AMERYKA PŁN. I EUROPA STANĄ SIĘ WIODĄCYMI REGIONAMI ŚWIATOWEGO RYNKU KAMER DEFINIOWANYCH PROGRAMOWO. TU SPRZEDAWCY ZAPEWNIAJĄ NAJNOWOCZEŚNIEJSZE ROZWIĄZANIA. NOWE PROJEKTY I MODERNIZACJA KAMER STANDARDOWYCH DO KAMER DEFINIOWANYCH PROGRAMOWO W REGIONIE AZJI I PACYFIKU MAJĄ DO 2027 R. ZWIĘKSZYĆ RYNEK SDC W REGIONIE. OCZEKUJE SIĘ, ŻE CORAZ POWSZECHNIEJSZE STOSOWANIE AUTOMATYZACJI I ROSNĄCA POTRZEBA ZDALNEGO ZARZĄDZANIA ZASOBAMI BĘDZIE NAPĘDZAĆ GLOBALNY RYNEK TYCH ROZWIĄZAŃ W NAJBLIŻSZEJ PRZYSZŁOŚCI

(źródło: Software-defined Camera, SDC, Market – Global Industry Analysis, Size, Share, Growth, Trends, and Forecast, 2019–2027)

JAN T. GRUSZNIC

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

5) Urządzenia PoE instalowane między przełącznikiem sieciowym a urządzeniami sieciowymi, które muszą być zasilone przez okablowanie ethernetowe. Urządzenie *midspan* jest przezroczyste dla komunikacji TCP/IP.

6) https://www.abiresearch.com/press/global-installed-base-smart-city-cameras-ai-chipset-reach-over-350-million-2025/ , 29-07-2021

7) ARM Limited zapewnia usługi w chmurze i rozwiązania Internetu rzeczy (IoT). Firma koncentruje się na projektowaniu i rozwoju procesorów komputerowych, kontrolerów pamięci, systemów protokołów internetowych, audio, wideo i audio, procesorów graficznych, zabezpieczeń i urządzeń pamięci masowej. W roku 2005 wyprodukowano blisko 1,7 miliarda procesorów opartych na technologii ARM, co stanowiło 75% wszystkich 32-bitowych procesorów na rynku

8) „Software-Defined Cameras for Edge Computing of the Future", Parag Beeraka, ARM, 30-05-2021

9) IHS Markit Security Technologies Top Trends For 2019, 2018 r.

Zdalny monitoring wizyjny smart monitoring?

Daniel Kamiński

Na świecie jest już zainstalowanych ponad miliard kamer. Czy dzięki nim jest bezpieczniej? Wiele raportów wskazuje, że stosowanie kamer w miejscach publicznych zredukowało liczbę przestępstw. Analizując nagrania z włamań do obiektów, można jednak zauważyć, że przestępcy nie obawiają się kamer.

MONITORING WIZYJNY – PRZECIEŻ TO NIE DZIAŁA!

Tradycyjny system monitoringu wizyjnego składa się z kilku kamer, monitora i rejestratora. Kamery są montowane w widocznych miejscach, mają być widoczne dla klientów, pracowników czy potencjalnych intruzów. Z tego względu większość utożsamia kamery z systemem monitoringu i na tej podstawie buduje swoje wyobrażenie o ochronie. Mam kamery, więc jestem chroniony. Część osób podgląda na bieżąco obrazy z kamer na monitorze. Weryfikują godziny otwarcia sklepów, liczbę klientów w punktach usługowych, obecność palet w strefie załadunku itp. Zbierane są doświadczenia, czasem negatywne, gdy obraz z kamery jest np. zamazany lub nieczytelny. Wtedy wzywa się serwis, aby przemyć obiektyw, usunąć pajęczyny, dostroić obraz, poprawić połączenia. Takie osoby bardziej realistycznie podchodzą do korzystania z kamer. Tylko nieliczni mają potrzebę analizowania archiwum. Musi się coś wydarzyć, aby pojawiła się potrzeba przeglądania historii. Może to być szkoda komunikacyjna na parkingu i chęć zidentyfikowania sprawcy. Może być reklamacja dotycząca dostawy i konieczność potwierdzenia kompletacji wysyłki. Oczywiście może to być kradzież i potrzeba weryfikacji, kto jej dokonał. Wówczas często pojawia się zaskoczenie, np. okazuje się, że obraz się nie nagrał! Osoby, które tego doświadczyły, negatywnie odnoszą się do usług monitoringu wizyjnego.

DLACZEGO WŁAMYWACZE NIE BOJĄ SIĘ KAMER?

Ważna uwaga: wg tradycyjnego podejścia system monitoringu wizyjnego jest nastawiony na prewencję. Nie stanowi aktywnej ochrony. W przypadku kradzieży pozwala jedynie odszukać w archiwalnym materiale, co się wydarzyło, o ile znany jest czas zdarzenia. Jeśli minęło już kilka dni, to odszukanie zdarzenia zajmie sporo czasu. Taką wiedzę na temat działania tradycyjnego systemu monitoringu wizyjnego ma większość złodziei. Po pierwsze wiedzą, że kamera nie powiadomi właściciela o tym, że intruz jest w obiekcie. Po drugie istnieje prawdopodobieństwo, że dysk rejestratora już się zużył i nic się nie nagrywa. A nawet jeśli się nagrywa, to obraz będzie nieostry. Dlatego wystarczy, że założą czapkę z daszkiem, aby w razie złapania twierdzić, że to nie ich wizerunek.

CZEGO NIE LUBIĄ WŁAMYWACZE?

Jest kilka rzeczy, których nie lubią osoby dokonujące kradzieży. Głównie nie lubią zdemaskowania. Na złodzieju czapka gore – mówi przysłowie. Złodziej w trakcie włamania jest zestresowany. Wykrycie intruza w obiekcie powoduje jego ekstremalne zaskoczenie. Wystarczy szczekanie psa czy zadziałanie czujnika zmierzchowego, aby zniechęcić włamywacza, przynajmniej na chwilę. Jeszcze lepiej, niezależnie od pory dnia, zadziała system alarmowy, który może dodatkowo uruchomić syrenę.

Ważny warunek: szczekanie psa, włączenie się oświetlenia w nocy czy wycie sygnalizatora musi sprowokować czyjąś reakcję – pojawienie się sąsiada w oknie, zatrzymanie się przechodnia, wyjście pracownika itp. Każda z tych sytuacji oznacza dla włamywacza duże ryzyko zdemaskowania. A to stres. Włamywacz poszuka innych miejsc, którymi nikt się nie interesuje. Ważny jest również czas przeznaczony na dokonanie kradzieży. W miejscach, które są wyposażone w dobre zabezpieczenia mechaniczne, włamywacz musi poświęcić dużo czasu na ich pokonanie. Im dłużej będzie wiercił czy rozbijał, tym większe prawdopodobieństwo, że ktoś go zauważy. Dlatego obiekty znajdujące się na uboczu są bardziej narażone na ryzyko włamań.

Warto wiedzieć, że w miejscach, gdzie jest duże zainteresowanie otoczenia, kradzież z włamaniem zajmuje tylko kilka minut. Z kolei obiekty znajdujące się na uboczu włamywacze mogą plądrować przez cały weekend. Wielkość szkód jest wtedy znacznie większa. I niestety nie zależy od tego, czy w obiekcie są kamery, czy ich nie ma.

GŁOŚNIKI – ZDALNA REAKCJA NA ALARMY WIDEO

Do niedawna popularnym rozwiązaniem problemu włamywaczy było zatrudnienie pracowników ochrony. Zajmowali się oni lokalną obserwacją obrazów z kamer, wykonywali okresowe obchody, pokazując, że w obiekcie są ludzie, oraz reagowali na zdarzenia alarmowe. Kamery wspierały ich w pracy oraz stanowiły ewidencję dla inwestora.

W ostatnim czasie sporo się jednak zmieniło. Koszty pracy wzrastały kilkakrotnie. Pandemia COVID-19 spowolniła rozwój części przedsiębiorstw i spowodowała powszechną obawę przed wzajemnymi bliskimi kontaktami. W efekcie koszty ochrony fizycznej wzrosły, a klienci zaczęli poszukiwać zautomatyzowanych rozwiązań pozwalających utrzymać odpowiedni poziom bezpieczeństwa w obiektach. Rozpoczęła się transformacja usług ochrony wykorzystująca nowe technologie i zdalne zarządzanie bezpieczeństwem. Model monitoringu wizyjnego rozszerza się o detekcję zagrożeń, powiadomienia o zdarzeniu oraz zdalną reakcję operatorów.

Coraz częściej zdalny monitoring wizyjny zaczyna wypierać ochronę fizyczną przy zachowaniu poziomu bezpieczeństwa. Pracownicy ochrony zdalnie obserwują obrazy z kamer, wykonują wirtualne obchody wideo oraz reagują na zdarzenia alarmowe. Pierwszą reakcją są komunikaty głosowe nadawane poprzez głośniki. Zidentyfikowany intruz otrzymuje szybką informację, że został wykryty. Następnie dostaje polecenie, że ma opuścić chroniony teren, a patrol interwencyjny jest w drodze.

Głośniki sprawdzają się równie dobrze w przypadku czynności porządkowych. Jeśli kierowca zaparkuje w strefie zakazu, blokując np. dostęp do śmietnika, operator może od razu polecić mu przeparkowanie pojazdu. Nie trzeba szukać właściciela auta, można zareagować w momencie, gdy się znajduje jeszcze w pojeździe.

FAŁSZYWE ALARMY – MROCZNA STRONA MONITORINGU WIZYJNEGO

Zdalny monitoring wizyjny wymaga właściwego podejścia oraz odpowiednich urządzeń. Tradycyjne rozwiązania telewizji dozorowej niestety się nie sprawdzają – generują dużo fałszywych alarmów. Funkcja detekcji ruchu w zwykłej kamerze pozwala zmniejszyć ilość archiwizowanego materiału, ale nie sprawdza się w zdalnym monitoringu, ponieważ może generować tysiące zdarzeń dziennie. W kamerach coraz częściej pojawiają się funkcje przekroczenia linii lub wejścia w zaznaczony obszar. Są to pożądane funkcje, ale w tańszych kamerach (o gorszej jakości obrazu) nie są odporne na warunki środowiskowe (deszcz, śnieg), zwierzęta, owady, refleksy świateł z przejeżdżających pojazdów, przez co generują nawet kilkaset alarmów z jednej kamery w ciągu dnia. Taka liczba alarmów powoduje, że usługa zdalnego monitoringu jest nieopłacalna w realizacji. Ponadto operator monitoringu, który obsługuje podczas dyżuru tysiące fałszywych alarmów, może się pomylić i pominąć alarm prawdziwy, a to oznacza dodatkowe straty.

Trzeba też mieć świadomość tego, że wiele firm ochrony dopiero się uczy świadczyć usługi monitoringu wizyjnego. Często mają jednego operatora i dopiero odkrywają wyzwania, jakie niesie ta usługa. Ale szybko się rozwijają, bo zainteresowanie klientów dynamicznie rośnie.

SMART MONITORING – CZYLI JAK OGRANICZYĆ LICZBĘ ALARMÓW?

Opcji jest kilka. Po pierwsze warto korzystać z rozwiązań CCTV/VSS wyposażonych w technologię inteligentnej analizy obrazu (VCA/IVA). Oferują ją droższe modele kamer z tzw. mechanizmem uczenia maszynowego. Można też wykorzystać dedykowane urządzenia do analizy obrazu instalowane niezależnie od kamer. Co prawda nie ma jeszcze w 100% skutecznych

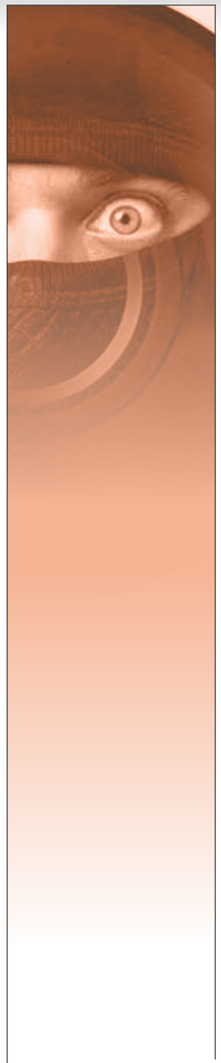
algorytmów analizy obrazu, ale tego typu rozwiązania generują znacznie mniej alarmów fałszywych.
Inną opcją jest zastosowanie czujek zewnętrznych (systemu alarmowego), które będą wykrywać zagrożenia. Mogą to być czujki ruchu, bariery optyczne, radary czy kable sensoryczne (wkopywane w ziemię lub montowane na ogrodzeniu). Bardziej zaawansowane czujki z analizą cyfrową sygnałów będą generowały znacznie mniej alarmów, ale ich koszt jest większy.
Niezależnie od tego, czy jest to analiza obrazu, czy czujki zewnętrzne, ważna jest jakość montażu kamer i detektorów. Gdy są nieodpowiednio skonfigurowane po zainstalowaniu, powodują dużo alarmów; gdy poprawnie, nie generują ich. Należy też pamiętać, że wymagają sezonowej konserwacji, aby jakość detekcji się nie pogorszyła.
Recepta na sukces? Od strony obiektu najbardziej skutecznym rozwiązaniem ograniczenia uciążliwych zdarzeń alarmowych będzie zastosowanie zarówno algorytmów analizy obrazu, jak i czujek, które muszą być właściwie zainstalowane. Oczywiście dobór rozwiązań jest zależny od rodzaju ochranianego obiektu.

ANALIZA OBIEKTÓW W CHMURZE – LUDZIE I POJAZDY

Zarówno czujki zewnętrzne, jak i analiza obrazu z kamery mająca na celu identyfikację intruza mają ograniczenia. Częstym problemem są alarmy wywołane przez dziki, lisy, koty czy inne zwierzęta. Z obsługą kilku obiektów operator monitoringu dobrze sobie radzi. Widzi, że system działa, i ma satysfakcję ze swojej pracy. Jednak gdy na jednego operatora przypada 80 czy 100 obiektów, obsługa niepotrzebnych, uciążliwych alarmów stanowi duże wyzwanie. Wtedy, z perspektywy centrum monitoringu, przydatna jest identyfikacja osób i pojazdów w obrazie pozwalająca odfiltrować niepotrzebne do obsługi zdarzenia. Można to uzyskać dzięki dedykowanemu serwerowi z funkcjami analizy obrazu albo korzystając z usług w chmurze. Jedno i drugie rozwiązanie wymagają wsparcia przez sztuczną inteligencję. Zaletą rozwiązania chmurowego jest duża ilość obsługiwanych strumieni wizyjnych. Im więcej podłączonych kamer, tym lepsze efekty pracy algorytmów sztucznej inteligencji. Można powiązać rozpoznawanie zachowań z rodzajem obiektów oraz dostosowywać algorytmy do sytuacji w nich.

ROLA OBSŁUGI CENTRUM MONITORINGU

Należy podkreślić, że ostateczną decyzję zawsze podejmuje człowiek. Opisane rozwiązania i algorytmy VCA mają uwolnić operatora od niepotrzebnej pracy. Ale to on decyduje, czy przekazać komunikat przez głośnik, wysłać załogę interwencyjną, czy powiadomić klienta.
Praca operatora jest w pewnym sensie powtarzalna, dlatego ułatwiają ją procedury obsługi alarmów. Będą one inne w przypadku ochrony parku maszynowego na budowie, inne w ochronie ogrodu zewnętrznego marketu budowlanego czy osiedla mieszkaniowego. Przypominam, że wiele firm uczy się dopiero świadczyć usługi zdalnego monitoringu, więc posiadają jedną procedurę – operator odpowiada za wszystko. Niestety tak się nie da, trzeba od razu określić zakres usług ochrony. Nie tylko po to, by analiza obrazu mogła być prawidłowo wdrożona, ale również po to, aby operator mógł szybko podejmować decyzje.



BIZNESOWE WYKORZYSTANIE ANALIZY OBRAZU – ANALIZA ZACHOWAŃ

Transformacja usług ochrony zachęca klientów do poszukiwania dodatkowych zastosowań rozwiązań, za które płacą. Kamery i czujki mogą być traktowane jako sensory IoT przekazujące dane do chmury. Tam dane są poddawane analizie i przedstawiane w postaci biznesowych raportów.
Zastosowanie kamer z analizą obrazu umożliwia liczenie klientów, sygnalizowanie odstępstw od standardów BHP (np. brak kasku na terenie budowy) czy wykrywanie zachowań wskazujących na kradzież sklepową. Coraz częściej z systemów kojarzonych z ochroną chcą korzystać działy marketingu, sprzedaży, logistyki, transportu czy produkcji. Moim zdaniem to dobra informacja dla naszej branży. Zainteresowanie nimi będzie rosło. Ale to również olbrzymie wyzwanie, ponieważ potrzebne będzie lepsze zrozumienie procesów obecnych w organizacjach naszych klientów. Ochrona już nie wystarczy, ważna jest wartość dodana.

PODSUMOWANIE

Trudny czas wymusza zmiany rynkowe. Usługi ochrony fizycznej na tym stracą, ale zyskają usługi zabezpieczenia technicznego. Część firm już to zauważyła i dostosowała ofertę lub jest w trakcie jej dostosowania.
Usługi techniczne stały się bardziej zaawansowane. Dziś kamera już nie wystarczy. Potrzebne są inteligentna analiza obrazu, zastosowanie głośników, właściwe oprogramowanie w centrum monitoringu oraz analiza zachowań do wykorzystania w biznesie. Zmiany te będą miały wpływ na klientów, usługodawców i dostawców rozwiązań. Część firm zniknie z rynku, ale powstaną nowe, bardziej nowoczesne. W cenie będą wiedza i specjalizacja, kluczem zaś dostępność specjalistów.

DANIEL KAMIŃSKI

Absolwent kierunku Telekomunikacji WAT oraz Kierowania Systemami Teleinformatycznymi AON. Od 1995 r. w branży zabezpieczeń technicznych związany z monitoringiem alarmów. Pierwsze 10 lat w grupie AAT/CMA odpowiadał za utrzymanie ciągłości działania centrum monitorowania, następnie w międzynarodowych firmach G4S i ADT za monitoring, instalacje i serwis. W ostatnich latach wykorzystywał swoje doświadczenie w firmach Juwentus oraz EBS. Od ponad 20 lat dzieli się swoją wiedzą na łamach czasopism branżowych. Wykładowca PISA, członek sekcji zabezpieczeń technicznych PIO.

Dzięki wprowadzeniu profilaktyki samobójstw wśród osób pozbawionych wolności liczba skutecznych prób samobójczych od 2007 r. istotnie spadła[1]. Prewencja wśród osadzonych realizowana jest we wszystkich jednostkach penitencjarnych kraju.

Czy inteligentna analiza wizyjna

zapobiegnie samobójstwom w celi więziennej?

Cz. 1. Skuteczność pracy operatora

Cezary Mecwaldowski

Robert Poklek

Zgodnie z instrukcją zawierającą 3-stopniowy model oddziaływań: profilaktyka presuicydalna I rzędu (dla wszystkich osadzonych), II rzędu (dla osadzonych z wysokim ryzykiem suicydalnym) oraz profilaktyka postsuicydalna (dla osadzonych po próbie samobójczej) działania te wymagają koordynacji i sprawnej komunikacji wielu pionów służby więziennej[2]. W tym celu wykorzystywany jest system dozoru wizyjnego, z wyznaczonym stanowiskiem operatora systemu tzw. monitorowego.

Nadal niestety zdarzają się skuteczne samobójstwa i, co dziwne, także w celach stale monitorowanych (24 godz. na dobę). Kiedy w poddanej dozorowi wizyjnemu celi stale obserwowanej przez funkcjonariusza ginie kolejny osadzony, trudno nie zadać sobie pytania: jak to było możliwe? Okoliczności na pierwszy rzut oka wydają się nieprawdopodobne, żeby nie zauważył on przez dłuższy czas np. osadzonego wiszącego na kracie czy siedzącego na łóżku z workiem foliowym na głowie. W takich sytuacjach operatorom „monitorowym" stawiane są zarzuty dyscyplinarne, a prokuratura prowadzi przeciwko nim śledztwo w sprawie karnej. Jednak czy słusznie wyciąga się konsekwencje wobec osoby, która *de facto* nie była w stanie dostrzec i zareagować na widoczny na ekranie monitora akt samobójczy? Jest kilka głównych powodów takiego stanu rzeczy i braku właściwej reakcji na zachowania osadzonego:

- Indywidualne właściwości wzroku (próg wrażliwości sensorycznej) i jego wady powodują, że niektóre bodźce w ogóle nie zostaną zarejestrowane percepcyjnie. Ponadto nie weryfikuje się parametrów jakościowych systemu dozoru wizyjnego, pozostawiając je wyłącznie subiektywnej ocenie.
- Nie da się objąć wzrokiem jednocześnie wszystkich obrazów na monitorach, ponieważ wzrok skupia się na wąskim wycinku całości (widzenie centralne). Tworzenie stanowiska operatora, które nie uwzględnia zasad ergonomii, znacząco utrudnia obserwację.
- Monotonia powoduje przyzwyczajenie się do widoku obrazów (habituacja) i obniżenie koncentracji uwagi (dryftowanie); jedynie bardzo silne bodźce są w stanie wzbudzić zainteresowanie znużonego operatora.
- Obserwacja wielu obrazów i przechodzenie do kolejnych powoduje, że operator przenosi percepcję z obrazu na obraz z kilkusekundowym opóźnieniem pomiędzy obrazami. Ponadto nie ma zachowanej pełnej sekwencji zachowania więźnia i kontekstu sytuacyjnego, dlatego bez oglądu całości trudno zinterpretować je jako zagrożenie czy przygotowanie do samobójstwa.
- Istnieje zjawisko „ślepoty z nieuwagi" polegające na nieświadomym pomijaniu niektórych bodźców w celu koncentracji na innych, uznanych za ważniejsze (nastawienie poznawcze).

Media również nie pozostają bierne i co jakiś czas donoszą o samobójstwach i zgonach więźniów w monitorowanych celach. Opinią publiczną targają wątpliwości co do okoliczności, w jakich dochodziło do tych samobójstw, zwłaszcza gdy dotyczyły osadzonych będących ważnymi świadkami lub podejrzanymi. Kierownictwo Służby Więziennej reaguje montowaniem kolejnych kamer w celach i innych miejscach przebywania więźniów. Należy podkreślić, że system monitoringu wizyjnego to nie tylko sprzęt i stanowisko operatora, ale także niezwykle ważny czynnik ludzki, z jego możliwościami i ułomnościami, dlatego powinien stanowić uzupełnienie innych sposobów profilaktyki suicydalnej.
Jak wynika z różnych badań prowadzonych w Anglii i USA, skuteczność obserwatora („sprawność obserwacji w przedziale czasu") waha się od 13 do 30%[3]. Odpowiadają za to różne zjawiska psychofizyczne, jakim podlega operator systemu dozoru wizyjnego. Analizując literaturę przedmiotu z zakresu psychologii procesów poznawczych, można dojść do wniosku, że nie jest możliwe zaobserwowanie wszystkich zdarzeń, które rozgrywają się w polu widzenia. Innymi słowy można na coś patrzeć i tego nie widzieć. Analizując pracę obserwatora na stanowisku monitorowego

1 Odpowiedź na interpelację poselską nr 8697 w sprawie programu zapobiegania samobójstwom w Polsce.

2 S. Lizyńczyk, *Próby i skuteczne samobójstwa w polskim systemie penitencjarnym w latach 2010– 2013 wybrane charakterystyki penitencjarne* „Profilaktyka Społeczna i Resocjalizacja" 2014, nr. 23, s. 19.

3 dr H. Uttam Keval, *Efektywność, projektowanie, konfiguracja i stosowanie telewizji dozorowej*. Część badawcza pracy doktorskiej Uniwersytet Londyński 2009 r.

pod kątem psychologicznych mechanizmów zaangażowanych w proces stałej obserwacji, należy zwrócić uwagę na jego kompetencje ujmowane w dwóch podstawowych kryteriach: poznawczym i osobowościowym. Kryterium poznawcze odnosi się do wrażeń (progu wrażliwości na bodziec), spostrzegania (percepcji, czyli łączenia odbieranych wrażeń z doświadczeniem i nadawanie im logicznego sensu), czasu reakcji, koordynacji wzrokowo-ruchowej, procesów uwagi (trwałości, przerzutności, podzielności) i pamięci (długotrwałej i krótkotrwałej) oraz funkcji wykonawczych (ocena, przewidywanie). Duża część z nich to predyspozycje wrodzone i fizjologiczne właściwości organizmu. Oprócz poznawczego istnieje kryterium związane z cechami osobowości, które wpływają na indywidualne reakcje na poziomie zarówno emocjonalnym, jak i behawioralnym, determinując zaangażowanie i sposób wykonania pracy. Właściwości te mogą podlegać modyfikacji w procesie szkoleniowym.

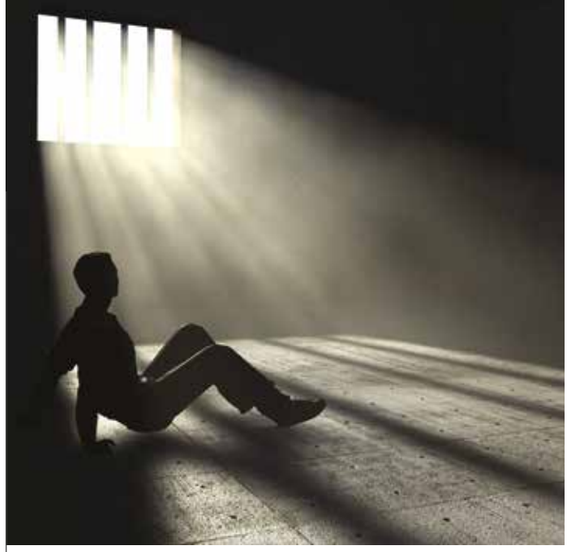
Autorzy artykułu od lat prowadzą badania nad poprawą efektywności pracy operatora systemu dozoru wizyjnego w Służbie Więziennej, realizującego stałą obserwację zachowania osadzonych w celach. Przeprowadzili m.in. badania eksperymentalne z wykorzystaniem tzw. testu goryla[4] opracowanego przez D. Simonsa i Ch. Chabrisa[5] z materiałem filmowym D. Simonsa z 2010 r.[6] w grupie 197 funkcjonariuszy – słuchaczy szkolenia zawodowego (155 badanych) oraz funkcjonariuszy wyższego szczebla. Wśród nich byli dyrektorzy jednostek penitencjarnych, kierownicy działu ochrony, psychologowie więzienni oraz specjaliści z Okręgowych Inspektoratów Służby Więziennej zajmujący się kwestiami ochronnymi, logistycznymi i informatycznymi, a także psychologowie więzienni (42 badanych).

Badania wykazały, że zdecydowana większość szeregowych funkcjonariuszy uczestniczących w szkoleniu zawodowym nie jest percepcyjnie zdolna do prawidłowego pełnienia służby na stanowisku operatora monitoringu wizyjnego. Zaledwie 8 osób spośród ponad 150 badanych byłoby zdolne do jednoczesnego zauważenia obecności intruza w zakazanym miejscu oraz ucieczki osadzonego, przy równoczesnym wykonywaniu innych zadań służbowych. Pozostali, nawet gdyby zauważyli obecność niepowołanej osoby, to nie dostrzegliby zniknięcia osoby z pola widzenia. Również funkcjonariusze wyższego szczebla piastujący kierownicze i nadzorcze stanowiska nie wykazują się wyższym poziomem zdolności percepcyjnych. Ich spostrzegawczość dotyczy wyłącznie sytuacji wychwytywania braku osób w polu obserwacji.

Nie każdy funkcjonariusz nadaje się do pracy operatora „monitorowego", ponieważ nie każdy jest w stanie zaobserwować zdarzenia wymagające reakcji z jego strony, co jest zbieżne z doniesieniami w literaturze przedmiotu o tzw. ślepocie z braku uwagi.

W konkluzji autorzy dochodzą do wniosku, że w dalszej części badań należy skupić się na poszukiwaniu narzędzi selekcji (zarówno w postaci testów psychologicznych, jak i materiałów wizualnych), doskonaleniu procedur rekrutacji i szkolenia, optymalizowaniu ergonomii stanowiska do monitoringu wizyjnego oraz poszukiwaniu technologii informatycznych wspierających operatora „monitorowego" (np. inteligentna analiza obrazu, wzbudzanie czujności obserwatora, automatyczne sygnalizowanie zdarzeń krytycznych)[7].

W części drugiej artykułu zostaną zaprezentowane technologie informatyczne wspierające operatora systemu monitoringu, ilustrowane przykładami z badania dotyczącego zastosowania inteligentnej analizy wizyjnej w COSSW w Kaliszu.



NIE KAŻDY FUNKCJONARIUSZ NADAJE SIĘ DO PRACY OPERATORA „MONITOROWEGO", PONIEWAŻ NIE KAŻDY JEST W STANIE ZAOBSERWOWAĆ ZDARZENIA WYMAGAJĄCE REAKCJI Z JEGO STRONY, CO JEST ZBIEŻNE Z DONIESIENIAMI W LITERATURZE PRZEDMIOTU O TZW. ŚLEPOCIE Z BRAKU UWAGI

MGR INŻ. CEZARY MECWALDOWSKI

Starszy wykładowca zajmujący się szkoleniami zawodowymi i specjalistycznymi z zakresu zabezpieczeń elektronicznych, urządzeń do kontroli. Projektant z praktyką zagraniczną. Absolwent Politechniki Łódzkiej o specjalizacjach: energetyka przemysłowa i informatyka stosowana. Wykładowca Centralnego Ośrodka Szkolenia Służby Więziennej oraz Ośrodka Szkolenia Polskiej Izby Systemów Alarmowych

DR ROBERT POKLEK

Psycholog, adiunkt na Wydziale Pedagogiczno-Artystycznym w Kaliszu Uniwersytetu im. Adama Mickiewicza w Poznaniu. Członek Polskiego Towarzystwa Zapobiegania Samobójstwom

4 Badanie polega na prezentacji przez 30 s filmu z 6 graczami podającymi sobie piłki (3 osoby w białych i 3 osoby w czarnych koszulkach). Zadaniem obserwatorów jest policzyć, ile było podań osób w białych koszulkach. W trakcie ekspozycji po ok. 20 s na środek planu wychodzi człowiek przebrany za goryla, a w tym czasie jedna osoba w czarnej koszulce wychodzi z kadru. Jednocześnie następuje zmiana koloru kurtyny stanowiącej tło. Badanie odpowiada na pytania: 1) Ile osób prawidłowo wykona zadanie – policzy podania? 2) Ile osób zauważy wtargnięcie intruza w pole obserwacji i zniknięcie z pola widzenia jednej osoby oraz zmianę warunków obserwacji?

5 Ch. Chabris, D. Simons, *Niewidzialny goryl. Dlaczego intuicja nas zawodzi?*, Wyd. Laurum, Warszawa 2011.

6 Materiał filmowy dostępny w sieci https://www.youtube.com/watch?v=I-GQmdoK_D.J. Simons, C.F. Chabris, ZfY [dostęp: 26.09.2017].

7 R. Poklek, C. Mecwaldowski, *Video surveillance of prisoners in Polish Prison Service. Observer's perspective*, „Journal of Humanities and Social Science", (February 2018),Volume 23, Issue 2, Ver. 3, s. 41.

Synology spełnia potrzeby

celulozowni i papierni w Archangielsku

Archangielska celulozownia i papiernia (Archangelsk PPM) jest jednym z wiodących europejskich przedsiębiorstw przetwórstwa chemicznego drewna. To największy producent tektury falistej i jeden z liderów w produkcji celulozy w Rosji.

ZADANIE

Do roku 2014 dozór wizyjny w zakładzie powierzano wykonawcy, który był odpowiedzialny za konfigurację urządzeń, modernizację i serwis. W przedsiębiorstwie brakowało przejrzystej struktury i możliwości skalowania systemu. Zostały zakupione i zainstalowane kamery i rejestratory różnych producentów. W rezultacie zakład wyposażono w zestaw urządzeń różnych marek, które nie mogły zapewnić stabilnej pracy systemu jako całości, sprawiając przy tym trudności w konserwacji.
Jednocześnie istniejący system dozoru wizyjnego nie był wyposażony w narzędzia do szczegółowego monitorowania zasobów i nie gwarantował bezpieczeństwa archiwum wideo. Wyzwaniem stojącym przed przedsiębiorstwem była wymiana dotychczasowych urządzeń do rejestracji obrazu i kamer monitoringu wizyjnego.

DECYZJA

Dział IT zakładu, bazując na dotychczasowych doświadczeniach w użytkowaniu urządzeń oraz dobrej współpracy z działem wsparcia technicznego firmy Synology, złożył ofertę na nowy sprzęt w celu sprawdzenia jego możliwości jako systemu rejestracji i monitoringu wizyjnego w trybie testowym. Pozytywne wyniki testów pozwoliły działowi IT zakładu opracować i wdrożyć system rejestracji spełniający wszystkie wymagania. Podstawą obecnego systemu monitoringu wizyjnego jest zakupiony przez firmę kilka lat temu serwer RS10613xs+, który służy do przechowywania materiału wideo z 90 kamer. Kamery są połączone w sieć z wieloma urządzeniami VisualStation VS360HD, które są w polu widzenia dyspozytorów oraz operatorów i umożliwiają jednoczesne oglądanie materiału wizyjnego w czasie rzeczywistym. W razie potrzeby możliwe jest przeglądanie zapisów z archiwum nawet po kilku miesiącach.
W roku 2016 zakupiono trzy kolejne serwery RS18016xs+ umożliwiające skalowanie (rozbudowę) systemu monitoringu wizyjnego, a w 2017 r. trzy kolejne RS3617xs+ i sześć modułów rozszerzających RX1217RP. Wszystkie urządzenia są używane wyłącznie na potrzeby systemów dozoru wizyjnego i telewizji przemysłowej, testowane są też inne funkcje już zakupionych produktów firmy Synology. Obecnie zainstalowano ponad 500 kamer.
System monitoringu wizyjnego służy do monitorowania procesów produkcyjnych i działa w następujący sposób. Sygnał z około 90 kamer zainstalowanych w różnych warsztatach produkcyjnych przesyłany jest do serwerów RS3617xs+ i RS18016xs+, a następnie dystrybuowany do VisualStation VS960HD, VS360HD. Dostęp do obrazów z kamer jest ograniczony prawami użytkownika, tj. dyspozytor jednego warsztatu ma dostęp do kamer zainstalowanych tylko w swoim warsztacie. Na terenie przedsiębiorstwa istnieje sześć takich systemów.

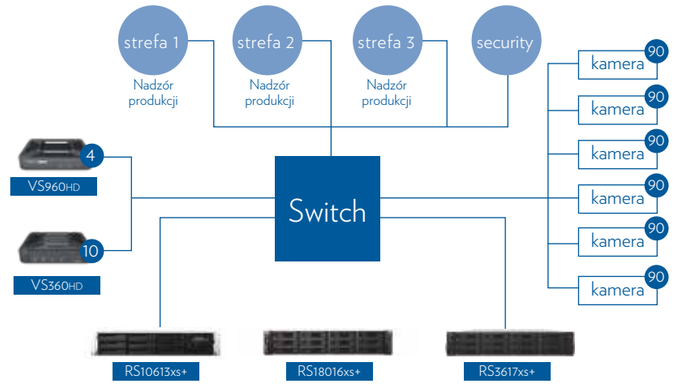
KORZYŚCI

- **Rzetelność i niezawodność archiwum**
  W wyniku wymiany sprzętu firma otrzymała niezawodne i odporne na uszkodzenia rozwiązanie do przechowywania dużej ilości materiału wideo.
- **Łatwa konfiguracja i zarządzanie dzięki dostępowi z przeglądarki**
  Aplikacja Surveillance Station umożliwia scentralizowane zarządzanie wszystkimi kamerami i serwerami, również z poziomu przeglądarki, znacznie upraszczając administrowanie systemem.
- **Obsługa kamer różnych producentów w ramach tego samego systemu dozoru wizyjnego**
  Wcześniej były to rozwiązania różnych producentów, wymagające ciągłego monitorowania wersji i wszechstronnej kompatybilności, dziś obrazy ze wszystkich kamer zakładu są przesyłane na serwery Synology za pomocą Surveillance Station.

W razie dodatkowych pytań czy chęci bezpłatnego przetestowania rozwiązań Synology zapraszamy do kontaktu: pl_sales@synology.com

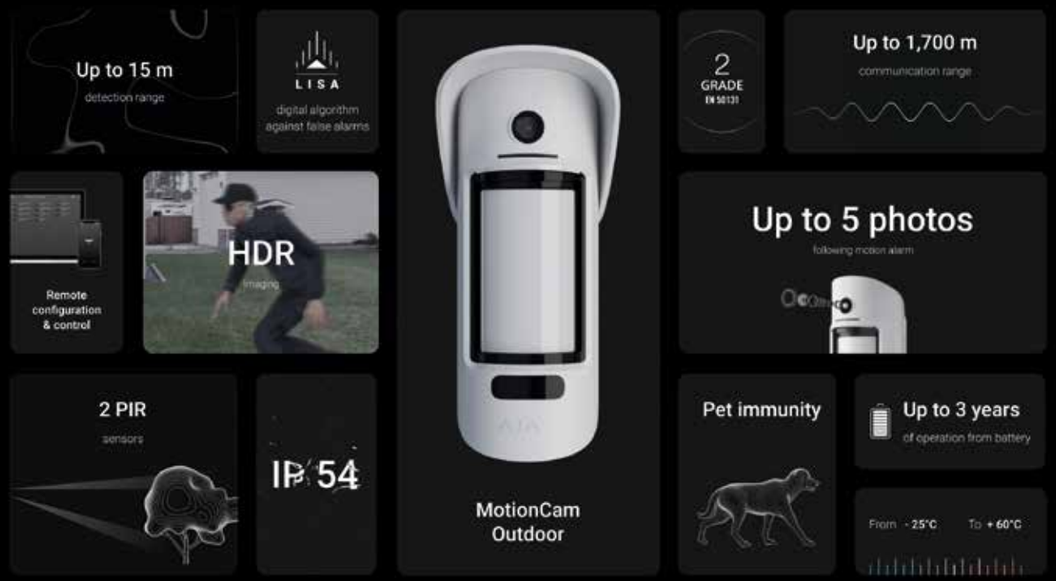
SYNOLOGY

**Grafenberger Allee 295,
40237 Düsseldorf, Niemcy
www.synology.com/pl-pl/**



MotionCam Outdoor:

weryfikacja fotograficzna nie tylko na posesji



MotionCam Outdoor firmy Ajax Systems, nowa bezprzewodowa czujka ruchu z wbudowanym aparatem fotograficznym, zapewnia spokój właścicielowi i ogranicza liczbę niepotrzebnych interwencji patrolu. Natychmiastowe i niezawodne wykrywanie intruzów, bardzo niskie zużycie energii, wyraźne zdjęcia o każdej porze dnia i nocy, przy każdej pogodzie – wszystko, by zapewnić profesjonalną ochronę terenu.

TECHNOLOGIA ZAPOBIEGAJĄCA FAŁSZYWYM ALARMOM

Detektor MotionCam Outdoor jest wyposażony w system dwóch sensorów na podczerwień, które, dzięki algorytmowi programowemu LISA, wykrywają ruch człowieka z wysoką dokładnością na odległość do 15 metrów. LISA przeprowadza analizę korelacyjną i spektralną sygnału, dzięki czemu czujka natychmiast odróżnia prawdziwe zagrożenia od zakłóceń.
Gdy intruz wejdzie na twój teren, system natychmiast uruchomi alarm. W zależności od ustawień system po uruchomieniu alarmu wykonuje serię od 2 do 5 zdjęć. Weryfikacja fotograficzna jest wyświetlana w aplikacjach mobilnych Ajax użytkowników mających odpowiednie uprawnienia.

Fot. Ajax potrzebuje zaledwie 9 sekund od wykrycia ruchu do wyświetlenia pierwszego zdjęcia na twoim smartfonie

Zespół Ajax opracował wyspecjalizowaną kamerę, dzięki której zdjęcia są wyraźne i czytelne nawet w trudnych warunkach oświetleniowych. Szerokokątny obiektyw w metalowej obudowie ze szklaną optyką zapewnia wyraźne zdjęcia pod kątem 50°. W jasnym świetle automatycznie uruchamia się filtr podczerwieni, a w ciemności włącza się mocne podświetlenie podczerwone. Dzięki temu zdjęcia są wyraźne, z właściwym odwzorowaniem kolorów i bez zniekształconych brzegów.

MotionCam Outdoor robi zdjęcia w jakości HDR. Mówiąc prościej, aparat wykonuje dwa kolejne zdjęcia o krótkim i długim czasie ekspozycji. Procesor natychmiast łączy te ujęcia, wyrównuje jaśniejsze i ciemniejsze obszary, a następnie kompresuje obraz, aby zapewnić najszybsze możliwe przesyłanie za pośrednictwem protokołu Wings.

Wings to szyfrowany protokół radiowy opracowany przez Ajax Systems. Dzięki komunikacji z hubem na odległość do 1700 m Wings obsługuje do 200 czujek MotionCam w systemie, a to wszystko bez wymaganego połączenia Wi-Fi lub podłączonego zasilania.

NARZĘDZIE GODNE PROFESJONALISTY

MotionCam Outdoor to prawdziwy skarb dla instalatorów i firm monitorujących. Aby dodać czujkę do systemu, wystarczy zeskanować kod QR przy użyciu aplikacji Ajax, nazwać ją i przypisać jej miejsce na posesji. Inżynier może z łatwością zamontować czujkę za pomocą klamry SmartBracket i skonfigurować ją w aplikacji, wykonując testy obszaru wykrywania i siły sygnału bez demontowania obudowy. W razie konieczności MotionCam Outdoor można tymczasowo wyłączyć lub zmienić ustawienia systemu bez wizyty na miejscu.

Monitorowanie alarmów z MotionCam Outdoor to proces, który nie wymaga dużego doświadczenia. Dzięki funkcjonalnej aplikacji Ajax PRO Desktop operatorzy w centrach monitorowania mają zapewnione najlepsze doświadczenia użytkownika. Weryfikacja fotograficzna, szczegółowe dzienniki, plany posesji i trasy, patrole interwencyjne — wszystko jest dostępne za jednym kliknięciem.

Weryfikacja fotograficzna jest dostępna również dla stacji monitorowania, niezależnie od używanego oprogramowania. Zintegrowaliśmy fotograficzną weryfikację alarmów z ponad tuzinem aplikacji monitorujących, w tym Manitou, SBN, Patriot i Mastermind. Lista ta ciągle się powiększa.

GRUNT TO NIEZAWODNOŚĆ

MotionCam Outdoor to profesjonalny detektor stopnia 2. Zaawansowany system antymaskingu reaguje na zasłonięcie obudowy i zamalowanie soczewki. Element wykrywający manipulacje natychmiast powiadomi o otwarciu obudowy lub demontażu czujki z klamry SmartBracket. Krótkie interwały ping pomagają wykryć utratę łączności z hubem szybciej niż w minutę, nawet jeśli system alarmowy jest rozbrojony.

Elektronika czujki jest przygotowana na nagłe zmiany temperatury, a specjalny daszek w obudowie chroni czujniki maskingu przed deszczem i śniegiem. Mimo wbudowanego aparatu i dwóch czujników na podczerwień MotionCam Outdoor może pracować do 3 lat na zainstalowanej baterii. Autonomia w połączeniu z obudową odporną na warunki atmosferyczne i zasięgiem komunikacji do 1700 m od huba sprawiają, że MotionCam Outdoor ochroni nawet najodleglejsze zakątki terenu.

SECUR GLOBAL

tel.: +48 577 311 618
biuro@securglobal.pl
https://ajax.systems/pl/

Innowacja w systemach

sygnalizacji włamania i kontroli dostępu

Projekty budynków charakteryzują się różną architekturą, wielkością czy złożonością. Dlatego do zabezpieczenia tak zróżnicowanych realizacji potrzebny jest modułowy, a zarazem estetyczny system bezpieczeństwa.

Nowoczesne systemy alarmowe to instalacje, które spełniają oczekiwania użytkowników teraźniejsze i przyszłe. Dzięki możliwości wygodnego rozbudowywania, bez konieczności wymiany sprzętu a jedynie poprzez zmianę licencji, łatwo można dopasować zakresu funkcji do zmieniających się potrzeb. Dodać można takie funkcje, jak redundancja, klastry lub określone integracje.
System alarmowy, z uwagi na technologię łączenia urządzeń, może występować jako: przewodowy, bezprzewodowy lub hybrydowy.

SKALOWALNOŚĆ I INTEGRACJA

Skalowalność systemu pozwala na wykorzystanie go w dużych projektach. Istniejący sprzęt można również łatwo rozbudować, gdy zaistnieje potrzeba dostosowania do przyszłych wymagań. Taka możliwość niweluje konieczność ponoszenia kosztownych inwestycji w sprzęt i robociznę w przyszłości, jeśli pojawi się konieczność rozszerzenia instalacji.

Rozwiązanie doskonale nadaje się do integracji z innymi systemami, takimi jak Security Management System (SMS), Building Management System (BMS) lub systemami automatyki budynkowej, np. KNX lub Crestron. Dostępne API umożliwia integrację z innymi systemami oraz wymianę informacji z systemu bezpieczeństwa. Bezpieczeństwo transmisji danych zapewniają połączenia szyfrowane.

REDUNDANCJA

Gwarancja nieprzerwanego działania systemu ma kluczowe znaczenie w rozwiązaniach stosowanych zwłaszcza w miejscach wysokiego ryzyka. Wyjątkowość rozwiązania polega właśnie na możliwości zastosowania instalacji redundantnej. Zazwyczaj system bezpieczeństwa zawodzi całkowicie w przypadku nieprawidłowego działania centrali. Natomiast dzięki redundantnej budowie systemu sygnalizacji włamania i napadu ochrona obiektu jest kontynuowana nawet w przypadku przerwania kabla lub awarii panelu sterowania. Instalacja działa również podczas konserwacji.

KLAWIATURA

Prosta konstrukcja manipulatora sprawia, że jego obsługa jest intuicyjna. Istotne, żeby manipulator w wersji z wbudowanym czytnikiem kart był wyposażony w jedną z najbezpieczniejszych technologii szyfrowania DESFire EV2. Unikalne zakodowane tagi lub karty dostępu gwarantują, że nie można ich skopiować, a przy tym spełniają zasadę bezpiecznego odczytu. Ponadto stosowana zasada czworga oczu umożliwia uzbrajanie/rozbrajanie systemu tylko wtedy, gdy dwie osoby wykonują tę czynność niezależnie. Stanowi to dodatkowe zabezpieczenie, które może być np. niezbędne do ochrony obszarów, w których przechowywane są towary o wysokiej wartości.
Ciekawą cechą manipulatora jest funkcja dopasowania języka klawiatury do użytkownika, który po przyłożeniu karty aktywuje system.

UNii – BEZPIECZNE ROZWIĄZANIE NA LATA

Jaki system sygnalizacji włamania i napadu potrafi spełnić wszystkie powyższe założenia? To UNii, opracowywany i produkowany przez holenderską firmę Alphatronics, która od dziesięcioleci specjalizuje się w tworzeniu systemów zabezpieczeń. Rozwiązania są projektowane we współpracy z klientami i użytkownikami końcowymi, dzięki czemu idealnie dopasowują się do zmieniających się wymagań użytkownika. Bezpieczeństwo, wygoda dla użytkownika i prosta instalacja były podstawowymi wyznacznikami w trakcie opracowywania systemu UNii.

Nowa era

SCHRACK SECONET

Schrack Seconet jest austriacką firmą zajmującą się zaawansowanymi technologicznie systemami ochrony przeciwpożarowej, komunikacji szpitalnej i bezpieczeństwa. Jesteśmy jednym z największych i najbardziej znanych producentów tych rozwiązań na świecie.

Jesteśmy obecni w Polsce, Szwecji, Rosji, Turcji, Rumunii, Słowacji, Czechach, na Węgrzech a także w wielu krajach Europy Wschodniej i Środkowej oraz Azji i Afryki. W Austrii Schrack Seconet ma sześć oddziałów, z siedzibą główną w Wiedniu.
W ramach Grupy Securitas w Szwajcarii trzy międzynarodowe centra kompetencyjne zapewniają najlepszy możliwy postęp w rozwoju swoich dziedzin, a Schrack Seconet odpowiada za rozwój systemów sygnalizacji pożarowej i komunikacji. W ten sposób austriackie *know-how* przepływa do międzynarodowej współpracy i przyczynia się do zabezpieczania obiektów na całym świecie.

NASZE POCZĄTKI

Początki firmy sięgają okresu wielkiej rewolucji przemysłowej XIX wieku; wtedy na terenie dzisiejszej Austrii i Niemiec powstawały pierwsze zakłady produkujące urządzenia elektrotechniczne, stanowiąc podwaliny dzisiejszych koncernów zarówno w Europie, jak i w Stanach Zjednoczonych czy Japonii. Nazwa firmy wywodzi się od nazwiska pomysłodawcy, przedsiębiorcy i naukowca – Eduarda Schracka, który zapoczątkował badania i konstruował pierwsze urządzenia radiotechniczne będące pierwowzorami dzisiejszych systemów sygnalizacji pożarowej.
Zakrojona na szeroką skalę produkcja prowadzona przez doktora Schracka w pierwszych latach XX wieku, po przerwie wywołanej zniszczeniami II wojny światowej jest kontynuowana do dziś. Już w latach 70. firma stworzyła jedną z pierwszych na świecie sterowanych mikroprocesorowo central sygnalizacji pożarowej, a w roku 1997 przystąpiła do jednego z największych koncernów w branży zabezpieczeń – Securitas AG, stanowiącego obecnie jedną z najważniejszych platform rozwoju branży bezpieczeństwa.

SCHRACK SECONET POLSKA

W 1998 r. powstała Schrack Seconet Polska Sp. z o.o., która zastąpiła działające od połowy lat 80. na rynku polskim przedstawicielstwo firmy austriackiej, stając się tym samym jedynym bezpośrednim reprezentantem producenta w naszym kraju. W trakcie trzydziestokilkuletniej działalności w Polsce firma zabezpieczyła ponad 10 tys. obiektów w całą gamę systemów ochrony przeciwpożarowej.

Najwyższą jakość i najwyższy poziom satysfakcji dla użytkowników systemów w Polsce gwarantuje doskonale rozwinięta w kraju sieć Autoryzowanych Partnerów. Należą do niej najlepsze w branży firmy mogące pochwalić się bogatym doświadczeniem oraz znakomitym przygotowaniem do świadczenia usług naszym klientom. Kwalifikacje potwierdzane są odpowiednimi certyfikatami uzyskanymi po odbyciu szeregu szkoleń zarówno w Polsce, jak i w naszym centrum szkoleniowym w Wiedniu. Najwyższą wartością dla Schrack Seconet jest jakość świadczonych usług w połączeniu z najlepszą wartością użytkową i niezawodnością produktów.

NOWA ERA! TU I TERAZ

Rok 2020 był dla większości firm na całym świecie niezwykłym wyzwaniem. Musieliśmy mierzyć się nie tylko z nieprzewidywalną pandemią, ale przede wszystkim z jej skutkami. Firma Schrack Seconet Polska dzięki niezawodnym rozwiązaniom, ciężkiej pracy zespołowej, przemyślanym działaniom sprzedażowym i marketingowym dokonała po raz kolejny niemożliwego – osiągnęła najlepsze wyniki sprzedaży i przeszkoliła kolejnych kilkaset wykwalifikowanych specjalistów. Od maja 2020 r. pod nowymi sterami doświadczanego kolegi z zespołu, ale już w roli Prezesa Zarządu, zaczęliśmy się przygotowywać do kolejnych zmian, jakie przyniósł rok 2021. I ten proces także przebiegł doskonale!

W Schrack Seconet rozpoczęła się nowa era! Zapoczątkowała ją kompleksowa zmiana wizerunku firmy. Nadszedł czas, aby skoncentrować działania na TU i TERAZ. Efektem szczegółowej analizy wizerunku marki Schrack Seconet jest nowy projekt logo, który podkreśla cyfrowy kierunek rozwoju firmy. Prosto, nowocześnie, bez zbędnej ekstrawagancji i z najważniejszym dla nas elementem ludzkim.

Proces rebrandingu firmy rozpoczął się w czerwcu. Sukcesywnie wprowadzamy zmiany w bardzo obszernej dokumentacji produktowej oraz we wszystkich materiałach marketingowych. W lipcu została także uruchomiona nowa międzynarodowa strona internetowa uwzględniająca potrzeby i oczekiwania rynku polskiego, z zachowaniem m.in. strefy logowania dla autoryzowanych firm oraz strefy dla projektantów. Na stronie będzie można zapoznać się z polityką sprzedaży Schrack Seconet w Polsce, zasadach certyfikacji oraz listą firm autoryzowanych reprezentujących nas na rynku.

WKRACZAMY W PRZYSZŁOŚĆ NA SOLIDNYCH PODSTAWACH

W dziedzinie ochrony przeciwpożarowej już teraz wprowadzamy na rynek nasz pionierski, udoskonalony system sygnalizacji pożarowej Integral EvoxX i wkraczamy w cyfrową przyszłość ściśle związaną z rozwiązaniami chmurowymi. W lipcu zakończy się cykl szkoleń aktualizacyjnych. Wszystkie firmy partnerskie, a tym samym ponad ośmiuset wykwalifikowanych specjalistów otrzyma nowe certyfikaty potwierdzające ich kompetencje w obszarze systemów sygnalizacji pożarowej Schrack Seconet, z uwzględnieniem najnowszego rozwiązania Integral EvoxX.

W zespole Schrack Seconet Polska stale pracujemy nad udoskonalaniem certyfikowanego systemu zarządzania bezpieczeństwem pożarowym SIS-Fire, by zapewnić jeszcze większe bezpieczeństwo oraz zarządzanie dużymi i skomplikowanymi technologicznie obiektami. Wiele miesięcy temu rozpoczęliśmy także prace nad rozwiązaniami dotyczącymi sterowania urządzeniami przeciwpożarowymi i ich zasilania. O najnowszych produktach z tego obszaru będziemy mogli opowiedzieć Państwu w kolejnych wydaniach a&s Polska.

Mamy również świetne wiadomości z sektora opieki zdrowotnej. Firma CCS Care Communication Solutions GmbH z siedzibą w Wiedniu jest teraz częścią rodziny Schrack Seconet i działa na rynku międzynarodowym pod nazwą Schrack Seconet Care Communication. Dążymy do tego, aby stać się w tej dziedzinie liderem na arenie międzynarodowej.

„CHRONIMY ŻYCIE. ZABEZPIECZAMY WARTOŚCI” – WSZELKIE NASZE DZIAŁANIA W KAŻDYM OBSZARZE SĄ UKIERUNKOWANE NA OSIĄGNIĘCIE TEGO CELU. NIE PRZESTAJEMY PRACOWAĆ NAD INNOWACJAMI I NOWYMI ROZWIĄZANIAMI, ABY DZIEŃ PO DNIU DOTRZYMYWAĆ TEJ OBIETNICY

Pozostaje wszystko co najlepsze. Co się zatem zmienia dla Państwa? Teraz możemy zaoferować jeszcze szersze portfolio oraz jeszcze więcej kompetencji, by spełnić wszystkie wymagania klientów. I to jest jedyna rzecz, która się zmienia. Tak jak do tej pory mogą Państwo liczyć na naszą wiarygodność i usługi najwyższej jakości.

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

Trendy w kontroli dostępu w 2021 r.

System kontroli dostępu ma umożliwiać dostęp do chronionego budynku, biura czy pomieszczenia tylko osobom uprawnionym. W świecie zagrożonym kolejnymi falami pandemii może spełniać też inne zadania niż tylko z zakresu zabezpieczeń i oferować nowe możliwości, np. związane z ograniczeniami sanitarnymi. Przedstawiamy trendy technologiczne w kontroli dostępu w roku 2021, które, wg analityków portalu asmag.com, nadal będzie kreować pandemia.

a&s International

MONITOROWANIE ZAJĘTOŚCI PRZESTRZENI

Użytkownicy inteligentnych budynków biurowych coraz częściej korzystają z rozwiązań dotyczących monitorowania zajętości wynajmowanej przestrzeni oraz analizują wykorzystanie swojej przestrzeni przez personel i pracowników. Według raportu Memoori szacuje się, że do 2024 r. rynek analiz obłożenia osiągnie 5,73 mld USD, co oznacza wzrost CAGR na poziomie 21,5 proc.

Zastosowanie funkcji kontroli zajętości przestrzeni w systemach KD po pandemii przyspieszy, już teraz użytkownicy korzystają z analiz do monitorowania przemieszczania się osób przy konieczności zachowania dystansu społecznego. Technologie sztucznej inteligencji i uczenia maszynowego (AI/ML) dostarczające danych z systemu KD będą wspierać działania właścicieli budynków w tym zakresie. Potrzeba zapewnienia środowiska pracy wolnego od wirusów podczas powrotu do biur po COVID-19, a także wymogi dotyczące utrzymania dystansu społecznego zwiększyły zainteresowanie bardziej wyrafinowanymi metodami zarządzania obłożeniem przestrzeni i jej kontroli.

Innym powodem, dla którego warto korzystać z takich analiz, jest postępująca konsolidacja przestrzeni. Wiele firm w trakcie pandemii utrzymywało puste biura, nadal za nie płacąc. Wnioski z analiz przełożą się na podjęcie lepszych decyzji, np. które części budynku należy zredukować, wydzierżawić lub zamknąć.

CORAZ WIĘKSZE ZATARCIE RÓŻNIC POMIĘDZY KD, BMS I VMS

W najbliższej perspektywie zapotrzebowanie na dobrze zintegrowany system kontroli dostępu będzie się utrzymywać. Nie jest to już tylko integracja z innymi systemami zabezpieczeń, np. monitoringu wizyjnego czy sygnalizacji włamania, ale raczej złożona integracja technologii KD z systemami zarządzania budynkiem (BMS), zarządzania gośćmi (VMS) i innymi zasobami przedsiębiorstwa, wspierająca bezkontaktową obsługę i automatyzację – wszystko, co w trakcie pandemii jest potrzebne bardziej niż kiedykolwiek.

Systemy kontroli dostępu są idealną płaszczyzną do integracji z systemami zarządzania wizytami, automatyki budynkowej, wydajnością pracowników czy zaangażowaniem klienta. W przypadku VMS odwiedzający jest zawsze gościem konkretnego pracownika firmy, którego dane są już w bazie danych systemu KD. Można więc łatwo i naturalnie zintegrować dane gości z aktualną bazą KD.

To samo dotyczy automatyki budynkowej; większość z tego, czym zarządza, dotyczy tworzenia wygodnego i bezpiecznego środowiska dla przebywających w obiekcie. W systemie KD są informacje, kim są osoby przebywające w budynku, gdzie się aktualnie znajdują i kiedy mogą tam przebywać. Dzięki tym danym można dostosować panujące warunki do preferencji osób tam pracujących. Zacieranie różnic między systemami KD, BMS czy VMS będzie postępowało.

ZGODNOŚĆ Z PRZEPISAMI

Technologia i rozwiązania kontroli dostępu muszą być projektowane i budowane tak, aby spełniały potrzeby użytkowników w zakresie zgodności z przepisami, które będą dominować w erze po pandemii. Dla przykładu, systemy zarządzania gośćmi mają wbudowane funkcje śledzenia kontaktów. Jeśli później okaże się, że gość został zarażony, wszystkie osoby, z którymi miał kontakt, mogą zostać odnalezione i poproszone o podjęcie środków zapobiegawczych, np. przejścia na kwarantannę.

Przewiduje się, że pojawi się znacznie więcej wymagań dotyczących zgodności z przepisami. Na przykład wymóg, aby gość lub wykonawca wchodzący na teren obiektu był zaszczepiony lub miał zaświadczenia, że nie miał kontaktu z osobą zakażoną. Według analityków w trakcie i po pandemii bardziej niż o samą pandemię będzie chodziło o zgodność z przepisami.

MOBILNA KONTROLA DOSTĘPU

Uwierzytelnianie mobilne, w którego ramach użytkownik używa swojego urządzenia mobilnego do otwierania drzwi, stało się modną technologią kontroli dostępu. Niedawne badanie przeprowadzone przez HID Global pokazuje, że korzystanie z dostępu mobilnego nadal rośnie – aż 25% organizacji wdrożyło tę technologię w całości lub częściowo. Ponieważ karty dostępu można ukraść, łatwo zgubić, a ich wykonanie jest droższe, korzystanie z urządzenia mobilnego ma uzasadnienie, np. w biurach czy dużych kampusach, gdzie masowe wydawanie kart jest kosztowne.

COVID-19 spowodował wzrost zapotrzebowania na bezdotykową kontrolę dostępu, a technologia mobilna wpisuje się w ten trend. W czasach przed pandemią standardową praktyką kontroli dostępu dla zewnętrznych wykonawców i gości było kierowanie ich do recepcji w celu osobistego poświadczenia prawa do wejścia. Gdy pandemia się rozprzestrzeniła, a organizacje starały się ograniczyć pracownikom ryzyko zakażenia się wirusem, chętniej korzystano z możliwości identyfikacji mobilnej.

BEZKONTAKTOWA BIOMETRIA

Najpopularniejszą biometryczną metodą autoryzacji stosowaną w systemach kontroli dostępu jest nadal identyfikacja za pomocą odcisku palca. Ma ona pewne wady, np. spowalnia przepustowość, a jako metoda dotykowa stanowi w dobie pandemii zagrożenie sanitarne. Dlatego obecnie biometria bezkontaktowa, zyskując na popularności, ma duże szanse stać się wyraźnym trendem. W przyszłości rynek będzie wymagać systemów bezdotykowych. Dodajmy, że „bezkontaktowa kontrola dostępu" była w 2020 r. jedną z fraz najczęściej wyszukiwanych w Internecie. Rynek zbliżeniowej kontroli dostępu nie rozwinął się nagle, ale z powodu pandemii akceptacja tej technologii znacznie przyspieszyła. Wielu nowych dostawców weszło w tę przestrzeń z powodu podaży i popytu.

Ta technologia doskonale sprawdza się w systemach zarządzania gośćmi. Bezkontaktowe zarządzanie nie wymaga interakcji między osobami w całym procesie składania wniosku o wizytę, samodzielnej odprawy i wejścia. Ta sekwencja jest w rzeczywistości bardzo podobna do tej, która jest wymagana w „bezdotykowym" systemie kontroli dostępu, w którym wszystko odbywa się drogą mobilną, najchętniej online. Użytkownik lub odwiedzający mogą zarejestrować się online (np. za pomocą biometrii twarzy, zaakceptowanej z powodu pandemii metody identyfikacji), dostać potwierdzenie wizyty, a następnie uzyskać dostęp do przydzielonych obszarów za pomocą telefonu komórkowego.

Rozpoznawanie twarzy można teraz integrować z innymi technologiami, aby skuteczniej walczyć z COVID-19. Dostępne są czytniki rozpoznawania twarzy, które wykorzystując sztuczną inteligencję, mogą określić, czy dana osoba nosi maseczkę lub ma podwyższoną temperaturę, i nie przyznać jej dostępu do obiektu. Popyt w tych obszarach wzrośnie, ponieważ pandemia nadal jest dużym problemem na całym świecie.

KONTROLA DOSTĘPU W CHMURZE

Podobnie jak zainteresowanie dozorem wizyjnym jako usługą, rośnie też zainteresowanie usługą kontroli dostępu w chmurze (ACaaS). Oczekuje się, że COVID-19 przyspieszy ten trend ze względu na różne korzyści. Po pierwsze, w przeciwieństwie do lokalnych elektronicznych systemów kontroli dostępu, które wymagają serwerów, okablowania i opłat licencyjnych, ACaaS ma niższe koszty początkowe. Pobiera się tylko opłatę abonamentową uzależnioną od potrzeb użytkownika. Może to być atrakcyjne dla przedsiębiorców będących użytkownikami końcowymi, którzy ucierpieli finansowo w następstwie COVID-19.

Oszczędności przynoszą też dane hostowane centralnie w chmurze, a nie na urządzeniach lokalnych, dzięki czemu nie trzeba planować napraw i konserwacji, które wymagają wizyt na miejscu i mogą być sprzeczne z wytycznymi dotyczącymi pandemii. Dzięki chmurze pewne operacje, takie jak wydawanie i odwoływanie poświadczeń, mogą być wykonywane zdalnie. Pracownik nie musi przebywać w obiekcie, co jest ważne w przypadku pracy w trybie *home office.* Co istotne, KD w chmurze jest też mniej podatna na cyberzagrożenia.

CYBERBEZPIECZEŃSTWO A ZARZĄDZANIE TOŻSAMOŚCIĄ

Dominującym w 2021 r. trendem technologicznym w systemach kontroli dostępu jest cyberbezpieczeństwo. Napędzają go dwa czynniki. Po pierwsze, urządzenia elektronicznych systemów kontroli dostępu stają się coraz bardziej elementami online, podatnymi na włamania. Po drugie, teraz, gdy COVID-19 „wysłał" pracowników na całym świecie do pracy zdalnej, bezpieczny zdalny dostęp do zasobów przedsiębiorstwa stał się ważniejszy niż kiedykolwiek.

Rozwiązania, które zmienią przyszłość kontroli dostępu

Jakub Kozak

Regional Sales Manager ECE

Według amerykańskiego stowarzyszenia Security Industry Association[1] najbardziej godnymi uwagi megatrendami w zakresie zabezpieczeń w tym roku są: rozwiązania bezdotykowe (zbliżeniowe), rozpoznawanie twarzy oraz przejście na modele usługowe[2]. Poniżej przedstawiamy własne prognozy, które będą kształtować świat elektronicznych systemów kontroli dostępu w 2021 r. i później.

MIGRACJA DO CHMURY

Kontrola dostępu przenosi się do chmury. Jako usługa (ACaaS) sprawia, że wdrożenie i utrzymanie systemu KD klasy korporacyjnej jest łatwiejsze i tańsze. Umożliwia użytkownikom końcowym przyznanie lub ograniczenie dostępu ze scentralizowanej platformy w dowolnym momencie i z dowolnego miejsca za pośrednictwem urządzeń mobilnych lub Internetu.
Rozwiązanie ACaaS pozwala firmom skupić się na bezpieczeństwie pracowników, gości i zasobów, bez kłopotów związanych z konserwacją systemu. Wymaga znacznie mniej urządzeń, ogranicza czas i zaangażowanie działu IT. Ponadto do bezpiecznego łączenia się z chmurą dostawcy mogą wykorzystać istniejące już kontrolery, moduły czy zamki elektroniczne.

ZARZĄDZANIE TOŻSAMOŚCIĄ

Kontrola dostępu przekształciła się w coś więcej niż tylko nieprzyznawanie dostępu osobom nieuprawnionym, ale również podszywającym się pod cudzą tożsamość oszustom posługującym się nie swoją kartą. Dlatego coraz więcej firm zaczyna zarządzać tożsamościami, a nie tylko posiadaczami kart. Tożsamości to cyfrowe profile każdej osoby, która ma kontakt z organizacją. Profile te mogą zawierać wiele atrybutów: stanowisko w firmie, wynagrodzenie, staż pracy, kwalifikacje, akredytacje i inne.

Korzystając z systemu zarządzania tożsamością i dostępem, można automatycznie przypisywać uprawnienia pracownikom do budynków. Eliminuje to obciążenie zasobów zadaniami związanymi z żądaniem i przyznawaniem uprawnień, zapewniając jednocześnie spełnienie standardów zgodności.

UNIFIKACJA

Jest wiele ważnych elementów systemu zabezpieczeń – kontrola dostępu, dozór wizyjny, wykrywanie włamań – i wszystkie one powinny bezproblemowo ze sobą współpracować, zapewniając kompleksowe rozwiązanie. Wybierając nowoczesny system kontroli dostępu IP, rozsądnie byłoby zdecydować się na taki, który jest zunifikowany z innymi funkcjami systemu bezpieczeństwa.

Zintegrowany system przenosi komponenty rozwiązania zabezpieczającego poza zwykłe połączenie. Stanowi jedną platformę, która zarządza wszystkimi funkcjami dozoru wizyjnego i kontroli dostępu za pośrednictwem jednego interfejsu użytkownika. Maksymalizuje to wykorzystanie infrastruktury, zapewnia bezproblemowe aktualizacje i ujednolicone zarządzanie poziomem zagrożeń. Ponadto pracownikom łatwiej jest nauczyć się obsługi jednego systemu.

Moduł KD będący częścią platformy IP Gentec Security Center oferuje takie podejście. Jako system prawdziwie otwarty łączy się z dużą i wciąż rosnącą liczbą urządzeń KD innych firm. Bezproblemowo zintegrowany z systemami wizyjnymi i innymi systemami zabezpieczeń, zapewnia wgląd w operacje dotyczące chronionych obszarów organizacji, co prowadzi do bardziej świadomych decyzji i usprawnia funkcjonowanie organizacji.

BEZPIECZEŃSTWO CYBERNETYCZNE

Ataki na systemy KD zazwyczaj koncentrowały się na przełamaniu zewnętrznych zabezpieczeń, aby uzyskać nieuprawnione wejście do obiektu. Ponieważ nowoczesne systemy KD oparte na protokole IP są elementami sieci informatycznych, należy wdrożyć procesy, które zapewnią, że nie będą one stanowić drogi wejścia dla intruzów w celu uzyskania dostępu do obiektu.

Niestety użytkownicy końcowi często zapominają o ryzyku związanym ze słabą higieną cybernetyczną i skupiają się na „atrakcyjnych oszczędnościach" kosztów od dostawców, którzy nie zawsze dbają o ich interes lub dobro ich organizacji. Inwestorzy muszą zwracać się do dostawców oferujących ochronę przed cyberzagrożeniami, z kompleksową szyfrowaną komunikacją dla oprogramowania i urządzeń, bezpiecznym uwierzytelnianiem opartym na poświadczeniach i certyfikatach cyfrowych.

GENETEC

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

[1] www.securityindustry.org
[2] https://www.securityindustry.org/report/2021-security-megatrends-report/

Systemy kontroli dostępu dopasowane do potrzeb

System kontroli dostępu jest istotnym elementem zabezpieczenia każdego obiektu. Nie tylko nadzoruje wejście i steruje dostępem do budynku czy pomieszczenia, przyznając dostęp tylko osobom uprawnionym, ale także oferuje funkcje takie jak RCP, analiza ruchu osobowego w danym obszarze czy integracja z innymi systemami automatyki budynkowej. Aby wybrać rozwiązanie spełniające potrzeby organizacji, należy wziąć pod uwagę wymagania wszystkich interesariuszy. Innych funkcji będzie oczekiwał zarząd, innych security menedżerowie, a jeszcze innych pracownicy czy goście firmy. Na co przy wyborze systemu KD zwracają dziś uwagę klienci? Zapytaliśmy o to przedstawicieli firm oferujących tego typu rozwiązania na rynku polskim.

Obserwujemy przyspieszony rozwój technologiczny systemów KD, które pracują w środowisku IT (sieciowymi) ze wszystkimi tego konsekwencjami. Rozwój po części wynika z nowych potrzeb wywołanych koniecznością utrzymania wymogów sanitarnych w trakcie pandemii COVID-19 oraz zmianą trybu pracy ze stacjonarnego na zdalny.
Jedno jest pewne, aby sprawnie funkcjonować, firma musi dziś inwestować w nowoczesne technologie. – *Obecność elektronicznego systemu kontroli dostępu stała się w zasadzie obowiązkowym elementem wyposażenia budynków znajdujących się w fazie projektowania lub budowy i jest tylko kwestią czasu, kiedy jej działaniem zostaną objęte obiekty wcześniej zbudowane* – komentuje Łukasz Gliniecki z firmy Roger.

ŁATWE UŻYTKOWANIE

Użytkownicy systemów kontroli dostępu oczekują ułatwień oferowanych przez najnowsze technologie i aplikacje, z których korzystają już w codziennym życiu, przede wszystkim unifikacji rozwiązań związanych z nadawaniem uprawnień, przy jednoczesnym utrzymaniu wysokiego poziomu bezpieczeństwa. – *Według nas są trzy kluczowe elementy oceny sukcesu systemu kontroli dostępu: wygoda, wydajność i bezpieczeństwo. Łączne ich spełnienie oraz łatwość obsługi systemu czynią go bardziej atrakcyjnym dla kupującego. Wśród wiodących najnowocześniejszych technologii KD dużym zainteresowaniem cieszą się inteligentne karty (smart cards) i biometria* – zauważa Miguel Blanco z ZKTeco Europe.

Ważna jest prosta i wygodna obsługa systemu. Dominuje oprogramowanie obsługiwane z poziomu popularnych przeglądarek internetowych, bez konieczności instalacji na każdej stacji roboczej. Pandemia koronawirusa przyniosła znaczący wzrost zainteresowania bezdotykowymi systemami kontroli dostępu, opartymi m.in. na aplikacjach mobilnych, kodach QR czy biometrii, które wypierają popularne karty dostępu. – *Odejście od kart dostępu minimalizuje ryzyko wejścia do budynku lub danej strefy osoby, która w posiadanie takiej karty weszła w sposób nieuprawniony* – wyjaśnia Adam Brzezicki z Axis Communications.

Wymagania na systemy kontroli dostępu różnią się w zależności od rodzaju obiektu, w którym będą zainstalowane. Mogą mieć znaczenie różne elementy, ale liczą się przede wszystkim bezpieczeństwo i niezawodność danego rozwiązania. – *Niebagatelne znaczenie mają skalowalność i ochrona inwestycji, czyli z jednej strony to, że system KD może być rozbudowywany wraz z rozwojem przedsiębiorstwa, z drugiej, że jest zawsze na czasie, w zgodzie z aktualnymi wymogami i kompatybilny z nowymi systemami operacyjnymi i bazami danych* – podkreśla Rafał Tamborski z Dormakaba.

INTEGRACJA

Obecne trendy rynkowe związane z funkcjonalnością kontroli dostępu dotyczą głównie elastyczności w zakresie możliwości ich integracji z innymi systemami lub elementami wyposażenia budynku. – *Dotyczy to integracji zarówno z systemami CCTV, SSWIN, domofonowymi, jak i z systemami RCP, sterowania windami czy też automatyki budynkowej. Nowoczesny system musi mieć także możliwość obsługi czytników biometrycznych i wykorzystywania bezpiecznych uwierzytelnień mobilnych* – zauważa Beata Idziak z Assa Abloy.

Potrzebę integracji podkreśla również Łukasz Gliniecki z firmy Roger: *W sektorze biznesu klienci poszukują systemów o dużej zdolności do integracji z innymi, współistniejącymi w budynku systemami elektronicznymi. Powszechnie oczekuje się, że system KD obejmie również kontrolę dostępu do wind oraz parkingu. Coraz większym zainteresowaniem cieszy się w tej grupie odbiorców identyfikacja mobilna, która umożliwia wykorzystanie telefonu komórkowego do identyfikacji użytkowników systemu.*

ROZWIĄZANIA W CHMURZE

Skuteczność zarządzania tożsamością i uprawnieniami w chmurze ma kluczowe znaczenie dla utrzymania zakładanego poziomu bezpieczeństwa. W miarę zdobywania wiedzy o zaawansowanej funkcjonalności rozwiązań kontroli dostępu użytkownicy i administratorzy stawiają coraz większe wymagania swoim systemom. – *Wielu klientów wygodę kojarzy ze zdalnym dostępem do systemu z dowolnego miejsca. Ponieważ technologie mobilne wciąż się rozwijają, użytkownicy oczekują realizacji dostępu za pośrednictwem chmury z wykorzystaniem komputerów mobilnych lub smartfonów. Opcje te stają się coraz bardziej popularne, a zarządzanie systemami KD wygodniejsze* – wyjaśnia Miguel Blanco.

Rozwiązania w chmurze dają użytkownikom pewność działania systemu nawet w przypadku awarii urządzenia. – *Dostęp przez przeglądarkę to nie tylko komfort i wygoda, ale również bezpieczeństwo. Pliki konfiguracyjne nie są przechowywane na komputerze operatora (użytkownika programu), dzięki temu w przypadku awarii wystarczy uruchomić nowy komputer, skonfigurować połączenia sieciowe i zainstalować przeglądarkę* – podkreśla Maciej Nowak z firmy Satel.

Na aspekt finansowy wynikający z przeniesienia funkcji systemu kontroli dostępu do chmury wskazuje Jakub Sobek z firmy Linc Polska: *Dzięki temu, że system kontroli dostępu może pracować w chmurze, zespół IT poświęca znacznie mniej czasu na jego utrzymanie. Pozwala to zaoszczędzić godziny pracy, które mogą być wykorzystane w realizacji istotniejszych zadań. Kontrola dostępu oparta na chmurze korzysta z wiedzy ekspertów z tej dziedziny, którzy cały czas czuwają nad bezpieczeństwem systemu. Wszystkie aktualizacje są wykonywane automatycznie, bez angażowania pracowników IT.*

BEZPIECZEŃSTWO CYFROWE

Uwaga inwestorów kierowana jest na kwestie związane z tzw. higieną cyfrową najważniejszych elementów sieciowego systemu KD, takich jak kontrolery IP. Jak zauważa Adam Brzezicki: *Warto stawiać na certyfikowane*

urządzenia z rozbudowaną ochroną przed cyberatakiem, gdyż tylko takie mogą skutecznie zapobiegać nieautoryzowanemu dostępowi. Standardem w przypadku kontrolerów drzwi jest już funkcja tzw. bezpiecznego uruchamiania gwarantująca, że oprogramowanie danego urządzenia nie zostało zainfekowane, np. oprogramowaniem typu malware. Odpowiednie protokoły bezpieczeństwa pozwalają też wyłapywać ewentualne niepożądane ingerencje w ustawienia urządzenia.
Wielu inwestorów ma już świadomość zagrożeń związanych z niezabezpieczoną transmisją danych w całym systemie KD, rozumie wagę i konieczność zabezpieczeń przed atakami hakerów. *– Klienci oczekują szyfrowania komunikacji pomiędzy wszystkimi elementami systemu, od czytników po serwery, ale chcą również mieć dane uwierzytelniające lub karty kontroli dostępu, które zapewniają zarówno wysokie bezpieczeństwo, łatwość użytkowania, jak i efektywność kosztową. Z tej perspektywy widać tendencję do standaryzacji kart, która gwarantuje nie tylko wysoką jakość, ale także większą konkurencję pomiędzy dostawcami. To powoduje, że użytkownik końcowy ma szansę wybrać najlepsze dla siebie rozwiązanie* – podkreśla Jakub Kozak z firmy Genetec.

KOSZT SYSTEMU

Dla wielu inwestorów, zwłaszcza w branżach najbardziej dotkniętych skutkami pandemii, najczęstszymi kryteriami wyboru systemu kontroli dostępu jest jego cena. Trzeba jednak mieć świadomość tego, że *na koszt całości składa się zarówno koszt zakupu, instalacji, jak i późniejszej eksploatacji* – mówi Krzysztof Ratajczak z Winkhaus Polska. Wskazuje jednocześnie, że inwestorzy miewają problemy z określeniem swoich potrzeb, a zwłaszcza ich rozwoju w przyszłości. *– Wybór KD może determinować w dalszej przyszłości to, jak obiekt może być zarządzany i czy zostawimy sobie dużą elastyczność w tym zakresie* – dodaje.

RÓŻNE BRANŻE, WSPÓLNY MIANOWNIK

Każda branża ma swoje konkretne potrzeby. Nawet w ramach jednego sektora klienci mają zróżnicowane, specyficzne oczekiwania związane z organizacją danego przedsiębiorstwa, wewnętrznymi procedurami czy przepisami krajowymi. Jedna kwestia pozostaje niezmienna – wszyscy klienci doceniają możliwość określenia czasu dostępu danego użytkownika do wybranej strefy już na etapie tworzenia mu „konta" w systemie. Innym oczekiwaniem jest możliwość generowania raportów zawierających informacje o użytkownikach aktualnie przebywających w obiekcie. Ustalenie kto, kiedy i do jakiego pomieszczenia uzyskał dostęp *ma szczególne znaczenia w sytuacji zagrożenia i konieczności przeprowadzenia ewakuacji. Dzięki takim informacjom można szybko zweryfikować liczbę osób w danej strefie, jak również sprawdzić, gdzie aktualnie znajdują się konkretne osoby* – wskazuje Maciej Nowak.

Niezmiennie pojawia się potrzeba zapewnienia wymaganego poziomu bezpieczeństwa, optymalizacji funkcjonowania systemu i komfortu jego użytkowania. *– Optymalny poziom zabezpieczenia obiektu i wymiana danych pomiędzy elementami systemu KD i stworzenie zintegrowanego systemu bezpieczeństwa na miarę potrzeb daje oszczędności na wielu poziomach wykorzystywania i obsługi systemu, np. elastyczności w doborze opcji systemowych i poziomu zabezpieczenia wymiany danych, możliwości zdalnego monitoringu i zarządzania systemem czy optymalizacji oraz konsolidacji obsługi zintegrowanego systemu bezpieczeństwa obiektu* – ocenia Beata Idziak.

Wdrożenie systemu kontroli dostępu przynosi też wymierne oszczędności finansowe. W wielu obiektach można dzięki SKD zrezygnować z portierni wydającej klucze i wyeliminować problem zarządzania fizycznymi kluczami do poszczególnych pomieszczeń. *– Nakłady finansowe związane z implementacją systemu są niewielkie w stosunku do możliwości, jakie uzyskuje potencjalny użytkownik poprzez lepszą organizację, wygodniejsze administrowanie i optymalizację pracy* – podkreśla Krzysztof Ratajczak.

Decyzje o zakresie wdrożenia, modernizacji lub rozbudowy systemu KD podejmowane przez inwestora zależą m.in. od wielkości budżetu. Możliwość wykazania zwrotu z inwestycji stanowi kolejny argument przemawiający za zakupem. *– Bezdotykowe systemy biometryczne mogą dać oszczędności na wiele sposobów. Eliminują potrzebę wydawania lub wymiany kart i kluczy, co potencjalnie może być dużym wydatkiem. Inne kwestie dotyczące oszczędności kosztów są związane z czasem na weryfikację, jaki zyskują użytkownicy i administratorzy. Nie wspominając o ekonomicznych skutkach naruszenia bezpieczeństwa, kosztach utraty danych, weryfikacji integralności informacji, utracie wiarygodności marki i kosztach alternatywnych przyszłego biznesu. Systemy te umożliwiają także szybki proces adaptacji do przepisów rządowych dotyczących RODO* – wymienia Miguel Blanco.

Inne wymagania ma bank z wieloma oddziałami usytuowanymi w całym kraju, inne pojedynczy obiekt hotelowy. Obiekty bankowe, mając duży poziom ryzyka, wymagają wysokiego stopnia zabezpieczenia i zaawansowanych funkcji, natomiast hotele przede wszystkim dodawania użytkowników i udzielania im autoryzacji bardziej w celach organizacyjnych. *– Jeśli jest to system rozproszony i inwestor ma kilka, kilkanaście lub kilkadziesiąt obiektów do zarządzania, to przede wszystkim zwraca uwagę na to, by system był jednolity, gdyż powinien być zarządzany z centralnego miejsca. Częstym scenariuszem jest posiadanie lokalnych administratorów systemu KD, ale inwestorzy oczekują, aby ich system był elastyczny pod tym kątem* – mówi Karol Radzajewski z Hikvision Poland.

HOTELE

Dla branży hotelarskiej istotne są szybkość i łatwość udostępniania gościom dostępu do ich pokoi. *– To systemy kontroli dostępu oparte na technologii chmurowej pozwalają na łatwe aktywowanie dostępu do pokoju hotelowego aplikacją wprost na telefon gościa. Branża turystyczna to nie tylko hotele, to także wynajem apartamentów lub domów. Tutaj także zdalne przekazanie „kluczy" do obiektu jest olbrzymim ułatwieniem i profesjonalizuje całą usługę wynajmu* – wyjaśnia Jakub Sobek.

Od systemu kontroli dostępu w branży hotelarskiej oczekuje się obecnie również sterowania automatyką budynkową (oświetlenie, klimatyzacja, sygnalizacje usług hotelowych). *– Karta, często spersonalizowana, pełni też funkcję swoistej wizytówki hotelu. Coraz częściej pojawia się dostęp zdalny z uprawnieniami wysyłanymi na telefon gościa. Sieci hotelowe oferują już aplikacje mobilne, automatycznie prowadzące gości przez cały proces wynajmu pokoju. Ważna jest więc możliwość integracji z systemami PMS (Property Management System) oraz systemami automatyki w pokoju hotelowym* – podkreśla Rafał Tamborski.

Na inny aspekt wskazuje Łukasz Gliniecki: *Czynnikiem branym pod uwagę w hotelach jest estetyka urządzeń. Preferowane są urządzenia podtynkowe, ze szklanym panelem czołowym, trwałe, a zarazem eleganckie, dobrze komponujące się we wnętrzach nowoczesnych i tradycyjnych.*

SEKTOR FINANSOWY

Wymagania sektora finansowego dotyczą przede wszystkim zagwarantowania odpowiedniego poziomu bezpieczeństwa całego rozwiązania, mniej jego ergonomii. *– W sektorze finansowym ogromny nacisk kładzie się na zabezpieczenia na każdym możliwym kroku, począwszy od czytnika i technologii wykorzystywanych kart, komunikacji czytnika z kontrolerem, serwerem czy oprogramowania do zarządzania takim systemem* – zauważa Karol Radzajewski.

Dostęp do stref zamkniętych dla klientów mają tylko osoby upoważnione. *– Kontrola dostępu do specjalnych stref może wymagać dodatkowej autoryzacji, np. kartą RFID i kodem PIN, weryfikacją biometryczną czy nawet dodatkowych urządzeń fizycznej kontroli dostępu, takich jak śluza osobowa z wbudowaną wagą. Szyfrowana komunikacja, najbezpieczniejsze technologie zbliżeniowe to standardowe wytyczne w tym sektorze* – wyjaśnia Rafał Tamborski.

Szczególną uwagę zwraca się na zapewnienie cyberbezpieczeństwa wdrażanych rozwiązań. *– Ważne jest zabezpieczenie każdego, pojedynczego elementu systemu. Pełne szyfrowanie przesyłanych danych, certyfikacja poszczególnych urządzeń podłączanych do sieci oraz ciągłe aktualizacje bezpieczeństwa to elementy niezbędne w sektorze finansowym* – dodaje Jakub Sobek.

Na aspekty cyberbezpieczeństwa i elastyczności systemu zwraca również uwagę Jakub Kozak: *Banki komercyjne mają zazwyczaj jeden duży budynek centrali, kilka większych biur regionalnych i setki mniejszych lokalizacji. Z punktu widzenia centrali może zajść potrzeba posiadania informacji, a czasem zarządzania małymi biurami regionalnymi, ale nie będzie to wymagane w drugą stronę. Małe biura nie potrzebują, a nawet nie powinny mieć dostępu do danych z systemu kontroli dostępu w centrali. Nowoczesny system KD powinien być na tyle elastyczny, aby umożliwić zbudowanie takiej hierarchicznej struktury systemu. Pamiętajmy również, że istnieją specjalne strefy banku, do których wymagane są wysoko zaawansowane funkcje kontroli dostępu. Dotyczy to dostępu zarówno fizycznego, jak i do jego zasobów sieciowych. Funkcje te powinny działać również w przypadku utraty dostępu do serwera, więc ryzyko, że system nie będzie działał poprawnie, jest niewielkie.*

W pierwszym kwartale 2021 r. liczba firm z branży turystycznej wykreślonych z rejestru KRS przekroczyła liczbę nowo powstałych. Z polskiego rynku turystycznego zniknęło bezpowrotnie blisko

80

FIRM,

działalność zawiesiło niemal

500

HOTELI I OBIEKTÓW NOCLEGOWYCH.

To

50%

więcej niż w analogicznym okresie poprzedniego roku

ASSA ABLOY

www.assaabloyopeningsolutions.pl

Incedo™ Business – elastyczny, skalowalny system KD

FIRMA ASSA ABLOY, GLOBALNY PRODUCENT SZEROKIEJ GAMY KOMPONENTÓW ZWIĄZANYCH Z KONTROLĄ DOSTĘPU, M.IN. CZYTNIKÓW HID, ZAMKÓW ELEKTRYCZNYCH I ELEKTROMOTORYCZNYCH, BEZPRZEWODOWYCH OKUĆ I ZAMKÓW APERIO, ELEKTRORYGLI, ZWÓR ELEKTROMAGNETYCZNYCH CZY SAMOZAMYKACZY, ZDECYDOWAŁA SIĘ NA WDROŻENIE NOWEJ PLATFORMY ZARZĄDZAJĄCEJ KONTROLĄ DOSTĘPU – INCEDOTM BUSINESS.

System został tak zaprojektowany, aby mógł zapewniać maksymalną użyteczność, elastyczność i przyjazną obsługę. Jest skalowalny, łatwo go rozbudować o nowe elementy, a przy tym szybki w instalacji. Dzięki modułowej platformie użytkownik w prosty sposób wybiera urządzenia zabezpieczające i technologię identyfikacji dostosowane do swoich wymagań oraz odpowiednią opcję systemu zarządzania. Przyjazny w obsłudze, intuicyjny interfejs użytkownika umożliwia sprawne zarządzanie dostępem do pomieszczeń praktycznie z każdego miejsca z poziomu dowolnej przeglądarki internetowej.

Platforma Incedo™ jest na tyle otwarta, że można dostosować się do najnowszych zmian technologicznych, łącząc bezpieczne punkty dostępu z inteligentnymi technologiami identyfikacji, np. uwierzytelnieniami mobilnymi *(mobile access)* i biometrycznymi. Ponadto umożliwia współpracę z innymi systemami zabezpieczeń, takimi jak telewizja dozorowa, sygnalizacja włamania, VSM czy interkomy, w celu stworzenia uniwersalnego, niezwodnego systemu zarządzania bezpieczeństwem obiektu.

W systemie Incedo™ Business przewidziano też możliwość integracji z innymi systemami w budynku, np. sterowanie windami, BMS, RCP czy moduły obsługi gości. Jest to istotne dla menedżerów budynku, którzy dzięki temu mają większą kontrolę i gwarancję bezpieczeństwa. Zyskają na tym także administratorzy systemów ze względu na większe możliwości operacyjne w ramach dostępnego budżetu – jeden skalowalny system pozwoli im zakładać, usuwać lub modyfikować profile dostępu oraz monitorować poruszanie się osób po budynku w czasie rzeczywistym. Dzięki takim funkcjom Incedo™ Business zrealizuje oczekiwania najbardziej wymagających użytkowników.

ROGER

www.roger.pl

Zapowiedź wdrożenia systemu KD RVOS

W NAJBLIŻSZYCH MIESIĄCACH DO OFERTY FIRMY ROGER BĘDĄ STOPNIOWO DODAWANE ELEMENTY NOWEGO SYSTEMU KONTROLI DOSTĘPU O NAZWIE RVOS. W ODRÓŻNIENIU OD OFEROWANEGO OD KILKU LAT SYSTEMU RACS 5, ZAAWANSOWANEGO FUNKCJONALNIE I PRZEZNACZONEGO DLA SEKTORA PROJEKTÓW KD, SYSTEM RVOS OFERUJE PODSTAWOWE, POWSZECHNIE OCZEKIWANE FUNKCJE KONTROLI DOSTĘPU WYMAGANE W POPULARNYCH INSTALACJACH KD.

RVOS jest systemem hybrydowym złożonym z urządzeń przewodowych i bezprzewodowych. W grupie urządzeń bezprzewodowych znajdują się zasilane bateryjnie zamki mechatroniczne serii VCL-2. Są one montowane na skrzydle drzwi i działają wg formuły offline, w której dane o uprawnieniach dostępu są zapisane na karcie dostępowej użytkownika systemu.

W skład grupy przewodowej wchodzą kontrolery dostępu typu VCT82, VC88 i VC6. Kontroler VCT82 jest montowany na ścianie i zasilany przewodowo, lecz podobnie jak zamek VCL-2 dostęp przyznaje na podstawie uprawnień zapisanych na karcie zbliżeniowej. VC88 oraz VC6 to kontrolery przewodowe online, które raportują zdarzenia w czasie rzeczywistym, a dostęp przyznają na podstawie danych znajdujących się w ich wewnętrznych bazach danych.

Kontroler VC6 obsługuje do sześciu przejść przewodowych i współpracuje z urządzeniami peryferyjnymi wykorzystywanymi w systemie RACS 5 (terminale serii MCT i ekspandery serii MCX).

Kontroler VC88 ma wbudowany czytnik zbliżeniowy i umożliwia kontrolę jednego przejścia, a także pełni funkcję czytnika aktualizującego uprawnienia dostępu zapisane na kartach zbliżeniowych. Jego użycie nie jest obligatoryjne w systemie RVOS, niemniej jego obecność umożliwia automatyczne usuwanie z systemu kart zagubionych, co jest często krytycznym wymaganiem stawianym przed systemem KD. Bez względu na rodzaj urządzenia w systemie RVOS użytkownik posługuje się tą samą kartą zbliżeniową.

W dalszej perspektywie do systemu RVOS planowane jest dodanie tzw. kontrolera nadrzędnego, umożliwiającego zarządzanie systemem za pomocą aplikacji webowej i aplikacji chmurowej służącej do konfiguracji i obsługi systemu.

NEDAP SECURITY MANAGEMENT

www.nedapsecurity.com/pl/

Efektywna współpraca systemów windowych z kontrolą dostępu AEOS

POMIMO KOLEJNYCH LOCKDOWNÓW SPOWODOWANYCH PANDEMIĄ RYNEK NIERUCHOMOŚCI ODMRAŻA SIĘ, ZASKAKUJĄC NOWYMI PROJEKTAMI OBIEKTÓW BIUROWYCH. ROŚNIE ZAPOTRZEBOWANIE NA ZAAWANSOWANE SYSTEMY ZARZĄDZANIA WINDAMI. WIELE KORZYŚCI DAJE POŁĄCZENIE SYSTEMU WINDOWEGO Z SYSTEMEM KONTROLI DOSTĘPU. NAJWAŻNIEJSZĄ JEST MOŻLIWOŚĆ ZARZĄDZANIA AUTORYZACJAMI, KARTAMI I ZDARZENIAMI Z JEDNEGO MIEJSCA. TO WŁAŚNIE SYSTEM KD POWINIEN PRZEJMOWAĆ TĘ ROLĘ, STANOWIĄC CENTRALNY PUNKT ZARZĄDZANIA BEZPIECZEŃSTWEM I RUCHEM OSÓB W BUDYNKU.

Klasyczne systemy sterowania windami nie przetwarzają żadnych danych. W związku z tym nie wiadomo, ile osób czeka na windę, gdzie się znajdują i na które piętro chcą się dostać. Powoduje to kolejki w holach windowych oraz przepełnione kabiny. Połączenie systemów kontroli dostępu AEOS i windowego ma trzy najważniejsze zalety:

- **Poprawa bezpieczeństwa**. Dzisiejsze obiekty wymagają skupienia się na kwestiach bezpieczeństwa. Niezmiernie istotna jest możliwość zarządzania tym, kto, gdzie i na jakich zasadach ma dostęp do pięter i stref.
- **Wygodniejsza obsługa**. Dzięki temu, że to system wskazuje użytkownikom, do której windy powinni się udać, znikają kolejki w holach windowych, a osoby podróżują szybciej. Zwiększa się wygoda obsługi dla administratora systemu KD w budynku, który korzysta z jednego interfejsu w celu zarządzania ww. elementami.
- **Łatwość integracji** z innymi systemami. AEOS przechowuje dane użytkowników i ich autoryzacji, więc inne systemy mogą się komunikować z jednym źródłem danych. To skraca czas i ułatwia tworzenie nowych integracji z takimi aplikacjami, jak Smart Building czy Visitor Management System.

Aby zaawansowany system windowy działał w zamierzony sposób, musi mieć informacje o użytkownikach, by ich właściwie obsłużyć. Problemem jest, jeśli dane są wprowadzane w dwóch miejscach. W systemie AEOS dane są spójne i zlokalizowane w jednym miejscu. To AEOS identyfikuje użytkowników i przesyła dane do systemu windowego (np. Schindler PORT, Kone Access, Kone ELI czy Compass Plus).

SALTO

www.saltoks.com

Platforma kontroli dostępu SALTO KS

SALTO SYSTEMS ZOSTAŁO ZAŁOŻONE W 2001 R. Z ZAMIAREM ZREWOLUCJONIZOWANIA, USPRAWNIENIA I STWORZENIA ZAAWANSOWANEJ ORAZ PROSTEJ W OBSŁUDZE TECHNOLOGII KONTROLI DOSTĘPU

Produkty takie, jak wirtualna sieć SALTO, gwałtownie przyspieszyły rozwój firmy, która zaopatruje w elektroniczną kontrolę dostępu miliony klientów na całym świecie. Teraz takie zabezpieczenia są w zasięgu każdego dzięki usłudze SALTO KS „Keys as a Service".

Platforma kontroli dostępu SALTO KS jest idealnym rozwiązaniem m.in. dla osób, które nie chcą lub nie mogą pozwolić sobie na okablowanie budynku lub utrzymywanie własnej serwerowni, a chciałyby np. monitorować zdarzenia w obiekcie zdalnie bądź wydawać klucze mobilne swoim pracownikom czy gościom. SALTO Systems oferuje już nie tylko bezprzewodowe okucia, do których funkcjonowania potrzebny jest jedynie dostęp do Internetu, ale przede wszystkim miejsce w chmurze. Takie połączenie ma wiele zalet.

Kontrola dostępu w chmurze nie wymaga żadnych dodatkowych działań ze strony klienta w celu utrzymania lub zarządzania systemem – dzięki natychmiastowym aktualizacjom i dodatkom jest on zawsze przygotowany i dostosowany do zmieniających się potrzeb użytkowników. Zarządzanie kontrolą dostępu w chmurze jest możliwe z dowolnego miejsca na Ziemi. Niezbędne do tego jest jedynie urządzenie – telefon, tablet lub komputer – z połączeniem internetowym.

Platforma SALTO KS zapewnia monitorowanie stanu urządzeń kontroli dostępu w czasie rzeczywistym i natychmiastowe rozwiązywanie wszelkich problemów. Przyjazny użytkownikowi interfejs, który jest aktualizowany zgodnie z trendami w społecznościach technicznych i mediach, sprawia, że platforma jest bardzo łatwa w użyciu. Nie ma już potrzeby wymiany zamków w przypadku zgubienia lub kradzieży kluczy. Wystarczy zdalnie zablokować istniejące dostępy (tagi, karty bądź klucze mobilne) i wydać nowe.

SALTO KS oznacza rewolucję na rynku kontroli dostępu i sprawia, że staje się ona znacznie prostsza w użyciu niż kiedykolwiek wcześniej.

WINKHAUS

www.winkhaus.com/pl-pl

Elektroniczna klamka do drzwi wewnętrznych Winkhaus ETB-IM

BEZPRZEWODOWA KLAMKA ETB-IM FIRMY WINKHAUS JEST IDEALNYM ROZWIĄZANIEM DO DRZWI W HOTELACH, BIURACH I WSZĘDZIE TAM, GDZIE UZASADNIENIE MA MONTAŻ DRZWI NA KARTĘ ZBLIŻENIOWĄ. KLAMKA MOŻE BYĆ ZASTOSOWANA DO DRZWI WEWNĘTRZNYCH KAŻDEGO TYPU WYPOSAŻONYCH W ZAMEK WPUSZCZANY, Z FUNKCJĄ ZAPADKI LUB SAMORYGLUJĄCY ZAMEK AUTOMATYCZNY. JEJ KOMPONENTY SĄ ZMONTOWANE FABRYCZNIE, BY UŁATWIĆ INSTALACJĘ.

Montaż klamki nie wymaga okablowania i nie narusza struktury drzwi, ponieważ nie wymaga frezowania. Równie szybko, za pomocą standardowego narzędzia, można przeprowadzić zmianę kierunku klamki oraz wymianę baterii. Klamkę ETB-IM można instalować w nowych, a także już działających systemach dostępowych Winkhaus blueSmart.

Kontrolowana jednostronnie klamka ma funkcję otwierania pojedynczego bądź stałego (ustawienie ręczne lub automatyczne). Działa podobnie jak klasyczny szyld drzwiowy, czyli nie na rygiel zamka, ale na jego język. Jeśli klamka jest ustawiona w tryb ręczny, wymagana jest najpierw autoryzacja kluczem, kartą RFID lub brelokiem. Po przyłożeniu identyfikatora do klamki następuje zasprzęglenie zamka, trzpień przenosi napęd na język zamka i w ciągu kilku sekund użytkownik może otworzyć drzwi.
By wyjść z pomieszczenia, wystarczy tylko nacisnąć klamkę zamontowaną po wewnętrznej stronie drzwi. Jeśli zaś klamka jest ustawiona na automatyczny tryb biurowy, wejścia i wyjścia nie muszą być autoryzowane przy każdym użyciu. To komfortowa funkcja w obiektach, gdzie każdorazowa autoryzacja jest zbędna.

Klamka ETB-IM ma wewnętrzny zegar z kalendarzem, można więc elastycznie programować zakres czasowy, w którym będzie spełniała nadaną przez administratora funkcję. Zawiera także pamięć wejść i wyjść, zapamiętuje do 2 tys. zdarzeń. Klamka jest dostępna w kolorach czarnym i białym.

ZKTeco

www.zkteco.eu

Nowe zaawansowane rozwiązania do rozpoznawania tablic rejestracyjnych

FIRMA ZKTeco SPECJALIZUJE SIĘ W SYSTEMACH KONTROLI DOSTĘPU I TECHNOLOGIACH BIOMETRYCZNYCH. JEJ EUROPEJSKI ODDZIAŁ OPRACOWAŁ ŁATWĄ W INSTALACJI I NIEDROGĄ KAMERĘ ZK-LPR CAR ID Z WBUDOWANYM OPROGRAMOWANIEM DO ROZPOZNAWANIA NUMERÓW TABLIC REJESTRACYJNYCH.

Rozwiązanie to może opcjonalnie integrować kontrolery dostępu ZKTeco, a także urządzenia na szynę DIN lub dowolne urządzenia innej firmy, umożliwiając połączenie między kamerą LPR a systemem zabezpieczeń.
Jak działa system ZK-LPR Car ID w porównaniu z innymi kamerami LPR? Gdy pojazd dojeżdża do punktu kontrolnego, czytnik tablic rejestracyjnych ZK-LPR Car ID przechwytuje obraz wizyjny i przekształca go w dane. Dane te są przetwarzane za pomocą zaawansowanych algorytmów i powiązane z wewnętrzną bazą danych, co pozwala na ultraszybką weryfikację i decyzję dotyczącą wjazdu pojazdu.
Podczas gdy w tradycyjnych systemach LPR najlepszą wydajność osiąga się przy użyciu jednej kamery na pas, LPR ZK-LPR Car ID rozpoznaje tablice rejestracyjne pojazdów poruszających się dwoma różnymi pasami i pozwala określić wjeżdżające lub wyjeżdżające pojazdy na każdym pasie ruchu.

ZK-LPR Car ID jest w pełni zintegrowany z modułem parkingowym ZKBioSecurity. Umożliwia też integrację z oprogramowaniem innych firm.

Dzięki ZKBioSecurity można sprawdzić dodatkowe zabezpieczenia, uzyskać dostęp do obrazu z kamery z poziomu oprogramowania i wyświetlić szczegóły dziennika aktywności LPR.

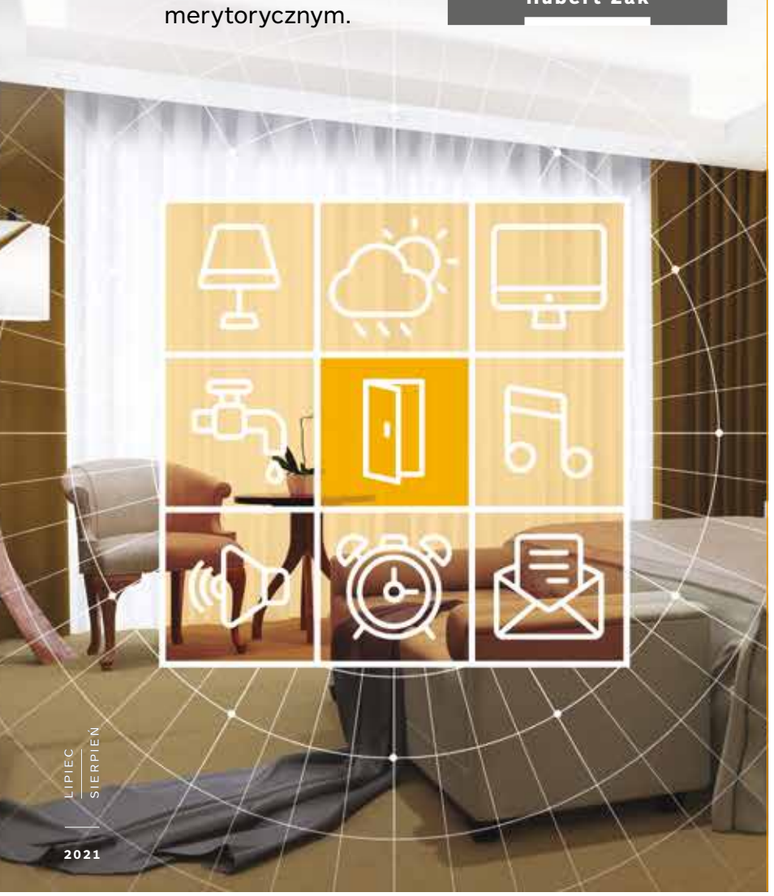
W trybie offline kamera LPR pracuje autonomicznie, korzystając z list generowanych przez oprogramowanie ZKBioSecurity. Wyśle każdy przechwycony obraz LPR do katalogu FTP, dzięki czemu wykryte tablice mogą być rozpoznane z poziomu oprogramowania ZKBioSecurity. Rejestrację numerów tablic można zaprogramować w trybie offline.
ZK-LPR Car ID ma trzy tryby wykrywania: wykrywanie wjazdu, wykrywanie ruchu pojazdu i swobodny ruch pojazdu. Odczytuje i rejestruje numery poruszających się pojazdów do prędkości 20 km/h oraz identyfikuje tablice rejestracyjne z ponad 80 krajów.

Wpływ COVID-19

na bezpieczeństwo w obiektach hotelowych

Wpływ pandemii COVID-19 na bezpieczeństwo w obiektach hotelowych należy rozpatrywać w dwóch współdzielonych obszarach: w zakresie technicznym oraz merytorycznym.

Hubert Żak



Na początku pandemii obiekty hotelowe stanęły przed kompletnie nowym wyzwaniem, z którym mierzy się do tej pory cały świat. Dzięki wytężonej pracy ekspertów, zespołów hotelowych i grup naukowych w znacznym stopniu udało się zaimplementować wiele rozwiązań, by w maksymalnym możliwym stopniu zapewnić bezpieczeństwo gości i obsługi oraz zminimalizować ryzyko zakażenia. Biorąc pod uwagę aspekt techniczny, należy wymienić działania w trzech głównych obszarach:

- **Pierwszy obszar to urządzenia mobilne**, np. mobilne zestawy termowizyjne, zamgławiacze, urządzenia ozonujące, mobilne zestawy UV, zestawy detekcyjno-dezynfekcyjne itd.
- **Drugi obszar to urządzenia wspomagające**, czyli wszystkie urządzenia i systemy analityczne, np. liczące osoby w strefie, urządzenia dedykowane do kontroli ruchu, ograniczające liczbę osób w strefach, rozbudowa istniejących rozwiązań systemowych o dodatkowe urządzenia mierzące temperaturę, śluzy czy urządzenia organizacji ruchu.
- **Trzeci obszar to urządzenia systemów podstawowych**, takie jak specjalne filtry i systemy UV wbudowane w istniejące instalacje obiektu – systemy wentylacji, urządzenia filtrujące, instalacje klimatyzacji w zakresie wirusologicznym, wymiana i rozbudowa systemów obiegu powietrza.

We wszystkich tych obszarach, w zależności od charakterystyki obiektu, rozwiązania wdrażano łącznie lub wybiórczo, dążąc do uzyskania konkretnych parametrów pozwalających na zminimalizowanie ryzyka ekspansji wirusa. Celem było wykluczenie czynnika wirusologicznego i jednocześnie, w przypadku jego wystąpienia, uzyskanie maksymalnej możliwości zatrzymania i rozprzestrzeniania się go w innych obszarach, poprzez możliwość wyłączenia lub zabezpieczenia strefy niebezpiecznej.

W miarę upływu czasu i szybkiego dostosowywania technologii przez producentów proces zabezpieczania przed rozprzestrzenianiem się wirusa rozwijał się coraz lepiej dzięki uzyskiwaniu coraz wyższych parametrów pracy. Dotychczas najlepszą stosowaną metodą jest zasada dublowania, polegająca na uzupełnieniu jednej metody ochronnej, np. dezynfekcji przez zamgławianie, drugą dodatkową, m.in. procesem ozonowania, dezynfekcji chemicznej, dezynfekcji za pomocą UV lub innej, równie wydajnej metody. Innym przykładem tej metody może być wykorzystanie kamery termowizyjnej z funkcjami analitycznymi, która wykrywa osobę o podwyższonej temperaturze i przekazuje sygnał do operatora.

AKTUALNE ZABEZPIECZENIA DOTYCZĄCE ZDROWIA I ŻYCIA BĘDĄ WSPOMAGAĆ GOŚCI HOTELOWYCH I PRACOWNIKÓW PRZEZ KOLEJNE LATA, DYNAMICZNIE ROZWIJAJĄC SIĘ WRAZ Z POTRZEBAMI RYNKU I JAKOŚCIĄ ŚWIADCZONYCH USŁUG HOTELOWYCH

Po otrzymaniu takiego sygnału operator odseparowuje osobę w strefie bezpiecznej zamkniętej i wdraża ręczny pomiar temperatury za pomocą urządzeń bezdotykowych. Dzięki zastosowaniu metody podwajania uzyskuje się informacje z dwóch niezależnych źródeł.

Większość grup hotelowych we współpracy z zespołami doradczymi i ekspertami wdrożyła takie rozwiązania w swoich hotelach, co w istocie pokazało, że są to jedne z najlepiej przygotowanych obiektów w zakresie przeciwdziałania rozprzestrzenianiu się wirusa.

Trochę inaczej sytuacja wygląda w małych, niekorporacyjnych i niesieciowych obiektach hotelowych. Część z nich, z braku rozwiązań systemowych, zwracała się indywidualnie do specjalistów lub realizowała rozwiązania we własnym zakresie. Z powodu braku narzędzi kontrolnych jedyny zakres, jaki można obiektywnie ocenić, dotyczy projektów zrealizowanych na podstawie danych firm instalacyjnych lub dystrybutorów i przy wsparciu informacjami zawartymi na stronach internetowych hotelu lub innymi źródłami informacji o obiekcie.

W zakresie realizowanego poziomu bezpieczeństwa każdy gość ma prawo zażądać od właściciela lub obsługi informacji o zastosowanych środkach, a hotel ma obowiązek takiej informacji udzielić. Pomimo braku scentralizowanych ogólnych zasad zabezpieczenia wprowadzone w obiektach hotelowych czynią je jednymi z najlepiej chronionych obiektów użyteczności publicznej na rynku.

Oddzielnie należy pochylić się nad aspektem merytorycznym. Doskonale wiadomo, że nawet najlepszy system czy najlepsze urządzenie bez umiejętnego wykorzystania przez użytkownika pozostaje tylko bezwartościowym zbiorem przeprowadzonych czynności i uzyskanych informacji. Co zatem się sprawdziło w przypadku epidemii? Zadziałały tu odpowiednio przygotowane i wdrożone procedury oraz algorytmy działania w konkretnych sytuacjach.

W obiektach hotelowych stworzono schematy, wykorzystując narzędzia analizy ryzyka *(risk management)* z zakresu procedur bezpieczeństwa i innych niezbędnych aspektów, zapewniających najwyższy poziom ochrony pracowników i gości hotelowych. Opracowano i oceniono każde możliwe ryzyko, co stało się punktem wyjścia do dalszej analizy i definicji. Zapoznając się z ryzykiem w danym obszarze, np. dostawy towaru, obecności gości w recepcji, wystąpienia choroby w trakcie pobytu czy innych aspektów codziennej pracy hotelu, przygotowano instrukcje, które jasno i przejrzyście określają bezwzględny sposób postępowania w przypadku wystąpienia danego ryzyka lub innych zdefiniowanych wcześniej zagrożeń.

Kolejnym etapem było wdrożenie procedur, w których procesie w sposób stały i cykliczny szkoli się pracowników, dostawców usług, pracowników outsourcingu oraz inne osoby wykonujące pracę na terenie obiektu hotelowego. Stały tryb szkolenia pozwala na utrzymanie wysokiej efektywności. W hotelach sukcesywnie przeprowadza się ćwiczenia zawarte w instrukcjach i procedurach w zakresie schematów postępowań i obsługi sprzętu.

Takie rozwiązania gwarantują minimalizowanie ryzyka, co przełożyło się na niewielką liczbę osób zakażonych przebywających w obiektach hotelowych. Minusem niestety większości procedur jest konieczność indywidualnego dostosowywania ich do charakterystyki obiektu, przy czym podstawowe założenia muszą pozostać niezmienne.

Podsumowując, wpływ pandemii na bezpieczeństwo zarówno techniczne, jak i fizyczne w hotelach był i jest znaczny. Rozwiązania i procedury ewoluują w miarę dynamicznych zmian sytuacji epidemiologicznej. Wydaje się, że na wiele z tych rozwiązań rynek czekał od dawna. Niestety, sprawdza się stara zasada, że dopiero w obliczu kryzysu branże technologiczna, innowacyjna i badawcza oraz szeroko pojęte służby bezpieczeństwa potrafią nawiązać współpracę, wymieniać dane i rozwijać w sposób konstruktywny wiele poszukiwanych rozwiązań.

Bez względu na to, kiedy i w jaki sposób pandemia się zakończy lub czy będzie ona z nami jeszcze długo, rozwój zabezpieczeń w obiektach hotelowych i użyteczności publicznej znacznie przyspieszył. Aktualne zabezpieczenia dotyczące zdrowia i życia będą wspomagać gości hotelowych i pracowników przez kolejne lata, dynamicznie rozwijając się wraz z potrzebami rynku i jakością świadczonych usług hotelowych.

HUBERT ŻAK

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

ZETTLER PROFILE Flexible

w hotelu

Wymagania dotyczące instalacji systemu sygnalizacji pożarowej w hotelu zwykle obejmują konieczność zabezpieczenia różnych przestrzeni – pokoi gościnnych, dróg ewakuacyjnych, pomieszczeń kuchennych i technicznych czy garaży. Niezawodność systemu jest priorytetowa, gdyż jego podstawową funkcją jest ochrona życia. Ważne, by wybrany system skutecznie chronił hotel, działał niezawodnie i powodował jak najmniej zakłóceń dla gości.

Ryzyko: Większość pokoi hotelowych dysponuje łazienką z wanną lub prysznicem. Generowana z nich znaczna ilość pary wodnej może powodować fałszywe alarmy pożarowe w niektórych systemach sygnalizacji pożarowej.
Rozwiązanie: Jeżeli zainstalujemy czujki wielosensorowe 850PC w każdej sypialni, para wydobywająca się z łazienki NIE WŁĄCZY alarmu. Taka czujka nadal będzie bardzo czuła na produkty spalania generowane przez tlący się pożar (ma zdolność do wykrywania gazów spalinowych, tj. tlenku węgla) i uruchomi alarm nawet wcześniej niż czujka dymu o normalnej czułości.
Czujki z serii 850 i 830 są dostępne w wersjach z wbudowanym izolatorem zwarć lub bez niego i wykorzystują zaawansowaną sygnalizację cyfrową, aby zapewnić niezawodną komunikację z centralą SSP. Ręczne narzędzie serwisowe umożliwia komunikację z czujką (dwukierunkowa łączność IR), dzięki czemu dostęp w celu serwisowania i testowania czujek jest łatwy i szybki z poziomu podłogi, bez konieczności stosowania podnośników czy drabin.

Ryzyko: Drzwi ppoż. w hotelu są istotną częścią ochrony życia w każdym scenariuszu rozwoju pożaru. Dym może szybko rozprzestrzeniać się na drogi ewakuacyjne, takie jak korytarze i klatki schodowe, ograniczając dostęp i uniemożliwiając gościom bezpieczne wydostanie się z budynku.
Rozwiązanie: Drzwi ppoż. mogą być sterowane i nadzorowane za pomocą modułu kontroli drzwi TSM800 zaprojektowanego specjalnie do nich. Ma system samomonitorowania, który sprawdza komunikację z centralą i wykrywa obecność napięcia na pętli. Monitoruje też niezbędne zasilanie pomocnicze, zasilające elektromagnes przytrzymujący drzwi. W razie wykrycia usterki lub programowego odłączenia modułu z poziomu menu centrali moduł zwolni drzwi do pozycji zamkniętej, zapewniając szczelność przegrody ppoż.

Ryzyko: Co się stanie, gdy SSP zostanie przypadkowo aktywowany? Aby uniknąć niepotrzebnych zakłóceń dla gości, incydenty powinny być zawsze sprawdzone przed podjęciem decyzji o ewakuacji.
Rozwiązanie: Centrale PROFILE Flexible umożliwiają dowolną konfigurację działania systemu na wypadek pożaru. Konfigurując matrycę sterowań, urządzenia można skonfigurować tak, aby działały: indywidualnie i natychmiast, indywidualnie i z opóźnieniem lub w połączeniu z innym urządzeniem (w tzw. koincydencji). Możliwości programowe są w zasadzie nieograniczone i pozwalają dostosować pracę instalacji do dowolnego scenariusza zdarzeń. Wszelkie sprawdzenia alarmów muszą być przeprowadzane szybko i pod ścisłą kontrolą, przy obowiązujących limitach czasowych, a jeśli określone czasy reakcji zostaną przekroczone, system automatycznie uruchomi ewakuację.

Ryzyko: Alarmowanie i przeprowadzanie ewakuacji w nocy, gdy goście hotelowi śpią, jest zawsze ogromnym wyzwaniem. W hotelu, w którym większość mieszkańców zapewne nie zna dokładnie swojego otoczenia, wczesne ostrzeżenie o pożarze ma zasadnicze znaczenie dla ochrony życia.
Rozwiązanie: Sygnalizatory akustyczne muszą być w 100% sprawne i na tyle głośne, aby obudzić śpiące osoby. Każda centrala PROFILE Flexible umożliwia konfigurowanie i uruchamianie testowania sygnalizatorów z poziomu centrali. Funkcja monitorowania dźwięku odbitego pozwala testować wszystkie sygnalizatory przez zainicjowanie testu trwającego ok. 15 s, po którym każdy niedziałający sygnalizator zostaje zgłoszony do centrali. Sygnalizatory można testować ręcznie w grupach, piętro po piętrze, strefa po strefie, zależnie od konfiguracji trybu testowego. Centrala pozwala też zaprogramować funkcję cyklicznego autotestu wszystkich sygnalizatorów.
System sygnalizacji pożarowej ZETTLER stanowi idealne rozwiązanie dla specyficznych wymagań sektora hotelowego.

JOHNSON CONTROLS INTERNATIONAL
ul. Krakowiaków 50
02-255 Warszawa
pawel.jozwik@jci.com

Transformacja oddziałów bankowych

jak dziś zapewnić bezpieczeństwo?

Przez całe stulecia oddziały bankowe były fizycznym wyrazem wyobrażenia o bezpieczeństwie. Wzrost znaczenia cyfrowych usług bankowych wymusza jednak dynamiczną ewolucję placówek, które teraz coraz częściej służą przede wszystkim za centra doradztwa. Za tymi przemianami idzie także zmiana definicji bezpieczeństwa w oddziałach, szczególnie w czasach pandemii. Wsparciem mogą okazać się technologie wizyjne.

Bankowość detaliczna nieustannie się zmienia, a wraz z nią zmienia się też rola oddziału banku. Jeszcze 10 lat temu nikt nie sądził, że placówki mogą stać się bardziej nieformalnymi miejscami spotkań czy nawet kawiarniami, a przy tym centrami usług cyfrowych.

- Innowacje pozytywnie wpływają na jakość obsługi klientów, jednak wraz z nimi konieczne jest wprowadzenie nowych metod zapewnienia bezpieczeństwa. Stworzenie przyjaznego, a jednocześnie bezpiecznego środowiska w oddziałach bankowych staje się wyjątkowym wyzwaniem w dobie pandemii, na które mogą odpowiedzieć nowoczesne technologie cyfrowe, takie jak systemy wizyjne, aplikacje wykorzystujące sztuczną inteligencję czy systemy audio – mówi Bogumił Szymanek z Axis Communications.

OPTYMALIZACJA PRZESTRZENI

Niestety, jednym z pierwszych skojarzeń, jakie często przychodzą nam do głowy na myśl o oddziałach bankowych, są kolejki. Nikt za nimi nie przepada, trudno też zachować w nich odpowiedni dystans społeczny. Tymczasem sieciowe kamery z analityką monitorowania długości kolejek zapewniają dostęp do niezbędnych informacji na ich temat w czasie rzeczywistym. W chwili, gdy liczba oczekujących osób przekroczy określony limit, system sam może poinformować personel o konieczności otwarcia dodatkowego stanowiska. Statystyki dotyczące kolejek i ich tworzenia się w ciągu dnia są pomocne w dostosowaniu zasobów kadrowych do potrzeb klientów.

Narzędzia analityczne mogą również zliczać osoby obecne w danej chwili w oddziale lub jego określonych obszarach. Jest to funkcja pomocna dla kierowników placówek, którzy mogą sprawniej zarządzać przestrzenią i personelem. Ponadto rozwiązania te pozwalają zachować odpowiedni dystans społeczny. Przykładem mogą być systemy, które samodzielnie zliczają osoby wchodzące do oddziału. Po osiągnięciu określonego limitu na ekranie zainstalowanym przed wejściem automatycznie pojawi się informacja z prośbą o zaczekanie do momentu, aż ktoś opuści bank.

KLUCZOWA ROLA DŹWIĘKU

Innym rozwiązaniem, które dopiero zyskuje na popularności w bankowości, są sieciowe systemy audio. Ich podstawową rolą jest zarządzanie dźwiękiem na terenie placówki, w tym również muzyką. Ta ostatnia może nie tylko umilać klientom czas oczekiwania, ale także wspierać bezpieczeństwo. Przykładowo, w niektórych obszarach banku, gdzie wymagana jest większa poufność, podkład muzyczny może być odpowiednio zmieniony, podobnie jak jego głośność.

Oprócz muzyki system audio połączony z sieciowymi kamerami monitoringu może pomóc w zapobieganiu potencjalnym zagrożeniom za pomocą wcześniej przygotowanych nagrań głosowych. Tego typu rozwiązania, np. po wykryciu przekroczenia limitu osób na metr kwadratowy bądź braku maseczki na twarzy klienta, nadadzą automatycznie stosowny komunikat. Takie systemy są przydatne nie tylko w czasach pandemii. W przyszłości mogą np. nadawać komunikat powitalny, wzbogacając tym samym doświadczenie klienta, czy też dbać o bezpieczeństwo, wypraszając podejrzanie zachowującego się gościa z przedsionka bankomatu.

NIE TYLKO KLIENCI

Kwestie bezpieczeństwa dotyczą nie tylko klientów, ale także pracowników. Obecnie, w toku wielu obowiązków związanych z obsługą klienta w placówce bankowej, mogą oni zwyczajnie zapominać o koniecznej regularnej dezynfekcji. Systemy audio funkcjonujące poza obszarami dostępnymi dla klientów mogą co jakiś czas przypominać o potrzebie mycia rąk, konieczności noszenia maseczek czy zachowywania odpowiedniego dystansu. Wejścia do stref pracowniczych mogą zostać wyposażone w bezdotykowe systemy kontroli dostępu, bazujące np. na aplikacji mobilnej lub kodach QR. Dzięki temu pracownicy nie będą musieli być narażeni na dotykanie ryzykownych elementów, np. klamek czy klawiatur dostępowych.

– Warto podkreślić, że każde z wymienionych rozwiązań ma potencjał długookresowy, związany nie tylko z pandemią. Systemy wykorzystywane dzisiaj do zachowania dystansu, jutro pomogą optymalizować pracę oddziału. W dobie coraz bardziej rozproszonej obsługi klienta, już nie tylko z poziomu biurka czy okienka, staje się to szczególnie ważne, by w parze z jego pozytywnym doświadczeniem szedł także wysoki poziom bezpieczeństwa – dodaje Bogumił Szymanek.

STWORZENIE PRZYJAZNEGO, A JEDNOCZEŚNIE BEZPIECZNEGO ŚRODOWISKA W ODDZIAŁACH BANKOWYCH STAJE SIĘ WYJĄTKOWYM WYZWANIEM W DOBIE PANDEMII, NA KTÓRE MOGĄ ODPOWIEDZIEĆ NOWOCZESNE TECHNOLOGIE CYFROWE, TAKIE JAK SYSTEMY WIZYJNE, APLIKACJE WYKORZYSTUJĄCE SZTUCZNĄ INTELIGENCJĘ CZY SYSTEMY AUDIO

SYSTEMY WYKORZYSTYWANE DZISIAJ DO ZACHOWANIA DYSTANSU, JUTRO POMOGĄ OPTYMALIZOWAĆ PRACĘ ODDZIAŁU W DOBIE CORAZ BARDZIEJ ROZPROSZONEJ OBSŁUGI KLIENTA, JUŻ NIE TYLKO Z POZIOMU BIURKA CZY OKIENKA, STAJE SIĘ TO SZCZEGÓLNIE WAŻNE, BY W PARZE Z JEGO POZYTYWNYM DOŚWIADCZENIEM SZEDŁ TAKŻE WYSOKI POZIOM BEZPIECZEŃSTWA

AXIS COMMUNICATIONS POLAND

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

Technologie które robią wrażenie na bank

Zapewnienie bezpieczeństwa zawsze było dla branży bankowej kluczową kwestią. Instytucje finansowe wymagają rozwiązań na najwyższym poziomie, gwarantujących sprawne reagowanie na zdarzenia. Zastosowanie systemów monitoringu wizyjnego w bankach jest standardem od wielu lat, jednak obserwowanie obrazów z wielu kamer jednocześnie oraz należyte reagowanie na sytuacje alarmowe i wszelkie nietypowe zachowania jest ograniczone możliwościami percepcji pracownika ochrony. Powodowało to niejednokrotnie opóźnioną reakcją lub przeoczenie zdarzenia, co może mieć nieodwracalne skutki finansowe.

Hikvision, jako wiodący producent systemów telewizji dozorowej (CCTV/VSS) oraz wielu innych systemów podnoszących poziom bezpieczeństwa we wszelkiego rodzaju obiektach, z dumą oferuje kompletne rozwiązanie, które nie tylko poprawia bezpieczeństwo w trakcie codziennych operacji, ale też stale buduje zaufanie klientów. Rozwiązania Hikvision mają zastosowanie nie tylko w oddziałach banków, ale również w bankomatach, transporcie pieniędzy, jak również w scentralizowanych i lokalnych centrach monitoringu.

Mimo rosnącej popularności bankowości cyfrowej i nowych technologii finansowych tradycyjne oddziały banków wciąż zajmują ważne miejsce w życiu przeciętnego konsumenta. Świadczą usługi o wysokiej wartości, które klienci wolą realizować tylko w kontakcie osobistym z pracownikiem banku. Są to głównie pożyczki, kredyty hipoteczne, inwestowanie w produkty finansowe, otwieranie pierwszego rachunku bieżącego i tak dalej.

Poczucie bezpieczeństwa w banku jest sprawą kluczową dla klientów, zarówno jeśli chodzi o bezpieczeństwo osobiste, jak i złożone depozyty. To właśnie pomagają osiągnąć technologie Hikvision.

Jednym z pierwszych rozwiązań, jakie w dobie wciąż niestety szalejącej pandemii COVID-19 możemy spotkać tuż przed wejściem do każdego oddziału bankowego, jest wyświetlacz wskazujący aktualną liczbę osób w obiekcie, z informacją, czy jest możliwe wejście do środka bez łamania aktualnych ograniczeń. Zastosowanie ma tutaj kamera licząca przebywające wewnątrz banku osoby, z pominięciem pracowników obsługi, których – dzięki technologii rozpoznawania twarzy – system wychwytuje i pomija w obliczeniach. Zaraz po wejściu do środka napotykamy kamerę termowizyjną do pomiaru temperatury ciała z dokładnością ±0,2°C. Jeśli w polu jej widzenia pojawi się osoba, której temperatura przekracza wcześniej ustawioną wartość, jest w stanie zaalarmować obsługę.

Wspomnianą już technologię rozpoznawania twarzy w kamerach Hikvision ochrona obiektu wykorzystuje do natychmiastowego wychwycenia wejścia osoby niepożądanej, umieszczonej na tzw. czarnej liście. Zastosowana technologia, dzięki sprawnemu przeszukiwaniu nagrań i wskazaniu zdjęcia lub stop-klatki tej osoby, znacznie przyspiesza pracę pracowników ochrony. Wyszukiwanie nagrań możliwe jest też na podstawie charakterystycznych cech, np. przybliżony wiek, kolor skóry, włosów, ubrań czy innych. Wynikiem wspomnianych możliwości jest lista nagrań, na których interesująca nas osoba występuje, nie ma więc konieczności przeszukiwanie całego zarejestrowanego materiału wizyjnego, a jedynie wskazanych fragmentów.

W bardzo podobny sposób realizowana jest obserwacja okolicy banku. Materiał wizyjny jest zapisywany z uwzględnieniem rozpoznawania cech ludzi, a także cech charakterystycznych samochodów, takich jak numery tablic rejestracyjnych, marka, kolor itd. Również w tych zastosowaniach rozpoznanie pojazdu znajdującego się na czarnej liście lub w strefie, w której nie powinien się znajdować, czy też stojącego tam zbyt długo może automatycznie poinformować obsługę i uruchomić śledzenie.

W przypadku kamer zewnętrznych największe wrażenie na użytkownikach systemu robią technologie AcuSense oraz ColorVu, dzięki którym pracownicy ochrony obserwują obraz w kolorze, ze wszystkimi szczegółami, nie tylko w dzień przy dobrym oświetleniu, ale również w nocy, nawet przy całkowitej ciemności. Co ważne, ochrona jest informowana jedynie w sytuacjach niewłaściwych zachowań spowodowanych przez człowieka i/lub samochód. Alarmu nie wzbudzają takie zdarzenia, jak wtargnięcie zwierzęcia, ruch liści, drzew, cieni czy np. ostre światło padające bezpośrednio w obiektyw.

Technologie zaszyte we współczesnych kamerach mają wiele dodatkowych możliwości analitycznych, m.in. analizowanie długości kolejek. Czas oczekiwania ma zazwyczaj niekorzystny wpływ na wrażenia klientów, dlatego kamery monitorujące w czasie rzeczywistym wysyłają powiadomienia, gdy w kolejce jest zbyt wiele osób i należy np. uruchomić drugą kasę. Ponadto menedżerowie mogą sprawdzać dane dotyczące kolejek w celu oceny pracy pracowników i śledzenia wydajności.

Każda transakcja, która ma miejsce w banku, jest ważna i musi być ewidencjonowana. Zastosowanie rozdzielczości 4K w kamerach standardowych oraz jeszcze wyższej w modelach specjalistycznych zapewnia prawidłowe rejestrowanie szczegółów transakcji i przechowywanie ich w celu sprawdzenia w razie potrzeby. Doposażenie kamery w kartę SD gwarantuje zarejestrowanie materiału nawet po zerwanej komunikacji z rejestratorem.

Same urządzenia odpowiedzialne za nagrywanie i ewentualne późniejsze odtwarzanie zapisanego materiału dowodowego mają szereg funkcji gwarantujących ich ciągłą pracę, począwszy od bardzo stabilnego oprogramowania, poprzez zastosowanie technologii RAID (nadmiarowa macierz niezależnych dysków), po zastosowanie redundantnego rejestratora.

Wysoki poziom bezpieczeństwa jest zawsze priorytetem dla banków, dlatego również systemy kontroli dostępu nie pozostają w tyle za szybko rozwijającą się telewizją dozorową, umożliwiając zabezpieczenie wejścia do strefy zamkniętej na wiele różnych, powiązanych ze sobą metod identyfikacji. Należą do nich przede wszystkim rozpoznawanie cech biometrycznych, np. twarzy lub odcisków palców, powiązane np. z danymi na karcie zbliżeniowej i dodatkowo z wpisaniem właściwego kodu dostępu. Połączenie kilku technologii uwierzytelniania gwarantuje wejście jedynie osoby posiadającej odpowiednie uprawnienia, a obraz i cała operacja zostają zarejestrowane przez system.

Rozwój sztucznej inteligencji i innych zaawansowanych technologii nadzoru umożliwia bankom zbieranie wiarygodnych materiałów wideo do celów śledztwa, gromadzenie informacji na potrzeby świadomych decyzji biznesowych oraz usprawnianie procesów w celu skutecznego zarządzania oddziałami. Rozwiązania Hikvision maksymalizują wykorzystanie systemu bezpieczeństwa – zapewniają nie tylko bezpieczne środowisko, ale także przydatne narzędzia usprawniające biznes. Skorzystaj z najbardziej zaawansowanych technologii i maksymalizuj bezpieczeństwo, wydajność i zaufanie do banku w szybko zmieniającej się erze cyfrowej.

HIKVISION POLAND

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

Pełna kontrola nad bezpieczeństwem

Zaufanie klientów do instytucji finansowej zależy od tego, czy bezpieczeństwo danych nie zostanie zagrożone. Uczciwość, dbanie o reputację poprzez przestrzeganie lokalnych praw, przepisów i zasad etycznych są bardzo ważne, co nie oznacza, że muszą być skomplikowane.

i zarządzanie ryzykiem dzięki platformie **AEOS**

Dzięki platformie do zarządzania bezpieczeństwem AEOS klienci mają do dyspozycji szereg inteligentnych funkcji, takich jak *Anty-pass back*, *Manager First* (pozwala na wejście do konkretnego pomieszczenia użytkownikowi tylko wtedy, gdy jest tam jego przełożony) czy silnik reguł (przykładem może być wysłanie powiadomienia do administratora systemu o próbie wejścia przez drzwi, do których otwarcia dany użytkownik nie ma uprawnień). Dzięki temu można łatwo zarządzać ryzykiem oraz kontrolować przepływ osób i informacji bez względu na lokalizację i liczbę oddziałów.

SYSTEM AEOS ZAPOBIEGA KONFLIKTOWI INTERESÓW DZIĘKI AUTOMATYCZNEJ SEPARACJI DOSTĘPU MIĘDZY DEPARTAMENTAMI

Łatwo wyobrazić sobie sytuację, gdy dany pracownik działu marketingu może mieć dostęp do działów bankowości inwestycyjnej i księgowości. System można jednak tak skonfigurować, że jeśli pracownik był w dziale księgowości, nie będzie mógł wejść do działu bankowości inwestycyjnej przez określony czas, np. miesiąc. Jeżeli w ciągu tego miesiąca spróbuje jednak wejść do tych pomieszczeń, nie otrzyma dostępu, a kierownik ds. bezpieczeństwa momentalnie dostanie powiadomienie e-mailem lub SMS-em i będzie mógł natychmiast podjąć działania.

PRZESTRZEGANIE PROCEDUR I OSZCZĘDNOŚĆ CZASU DZIĘKI AUTOMATYCZNEMU ZARZĄDZANIU UPRAWNIENIAMI

Zazwyczaj instytucje finansowe mają kilka lokalizacji, wiele osób musi przemieszczać się pomiędzy nimi. Utrzymywanie aktualnych uprawnień jest niezbędne, ale bardzo czasochłonne w przypadku manualnej kontroli. System AEOS Rule Engine robi to automatycznie w odpowiedzi na wszelkie istotne modyfikacje, dzięki czemu uprawnienia są zawsze aktualne we wszystkich placówkach firmy, w dowolnym miejscu bez względu na lokalizację. Gdy pracownik zmieni dział, uprawnienia na jego karcie dostępu zmienią się automatycznie z chwilą, gdy jego nowe stanowisko zostanie aktywowane w systemie HR. Kontynuując wątek poprzedniego przykładu, na wcześniejszym stanowisku mógł on mieć dostęp do działów bankowości inwestycyjnej oraz do księgowości. Ponieważ teraz pracuje w dziale księgowości, nie ma już dostępu do bankowości inwestycyjnej, natomiast potrzebuje dostępu także do biur lokalnych – silnik reguł AEOS ustawia to automatycznie. Taki poziom automatyzacji oznacza duże zmniejszenie zadań administracyjnych dla szefów ds. bezpieczeństwa, dzięki czemu mogą oni skupić się na istotniejszych zadaniach.

WIĘKSZA WYDAJNOŚĆ PRZESTRZENI BIUROWEJ

Pandemia koronawirusa zmieniła kompletnie nasze podejście do wykorzystania przestrzeni biurowej ze względu na obowiązujące w danym momencie regulacje związane z COVID-19 czy też elastyczność co do wyboru miejsca pracy (biuro lub dom), jaką dziś firmy dają pracownikom. Zatem takie podejście wymusza również odpowiednią aranżację biura, m.in. stosowanie tzw. hot-desków wspieranych dedykowanymi szafkami, w których dany pracownik może przechowywać swoje rzeczy.

Myśląc o elastyczności, nie można zapominać o bezpieczeństwie. Wiele organizacji stosuje politykę czystych biurek, aby zminimalizować ryzyko, że informacje niejawne lub wrażliwe mogą być oglądane przez niewłaściwe osoby. System AEOS Locker Management ułatwia to zadanie zarówno pracownikom, jak i osobom zarządzającym. Pracownicy mogą otwierać szafki za pomocą karty dostępu, co eliminuje gubienie kluczy. Szafki można przypisać do poszczególnych osób na dłuższy okres lub też pracownicy mogą z nich korzystać dynamicznie.

Dynamiczne zarządzanie szafkami umożliwia bardziej efektywne wykorzystanie przestrzeni roboczej. Nie potrzebujemy jednej szafki na osobę, pracownicy po prostu korzystają z każdej wolnej, gdy jej potrzebują. Zatem potrzebna jest mniejsza liczba szafek, co oszczędza miejsce i koszty. Ponadto szafki można umieścić w dowolnym miejscu – nie ma potrzeby umieszczania ich przy każdym biurku. Dobrym przykładem jest również zastosowanie szafek dla danego działu. Pracownik może być upoważniony do korzystania z centralnej szafki w godzinach pracy, np. podczas spotkań. Jego karta dostępu upoważnia również do otwierania szafek na dokumenty archiwalne w jego departamencie. Ten konkretny pracownik i jego bezpośredni współpracownicy mają dostęp do tych archiwów, ale inni pracownicy z dostępem do tego działu już nie.

AEOS SPEŁNIA NAJWYŻSZE STANDARDY W ZAKRESIE BEZPIECZEŃSTWA

Ze względu na profil działalności i wynikające z niego regulacje instytucje finansowe szczególną wagę przykładają do niezawodności kluczowych komponentów. Platforma AEOS także w tym zakresie spełnia restrykcyjne wymagania dzięki redundancji najważniejszych komponentów. Mówiąc o bezpieczeństwie, należy podkreślić również szyfrowaną komunikację na każdym etapie wymiany danych. System kontroli dostępu Nedap pozwala na zastosowanie tzw. reguły End-to-End, polegającej na przeniesieniu kluczy szyfrujących z czytnika na kontroler, który jest instalowany po bezpiecznej stronie drzwi, a zatem liczba osób mających do niego dostęp jest znacznie zawężona.

Uzupełnieniem jest coraz częściej wymagany przez klientów standard 802.1x weryfikujący dostęp kontrolera drzwiowego do sieci LAN czy proces logowania wykorzystujący dwuskładnikowy etap weryfikacji poprzez podanie hasła do aplikacji oraz dedykowanego jednorazowego kodu wysłanego np. na smartfon.

OTWARTA PLATFORMA

System bezpieczeństwa AEOS podąża za wymaganiami swoich klientów. Dzięki coraz szerszej współpracy firmy z partnerami technologicznymi można już korzystać m.in. z technologii biometrycznych (rozpoznawanie twarzy), integracji z systemem telewizji dozorowej, z wykorzystaniem dwukierunkowej wymiany danych, co w efekcie pozwala na szybką korelację zdarzeń z obu systemów i efektywną analizę incydentów. Dzięki otwartym interfejsom, tj. OSDP w wersji 2.2 możliwe jest także podłączenie w bezpieczny (szyfrowany) sposób czytników innych producentów – tym samym AEOS zapewni pełne wsparcie dla wszystkich najważniejszych technologii kartowych dostępnych na rynku: MIFARE DESFire, iClass/SEOS czy Legic. Dzięki współpracy z partnerami możemy zaoferować również wsparcie dla technologii mobilnych Bluetooth i NFC, które stają się coraz popularniejsze w przestrzeniach biurowych.

DOŚWIADCZENIE

Największe instytucje finansowe w Polsce i na świecie korzystają z platformy AEOS, a także doświadczenia zdobytego przez firmę Nedap. Zapraszamy do kontaktu z przedstawicielstwem w Polsce, aby uzyskać więcej informacji nt. dedykowanych rozwiązań dla sektora finansowego.

Głos branży

HOTELE I INSTYTUCJE FINANSOWE SĄ OBIEKTAMI WYMAGAJĄCYMI SZCZEGÓLNEJ OCHRONY. ZARZĄDZAJĄCY NIMI MUSZĄ DBAĆ O BEZPIECZEŃSTWO ZARÓWNO GOŚCI, JAK I PRACOWNIKÓW, ZWŁASZCZA W CZASIE PANDEMII, KTÓRA NADAL NAM ZAGRAŻA.

Barbara Podwysocka

Polski Holding Hotelowy

O bezpieczeństwie w hotelach

Po ponad roku trwania pandemii branża hotelowa ponownie rozpoczęła sezon wakacyjny. Zgodnie z obowiązującymi obostrzeniami i limitami może być 75 proc. zajętych pokoi, w limity nie są wliczane osoby zaszczepione.
W obecnym sezonie właściciele hoteli mają dużo większe doświadczenie. Potrafią przeanalizować ryzyko i jednocześnie ocenić oczekiwania gości, które w tym roku zdecydowanie różnią się od poprzedniego. Zmęczenie pandemią, ograniczeniami, a do tego pojawiające się problemy natury ekonomicznej i społecznej powodują, że potrzeby gościa są rozpatrywane w sposób bardziej indywidualny. Branża hotelarska ma zatem niełatwe zadanie łączenia przestrzegania obostrzeń i dbania o bezpieczeństwo sanitarne i fizyczne gości z ich potrzebami, zwłaszcza gdy w czasie wakacji chcą czuć się beztrosko i swobodnie.

We wszystkich obiektach Grupy Polskiego Holdingu Hotelowego przestrzegamy wymogów sanitarnych zgodnie z obowiązującymi zasadami sanitarnymi, w tym absolutnie podstawowymi, jak noszenie maseczek w przestrzeniach wspólnych obiektów, dezynfekcja i zachowanie dystansu społecznego. Ponadto we wszystkich obiektach naszej grupy pracownicy są przeszkoleni w zakresie przestrzegania obostrzeń i potrafią reagować na indywidualne potrzeby gości.
Niemniej jednak dla zachowania bezpieczeństwa gości w naszych hotelach i obiektach robimy coś więcej. Wprowadziliśmy rozwiązania teleinformatyczne pozwalające na zapewnienie bezpieczeństwa zarówno pracownikom, jak i naszym gościom. Zwiększając zastosowanie nowych inteligentnych rozwiązań tego typu, nie możemy jednak zapominać o tym, że hotele to usługa oparta na kontakcie z gościem, dlatego tak ważne jest zachowanie swoistej równowagi człowiek–technologia.

W tym roku Grupa Kapitałowa PHH kładzie również bardzo duży nacisk na szkolenia z zakresu pierwszej pomocy przedmedycznej, w tym obsługi i działania urządzeń typu AED (automatyczne defibrylatory zewnętrzne). Wszelkie działania podejmowane w tym zakresie mają jedną podstawę – bezpieczeństwo gości i pracowników. Zależy nam na tym, aby był to kolejny ważny krok w budowaniu kultury bezpieczeństwa całej Grupy Polskiego Holdingu Hotelowego.

Aspekt bezpieczeństwa w naszych obiektach od zawsze był dla nas bardzo ważny, stąd prośba do wszystkich gości o wyrozumiałość i pozytywne reakcje wobec egzekwowania przez hotelarzy obostrzeń sanitarnych. Aby odpoczynek w sezonie wakacyjnym mógł trwać beztrosko, musimy przestrzegać z pokorą wszelkich wytycznych i zasad, dla naszego wspólnego dobra i bezpieczeństwa.

Adam Latek

Latek Hotels, Polska Izba Hotelarzy

Bezpieczeństwo finansowe hotelu

Czy właściciele hoteli mogli mieć poczucie bezpieczeństwa finansowego w ostatnim roku? Podczas zamknięć obiektów przedsiębiorcy uruchamiali własne zasoby finansowe lub zasoby finansowe spółek powiązanych kapitałowo ze spółką hotelową. W wyniku zamknięć niektóre obiekty były nieoficjalnie wystawiane na sprzedaż i przejmowali je inni właściciele. Wstrzymano kredyty i zapomogi. Subwencje i dotacje nie były wystarczające. Rok 2020 na wielu przedsiębiorcach wymusił zmierzenie się z redukcją etatów i zamknięciem obiektu. Hotele funkcjonujące według wytycznych nie mogły się pochwalić wysoką frekwencją ani adekwatną ceną za usługi.
Jak zabezpieczyć się na wypadek globalnego kryzysu? Spoglądając analitycznie i ekonomicznie na gospodarkę światową, zauważamy, że co dekadę występują światowe kryzysy finansowe. Każdy z przedsiębiorców ma własny plan na krachy giełdowe czy czasy epidemii. Hotelarze, chcąc utrzymać obiekty, zasilają je finansowo z innego, wiodącego biznesu, jeśli taki posiadają.
Bezpieczeństwo finansowe to również świadome budowanie kapitału przez comiesięczne odkładanie rezerw księgowych na przyszłe inwestycje. Dokapitalizowanie obiektów noclegowych i rozbudowy obiektów hotelowych to również świadome inwestycje z planowanym kapitałem zwrotu. W każdym budynku, aby utrzymać jego wartość rynkową, należy dokonywać generalnych remontów: pokoi, recepcji, restauracji, spa, sali konferencyjnych i części ogólnodostępnych. To wiąże się z planowaniem nakładów również na systemy zabezpieczeń, ponieważ gość musi czuć się w hotelu bezpiecznie.
Kolejnym punktem długofalowej inwestycji jest marketing. Ponoszone koszty marketingu w budowaniu wizerunku powinno się wykazywać po stronie inwestycyjnej. Wielkim nieporozumieniem jest traktowanie marketingu jako kosztu. Spójność inwestycji w czasach po pandemii może przynieść zakładany sukces.

Adam Brzezicki

Axis Communications

Systemy monitoringu dla branży hotelarskiej

Branża hotelarska silnie odczuła negatywne skutki koronawirusowych restrykcji. W 2020 r. jej wyniki finansowe były znacząco niższe niż wyniki innych, również dotkniętych obostrzeniami sektorów gospodarki, a średnie obłożenie spadło o nawet 90%. Prognozy na kolejne miesiące wskazują, że zasady reżimu sanitarnego, choć łagodniejsze, pozostaną w obiektach hotelowych na długo. Powrót do obrotów sprzed pandemii będzie zatem zależał od tego, na ile hotelarze będą zdolni zapewnić gościom poczucie bezpieczeństwa i jak szybko dostosują swoje obiekty do funkcjonowania w nowych warunkach.

Naprzeciw wyzwaniom branży hotelarskiej wychodzi technologia. Coraz więcej obiektów borykających się z m.in. koniecznością zapobiegania gromadzeniu się gości w określonych miejscach decyduje się na zastosowanie zintegrowanych rozwiązań sieciowych – inteligentnych systemów kamer i głośników, które monitorują ruch i pozwalają na zdalne zarządzanie dostępem do określonych stref.
Kamery z funkcją rozpoznawania tablic rejestracyjnych sprawdzą się na hotelowych parkingach. System rozpozna numery samochodu gościa, który dokonał rezerwacji, i automatycznie odblokuje szlaban, a recepcjonista powita go przez interkom, wskaże konkretne miejsce postojowe i odpowie na ewentualne pytania. Dzięki zastosowaniu nowoczesnych stacji drzwiowych drzwi do budynku lub hotelowego pokoju goście mogą otworzyć za pomocą kodów QR, które otrzymają e-mailem lub SMS-em.
W hotelowych strefach relaksu znajdzie zastosowanie tzw. analiza przekroczenia limitu osób. Jeśli np. w basenie przebywać będzie komplet osób, oczekujący przed wejściem do danej strefy zobaczą na ekranie umieszczonym przy drzwiach wirtualnego asystenta, który może zachęcić do skorzystania w tym czasie z masażu. Automatyczne systemy audio mogą także pomagać w zarządzaniu muzyką w wybranych częściach hotelu, dopasowując ją np. do pory dnia.
Na podstawie danych zbieranych w czasie rzeczywistym urządzenia wyposażone w odpowiednie oprogramowanie są w stanie przewidzieć obłożenie poszczególnych stref w określonej chwili. Może to ułatwić menedżerom zarządzanie obiektem, a dzięki minimalizacji ryzyka w konsekwencji przełożyć się także na poczucie bezpieczeństwa i satysfakcji gości.

Marcin Walczuk

BCS

Hotele po pandemii

Branża hotelarska jest chyba jedną z najbardziej poszkodowanych przez pandemię COVID-19. Ograniczenia w przemieszczaniu się, przymusowe kwarantanny, zamknięte popularne kierunki wypoczynku czy po prostu zamknięte hotele w skuteczny sposób ograniczyły wpływy oraz zachwiały stabilnością całej branży. Aby móc przystosować się do wymogów świata po pandemii, nie można wstrzymać inwestycji w bezpieczeństwo gości hotelowych. Nowe rozwiązania, które pojawiły się w celu przeciwdziałania skutkom pandemii i ograniczenia jej rozprze-

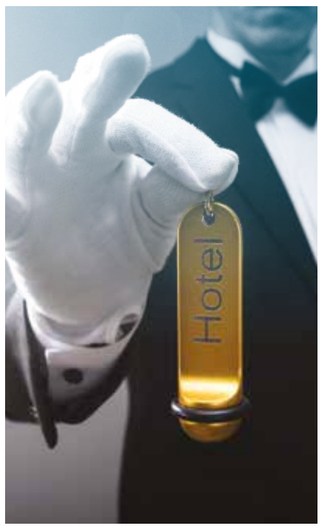
strzeniania się, z powodzeniem mogą być zastosowane również w hotelach. Będą to zarówno systemy do pomiaru temperatury ciała oparte na kamerach termowizyjnych, jak i bezdotykowe panele kontroli dostępu. Kamery wykorzystujące funkcję liczenia ludzi połączone z rejestratorem mogą monitorować kilka wejść do budynku i wyjść, sprawdzając tym samym, czy nie został przekroczony limit osób mogących jednocześnie przebywać w placówce. Pozwolą również sprawdzić, czy liczba osób w hotelu odpowiada liczbie gości w nim zameldowanych lub w razie ewakuacji czy wszyscy opuścili budynek.
Rejestratory i kamery BCS Line Ai z algorytmami sztucznej inteligencji wyposażone w funkcję rozpoznawania twarzy umożliwią porównanie osób przebywających na terenie hotelu z bazą danych gości i wychwycenie osób niepożądanych. Zastosowanie rozwiązań inteligentnych w serii BCS Line umożliwi systemowi reagowanie na zdarzenia szczególnego typu, takie jak przekroczenie linii, wtargnięcie, zbyt długie przebywanie w strefie, z opcją wskazania, jakiego typu obiekt (człowiek czy samochód) ma dany alarm uruchomić. Wykrywanie pozostawionych lub skradzionych przedmiotów też można z powodzeniem wykorzystać w monitoringu wizyjnym korytarzy hotelowych. Przy monitorowaniu parkingów nieodzowna będzie kamera do rozpoznawania tablic rejestracyjnych pojazdów, która w połączeniu z aplikacją BCS Manager ułatwi monitorowanie i przyznawanie dostępu na teren parkingu autom o właściwych numerach rejestracyjnych.
Biorąc pod uwagę, jak duże i rozległe potrafią być obiekty hotelowe, do ich zabezpieczenia potrzebne są urządzenia obsługujące znaczną liczbę kamer. Rejestratory 128-kanałowe pozwolą na monitorowanie hoteli średniej wielkości, ale po połączeniu z aplikacją BCS Manager można obsługiwać podgląd obrazów z dowolnej liczby urządzeń na jednej stacji roboczej i monitorować nawet największe obiekty. W takiej sytuacji ograniczeniem będzie tylko moc wspomnianej stacji, żeby wyświetlić odpowiednią liczbę kanałów.

Jakub Sobek

Linc Polska

Dajcie mi się po prostu wyspać

Wiele hoteli, nawet tych o najlepszej renomie, krytykowanych jest za czas obsługi w recepcji. Wielokrotnie przyjeżdżałem do hotelu po całym długim dniu pracy czy podróży i musiałem czekać w kolejce do recepcji, aby otrzymać klucz do pokoju. Na ogół okazywało się, że do wypełnienia są jeszcze karty meldunkowe, obowiązkowa do wysłuchania litania informacyjno-organizacyjno-porządkowa i dopiero wtedy otrzymywałem upragniony klucz. Najgorszy moment? Kiedy przy pokoju okazywało się, że klucz został źle zakodowany i nie otwiera drzwi. Ponownie: winda, oczekiwanie w kolejce, rozmowa w recepcji... A ja przecież chciałem się tylko wygodnie wyspać i zjeść śniadanie, tymczasem uwikłałem się w historię, która wydaje się nie mieć końca. Po takim początku dziewięć ręczników w pokoju i mydełka w wielu kolorach nie są żadnym pocieszeniem.
Zapewne można zrobić wszystko lepiej i szybciej, a każdy klient doceni podniesienie komfortu obsługi. To przecież pierwsze wrażenie jest najważniejsze, a nie można go powtórzyć.
Takie sytuacje można jednak bardzo łatwo wyeliminować, oferując klientowi dostęp bez klucza do jego pokoju. Już nie będzie trzeba pamiętać, by mieć przy sobie kartę do pokoju. Ileż to razy wychodzi się z pomieszczenia, mając pewność, że karta jest w kieszeni, by potem odkryć, że jednak jest inaczej. Zamiast tradycyjnej karty dane dostępowe wysyłane są na telefon komórkowy gościa. Wystarczy jedynie przyłożyć telefon do klamki lub zdalnie za pomocą aplikacji otworzyć drzwi. Te odblokowują się automatycznie, co jest szczególnie wygodne, kiedy ręce są zajęte bagażami i innymi podręcznymi rzeczami.
Integracja systemu płatności i hotelowych kart lojalnościowych z takim systemem przez API nie jest niczym trudnym. Wirtualny klucz otrzymujemy jeszcze przed przybyciem do hotelu, mając możliwość pominięcia recepcji. Płatność dokonywana jest automatyczne, a fakturę otrzymujemy na adres e-mail. Dla administracji hotelu znika problem zarządzania kluczami, a w tej samej aplikacji mogą zarządzać dostępami dla pracowników.
Łatwo, bezpiecznie, a co najważniejsze szybciej można w pokoju odpocząć.



Krzysztof Mika

Hikvision Poland

Bezpieczeństwo priorytetem dla banków

Technologia bardzo się rozwinęła. Jeszcze kilka lat temu szczytem możliwości kamery było wygenerowanie obrazu 2-, 3-megapikselowego. Dziś analityka zaszyta w kamerze wykrywa niepożądane zdarzenie, alarmując pracowników ochrony i umożliwiając ich szybką reakcję. Przydatną funkcją jest np. rozpoznawanie twarzy, która pozwala na identyfikację osób znajdujących się na tzw. czarnej liście, przez co uniemożliwia się im dostęp do konkretnej strefy.
To samo dotyczy samochodów zaparkowanych np. przed budynkiem banku lub chcących wjechać na parking. System odczytuje tablice rejestracyjne i na podstawie bazy danych może zaalarmować ochronę, jeśli pojazdu nie mam na liście uprawnionych.
Zaimplementowane funkcje analityczne pozwalają też wykryć niestandardowe zachowanie klienta zarówno tego w placówce, jak i oczekującego na wejście na ulicy. To ułatwienie dla operatorów w centrum monitoringu, którzy muszą śledzić obrazy czasami nawet z kilkudziesięciu kamer, a jak wiadomo, możliwości ich percepcji są ograniczone.
Pandemia wymusiła stosowanie odpowiednich rozwiązań. Chcąc dostosować się do przepisów sanitarno-epidemicznych, wykorzystuje się kamery mierzące temperaturę ciała oraz funkcję do zliczania osób, aby zachować dystans społeczny. Aktualna liczba klientów przebywających w placówce jest wyświetlana przed wejściem, dlatego każdy podchodzący do placówki wie, czy może już wejść do środka.
Dbanie o bezpieczeństwo zawsze musi być priorytetem dla banków, dlatego oprócz systemów telewizji dozorowej stosuje się również systemy kontroli dostępu umożliwiające zabezpieczenie wejścia do stref zamkniętych. Systemy te mogą korzystać z różnych metod identyfikacji, m.in. poprzez rozpoznawanie twarzy lub odcisków palców, które mogą być powiązane z danymi na karcie zbliżeniowej lub wpisaniem właściwego kodu dostępu. Połączenie kilku technologii gwarantuje, że tylko uprawniona osoba wejdzie do zabezpieczonego obszaru.
Mimo rosnącej popularności bankowości cyfrowej i nowych technologii tradycyjne oddziały banków wciąż zajmują ważne miejsce w życiu konsumenta. Dlatego bardzo ważne jest dbanie o bezpieczeństwo jego i jego finansów.

Emil Zarzecki

mBank

Wpływ pandemii na sektor finansowy

Pandemia wpłynęła na każdy aspekt naszego życia. Sektor bankowy odczuł jej skutki w każdym wymiarze swego funkcjonowania. Dla zespołów zajmujących się bezpieczeństwem w bankach ten czas stanowił nieoszacowane wcześniej wyzwanie. Zmieniła się znacząco matryca zagrożeń, których wpływ był wcześniej minimalizowany (m.in. ryzyko niedostępności usług bankowych w przypadku wystąpienia epidemii).
Obecnie istotną kwestią dla sektora jest wypracowanie standardów branżowych umożliwiających wykorzystanie najnowszych technologii z obszaru security. Mam tu na myśli m.in. technologie oparte na zaawansowanej analityce obrazu z użyciem technologii *deep learning* w systemach CCTV. Postęp w tej dziedzinie zwiększył dokładność metod uczenia się, a rosnąca skuteczność takich systemów przynosi ogromną wartość biznesową również dla branży security. Takie systemy dają duże możliwości wsparcia pracy pracowników ochrony fizycznej, dzięki czemu znacząco przyczyniają się do podniesienia poziomu bezpieczeństwa każdego chronionego obiektu czy procesu (np. procesów gotówkowych).
Kolejną ważną w mojej ocenie potrzebą sektora, wynikającą wprost ze zmieniającego się charakteru usług bankowych, tj. digitalizacji, jest automatyzacja procesów bezpieczeństwa fizycznego tam, gdzie to możliwe. Dziś placówki bankowe ewoluują i ten proces będzie trwał. Wynikająca z tej ewolucji automatyzacja procesów, poza zwiększeniem poziomu bezpieczeństwa, w dłuższym okresie przyczynia się również do obniżenia kosztów usług ochrony.
Bezdyskusyjnie czasy pracy zdalnej w trybie *home office* jeszcze bardziej podniosły znaczenie usług cyberbezpieczeństwa w każdej instytucji finansowej. W dobie coraz większej liczby ataków hakerskich i prób włamania do sieci firmowych bardzo ważnym elementem jest zapewnienie skutecznych zabezpieczeń IT w sieciach, gdzie pracują również systemy bezpieczeństwa fizycznego. Zapewnienie skutecznych metod monitorowania i usuwania podatności w infrastrukturze informatycznej organizacji to absolutny warunek must. Jego spełnienie dzisiejszy świat weryfikuje każdego dnia.

Anna Twardowska

Nedap Security Management

Nowe funkcje systemów KD

Jest wiele aspektów, które klienci biorą pod uwagę, decydując się na system kontroli dostępu. Ale z pewnością najczęściej rozpatrywane są kwestie dotyczące bezpieczeństwa systemu, jego skalowalności, wykorzystania wielu technologii kart oraz form identyfikatorów (karta, smartfon, QR kod czy tablice rejestracyjne). Istotnym aspektem jest także otwarta platforma. Integracja to słowo-klucz przy większości projektów.
Kolejną pożądaną funkcjonalnością systemów KD jest ich integracja z systemami dozoru wizyjnego, dzięki czemu klient ma możliwość z poziomu jednej aplikacji dokonać szybkiej analizy incydentu, optymalizując tym samym czas poświęcany na rozpatrywanie takich przypadków.
Klienci zwracają uwagę na możliwości integracji systemu KD z systemami zarządzania gośćmi, rezerwacji biurek oraz na wykorzystanie QR kodów i smartfonów zamiast standardowych kart. Coraz częściej poruszanymi tematami są otwarte standardy pozwalające na podłączanie czytników innych producentów, bez konieczności rezygnacji z szyfrowanej komunikacji.
Firmy z sektora finansowego zwracają natomiast większą uwagę na bezpieczeństwo systemów kontroli dostępu. Istotne jest tu stosowanie rozwiązań, które zapewniają szyfrowanie na każdym poziomie komunikacji. Dużą wagę przykładają do rozwiązań w zakresie ochrony przed cyberatakami. Zatem mechanizmy pozwalające na przeniesienie kluczy szyfrujących z czytnika na kontroler czy wykorzystanie certyfikatów do uwierzytelniania kontrolerów podłączanych do systemów mają duże znaczenie. Coraz częściej spotykamy się także z wymogiem wykorzystania standardu 802.1x, który umożliwia weryfikację dostępu kontrolera SKD do sieci LAN.
Tendencja do pracy w trybie hybrydowym oznacza coraz częstsze stosowanie biurek typu hot desk. W związku z brakiem przypisanego na stałe danej osobie biurka pojawia się potrzeba zorganizowania przestrzeni do pozostawiania swoich rzeczy. Z tego względu coraz większego znaczenia nabierają Lockery, czyli systemy szafek zarządzanych z poziomu systemu kontroli dostępu. Ten kierunek pozwala na wprowadzenie optymalizacji w zakresie efektywniejszego wykorzystania powierzchni biurowej.

BHP=HSE

Bezpieczeństwo i higiena pracy to multidyscyplinarna dziedzina wiedzy, zajmująca się bezpieczeństwem, zdrowiem i dobrem ludzi zarówno w pracy, jak i poza nią, popularnie znana jako HSE (Health – Zdrowie, Safety – Bezpieczeństwo, Environment – Środowisko).

Tomasz Guzikowski

W obecnych czasach, kiedy polscy przedsiębiorcy przykładają coraz większą wagę do kwestii bezpieczeństwa (nie tylko swoich pracowników), zapewnienia ciągłości dostaw i produkcji, ochrony środowiska, a także swoich kontraktorów, lokalnej społeczności i wizerunku w przestrzeni prowadzonej działalności, tradycyjnie rozumiane obszary, takie jak BHP, odchodzą pomału do lamusa bądź stanowią tylko mały element w układance, jaką jest bezpieczne środowisko pracy.

W zależności od wielkości podmiotu, jego struktury organizacyjnej i otoczenia, w jakim funkcjonuje, ale też dojrzałości organizacji, obszary te przybierają różne formy i mogą mieć zróżnicowany schemat. Oczywiście ramy funkcjonowania służb BHP oraz ich strukturę i obowiązki określają przepisy prawa. Jednak już dawno liczące się firmy zrozumiały, że takie podejście jest niewystarczające. Istnieje wiele norm i dobrych praktyk, które podpowiadają pracodawcom, w jaki sposób efektywnie zarządzać bezpieczeństwem w organizacji.

Szczególnie ma to zastosowanie w przemyśle, który charakteryzuje się ogromną różnorodnością - zarówno w zakresie stosowanych substancji i procesów, jak i urządzeń technologicznych. Ilości i rodzaje stosowanych substancji, wielkości parametrów operacyjnych, rodzaj i poziom stosowanych rozwiązań technologiczno-procesowych, charakterystyka lokalizacji oraz jakość systemu zarządzania bezpieczeństwem to główne elementy wpływające na rodzaj powstających zagrożeń i ich przyczyny. Przyczyną źródłową wielu katastrof przemysłowych są przede wszystkim błędy i niedopatrzenia w zarządzaniu bezpieczeństwem i ochroną środowiska. Ponadto dużą rolę w eskalacji skutków katastrof przemysłowych przypisuje się tzw. efektowi domina.

W ostatnich latach wzrost złożoności i różnorodności procesów chemicznych spowodował zwiększone ryzyko powstania niepożądanych zdarzeń. W konsekwencji odnotowano poważną liczbę pożarów, wybuchów czy skażeń środowiska. Analiza ponad 700 wypadków w przemyśle chemicznym wykazała, że ok. 30% z nich było spowodowanych awarią techniczną, 9% niewłaściwym przebiegiem reakcji chemicznej, a za ponad 48% wypadków odpowiadały tzw. błędy ludzkie.

W dużych zakładach produkcyjnych, szczególnie w zakładach chemicznych czy rafineriach, które najczęściej są zakwalifikowane do kategorii zakładów zwiększonego bądź dużego ryzyka wystąpienia awarii przemysłowej, wachlarz możliwych zagrożeń jest bardzo duży. Zapewnienie bezpieczeństwa nie jest tu proste i wymaga szerokiego podejścia, obejmującego zarówno kwestie związane z bezpieczeństwem prowadzonych procesów przemysłowych, jak

WEDŁUG WSPÓLNEGO KOMITETU MOP (MIĘDZYNARODOWEJ ORGANIZACJI PRACY) I WHO (ŚWIATOWEJ ORGANIZACJI ZDROWIA) DS. BEZPIECZEŃSTWA PRACY:

Główny nacisk na zdrowie zawodowe koncentruje się na trzech różnych celach: (i) utrzymanie i promowanie zdrowia i zdolności do pracy pracowników; (ii) poprawa środowiska pracy, aby stać się sprzyjającym bezpieczeństwu i zdrowiu oraz (iii) rozwój organizacji pracy i kultury pracy w kierunku wspierającym zdrowie i bezpieczeństwo w pracy, a tym samym również sprzyja pozytywnemu klimatowi społecznemu i sprawnemu funkcjonowaniu oraz może zwiększyć wydajność przedsiębiorstw. Pojęcie kultury pracy ma w tym kontekście oznaczać odbicie podstawowych systemów wartości przyjętych przez dane przedsiębiorstwo. Taka kultura znajduje odzwierciedlenie w praktyce w systemach zarządzania, polityce kadrowej, zasadach uczestnictwa, politykach szkoleniowych i zarządzaniu jakością przedsiębiorstwa.

i aktywnością zawodową pracowników odpowiedzialnych za prowadzenie tych procesów oraz prace utrzymaniowe, konserwacyjne, modernizacyjne i remontowe. Najczęściej takie zakłady wdrażają zintegrowane systemy bezpieczeństwa, które w sposób usystematyzowany pozwalają na zarządzanie bezpieczeństwem na każdym szczeblu organizacji. Obszar ten to również ciągłe doskonalenie, czyli – zgodnie z tzw. cyklem Deminga – planowanie, organizowanie, wdrażanie i monitorowanie działań korygujących dla osiągnięcia konkretnego celu.

Nieodłącznym elementem systemu zarządzania bezpieczeństwem jest również budowanie kultury bezpieczeństwa w organizacji, czyli zespół uznawanych wspólnie wartości, warunków, sposobów postępowań i zachowań uznawanych wspólnie, indywidualnie i grupowo w odniesieniu do zorganizowania systemu zapobiegania i ochrony przed awariami i wypadkami.

CORAZ BEZPIECZNIEJ

Poziom bezpieczeństwa w przemyśle od lat 60. bardzo się poprawił. W początkowej fazie starano się ograniczać liczbę awarii i wypadków, inwestując w nowe i bezpieczniejsze rozwiązania techniczne. Następnie skupiono się na zwiększaniu standardów pracy załogi i podnoszeniu świadomości wagi bezpieczeństwa poprzez dodatkowe szkolenia, systemy motywacyjne, ale również dokonując właściwej selekcji kandydatów do pracy. W kolejnym etapie zaczęto wprowadzać elementy zarządzania bezpieczeństwem oparte głównie na analizie zagrożeń i ocenie ryzyka.

Niemniej organizacje szybko się zorientowały, że kolejne działania nie ograniczają wypadkowości, a awarie nadal się zdarzają. Dlatego zaczęto tworzyć warunki do rozwoju i budowania kultury bezpieczeństwa w organizacjach, główny nacisk kładąc na relacje pracownik – organizacja oraz efektywną komunikację.

Stąd też wiele organizacji inwestuje w rozwój nie tylko obszarów związanych stricte z bezpieczeństwem pracy. Oprócz celów związanych typowo np. z wielkością produkcji i sprzedaży, ograniczeniem liczby wypadków czy awarii

stawiają sobie coraz ambitniejsze cele, by utrzymać jak najwyższą konkurencyjność na rynku.
Rozwój technologii pozwala na lepsze zabezpieczenie pracowników. Przykładami takich zabezpieczeń zbiorowych może być np. system zabezpieczeń, zamknięć i oznaczeń LOTO, który podnosi poziom bezpieczeństwa pracowników, zwłaszcza służb utrzymania ruchu. Dzięki niemu eliminuje się liczne zagrożenia wynikające z błędów ludzkich powstałych np. podczas napraw lub konserwacji różnego rodzaju maszyn i urządzeń, których niekontrolowane uruchomienie może stanowić zagrożenie zdrowia lub życia ludzi. Środki ochrony indywidualnej, które mają na celu jak najlepszą ochronę przed wpływem czynników szkodliwych i niebezpiecznych, są coraz wyższej jakości i coraz bardziej komfortowe w użytkowaniu.
Na rynku pojawia się też coraz więcej bardziej skutecznych elektronicznych systemów zabezpieczeń. Przykładem mogą być np. systemy antykolizyjnej pracy w przestrzeniach magazynowych, systemy lokalizujące i monitorujące pracowników, bazujące na technologii wykrywania przechyłu i bezruchu, które pozwalają na podjęcie natychmiastowej akcji ratowniczej w sytuacji wystąpienia zagrożenia, a także systemy łączności przemysłowej zaprojektowane do pracy w trudnych warunkach, szczególnie ważne w strefach, gdzie jest duże zapylenie i hałas czy zagrożenie wybuchem.
W służbie bezpieczeństwa projektuje się również inne elektroniczne systemy, takie jak systemy kontroli dostępu, które pozwalają na ograniczony dostępu do stref, pomieszczeń, maszyn czy urządzeń wyłącznie osobom uprawnionym, które posiadają odpowiednie i aktualne kompetencje, w tym szkolenia i wymagane uprawnienia.
Ponadto kamery przemysłowe monitorujące pracę (nie tylko urządzeń) i ostrzegające np. przed wysoką temperaturą czy drganiami, a także pracowników, którzy np. nie stosują wymaganych w danym obszarze środków ochrony indywidualnej (kasków, okularów czy kamizelek odblaskowych).

WIĘCEJ NIŻ REGULACJE

Obecnie pojęcie „bezpieczeństwo i higiena pracy" odnosi się nie tylko do prawnych wytycznych i procedur, ale także do programów, które chronią bezpieczeństwo, dobrostan

ZGODNIE Z DEFINICJĄ WHO „(...) ZDROWIE ZAWODOWE ZAJMUJE SIĘ WSZYSTKIMI ASPEKTAMI BEZPIECZEŃSTWA I HIGIENY PRACY I KŁADZIE SILNY NACISK NA PIERWOTNE ZAPOBIEGANIE ZAGROŻENIOM". ZDROWIE ZOSTAŁO ZDEFINIOWANE JAKO „STAN PEŁNEGO FIZYCZNEGO, PSYCHICZNEGO I SPOŁECZNEGO SAMOPOCZUCIA, A NIE TYLKO BRAK CHOROBY LUB UŁOMNOŚCI". ZDROWIE ZAWODOWE JEST WIELODYSCYPLINARNĄ DZIEDZINĄ OPIEKI ZDROWOTNEJ, UMOŻLIWIAJĄCĄ JEDNOSTCE PODJĘCIE ZAWODU W SPOSÓB, KTÓRY POWODUJE NAJMNIEJSZĄ SZKODĘ DLA JEJ ZDROWIA.

i zdrowie każdej osoby zaangażowanej w pracę lub zatrudnionej. Ogólnym celem każdego programu z tego obszaru jest stworzenie najlepszego, bezpiecznego środowiska pracy i zmniejszenie ryzyka wypadków, obrażeń i ofiar śmiertelnych w miejscu pracy.
Każda organizacja, bez względu na to, co robi, ma obowiązek przestrzegania standardów bezpieczeństwa i higieny pracy. W przeciwnym razie jest odpowiedzialna za wszelkie szkody lub wypadki, które wystąpią w związku z jej działalnością. Firma nie tylko ma prawny i finansowy obowiązek przestrzegania norm bezpieczeństwa i higieny pracy, ale także moralny obowiązek dbania o dobro swoich pracowników.
Działania podejmowane w tym zakresie chronią również zdrowie klientów i innych osób, które mogą być dotknięte działalnością organizacji, a także ogółu społeczeństwa. Gdy procedury bezpieczeństwa i higieny pracy są przestrzegane prawidłowo, mogą pomóc w zapobieganiu wypadkom oraz zmniejszyć ryzyko obrażeń i chorób pracowników. Pozwolą również obniżyć koszty związane ze zwolnieniem chorobowym, opieką medyczną i świadczeniami z tytułu niepełnosprawności. To z kolei sprawia, że koszty jednostkowe wytworzenia produktu również są niższe, mniejsza jest liczba awarii i wypadów (przestojów) produkcyjnych.
Niezależnie od rodzaju działalności organizacji nieszczęśliwy wypadek czy uszczerbek na zdrowiu może zdarzyć się zawsze. Każda praca naraża ludzi na zagrożenia, obciążenia występujące przy pracach ręcznych, kontakt z niebezpiecznymi maszynami lub substancjami niebezpiecznymi, energią

elektryczną, pracą z monitorem ekranowym, a nawet zagrożenia psychologiczne, takie jak stres. Powodem, dla którego nie ma jeszcze większej liczby wypadków i chorób spowodowanych pracą, jest to, że systemy prewencyjne są budowane przez pokolenia. Stan bezpieczeństwa nie rodzi się przypadkowo. Większość wypadków zdarza się, ponieważ nie udało się im zapobiec.

WYMIAR LUDZKI I BIZNESOWY

Każdego dnia ludzie umierają w wyniku wypadków przy pracy lub chorób związanych z pracą. Łącznie na świecie to ponad 2,78 mln zgonów rocznie. Ponadto każdego roku dochodzi do około 374 mln urazów związanych z pracą, co skutkuje średnio ponad 4-dniowymi nieobecnościami w pracy. Koszty ludzkie związane z codziennymi przeciwnościami losu są ogromne, a obciążenie ekonomiczne związane ze złymi praktykami w zakresie bezpieczeństwa i higieny pracy szacuje się na 3,94% światowego produktu krajowego brutto rocznie[1].
W Polsce w 2019 r. było 83 205 osób poszkodowanych w wypadkach, w tym 184 osoby w wypadkach śmiertelnych oraz 396 osób w wypadkach ciężkich. Natomiast liczba zatrudnionych w warunkach zagrożenia – czyli takich, w których występowały przekroczenia najwyższych dopuszczalnych stężeń i natężeń czynników szkodliwych w środowisku pracy – wynosiła w 2019 r. 72,9 w przeliczeniu na 1000 zatrudnionych[2].
Co ważne, firmy ubezpieczeniowe i banki są szczególnie uczulone na ryzyko finansowe w związku z zagrożeniami środowiskowymi i procesowymi. Chcą wiedzieć, jaki może być potencjalny wpływ oddziaływania produkcji na środowisko i majątek oraz jakie ryzyko finansowe, w tym ubezpieczeniowe, podejmują czy to przy finansowaniu czy ubezpieczaniu danego zakładu produkcyjnego lub inwestycji. Ponadto odbiorcy i użytkownicy produktów również stają się coraz bardziej wymagający. Produkty powinny być przyjazne dla środowiska, bezpieczne w użytkowaniu, a firmy powinny się legitymować stosownymi certyfikatami uwiarygodniającymi je na rynku.

1 Źródło: dane International Labour Organisation
2 Źródło: dane GUS

BEZPIECZEŃSTWO W STRATEGII CIECH-u – DOBRA PRAKTYKA

Wiele firm w polityce biznesowej idzie o krok dalej. Przykładem takich działań może być np. opracowanie i wdrożenie strategii ESG (*Environment* – Środowisko, *Social* – Społeczeństwo, *Governance* – Ład korporacyjny), której celem nadrzędnym jest zrównoważony rozwój.
Dla Grupy CIECH odpowiedzialne prowadzenie biznesu zawsze było podstawową zasadą, ponieważ rzeczywistą wartość w długim horyzoncie może budować tylko biznes odpowiedzialny, dbający, oprócz krótkoterminowych parametrów finansowych, o stabilność i zrównoważone relacje z otoczeniem – zarówno środowiskiem naturalnym, z którego zasobów korzysta organizacja, jak i z ludźmi wewnątrz firmy i dookoła niej.
W ramach strategii ESG Grupa CIECH przyjęła osiem zobowiązań. Trzy z nich dotyczą środowiska, trzy ludzi i społeczeństwa, a dwa relacji z innymi, przejrzystości i ładu korporacyjnego.
W grupie zobowiązań dla ludzi i społeczeństwa na pierwszym miejscu jest oczywiście bezpieczeństwo. Celem nadrzędnym jest zero wypadków. Działalność produkcyjna wiąże się z ryzykiem – pracownicy na co dzień mają do czynienia m.in. z wysokim ciśnieniem i temperaturą, substancjami o działaniu drażniącym czy ruchomymi częściami urządzeń. Można je opanować i zminimalizować tylko poprzez rygorystyczne przestrzeganie wysokich standardów bezpieczeństwa i wymaganie tego samego od wszystkich podwykonawców i kooperantów. Praca nad kulturą bezpieczeństwa jest ciągła, długoterminowa i wymaga zaangażowania od wszystkich pracowników. Na każdym szczeblu organizacji funkcjonują matryce celów w zakresie bezpieczeństwa i warunków pracy, a procesy związane z raportowaniem w tym obszarze są zdigitalizowane, pozwalając na obserwację najważniejszych wskaźników w czasie rzeczywistym. Grupa CIECH ma ambicję być jednym z najlepszych pracodawców w swojej branży, dlatego ciągłe doskonalenie procesów bezpieczeństwa to jeden z głównych filarów jej ogólnej strategii.

Plan minimum to system zarządzania bezpieczeństwem i higieną pracy, w tym polityka, określone i mierzalne cele, planowanie działań, wskazanie osób odpowiedzialnych, jasne procedury, programy szkoleniowe dostosowane do potrzeb poszczególnych grup pracowników, właściwa komunikacja, zarządzanie ryzykiem zawodowym, a także zapobieganie i reagowanie na wypadki i awarie.
Dbałość o zdrowie i bezpieczeństwo to nie tylko odpowiedzialność społeczna. Ma również sens biznesowy i należy uznać ją za równie ważną, jak osiągnięcie innego kluczowego celu biznesowego. Jak określa Europejska Agencja Bezpieczeństwa i Zdrowia w Pracy: *Przedsiębiorstwa przestrzegające wyższych norm bezpieczeństwa i higieny pracy osiągają lepsze wyniki i mają stabilniejszą pozycję. Każde euro zainwestowane w BHP zwraca się w postaci 2,2 euro, a stosunek kosztów poprawy bezpieczeństwa i higieny pracy do jego korzyści wypada na plus.*

TOMASZ GUZIKOWSKI

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

O bezpiecznym szpitalu

w konwencji burzy mózgów

W artykule poruszającym tematykę bezpiecznego lotniska (a&s 1/2021) pozwoliłem sobie zauważyć, że to obiekt wyjątkowy, trudny, pełen pułapek projektowych. Obecnie, przygotowując się do podjęcia tematyki szpitala, analizując problematykę wyposażenia instalacji szpitalnych, doznałem olśnienia – doszedłem do wniosku, że jest ona co najmniej podobnie skomplikowana, a niekiedy nawet bardziej. Moich przemyśleń nie opieram na doświadczeniach z konkretnych realizacji, ale na gruntownej analizie tego tematu. To raczej „burza mózgów", stawianie nieoczywistych pytań, szukanie nieszablonowych rozwiązań.

Michał Zalewski

Zagadnień, które chciałbym poruszyć, jest wiele. Starałem się wybrać ważne i ciekawe, a mam nadzieję, że również zaskakujące. Pierwszy temat będzie nawiązywał do konkretnej integracji, doskonale pasującej do zilustrowania pytania o zasadność i sens integracji, czy to konieczność, okazja, fanaberia czy kłopoty.

Na początku tło: szpital to miejsce szczególne, narażone na sytuacje kryzysowe, gdzie walczy się o życie pacjentów. W sytuacji kryzysowej warunkiem koniecznym do szybkiego, elastycznego, a jednocześnie skutecznego reagowania na pojawiające się zagrożenia i nieprzewidziane komplikacje czasem prostych przypadków klinicznych jest szybka, pewna i skuteczna komunikacja. Szpital posiada kilka systemów komunikacyjnych: DSO, instalacja przywoławcza, interkomy, system telefoniczny. Ponadto wiele telefonów komórkowych, które potencjalnie umożliwiają komunikację, posiada zarówno personel, jak i pacjenci oraz osoby odwiedzające. Każdy z tych systemów najczęściej działa indywidualnie, pełni przypisane mu funkcje. Nie są mi znane realizacje integracji takich systemów, a w tym wypadku moim zdaniem to konieczność, a już na pewno okazja.

System DSO z racji pełnionych funkcji wyróżnia niezawodność działania gwarantowana przez cechy tego systemu: redundancja i kontrola ciągłości linii głośnikowych, redundancja wzmacniaczy i procesorów, zespoły kablowe o odpowiedniej odporności ogniowej. To na plus tego systemu. Na minus: ograniczona liczba stref rozgłaszania uniemożliwiająca elastyczne komunikowanie do określonych obszarów, ograniczone możliwości rozgłaszania w salach operacyjnych.

System przywoławczy obejmuje funkcje nowoczesnych systemów opartych na technologii IP: elastyczne, a jednocześnie precyzyjne kierowanie komunikatów do określonych odbiorców, zarówno informacji tekstowych, jak i połączeń głosowych oraz funkcje przywołania pomocy, funkcje priorytetowości komunikatów. Są też takie systemy przyzywowe, które pozwalają na integrację z urządzeniami mobilnymi, i warto ich szukać.

System telefoniczny to bardzo precyzyjny system komunikacji pomiędzy poszczególnymi osobami, ale przewodowy pozostaje mało elastyczny. Uzupełniony o komunikację DECT jest bardziej skuteczny, ale wymaga od personelu zadbania np. o stan jego baterii i noszenia dodatkowego urządzenia. No i wreszcie „system" składający się z prywatnych czy prywatno-służbowych telefonów komórkowych personelu, pacjentów oraz odwiedzających.

Jak widać, jest wiele urządzeń, systemów, funkcji i możliwości – wszystkie służą do komunikacji, mniej lub bardziej wyrafinowanej, mniej lub bardziej skutecznej. Każdy z nich ma wyjątkowe cechy stanowiące ich zalety i inne będące ich ograniczeniami.

A gdyby tak pokusić się o zintegrowanie tych systemów? Najpierw trzeba by było odpowiedzieć na pytanie, po co. Otóż zastanowiłbym się nad integracją DSO i systemu przywoławczego, tak by w przypadku konieczności szerokiego, głośnego poinformowania jednocześnie wielu osób było możliwe skuteczne nadanie komunikatów za pośrednictwem systemu DSO z różnych miejsc, nie tylko z poziomu mikrofonu DSO. Z kolei przesyłanie odpowiednich komunikatów w drugą stronę – z DSO do systemu przywoławczego – pozwoliłoby na powiadomienie o zagrożeniach, np. osoby przeprowadzające operacje w obszarach, w których nie można umieszczać głośników DSO. Potencjalna integracja instalacji centrali telefonicznej z DSO natomiast zapewniłaby dowolnej osobie posiadającej odpowiednie uprawniania nadanie precyzyjnego komunikatu bezpośrednio, bez konieczności szukania pomocy służb technicznych. Wiele central ma taką funkcjonalność, zastanówmy się nad ich wykorzystaniem. Są dostępne na rynku systemy przyzywowe, które pozwalają na integrację z nimi urządzeń mobilnych.

Kończąc ten wątek, chciałbym poruszyć temat wykorzystania prywatnych telefonów komórkowych w komunikacji w szpitalu. Skłonienie użytkowników do udostępnienia swoich numerów telefonów może być trudne, ale gdyby opracować aplikację komunikacyjną, do której logowanie następuje poprzez sczytanie kodu QR na wejściu do szpitala i po wyjściu wylogowanie się tą samą metodą? Można by wtedy w systemie telekomunikacyjnym utworzyć plan powiązań konkretnych numerów komórkowych z funkcjami personelu, swego rodzaju mapę przekierowań połączeń i komunikatów do osób rzeczywiście przebywających w szpitalu, wg ich ścisłych kompetencji i bez narażania ich na naruszanie prywatności poza godzinami pracy. Pacjenci zaś otrzymaliby możliwość dokładnej komunikacji w sprawach bieżących, porządkowych. W tym konkretnym przypadku nie ma mowy o fanaberii. Należy jednak pamiętać, by zawiłości integracji nie spowodowały dysfunkcji podstawowych cech systemów, bo wtedy pojawią się kłopoty.

Nie byłbym sobą, gdybym nie poruszył kwestii uruchomień i problemów z tym związanych. Zahaczę o nie przy okazji drugiego wątku, trochę oderwanego na pierwszy rzut oka od branży security. A jest niezwykle ważny, dotyczy zasilania budynku w energię elektryczną. Chciałbym zwrócić uwagę na tzw. strażnika mocy. Jest to bardzo precyzyjny układ automatyki pozwalający na odłączanie zasilania odbiorników o niższym priorytecie i utrzymywanie dla istotnych takich jak zasilanie sali operacyjnej zarówno aparatury medycznej, jak i wentylacji czy klimatyzacji. Taki układ sterowania powinien powstać po szczegółowej analizie bilansu mocy wykonanej równolegle z analizą operacyjną potrzeb szpitala w sytuacjach kryzysowych.

Często byłem świadkiem i uczestnikiem dyskusji, czy np. systemy SSP, DSO, CCTV, wentylacji i klimatyzacji, czy też system telekomunikacyjny budynku powinno się zasilać z agregatu. Odpowiedź jest oczywista: moim zdaniem tak, ale należy zadbać o możliwość mniej lub bardziej automatycznego odłączania poszczególnych urządzeń w sytuacjach awaryjnych. Ważne, by przy projektowaniu poszczególnych systemów zaplanować takie działania, przeliczyć wyniki (spadki zapotrzebowania mocy), zawrzeć te dane w instrukcjach budynku, by obsługa techniczna w sytuacji kryzysowej mogła podejmować decyzje oparte na konkretnych danych, by nie była skazana na poszukiwanie takich informacji w dokumentacji powykonawczej.

Drugą w tym wątku kwestią jest uruchamianie i testowanie systemu zasilania awaryjnego. W zwykłych budynkach w ramach testów systemu SZR (system zasilania rezerwowego) i strażnika mocy wykonuje się tzw. Blackout Test / Black Building Test. Budynek opuszczają użytkownicy, natomiast osoby, które muszą pozostać, powiadamia się o testach. Następnie symuluje się poszczególne awarie, następuje sprawdzenie, czy wszystkie niezbędne urządzenia działają prawidłowo, np. czy windy nie utknęły między piętrami, czy działa wentylacja pożarowa, czy w systemie CCTV nie zawiesiły się switche i serwery.

Ale jak przeprowadzić tego typu testy w szpitalu? Zapnę artykuł pewną klamrą, na lotnisku takie testy przeprowadzałem, nie jest łatwo, ale można. Czy można w szpitalu poprzestać na sprawdzeniu działania agregatu bez obciążenia? Czy można takie testy przeprowadzić w trakcie pracy szpitala? Jak zorganizować, przygotować i przeprowadzić takie testy? Moim zdaniem projektant układu zasilania powinien zadać sobie takie pytania, zapewne jeszcze inne, być może trudniejsze. Pozostawienie ich bez odpowiedzi i rozwiązań skazuje służby techniczne na brak możliwości przeprowadzania takich testów, co może skutkować sprowadzeniem niebezpieczeństwa na pacjentów.

Im dłużej zastanawiam się nad odpowiedziami, tym więcej widzę problemów. Mam nadzieję, że poruszając ten temat, wyprowadziłem Czytelnika poza strefę komfortu, wszak celem moim było pobudzenie do refleksji i do dyskusji na ten temat. Projektując systemy i instalacje w szpitalu, przewidując ich potencjalne awarie, starając się znajdować sposoby na ograniczanie ich skutków, zawsze będziemy życzyć sobie, by nigdy nie były potrzebne, ale przewidywać je trzeba.

MICHAŁ ZALEWSKI

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

Wektory ataków socjotechnicznych

Tomasz Dacka

Budujemy zaawansowany system zabezpieczeń. Chronione obiekty lub urządzenia wyposażamy w kontrolę dostępu, system dozoru wizyjnego, system sygnalizacji włamania i napadu. Nad wszystkim czuwa ochrona. Budujemy też odpowiednie procedury, integrujemy technikę. Uważamy, że mamy w miarę „szczelny" system ochrony.

Potencjalny intruz miałby spore problemy, aby przełamać te wszystkie zabezpieczenia, i doskonale o tym wie. Na koniec dnia okazuje się, że jednak nieproszony gość dostał się do chronionych stref. W jaki sposób? Jak wielkie musi być nasze zdziwienie, gdy okaże się, że praktycznie sami go tam wpuściliśmy. W miłej atmosferze pomogliśmy mu pokonać wszystkie, tak mozolnie przez nas budowane zabezpieczenia. Bez wzbudzenia alarmu, bez zidentyfikowania incydentu, bez dźwięku tłuczonego szkła…

Tak właśnie działa inżynieria społeczna i ataki na niej oparte. Przyjrzyjmy się zatem, z czym tak naprawdę mierzymy się codziennie, co nam zagraża i w jaki sposób możemy to ryzyko adresować.
Inżyniera społeczna *(social engineering)* lub socjotechnika to nic innego jak działanie mające na celu wyłudzenie informacji za pomocą różnych metod manipulacji. Jest najbardziej rozpowszechnioną metodą ataków zarówno na pojedyncze osoby, jak i firmy czy grupy społecznościowe. Dobrze przygotowany atak socjotechniczny trudno wykryć ze względu na to, że w głównej mierze jest wymierzony bezpośrednio w człowieka, wykorzystuje jego zaufanie i przyzwyczajenia. Jest w stanie sprawić, że wykonujemy czynności, których byśmy nie wykonali.

PRZED CZYM ZATEM NALEŻY SIĘ CHRONIĆ, JAKIMI ZASADAMI KIERUJE SIĘ ZAZWYCZAJ INTRUZ PRÓBUJĄCY WYKORZYSTAĆ NAS JAKO ŚRODEK DO CELU?

Być lubianym, grzecznym i uprzejmym – kiedy ktoś jest lubiany, zachowuje się w sposób uprzejmy, a zarazem prosi o rzeczy, które wydają się nam w pewnym stopniu uzasadnione, tym chętniej taką prośbę spełniamy. Może to być miła e-mailowa prośba od (tak nam się przynajmniej wydaje) koordynatora ochrony o nieuzbrajanie systemu alarmowego w danej strefie z powodu długiego i ważnego spotkania, z notyfikacją, że dla komfortu ochrony on sam specjalnie przyjedzie i będzie ją (strefę) nadzorował. Brzmi zupełnie inaczej niż surowy nakaz, który od razu budzi w nas niechęć i podejrzenia.

Konsensus – odwołuje się do zasady, że bez dokładnego wskazania, co należy w danej sytuacji robić, wielu ludzi zachowuje się w sposób, w jaki ich zdaniem zachowałaby się większość. W takiej sytuacji przekonujemy nasz cel, że odmowa spełnienia prośby jest czymś dziwnym, bo przecież nikt wcześniej tego nie negował. Jest to kluczowa cecha wykorzystywana jako wektor ataku przy starcie lub zmianach w organizacji bezpieczeństwa. Do tej pory przepuszczałem kobiety przodem w drzwiach, co prawda nie było wtedy systemu kontroli dostępu, ale dobre maniery przecież nadal mnie zobowiązują. Inną, sprawdzoną metodą jest zamieszczanie wielu pochlebnych opinii nt. strony internetowej czy danego produktu. Same opinie są oczywiście tak samo fałszywe jak strona, do której prowadzą, ale automatycznie budują w nas zaufanie.

Autorytet i zastraszanie – zazwyczaj trudno nam odmawiać osobom o wyższej pozycji biznesowej lub zaufanej profesji społecznej. Atakujący może wcielić się w policjanta, wysoko postawioną na szczeblu firmowym osobę, strażaka czy lekarza i próbować wykorzystać tę pozycję.

„Unikat" w trybie pilnym – chyba każdy z nas napotkał wielką okazję (np. cenową), która przejdzie koło nosa, jeśli nie zdecydujemy się właśnie teraz z niej skorzystać. Tak, to jest również metoda socjotechniczna wykorzystywana głównie w sprzedaży. W taki sposób można również zbierać dane logowania użytkowników (np. obiecując usługę darmowego dostępu do pewnych usług, m.in. Microsoft 365), licząc na to, że w pośpiechu osoby podadzą dokładnie takie same loginy, jakie wykorzystują np. w swojej bankowości elektronicznej.

DLACZEGO W CELU DOBREGO PRZYGOTOWANIA ATAKU SOCJOTECHNICZNEGO TRZEBA PRZEBIĆ SIĘ W PIERWSZEJ KOLEJNOŚCI M.IN. PRZEZ ZABEZPIECZENIA FIZYCZNE?

Przejdźmy na chwilę na drugą stronę barykady. Aby nasz atak socjotechniczny był skuteczny, musimy zebrać o celu jak najwięcej precyzyjnych informacji. Zazwyczaj zbieranie danych (imiona, nazwiska, stanowiska) nie nastręcza problemu, natomiast rozpoznanie środowiska pracy już tak. Dla przygotowującego atak wszystkie informacje są cenne: nazwa działu, liczba osób, struktura organizacyjna, numery telefonów, adresy e-mailowe, faktury, zamówienia. Jak zatem tego dokonać? Jak wejść w posiadanie danych operacyjnych, które pomogą nam uwierzytelnić nasz przekaz?

- **CENNE ŚMIECI** *(dumpster diving)*

Niezabezpieczone pojemniki, kontenery na śmieci są świetnym miejscem pozyskania wielu cennych danych. Mimo że migrujemy obecnie do świata cyfrowego, wciąż wiele organizacji bazuje na papierowym modelu wymiany informacji. W śmieciach zresztą można znaleźć nie tylko papier, ale także inne środki przekazu informacji, np. płyty, pamięci przenośne, a nawet dyski twarde (sic!). Dlatego tak ważne jest, aby również pomieszczenia (strefy) przeznaczone na śmietniki zabezpieczać za pomocą środków technicznych i kontrolować dostęp do nich. Dobrą praktyką jest również wdrożenie procedur dotyczących zasad pozbywania się nośników danych.

- **PATRZ ZA SIEBIE** *(shoulder surfing)*

Temat ten był wielokrotnie poruszany w mediach społecznościowych w kontekście osób podróżujących środkami transportu publicznego. Zostawiony laptop osób publicznych, z którego można czytać jak z książki,

jest chyba najlepszym tego przykładem. W takim wypadku podejrzenie haseł, kodów PIN również nie stanowi problemu. Co sprytniejsi potrafią wykorzystywać specjalne lornetki (długi dystans) czy nawet nasz system CCTV. Z tego powodu tak istotne jest budowanie bezpiecznego środowiska pracy, szczególnie dla osób, które są w posiadaniu kluczowych informacji. Ważne, by mieć wdrożony nawyk blokowania komputera za każdym razem, kiedy od niego odchodzimy.

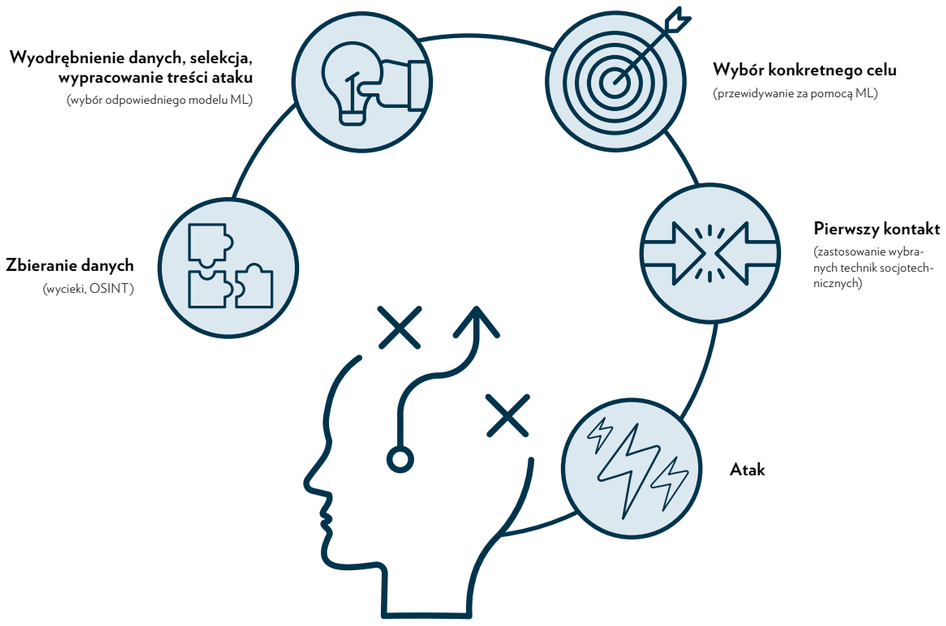
- **NA PRZEKÓR ROZLICZALNOŚCI** *(tailgating)*

Jest to bez wątpienia wyzwanie dla każdego procesu realizowanego za pomocą systemu kontroli dostępu. To nic innego, jak wchodzenie na tzw. plecach bez autentykacji i autoryzacji osoby przekraczającej kontrolowane przejście (oczywiście jeśli zabezpieczenia mechaniczne na to pozwalają). Odmianą tego typu zachowania jest tzw. *piggy backing*, czyli sytuacja, kiedy pracownik wpuszcza osobę bez uprawnień do wejścia do danej strefy. Przykłady można mnożyć: obładowany paczkami kurier, serwis sprzątający proszący o przytrzymanie drzwi, aby mógł wjechać z wózkiem, ktoś, kto „zgubił" swoją kartę, przekonująco proszący o pomoc lub po prostu osoba, która z premedytacją działa wspólnie i w porozumieniu z osobą, którą wpuszcza, a której wejście nie zostaje odnotowane w systemie kontroli dostępu.

WYMIENIONE METODY NAJCZĘŚCIEJ SĄ MATERIALIZOWANE ZA POMOCĄ ATAKÓW – TAKICH JAK PHISHING, VISHING, WHALING.

Phishing – jest kombinacją socjotechniki i budowania fałszywych źródeł, do których chcemy, aby nasza ofiara dotarła (np. fałszywa strona banku czy innej popularnej usługi). Wykorzystuje metody socjotechniczne w celu skłonienia osób do dotarcia np. na fałszywą stronę (najczęściej za pomocą specjalnie spreparowanych e-maili czy SMS-ów) i tam do podawania swoich danych do logowania się w przekonaniu, że znajdują się w znanym i bezpiecznym źródle (np. na dobrze podrobionej stronie logowania się do bankowości elektronicznej). Dane te automatycznie trafiają do oszustów. W taki sam sposób możemy narazić nasze systemy bezpieczeństwa na kompromitację, dając intruzom dostęp do zarządzania nimi. *Phishing* zazwyczaj jest wysyłany masowo, bez większego rozpoznania adresatów.
Spear phishing natomiast bazuje już na informacjach wcześniej zebranych na temat celu/celów. Stąd tak ważne jest komunikowanie na zewnątrz tylko tych informacji, które są konieczne do prowadzenia działalności. W takim wypadku fałszywy e-mail będzie łudząco przypominał firmowy wraz z aktualną stopką, będzie dotyczył kwestii, które obecnie są w firmie omawiane, będzie zbudowany w formie adekwatnej do adresata oraz nadawcy. W natłoku codziennych obowiązków będzie nam trudno go odróżnić od masy innych służbowych e-maili.
Whaling – to nic innego jak *spear phishing* wysyłany do osób z wysokiego szczebla zarządczego firmy (tzw. C – Team). W takim wypadku bardzo istotną kwestią jest dotarcie do takich osób z misją budowania świadomości bezpieczeństwa, zanim zrobią to nasi adwersarze.
Vishing – najwięcej (statystycznie) ataków socjotechnicznych przeprowadza się pocztą e-mail. Nie oznacza to jednak, że tylko tym kanałem komunikacji intruzi próbują do nas dotrzeć. *Vishing* rozumie się jako *phishing* wykorzystujący kanał głosowy (VoIP, telefonia). Najlepszym przykładem jest telefon „z banku" z prośbą o zweryfikowanie danych dostępowych do konta, czego banki nigdy nie robią! Atakujący zakłada w tym przypadku, że osobie, do której dzwoni, będzie trudniej odmówić podania danych przez telefon niż e-mailowo czy przez SMS *(SMiShing* wykorzystuje SMS-y).
Dużą popularność zyskują również inne kanały komunikacji, np. komunikatory czy serwisy społecznościowe. Stąd istotne jest, aby np. operator centrum nadzoru czy administrator systemów bezpieczeństwa nie korzystali z prywatnej poczty czy portali społecznościowych na służbowych komputerach (dochodzi też niebezpieczeństwo zainfekowania komputera złośliwym oprogramowaniem). Konta firmowe są chronione zdecydowanie lepiej niż konta prywatne, stąd prawdopodobieństwo dotarcia fałszywego e-maila na adres służbowy jest mniejsze, choć możliwe.

Rys. 1. Cykl ataku socjotechnicznego wspartego technologią Machine Learning (ML)



Rys. 2. Schemat ataku socjotechnicznego

JAK ZATEM RADZIĆ SOBIE Z TEGO TYPU ZAGROŻENIAMI?

Kluczowym elementem tej gry jest człowiek i na człowieku powinniśmy w pierwszej kolejności skupić swoją uwagę. Dobrym pomysłem jest stałe podnoszenie świadomości zagrożeń nas samych i naszych pracowników. Jest to zadanie żmudne i trudne, jednak konieczne, aby skutecznie zaadresować ryzyka związane z atakami socjotechnicznymi. Służą temu specjalnie zbudowane kampanie *security awareness* uczące, jak odpowiednio rozpoznać zagrożenie i na nie zareagować. Zazwyczaj opierają się na następujących założeniach czy zaleceniach:

- pracownicy powinni zostać przeszkoleni z zakresu ataków socjotechnicznych, aby rozumieć zagrożenie i umieć je rozpoznawać,
- organizacja powinna wdrożyć odpowiednie procedury opisujące dostępy uprzywilejowane do konkretnych zasobów,
- należy wdrożyć system powiadamiania o potencjalnych atakach (np. odpowiedni przycisk w kliencie poczty elektronicznej),
- nie powinno się zamieszczać informacji służbowych na portalach społecznościowych, nie wolno stosować tych samych haseł na zewnątrz (np. to samo hasło do poczty korporacyjnej i prywatnej),
- dokumenty należy trwale zniszczyć przed ich pozbyciem się, a cały proces powinien być ujęty w procedurach i udokumentowany,
- dobrą praktyką jest zastosowanie wieloskładnikowej autentykacji użytkowników (w połączeniu ze stosowaniem różnych haseł do poszczególnych kont, szyfrowaniem dysków i zapewnieniem bezpieczeństwa wykorzystywanych urządzeń mobilnych),
- ograniczenie używania kont administratora tylko do czynności niezbędnych.

Ważne, aby tak zbudowana kampania została przygotowana pod kątem indywidualnych potrzeb i zagrożeń konkretnych instytucji, firm. Na szczęście na rynku polskim tego typu usługi są już świadczone. Na pewno nie wystarczy e-mail wysłany hurtowo czy sucha prezentacja ostrzegająca przed konsekwencjami wycieku naszych danych.

Ataki socjotechniczne wymierzone są we wszystkie obszary działalności biznesu, w miejsca, gdzie zauważono jakiekolwiek prawdopodobieństwo, aby wyłudzić dane czy pieniądze. Intruzów nie obowiązują żadne zasady (o czym świadczą przypadki ataków na szpitale w czasie pandemii COVID czy granie na uczuciach ludzkich, wykorzystując do ataków przypadki chorych dzieci). Specjaliści bezpieczeństwa fizycznego na pewno w pojedynkę tej walki nie wygrają, ale mogą być ważną częścią defensywy, ograniczając dostęp do pozyskiwania danych oraz podnosząc w swoim środowisku ogólnie pojętą świadomość bezpieczeństwa. Skompromitowany system CCTV lub KD stanowi świetne źródło pozyskiwania informacji, danych, które w przyszłości mogą posłużyć intruzom do dokładnego przygotowania się do ataku socjotechnicznego. Nabyte w pracy dobre nawyki na pewno zaprocentują również w życiu prywatnym.

TOMASZ DACKA

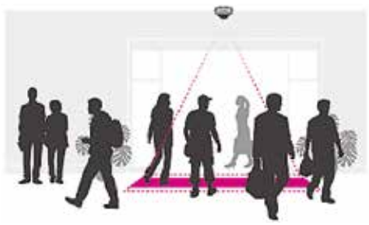
Ekspert bezpieczeństwa fizycznego. Z branżą związany ponad 12-letnim doświadczeniem, zwolennik holistycznego podejścia do zarządzania bezpieczeństwem. Prywatnie entuzjasta architektury przedwojennej Warszawy.

Nowości od Axis Communications

Łatwiejszy dozór pojazdów

Axis Communications wprowadziło właśnie na rynek dwa kompletne zestawy do monitorowania pojazdów, obejmujące kamery i oprogramowanie. Aplikacja AXIS License Plate Verifier i technologia OptimizedIR zapewniają weryfikację tablic rejestracyjnych w trybie 24/7.
Zestaw AXIS P1455-LE-3 idealnie sprawdza się w przypadku swobodnego ruchu pojazdów z niewielką prędkością, np. na terenie centrów miast, ogrodzonych osiedli czy kampusów uczelnianych. Zawiera kompaktową, odporną na warunki atmosferyczne i wytrzymałą (o klasie ochrony obudowy IK10) stałopozycyjną kamerę typu bullet o rozdzielczości HDTV 1080p, z 29-mm teleobiektywem, który dzięki dużej gęstości pikseli pozwala uzyskiwać ostre obrazy tablic rejestracyjnych z odległości nawet 20 metrów.
AXIS P3245-LVE-3 jest z kolei łatwym w instalacji zestawem sterującym dostępem pojazdów. Weryfikuje tablice rejestracyjne przez ich porównywanie z przechowywaną w kamerze listą numerów tablic autoryzowanych i tych, którym autoryzację cofnięto. Obsługuje różne poziomy zabezpieczeń oraz umożliwia zarówno podstawowe zarządzanie wjazdem i wyjazdem, jak i bardziej zaawansowane ustawienia. Wandaloodporna stałopozycyjna kamera kopułkowa o rozdzielczości HDTV 1080p jest bezpieczna w eksploatacji nawet w przypadku montażu na wysokości łatwo dostępnej dla człowieka.

Więcej niż tylko zliczanie osób



Aplikacja AXIS People Counter zlicza osoby poruszające się po takich obiektach, jak sklepy, hotele, dworce kolejowe, lotniska czy budynki administracji publicznej. Jej funkcjonalność pozwala na jednoczesne liczenie osób poruszających się w różnych kierunkach, co daje natychmiastowy dostęp do danych dotyczących trendów odwiedzin oraz natężenia ruchu w określonych strefach.
Nowa funkcjonalność aplikacji, pozwalająca wykrywać wejścia do określonej strefy poza ustalonym przedziałem czasowym lub ruch w niewłaściwym kierunku, może np. wspomagać systemy KD w obiektach IK.
Zaktualizowana wersja aplikacji AXIS People Counter umożliwia:

- Optymalizację efektywności obsługi klienta.
- Identyfikowanie trendów odwiedzin.
- Szacowanie poziomu natężenia ruchu.
- Ocenę operacyjną funkcjonowania obiektów.
- Dostarczanie wiedzy o możliwych ulepszeniach obsługi.

Aplikacja w zaktualizowanej wersji pozwala na zdalną konfigurację ustawień poszczególnych urządzeń oraz umożliwia monitorowanie i zarządzanie zdarzeniami w czasie rzeczywistym. Daje to operatorom bezpośredni dostęp do statystyk pochodzących ze wszystkich połączonych kamer. Oznacza to możliwość jednoczesnego sprawdzania i porównywania wielu obiektów z poziomu jednej lokalizacji centralnej.

Więcej na www.axis.com/pl-pl

Wizualizacja systemu RACS 5 v2.0 w nowym module Map

Firma Roger wprowadza do oferty kolejną wersję systemu kontroli dostępu i automatyki budynkowej o oznaczeniu RACS 5 v2.0. Wersja ta zawiera wiele udoskonaleń i nowych funkcjonalności, spośród których do najważniejszych należy zaliczyć możliwość obsługi rozproszonych terytorialnie systemów kontroli dostępu oraz rozbudowany moduł monitorowania pracy systemu w trybie graficznym (Mapy).

W nowym module Map wprowadzono możliwość powiększania, pomniejszania i przesuwania obrazu oraz płynnego definiowania wielkości elementów map, a także tworzenia własnych elementów graficznych. Ponadto dodano obsługę wybranych grafik wektorowych oraz możliwość tworzenia zestawu map w układzie hierarchicznym.
Nowy moduł Map umożliwia śledzenie w czasie rzeczywistym liczby osób znajdujących się w kontrolowanych strefach obecności, ma także możliwość definiowania na mapie obszarów reprezentujących strefy alarmowe, wraz z sygnalizacją ich aktualnego stanu.
Monitorowanie systemu w trybie graficznym obejmuje zarówno system kontroli dostępu, jak i zintegrowane z nim systemy VSS/CCTV (Dahua, Hikvision, BCS, IPOX, ONVIF) oraz SSWiN (INTEGRA, Galaxy).
Moduł Map jest jednym ze stale rozwijanych elementów systemu i w niedalekiej przyszłości planowane jest jego poszerzenie o możliwość wizualizacji kolejnych popularnych systemów bezpieczeństwa i automatyki budynkowej.

Więcej na www.roger.pl

Nowe kamery termowizyjne Wisenet QVGA

Firma Hanwha Techwin poszerzyła ofertę przystępnych cenowo kamer termowizyjnych serii Wisenet T o rozdzielczości QVGA, wprowadzając dwa nowe modele przeznaczone do ochrony obwodowej rozległych terenów otwartych.

Wisenet TNO-3050T ma obiektyw o stałej ogniskowej 35 mm, wykrywa pojazdy z odległości do 4400 m oraz ludzi z odległości do 1750 m. Natomiast Wisenet TNO-3050T z obiektywem o stałej ogniskowej 19 mm wykrywa pojazdy z 2400 metrów i ludzi z 950 metrów. Obie kamery mają obudowy wandaloodporne przystosowane do pracy na zewnątrz (IK10/IP66). Wytwarzają obrazy o rozdzielczości 320 x 240 pikseli.
Kamery mają funkcję ostrzegania o znaczącej, nagłej zmianie temperatury w obserwowanej scenie. Operatorzy mogą zdefiniować trzy obszary szczególnego zainteresowania w polu ich widzenia. Mają też wbudowane funkcje analizy treści obrazu, m.in. wykrywanie wejścia/wyjścia do/z wyznaczonego obszaru, przekraczania wirtualnej linii, pojawiania się lub znikania obiektów, wykrywanie ruchu w określonym kierunku, wskazywanie osób wałęsających się w polu widzenia kamery, wykrywanie wstrząsów i prób sabotażu. Podczas pracy w całkowitej ciemności skuteczność kamer zostaje zwiększona przez funkcję analizy dźwięku, która rozpoznaje krytyczne odgłosy (strzały, eksplozje, krzyki, dźwięk tłuczenia szkła).
Oprogramowanie kamer jest zgodne z otwartą platformą programową, dzięki temu mogą one obsługiwać aplikacje do analizy treści obrazu pochodzące od innych firm. Może to być np. aplikacja do wykrywania intruzów opracowana przez partnera technologicznego firmy Hanwha Techwin, firmę AI Tech.

Więcej na www.hanwha-security.eu/pl/

ARGUS RV rozwiązuje problem zarządzania SKD w obiektach rozproszonych

Telbud S.A. dysponuje platformą ARGUS RV zarządzającą systemami kontroli dostępu i pozwalającą na tworzenie rozproszonych struktur wieloserwerowych.

ARGUS RV bazuje na zaawansowanym oprogramowaniu komputerowego systemu dozoru i sterowania klasy PSIM. Rozwiązuje problem centralnego zarządzania systemami KD w wielu obiektach, w których funkcjonują systemy zabezpieczeń różnych producentów.
Platforma pozwala też na lokalne zarządzanie uprawnieniami dostępu w obiektach nadzorowanych i zarządzanych centralnie w sytuacji, gdy zostaje przerwana komunikacja ze zdalnym centrum zarządzania bezpieczeństwem.
ARGUS RV może realizować funkcjonalność integracji i zarządzania systemami kontroli dostępu, wykorzystując moduł oprogramowania Argus KD, który stanowi integralną część platformy i jest wyposażony w jednolity interfejs użytkownika do zarządzania uprawnieniami w systemach kontroli dostępu różnych producentów.
Drugi sposób integracji i zarządzania systemami KD wykorzystuje własne rozwiązania kontroli dostępu oparte na kontrolerach firmy Skalmex z oprogramowaniem zarządzającym Syndis KD firmy Mikronika.
Oprogramowanie ARGUS RV może pracować w konfiguracji wieloserwerowej hierarchicznej, dlatego oba sposoby integracji SKD rozwiązują problem lokalnego i centralnego zarządzania kontrolą dostępu działającą w rozproszonych obiektach.
Umożliwia też nadzorowanie przez operatorów Centrum Zarzadzania Bezpieczeństwem (CZB) pracy operatorów lokalnych oraz przejmowanie ich uprawnień związanych z obsługą i zarządzaniem określonymi systemami ochrony technicznej.

Więcej na https://telbud.pl/system-argus/argus-rv

WEBINARIUM:

Integracja GEMOS z systemem radarowym MAGOS

Właściwa integracja systemów bezpieczeństwa pozwala na ich łatwą i intuicyjną obsługę. Połączenie wszystkich elementów poprzez integrację w oprogramowaniu GEMOS adv.PSIM daje operatorowi pełną świadomość sytuacyjną, a to pozwala mu o wiele szybciej i skuteczniej reagować na potencjalne zagrożenia. Zmniejszają się też wydatki potrzebne na kontrolę i ochronę.

Modułowa budowa oprogramowania PSIM sprawia, że założoną instalację można bez przeszkód rozbudowywać, zachowując elastyczność w adaptacji. W rozległych obiektach GEMOS adv.PSIM jest to już wręcz niezbędne ze względu na złożoność technologii stosowanych w systemach zabezpieczenia technicznego.
Jedną z technologii stosowanych do zabezpieczenia dużych otwartych przestrzeni jest radiolokacja. Radary umożliwiają ciągły nadzór dużego terenu, co znacznie zmniejsza liczbę innych wymaganych czujników (detektorów), jednocześnie poprawiając zasięg detekcji i możliwości wykrycia niepożądanych obiektów w każdych warunkach atmosferycznych i oświetleniowych. Radary charakteryzują się wysoką dokładnością określanego położenia lub parametrów ruchu, co daje doskonałą skuteczność detekcji zagrożenia, nawet w zróżnicowanym otoczeniu.
O integracji systemów radarowych MAGOS z oprogramowaniem GEMOS adv.PSIM była mowa w trakcie webinarium zorganizowanym w lipcu br. Eksperci z firmy ElaCompil oraz Linc Polska omawiali takie zagadnienia, jak:

- Co to jest GEMOS adv.PSIM?
- Jakie korzyści daje integracja systemów heterogenicznych?
- Jaka jest zasada działania radaru?
- Jakie funkcje ma radar MAGOS?
- Jak prawidłowo zintegrować system radarowy MAGOS?
- Stały nadzór nad sprawnością systemów, czyli czym są moduły analityczne?

Zachęcamy do uczestnictwa w kolejnych webinariach. Wystarczy zapisać się na stronie: www.linc.pl/szkolenia.

Więcej na www.linc.pl

Bezpieczeństwo miejsca pracy zaczyna się od kontroli dostępu

Każdy ma prawo czuć się komfortowo w miejscu pracy. Jednak według najnowszych raportów aż 68% pracowników nie czuje się bezpiecznie w budynkach, w których pracuje na co dzień. Zebrane przez system Brivo anonimowe dane wyraźnie pokazują zmiany w codziennej aktywności użytkowników w czasie pandemii. Brivo pozwala obecnie monitorować aktywność ponad 25 milionów użytkowników w ponad 70 tysiącach różnych lokalizacji, takich jak biura, szkoły, urzędy, hotele, obiekty rządowe itd. Te dane pozwalają lepiej obserwować i rozumieć zmianę aktywności pracowników np. w kontekście poruszania się po biurze.

Ponieważ ponownie w czasach pandemii otwieramy drzwi dla swoich gości, to właśnie system Brivo może pomóc w odpowiedniej kontroli dostępu do budynku, a także w analizie i sterowaniu przepływem osób. To sposób na skuteczną odbudowę zaufania właśnie do miejsc pracy.
Najważniejsze funkcje platformy Brivo to m.in.:

- **Zliczanie osób** – wiadomo ile osób jest w budynku (np. w celu zarządzania limitami).
- **Raportowanie kontaktów** – możliwość sprawdzenia z kim dana osoba mogła mieć kontakt w ciągu dnia.
- **Publikacja informacji** – wyświetlanie użytkownikom komunikatów o obowiązujących ograniczeniach.
- **Raportowanie** – możliwość tworzenia złożonych raportów dostosowanych do indywidualnych potrzeb.
- **Zawieszanie dostępu** – szybkie i zdalne odbieranie uprawnień do wejścia do obiektu.
- **Status szczepienia** – egzekwowanie ograniczeń dostępu dla osób zaszczepionych lub nie.

Technologia Brivo aktywnie wspiera działania mające na celu ochronę zdrowia i bezpieczeństwa pracowników, klientów, studentów oraz mieszkańców. Wszystko po to, aby znów było naprawdę bezpieczne.

Więcej na www.smart-i.pl

MotionCam Outdoor

Bezprzewodowy zewnętrzny czujnik ruchu z aparatem fotograficznym do weryfikacji alarmów

Czujnik ruchu

Fotograficzna weryfikacja alarmów

Wykrywa ruch na obszarze wielkości 175 m²

IP55

Odporny na pył i rozpryski

Darmowe aplikacje dla instalatorów i użytkowników końcowych

ajax.systems

macOS Windows iOS Android

Miłego oglądania