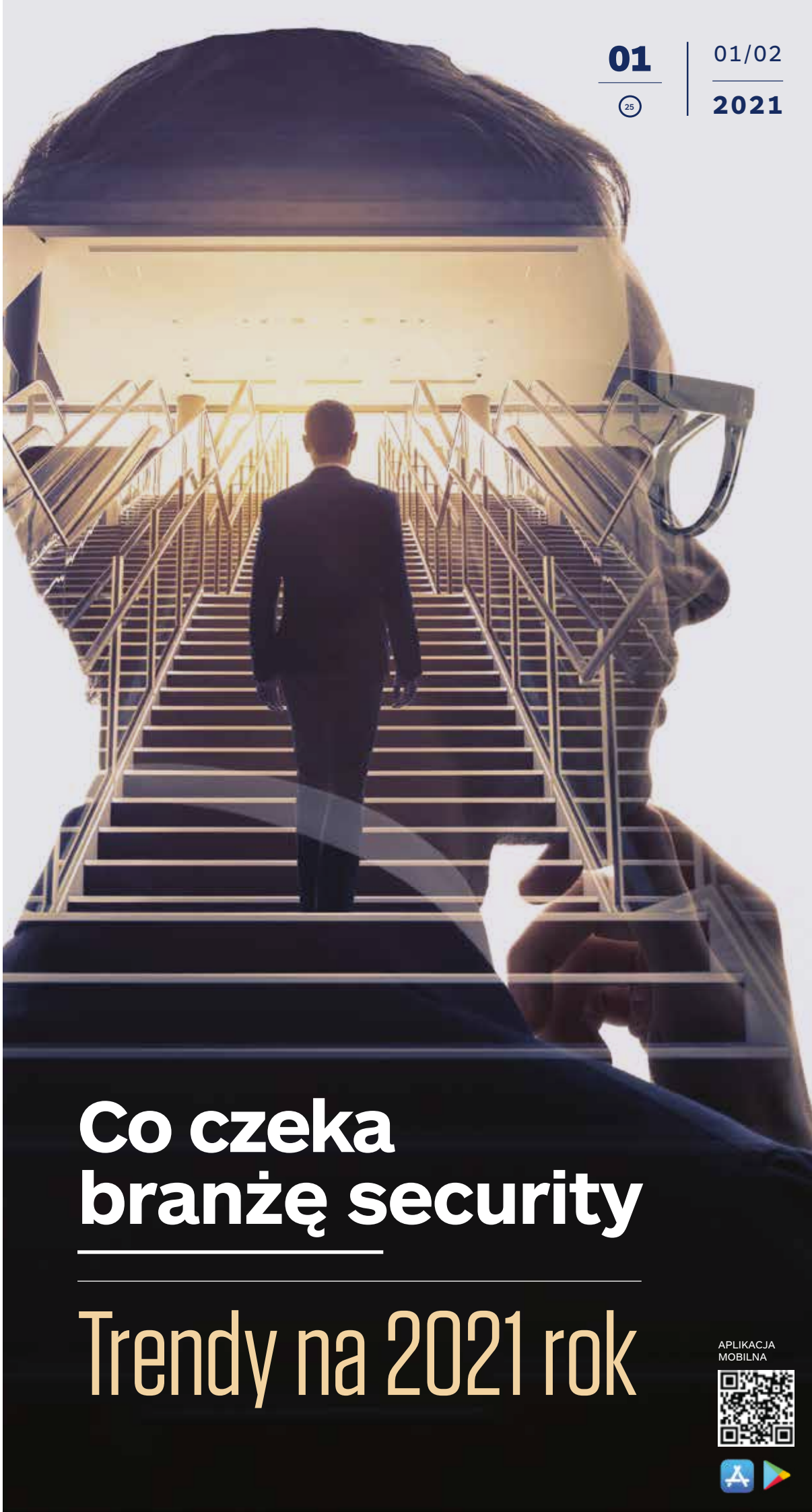
CZASOPISMO RYNKU SECURITY

a&s POLSKA

01
25

01/02
2021



TRENDY NA 2021 ROK

PODSUMOWANIA I PROGNOZY

Jaki wpływ na działalność firm branży security miała pandemia COVID-19? Jak oceniają kondycję rynku zabezpieczeń w Polsce w 2020 r.? Zapytaliśmy o to menedżerów najważniejszych firm działających na polskim rynku.

RYNEK SECURITY

SMA – UMOWA SERWISOWA OPROGRAMOWANIA

Utrzymanie ciągłości działania elektronicznych systemów zabezpieczeń jest zadaniem priorytetowym. Dostęp do aktualnych wersji oprogramowania i usług wsparcia jest więc konieczny. Branża nie jest przekonana do zawierania umów SMA.

TRANSPORT I LOGISTYKA

ZAKŁÓCENIA W ŁAŃCUCHU DOSTAW

Pandemia COVID-19 obnażyła słabe punkty w łańcuchach dostaw, które przysporzyły kłopotów w wielu branżach. Uwydatniła problemy wynikające z braku dywersyfikacji dostaw i uzależnienia się od jednego dostawcy.

Co czeka branżę security

Trendy na 2021 rok

APLIKACJA MOBILNA

www.aspolska.pl

ISSN 2451-5175

9 772451 517703 05

15 zł
(w tym 8% VAT)

BCS®
dla profesjonalistów

Nowa seria kamer

POTĘGA Ai

DETEKCJA TWARZY

5 STRUMIENI

4K ULTRA HD
ROZDZIELCZOŚĆ 4K

METADANE

LICZENIE LUDZI

POZOSTAWIENIE BAGAŻU

STABILIZACJA OBRAZU

PRZEKROCZENIE LINII

POLSKA MARKA BCS

WIĘCEJ INFORMACJI ZNAJDZIESZ
W PRODUKCIE NUMERU NA STR. 8

www.bcscctv.pl
https://www.facebook.com/bcscctvpl/

Drodzy Czytelnicy

Rok 2020 był szczególny. Nagle znaleźliśmy się w nowej, niestabilnej rzeczywistości. Utrudnienia związane z pandemią COVID-19 – praca zdalna, lockdown, nieterminowe dostawy towarów lub ich brak, uzależnienie od jednego dostawcy – negatywnie wpłynęły na ciągłość działania wielu przedsiębiorstw. Jak poradziły sobie polskie firmy branży security? Na pewno pandemia wyzwoliła kreatywność i przyspieszyła procesy cyfryzacji w działalności biznesowej. O podsumowanie roku 2020 poprosiliśmy przedstawicieli najważniejszych firm na polskim rynku zabezpieczeń (s. 16).

Wszyscy zastanawiamy się, jaka czeka nas przyszłość i jak szybko wrócimy do „normalności". W Europie przeważa ostrożny optymizm (s. 26), czy taki sam nastrój utrzymuje się na świecie? Firma badawcza Memoori prognozuje dwa scenariusze rozwoju sytuacji. Miejmy nadzieję, że sprawdzi się ten bardziej optymistyczny (s. 30). A jakie nowe technologie IT mają szansę stać się powszechne w 2021 r.? Prezentujemy je przez pryzmat badań ankietowych i raportów dwóch firm (s. 32 i 36). Szerzej o cyberwyzwaniach stojących przed biznesem piszemy na s. 38.

Oprogramowanie zawsze było ważnym narzędziem w rozwoju naszej branży. Dostęp do aktualnych jego wersji i usług wsparcia technicznego jest konieczny do utrzymania ciągłości działania elektronicznych systemów zabezpieczeń. A co to jest *Software Maintenance Agreement*, jakie rodzaje umów SMA funkcjonują w branży i jakie korzyści zapewnia umowa serwisowa oprogramowania – wyjaśniamy na s. 40.

Pandemia pokazała, jak kluczowym aspektem dla funkcjonowania firm jest zapewnienie ciągłości dostaw. Temat przewodni numeru – bezpieczeństwo transportu i logistyki – rozpoczynamy od omówienia zakłóceń w łańcuchach dostaw spowodowanych przez COVID-19 i sposobów ich ograniczania (s. 50). O możliwych korzyściach, jakie w zarządzaniu flotą pojazdów zapewni technologia 5G, i o wyzwaniach z nią związanych – w artykule na s. 54. Terminal pasażerski międzynarodowego portu lotniczego to najtrudniejszy do zabezpieczenia obiekt. Wybranymi problemami projektowymi i wskazówkami uruchomieniowymi dzieli się znany już czytelnikom inżynier uruchomieniowy (s. 58). Temat przewodni zamykają wypowiedzi oferentów i użytkowników systemów (s. 70).

W związku ze zmianą w funkcjonowaniu całego kraju my także podjęliśmy niezbędne środki i działania, by nie pozostawić naszych Czytelników bez interesujących ich treści, a partnerów biznesowych i reklamodawców bez możliwości skutecznego dotarcia do rynku. Skierowaliśmy dystrybucję naszego czasopisma bezpośrednio do domów Czytelników – ten ruch okazał się sukcesem, a liczba naszych prenumeratorów wzrosła o 28 proc., osiągając ponad 6 tys. Silniejszy akcent kładziemy też na działania online. Nasz portal aspolska.pl odwiedziło w tym roku ponad 50 tys. użytkowników!

Zmieniliśmy również formułę naszego największego wydarzenia – Warsaw Security Summit. Mamy nadzieję, że w tym roku uda się nam je zorganizować w wersji hybrydowej (łączonej: stacjonarnej i online) i chociaż z częścią naszych branżowych przyjaciół i znajomych spotkamy się wreszcie osobiście (z zachowaniem obowiązujących rygorów epidemicznych i reżimów sanitarnych).

Marta Dynakowska
REDAKTOR NACZELNA

Jan T. Grusznic
Z-CA REDAKTORA NACZELNEGO

Mariusz Kucharski
DYREKTOR ZARZĄDZAJĄCY

a&S POLSKA

REDAKCJA

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

Dyrektor zarządzający
Mariusz Kucharski

Redaktor naczelna
Marta Dynakowska

Z-ca redaktora naczelnego
Jan T. Grusznic

Dział reklamy i marketingu
Iwona Krawiec

Dział projektów specjalnych
Jolanta A. Kucharska
Aleksandra Czapska

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

Korekta
Jolanta Kucharska

Projekt graficzny i skład
Kalwala Studio

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

Prenumerata
www.aspolska.pl/prenumerata

a&S POLSKA
01
25
01/02
2021

SPIS TREŚCI

AXIS COMMUNICATIONS

www.axis.com/pl

Bezpłatne oprogramowanie do zarządzania audio od Axis

AXIS AUDIO MANAGER EDGE TO NOWE ROZWIĄZANIE DO ZARZĄDZANIA SYSTEMEM AUDIO WBUDOWANYM W GŁOŚNIKI SIECIOWE AXIS. ROZSZERZONE OPROGRAMOWANIE, OPRACOWANE Z MYŚLĄ O OBSŁUDZE NAWET 200 GŁOŚNIKÓW W MAKS. 20 STREFACH, JEST PRZEZNACZONE DLA MAŁYCH I ŚREDNICH LOKALIZACJI, NP. SKLEPÓW. JEST DOSTĘPNE JAKO BEZPŁATNA AKTUALIZACJA DLA WSZYSTKICH POSIADACZY GŁOŚNIKÓW SIECIOWYCH AXIS.

Głośniki sieciowe Axis wspierają rozwiązania bezpieczeństwa m.in. dzięki emitowaniu komunikatów głosowych. Oprogramowanie Axis Audio Manager Edge zawiera ułatwiające zarządzanie treścią funkcje, za pomocą których użytkownik może łączyć emitowane na żywo lub gotowe zapowiedzi, reklamy i tło muzyczne.
Umożliwia łatwą instalację, konfigurację i użytkowanie głośników, zawiera też proste funkcje harmonogramu do cotygodniowego planowania treści.
Odrębne prawa dostępu dla administratorów, menedżerów treści i pozostałych użytkowników sprawiają, że poszczególnym osobom można przypisać tylko niezbędne uprawnienia, obniżając ryzyko błędów i nieprawidłowego działania systemu.
Wbudowany system monitoringu i powiązany z nim pulpit do wyświetlania danych pozwalają szybko uzyskiwać informacje nt. ewentualnych problemów wymagających rozwiązania.
Do systemów audio, obejmujących więcej niż jedną lokalizację, w I kwartale br. zostanie udostępniona działająca w chmurze usługa zarządzania wieloma lokalizacjami Axis Audio Manager Center, która umożliwi rozbudowę systemu do kilku tysięcy lokalizacji.

BCS

www.bcscctv.pl

Nowa seria kamer BCS Line 9000

NOWA SERIA KAMER IP BCS LINE Z RODZINY KAMER AI – SERIA 9000 SKŁADA SIĘ Z TRZECH MODELI O ROZDZIELCZOŚCI 12 MPIX, DOSTĘPNYCH W TRZECH TYPACH OBUDOWY: KLASYCZNEJ KOMPAKTOWEJ, OBUDOWIE TUBOWEJ ZE ZINTEGROWANĄ PUSZKĄ MONTAŻOWĄ ORAZ KOPUŁOWEJ.

Głównym atutem kamer tej serii jest ich wysoka rozdzielczość. Kamery 12-Mpix w dalszym ciągu nie są codziennością, mimo że są dostępne na rynku od lat.
Nowością jest połączenie wysokiej rozdzielczości z szeregiem funkcji analizy wideo w jednej kamerze, co dotychczas wymagało zastosowania kilku urządzeń. Na przykład możliwość gromadzenia metadanych o obiektach widocznych przed kamerą była do tej pory dostępna jedynie w rejestratorach serii AI. Funkcja ta umożliwia błyskawiczne wyszukanie obiektu na podstawie cechy, wg której nagrania są filtrowane, co skraca czas potrzebny na ich przegląd.

Ponadto kamera obsługuje funkcje liczenia ludzi i może to robić jednocześnie w 4 strefach lub monitorować pod tym kątem 4 przejścia. Przy kontroli ruchu samochodowego przydatna może być funkcja rozpoznawania numerów tablic rejestracyjnych, co do tej pory wymagało użycia kamery przeznaczonej do tego celu.

Modele serii 9000 obsługują również „zwykle" funkcje analizy wizyjnej, np. przekroczenie linii czy wtargnięcie w strefę, z możliwością wskazania konkretnego typu obiektu, który taki alarm ma uruchamiać.

Przy zastosowaniu tak zaawansowanych kamer jedynym problemem będzie dobór odpowiedniego typu obudowy, ponieważ każdy model oferuje taki sam wachlarz możliwości.

COMMAX

www.commax.pl

Nowa jakość systemów wideodomofonowych

COMMAX ROZSZERZYŁ GAMĘ PRODUKTÓW WIDEODOMOFONOWYCH O NOWE ROZDZIELCZOŚCI FULL HD. MONITOR COMMAX CDV-70MF Z PANORAMICZNYM EKRANEM O WIELKOŚCI 7" OPRÓCZ OBSŁUGI STANDARDOWYCH KAMER WYŚWIETLA OBRAZ Z PANELI WEJŚCIOWYCH WYPOSAŻONYCH W OPTYKĘ HD 1080P (2MPIX), CO PRZEKŁADA SIĘ NA 3-4-KROTNIE WIĘKSZĄ SZCZEGÓŁOWOŚĆ OBRAZU W PORÓWNANIU DO STANDARDOWYCH KAMER ANALOGOWYCH.

Zwiększenie jakości toru wideo nie wymaga dodatkowych zabiegów instalacyjnych – system pracuje poprawnie na standardowym oprzewodowaniu. Monitor może również wyświetlać obrazy z dodatkowych kamer obserwacyjnych pracujących również w rozdzielczości AHD 2Mpix, a funkcja PIP pozwala wyświetlić obrazy z panelu i dodatkowej kamery jednocześnie.
Wbudowany moduł pamięci umożliwiający rozbudowę o karty microSD zapisze zdjęcia lub filmy podczas wywołania monitora oraz w przypadku wykrycia ruchu na obrazie z wybranej kamery. Obsługę ułatwia ekran dotykowy. Monitory występują w dwóch wersjach kolorystycznych: klasycznej – białoperłowej oraz designerskiej – ciemnoszarej z granatowym akcentem wokół ekranu.
Monitor obsługuje panele wejściowe COMMAX – zarówno analogowe, jak i szeroką gamę paneli z optyką HD 2 i 1,3 Mpix. Użytkownik może wybrać modele dedykowane na wąskie słupki (np. DRC-4CPHD) lub klasyczne (np. DRC-40YFD) oraz wyposażone w czytnik kart/breloków i/lub klawiaturę kodową umożliwiające otwarcie furtki i bramy za pomocą kodu i/lub transpondera zbliżeniowego (np. DRC-40DKHD).

GDE POLSKA

www.gde.pl

IWH-43PIX – nowa inteligenta kamera MAZi+

MAZI KONTYNUUJE WPROWADZANIE NOWYCH MODELI I ZASTĘPOWANIE STARSZYCH URZĄDZEŃ NOWYMI. PO REJESTRATORACH HD ORAZ IP SUKCESYWNIE JEST ODŚWIEŻANA OFERTA KAMER IP. JEDNĄ Z NOWOŚCI JEST KAMERA IWH-43PIX Z FUNKCJAMI DEEP LEARNING.

Dzięki zastosowaniu technik uczenia maszynowego staje się możliwa eliminacja podstawowej wady klasycznych kamer CCTV – fałszywych alarmów wywoływanych przez klasyczną detekcję ruchu.
Za pomocą funkcji Deep Learning zrealizowano detekcję wtargnięcia, przekroczenia linii, wejście w obszar oraz wyjście z obszaru. Dla każdej z nich można określić obiekt, na który kamera ma zareagować (np. człowiek, pojazd) oraz jego minimalny i maksymalny rozmiar. Tym samym można wyeliminować np. ruch liści na drzewach, cienie, zwierzęta, deszcz, owady.
Zaletą jest też obsługa kamer przez najnowsze przeglądarki, np. Edge, Firefox oraz przez Internet Explorer. Kamera ma wejście i wyjście alarmowe, wejście i wyjście audio oraz podświetlenia światłem białym.
To nie koniec możliwości kamery. W kamerę wbudowano także mikrofon i głośnik. Użytkownik może ustawić odtwarzanie własnych komunikatów słownych czy nagranych dźwięków, a także włączyć podświetlenia światłem białym po wystąpieniu zdarzenia alarmowego.
Kamera ma rozdzielczość 4 Mpix, obsługuje kodeki H.264/H.264+/H.265/H.265+, obiektyw 4 mm (pole widzenia ok. 83°) i podświetlenie w podczerwieni o zasięgu do 60 m.

Wyłącznym partnerem firmy MAZi Security Systems jest GDE Polska.

HIKVISION

www.hikvision.com/pl

Nowe kamery Hikvision serii iDS-2CD7 – potęga AI

SZTUCZNA INTELIGENCJA WSPIERA CORAZ WIĘCEJ PROCESÓW ANALIZY OBRAZU W TELEWIZJI DOZOROWEJ, A DOSKONAŁYM TEGO PRZYKŁADEM SĄ NOWE KAMERY HIKVISION SERII 7. MOŻNA JE PODZIELIĆ NA DWIE GRUPY: MODELE OBSŁUGUJĄCE 6 SCENARIUSZY WSPIERANYCH ALGORYTMAMI AI ORAZ MODELE DEDYKOWANE DO ROZPOZNAWANIA NUMERÓW TABLIC REJESTRACYJNYCH (ANPR).

Kamery pierwszej grupy realizują:
1) **rozpoznawanie twarzy** (baza danych do 10 tys. osób) z opcją automatycznego powiadomienia w momencie wykrycia osoby,
2) **zliczanie osób**, z funkcją filtrowania obsługi sklepu (wyniki nie są zakłócane przez personel wchodzący/wychodzący itp.),
3) **zarządzanie kolejkami** oparte na rozpoznawaniu konkretnych obiektów (faktyczne osoby stojące w kolejce, a nie np. wózki z zakupami),
4) **detekcję osób**, z rozpoznawaniem twarzy i dodatkowymi informacjami: wiek, płeć, czy nosi okulary, ma zarost, plecak, maseczkę ochronną, kolor ubioru itp.
5) **ochronę obwodową wspierającą** detekcję obiektów (pojazd i/lub człowiek), z jednoczesnym filtrowaniem fałszywych alarmów wywołanych np. przez zwierzęta, ruchome gałęzie itp.,
6) **detekcję kasków ochronnych**, pożądaną np. na placu budowy czy w pomieszczeniach fabrycznych.

Kamery z grupy ANPR mają natomiast 3-stopniową analizę obrazu: **sprawdzają,** czy analizowany obiekt to rzeczywiście pojazd, następnie **wyszukują** tablicę rejestracyjną, a w ostatnim kroku **odczytują** znaki.
Znacznie zmniejsza to liczbę błędnych odczytów (pochodzących np. z napisów na boku lub dachu pojazdu).

JOHNSON CONTROLS

www.jci.com

TL405LE – nowy podwójny (Ethernet + LTE) komunikator Johnson Controls

NOWOCZESNY SYSTEM ALARMOWY NIE MOŻE OBEJŚĆ SIĘ BEZ SPRAWNEJ I PRZEDE WSZYSTKIM BEZPIECZNEJ KOMUNIKACJI. NOWY KOMUNIKATOR FIRMY JOHNSON CONTROLS TL405LE W PROSTY SPOSÓB ZAPEWNIA POŁĄCZENIE PRAKTYCZNIE DOWOLNEJ INSTALACJI SSWIN Z ODBIORNIKIEM KLASY SURGARD ORAZ, POPRZEZ SYSTEM ZDALNEGO ZARZĄDZANIA POWERMANAGE, TAKŻE Z BEZPŁATNĄ APLIKACJĄ MOBILNĄ CONNECTALARM.

NTL405LE jest wyposażony w najnowszy układ LTE, łączność Ethernet oraz Wi-Fi. Umożliwia podłączenie 6 wejść/wyjść oraz linii PSTN z centrali alarmowej. Wyjściami można sterować przy użyciu wiadomości SMS, numeru clip i aplikacji mobilnej ConnectAlarm.
Połączenie LTE i Ethernet w jednym urządzeniu stanowi dodatkowe zabezpieczenie w razie problemów z łączem internetowym w obiekcie bądź z zasięgiem GSM. Instalując TL405LE, mamy gwarancję, że nawet starszy system alarmowy udźwignie najnowsze systemy komunikacji i zapewni użytkownikom stały dostęp do domu.
Producent postarał się, by programowanie komunikatora było intuicyjne i nie sprawiało instalatorowi żadnych problemów. W tym celu można użyć popularnego oprogramowania DLS 5 lub wgrać ustawienia za pomocą portu USB. Łącząc TL405LE z serwerem PowerManage, mamy dodatkowy dostęp do zdalnej diagnostyki i wygodnego zarządzania całym systemem.
Już niedługo komunikatory LTE zastąpią wycofywane urządzenia 2G i 3G. Jest to więc inwestycja na wiele lat, która zapewni najnowocześniejszą łączność z praktycznie każdą centralą przewodową na rynku.

LINC POLSKA

www.linc.pl

MOBOTIX S74 = wydajność, elastyczność i doskonałość

JESZCZE ŻADNA KAMERA NIE BYŁA TAK ELASTYCZNA - MOBOTIX S74 WYZNACZA NOWE STANDARDY W ZAKRESIE FUNKCJONALNOŚCI, JAKOŚCI I WYDAJNOŚCI.

Dzięki połączeniu w jednym urządzeniu czterech modułów wizyjnych oraz funkcjonalnych S74 jest najbardziej wydajnym systemem wideo MOBOTIX IoT w historii. Ukryta obudowa kamery pozwala na dyskretną instalację samych modułów. Dzięki kablom modułowym o długości do 3 m można obserwować wiele różnych stref za pomocą tylko jednej kamery.

Oprócz tradycyjnych modułów wizyjnych do S74 można podłączyć: moduł termowizyjny, dodatkowy czujnik PIR wraz z termometrem i czujnikiem oświetlenia oraz moduł głośnika.

Rewolucyjną zmianą, jaką wprowadza platforma MOBOTIX 7, są aplikacje korzystające z algorytmów AI. Można zastosować te stworzone przez firmę MOBOTIX lub korzystając z narzędzi deweloperskich, napisać własne. Aplikacje są dostępne pojedynczo lub jako pakiety do konkretnych zastosowań, m.in. transportu, ochrony obiektów przemysłowych, użyteczności publicznej, sklepów czy szpitali.

Nowe funkcje dają prawdziwie nieograniczone możliwości stosowania kamer S74. Przykładowo S74 można wyposażyć w dwa przetworniki wizyjne obserwujące różne strefy, a odpowiednie aplikacje MOBOTIX pozwolą realizować dodatkowe zadania.

Można np. równolegle rozpoznawać tablice rejestracyjne w obszarze wjazdowym lub wykrywać wtargnięcia w strefie perymetrycznej. Wszystko to umożliwia jeden kompaktowy system MOBOTIX S74.

MIWI-URMET

www.miwiurmet.pl

Kamery LPR Milesight

LPR (LICENCE PLATE RECOGNITION) TO TECHNOLOGIA WYKORZYSTUJĄCA OPTYCZNE ROZPOZNAWANIE ZNAKÓW NA OBRAZACH DO AUTOMATYCZNEGO ODCZYTYWANIA NUMERÓW TABLIC REJESTRACYJNYCH POJAZDÓW.

W przypadku firmy Milesight algorytm LPR jest osadzony bezpośrednio w kamerach i umożliwia odczyt tablic na wysokim poziomie rozpoznawalności, przy prędkościach dochodzących do 120 km/h. Co więcej, kamery LPR Milesight, oprócz automatycznego rozpoznawania numerów rejestracyjnych, potrafią zidentyfikować więcej cech pojazdu, takich jak marka czy kolor.

LPR wbudowany w kamery Milesight automatycznie wykrywa i przechwytuje numery tablic rejestracyjnych w czasie rzeczywistym i porównuje z predefiniowaną listą, a następnie podejmuje odpowiednie działania, takie jak generowanie ostrzeżenia, gdy numery rejestracyjne znajdują się na czarnej liście lub otwarcie szlabanu w przypadku detekcji pojazdów mających zgodę na wjazd.

System automatycznego rozpoznawania numerów tablic rejestracyjnych jest obecnie stosowany w wielu miejscach wymagających kontroli ruchu pojazdów.

Wykorzystując komunikację sieciową, kamery LPR Milesight mogą w szybki sposób stać się elementem kontroli dostępu, np. systemu PROTEGE.

Więcej informacji można uzyskać na www.miwiurmet.pl

NEDAP SECURITY MANAGEMENT

www.nedapsecurity.com/pl/

Rozpoznawanie twarzy w kontroli dostępu AEOS

WYKORZYSTANIE TECHNOLOGII BIOMETRYCZNEGO ROZPOZNAWANIA TWARZY DO IDENTYFIKACJI OSÓB, A TYM SAMYM NADAWANIA LUB ODMAWIANIA IM PRAWA DOSTĘPU, STAJE SIĘ CORAZ WAŻNIEJSZE.

Zwiększa bezpieczeństwo i pewność poprawnej autoryzacji (inne identyfikatory, np. karty KD, można zgubić czy podrobić). Biometria twarzy może też stanowić dodatkowy (drugi) element weryfikacji. Rozwiązanie jest wygodne, ponieważ nie trzeba szukać identyfikatora ani wpisywać kodu PIN. Co najważniejsze, biorąc pod uwagę zagrożenia związane z pandemią COVID-19, jest to sposób bezdotykowy.

Funkcjonalność rozpoznawania twarzy jest dostępna w systemie kontroli dostępu AEOS dzięki integracji opracowanej z partnerem technologicznym Nedap, firmą Thales. Integracja ta obejmuje zarządzanie KD oraz identyfikację osoby – z poziomu jednego interfejsu systemu AEOS.

Możliwa jest autoryzacja i przyznanie prawa dostępu następuje poprzez porównanie obrazu twarzy „na żywo" z obrazem przypisanym do identyfikatora lub wyszukanym w bazie zarejestrowanych zdjęć.

Jeden interfejs do administracji, zarządzania i monitorowania upraszcza pracę służb nadzorujących odpowiedzialnych za systemy bezpieczeństwa.

System rozpoznaje nawet osoby noszące maseczkę na twarzy i można go tak skonfigurować, aby uwierzytelniać się łącznie z kartą lub bez niej. Można go również łatwo rozbudować o dowolną liczbę punktów kontroli dostępu i dowolną liczbę zdjęć osób zapisanych w bazie danych.

Więcej na: https://www.nedapsecurity.com/pl/

OPTEX SECURITY

www.optex-europe.com/pl

NOWOŚĆ! Funkcjonalność kamery w popularnych czujkach zewnętrznych serii VX Infinity

OPTEX SECURITY WPROWADZA NA POLSKI RYNEK MODUŁ KAMERY VXI-CMOD. ROZSZERZA ON FUNKCJONALNOŚĆ POPULARNYCH CZUJEK ZEWNĘTRZNYCH SERII VXI. VXI-CMOD TO BEZPRZEWODOWY MODUŁ KAMERY PANORAMICZNEJ FULL HD O KĄCIE DETEKCJI 180°, WYPOSAŻONY W OŚWIETLACZ PODCZERWIENI ORAZ MIKROFON.

W komplecie z czujką serii VXi tworzy kompletne rozwiązanie do wizyjnej weryfikacji alarmów. Takie rozwiązanie szczególnie dobrze sprawdzi się w użytkowaniu w warunkach domowych.
Jak to działa? Czujkę VXi wraz z modułem VXi-CMOD podłączamy do prądu oraz sieci Wi-Fi, a powiadomienia o zarejestrowanych zdarzeniach otrzymujemy na smartfon poprzez intuicyjną aplikację Optex Vision App (dostępna na iOS oraz Android). Dzięki funkcjonalności RTSP istnieje również możliwość przesyłania podglądu z kamery do istniejącego systemu alarmowego lub rejestratora NVR.
Zestaw można wykorzystać nie tylko do detekcji intruza, ale także do monitorowania aktywności wokół domu: powrót domowników, przybycie kuriera, wizyta niezapowiedzianych gości. Czujki z serii VX Infinity zapewniają niezawodne wykrywanie zbliżających się obiektów w zasięgu 12 m i kącie detekcji 90°, a sprawdzona konstrukcja zapewnia odporność na małe zwierzęta. Moduł VXi-CMOD można zamontować w dowolnym przewodowym modelu serii VXi (VXi-ST, AM, DAM).

Więcej informacji jest dostępnych na www.optex-europe.com/pl.

SCHRACK-SECONET

www.schrack-seconet.pl

SIS-FIRE – system integrujący urządzenia przeciwpożarowe

SYSTEM INTEGRUJĄCY URZĄDZENIA PRZECIWPOŻAROWE SIS-FIRE STOSOWANY JEST DO WIZUALIZACJI, STEROWANIA I ZARZĄDZANIA URZĄDZENIAMI PPOŻ., A TAKŻE DO INTEGRACJI INNYCH URZĄDZEŃ I SYSTEMÓW MAJĄCYCH WPŁYW NA BEZPIECZEŃSTWO POŻAROWE (KRYZYSOWE) OBIEKTU W CELU ZAPEWNIENIA JEGO MAKS. POZIOMU OCHRONY.

W 2020 r. wprowadzono kolejną wersję systemu (V4), która przeszła wymaganą procedurę certyfikacyjną w CNBOP-PIB (krajowy certyfikat stałości właściwości użytkowych nr 063-UWB-0305 oraz świadectwo dopuszczenia CNBOP nr 4194/2020).
Platforma informatyczna SIS-FIRE / SIS-FIRE Lite ściśle współpracuje z systemem sygnalizacji pożarowej i sterowania urządzeniami przeciwpożarowymi Integral IP oraz dźwiękowym systemem ostrzegawczym APS-APROSYS.
Podstawową zaletą systemu SIS-FIRE jest jego elastyczność, umożliwiająca optymalny – z perspektywy konkretnego typu obiektu – dobór elementów i funkcji, z zapewnieniem ścisłej współpracy i podziału kompetencji pomiędzy elementami systemu bezpieczeństwa pożarowego.
Opcjonalnie platforma informatyczna SIS-FIRE jest dostępna w wersji redundantnej, co – w połączeniu z redundantnym systemem Integral IP MX – zapewnia ciągłość działania również w przypadku wystąpienia awarii kluczowych elementów instalacji.
Istotną cechą systemu integrującego (w przeciwieństwie do standardowego SSP) jest możliwość spełnienia nieograniczonej liczby zadań i funkcji logicznych związanych z obsługą, sterowaniem i nadzorowaniem zintegrowanych systemów w obiekcie.

TP-LINK

www.tp-link.com.pl

TP-Link TL-SG3428XMP – przełącznik zarządzalny L2+, 24x Gb PoE+, 4x SFP+ 10G

TEN WYDAJNY ZARZĄDZALNY PRZEŁĄCZNIK L2+ JEST PRZEZNACZONY DO BUDOWY PROFESJONALNYCH SIECI W MAŁYCH I ŚREDNICH FIRMACH. JEST KOMPATYBILNY Z PLATFORMĄ OMADA SDN DO PROGRAMOWEGO STEROWANIA INFRASTRUKTURĄ SIECIOWĄ ZA POŚREDNICTWEM CHMURY.

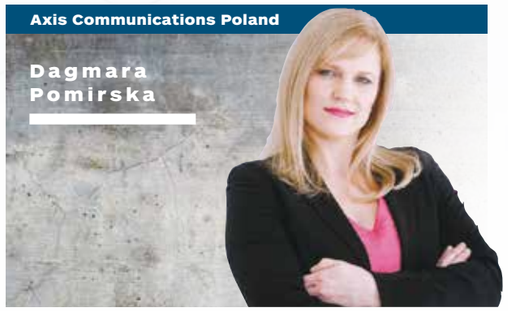
Switch został wyposażony w 24 porty PoE 10/100/1000 Mb/s zgodne ze standardami 802.3at/af, mogące łącznie dostarczyć 384 W mocy, co umożliwia podłączenie urządzeń typu punkty dostępowe, telefony IP i kamery IP. Pozwala zasilić urządzenia odbiorcze do 30 W na każdy port. Ma także 4 osobne sloty SFP+ (10G) umożliwiające integrację w sieciach o wysokiej przepustowości.
Tworzenie bezpiecznej sieci wspomagają liczne funkcje zarządzające – 802.1Q VLAN, izolacja portów, mirroring portów, STP/RSTP/MSTP, agregacja portów (LACP), funkcja kontroli przepływu 802.3x, ACL, funkcje L2+ tj. routing statyczny oraz Quality of Service (QoS, od L2 do L4).
Przełącznik jest prosty w obsłudze i zarządzaniu, w pełni kompatybilny z platformą Omada SDN do programowego sterowania infrastrukturą sieciową, która integruje działanie urządzeń sieciowych od TP-Link, zapewniając kompleksowe zarządzanie centralne z chmury za pomocą interfejsu przeglądarkowego lub aplikacji mobilnej. TP-Link Omada SDN umożliwia utworzenie wysoce skalowalnej sieci LAN i WLAN. Przekłada się to na płynne połączenia przewodowe i bezprzewodowe, niezbędne m.in. w hotelach, szkołach, biurach czy urzędach.
Produkt jest objęty 5-letnią gwarancją producenta.

a&S POLSKA

RYNEK SECURITY W POLSCE PODSUMOWANIE ROKU 2020

Jaki wpływ na działalność firm branży security miała pandemia COVID-19? Jak menedżerowie oceniają kondycję rynku security w Polsce w 2020 r.? Jakie są perspektywy rozwoju polskiego rynku security w 2021 r.? Zapytaliśmy o to przedstawicieli najważniejszych firm polskiej branży security.

Axis Communications Poland



Rok 2020 był z pewnością zaskakujący. Choć byliśmy przygotowani na wiele nietypowych wyzwań, finalnie wynik sprzedaży w Axis Communications okazał się wyższy niż w 2019 r., co nie tylko cieszy, ale także pozwala z optymizmem patrzeć w przyszłość. Rynek security w Polsce jest bowiem wciąż nienasycony. Pandemia, choć wiązała się ze zmianą realiów biznesowych – przejściem na zdalne zarządzanie produkcją czy zdalny kontakt z innymi uczestnikami rynku – przyspieszyła także część procesów, które miały miejsce już wcześniej. Wielu klientów zauważyło, że digitalizacja jest warunkiem koniecznym do dalszego prowadzenia biznesu, i zdecydowało się na inwestycje, które dotychczas odkładali w czasie. Tym samym czas lockdownu został efektywnie wykorzystany m.in. na poszerzenie infrastruktury monitoringu, automatyzację procesów czy wdrożenie rozwiązań AI.

Oczywiście nie każdy sektor rozwijał się równie dynamicznie. W związku z obostrzeniami zauważyliśmy zmniejszony poziom inwestycji w branżach hotelowej i restauracyjnej. Jednocześnie coraz więcej firm związanych z sektorem medycznym, transportowym i logistycznym czy infrastrukturą krytyczną zauważyło, że rozwiązania security to nie tylko kwestia ochrony, ale także możliwość dostosowania się do wprowadzonych regulacji i dbałość o zdrowie pracowników. Zautomatyzowane systemy wykrywające, czy dana osoba nosi maseczkę bądź utrzymuje dystans społeczny, umożliwiają bowiem bezproblemowe kontynuowanie pracy w zakładzie. Tego typu analityka, a także umożliwiające integrację otwarte rozwiązania end-to-end były w tym roku produktami poszukiwanymi i wierzymy, że ich popularność będzie rosła także w 2021 r.

Kondycja rynku w nadchodzących miesiącach z pewnością będzie zależała od tego, w jakim stopniu pandemia wpłynie na możliwości finansowania rozwiązań security. Sądzimy, że jeśli budżety zostaną utrzymane na podobnym poziomie, dalej będziemy obserwować przyspieszenie automatyzacji, która w długim terminie pozwoli klientom ograniczyć koszty związane z ochroną. Z pewnością ważnym zagadnieniem będzie też cyberbezpieczeństwo – w dobie zdalnego zarządzania może być ono jednym z rynkowych wyzwań i to właśnie jemu firmy naszej branży powinny poświęcić szczególną uwagę.

Oprócz cyberbezpieczeństwa w Axis Communications chcemy skupić się na kontynuowaniu naszej strategii tworzenia bezpieczniejszego i bardziej inteligentnego świata. Będziemy to robić, inwestując dalej w badania i rozwój nowych produktów oraz wdrażając coraz częściej systemy zintegrowane u naszych klientów. Wśród nich znajdą się na pewno rozwiązania dla mniejszych i średnich przedsiębiorstw oparte na otwartej platformie, w tym m.in. systemy dostępowe, kamery przetwarzające dane na brzegu sieci i systemy audio. Niezmiennie pragniemy, aby polskie miasta stawały się prawdziwymi smart cities, a wraz z nimi unowocześniały się także transport i przemysł.

Niezwykle ważni są dla nas również nasi Partnerzy i Dystrybutorzy. W 2020 naszym wspólnym sukcesem była pierwsza całkowicie internetowa konferencja security: Axis Talk; planujemy powtórzyć to wydarzenie również w roku obecnym. Miniony rok udowodnił, że zdalny kontakt nie stanowi przeszkody, a często może być nawet impulsem do rozwoju, dlatego w 2021 r. widzimy przede wszystkim wiele szans do wykorzystania.

AxxonSoft

Piszę te słowa zaledwie dzień po zakończeniu AxxonSoft Annual Conference '21 (tym razem w formule online) i mam przewrotne wrażenie, że czas pandemii został przepracowany najefektywniej od chwili, z którą rozpoczęła się moja przygoda z AxxonSoft. Takiego skoku naprzód nie pamiętam. Nowe technologie informatyczne znowu zmieniają rynek security.

Dzisiaj na nikim nie robią już wrażenia analiza wizyjna czy sieci neuronowe, co było jakże „ciepłą bułeczką" w ostatnich latach. Sektor IT doskonale wykorzystał swoją przewagę w czasach *home office* i jeszcze bardziej nas od siebie uzależnił. Praca zdalna zupełnie zmieniła, zachowawcze dotąd, podejście rynku do usług w chmurze. O prywatną chmurę, systemy hybrydowe czy monitoring wielodomenowy pytają najwięksi klienci rynku security. Chcemy mieć wszystko na oku, ale z dowolnego miejsca, zdalnie, szybko i przede wszystkim bezpiecznie. A także tanio. Ale to się akurat nie zmieniło.

Czy mogło być inaczej, skoro niemal wszyscy rok 2020 spędziliśmy, właśnie pracując zdalnie? Oczywiście był to rekordowy rok dla AxxonSoft zarówno globalnie, jak i w Polsce. Niemal wszystkie kraje zaliczyły solidne wzrosty i nie ma w tym ani szczęścia, ani przypadku. To produkt się obronił.

Liderem sprzedaży są Stany Zjednoczone i tam też, w Kalifornii (San Jose), koncentrujemy swój rozwój technologiczny. W Europie natomiast doczekaliśmy się nowej struktury (AxxonSoft Europe) oraz mocnego wejścia na nieco uśpione dotychczas rynki, takie jak we Francji czy w Hiszpanii. Z polskiej perspektywy bardzo nas to cieszy, ponieważ wzmocnienie zespołu w Europie z pewnością ugruntuje naszą pozycję wśród liderów rynku VMS/PSIM.

Rok 2021 zapowiada się fascynująco, mamy apetyt na kolejne rekordy, rozwój zespołu i ambitne projekty. Oby pracy znów było za dużo. Życzmy sobie wszyscy zdrowia i idźmy wraz z trendami do przodu!

Bosch Building Technologies

Mimo wyzwań, jakie przyniosła nam pandemia, Bosch Building Technologies zakończył rok 2020 dobrym wynikiem finansowym. Wymagało to z naszej strony koncentracji na rynkach wertykalnych najmniej dotkniętych kryzysem oraz dostosowania sposobu działania do nowej sytuacji. Posłużę się tu przykładem. COVID-19 zmienił sposób komunikacji z rynkiem oraz wewnątrz w firmie. Do dzisiaj w trosce o bezpieczeństwo naszych pracowników i klientów ograniczamy do minimum liczbę kontaktów bezpośrednich. Postawiliśmy na komunikację zdalną.

W trybie zdalnym wprowadzamy na rynek nowe produkty, a nawet prowadzimy szkolenia techniczne. Wyposażyliśmy się w odpowiednie narzędzia do zdalnej komunikacji, dostosowaliśmy do nowych potrzeb naszą salę szkoleniową oraz zakres i program szkoleń. Wszystkie te działania spotykają się z bardzo dobrym odzewem naszych klientów. Oczywiście nawet najskuteczniejsza komunikacja zdalna nie zastąpi kontaktów bezpośrednich, szczególnie w zakresie budowania relacji z nowym klientami. COVID-19 miał duży wpływ na kondycję rynku security w Polsce. Realizacja części inwestycji została znacząco opóźniona. Znane są przykłady, że inwestorzy nie decydują się na rozpoczęcie wcześniej planowych projektów, szczególnie w branżach związanych z turystyką czy hotelarstwem. Z podobną sytuacją mamy również do czynienia w przypadku inwestycji w powierzchnie biurowe. W rezultacie walka konkurencyjna na rynku mocna się zaostrzyła.
W tym pełnym wyzwań roku po raz kolejny przekonaliśmy się, jak ważnym czynnikiem sukcesu są dobre długofalowe relacje z klientami oraz przewidywalność i wiarygodność producenta. Dzięki tym właśnie elementom udało nam się realizować nasze cele bez konieczności podejmowania decyzji, które długoterminowo nie służyłyby biznesowi.
Rok 2021 jest przełomowy dla Bosch Building Technologies. Diametralnie zmieniamy naszą ofertę w zakresie systemów sygnalizacji pożarowej oraz dźwiękowych systemów ostrzegawczych. Wprowadzamy nowe centrale pożarowe AVENAR 2000 i 8000 oraz nowy system nagłośnieniowo-ostrzegawczy PRAESENSA. Najbliższe miesiące poświęcimy na działania skierowane do naszych partnerów, instalatorów, projektantów i klientów końcowych, promujące nasze nowości produktowe. Jestem przekonany, że ze względu na unikalne funkcjonalności oba produkty zdecydowanie zmienią układ sił na rynku.
Branża security jest ściśle powiązana z rynkiem budowlanym. Niezależnie od sytuacji związanej z pandemią COVID-19 prognozy dla rynku budowlanego na rok 2021 nie są korzystne. Dotyczy to przede wszystkim budownictwa kubaturowego niemieszkaniowego, które ma szczególne znaczenie dla firm, takich jak Bosch Building Technologies, koncentrujących się na kompleksowych, dużych projektach. Nie jest to jednak pierwszy rok, w którym zmierzymy się z niekorzystnymi prognozami rynku budowlanego i mamy oczywiście na to plan.
Dodatkowym zagrożeniem dla rynku security może być ogólny klimat inwestycyjny. Niepewność związana z COVID-19 nie sprzyja podejmowaniu przez inwestorów decyzji o nowych inwestycjach. Szansą są wszelkie obszary stanowiące alternatywę dla rynku budowlanego, takie jak transport, przemysł czy coraz szybciej rozwijający się rynek usług.
Myślę, że znaczącą rolę będą też miały małe projekty, gdzie inwestorem jest przeciętny „Kowalski". Ta część rynku w rzeczywistości cały czas jest napędzana konsumpcją i ma się bardzo dobrze. Odczuwamy to również jako Bosch Building Technologies, miesiąc za miesiącem bijąc kolejne rekordy sprzedaży czujek alarmowych.

Ela-compil

W minionym roku stanęliśmy w obliczu bezprecedensowej sytuacji związanej z pandemią i niespotykanymi dotychczas ograniczeniami, zatem musieliśmy się wykazać wyjątkową elastycznością w działaniu. Udało nam się płynnie przejść ze świata offline do online. Miękko weszliśmy w nowy tryb pracy, a nasz zespół z dużą plastycznością odnalazł się w nowych warunkach. Wszystkie zmiany były dla nas łatwe do zaimplementowania, ponieważ jesteśmy firmą technologiczną, która stara się wyprzedzać potrzeby rynku security i oferować technologię o niespotykanej funkcjonalności, zaimplementowaną przez programistów w najnowszym środowisku. Pracujemy w oparciu o zwinne techniki zarządzania, a szybka reakcja na zmiany jest wpisana w nasze DNA.

Wielu z nas relacje na żywo zamieniło na relacje wirtualne i komunikację zdalną. Wpłynęło to na coraz częstsze korzystanie z platform online, jak również wzrost zaangażowania użytkowników, co widzimy w naszych mediach społecznościowych. Bardzo szybko okazało się, że większość spraw możemy zorganizować zdalnie, nie tracąc na jakości, a dostarczając wartościowe treści.

Rozwój zdalnej technologii streamingowej pozwolił nam być bliżej klienta, a także zwiększyć zasięg i komunikować się z rynkiem na dużo większą skalę niż dotychczas. Dzięki temu udało się utrzymać kontakt z partnerami i – paradoksalnie – przeprowadzić prezentacje i szkolenia dla dużo szerszego grona niż w latach poprzedzających erę online. Klienci otrzymali zdalny dostęp do naszych specjalistów i do specjalistycznej wiedzy, nowe zwyczaje użytkowników i zdalny sposób komunikacji już z nami zostaną, gdyż są tańsze, wygodniejsze i szybsze. Nie zmienia to faktu, że tęsknimy za spotkaniami.
Mimo wielu zmian na rynku i światowego kryzysu udało nam się zrealizować plan sprzedażowy, co dobrze wróży na przyszłość. Pokazuje stabilność u naszych kontrahentów i ugruntowaną pozycję firmy Ela-compil na rynku. Zamierzamy powiększyć swoje zasoby w dziale R&D i w dziale technicznym. Pomyślny biznesowo rok zaowocował strategiczną decyzją o ekspansji naszych rozwiązań na rynki zagraniczne. Podjęliśmy już działania w celu zbudowania działu eksportu. Podsumowując rok 2020, musimy przyznać, że był to dla nas rok, w którym utrzymaliśmy sprzedaż na planowanym poziomie, a także rozwinęliśmy się technologicznie. Nasz nowy moduł GEMOS MOSAIC zdobył nawet Złoty Medal Targów Securex 2020.
Co przyniesie rok 2021? Przede wszystkim kontynuację trendów, jakie mogliśmy zaobserwować w ostatnich miesiącach. Będą to m.in. wprowadzanie na rynek nowych aplikacji, większa popularność technologii, po które programiści chętnie sięgali w 2020 r., oraz poszukiwanie przez firmy wsparcia IT związanego ze zmianą sposobu pracy i zwyczajów konsumentów podczas pandemii. Wraz ze zwiększaniem się roli cyfryzacji w funkcjonowaniu firm będzie także rosło znaczenie narzędzi do zapewniania cyberbezpieczeństwa.

Genetec

Firma Genetec bardzo szybko zareagowała na pandemię COVID-19, wdrażając skuteczne działania, które, co najważniejsze, zminimalizowały zakłócenia pracy naszym klientom na całym świecie. W ciągu 24 godzin od przejścia na pracę zdalną, tuż po wydaniu przez władze lokalne zarządzeń dotyczących reżimów sanitarnych, osiągnęliśmy prawie pełną zdolność operacyjną, a 95% naszych pracowników było w pełni dyspozycyjnych online.

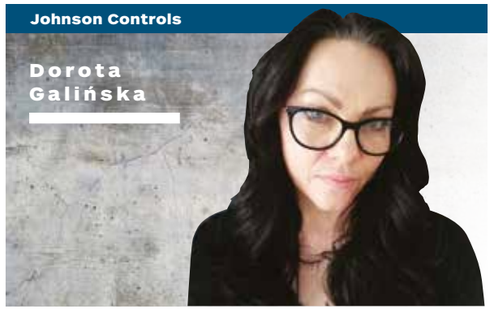
Z wyjątkiem kilku partnerów, którzy musieli na jakiś czas zamknąć swoją działalność, oraz pewnych tymczasowych ograniczeń dotyczących osobistego doradztwa i wdrażania systemu ten trudny rok okazał się niezwykle aktywny dla naszej firmy i całej branży zabezpieczeń technicznych.
Zwracając uwagę na nowe wyzwania biznesowe, w 2020 r. rozpoczęliśmy ambitną, całkowicie cyfrową strategię, w tym niezwykle udaną wirtualną konferencję ConnectDX, które przyciągnęły prawie 5 tys. specjalistów ds. zabezpieczeń technicznych z całego świata. Aby zapewnić spójne, wartościowe relacje z klientami, ich obsługę i wsparcie, opracowaliśmy solidny nowy system zarządzania szkoleniami, który wdrożyliśmy latem. Uruchomiliśmy również program podcastów „Engage: A Genetec podcast", emitowany dwa razy w tygodniu, w których wypowiadają się eksperci z różnych specjalności, poruszając szeroki zakres tematów, od cyberbezpieczeństwa po strategie dotyczące prywatności i inteligentnego miasta.
Podsumowując, w roku, w którym nic nie było pewne, wdrożyliśmy system połączenia całego naszego zespołu na świecie, a nawet uruchomiliśmy nowy oddział w Wiedniu obsługujący rejon DACH.
Jeśli chodzi o zapotrzebowanie w gospodarce, okres ten charakteryzował się szeregiem nowych i innowacyjnych zastosowań naszej technologii, która bezpośrednio pomagała sprostać wyjątkowym wyzwaniom podczas pandemii. Na wczesnym etapie jej wybuchu w USA największe centrum kongresowe McCormick Place, które zostało przekształcone w tymczasowe centrum leczenia COVID-19, zwróciło się do nas z prośbą o opracowanie rozwiązania umożliwiającego śledzenie kontaktów oraz wykrywanie drogi zakażeń koronawirusem za pomocą danych z systemu kontroli dostępu. Inne rozwiązanie specyficzne dla pandemii dostarczyliśmy do dużego szpitala w USA na wschodnim wybrzeżu. Wykorzystano tam nasz system komunikacyjny Sipelia™ oparty na protokole SIP *(Session Initiation Protocol)*, aby umożliwić bezpieczną komunikację z pacjentami chorymi na COVID-19, jednocześnie zmniejszając ryzyko zakażenia przez personel medyczny. Dostosowaliśmy również pracę naszych systemów kontroli dostępu Genetec ClearID™ i Synergis™, które zastosowano w głównym kampusie Genetec w Montrealu, aby umożliwić placówkom opieki zdrowotnej skuteczne zarządzanie dystrybucją środków ochrony indywidualnej.
Patrząc na sektory najbardziej dotknięte pandemią, np. porty lotnicze, byliśmy mile zaskoczeni tym, że wiele dużych projektów na lotniskach jest kontynuowanych zgodnie z planem na 2020 r. Podczas gdy firmy zajmujące się handlem, sportem i rozrywką musiały zostać zamknięte z powodu lockdownu, wiele innych, takich jak przedsiębiorstwa użyteczności publicznej czy dystrybucji ropy i gazu, było w stanie kontynuować podstawową pracę i zdecydowało się wykorzystać ten czas na wykonanie ważnych prac konserwacyjnych i realizację projektów strategicznych.
Polska doświadczyła takich samych skutków pandemii, jak pozostała część Europy i świata. Takie zjawiska, jak zwiększona cyberprzestępczość, nowe zastosowania elektronicznych systemów zabezpieczeń do walki z wirusem SARS-CoV-2 (o czym wcześniej wspomniałem) oraz ogólne przyspieszenie transformacji cyfrowej przyczyniły się do przejścia do chmury lub chmury hybrydowej. Umożliwiają to nasze produkty Genetec™ Security Center i Genetec Mission Control™.
W nadchodzącym roku spodziewamy się dalszego rozwoju w obszarach przemysłowego Internetu Rzeczy, infrastruktury krytycznej i oczywiście inteligentnych miast.

Hikvision Poland

Rok 2020 zaczął się dla nas jak każdy poprzedni. Mieliśmy za sobą pełen sukcesów jubileuszowy 5. rok działalności Hikvision w Polsce, a przed sobą nowe ambitne plany i wyzwania, które z dużym zaangażowaniem zaczęliśmy realizować od pierwszych dni 2020 r. Wszystko szło bardzo dobrze, i choć już pod koniec stycznia zaczęło do nas docierać coraz więcej niepokojących sygnałów na temat pandemii, szybko przekonaliśmy się, że pierwszy kwartał będzie dla nas bardzo udany. Świetnie układały się nasze działania marketingowe i sprzedażowe oraz rozpoczęte projekty wewnętrzne. Wszystko zmieniło się 20 marca, kiedy to musieliśmy opuścić biura i zorganizować pracę w domach. Razem z tysiącami menedżerów w Polsce stanęliśmy w obliczu sytuacji, z jaką nigdy wcześniej nie mieliśmy do czynienia, którą znaliśmy tylko z filmów katastroficznych, a nam przyszło zmierzyć się z nią w rzeczywistości. Stanęliśmy przed próbą umiejętnego dostosowania się do nagle zmieniającego się otoczenia, którą nasz zespół przeszedł wzorowo.

Już kilka dni po wprowadzeniu ograniczeń mieliśmy opracowaną w szczegółach nową strategię i plan działań na czas ograniczeń w gospodarce. Konsekwentnie realizowaliśmy nasze plany w zakresie rozwoju sprzedaży dystrybucyjnej i projektowej, a w odpowiedzi na potrzeby rynku związane z ochroną zdrowia w naszej ofercie pojawiły się urządzenia do pomiaru temperatury. Przez kolejnych kilka miesięcy to właśnie one były najbardziej poszukiwanymi rozwiązaniami na rynku zabezpieczeń, i choć zapotrzebowanie często przewyższało możliwości produkcyjne, udało nam się dostarczyć je do najważniejszych obiektów w kraju. Nie bez znaczenia było również ogromne zaangażowanie naszych partnerów, którzy jak zawsze współpracowali z nami w szerokim zakresie. W kolejnych kilku miesiącach, w ramach pomocy służbie zdrowia w walce z pandemią, dostarczyliśmy bezpłatnie do zakładów opieki zdrowotnej ogromne ilości środków ochrony osobistej dla personelu i kilkanaście zestawów do pomiaru temperatury.
Wraz z odmrożeniem gospodarki wróciliśmy do normalnej, w miarę możliwości, pracy. Musieliśmy co prawda zrezygnować ze wszystkich zaplanowanych aktywności wymagających bezpośredniego kontaktu z klientami, ale prowadząc dziesiątki webinariów, mogliśmy przeszkolić kilkaset osób w szerokim zakresie tematycznym. Ogromnym sukcesem zakończyły się również promocje organizowane dla naszych klientów uczestniczących w programie partnerskim. W drugiej połowie roku wróciliśmy do pierwotnej strategii na rok 2020 i kontynuowaliśmy ją już do końca. Z powodu wielu ograniczeń, jakich doświadczaliśmy w minionym roku, dla wielu firm był on bardzo trudny, choć dla Hikvision zakończył się bardzo dobrze. Kolejny rok z rzędu zanotowaliśmy bardzo wysokie wzrosty sprzedaży, grono naszych klientów poszerza się, podobnie jak nasz zespół, więc z optymizmem patrzymy w rok 2021, mając jednak stale na względzie to, że wciąż operujemy w warunkach pandemii. Nasze założenia na ten rok są ambitne, a lista pomysłów i planów działań do zrealizowania bardzo długa. Tyle że teraz jesteśmy bogatsi o doświadczenia z minionego roku, mamy więc przygotowane najróżniejsze scenariusze możliwych działań.
A jaki będzie 2021 rok – tylko nieliczni podejmują się głośno mówić na temat jakichkolwiek prognoz dla branży security. Na pewno realne jest spowolnienie spowodowane przesunięciami terminów zwłaszcza dużych projektów, mniejszym zapotrzebowaniem na nowe powierzchnie biurowe i handlowe lub szeroko pojętą zmianą modelu pracy w Polsce. Natomiast jesteśmy przekonani, że mimo wszystko istnieje wiele przesłanek, aby bieżący rok był nie mniej udany dla nas i dla naszych Partnerów niż miniony. I tego właśnie życzymy całej branży na ten Nowy Rok!

Johnson Controls



Rok 2020 był dla nas rokiem szczególnym ze względu na wybuch pandemii. Ograniczył wiele naszych aktywności, zwłaszcza możliwości przemieszczania się i spotkań osobistych, a także organizacji szkoleń stacjonarnych. Mimo tych problemów przemodelowaliśmy nasz sposób komunikacji oraz wymiany informacji z klientami. Zorganizowaliśmy cykl szkoleń produktowych w wersji online. Z powodzeniem także zrealizowaliśmy kilka prestiżowych projektów, wśród których znalazł się jeden z najwyższych wieżowców stolicy – Warsaw Unit.

Pandemia COVID-19 nauczyła nas sprawniejszej komunikacji z klientami, ponieważ nie zawsze udawało nam się spotkać z nimi bezpośrednio. Nie zauważyliśmy jednak spadku zainteresowania naszą ofertą, a wręcz przeciwnie – wiemy, że udoskonalając ją oraz nieustannie pozyskując nowe projekty, umacniamy naszą pozycję na rynku security.

W 2021 roku planujemy uzyskanie świadectw dopuszczenia dla nowych produktów, w tym centrali sterującej stałymi urządzeniami gazowymi/SUG, centrali sterującej urządzeniami przeciwpożarowymi, systemu integrującego urządzenia ppoż. Proces certyfikacji stałości właściwości użytkowych chcemy przeprowadzić dla kabla sensorycznego ZETTLER SensorLaser Plus. Nowości te uzupełnią szerokie portfolio naszych produktów.

Linc Polska

Transformacja to określenie, które przez kolejne lata będzie mi się kojarzyć z rokiem 2020. Chociaż jak wszyscy spotykaliśmy się z pewnymi ograniczeniami i obostrzeniami, to miniony rok był dla naszej firmy łaskawy. Oczywiście musieliśmy się przystosować do zmieniającej się rzeczywistości, ale ta sytuacja tylko przyspieszyła podjęcie wielu decyzji, które planowaliśmy już od dawna. W ten sposób uruchomiliśmy cykl szkoleń online dla naszych partnerów. Okazało się, że taka forma kontaktu i edukacji znakomicie się sprawdza. Zdalne spotkania biznesowe pokazały, że wiele rzeczy można omówić, nie tracąc czasu na dojazdy. To pozwala znacznie efektywniej wykorzystywać dostępne zasoby. Ze względu na przeniesienie części procesów do naszych domów mieliśmy także okazję przetestować narzędzia do pracy zdalnej. W efekcie mogliśmy przyspieszyć digitalizację wszystkich realizowanych przez nas działań. Z pewnością zaprocentuje to w najbliższej przyszłości.

W tym trudnym czasie istotne było dla nas także wspieranie naszych biznesowych partnerów. Dlatego staraliśmy się skupiać na tych rozwiązaniach, na które w danym momencie na rynku było największe zapotrzebowanie. W konsekwencji przystosowaliśmy portfolio oferowanych przez nas rozwiązań do zmieniających się oczekiwań klientów. Dużo czasu poświęciliśmy na szkolenia związane z termowizyjnym pomiarem temperatury, wiedząc, jak wiele błędów jest popełnianych w tym zakresie. Zrozumieliśmy, jak ważna i konieczna jest edukacja w obszarze radiometrii. Chcemy, aby oferowane przez nas produkty były sprzedawane we właściwy sposób przez kompetentnych handlowców.
Ze względu na rozwój naszej firmy podjęliśmy decyzję o przeniesieniu się do nowej, bardziej przestronnej lokalizacji. Nowe miejsce zagwarantuje jeszcze lepsze wsparcie działań naszych partnerów. Większa przestrzeń to również większe możliwości. Zmieniamy się, by wraz z Państwem z optymizmem patrzeć w przyszłość.
W tym roku podjęliśmy także decyzję, która wiąże się z kolejną istotną zmianą. Na przestrzeni lat liczba rozwiązań i produktów, jakie wprowadziliśmy do naszego portfolio, znacznie się powiększyła. Z tego względu postanowiliśmy uporządkować nasz asortyment i dwa rodzaje rozwiązań przenieść do nowych firm. Spółka Linc Polska bez zmian pozostaje dystrybutorem sprzętu. Nowo powstała marka Smart-i będzie oferować usługi oraz rozwiązania w chmurze. Z kolei firma VCS – Virtual CTRL Solutions – będzie zajmowała się sprzedażą wież do systemów monitoringu wizyjnego, kołowrotków wejściowych, kontenerów recepcyjnych oraz rozwiązań związanych z alternatywnymi źródłami zasilania. Taki podział oferty na poszczególne firmy pozwala nam na usystematyzowanie struktury wewnętrznej, a także na czytelniejszą formę kanałów sprzedaży.
Z optymizmem patrzymy w rok 2021, mając nadzieję, że sytuacja zacznie powoli się normalizować, a podjęte działania tylko nas umocnią. Wszystkim życzymy przede wszystkim zdrowia.

Milestone Systems

Pandemia ma oczywiście negatywny wpływ na światową gospodarkę i kondycję wielu branż, ale jednocześnie podkreśliła zalety technologii wideo i uwypukliła korzyści z niej płynące, m.in. wsparcie rozwoju Internetu Rzeczy (IoT) i automatyzacji – technologii, o których wiele się mówiło, ale jeszcze nie wszyscy je wprowadzili.

Jeśli chodzi o działalność Milestone, jesteśmy w tej dogodnej sytuacji, że większość naszej pracy można wykonać w domu. Mamy infrastrukturę IT (komputery, VPN, domowe połączenia internetowe) i kulturę, która to wspiera. Na początku pandemii z dnia na dzień we wszystkich regionach wysłaliśmy więc pracowników do domów. Nie musieliśmy dokonywać żadnych zmian w umowach itp., ponieważ zachowaliśmy wszystkie warunki: wynagrodzenia, świadczenia itp. Wszelkie inicjatywy mające na celu obniżenie kosztów, które miały wpływ na warunki zatrudnienia, były podejmowane na zasadzie dobrowolności i w związku z tym poprawki nie były konieczne.
Branża security rośnie, a wymagania i potrzeby użytkowników wciąż ewoluują. Niektóre obejmują integrację z innymi niż kamery dozorowe urządzeniami IoT. Stymulujemy innowacje i zwiększamy wartość dla naszych partnerów, integratorów systemów i klientów końcowych dzięki naszym trzem nowym rozwiązaniom wprowadzonym w 2020 r., a także wzmacnianiu całej społeczności (Marketplace 2.0). Fundamentalnymi czynnikami napędzającymi nasz rynek i zarazem najwyższymi priorytetami Milestone są nadal cyberbezpieczeństwo i zgodność z przepisami dotyczącymi prywatności.

Rok 2020 był wyjątkowy. Firmy musiały szybko dostosować się do nowych realiów i ulepszyć swoje strategie biznesowe, aby ukończyć rozpoczęte projekty, a także dotrzeć do nowych klientów. Zauważyliśmy, że te bezprecedensowe potrzeby faktycznie zmusiły firmy w Polsce do uelastycznienia i kreatywności.
Dziś rola systemów wideo wykracza poza funkcje bezpieczeństwa. Pojawiło się wiele nowych istotnych możliwości pozwalających sprostać wyzwaniom „nowej normalności". Będziemy kontynuować wysiłki w zapewnieniu naszej społeczności i naszym klientom otwartej platformy do zarządzania materiałem wizyjnym. Pracujemy nad nowymi produktami w portfolio, a także przyspieszamy współpracę z partnerami technologicznymi.
W ostatnich kilku miesiącach byliśmy świadkami szybkiego przyspieszania cyfryzacji procesów biznesowych w organizacjach, by mogły zachować zdolność operacyjną, działać zdalnie i wprowadzać nowe usprawnienia. Przykładowo, systemy dozorowe wspomagają teraz firmy w automatyzacji procesów logistycznych, aby mogły minimalizować kontakty osobiste i utrzymać bezpieczny dystans społeczny. Systemy dozorowe już teraz przekształcają środowisko handlu detalicznego, transportu i logistyki oraz coraz bardziej „inteligentne" miasta, pełniąc funkcję „oczu" dla urządzeń Internetu Rzeczy. Rozwój ten będzie przyspieszał w 2021 r.
Naszym celem jest oferowanie klientom najbardziej zaawansowanych i innowacyjnych rozwiązań, nadal będziemy wspierać swoich partnerów w Polsce w sprostaniu rosnącym, złożonym wymaganiom rynku. W roku 2021 będziemy kontynuować wdrażanie zaawansowanych funkcji poprawiających obsługę klienta i zapewniających bezpieczeństwo przy jednoczesnym wzroście wydajności operacyjnej. Milestone, ze swoją otwartą platformą VMS, zapewnia bezpieczne, skalowalne i innowacyjne rozwiązania klientom z różnych sektorów gospodarki w Polsce. W tym roku obserwujemy zwiększony popyt na projekty Smart and Safe City, transport i logistykę, a także opiekę zdrowotną i handel detaliczny.

MIWI-URMET

Analiza wpływu COVID-19 na działalność MIWI-URMET w 2020 r. jest bardzo trudna. Tak naprawdę w normalnym, przewidywalnym otoczeniu działaliśmy jedynie przez dwa, trzy pierwsze miesiące ubiegłego roku. Udało nam się jeszcze w tym czasie zorganizować z sukcesem dla ok. 100 osób, w Sopocie, kolejną edycję konferencji *Innowacyjne Rozwiązania dla Budownictwa* oraz wziąć udział w seminarium zarządców nieruchomości w Łodzi. W marcu znaleźliśmy się w nowej rzeczywistości.

Skala obaw była olbrzymia. Zastanawialiśmy się, ilu pracowników zachoruje, czy będą kontynuowane inwestycje, na które mieliśmy dostarczać nasze systemy i urządzenia, w jakim stopniu wprowadzane przez rząd restrykcje wpłyną na funkcjonowanie gospodarki i naszej firmy, co z dostawami od naszych zagranicznych kontrahentów itd. Na bieżąco wymienialiśmy się informacjami i opiniami z naszymi biznesowymi partnerami. Jak większość firm przeszliśmy profilaktycznie na hybrydową organizację pracy, większość kontaktów z klientami i działania promocyjne (szkolenia, prezentacje itp.) odbywały się zdalnie.
Okazało się, że obawy w dużej mierze były nieuzasadnione. Paradoksalnie to był dobry rok dla firmy w zakresie sprzedaży i zrealizowanej marży. Związane to było głównie z kontynuacją dużych projektów zintegrowanych systemów KD i CCTV. Reasumując, COVID-19 zbytnio nam nie przeszkodził w osiągnięciu zakładanych celów, ale można przypuszczać, że w roku bez pandemii uzyskalibyśmy jeszcze lepsze wyniki.
Z moich obserwacji wynika, że w skali całego 2020 roku COVID-19 nie zahamował znacząco przychodów na krajowym rynku security. Część firm bardzo szybko zareagowała na koniunkturalny wzrost zapotrzebowania na rozwiązania termowizyjne, systemy wideo i interkomowe, rekompensując sobie w ten sposób spadki popytu w innych grupach asortymentowych. Natomiast wypowiadanie się nt. perspektyw polskiego rynku security w 2021 r. jest niezmiernie trudne. Wiadomo, że jest on ściśle skorelowany z całą światową gospodarką, w tym oczywiście gospodarką Polski. Należy liczyć się ze zmniejszeniem wydatków na inwestycje (m.in. w obszarze hoteli, biurowców, centrów handlowych czy lotnisk cywilnych), a w konsekwencji z ograniczeniem wydatków na systemy zabezpieczeń. W bieżącym roku można natomiast spodziewać się realizacji projektów rozpoczętych wcześniej. Część sektorów nadal będzie się rozwijała ze względu na ich strategiczne znaczenie i finansowanie ze środków publicznych. Zwiększy się również zainteresowanie nowoczesnymi technologiami w zakresie analityki, wykorzystywanymi w systemach kontroli dostępu i monitoringu wizyjnego.
Plany naszej firmy na 2021 r. uwzględniają w sposób oczywisty wszystkie wymienione zagrożenia oraz przewidywane szanse. Wiadomo, że w sytuacji dużej nieprzewidywalności otoczenia gospodarczego horyzont planowania uległ znacznemu skróceniu.
Jesteśmy jednak umiarkowanymi optymistami. Zakładamy kontynuację dostaw naszych systemów na inwestycje o strategicznym znaczeniu dla kraju. Szybki rozwój technologii, głównie w zakresie analityki, w systemach będących w ofercie firmy, jest szansą na zwiększenie naszej konkurencyjności, co nawet przy kurczącym się rynku security daje nam nadzieję na osiągnięcie dobrych wyników. Przewidujemy też większą dynamikę sprzedaży zaawansowanego technologicznie systemu sygnalizacji pożarowej HOCHIKI & NSC z hybrydową funkcją bezprzewodową, będącego od zeszłego roku w naszej ofercie. Nadal będziemy oferować naszym klientom (integratorom, administratorom systemów, projektantom) szkolenia oraz wsparcie techniczne i wsparcie projektowe oraz pomoc przy uruchomieniu.
Zakładamy, że duża mobilizacja całej załogi firmy, atrakcyjność oferty, rozwój współpracy z kluczowymi klientami oraz pozyskanie nowych partnerów biznesowych pozwoli nam zrealizować założone cele.

Nedap Security Management

Paradoksalnie rok 2020, który był rokiem kryzysu, po raz kolejny wzmocnił naszą pozycję na polskim rynku. Nedap Security Management osiągnął rekordowe przychody w Polsce. Sytuacja spowodowana pojawieniem się wirusa SARS-CoV-2 zaskoczyła nas wszystkich, była na początku wielką niewiadomą i wyzwaniem. Jednak kolejne miesiące pokazały, że dobrze odnaleźliśmy się w dynamicznie zmieniającej się sytuacji. Nawiązaliśmy współpracę z nowymi klientami z sektora automotive, real estate, finansowego, ubezpieczeń czy produkcji katod do akumulatorów. Korzystając z okazji, chcieliśmy podziękować naszym obecnym klientom i partnerom za okazane zaufanie, które pozwoliło nam na osiągnięcie tak znakomitych wyników w 2020 r.

Obserwujemy wpływ pandemii na funkcjonowanie naszego rynku, jednak nie przewidujemy spowolnienia wzrostu przychodów ze sprzedaży w Polsce w nadchodzącym roku. Zakładamy, że dobre wyniki w ubiegłym roku oraz rozpoczęte projekty będą fundamentem do dalszego dynamicznego wzrostu.
Nedap, jako globalna firma technologiczna, kładzie duży nacisk na rozwój i w tym roku nieprzerwanie będzie inwestować w nowości. Kolejną istotną kwestią jest postęp we współpracy z certyfikowanymi partnerami, budowanie ich kompetencji i wspieranie we wspólnie realizowanych projektach. Dużą dynamikę wzrostu zakładamy także we współpracy z partnerami technologicznymi, dlatego też cały czas rozwijamy zakres integracji, z których mogą korzystać nasi klienci w takich obszarach, jak biometria, czytniki mobilne, integracje z windami czy visitor management system.
Pandemia bardzo wpłynęła na formę naszej codziennej pracy. Mając na uwadze zdrowie naszych pracowników, partnerów handlowych i klientów, realizujemy szkolenia w formie online. Zależy nam jednak na odejściu od standardowej formy webinariów, która naszym zdaniem już się wyczerpała. Pilnie pracujemy, aby w najbliższych miesiącach wypuścić nową serię szkoleń w zupełnie nowej odsłonie. Zaplanowaliśmy wiele nowych działań mających na celu szerzenie wiedzy o bezpieczeństwie i dostosowaliśmy ich formę do obecnych realiów.
Życzymy czytelnikom a&s bezpieczeństwa na co dzień – to dla nas szczególnie ważne, ponieważ uważamy, że bezpieczeństwo to nie tylko technologia, to ludzie i ich codzienne życie.

POLON-ALFA

Rok 2020 dla POLON ALFA był czasem wyjątkowym – okresem zmian w wielu obszarach, olbrzymiego zaangażowania i wytężonej pracy całego zespołu (ogromne podziękowania), realizacji ambitnych celów, ale przede wszystkim satysfakcji z faktu, że możemy jeszcze lepiej i sprawniej odpowiadać na potrzeby klientów.

Pierwsze miesiące 2020 r. to prace finałowe nad nową halą produkcyjno-magazynową o powierzchni 8 tys. m^2, znacznie poszerzającą nasze możliwości produkcyjne. To również doposażanie nowych linii produkcyjnych w najnowsze zdobycze techniki, dzięki czemu produkcja urządzeń z logo POLON-ALFA może przebiegać zgodnie z najnowszymi trendami. Ta olbrzymia inwestycja w przyszłość pozwoli nam jeszcze szybciej rozwijać się nie tylko lokalnie, ale także poza Polską i Europą.
Koniec pierwszego kwartału 2020 r. zbiegł się z początkiem pandemii COVID-19 w Polsce, która przyniosła niespotykane dotychczas ograniczenia w bezpośrednich kontaktach, a co za tym idzie konieczność przeformułowania zasad działania na wielu płaszczyznach. Z jednej strony pozwoliła nam zrozumieć, że wiele rzeczy można zrobić online, z drugiej – uświadomiła, jak bardzo może nam brakować bezpośrednich spotkań.
Pandemia w przypadku firmy POLON-ALFA nie wpłynęła na redukcję zatrudnienia, wręcz przeciwnie – powiększyliśmy grono pracowników w Polsce o kilkadziesiąt osób, wzmocniliśmy zespół specjalistów technicznych i handlowych, powiększyliśmy także zespół pracowników produkcyjnych, odpowiadając na zwiększone zapotrzebowanie na nasze rozwiązania.
POLON-ALFA nieustannie pracuje nad rozwojem koncepcji oraz idących za tym konkretnych rozwiązań i urządzeń wspierających bezpieczeństwo pożarowe. Nie inaczej będzie w roku 2021. Dalej rozwijamy niezwykle dobrze przyjętą serię POLON 6000, dedykowaną średnim i dużym obiektom, dodajemy adresowalne podcentrale: gaszeniowe, wykrywania gazu, dużą gamę adresowalnych urządzeń uzupełniających. Jeszcze w pierwszym kwartale br. wprowadzimy do sprzedaży nowe, małe centrale wykrywania gazu, a w drugiej połowie roku możemy się spodziewać nowoczesnej, odpowiadającej na dzisiejsze potrzeby linii rozwiązań dedykowanych bezpieczeństwu pożarowemu w małych i średnich obiektach.
Wpływ pandemii na rynek security w Polsce, z naszej perspektywy, nie jest jednoznaczny. W konsekwencji przeciągającej się sytuacji zagrożenia pandemicznego można się spodziewać ograniczenia inwestycji, szczególnie w obszarze obiektów biurowych, hoteli czy szeroko pojętej rozrywki, w tym obiektów sportowych. Ze względu na przesunięcie czasowe realizacji systemów zabezpieczeń w nowych inwestycjach przyjdzie nam się mierzyć z tymi problemami w najbliższych i nieco bardziej odległych kwartałach. O ile w przypadku hoteli i obiektów sportowych możemy się spodziewać wyraźnego odbicia po ustąpieniu pandemii, o tyle w przypadku powierzchni biurowych negatywny trend może utrzymywać się dłużej.
Reasumując, życzymy wszystkim dobrego 2021 roku, szybkiego powrotu do normalności, bliskich, satysfakcjonujących kontaktów, rynku zabezpieczeń co najmniej tak dobrego jak w ostatnich latach. Do usłyszenia, zobaczenia, do spotkania... już niedługo.

Roger

Rok 2020 był wyjątkowy i zapewne pozostanie w naszej pamięci na długie lata. Po wybuchu pandemii pod koniec I kwartału w efekcie zamrożenia gospodarek zanotowaliśmy znaczny spadek obrotów w kwietniu i maju. W kolejnych kwartałach rynek się odbudował, co ostatecznie pozwoliło zamknąć rok 2020 z zaplanowanym wzrostem sprzedaży.

Główny produkt firmy, jakim jest system kontroli dostępu i automatyki budynkowej RACS 5, umacniał się w ciągu roku na rynku projektowym. Zarówno wykonawcy, jak i inwestorzy docenili potencjał funkcjonalny, stabilność, szeroko rozumiane wsparcie techniczne oraz wysoki poziom bezpieczeństwa oferowanego przez system i z coraz większym przekonaniem decydowali się na jego wybór. W ciągu roku ogólna liczba przejść obsługiwanych przez systemy RACS 5 powiększyła się o kolejne 20 tys. i była ponad 20% większa niż w roku 2019.
W minionym roku z sukcesem wdrożyliśmy nasze rozwiązania w wielu prestiżowych obiektach. Głównie były to biurowce, obiekty sektora publicznego, uczelnie wyższe, szpitale, infrastruktura krytyczna i zakłady przemysłowe. W znacznej mierze sukcesy te były efektem prac przygotowawczych, które rozpoczynaliśmy z naszymi partnerami w latach 2018-19. Korzystając z okazji, chciałbym serdecznie podziękować wszystkim naszym partnerom biznesowym oraz przekazać im wyrazy uznania, ponieważ to właśnie dzięki nim w tym trudnym czasie możliwe było osiągnięcie pomyślnego wyniku w roku 2020. Z opinii, jakie słyszymy od naszych klientów, wynika, iż doceniają polski produkt, który już od kilku lat udowadnia swoją stabilność w obiektach liczących po kilkaset przejść oraz wysoki poziom oferowanej przez firmę obsługi klienta.
W ubiegłym roku oferta firmy została poszerzona o depozytory kluczy serii RKD32, co spotkało się z dużym zainteresowaniem rynku. Wdrożone do oferty depozytory kluczy mogą pracować zarówno autonomicznie, jak i być elementem systemu kontroli dostępu RACS 5, co jest ich istotnym walorem, pozwala bowiem uprościć i ulepszyć proces zarządzania i użytkowania budynku w ramach jednej platformy oprogramowania.
W roku 2020 prace rozwojowe były skupione wokół integracji systemu RACS 5 z innymi systemami współbieżnie wykorzystywanymi w nowoczesnych budynkach. Działania te zaowocowały nowymi lub ulepszonymi integracjami z systemami alarmowymi, systemami wind wiodących dostawców oraz integracjami z kolejnymi platformami SMS, VMS oraz PSIM.
W 2021 roku mamy w planach dalszy rozwój oprogramowania pod kątem integracji. Kierunki rozwoju wyznaczają nam z jednej strony pozyskane projekty, z drugiej – systemy kontroli dostępu wiodących zachodnich dostawców. Chcemy również wprowadzić do oferty uproszczoną wersję systemu RACS 5, która znajdzie zastosowanie w mniejszych instalacjach, oraz inne nowe produkty i rozwiązania, o których będziemy informować na bieżąco.
Z informacji dostępnych w strefie publicznej wynika, że pandemia szybko nie przeminie i jesteśmy świadomi możliwego spowolnienia gospodarczego. Liczymy, że program ożywienia gospodarczego z funduszy Unii Europejskiej będzie w znacznej mierze kompensował negatywne skutki pandemii, niemniej zakładamy, że w ostatecznym rozrachunku gospodarki w latach 2021–2022 nie będą w stanie uzyskać poziomu rozwoju obserwowanego przed pandemią.

SATEL

Nowa rzeczywistość – bo tak możemy określić to, co w 2020 r. przyniosło pojawienie się koronawirusa SARS-CoV-2 – zmusiła nas wszystkich do zmiany nie tylko przyzwyczajeń, ale także podejścia do pracy. Nikt nie wiedział, jak długo potrwają wprowadzane obostrzenia i jak będzie zmieniać się ich skala. Konieczne było więc wdrożenie środków bezpieczeństwa na terenie firmy.

Chodziło o to, aby zachować ciągłość produkcji, jednocześnie jak najmniej ograniczając swobodę działania osób biorących udział w poszczególnych procesach, co stanowiło nie lada wyzwanie. Z kolei duża część pracowników biurowych przeszła w tryb pracy zdalnej. W przypadku działów takich jak R&D było to dużym przedsięwzięciem. Wymagało ogromnej elastyczności nie tylko od pracodawcy (udostępnienie sprzętu i wszelkich zaawansowanych narzędzi informatycznych), ale także od pracownika, aby był w stanie w domowym zaciszu wygospodarować przestrzeń dla nierzadko wielu różnych naszych produktów. W obliczu tak dużego rozproszenia zespołu kluczową kwestią był sprawny przepływ informacji. W tym celu wdrożyliśmy różnego rodzaju komunikatory i wspólne bazy wiedzy. Ponadto duża część procesów wewnątrz firmy została zautomatyzowana, m.in. w obszarze obsługi klientów i dystrybucji. W związku ze stanem epidemii wstrzymaliśmy szkolenia i spotkania biznesowe *face to face*. One także zostały przeniesione do sfery cyfrowej. Przykładem może być wdrożony program webinariów, czyli szkoleń i prezentacji online dla instalatorów i przedstawicieli dystrybucji.
Odpowiedzią rynku na nową sytuację na świecie było zwiększone zapotrzebowanie na instalacje SSWiN, zwłaszcza ze strony inwestorów prywatnych oraz małych i średnich firm, wynikające z rosnących w tym okresie obaw o bezpieczeństwo obiektów i mienia. Choć początkowo lockdown uniemożliwiał instalatorom realizację zleceń, to po czasie, wraz z luzowaniem obostrzeń, liczba nowych zamówień stopniowo rosła. W przypadku odbiorców z sektora przemysłowego większym zainteresowaniem zaczęły się cieszyć narzędzia do automatyzacji procesów. Kluczowa okazała się możliwość komunikacji z systemami automatyki oraz zdalne zarządzanie nimi. Zaobserwowaliśmy wzmożony popyt na rozwiązania bezprzewodowe.
Ogólnoświatowa niepewność związana z pandemią i jej gospodarczymi skutkami wyhamowała część branż, jednocześnie wpływając na rozwój innych. Kondycja przedsiębiorstw w ostatnim roku zależała przede wszystkim od rodzaju prowadzonej działalności (produkcja, handel, instalacje) oraz możliwości szybkiej adaptacji rozwiązań, produktów lub usług do nowych warunków społecznych i gospodarczych. W wielu przypadkach zmieniły się priorytety, konieczne były reformy wewnątrz organizacji – wprowadzenie nowych kompetencji, korekty procedur, nowe technologie.

W roku 2021 firma Satel planuje rozwijać się zgodnie z aktualnymi wymaganiami klientów – stawiamy na rozwój oferty automatyki budynkowej, systemów bezprzewodowych oraz nowoczesnych narzędzi dla komunikacji i zdalnego zarządzania systemami. Są to bowiem kierunki, w których naszym zdaniem podąża rynek, szczególnie istotne mogą okazać się systemy zintegrowane.
Na koniec należy zauważyć, że dzisiaj (styczeń 2021 r.) trudno oceniać szanse i zagrożenia dla branży – wszystko zależy od stanu gospodarki krajowej i światowej oraz jego wpływu na sytuację ekonomiczną gospodarstw domowych oraz przedsiębiorstw czy instytucji.

Schrack Seconet Polska

Pandemia i jej skutki będą miały ogromny wpływ na funkcjonowanie rynku w ciągu najbliższych kilku lat. Mimo wielu niewiadomych, które może ze sobą przynieść 2021 r., chcemy nadal utrzymywać realizację naszych celów i zobowiązań na tym samym, wysokim poziomie. W roku 2020, mimo nie najlepszej sytuacji rynkowej, udało nam się osiągać wszystkie postawione cele, a plany sprzedażowe zdecydowanie przekroczyć. Nadal się rozwijamy – do zespołu handlowego w Warszawie i w Gdańsku dołączyło w ostatnim roku dwóch doświadczonych menedżerów, co także przyczyniło się bardzo dobrych wyników firmy w 2020 r.

W bieżącym roku możemy się spodziewać kontynuacji ograniczeń oraz przesunięć terminów realizowanych inwestycji. Wyzwaniem dla nas na rok 2021 jest przede wszystkim utrzymanie firmy w jak najlepszej kondycji, a samego wyniku na poziomie nie gorszym niż w minionym roku. Dziś możemy mówić wyłącznie o przewidywaniach, przeprowadzać szczegółowe analizy aktualnej sytuacji w poszczególnych sektorach i mieć nadzieję, że dynamiczny polski rynek budowlany podoła trudnościom związanym ze skutkami pandemii. Dobrym prognostykiem na pewno są pozytywne nastawienie i nastroje większości naszych partnerów biznesowych w odniesieniu do aktualnej sytuacji rynkowej w branży systemów bezpieczeństwa.
Jako firma nie zamierzamy zwalniać tempa, odnajdujemy się w tej niecodziennej sytuacji, dostosowaliśmy nasze działania do warunków panujących na świecie. W minionym roku nie odnotowywaliśmy opóźnień w dostawach towarów, zachowując jednocześnie ciągłość produkcji. Nie spodziewamy się, by ta sytuacja uległa zmianie w bieżącym roku.
Rozpoczęty 2021 rok to dla nas wiele wyzwań. W najbliższych miesiącach planujemy wprowadzić na rynek polski nowe rozwiązania, m.in. najnowszą generację central sygnalizacji pożarowej Integral EvoxX czy produkt związany ze sterowaniem urządzeniami pożarowymi, który umożliwi nam zaoferowanie partnerom kompleksowego rozwiązania: począwszy od detekcji, poprzez sterowanie, a skończywszy na zasilaniu urządzeń przeciwpożarowych (np. wentylatory pożarowe) i certyfikowanym systemie zarządzania bezpieczeństwem pożarowym SIS-FIRE. Prace nad tymi rozwiązaniami rozpoczęliśmy wiele miesięcy temu. Rynek związany z systemami bezpieczeństwa pożarowego skupiony jest dziś mocno na sterowaniu urządzeniami przeciwpożarowymi, ich zasilaniu oraz na certyfikowanych systemach zarządzania bezpieczeństwem pożarowym. To właśnie na tych obszarach będziemy koncentrować nasze prace i działania w najbliższym czasie.
Trwająca już rok pandemia wpłynęła także na wzrost zainteresowania narzędziami zdalnego dostępu do systemów sygnalizacji pożarowej Schrack Seconet – Integral Remote. Rozwiązania te umożliwiają dostęp online do wszystkich podstawowych funkcji systemu Integral IP, dając gwarancję kontroli obiektu przez 24 godziny na dobę oraz realizację większości prac serwisowych bez konieczności wizyty w obiekcie. Takich rozwiązań potrzebuje dziś rynek, aby jeszcze bardziej zwiększyć nie tylko bezpieczeństwo obiektów, ale przede wszystkim ludzi.
Mimo całej nietypowej, nadal trudnej dla wszystkich sytuacji patrzymy z optymizmem w przyszłość. Czujemy ogromne wsparcie partnerów, codziennie wspólnie wdrażamy nasze rozwiązania w wielu ciekawych technologicznie obiektach w Polsce. Ogromnie nas cieszy zadowolenie klientów, którzy w kolejnych swoich inwestycjach stawiają poprzeczkę coraz wyżej, dając nam tym samym szansę na ciągłe udoskonalanie naszych produktów w odniesieniu do wymagającego rynku w Polsce.
Wierzymy, że systematyczne działania, przede wszystkim ich dostosowanie do zmieniających się warunków, pozwolą nam na utrzymanie stabilnej pozycji na polskim rynku systemów bezpieczeństwa pożarowego.

Securitas Polska

Rok 2020 był na pewno trudny. Zagrożenie, z jakim przyszło się nam mierzyć oraz ograniczenia z tego wynikające to coś, czego nikt nie przewidywał. Mimo wszystko myślę, że pierwszy szok został zastąpiony energią i mobilizacją do działania. Od razu określiliśmy trzy priorytety w naszej działalności. Po pierwsze bezpieczeństwo naszych pracowników. Po drugie pełne możliwe wsparcie dla naszych klientów. Po trzecie twarde zasady w zakresie zachowania płynności finansowej – bez tego nie bylibyśmy w stanie realizować dwóch pierwszych zadań.

Dość szybko, we współpracy z naszymi klientami, opracowaliśmy i wdrożyliśmy stosowne procedury i jasne zasady wspólnego funkcjonowania. Zadbaliśmy o bezpieczeństwo naszych pracowników, zapewniając im dostęp do środków ochrony, tym samym zachowaliśmy ciągłość realizacji usług.

Paradoksalnie czasy kryzysu powinny być szansą dla branży ochrony, bo właśnie w takich sytuacjach ryzyko zagrożeń rośnie. Poza tym każdy kryzys, tak jak każda rewolucja, zmusza do kreatywnego myślenia, szukania rozwiązań, innowacji. W tym konkretnym przypadku nie było inaczej. Uruchomiliśmy nowe usługi będące odpowiedzią na zapotrzebowanie rynku, takie jak dekontaminacja. Odnotowaliśmy przyspieszony rozwój produktów i rozwiązań technicznych, które umożliwiają ograniczenie kontaktu pomiędzy ludźmi i zdalną obsługę wybranych procesów. Automatyczny pomiar temperatury, zliczanie i limitowanie osób, elektroniczne systemy awizacji (Securitas smartIN i Securitas smartGATE), systemy zdalnego nadzoru wizyjnego z analityką obrazu to tylko część elementów, które w ubiegłym roku cieszyły się zwiększonym zainteresowaniem.

Nie obyło się bez wyzwań. Kilkakrotnie mieliśmy do czynienia z różnego rodzaju ograniczeniami, lockdownami, przerwami w produkcji, które w efekcie były przyczyną czasowego ograniczania przez klientów składu osobowego zespołów ochrony. Odnotowaliśmy też kilka przypadków zawieszenia działalności biznesowej, co wiązało się z ustaniem kontraktów, część klientów ze względu na zagrożenia spowolniła procesy przetargowe i zakupowe lub odsunęła je w czasie. Wielu naszych klientów postanowiło zainwestować w technikę, tak aby w perspektywie długofalowej uzyskać odpowiedni efekt optymalizacji kosztów, przy jednoczesnym podniesieniu jakości systemów bezpieczeństwa.

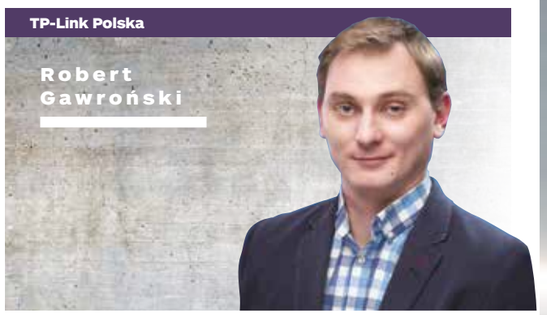
Uważam, że rok 2020 dla branży ochrony był dobrym rokiem, szczególnie dla firm, które nie boją się wyzwań, innowacji i zatrudniają pracowników potrafiących mierzyć się z problemami. Oczywiście żelazna dyscyplina kosztowa na pewno nie pozostała tutaj bez znaczenia.
Wiele wskazuje na to, że rok 2021 będzie dość podobny. Przynajmniej w kwestii zagrożeń niewiele się zmieni, więc i nasze priorytety na razie pozostają niezmienne. Dla branży widzę nadal szansę na rozwój nowych kierunków, choć zapewne nie wszyscy wytrzymają trudne warunki działania, mierząc się chociażby z odroczonymi płatnościami ze strony klientów czy też brakiem zasobów i możliwości sprostania specyficznym oczekiwaniom.
Wierzę, że z tej całej sytuacji wyjdziemy silniejsi, przede wszystkim jako ludzie i zespoły, a co za tym idzie również jako firma.

SUMA SOLUTIONS

Rok 2020 był dla branży, ze względu na rozwój pandemii COVID- 19, na pewno inny niż poprzednie. Dla nas pod względem finansowym nie różnił się znacząco od poprzednich, a firma wypracowała nawet większą sprzedaż. Obawy, które pojawiły się na początku pandemii o ciągłość dostaw, opóźnienia w realizacji zaplanowanych inwestycji, spadek wolumenu sprzedaży, zarażenia pracowników i związane z tym ograniczenie działalności, na szczęście w naszym przypadku się nie potwierdziły.

Zdywersyfikowana grupa klientów pozwoliła nam przejść przez ten rok bez większych turbulencji. Nie odnotowaliśmy ani spadku sprzedaży, ani pogorszenia dyscypliny płatniczej. Dostosowaliśmy strategie do przewidywań. Jednak sporo firm instalacyjnych, szczególnie mniejszych, które nie były przygotowane finansowo do dłuższych przestojów, zamknęło lub zawiesiło swoją działalność.
Z powodu pandemii COVID-19 zwiększyło się zainteresowanie systemami zdalnego dozoru, zliczania osób, analizy wizyjnej i sztucznej inteligencji, pomocnych w zachowaniu wymaganego dystansowania społecznego. Szczególnie właściciele sklepów wielkopowierzchniowych intensywnie poszukiwali kamer wyposażonych w odpowiednie oprogramowanie, dostarczających informacji w czasie rzeczywistym o liczbie osób w obiekcie, wykrywających osoby bez maseczki.
Trudno dzisiaj jednoznacznie prognozować, jak będzie wyglądał rynek security w 2021 roku. Niewątpliwie część inwestycji, projektów i wdrożeń systemów bezpieczeństwa została lub zostanie odłożonych czy to ze względu na oszczędności, czy ograniczenia związane z COVID-19. Można się jednak spodziewać, że nie jest to sytuacja stała i po zniesieniu ograniczeń związanych z pandemią inwestycje security zostaną wznowione.

TP-Link Polska



Kryzys związany z pandemią koronawirusa na szczęście nas nie dotknął. Podobnie jak chyba cała branża security czy też szeroko rozumiane IT, zauważyliśmy wzrost popytu na nasze produkty, który był na tyle duży, że nawet okresowo pojawiały się problemy z dostępnością urządzeń. To przełożyło się na świetne wyniki finansowe w 2020 roku.

Organizacyjnie pandemia COVID-19 stanowiła pewnego rodzaju wyzwanie. Cały nasz zespół i wszystkie procesy wewnątrz firmy trzeba było szybko przystosować do pracy zdalnej, zmieniły się formy i kanały komunikacji z partnerami i klientami. Na szczęście nasz zgrany i dynamiczny zespół świetnie poradził sobie z tym zadaniem.
Zanotowaliśmy kilkudziesięcioprocentowe wzrosty sprzedaży naszych przełączników PoE, które są stosowane przy instalacjach monitoringu CCTV. Najdynamiczniej rosła sprzedaż małych, kilkuportowych switchy, które są najczęściej używane do domowych systemów dozorowych. Z rozmów z naszymi partnerami wynika, że to był dobry rok dla całej branży. Mimo początkowych obaw przez cały rok nie brakowało nowych projektów.
W tym roku TP-Link planuje mocniej zaznaczyć swoją obecność na rynku security. Poza dalszym poszerzaniem portfolio urządzeń sieciowych planujemy wprowadzenie na rynek również serii kamer CCTV pod własną marką. Największą szansą w 2021 r. będzie oczekiwane przez wszystkich odmrożenie gospodarki. Ponowne otwarcie galerii handlowych, hoteli i restauracji to szansa na nowe projekty od klientów z tych sektorów. Znakiem zapytania pozostają projekty realizowane przez jednostki administracji publicznej. Istnieje ryzyko, że ogromne środki inwestowane przez rząd w walkę z epidemią i tarcze antykryzysowe odbiją się na kondycji „budżetówki" i jednostki te nie będą miały środków na inwestycje.

Rynek security w Europie

Przeważa ostrożny optymizm

Po trudnym pandemicznym roku na rynku zabezpieczeń technicznych branża patrzy w przyszłość z ostrożnym optymizmem. Jaki jest obecny stan rynku security w Europie? Czego spodziewamy się w 2021 roku?

a&s International

Europa mocno ucierpiała na skutek pandemii COVID-19. Według danych Worldometers z grudnia 2020 r. wirus SARS-CoV-2 zakaził na Starym Kontynencie prawie 30 mln osób, z czego zmarło ponad 600 tys. chorych.

Pandemia wywołała ogromne perturbacje w biznesie. Europejskie firmy zmagały się z dużymi problemami spowodowanymi albo zamknięciem i wstrzymaniem ich pracy, albo znacznymi utrudnieniami w wykonywanej działalności. W raporcie McKinsey z października 2020 r. podano, że 11% europejskich małych i średnich przedsiębiorstw spodziewa się ogłoszenia upadłości w ciągu pół roku. Z kolei w innym raporcie (GlobalData) podano, że w kwietniu 2020 r., czyli w szczytowym momencie pierwszej fali pandemii, z powodu COVID-19 ponad 20% projektów w Europie, na Bliskim Wschodzie i w Afryce zostało znacznie opóźnionych lub anulowanych. A to ma ogromny wpływ na europejski rynek zabezpieczeń.

– *Na skutek pandemii ludzie faktycznie nie są w stanie dotrzeć na miejsce, aby wykonywać swoją pracę, np. instalację urządzeń. To oczywiście opóźniło realizację wielu projektów. Zmniejszono także budżety na inwestycje, a zaplanowane instalacje zostały opóźnione z powodu koniecznych zamknięć w czasie lockdownu* – zauważa Phillip Antoniou, wiceprezes ds. sprzedaży na region EMEA i APAC w firmie MOBOTIX.

TEN ROK ZAPOWIADA SIĘ LEPIEJ

Prognozy na ten rok są dla Europy bardziej optymistyczne. Bank Światowy przewiduje, że PKB strefy euro wzrośnie o 3,6% (po spadku o 7,4% w 2020 r.). To ważny wskaźnik, który będzie skutkował odmrożeniem części wstrzymanych projektów. Rynek wciąż czeka także na powrót do względnej normalności sprzed pandemii, który jest spodziewany, gdy uzyskamy tzw. odporność stadną w Europie.

– *Mamy nadzieję, że tradycyjny rynek security odżyje, gdy sytuacja ustabilizuje się wraz z postępem w realizacji programów szczepień* – komentuje Malou Toft, wiceprezes na region EMEA w Milestone Systems.

– *W 2021 r. spodziewamy się wzrostów na rynku zabezpieczeń, a wnioski wyciągnięte z ubiegłego roku i powszechne szczepienia powinny pomóc branży w lepszym zarządzaniu sytuacją związaną z pandemią* – przewiduje Verena Rathjen, wiceprezes ds. sprzedaży EMEA w Axis Communications.

NOWA NORMALNOŚĆ – NOWE OCZEKIWANIA

Wraz z przygotowywaniem się do życia w „nowej normalności" pojawiają się nowe wymagania w zakresie bezpieczeństwa. Rola elektronicznych systemów zabezpieczeń dzięki rozwojowi nowych technologii rozszerzyła się ze swej tradycyjnej domeny ochrony osób i mienia na nowe obszary: wsparcie użytkowników w cyfryzacji biznesu, ograniczanie infekcji i ich kontrola.

– *Pandemia miała negatywny wpływ na światową gospodarkę i wiele gałęzi przemysłu, w tym branżę security. Jednocześnie przyniosła wiele potencjalnych korzyści i zastosowań technologii wizyjnych, które znacznie wykraczają poza tradycyjną funkcję zabezpieczeń* – zauważa Malou Toft z Milestone. – *Kamery dozorowe pomagają teraz firmom w kontroli dystansu społecznego, ograniczają interwencje i automatyzują procesy logistyczne. Wygląda na to, że ten rozwój będzie wciąż przyspieszał i stanie się silnym motorem wzrostu w tym roku i kolejnych latach.*

Europejski rynek security nie uniknął skutków pandemii. Zmieniły się potrzeby i wymagania klientów, pojawiły się nowe wyzwania w łańcuchach dostaw, a klienci i pracownicy przeszli z trybu pracy stacjonarnej na pracę zdalną. W rezultacie wzrosło zapotrzebowanie na specyficzne rozwiązania security, pomocne w rozwiązywaniu nowych problemów.

– *Na pierwszy plan wysunęły się bezdotykowe systemy kontroli dostępu, rozwiązania do zliczania osób oraz systemy zdalnego monitorowania wspierane zaawansowaną analizą audio i wideo. Technologie te wdrożono, aby sprostać dzisiejszym wyzwaniom, ale nie stracą na aktualności w przyszłości, nawet jeśli cel i zakres ich zastosowania się zmieni* – prognozuje Verena Rathjen z Axis Communications.

GDZIE ROŚNIE POPYT NA SECURITY

Zastosowania elektronicznych systemów zabezpieczeń mogą w niektórych sektorach przynieść korzyści i nowe możliwości, zwłaszcza że są one zgodne z przepisami dotyczącymi ochrony zdrowia po pandemii. Jedną z takich branż jest służba zdrowia. Stosowanie rozwiązań ze zintegrowaną analityką obrazu w urządzeniach brzegowych może na przykład wesprzeć lekarzy w diagnostyce pacjenta i monitorowaniu jego parametrów życiowych w czasie rzeczywistym.

– *Sektor opieki zdrowotnej stał się dla nas jeszcze ważniejszy niż dotąd. Wykorzystanie algorytmów analizy obrazu do wykrywania maseczek na twarzy i kontroli zachowania dystansu społecznego, mierzenie*

Z POWODU COVID-19 W EUROPIE, NA BLISKIM WSCHODZIE I W AFRYCE ZOSTAŁO ZNACZNIE OPÓŹNIONYCH LUB ANULOWANYCH PONAD 20% PROJEKTÓW

temperatury stają się obecnie wymogiem w funkcjonowaniu placówek służby zdrowia – powiedział Phillip Antoniou z MOBOTIX.

Zapotrzebowanie na rozwiązania związane z zachowaniem środków bezpieczeństwa w dobie pandemii COVID-19 wzrośnie również w obiektach infrastruktury krytycznej. Ich menedżerowie zmagają się z problemami w utrzymaniu ciągłości działania przy zmniejszonej liczbie pracowników.

– *Pandemia może powodować większą gotowość do inwestowania w zabezpieczenia w pewnych sektorach, np. w infrastrukturę krytyczną. Wiele firm ma już świadomość, jak w tych szczególnych czasach ważne jest bezpieczeństwo przedsiębiorstw niezbędnych do funkcjonowania całego społeczeństwa, m.in. dostarczających energię czy wodę, przy jednoczesnym ograniczeniu kontaktów międzyludzkich do niezbędnego minimum* – ocenia Verena Rathjen z Axis Communications.

Oczekuje się również wzrostu wydatków na systemy zabezpieczeń w sektorze publicznym, nie tylko na walkę z COVID-19, ale także w ramach realizacji strategii *smart city* w obliczu postępującej urbanizacji. W wielu europejskich krajach sektor publiczny wprowadził limity osób mogących jednocześnie przebywać w określonym miejscu oraz inne rygorystyczne wymagania związane z utrzymaniem reżimu sanitarnego, m.in. konieczność noszenia maseczek na twarzy. Podobne regulacje dotyczą także atrakcyjnych turystycznie miejsc, skupiających zazwyczaj dużo ludzi.

Wstrzymane zostały natomiast nowe inwestycje w kontrolę dostępu w budynkach biurowych i hotelach. Eksperci spodziewają się, że rynek hotelowy i nieruchomości komercyjnych zacznie się powoli dźwigać od połowy roku, będzie to jednak zależało od aktualnej sytuacji epidemicznej i rządowych restrykcji nałożonych na te sektory.

RODO NA STRAŻY DANYCH OSOBOWYCH

Dominujące na europejskim rynku zabezpieczeń trendy wskazują na większą popularność analizy danych wizyjnych w chmurze i urządzeniach brzegowych. Bezpieczeństwo oparte na chmurze (systemy dozoru wizyjnego, kontroli dostępu, sygnalizacji włamania i napadu) będzie rosło wraz z większą gotowością do adaptacji. Częściej będą też wdrażane inteligentne i wszechstronne systemy kamer sieciowych – będzie to miało większy sens biznesowy w perspektywie rozwoju technologii IoT i topologii sieci.

– *W sektorze dozoru wizyjnego spodziewamy się podejścia bardziej horyzontalnego, wdrażania inteligentnych rozwiązań na serwerach i w chmurze, które zwiększą wydajność i efektywność* – ocenia Verena Rathjen z Axis Communications. – *Przykładowo funkcje analityczne zaimplementowane w kamerze dozorowej mogą wyzwolić alert. W takiej sytuacji operator, uzyskując dostęp do transmisji na żywo za pośrednictwem aplikacji chmurowej, może to zdarzenie zweryfikować i odpowiednio na nie zareagować.*

Ale co najważniejsze, częstsze stosowanie funkcji analizujących coraz większe zbiory danych wizyjnych – nawet w celu zapobiegania rozszerzaniu się pandemii – doprowadziło do zwiększenia świadomości na temat konieczności ochrony prywatności i ochrony danych osobowych, która jest podstawą RODO. A zgodność z tymi przepisami staje się teraz ważniejsza niż kiedykolwiek.

– *Podczas pandemii przekonaliśmy się, że technologie wizyjne odgrywają coraz ważniejszą rolę w zapewnianiu ludziom bezpieczeństwa i ochrony zdrowia, m.in. dzięki takim zastosowaniom, jak liczenie przemieszczających się osób, monitorowanie przestrzegania dystansu społecznego czy bezdotykowy pomiar temperatury i rozpoznawanie twarzy w celu uprawnienia przez systemem kontroli dostępu do wejścia do pomieszczenia. Badania wskazują, że to właśnie ochrona prywatności jest najważniejszą kwestią dla inwestorów, którzy są zainteresowani wykorzystaniem tych nowych środków dozoru* – podsumowuje Malou Toft z Milestone.

To pokazuje, że budowanie zaufania zarówno klientów, jak i całej opinii publicznej musi być priorytetem, zwłaszcza w miarę dalszego upowszechniania technologii wizyjnych do śledzenia kontaktów międzyludzkich. Coraz częstsze wdrażanie takich rozwiązań nie daje firmom pozwolenia na żadne odstępstwa od poszanowania prywatności osób i przestrzegania przepisów RODO. Co więcej, wymaga ścisłej ochrony zgromadzonych danych przed ich utratą.

– *Przykładamy coraz większą wagę, aby zagwarantować cyberbezpieczeństwo naszych rozwiązań* – deklaruje Phillip Antoniou z MOBOTIX. – *Przez ostatnie dwa lata widzieliśmy wielokrotnie, jak wielkie międzynarodowe korporacje czy nawet mniejsze firmy lokalne ucierpiały z powodu wycieku danych. To ogromny problem, który wpływa negatywnie na zaufanie klientów. Staje się także coraz większym problemem ze względu na wysokie kary finansowe nakładane za łamanie przepisów RODO. Coraz więcej osób chce wiedzieć, jakie dane, w jaki sposób i przez kogo są przechowywane. Nakłada to na firmy odpowiedzialność za inwestowanie w rozwiązania zabezpieczające przed cyberatakami.*

Po katastrofalnym roku 2020 europejska branża security spodziewa się lepszych czasów. Dostawcy elektronicznych systemów zabezpieczeń zapowiadają nowe rozwiązania, które mają pomóc użytkownikom w przystosowaniu się do „nowej normalności" po pandemii. Muszą sobie jednak zdawać sprawę, że inwestorzy wymagają gwarancji cyberbezpieczeństwa gromadzonych danych osobowych i ochrony prywatności – szczególnie w rozwiązaniach security stosowanych do monitorowania kontaktów międzyludzkich i przestrzegania dystansu społecznego. Tylko wtedy dostawca ma szansę na europejskim rynku.

DOSTAWCY ELEKTRONICZNYCH SYSTEMÓW ZABEZPIECZEŃ ZAPOWIADAJĄ NOWE ROZWIĄZANIA, KTÓRE POMOGĄ PRZYSTOSOWAĆ SIĘ DO „NOWEJ NORMALNOŚCI" PO PANDEMII

W okowach COVID-19

Branża elektronicznych systemów zabezpieczeń w latach 2020–2025

Firma badawcza Memoori przedstawiła w grudniu 2020 r. raport dotyczący wpływu pandemii na rynki kontroli dostępu, dozoru wizyjnego oraz sygnalizacji włamania i ochrony obwodowej.

W marcu 2020 r. Światowa Organizacja Zdrowia (WHO) ogłosiła COVID-19 ogólnoświatową pandemią. W ciągu kilku tygodni stało się jasne, że z dużym prawdopodobieństwem spowoduje ona najgorszą w ostatnich 100 latach recesję na świecie. W czerwcu 2020 r. Bank Światowy opublikował bazową prognozę przewidującą 5,2-proc. spadek globalnego PKB w 2020 r.

W tym kontekście w raporcie oszacowano – na podstawie przyjętych dwóch scenariuszy – stan globalnego rynku elektronicznych systemów zabezpieczeń w perspektywie do roku 2025 *(rys. 1)*. W III i IV kw. 2020 r. cały świat doświadczył drugiej fali COVID-19, wiele krajów wprowadziło *lockdown*. Drugi scenariusz wydaje się bardziej prawdopodobny, ponieważ światowe rynki potrzebują około roku, aby powrócić do normalności, a masowe globalne szczepienia zajmą co najmniej 18 miesięcy. Prawdopodobieństwo, że się sprawdzi, jest szacowane na 65%.

Mimo takich przewidywań eksperci Memoori są nadal przekonani o stabilności branży i możliwościach wzrostu w perspektywie średnio- i długoterminowej. Jest mało prawdopodobne, aby czynniki napędzające rynek, takie jak zagrożenie terroryzmem i przestępczością, osłabły. Urbanizacja i inteligentna infrastruktura natomiast pobudzą popyt na większą liczbę coraz lepszych systemów zabezpieczeń.

Raport jest już 12. szczegółową analizą roczną, która obejmuje wszystkie czynniki wpływające na przyszłość branży security. W tym celu dokonano ogólnej oceny struktury i wielkości całej branży elektronicznych i mechanicznych systemów zabezpieczeń, a następnie z podziałem wg produktów i wielkości sprzedaży w odniesieniu do głównych sektorów i regionów geograficznych do 2025 r.

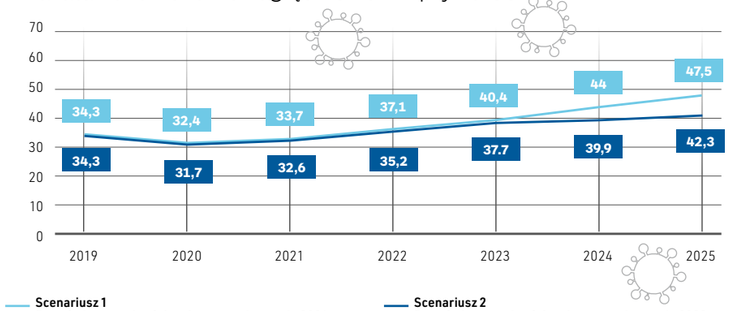
JAKI WPŁYW NA BRANŻĘ MIAŁA PANDEMIA COVID-19?

– Wybuch pandemii zmusił dostawców do radykalnego przemyślenia wielu aspektów prowadzonej działalności, zwłaszcza odporności na czynniki zewnętrzne. Jednocześnie zwrócił uwagę na kwestię lepszego skoordynowania i bardziej odpornego łańcucha dostaw. Działalność w sektorze dozoru wizyjnego jest zbyt uzależniona od chińskich producentów OEM-owych i komponentów. Zamknięcie wielu fabryk w Państwie Środka w pierwszych dwóch miesiącach 2020 r. spowodowało czasowe problemy w łańcuchu dostaw.

– Produkty z zakresu elektronicznych systemów zabezpieczeń sprostały wyzwaniom, pomagając we wdrażaniu protokołów zachowania dystansu społecznego. Wykorzystano istniejące systemy kontroli dostępu i dozoru wizyjnego z analityką wspieraną przez sztuczną inteligencję. Było również duże zapotrzebowanie na kamery termowizyjne do pomiaru temperatury ludzi. Ich przydatność została jednak zakwestionowana przez WHO, która stwierdziła, że sama kontrola temperatury może być niezbyt skuteczna.

– Szacuje się, że łączna wartość światowej produkcji urządzeń z zakresu technicznych systemów zabezpieczeń w 2020 r. wyniesie (w cenach fabrycznych) 31,7 mld USD, co oznacza spadek o ponad 7,5% w stosunku do 2019 r. Sprzedaż zmniejszyła się w pierwszych trzech kwartałach 2020 r. za sprawą COVID-19. Pandemia zatrzymała tendencję wzrostową, jaka miała miejsce przez ostatnich 11 lat.

Rys. 1. Prognozy dla branży elektronicznych systemów zabezpieczeń na lata 2020-2025 z uwzględnieniem wpływu COVID-19



Zakładając rozwój sytuacji wg drugiego scenariusza, produkcja powinna wrócić do normy w trzecim kwartale 2021 r. i do końca tego roku wzrosnąć o prawie 3%. W każdym z trzech sektorów (systemy KD, VSS, alarmowe) i w zależności od strefy geograficznej stopy wzrostu będą jednak się różniły. Do końca 2025 r. rynek może osiągnąć wartość ponad 42 mld USD, a CAGR w najbliższych 5 latach wynieść 6%.

Chiny nadal będą zwiększały swój udział w rynku zabezpieczeń technicznych. Tamtejszy rynek szybko się rozwija dzięki boomowi w nowym budownictwie oraz projektom dozoru wizyjnego, tzw. *Sharp Eyes*, napędzanym przez sektor publiczny. Dla producentów zagranicznych jednak niewiele z tego ogromnego rozwijającego się rynku jest dostępne i mało prawdopodobne, że takie się stanie się w najbliższej przyszłości ze względu na trwające napięcia polityczne i handlowe pomiędzy USA a Chinami.

Raport został opublikowany na **www.memoori.com**

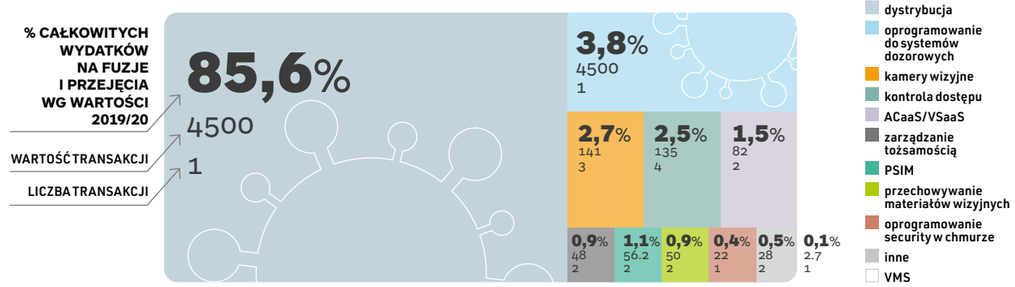
W RAPORCIE PRZEDSTAWIONO WSZYSTKIE KLUCZOWE FAKTY I WNIOSKI POZWALAJĄCE ZROZUMIEĆ, CO KSZTAŁTUJE PRZYSZŁOŚĆ BRANŻY ZABEZPIECZEŃ TECHNICZNYCH.

– W miarę upływu czasu po pandemii dostawcy będą musieli dokładnie badać potrzeby klientów, zwłaszcza tych, którzy poważnie ucierpieli. Tym firmom bowiem będzie trudniej znaleźć budżet na inwestycje i dlatego muszą być przekonane o zwrocie z inwestycji. Usługi ACaaS ***(Access Control as a Service)*** oraz VSaaS ***(Video Surveillance as a Service)*** mogą zapewnić rozwiązanie tego problemu – są dowody na znaczne przyspieszenie wzrostu usług w chmurze.

– Oprogramowanie zawsze było ważnym czynnikiem w rozwoju i wzroście branży zabezpieczeń technicznych. Wkraczamy teraz w nową epokę w sektorze dozoru wizyjnego, w którym ogromną rolę odgrywa sztuczna inteligencja (AI). Technologia AI może i będzie stanowić bezpośredni i ogromny wkład w zwiększenie wydajności i wartości rozwiązań w zakresie dozoru wizyjnego. Systemy zabezpieczeń jednak nie są wyspą i w wielu przypadkach będą musiały być połączone z szerszym IoT, ponieważ wszystkie informacje mają być przekształcone w dane możliwe do wykorzystania w praktyce.

– Średnia roczna wartość transakcji fuzji i przejęć w ostatnich 13 latach wynosi 6717 mln USD. W 2020 r. zidentyfikowano 20 takich transakcji, 26 – rok wcześniej. W 2020 r. wartość fuzji i przejęć wyniosła 5285 mln USD i była wyższa niż w 2019 r., ale nadal niższa niż średnia z 13 lat. Fuzje i przejęcia wyceniane wg wartości znajdują się obecnie w cyklu spadkowym ***(rys. 2)***.

Rys. 2. Fuzje i przejęcia według segmentów biznesowych



Przełomowe lata 20.

Rok 2020 oraz prognozy na 2021 r. wg OVHcloud

Miniony rok wywrócił wszystko do góry nogami. Obowiązek zachowania fizycznego dystansu przeniósł wiele osób do wirtualnego świata. W czasie gdy wiele branż, takich jak gastronomia czy hotelarstwo, musiało zawiesić swoją działalność, sektor IT rozwijał się w przyspieszonym tempie, a chmura obliczeniowa, usługi w chmurze i e-commerce stały się dla wielu normalnością. I chociaż rok 2020 zapamiętamy na długo, to z pewnością zaowocuje on wieloma ciekawymi trendami technologicznymi. Czy pozwolą one spojrzeć w nadchodzącą przyszłość z optymizmem?

PODSUMOWANIE 2020 ROKU W BRANŻY TECHNOLOGICZNEJ

Wielbiciele nowinek technologicznych i fani fantastyki naukowej od lat rozmyślali nad futurystycznie jeszcze kiedyś brzmiącym rokiem 2020. Oprócz zalet życia w świecie zaawansowanej technologii niektórzy zastanawiali się również nad jej negatywnymi konsekwencjami. Gdy jednak pełni nadziei wchodziliśmy w nowy rok, nikt nie przewidywał, jak wyczerpujący się okaże. Ostatnie 12 miesięcy upłynęło nam pod znakiem wielu istotnych wydarzeń.

1 ZWARCI I GOTOWI

Pandemia w 2020 r. to tragedie poszczególnych ludzi i narodów. To także seria wyzwań. Z jednej strony koncerny farmaceutyczne ruszyły do opracowania szczepionek w możliwie najkrótszym czasie, z drugiej – Polacy przenieśli do swoich mieszkań nie tylko biura, ale także szkoły, gabinety lekarskie, restauracje czy sale kinowe. Poziom edukacji, rzetelność telewizyt czy efektywność wykonywanej pracy pod dyktando e-testów czy zdalnych lekcji można różnie oceniać. Najważniejsze jednak, że konieczne rozwiązania były powszechnie dostępne, istniały narzędzia i niezbędna infrastruktura – aplikacje do prowadzenia spotkań i przesyłania filmów, Internet szerokopasmowy czy sprzęt komputerowy. Oczywiście, można było sprawniej i lepiej, ale wyobraźmy sobie *lockdown* choćby dekadę temu, przecież nasza codzienność wyglądałaby zupełnie inaczej. Mimo wszystko obecny wynik należy uznać za sukces, a z pewnością rok 2021 pozwoli udoskonalić wiele elementów.

2 SZYBSZA CYFRYZACJA

Jedną z trudności, jakie przyniósł mijający rok, był brak stabilności. Z dnia na dzień konieczne stało się dostosowanie planów, preferencji i przyzwyczajeń do nowych warunków. Okazało się, że niemal każda potrzeba: od kontaktu z drugim człowiekiem, przez zakupy, po realizację recepty łączy się ze zmianą. Konsumenci, usługodawcy i sprzedawcy zaczęli szukać nowych możliwości. Konieczność zapewnienia ciągłości biznesowej zmotywowała wiele firm do działania i zrealizowania odkładanej od lat transformacji cyfrowej, spełniając przy tym restrykcyjne wymagania dotyczące bezpieczeństwa danych i prywatności. Ponieważ świat zamknął się niemal z dnia na dzień, na co wiele sektorów nie było przygotowanych, innego wymiaru nabrały wzajemne wsparcie i współpraca. Przykładem są firmy IT, które już na początku pandemii powołały organizacje pomocowe, takie jak europejska inicjatywa „Open Solidarity" czy „Tech to the Rescue", dzięki którym potrzebujące firmy mogły skorzystać ze wsparcia narzędziowego i wiedzy eksperckiej w cyfryzacji.

3 CYBERSUWERENNOŚĆ EUROPY

Bez wątpienia donośniej wybrzmiewała w 2020 r. kwestia cyfrowej suwerenności danych. Koncepcja oddania krytycznej infrastruktury informacyjnej europejskich podmiotów w ręce prywatnych firm podlegających prawu znacznie odbiegającemu od kontynentalnych standardów prowokowała pytania i dyskusje. Rozdrobnienie mapy politycznej Europy utrudniało jednak opracowanie jednolitego planu. Aby znaleźć rozwiązanie i stworzyć zaufaną ofertę usług chmury publicznej na potrzeby rynków europejskich, dla których kluczowa jest suwerenność danych oraz zgodność z RODO, z inicjatywy francusko-niemieckiej powołano międzynarodowy projekt Gaia-X, którego OVHcloud było jednym z założycieli. Obecnie opracowywane są kolejne narzędzia, które mogą służyć europejskim firmom, a jednocześnie zapewniać standardy ochrony danych kluczowe dla Europy.

4 BLOCKCHAIN

Rewolucja *blockchain* wydaje się wciąż przed nami. Technologia *blockchain*, która wymusiła współpracę pomiędzy konkurującymi ze sobą instytucjami finansowymi, będąc hitem roku 2019, nie zmieniła świata. Niewykluczone jednak, że wkrótce znów usłyszymy o *blockchainie*, który wciąż może zrewolucjonizować ekonomię i przyczynić się do gospodarczego boomu, zwłaszcza że jako pierwsza potencjał w tym zakresie doceniła branża finansowa.

5 WIRTUALNIE BLISKO

Przymus fizycznego dystansu obrócił o 180 stopni formę świadczenia pracy i od miesięcy otwarte pozostaje pytanie, czy wrócimy na pełny etat do biur. Obostrzenia przyspieszyły otwieranie się biznesu na szerokie zastosowanie Rzeczywistości Wirtualnej (VR). Wyszkolenie pracownika w bezpiecznym wirtualnym środowisku pozwala mu nie tylko przećwiczyć mniej i bardziej typowe scenariusze wydarzeń, ale także zyskać niezbędną pamięć sytuacyjną. A wszystko to bez konieczności zatrzymywania działania zakładu i ryzyka wypadków. Co ciekawe, w 2020 r. VR współpracująca z komputerami PC wreszcie doczekała się gier AAA, ale to też rok, w którym cała Polska zobaczyła zdalne lekcje prowadzone w poznańskiej szkole z wykorzystaniem rzeczywistości wirtualnej. To też rok pierwszych konferencji i spotkań biznesowych prowadzoneych w wirtualnej przestrzeni.

TRENDY TECHNOLOGICZNE, NA KTÓRE CZEKAMY W 2021

Oprócz symbolicznego znaczenia nowy rok nie należy do przełomowych momentów. Gdy zegary wybijają północ, a my sięgamy po okazjonalną lampkę szampana, w naszym życiu przeważnie nie zmienia się nic oprócz daty w kalendarzu. Mimo to nowy rok zawsze wywołuje dreszcz ekscytacji, choć branża IT nie zmienia się z dnia na dzień. Nowe przełomowe rozwiązania są w rzeczywistości rozwijane latami, zanim przyjdzie ich czas. Jakie trendy wypłyną lub umocnią się w 2021 r.?

1 BLIŻEJ KLIENTA

Wczoraj offline, dziś online. Boom przenoszenia biznesów do sieci i skokowy wręcz rozwój e-commerce skłoniły nowe grupy konsumentów do zmiany swoich nawyków. Dotąd nieufni i niechętni, zmuszeni sytuacją zaczęli szukać w sieci potrzebnych produktów i usług. Jedna trzecia, wg badań, deklaruje, że nadal będzie robić zakupy w e-sklepach, ale co postanowi reszta? Aby pozostać w grze, nie wystarczy już tylko uruchomić e-biznes. W 2021 r. konieczne będzie umiejętne zagospodarowanie klientów, którzy zaufali wirtualnej rzeczywistości, a zarazem dbanie o jakość usług – a więc w cenie będzie UX, zbieranie danych i ich analityka. Na pewno zrobi to konkurencja.

2 WDROŻENIE TECHNOLOGII 5G

Rośnie pula urządzeń mobilnych mogących korzystać z nowoczesnych sieci piątej generacji. Od roku na rynku dostępne są rozwiązania umożliwiające działanie w sieci 5G. Okraszone kontrowersjami, przedłużające się oczekiwanie na aukcję operatorskich częstotliwości 5G już w 2020 r. sprawiło, że głodne nowości firmy odważyły się podejmować ograniczone przestrzennie eksperymenty z nową siecią. W roku 2021 nie uda się już utrzymać 5G na smyczy, tym bardziej że media naukowe donoszą o koncepcjach sieci szóstej oraz siódmej generacji.

3 SZTUCZNA INTELIGENCJA (AI)

Niezależnie od tego, czy jesteśmy zwolennikami sztucznej inteligencji, czy jej przeciwnikami, AI już teraz towarzyszy nam w życiu codziennym i nic nie wskazuje na to, aby miało się to zmienić. Wystarczy spojrzeć na inteligentne chatboty wykorzystywane w sektorze usługowym. Wdrożenie tego rozwiązania odciążyło pracowników od mechanicznych czynności i podniosło satysfakcję klientów, którzy nie muszą już czekać na odpowiedź konsultantów. Pojawiły się też inne schematy wykorzystania algorytmów SI, takie jak zbieranie informacji na temat opieki zdrowotnej czy wskaźników dotyczących infekcji. Analizując zebrane dane i śledząc trendy, AI może przyczynić się do odkrywania niezauważalnych ludzkim okiem powiązań, które mogą pomóc w walce z pandemią... tą i następnymi.

4 KWANTOWI SIŁACZE

Coś, co jeszcze niedawno stawiano na jednej półce z teleporterem i podbojem kosmosu, wkrada się do powszechnej świadomości jako rzecz nie tyle „wykonalna", ile „oczywista". Po takich gigantach, jak IBM, Google czy Honeywell, w końcu 2020 r. do gry weszli Chińczycy. Ich specjalnie w tym celu zaprojektowany komputer kwantowy w ciągu kilku minut rozwiązał problem, który komputerom opartym na mechanice kwantowej zajęłby kilka miliardów lat. Imponujące. I choć wciąż więcej w tym prężenia muskułów i marketingu niż scenariuszy praktycznego zastosowania, rok 2021 może obfitować w pokazy siły kwantowych osiłków.

5 JESZCZE WIĘKSZA SUWERENNOŚĆ DANYCH?

Eksperci nie są pewni, jak zmiany w administracji amerykańskiej wpłyną na wojnę handlowo-technologiczną między Stanami Zjednoczynymi a Chinami. Szala może się przechylić w obie strony. Mimo że Europa znajduje się z boku tego konfliktu, ona także odczuwa jego skutki. Fragmentacja Starego Kontynentu, wielość języków, kultur, stopnia rozwoju i różnorodne prawodawstwo sprawiają, że Europa nie jest łatwym rynkiem. To także powód braku zdolności porozumienia się nawet w tych kluczowych sprawach. Zdaje się jednak, że w 2021 r. nastąpi przełom. Coraz głośniej słychać bowiem głosy promujące zajęcie wspólnego europejskiego stanowiska. Na sile przybierają takie inicjatywy, jak Gaia-X czy Open Trusted Cloud. Istotne jest także ogłoszenie przez Komisję Europejską gotowej (po 7 latach negocjacji) umowy ekonomicznej UE–Chiny.

Mówi się, że COVID-19 zrobił dla cyfryzacji nad Wisłą więcej niż wszystkie rekomendacje Komisji Europejskiej w tym temacie do tej pory. *W prognozach na rok 2020 Gartner przewidywał, że do 2021 r. inicjatywy dotyczące transformacji cyfrowej obejmą duże tradycyjne przedsiębiorstwa, ale będą trwały średnio dwa razy dłużej i będą kosztować dwa razy więcej, niż zakładano* – zauważył Robert Paszkiewicz, odpowiedzialny w OVHcloud za region Europy Środkowo-Wschodniej. – *Nikt jednak nie przewidział globalnej pandemii. A gdy wybuchła, w obliczu realnych i palących potrzeb wiele decyzji latami odkładanych i ciągnących się procesów zostało natychmiast wdrożonych. Potrzeba wymusiła działanie. Zostaliśmy wyrwani ze strefy komfortu i weszliśmy do strefy wpływów technologii.*

O ile przed *lockdownem* aż 73% firm nie inwestowało w nowe technologie, o tyle podczas pandemii wykorzystywało je już 91%, ponieważ pojawiły się wymierne, policzalne oczekiwania, a istniejąca technologia potrafiła je zaadresować. W 2021 roku te rozwiązania będą zapewne doskonalone i upowszechniane. Dzięki wirusowi zrobimy spory digitalowy krok naprzód.

Trendy technologiczne

na rok 2021 i kolejne lata

Trendy technologiczne prognozowane na bardziej odległą przyszłość mogą się ziścić szybciej, niż się nam wydaje. Innowacje technologiczne zapowiadają duże zmiany w nowym roku. Pandemia COVID-19 uświadomiła, jak kluczowa jest gotowość na nieoczekiwane. W biznesie wymaga odpornej skalowalnej infrastruktury IT, zapewniającej bezpieczeństwo i elastyczność.

TREND 1 – **5G I WI-FI 6 ZASYPUJĄ CYFROWĄ PRZEPAŚĆ**

W roku 2020 sieć była podstawą kontaktów społecznych, aktywności zawodowej i ekonomicznej codzienności – zakupów, organizacji spraw administracyjnych itp. Niestety dostęp do sieci ma zaledwie połowa światowej populacji (35% w krajach rozwijających się, 80% w rozwiniętych ekonomicznie). Różnice w dostępie do technologii miały szczególnie negatywny wpływ na mieszkańców obszarów wiejskich i osoby niezamożne.
Dziś dostęp do sieci stanowi jeden z fundamentów funkcjonowania społeczeństwa i ekonomii, w której powinni móc uczestniczyć, uczyć się i rozwijać wszyscy obywatele. Duże nadzieje pokłada się w nowych generacjach bezprzewodowych technologii komunikacyjnych, w tym 5G i Wi-Fi 6. Poprawią one przepustowość i szybkość, przyczynią się do zmniejszenia przestojów sieci, zwiększą też dostęp do niej wszędzie tam, gdzie zbudowanie infrastruktury przewodowej jest zbyt kosztowne. Eksperci Cisco postrzegają postęp w bezprzewodowym dostępie do sieci jako sposób na zniwelowanie cyfrowej przepaści, ponieważ technologie te napędzają rozwój i innowacje, z których skorzystają miliony ludzi.
Według badań PwC uzyskanie dostępu do sieci przez tych, którzy go obecnie nie mają, sprawiłoby, że do gospodarki światowej trafiłoby dodatkowe 6,7 bilionów USD, a kolejne 500 mln ludzi wyszłoby z ubóstwa.

TREND 2 – **HYBRYDOWA PRZYSZŁOŚĆ PRACY**

Na początku pandemii, kiedy zaczęły obowiązywać ograniczenia dotyczące kontaktów społecznych, biznes musiał dostosować się do wymogów pracy zdalnej. Jak wynika z raportu Cisco: *Workforce of the Future*, pracownicy chcą utrzymania wielu pozytywnych zmian, jakie niesie nowy sposób wykonywania obowiązków. Przed *lockdownem* tylko 5% uczestników badania przez większość czasu pracowało zdalnie. Obecnie aż 83% respondentów z Polski chce decydować o miejscu wykonywania obowiązków i samodzielnie zarządzać czasem pracy, nawet gdy biura zostaną otwarte.

A co z osobami, które nie pracują w środowisku biurowym, czyli z ponad 60% populacji zatrudnionych? W handlu detalicznym trend przeniesienia działalności z przestrzeni offline do online utrzymuje się już od pewnego czasu, COVID-19 jedynie te zmiany przyspieszył. Dla zatrudnionych w tym sektorze może to oznaczać zmianę profilu pracy. Praca online wymaga kompetencji administracyjnych potrzebnych do obsługi zamówień i klientów oraz zarządzania stanami magazynowymi i dostawami. Poza zdalne konsultacje może też wykroczyć służba zdrowia. Takie technologie, jak 5G, AI czy wirtualna, rozszerzona rzeczywistość ciągle się rozwijają, wizja operacji wykonywanych zdalnie może stać się realna. W zakładach produkcyjnych, w przemyśle paliwowym, gdzie konserwacje zapobiegawcze i predykcyjna stają się powszechnie stosowaną praktyką, część zadań może być wykonywana zdalnie.
Choć tempo zmian w takich sektorach, jak transport, przemysł czy rolnictwo nie będzie tak duże jak przy przejściu z pracy w biurze do pracy zdalnej, to długofalowy wpływ tych zmian na ekonomię może być znaczący.

TREND 3 – **APLIKACJE ZWIĘKSZAJĄCE ELASTYCZNOŚĆ I ODPORNOŚĆ BIZNESU**

Nieprzewidywalne zmiany w początkach pandemii wymusiły zdolność do szybkiego przystosowywania się firm. Chmura była kluczowym narzędziem, które to umożliwiło. Często była to jedyna droga do nabycia nowych zdolności. Dziesięć miesięcy po wybuchu pandemii aplikacje stanowiące rdzeń biznesu były już w powszechnym użyciu. Pracownicy stali się mobilni bardziej niż kiedykolwiek wcześniej, a obciążenia, jakim poddawane są systemy IT, nie mają precedensu.
Przyszłość, i to niedaleka, wymusi na zespołach IT jeszcze większą elastyczność. Korzystając z rozwiązań zapewniających wgląd w infrastrukturę IT, przejdą od monitorowania wszystkiego do monitorowania jedynie danych kluczowych. W miarę postępujących przemian dostęp do wrażliwych danych i automatyzacja staną się podstawą przyszłego wzrostu, możliwości konkurowania i odporności na wyzwania.

Według badania Cisco *2021 CIO and IT Decision Makers Trends Pulse* 68%% prezesów firm i decydentów IT w Polsce chciałoby lepiej niż dotychczas wykorzystywać w biznesie informacje pochodzące z analizy działania aplikacji.

TREND 4 – **SATYSFAKCJA KLIENTA TO ZA MAŁO**

Popularność inteligentnych i mobilnych urządzeń zmieniła model naszego życia. Dziś za pomocą aplikacji mobilnych można zrobić zakupy, wysłać przelew, uczyć się, zadbać o zdrowie. Aplikacje mobilne stały się kluczowym narzędziem do monitorowania kontaktów międzyludzkich i skutecznej analizy rozprzestrzeniania się koronawirusa. Umożliwiły organizacjom z sektorów prywatnego i publicznego nawiązywanie kontaktu z użytkownikami w sposób, jaki był nie do pomyślenia jeszcze kilka lat temu.
Na aplikacjach opiera się również większość procesów biznesowych. Najbardziej zaawansowane pozwalają nawiązać spersonalizowane relacje z klientem czy udzielać natychmiast odpowiedzi. Biznes musi nabyć zdolność szybkiego przekuwania ogromnej ilości informacji pochodzących z sieci w wiedzę stanowiącą podstawę dalszych skutecznych działań. Dobry kontakt przełoży się na pozytywne wrażenia i z czasem klient stanie się lojalny wobec marki.

56%
PREZESÓW Z POLSKI BIORĄCYCH UDZIAŁ W BADANIU CISCO *2021 CIO and IT Decision Makers Trends Pulse* potwierdziło, że dobre doświadczenia klienta to więcej niż tylko jego satysfakcja, to także przyjemność wynikająca z kontaktu z marką.

TREND 5 – **CYBERBEZPIECZEŃSTWO BEZ HASEŁ**

Mobilność, praca w rozproszonym środowisku i szersze korzystanie z usług w chmurze umożliwiły firmom zarówno skalowalność, jak i ograniczenie kosztów. Konieczność zapewnienia odpowiedniego poziomu bezpieczeństwa w nowej rzeczywistości postawiła przed biznesem nowe wyzwania. Ukradzione lub utracone dane logowania to potężne narzędzie w rękach cyberprzestępców, którzy wykorzystują masowe przejście na model pracy zdalnej. Bezpieczną techniką uwierzytelniania jest biometryczna weryfikacja tożsamości. Użytkownik uzyskuje dostęp do urządzenia lub aplikacji na podstawie wizerunku twarzy, zapisu linii papilarnych czy obrazu tęczówki – lub drogą uwierzytelnienia dwuelementowego.
Dostawcy usług z zakresu bezpieczeństwa pracują nad rozwojem identyfikacji biometrycznej. Organizacje muszą być na te zmiany przygotowane, niezbędne jest dostosowanie rozwiązań do wymogów nowych sposobów uwierzytelniania, które nie opierają się na haśle.

Jak wynika z raportu 2020 *Cisco Duo Trusted Access*, 80% służbowych urządzeń umożliwia logowanie za pomocą cech biometrycznych, odsetek ten w ciągu 5 lat wzrósł o 12%.

TREND 6 – **NOWE MODELE KONSUMPCJI TECHNOLOGII**

Organizacje przez długi czas inwestowały w uniwersalne rozwiązania technologiczne. W praktyce wiązało się to z koniecznością opłat za funkcje, z których nigdy zapewne nie skorzystają. Model *software as a service* umożliwia zakup tylko niezbędnych elementów usługi i rozbudowę zakresu świadczeń wraz z rozwojem firmy. Coraz więcej usług IT jest dostępnych za pośrednictwem aplikacji korzystających z infrastruktury firmowej lub chmury. Elastyczność i możliwość redukcji kosztów dzięki opłatom tylko za wykorzystane usługi sprawiają, że powrót do starych modeli rozliczeń jest już raczej niemożliwy.

Ponad 81% polskich CIO uczestniczących w badaniu Cisco potwierdziło, że możliwość przewidzenia skali wydatków na usługi IT i zarządzenie nimi, dzięki chmurze i elastycznym modelom konsumpcyjnym, jest ważna dla ich biznesu (dla 40% bardzo ważna).

CISCO SYSTEMS POLAND
ul. Domaniewska 39B
02-672 Warszawa
www.cisco.com

Raport

Cyberbezpieczeństwo: Trendy 2021

Przed jakimi wyzwaniami stanie biznes?

Rosnąca skala cyberzagrożeń, upowszechnienie się pracy zdalnej, sieć 5G i coraz częstsze wykorzystanie urządzeń IoT, a także przyspieszająca transformacja rozwiązań w chmurze zmuszają firmy do zwrócenia większej uwagi na bezpieczeństwo IT i adaptację nowych technologii.

Firma Xopero Software przedstawia raport **Cyberbezpieczeństwo: Trendy 2021** opracowany we współpracy z 21 ekspertami z 13 firm (m.in. Netia, Orange Polska, Oracle, Asseco Data Systems, NASK SA, QNAP, Sophos, TestArmy, Axence). To kolejna edycja jedynego w Polsce dokumentu poświęconego nowym kierunkom w branży bezpieczeństwa IT, tworzonego przez specjalistów z różnych firm.

RANSOMWARE ATAKUJE CO 11 SEKUND

W ostatnich miesiącach pojawił się nowy arsenał zagrożeń. Obawa przed nieznanym, masowe przechodzenie na tryb pracy zdalnej i rekordowo wysoki poziom dezinformacji po wybuchu pandemii pobudziły kreatywność przestępców. Skala zagrożeń znacznie wzrosła. Najgroźniejszy wciąż pozostaje ransomware, którego wg badań Xopero obawia się blisko 80% ankietowanych przedsiębiorców. Szacuje się, że w tym roku będzie uderzać co 11 sekund, a globalne straty mogą wynieść 20 mld dolarów. Dla porównania w 2015 r. było to zaledwie 325 mln.

Cyberprzestępcy wykorzystujący ransomware automatyzują ataki. Coraz częściej dzielą się też między sobą narzędziami. Ich łatwa dostępność na czarnym rynku sprawia, że także w tym roku będzie rosła aktywność początkujących hakerów, którzy wykorzystują głównie oprogramowanie umożliwiające atakowanie dużej liczby mniejszych celów – twierdzi Łukasz Formas, kierownik zespołu inżynierów w Sophos. – *Stale udoskonalane będą techniki i narzędzia, a gdy jedno zagrożenie zniknie, w jego miejsce szybko pojawią się kolejne.*

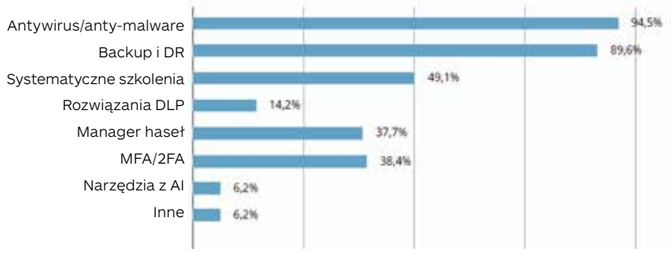
CLOUD COMPUTING: OD CHMURY NIE MA ODWROTU

Migracja do chmury wydaje się niezmiennie jednym z priorytetów firm – ponad 50% z nich uważa, że w najbliższym czasie wykorzystanie chmury będzie wyższe, niż planowano. Przyczyną są doświadczenia związane z pracą zdalną i koniecznością zapewnienia dostępności zasobów firmowych. Już dziś firmy przeznaczają na chmurę jedną trzecią swoich inwestycji w IT.

Ten rok ma szansę poważnie pobudzić korzystanie z chmury w Polsce. Zapowiedzi Microsoftu i Google'a już się materializują, a w 2021 r. doczekamy się w Polsce pierwszego regionu globalnej chmury publicznej – mówi Adam Kowalczyk, kierownik produktu w Netia SA. – *Tak duże inwestycje branżowych potentatów przyczyniają się do wzmożonego zainteresowania, a w konsekwencji bliższego poznania cloud computingu. Brak wiedzy jest największym wrogiem migracji do chmury.*

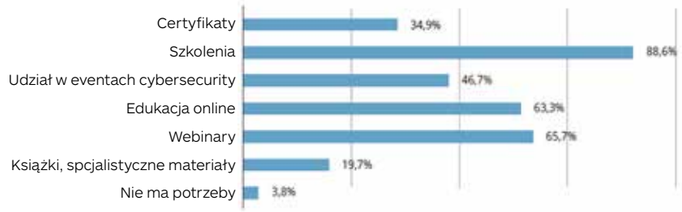
Niezaprzeczalnym trendem w 2021 r. będzie rozwój praktyki *multicloud*, czyli wykorzystania wielu heterogenicznych dostawców usług w chmurze. To z kolei pociągnie wzrost zapotrzebowania na rozwiązania zabezpieczające dane w chmurze i gwarantujące ciągłość działania. – *Jeśli miałbym wymienić tylko jedną usługę, która w 2021 r. ma szansę stać się wspólnym trendem dla chmury i cyberbezpieczeństwa, wskazałbym DRaaS. Nie jest to nowy pomysł, ale jego koszty są już na tyle niskie, a świadomość w firmach na tyle wysoka, że prognozuję znaczny wzrost popytu na te usługi w Polsce* – dodaje A. Kowalczyk.

Rys 1. W jaki sposób zapezpieczasz swoją infastrukturę IT?



Źródło: Raport Cyberbezpieczeństwo: Trendy 2021

Rys 2. Jakie działania powinna podjąć Twoja organizacja, aby podnieść kompetencje i umiejętności działu/zespołu IT?



Źródło: Raport Cyberbezpieczeństwo: Trendy 2021

UCZENIE MASZYNOWE – GDZIE KOŃCZY SIĘ PRAWDA, A ZACZYNA SZUM MEDIALNY?

Uczenie maszynowe niewątpliwie odegra istotną rolę w stworzeniu nowej klasy rozwiązań cyberbezpieczeństwa. 96% respondentów już korzysta z produktów security, które mają moduły sztucznej inteligencji. To blisko dwa razy więcej niż jeszcze trzy lata temu. Należy jednak odróżnić prawdę od marketingowej mrzonki. Z badań Xopero wynika, że nowa technologia znajduje zastosowanie m.in. w wykrywaniu zagrożeń (66,8%), skanowaniu skrzynek mailowych (42,9%), zautomatyzowanej analizie sieci (17%), wyszukiwaniu wzorców czy jako wsparcie w *threat hunting*. Uczenie maszynowe to jednak broń obosieczna – jeżeli może wspomóc zespół bezpieczeństwa, należy przyjąć, że może wesprzeć również przestępców.

BACKUP I DISASTER RECOVERY – NOWY STANDARD BEZPIECZEŃSTWA

Gdy sukces biznesu opiera się przede wszystkim na danych, konsekwencje ich utraty nigdy nie były poważniejsze. Szacuje się, że w ujęciu globalnym średni jednostkowy koszt związany z przestojem działalności firmy wynosi 1,52 mln dolarów! To wartość aż 40% łącznych kosztów incydentu bezpieczeństwa i obejmuje skutki utraty klientów, przestojów systemów i rosnące – z powodu strat wizerunkowych – koszty pozyskania nowych źródeł przychodów. Nic dziwnego, że statystycznie 93% firm bez rozwiązań do *backupu* i *disaster recovery* (DR) upada w rok po utracie danych.

Według badań Xopero Software backup jest drugim najchętniej wykorzystywanym rozwiązaniem z obszaru IT security, stając się standardem, z którego korzysta 89,6% ankietowanych. Plasuje się tuż za oprogramowaniem antywirusowym i antymalware (94,5%), które stało się właściwie fundamentem dzisiejszego podejścia do zabezpieczania danych i urządzeń firmowych.

Znajduje to odzwierciedlenie w globalnych statystykach. Rynek *backupu* i *disaster recovery* jest jednym ze stabilniej rozwijających się w branży cybersecurity. Prognozuje się, że jego wartość do 2022 r. wyniesie 11,59 mld dolarów. Ogromne znaczenie będzie miał też rozwój rynku przetwarzania w chmurze. Wartość rynku *backupu* w chmurze wzrośnie do 10,25 mld dolarów w 2025 r., przy założeniu średniej rocznej stopy wzrostu na poziomie aż 25,90% (!).

Zmiany, jakie zaszły na całym świecie w 2020 r., znalazły odzwierciedlenie w wyzwaniach stawianych producentom systemów do backupu i odtwarzania awaryjnego, którym muszą sprostać. Niektóre z rozwiązań są stosowane na rynku od wielu lat w formie, która niewiele się zmieniła, a ich architektura jest już przestarzała. Producenci tych rozwiązań mają za sobą „dług technologiczny", dodawanie nowych funkcjonalności trwa miesiącami, a czasem jest nieopłacalne lub nawet niemożliwe ze względu na wykorzystywaną technologię bądź architekturę samego systemu – twierdzi Grzegorz Bąk, Product Development Manager w Xopero Software. – *Świat IT zmienia się bardzo dynamicznie, gdyż w ułamkach sekund wykonywana jest niewyobrażalna liczba operacj. Dlatego warto obserwować nowości.*

SECURITY GAPS – CZŁOWIEK W EPICENTRUM ZAGROŻEŃ

Organizacje na całym świecie borykają się z problemem braku wykwalifikowanych pracowników IT. Z badań Xopero wynika, że ponad 55% ankietowanych zetknęło się z tym problemem, a dla części z nich (20%) jest on na tyle poważny, że braki w umiejętnościach mają negatywny wpływ na skuteczność zespołu.

Uważa się, że to człowiek – jego niewiedza, niekompetencje i nierozważne działania – są odpowiedzialne za większość incydentów bezpieczeństwa. Nieprzeszkoleni pracownicy zdalni mogą tylko utwierdzić specjalistów w tym przekonaniu.

W jaki sposób firmy mogą podnieść umiejętności zespołu? Ankietowani wskazali, że najistotniejsze z ich punktu widzenia są szkolenia, webinaria i edukacja w modelu online. Powinny on mieć charakter stały i konsekwentny, dopiero wówczas można mówić o cyberedukacji.

IOT WYMUSI ZMIANĘ PODEJŚCIA DO CYBERBEZPIECZEŃSTWA

Wyzwaniem na 2021 r. jest również stworzenie bezpiecznego Internetu Rzeczy (IoT) składający się już z 80 mld połączonych ze sobą urządzeń, których szybko przybywa. Niezapewnienie odpowiedniego bezpieczeństwa procesu ich wdrażania i brak stosownych aktualizacji czyni IoT szczególnie podatnym na ataki. Uwzględniając, że do 2024 r. 35% całkowitego mobilnego ruchu danych będzie przenoszonych za pośrednictwem sieci 5G, musimy już dziś nauczyć się zabezpieczać urządzenia inteligentne.

REKOMENDACJE SPECJALISTÓW

Oprócz branżowych prognoz i analiz cytowany raport zawiera komentarze i rady wielu specjalistów znanych firm IT. Ich analiza i wdrożenie pozwolą firmom efektywnie funkcjonować w cyberprzestrzeni, może wręcz zdecydować o ich dalszym istnieniu.

Software Maintenance Agreement

Korzyść czy zbędny wydatek?

Dla większości firm zakup oprogramowania istotnego z perspektywy utrzymania bezpieczeństwa jest często dużym wydatkiem. Nie chcąc ponosić dodatkowych cyklicznych kosztów utrzymania rozwiązania w jego najnowszej wersji w ramach tzw. *Software Maintenance Agreement* (SMA) – umowy wsparcia technicznego oprogramowania, zwanej również umową serwisową oprogramowania – firmy często z tego wsparcia rezygnują lub odkładają na bliżej nieokreśloną przyszłość. Prawda jest taka, że branża elektronicznych systemów zabezpieczeń nie jest przekonana do SMA. Zupełnie odwrotnie niż branża IT, która ogromną część rocznych budżetów przeznacza na opłacenie istniejących umów dotyczących wsparcia i utrzymania oprogramowania.

Porównanie branż security i IT pojawiło się nie bez powodu. Ciągła ewolucja systemów i aplikacji w naszej branży powoduje, że coraz częściej i głębiej integrujemy elektroniczne systemy zabezpieczeń z tymi zarządzanymi przez działy IT. Cyklicznie wykonywane testy penetracyjne wymuszają na dostarczanych rozwiązaniach, aby wszystkie urządzenia i programy pracujące we współdzielonej sieci były odpowiednio zabezpieczone i zgodne z bieżącą polityką bezpieczeństwa przedsiębiorstwa. W efekcie okazuje się, że od instalowanych przez nas urządzeń oraz aplikacji serwerowych i klienckich wymaga się spełnienia tych samych rygorystycznych kryteriów co od pozostałych elementów systemów wdrażanych pod egidą IT. To z kolei przekłada się na konieczność cyklicznej aktualizacji oprogramowania.

CZYM JEST SMA?

Konserwacja oprogramowania to szerokie działania obejmujące korektę błędów, rozszerzanie możliwości, usuwanie przestarzałych funkcji i optymalizację. Przyjmuje się, że każda praca w celu dokonania zmiany oprogramowania po jego uruchomieniu jest uważana za pracę konserwacyjną, której celem jest zachowanie wartości oprogramowania w czasie. Wartość tę można zwiększyć poprzez spełnienie dodatkowych wymagań funkcjonalnych, łatwiejszą obsługę, poprawę wydajności i wykorzystanie nowszych technologii. Umowa określa warunki wsparcia oraz deklaracje producenta oprogramowania w zakresie częstości ukazywania się nowych wersji i poprawek. Niekiedy zawiera też wysokość kosztów za aktualizacje. Dla większości wdrożeń moment obowiązywania SMA zaczyna się z chwilą podpisania umowy lub rozpoczęcia wdrożenia.

Dostawcy rozwiązań w chmurze (np. firma DMSI) pobierają opłaty miesięczne lub roczne, wtedy konserwacja jest częścią świadczonej przez nich usługi. Przychody z usług konserwacji zapewniają firmom tworzącym oprogramowanie środki na udoskonalanie ich produktów i nadążanie za zmianami technologicznymi, które poprawiają ergonomię pracy i zwiększają produktywność.

SMA W ELEKTRONICZNYCH SYSTEMACH ZABEZPIECZEŃ

W naszej branży dostępne są trzy rodzaje umów serwisowych, zależnie od producenta lub nawet produktu: bezpłatna SMA (błędnie uznawana za brak umowy, gdyż na ogół nie istnieje sformalizowany jej zapis), w formie cyklicznej opłaty (roczna, dwu-, trzy- lub pięcioletnia) za dostęp do aktualizacji i poprawek oraz jednorazowej opłaty migracyjnej (np. podniesienie wersji oprogramowania).

Bezpłatne umowy konserwacji są dość często spotykane w naszej branży. Przyzwyczaili nas do tego tacy producenci, jak Alnet, AxxonSoft, Dahua i Hikvision. Zakupione licencje są bezterminowe, a wsparcie i aktualizacje oprogramowania zgodnie z deklaracjami producentów zawsze bezpłatne. Informacje na ten temat są zawarte często jako wzmianki w kartach katalogowych oprogramowania lub instrukcjach konfiguracji czy obsługi. Niestety bywa i tak, że o SMA brak jakichkolwiek informacji w dostępnej dokumentacji. W takim wypadku warto poprosić przedstawiciela producenta o przedstawienie warunków.

Jakiś czas temu do oferentów bezpłatnych umów dołączył też Axis (jeszcze kilka lat temu w ofercie tego producenta znajdowała się opłata jednorazowa za podniesienie wersji oprogramowania, tzw. *upgrade license fee).* Nie jest to ruch nietypowy. W wielu branżach producenci oferują darmowy dostęp do poprawek i nowszych wersji swojego oprogramowania, jeśli jest ono dopełnieniem dla dostarczanego hardware'u stanowiącego ich główny przychód. Typowy natomiast jest brak jakiejkolwiek dokumentacji dotyczącej wsparcia i konserwacji dla takiego oprogramowania, a w konsekwencji brak wiedzy, czego można się spodziewać od producenta.

Axis, decydując się na bezpłatną opcję SMA, postanowił opisać zobowiązania, jakie ma producent wobec posiadacza licencji z tytułu jej zakupu. A zatem umowa nie uprawnia automatycznie użytkownika do aktualizacji i ulepszeń oprogramowania. Producent może jednak, okresowo i wg własnego uznania, dostarczać łatki, poprawki, uaktualnienia, wersje pomocy technicznej i konserwacji lub inne modyfikacje oprogramowania[1]. Axis postawił więc sprawę jasno: będziemy wydawać nowe wersje, ale w tempie, jakie nam odpowiada, wsparcie realizujemy na naszych zasadach. Bynajmniej nie jest to z mo-

1) https://www.axis.com/files/sales/acs_end_user_license_agreement.pdf

Jan T. Grusznic

Anna Twardowska, Nedap Security Management

W systemach bezpieczeństwa fizycznego standardem jest protokół IP. Korzystają one ze standardowego osprzętu z dedykowanym oprogramowaniem i przetwarzają duże ilości danych. W dużych przedsiębiorstwach systemy zabezpieczeń technicznych należą obecnie do systemów infrastruktury IT. W branży informatycznej aktualizuje się systemy, kiedy pojawia się nowa wersja przeglądarki internetowej lub oprogramowania. Jest to wręcz konieczne, by zagwarantować prawidłowy przebieg procesów w przedsiębiorstwie. System zarządzania bezpieczeństwem AEOS bazuje na standardowym osprzęcie, a o funkcjonalności decyduje oprogramowanie. Z tego względu istotne jest, aby było ono aktualne. Dysponując najnowszą wersją, można mieć pewność, że przedsiębiorstwu nic nie zagraża.

Krzysztof Ciesielski, DMSI

Obecnie coraz większą popularnością cieszy się technologia chmurowa i „sprzedaż" oprogramowania w modelu usługi, tj. SaaS – Software as a Service. W takim modelu biznesowo-technologicznym klienta nie dotyczy problem zachowania wartości oprogramowania, gdyż w każdym momencie trwania usługi otrzymuje pożądane i aktualne funkcjonalności. Nie musi też martwić się utratą licencji, wydajnością sprzętu i innymi kwestiami. Tego typu platformą chmurową jest Safestar i zapewniamy dla niej SMA, gdyż jest integralnym elementem tego modelu.

jej strony napiętnowanie, ale pochwała postawy. Ten szwedzki producent bowiem jako jedyny znany mi zdecydował się określić na co właściciel licencji może rzeczywiście liczyć, gdy wybiera darmową opcję SMA.

Po przeciwnej stronie darmowych SMA są umowy odnawiane odpłatnie i cyklicznie. Na takie podejście zdecydowały się firmy, których aplikacje można uznać za zaawansowane technicznie i technologicznie. Bosch, Genetec, Geutebrück, Nedap i Milestone pobierają opłatę roczną z tytułu konserwacji i pomocy technicznej kupionego oprogramowania. W ramach SMA producent deklaruje dostarczenie konkretnej liczby nowych wersji w czasie trwania umowy oraz warunki i czas wsparcia. W umowach często określa się też czas podjęcia zgłoszenia w zależności od jego priorytetu, jak również typ wsparcia (np. zdalne lub w miejscu wdrożenia).

Zakup SMA nie jest obowiązkowy, choć są wyjątki (np. Milestone na zakup licencji Corporate lub Genetec na wybrane licencje, np. obsługę central alarmowych firm trzecich). Co do zasady każda firma daje możliwość wyboru usługi serwisowej oraz okresu, na jaki można ją wykupić. Koszt roczny wynosi na ogół od ok. 8% do nawet 20% wartości licencji zakupionego oprogramowania.

Część producentów, np. Geutebrück, koszty wynikające z umowy SMA wlicza w cenę sprzedawanych urządzeń na 3 lata. Nedap dostarcza roczną, bezpłatną umowę serwisową do zakupionych licencji oprogramowania AEOS. Po takim (darmowym) okresie trwania umowy można zdecydować, czy wykupić ją na kolejny okres, czy też zrezygnować, nie widząc z jej posiadania żadnych profitów. Bosch (podobnie jak Nedap) jeszcze do niedawna dostarczał roczne umowy w ramach zakupionych licencji. Ostatnio zmienił politykę, oferując dwie opcje: darmową i płatną. W ramach darmowej polityki (tzw. opcja GO), która przypomina trochę wsparcie w uruchomieniu oprogramowania, „klienci są objęci programem pomocy technicznej przez 90 dni od aktywacji nowego pakietu licencyjnego oprogramowania"[2]. Płatna opcja PRO zapewnia dostęp do mniejszych i większych aktualizacji licencjonowanego oprogramowania oraz regularne aktualizacje zabezpieczeń IT pozwalające zwiększyć poziom ochrony danych. To typowe podejście dla płatnych SMA.

Wspomniałem o jeszcze jednej opcji, a mianowicie o jednorazowej opłacie migracyjnej lub tzw. opłacie z tytułu podniesienia wersji do wyższej.

Taką opcję oferuje m.in. Avigilon, jednocześnie zastrzegając, że świadczy wsparcie jedynie do wersji obowiązującej i jednej istotnej wersji wstecz (tzw. major release). Taka polityka nie należy do najczęściej stosowanych, poza Avigilonem nie znalazłem innych przykładów jej zastosowania.

5 KORZYŚCI PŁYNĄCYCH Z REGULARNEJ KONSERWACJI OPROGRAMOWANIA[3]

NAPRAWA BŁĘDÓW

W zarządzaniu konserwacją naprawa błędów ma priorytetowe znaczenie dla bezproblemowego działania oprogramowania. Proces ten polega na wyszukiwaniu błędów w kodzie i ich poprawianiu. A problemy mogą wystąpić niemal wszędzie: w sprzęcie, systemie operacyjnym lub dowolnej części oprogramowania.

DOSTĘP DO EKSPERTÓW TECHNICZNYCH

Żadne rozwiązanie programowe nie jest idealne, dlatego tak ważna jest możliwość otwarcia karty zgłoszenia usterki u producenta, który najlepiej zna swoje oprogramowanie. Jakość wsparcia ma największe znaczenie w sytuacjach, w których czas odgrywa kluczową rolę, gdy nie można dopuścić do przestojów i żmudnej czasochłonnej analizy logów z wielu urządzeń.

ROZSZERZENIE FUNKCJONALNOŚCI

Regularna konserwacja oprogramowania jest gwarancją wdrożenia funkcjonalności w celu dostosowania rozwiązania do zmieniającego się otoczenia rynkowego, m.in. nowe wersje platformy oprogramowania, nowe funkcje, aktualizacje sprzętu, nowe zasady komunikacji między urządzeniami i wszystkie inne aspekty wpływające na pracę systemu.

POPRAWA WYDAJNOŚCI

Deweloperzy wykrywają problemy, wykonując testy, i stale je rozwiązują, co naturalnie poprawia wydajność systemu. Ponadto wybrane elementy interfejsu użytkownika oraz kodu są usuwane i zastępowane nowymi rozwiązaniami, z wykorzystaniem najnowszych narzędzi i technologii. Zapobiega to powstawaniu „długu" technologicznego w produkcie i słabych punktów, które mogłyby sprzyjać szkodliwym działaniom, takim jak nieuprawniony dostęp lub wyciek informacji.

MOŻLIWOŚĆ AKTUALIZACJI

Niektóre funkcje mogą nie występować w produkcie zakupionym wcześniej, ale będą dostępne w zapowiadanej jego wersji. W czasie obowiązywania umowy serwisowej można aktualizować oprogramowanie do nowszej wersji. Pozostaje tylko decyzja o wykonaniu aktualizacji.

Maciej Pietrzak, Dahua Technology

Dahua Technology, oferując oprogramowanie VMS DSS Pro, stara się je stale udoskonalać. Kupując licencję, użytkownik nabywa jednocześnie możliwość korzystania z wszelkich aktualizacji producenta. Oferujemy również modyfikacje oprogramowania już na etapie wdrożenia całego systemu. Zależnie od złożoności nowej funkcjonalności i zasobów niezbędnych do jej wprowadzenia, usługa ta może być darmowa lub wyceniana indywidualnie. W grę wchodzi dostosowanie istniejących funkcji oraz dodawanie nowych modułów funkcjonalnych.

Jakub Kozak, Genetec

Cyberbezpieczeństwo to dzisiaj największe wyzwanie dla użytkowników systemów. Najlepszą strategią utrzymania odporności systemu jest jego ciągłe uaktualnianie. Program Genetec™ Advantage zapewnia bezpłatny dostęp do najnowszych wersji w przewidywalnym, łatwym do budżetowania modelu. Klienci mogą również wypróbować innowacyjne dodatkowe usługi bez konieczności dokonywania ich zakupu. Dostęp do pomocy technicznej premium zapewnia szybkie rozwiązanie wszelkich problemów napotkanych przez użytkowników systemu.

CZY POSIADANIE SMA MA SENS?

Robert Glass (amerykański inżynier oprogramowania znany z prac z dziedziny inżynierii oprogramowania, szczególnie w zakresie pomiaru jakości projektowania oprogramowania i studiów nad najnowszymi badaniami inżynierii oprogramowania) opisał fakt dotyczący konserwacji, który brzmi następująco: „60% kosztów oprogramowania to konserwacja, a około 60% kosztów konserwacji to poprawa"[4].

Zakupione, w pełni funkcjonalne oprogramowanie może nie ukazywać błędów w działaniu w fazie deweloperskiej, dopóki nie zostanie aktywnie wprowadzone do środowiska produkcyjnego. Innymi słowy – dopóki użytkownik z krwi i kości się nim nie zajmie. Posiadana umowa na konserwację ma zapewnić, że ewentualne błędy zostaną (kiedyś) przez producenta naprawione.

Rozwój technologiczny ma taką dynamikę, że dodawanie nowych, bardziej zaawansowanych urządzeń do istniejących systemów staje się nieuniknione. Umowa serwisowa od dostawcy oprogramowania obejmuje nie tylko pomoc w rozwiązywaniu problemów z kompatybilnością z nowszym sprzętem, ale też pomoc w rozwiązaniu problemów związanych z modyfikacją już istniejącego systemu.

Z kolei cykliczne aktualizacje i poprawki w ramach obowiązującej umowy SMA „przedłużają życie" oprogramowania zgodnego z najnowszymi trendami. Aktualizacje mogą obejmować poważne zmiany w oprogramowaniu (np. zmianę protokołu wymiany danych) lub drobne naprawy problemów zgłoszonych przez innych użytkowników, które poprawiają jakość pracy.

Tymczasem klient zadowolony z efektów wdrożenia rozwiązania po jednym bezproblemowym roku pracy systemu zaczyna kwestionować znaczenie umowy serwisowej. Z pobieżnej analizy może się często wydawać, że opłaty związane z SMA są zbędne, a rezygnacja z jej wykupu przyniesie firmie konkretne oszczędności.

Warto jednak pamiętać, że koszt wsparcia wg umowy obejmuje ważne poprawki błędów, rutynowe aktualizacje i rozwiązania krytycznych problemów, dostarczane w konkretnym czasie. Umowa wsparcia technicznego ustala w pewnym sensie wartość rocznych wydatków na bezpieczeństwo, eliminując nieprzewidziane wydatki związane z oprogramowaniem. Trzeba przyznać, że coroczna opłata w wysokości 1/5 wartości zakupionych licencji na oprogramowanie za wsparcie nie wydaje się tanim rozwiązaniem i jest postrzegana przez inwestorów jako „palenie pieniędzy". Na poparcie tej tezy można przytoczyć wyniki badania przeprowadzonego przez Campaign for Clear Licensing (CCL), które wykazało, że większość organizacji na ślepo odnawia umowy na utrzymanie oprogramowania[5].

Dostęp do ciągłych aktualizacji może wydawać się drogi. Niekiedy tańszym rozwiązaniem może być zaprzestanie płacenia za bieżącą konserwację i późniejszy zakup nowszej wersji oprogramowania. Jednorazowy zakup nowych licencji jest na pewno tańszy, ale do kosztu nowego oprogramowania należy doliczyć koszt wdrożenia i konfiguracji – czego na ogół się nie uwzględnia. Trzeba mieć świadomość, że przesiadka do znacząco nowszej wersji na ogół ogranicza możliwość przeniesienia istniejącej konfiguracji bez błędów i piętrzących się problemów, a to przekłada się na ogólny wyższy koszt wdrożenia.

W dzisiejszych warunkach ekonomicznych, gdy budżety są ograniczone i poddawane ścisłej kontroli, wiele przedsiębiorstw poszukuje sposobów na obniżenie długoterminowych całkowitych kosztów posiadania. Jednym z kluczowych obszarów, w którym inwestorzy w naszej branży chcą uzyskać szybki zwrot z inwestycji, jest utrzymanie ciągłości działania wdrożonych elektronicznych systemów zabezpieczeń. Dostęp do aktualnych wersji oprogramowania i usług wsparcia technicznego staje się kluczowy, gdy coś idzie nie tak. Jest to twój pas bezpieczeństwa. Twoja inwestycja w oprogramowanie jest chroniona, ponieważ jest ktoś, do kogo możesz zadzwonić, gdy nie wszystko działa zgodnie z oczekiwaniami.

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.

2) https://www.boschsecurity.com/pl/pl/rozwiazania/oprogramowanie-do-zarzadzania/bosch-software-assurance/#your-benefits

3) Na podstawie: https://blog.speech.com/2019/05/30/why-renew-your-software-maintenance-agreement/ 2020-11-01

4) https://www.fingent.com/blog/why-get-a-maintenance-contract-with-your-software-solution-provider/ 2020-10-22

5) Według CCL tylko 10 ze 100 badanych organizacji zaangażowało właściwe osoby w proces decyzyjny o przedłużeniu umów na konserwację. Reszta umów na konserwację oprogramowania była przedłużana albo przez właścicieli systemów, albo przez działy finansowe, którym zlecono wykonanie takiego zadania.

Centrale alarmowe PERFECTA

Łatwa konfiguracja, wygodna obsługa

Właściciele domów, mieszkań, lokali biurowych czy usługowych coraz częściej decydują się na montaż mniej lub bardziej zaawansowanego systemu sygnalizacji włamania i napadu. Jaką centralę warto wskazać inwestorom oczekującym od alarmu intuicyjnej codziennej obsługi, jeśli do zabezpieczenia obiektu wystarczą maksymalnie 32 czujki? Jakie rozwiązanie wybrać, by było ekonomiczne dla właściciela obiektu, a dla instalatora wygodne i łatwe w instalacji?

Poszukując optymalnego rozwiązania, które idealnie spełni wszystkie oczekiwania, warto przyjrzeć się centralom PERFECTA z oferty SATEL. Prosta konfiguracja (podobna jak w centralach serii CA), szeroki wachlarz urządzeń peryferyjnych (przewodowych i bezprzewodowych) oraz wygodne sterowanie to trzy cele, które przyświecały twórcom tych urządzeń.

W skład rodziny PERFECTA wchodzi aż 10 central różniących się maksymalną liczbą wejść, możliwością obsługi urządzeń bezprzewodowych, a także typem zintegrowanego modułu komunikacyjnego. Szeroki wybór modeli pozwala dobrać odpowiednie urządzenie do zabezpieczanego obiektu oraz oczekiwań inwestora. Na serię PERFECTA składają się:

- PERFECTA 16
- PERFECTA 16-WRL
- PERFECTA 32
- PERFECTA 32-WRL
- PERFECTA 32 LTE
- PERFECTA 32-WRL LTE
- PERFECTA-IP 32
- PERFECTA-IP 32-WRL
- PERFECTA-T 32
- PERFECTA-T 32-WRL

PODOBIEŃSTWA I RÓŻNICE

Wszystkie centrale posiadają na płycie po 8 wejść, przy czym ich liczbę można zwiększyć do 16 lub 32 (patrz: nazwa centrali). Nadzorowany obiekt można podzielić na dwie strefy, a w każdej z nich zdefiniować trzy tryby czuwania: nocny, dzienny i pełny. Wyjść może być maksymalnie 12 (lub 16 – PERFECTA WRL).
Modele z oznaczeniem WRL obsługują urządzenia radiowe 433 MHz, w tym czujki oraz sygnalizatory systemu MICRA, a także piloty i manipulatory bezprzewodowe.
Jeśli chodzi o moduły komunikacyjne, to wybrać można centrale z komunikatorem komórkowym pracującym w sieciach 2G (PERFECTA) lub 2G/3G/4G (PERFECTA LTE), ethernetowym (PERFECTA-IP) lub dialerem telefonicznym PSTN (PERFECTA-T).

OBSŁUGA, POWIADAMIANIE, MONITORING

Systemem można sterować za pomocą tradycyjnych manipulatorów lub pilotów. Alternatywę stanowi aplikacja mobilna PERFECTA CONTROL (oprócz PERFECTA-T), która umożliwia nie tylko zdalne włączanie i wyłączanie czuwania, ale także wgląd w stan systemu oraz wyświetlenie podglądu z kamer rozmieszczonych na obiekcie. Powiadomienia PUSH na bieżąco informują o występujących zdarzeniach. Centrale posiadające komunikatory komórkowe mogą realizować powiadomienia głosowe i SMS. Wiadomościami SMS można również wysyłać do central komendy sterujące.
Monitoring zdarzeń może być przesyłany do 2 niezależnych stacji monitorujących, obsługujących m.in. formaty: Contact ID i SIA, w zależności od modułu komunikacyjnego centrali, dostępne będą inne tory transmisji.

ŁATWE KONFIGUROWANIE

To, co łączy wszystkie modele i co szczególnie doceniają instalatorzy, to proste programowanie. Centrale można konfigurować na dwa sposoby. Pierwszy jest bardziej „tradycyjny", czyli z manipulatora (podobnie jak w starszych centralach CA). Drugi to praca z PERFECTA Soft, programem posiadającym przejrzysty i intuicyjny interfejs. Instalator jest krok po kroku prowadzony przez kolejne etapy tworzenia systemu, m.in. dostając podpowiedzi, jakie urządzenia można jeszcze podłączyć. Warto dodać, że konfigurowanie oraz aktualizacja oprogramowania central (oprócz PERFECTA-T) może odbywać się zdalnie za pośrednictwem sieci komórkowej lub Ethernet.

Podsumowując, centrale alarmowe rodziny PERFECTA to urządzenia, które mimo że należą do segmentu rozwiązań ekonomicznych, oferują całkiem spore możliwości, co z pewnością docenią inwestorzy oraz użytkownicy. Z kolei wygodne konfigurowanie to duża zaleta dla każdego instalatora.

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

Bezprzewodowy system alarmowy Ajax

Pełna ochrona przed włamaniem, pożarem i zalaniem każdego rodzaju obiektu

Ajax to profesjonalny bezprzewodowy system alarmowy chroniący przed włamaniem, pożarem i zalaniem. Linia produktów obejmuje 33 urządzenia w obudowach w czarnym i białym kolorze, w tym czujki ruchu, pożaru i zalania, centrale alarmowe (huby), syreny, klawiatury, przyciski alarmowe, urządzenia do automatyzacji inteligentnego domu itp.

JAK DZIAŁA AJAX

Wszechstronny system alarmowy. Ajax chroni obiekty każdego rodzaju (mieszkania, domy, biura, sklepy, a nawet zakłady produkcyjne) przed włamaniem, pożarem i zalaniem. Czujki ruchu są odporne na zwierzęta do wielkości 50 cm.
Dostępna jest także fotograficzna weryfikacja przyczyn alarmów. Czujki MotionCam z kamerą potwierdzają wystąpienie prawdziwego alarmu ograniczając niepotrzebne interwencje agencji ochrony. Wbudowana kamera nie rejestruje obrazu przez całą dobę; robi zdjęcia tylko w przypadku wykrycia ruchu, co zapewnia poczucie prywatności.Możliwe jest zintegrowanie zewnętrznego systemu CCTV z systemem Ajax.

Bezprzewodowy. Urządzenia Ajax komunikują się przez protokół radiowy Jeweller opracowany przez Ajax Systems, zapewniający dwukierunkową komunikację o zasięgu do 2000 m i wysokiej wydajności energetycznej – baterie w czujkach mają żywotność 5-7 lat.

Dane przesyłane przez protokół Jeweller są szyfrowane, a uwierzytelnianie uniemożliwia nieautoryzowany dostęp do urządzenia. W przypadku prób zagłuszania system przełącza się na wolną częstotliwość radiową i wysyła powiadomienia do użytkowników i agencji ochrony. Uruchomienie alarmu zajmuje systemowi Ajax zaledwie 0,15 s.

Niezawodny. Ajax spełnia wymagania europejskiej normy bezpieczeństwa EN 50131 i ma certyfikat Grade 2. Centrale sterujące (huby) są obsługiwane przez nasz system operacyjny OS Malevich, który się nie zawiesza i jest odporny na wirusy.
Awarie prądu to nie problem – hub ma baterię zapasową, która może działać przez 16 godzin. Dostępnych jest także kilka kanałów komunikacji: Ethernet, Wi-Fi, a także dwa gniazda karty SIM 2G/3G/4G (kanały różnią się w zależności od wersji huba). Działają jednocześnie, wzajemnie wspierając się w razie sytuacji alarmowej.

Szybka instalacja i konfiguracja. Urządzenia podłącza się do huba przez skanowanie kodu QR z poziomu aplikacji mobilnej Ajax. Proces ten trwa niespełna minutę.
System nie wymaga montażu przewodów w ścianach, więc można go łatwo zainstalować nawet w świeżo wyremontowanym wnętrzu. Można go w pełni skonfigurować zdalnie za pośrednictwem aplikacji mobilnej, bez konieczności pobytu w obiekcie. Ajax wysyła powiadomienie, gdy urządzenie nie działa prawidłowo lub wymaga wymiany baterii.

Dostępny dla Stacji Monitorowania Alarmów. System alarmowy Ajax można podłączyć do powszechnie używanych centralnych stacji monitorowania za pośrednictwem standardu Conctact ID lub SIA.

Aplikacja mobilna. Dostępne są aplikacje mobilne dla użytkowników (iOS, Android) oraz oprogramowanie dla specjalistów Ajax PRO – narzędzie dla inżynierów i Ajax PRO Desktop, czyli aplikacja komputerowa z funkcją monitorowania alarmów.

Automatyzacja bezpieczeństwa. Oferta Ajax obejmuje bezprzewodowo sterowane gniazdka *plug-and-play* z przekaźnikami niskoprądowymi, które umożliwiają zarządzanie zasilaniem poszczególnych urządzeń elektrycznych lub oświetleniem z poziomu aplikacji mobilnej Ajax.
Dzięki scenariuszom automatyzacji można skonfigurować system tak, aby automatycznie odpierał zagrożenia, wyłączając wodę przy pierwszych oznakach zalania, odcinając zasilanie podczas pożaru oraz konfigurując symulację aktywności domowych itp.

Hub 2 Plus – absolutna ochrona

Hub 2 Plus charakteryzuje się modułami komunikacyjnymi o najlepszych parametrach wśród hubów Ajax. Nowy hub obsługuje Wi-Fi i trzy standardy komunikacji cyfrowej, w tym LTE, czyli technologię 4G porównywalną pod kątem prędkości i niezawodności do Ethernet. Zwiększa to szybkość fotograficznej weryfikacji alarmów, poprawia skuteczność reakcji na alarm, tworząc nowy standard w branży zabezpieczeń. Jednak ulepszenia w nowym hubie wykraczają poza komunikację. Hub 2 Plus obsługuje 200 urządzeń, 100 kamer, 200 użytkowników i 64 scenariusze. Nowy procesor i zwiększona pojemność pamięci sprawiają, że Hub 2 Plus będzie przez długi czas o krok przed konkurencją.

Nieustanna łączność. Cztery niezależne kanały – Ethernet, Wi-Fi i dwie karty SIM – zapobiegają ryzyku utraty łączności na dwóch poziomach: fizycznym (przewodowe połączenie na wypadek utraty sygnału bezprzewodowego i odwrotnie) i na poziomie dostawcy usługi GSM (każdy kanał może być obsługiwany przez innego dostawcę). Jeśli dojdzie do problemów z łącznością, przełączanie między kanałami uruchamia się automatycznie.

Zawsze gotowy na niebezpieczeństwo. Firma Ajax zwróciła szczególną uwagę na prędkość połączenia Hub 2 Plus, aby przesyłanie animowanych serii zdjęć z czujników ruchu MotionCam do smartfonów użytkowników i stacji monitorowania zajmowało zaledwie kilka sekund nawet poprzez komórkowe połączenie z Internetem. Zdjęcia są przesyłane do Hub 2 Plus za pośrednictwem szyfrowanego protokołu radiowego Wings, a najszybsze połączenie internetowe służy do przesyłania zdarzeń z huba do użytkownika.
Jeśli chodzi o bezpieczeństwo, Hub 2 Plus polega na sprawdzonych autorskich technologiach Ajax Systems. Hub pracuje na systemie operacyjnym czasu rzeczywistego OS Malevich, chronionym przed awariami i cyberatakami, a na poziomie komunikacji między urządzeniami wykorzystuje Jeweller – szyfrowany protokół radiowy do komunikacji dwukierunkowej. Jeweller przesyła alarmy w zaledwie 0,15 s i przełącza się na częstotliwość zapasową w przypadku zakłóceń. Szyfrowana komunikacja i system operacyjny czasu rzeczywistego uniemożliwiają hakowanie urządzenia Hub 2 Plus.

Więcej scenariuszy. Z Hub 2 Plus użytkownicy mogą utworzyć do 64 scenariuszy do automatyzacji bezpieczeństwa. Zamknij rolety podczas uzbrajania, wyłącz wodę w razie zalania lub ogranicz potencjalne przyczyny pożaru – wszystkie te zadania można powierzyć Hub 2 Plus. Scenariusze można uruchamiać przez harmonogram lub naciśnięcie przycisku Button.

Więcej funkcji. Duża skala to „drugie imię" Hub 2 Plus. Obsługa do 200 użytkowników i urządzeń, 100 kamer wideo, 25 grup i 5 podwajaczy zasięgu ReX sprawia, że jest to uniwersalne rozwiązanie do ochrony mieszkań i obiektów biznesowych. W porównaniu z Hub 2, Hub 2 Plus ma 4,5 razy mocniejszy procesor i 8 razy więcej pamięci. Stanowi to solidną podstawę do ulepszeń systemu za pośrednictwem aktualizacji systemu operacyjnego OS Malevich. Proces aktualizacji odbywa się zdalnie i trwa kilka minut, a przy tym nie wymaga interwencji inżyniera ani użytkownika.

Markowa wygoda. Huby Ajax nie potrzebują klawiatury – wszystkim można zarządzać z poziomu aplikacji mobilnej. Firma opracowała łatwą w użyciu aplikację mobilną dla użytkowników końcowych i oddzielne aplikacje dla profesjonalistów, uwzględniające potrzeby instalatorów i operatorów stacji monitorowania. Aplikacje działają na wszystkich popularnych platformach: Android, iOS, Windows i MacOS.
Hub jest montowany do powierzchni przy użyciu uchwytu montażowego SmartBracket, dzięki czemu nie trzeba rozkręcać całej centrali. Aby zacząć pracę, wystarczy podłączyć hub do sieci i dodać go do aplikacji, skanując kod QR. Za pomocą aplikacji możesz zarządzać trybami bezpieczeństwa, przeglądać obrazy z podłączonych kamer i historię zdarzeń w systemie, zdalnie zarządzać urządzeniami elektrycznymi i tworzyć scenariusze do automatyki.
Od wersji 2.9 OS Malevich, wszystkie huby zyskały funkcję kopiowania danych z innego huba. Teraz przejście na Hub 2 Plus zajmuje ok. 15 minut. A to wszystko bez potrzeby podłączania urządzeń, zapraszania użytkowników i konfigurowania systemu.

Informacje o firmie. *Ajax Systems to europejski producent systemów alarmowych z rozwiązaniami dla inteligentnego domu. Siedziba firmy mieści się w Kijowie na Ukrainie. Firmę założył w 2011 r. Aleksandr Konotopskyi. Dziś inteligentne alarmy Ajax zapewniają ochronę ponad 830 tys. osób w 120 krajach na całym świecie, zabezpieczając przed włamaniami, pożarami i zalaniami. Ajax to najczęściej nagradzany system alarmowy w Europie.*

AJAX SYSTEMS
hello@ajax.systems
www.ajax.systems

SAFESTAR security cloud

Profesjonalne centrum monitoringu w chmurze

Profesjonalne centrum monitoringu jest jak Yeti – wszyscy o nim słyszeli, nikt nie widział. Dlaczego? Wynika to z faktu, że każdy ma własny pogląd, jak takie centrum powinno wyglądać i funkcjonować. Istnieją wprawdzie standardy i normy w tym zakresie, ale raczej mało kto je stosuje, ponieważ nie są prawnie wymagane. W związku z tym trudno obiektywnie ocenić, które centrum monitoringu jest profesjonalne i w jakim stopniu, ponieważ nie ma się do czego odnieść, nie ma skali ocen.

Krzysztof Ciesielski

Jednak niezależnie od tego, czy mówimy o centrum monitoringu w agencji ochrony, czy w firmie sieciowej, można się zgodzić, że jednym z najważniejszych elementów skutecznego działania centrum monitoringu jest właściwa organizacja obsługi zdarzeń i alarmów zarówno tych pochodzących z systemów i nadajników alarmowych, jak i generowanych przez systemy analizy wideo.

O profesjonalnym działaniu centrum monitorowania z pewnością świadczy dobrze zaplanowany i ujednolicony proces obsługi zdarzeń i alarmów. Najlepiej, aby były one obsługiwane wg tego samego schematu niezależnie od tego, z jakich systemów pochodzą.

Alarmy niosą ze sobą różne informacje pozwalające na identyfikację zagrożenia, a tym samym na podjęcie odpowiedniej i skutecznej interwencji. Taką możliwość daje chmurowa platforma do monitoringu i zarządzania bezpieczeństwem Safestar. Dzięki różnym polom danych i automatyzacji przy obsłudze alarmów reakcja jest szybka i właściwa, a obsługa zdarzeń z systemów alarmowych i dozoru wizyjnego ujednolicona, co standaryzuje i zdecydowanie upraszcza ich obsługę.

→ **Więcej informacji dotyczących systemu Safestar znajduje się na stronie safestar.pl. Z poziomu strony www można również założyć bezpłatne konto i w jego ramach zapoznać się z system, a także zacząć wykonywać usługi monitoringu z wykorzystaniem tego systemu.**

Przy obsłudze sygnałów z systemów dozorowych z analityką wideo platforma Safestar oferuje takie same udogodnienia, jak przy obsłudze sygnałów z systemów alarmowych. Chodzi o takie funkcjonalności, jak kolejkowanie czy grupowanie alarmów, możliwość stosowania harmonogramów, procedury, rejestry notatek, programowe uzbrojenia, wspólna aplikacja mobilna integrująca kilka systemów.

Dzięki możliwości oglądania obrazu online czy przeglądania prealarmów w trakcie obsługi alarmu można zdalnie ocenić sytuację w obiekcie. Wyświetlanie obrazu można połączyć z konkretnym sygnałem z czujek lub innych nadajników/systemów.

Dodając możliwość komunikacji głosowej poprzez głośnik umieszczony przy kamerze, operator może „na gorąco" przepędzić intruza, kierując do niego komunikat głosowy. Na końcu procesu obsługi alarmu jest wysłanie grupy interwencyjnej, jeżeli pojawi się taka konieczność.

Odsetek realnych alarmów obsługiwanych przez centra monitorowania waha się między 2 a 5% wszystkich zdarzeń – reszta to tzw. fałszywe alarmy. Korzystanie z Safestar w połączeniu z odpowiednim doborem sprzętu w obiekcie umożliwia wyeliminowanie zbędnych interwencji. Jednocześnie rejestracja przebiegu obsługi zdarzeń oraz raportowania pozwalają na udokumentowanie właściwego i starannego zrealizowania usług.

Przykładowo, w Safestar można wygenerować odpowiedni raport opatrzony zdjęciami z kamer. Analiza danych i raportowanie również w obszarze obsługi wideo jest kluczową funkcjonalnością Safestar. Jest ona ciągle rozbudowywana i dostosowana do potrzeb klientów.

Podsumowując, centrum monitoringu musi w sposób profesjonalny obsługiwać alarmy i umożliwiać rzetelne udokumentowanie tej obsługi. Obie te funkcjonalności zapewnia system Safestar i dlatego uważamy, że jest to obecnie najlepsze rozwiązanie dla profesjonalnych centrów monitoringu.

DMSI SOFTWARE

ul. Kłobucka 23c/119
02-699 Warszawa
tel. 22 112 17 97
biuro@dmsi.pl https://dmsi.pl

EBS przechodzi do Google Cloud

Firma EBS, polski producent systemów zabezpieczeń oraz rozwiązań do automatyzacji biznesu, przenosi we współpracy z Chmurą Krajową swoje aplikacje do Google Cloud. Zmiana ma związek z dynamicznym rozwojem firmy na rynkach międzynarodowych.

EBS specjalizuje się w zakresie Internetu Rzeczy (IoT), oferując zaawansowane systemy zabezpieczeń oraz rozwiązania umożliwiające automatyzację biznesu. Spółka jest twórcą m.in. pierwszego na świecie systemu monitoringu online pracowników. Z jej oferty korzystają firmy z branży ochrony i zakłady produkcyjne. Dzięki trzydziestoletniemu doświadczeniu oraz wynikom pracy działu badań i rozwoju przedsiębiorstwo zdobyło bardzo mocną pozycję na globalnym rynku tego typu rozwiązań. Firma jest obecna na pięciu kontynentach, pod jej kontrolą pracuje 3 mln urządzeń. To właśnie sukces na rynku międzynarodowym był impulsem do zmian w obszarze IT.

– Aplikacje zarządzające naszymi urządzeniami były dotychczas hostowane w serwerowni na terenie Polski. Jesteśmy obecni na tak odległych rynkach, jak obie Ameryki, Azja czy Afryka. Właśnie ze względu na skalę działania i potrzebę zapewnienia niezmiennie wysokiej jakości naszych usług niezależnie od lokalizacji pojawiła się potrzeba wdrożenia nowych rozwiązań. Musieliśmy mieć również pewność, że spełnione będą bardzo wysokie standardy bezpieczeństwa – mówi Tomasz Laudy, wiceprezes Zarządu EBS.

–Po analizie dostępnych technologii wraz z ekspertami Chmury Krajowej doszliśmy do wniosku, że najlepszym wyborem będzie Google Cloud. Dzięki globalnej dostępności serwerowni oraz szerokiemu spektrum gotowych narzędzi i rozwiązań Google, możemy nie tylko zlokalizować je bliżej naszych klientów, ale również przyspieszyć proces wdrażania naszych rozwiązań. Wszystko oczywiście przy zapewnieniu odpowiedniego poziomu bezpieczeństwa – podsumowuje Tomasz Laudy. Obecnie analizowane są kolejne obszary IT, które mogą zostać przeniesione do środowiska Google Cloud.

– Przeniesienie przez EBS aplikacji z dotychczasowych serwerów do Google Cloud jest doskonałym przykładem na to, że chmura obliczeniowa wspiera rozwój przedsiębiorstw. Globalny dostawca posiada serwerownie w różnych częściach świata. W przypadku firmy operującej globalnie, tak jak EBS, oznacza to możliwość bycia bliżej klienta – podkreśla Magdalena Hundz, Sales Executive Chmury Krajowej.

– Obecność polskich przedsiębiorstw na rynkach międzynarodowych będzie rosła, bo nasza gospodarka ma coraz więcej innowacyjnych produktów i usług do zaoferowania. Chcemy wspierać je w tym procesie, zapewniając dostęp do odpowiednich technologii – dodaje.

PRODUKTY EBS:

SMART COMMUNICATORS
Uniwersalne zastosowanie z dowolną centralą alarmową. Zdalne zarządzanie dzięki aplikacjom mobilnym dla instalatora i użytkownika.

ALARM SYSTEMS
Pełne portfolio: od profesjonalnego systemu alarmowego z elementami Smart Home w postaci AVA PRO, po klasyczne rozwiązanie, system Callisto.

LONE WORKER MONITORING
System monitoringu pracowników w czasie rzeczywistym (automatyczne wysyłania raportów, informacji do decydentów, supervisorów i pracowników ochrony).

EBS

ul. Bronisława Czecha 59,
04-555 Warszawa
https://ebssmart.com
office@ebssmart.com

Pandemia COVID-19 ujawniła słabe punkty w łańcuchach dostaw, które przysporzyły problemów w wielu branżach. Uwydatniła problemy związane z koncepcjami produkcyjnymi JIT/JIS oraz wynikające z braku dywersyfikacji dostaw i uzależnienia się od jednego dostawcy, a także potrzebę lepszego przygotowania się do wystąpienia nieprzewidzianych sytuacji. Firmy pracują więc nad zabezpieczeniem ciągłości dostaw, łatając luki w zarządzaniu, digitalizując łańcuchy dostaw oraz wdrażając sztuczną inteligencję i analizy predykcyjne.

Zakłócenia łańcuchów dostaw

spowodowane przez COVID-19

Eifeh Strom

a&s International

KORONAWIRUS OBNAŻA SŁABE PUNKTY W ZARZĄDZANIU ŁAŃCUCHEM DOSTAW

Świat nigdy wcześniej nie doświadczył zakłóceń w zarządzaniu łańcuchem dostaw na taką skalą, do jakiej przyczyniła się pandemia. Co więcej, nikt nie był na nie przygotowany. Koronawirus uwypuklił wszystkie wady metod zarządzania produkcją *just-in-time*[1]/*just-in-sequence*[2] (JIT/JIS) oraz luki w branży transportowej. Firmy muszą więc znaleźć sposoby rozwiązania tych problemów, aby zabezpieczyć swoje obecne i przyszłe potrzeby w całym łańcuchu dostaw.

- KONCEPCJE JIT/JIS

Na skutek COVID-19 mocno ucierpiał sektor produkcyjny. W czasie *lockdownu* zamknięto większość fabryk różnych branż, a łańcuchy dostaw na całym świecie zostały zakłócone. Najbardziej ucierpiały sektory, które w dużym stopniu opierają się na modelach JIT/JIS, np. przemysł motoryzacyjny. *Wynika to z faktu, że w tych branżach wszelkie zakłócenia ściśle zarządzanej produkcji natychmiast wywołają poważny skutek* – wyjaśnił Per Ädelroth, dyrektor ds. łańcucha dostaw w Axis Communications.

Przemysł motoryzacyjny od lat był pionierem w zakresie globalizacji i koncepcji JIT/JIS. Pandemia pokazała, jak bardzo wrażliwe i podatne na zakłócenia są te wymagające perfekcji koncepcje zarządzania w czasie kryzysu. Obnażając wady metod JIT/JIS, koronawirus zmusił firmy do ich ponownej oceny, które będą dywersyfikować swoje dostawy i planować niezbędny poziom zapasów, aby uniknąć zakłóceń.

- OTWARTA KOMUNIKACJA

Ważną rolę w łańcuchu dostaw odgrywają transport i łączność. Duże odległości między dostawcami a klientami zwiększają ryzyko wystąpienia wielu problemów. Mogą to być awarie u dostawców, tymczasowe ograniczenia eksportowe w kraju dostawcy i niedostępność dostawców usług logistycznych, zamykanie portów źródłowych czy docelowych, anulowanie połączeń lotniczych itp.

1) *Just-in-time* – metoda zarządzania stosowana w celu redukcji pracy w toku (work in progress) i poziomu zapasów w procesach produkcyjno-magazynowych.
2) *Just-in-sequence* – strategia inwentaryzacji, która dopasowuje się do zmienności produkcji na linii montażowej. Komponenty i części docierają na linię produkcyjną dokładnie na czas, zgodnie z planem, zanim zostaną zmontowane.

W przypadku Axis Communications ograniczenia w przewozach miały największy wpływ na firmę na wczesnych etapach pandemii – zarówno dotyczące wysyłki komponentów do zakładów produkcyjnych, jak i transportu gotowych produktów do partnerów i klientów.

Znaczna część ładunków jest przewożona liniami pasażerskimi, więc przy krajowych blokadach i ograniczeniach w podróżowaniu przepustowość została nagle i poważnie zmniejszona – stwierdziła Ulrika Magnusson, dyrektor globalnego łańcucha dostaw w Axis Communications. Reagując szybko w poszukiwaniu alternatywnych opcji transportu naziemnego, Axis był w stanie w dużej mierze rozwiązać ten problem.

Sprawą kluczową przy ustalaniu prawdopodobieństwa opóźnień w dostawach podczas COVID-19 jest również utrzymywanie otwartej i regularnej łączności z partnerami i klientami. Będąc z nimi w stałym kontakcie, można informować o tym, które zamówienie zostanie zmniejszone lub opóźnione, co pozwoli na szybkie wprowadzenie niezbędnych korekt lub znalezienie alternatywnych źródeł dostaw, gdyby zaszła taka potrzeba. Jest to szczególnie ważne, ponieważ prawdopodobieństwo, że dostawcy będą cierpieli z powodu braku materiałów lub przestojów w produkcji podczas pandemii, gwałtownie wzrosło.

WNIOSKI STRATEGICZNE

Kiedy w Chinach na początku ub. roku wybuchła epidemia koronawirusa i kraj zamknął fabryki, zatrzymał transport i zamknął granice, łańcuchy dostaw na całym świecie szybko odczuły te przestoje. Firmy na całym świecie czekały na ponowne otwarcie się Państwa Środka, doświadczając, co się może stać, gdy polega się tylko na jednym źródle zaopatrzenia. *Pandemia koronawirusa uświadomiła wszystkim, że zarządzanie łańcuchem dostaw ma znaczenie strategiczne. Szczególnie ważne jest w e-handlu. Przykładem może być firma Amazon i sposób, w jaki zdominowała rynek zamówień oraz prędkość dostaw napędzanych przez zarządzanie łańcuchem dostaw. W odniesieniu do znaczenia strategicznego jasno określono jego wagę* – powiedział Tom Craig, niezależny konsultant ds. łańcucha dostaw i logistyki.

W rezultacie firmy musiały zaktualizować swoją strategię łańcucha dostaw, aby mieć pewność, że ich działalność nie zostanie zawieszona podczas kolejnego przestoju z powodu braku zapasów.

PANDEMIA UŚWIADOMIŁA ZNACZENIE WŁAŚCIWEGO ZARZĄDZANIA ŁAŃCUCHEM DOSTAW. DYWERSYFIKACJA ŹRÓDEŁ I ZNALEZIENIE RÓWNOWAGI MIĘDZY PODAŻĄ A POPYTEM TO WAŻNE STRATEGICZNE WNIOSKI PŁYNĄCE Z DOŚWIADCZEŃ DOTYCZĄCYCH COVID-19

- DYWERSYFIKACJA ŁAŃCUCHA DOSTAW

Wirus szybko się rozprzestrzeniał na całym świecie, kolejne kraje zaczęły „wyłączać się" w różnym czasie i na różnych etapach. Wstrzymanie lokalnych produkcji powodowało okresowe niedobory produktów. Wiele firm szybko zdało sobie sprawę, że brak zróżnicowania zaopatrzenia był szkodliwy dla ich działalności. W rezultacie dywersyfikacja źródeł zaopatrzenia i niedopuszczenie do uzależnienia się od jednego dostawcy stało się sprawą kluczową na przyszłość. Axis Communications stosuje strategię „podwójnego zaopatrzenia", dzięki czemu ma innych dostawców podstawowych podzespołów, często z różnych krajów, którzy mogą utrzymywać dostawy do centrów produkcyjnych na miejscu. *Utrzymujemy tzw. zapas bezpieczeństwa niezbędnych podzespołów, mamy także umowy z dystrybutorami, by postępowali tak samo. To oznacza, że nigdy nie powinno zabraknąć nam niezbędnych elementów* – podkreślił Per Ädelroth.

Ulrika Magnusson dodała, że firma dostosowała swoją strategię dotyczącą centrów konfiguracji, w których na jednej linii produkcyjnej zwykle powstawała jedna seria produktów. Obecnie wiele centrów jest przystosowanych do uruchamiania takich samych linii produktów. Wdrażając te różne środki, firma ogranicza ryzyko zakłóceń na wypadek specyficznych problemów lokalnych.

- KONIECZNOŚĆ ZRÓWNOWAŻENIA PODAŻY I POPYTU

Firmy nie powinni się skupiać na środkach ochronnych dla pracowników i kwestiach operacyjnych. Już teraz muszą myśleć o zapewnieniu

ZARZĄDZANIE ŁAŃCUCHEM DOSTAW PODCZAS PANDEMII NABIERA CORAZ WIĘKSZEGO ZNACZENIA. DIGITALIZACJA NIE TYLKO USPRAWNI ZARZĄDZANIE, ALE TAKŻE ZMINIMALIZUJE PRZYSZŁE ZAGROŻENIA. POTRZEBA USPRAWNIENIA ZARZĄDZANIA ŁAŃCUCHEM DOSTAW NA WSZYSTKICH PŁASZCZYZNACH NIGDY NIE BYŁA TAK WAŻNA. CYFRYZACJA OZNACZA WYKORZYSTANIE MOŻLIWOŚCI TECHNOLOGICZNYCH, KTÓRE NA TO POZWALAJĄ

sobie możliwie płynnego rozruchu produkcji po pandemii. Przewidywanie wahań popytu konsumenckiego jest jednym z największych wyzwań związanych z zarządzaniem łańcuchem dostaw, a koronawirus jeszcze je utrudnił. Kryzys wywołany pandemią bezlitośnie ujawnił słabości w planowaniu popytu, strategiach zaopatrzenia – takich jak *offshore* vs. *onshore*, *single* vs. *multiple* itd., planowaniu sprzedaży i produkcji oraz organizacji łańcucha dostaw i przejrzystości w wielu firmach.

Specjaliści zwracają również uwagę na fakt, że wraz ze spowolnieniem i zamknięciem gospodarek zmniejszyła się m.in. liczba statków i kontenerów docierających do poszczególnych krajów, co spowodowało spowolnienie podaży towarów i trudności z nadążaniem za popytem. Nic więc dziwnego, że obecnie popyt szybko się zmienia i – jak można przewidzieć – ten trend będzie się utrzymywał. Gdy galerie handlowe i restauracje zamykano, firmy prowadzące sprzedaż detaliczną w tradycyjnych sklepach notowały spadek popytu.

W Internecie sytuacja była odwrotna, w czasie kwarantanny sprzedaż akcesoriów domowych szybko rosła, dlatego tak ważne jest umiejętne równoważenie podaży i popytu poprzez właściwe planowanie (m.in. zaopatrzenia, transportu, produkcji, sprzedaży), z uwzględnieniem organizowania magazynów buforowych dla krytycznych podzespołów produktu końcowego.

Firmy mające gruntownie przemyślane procesy planowania sprzedaży i operacji (S&OP), odpowiednie zapasy bezpieczeństwa w sieci oraz ogólną przejrzystość okazały się w przeważającej mierze bardziej solidne. W przyszłości konieczne będzie zwrócenie większej uwagi na ten aspekt, a to oznacza, że zarządzanie łańcuchem dostaw będzie prawdopodobnie odgrywać jeszcze większą i bardziej strategiczną rolę.

PRZYGOTUJ SIĘ NA CYFRYZACJĘ ZARZĄDZANIA ŁAŃCUCHEM DOSTAW

- DIGITALIZACJA

Odporność (resilience) to modne słowo w zarządzaniu łańcuchem dostaw – ocenił Tom Craig, niezależny konsultant. Głównym elementem tej odporności jest technologia (robotyka, drony, technika bezdotykowa, *blockchain*, sztuczna inteligencja itp.) oraz cyfryzacja. Firmy są obecnie zainteresowane możliwościami, jakie obiecuje cyfryzacja, aby nie tylko lepiej przygotować się na ekstremalne sytuacje w przyszłości, ale także opracować szczegółowe koncepcje ograniczania ryzyka. Eksperci wymieniają kilka cech, jakich zarządzający łańcuchem dostaw oczekują od swoich rozwiązań do zarządzania:

- prognozowanie, planowanie zapasów: prognozowanie, które uwzględnia zarówno trendy historyczne, jak i najnowsze tendencje w obecnym środowisku oraz pozwala odpowiednio na nie reagować;
- przetwarzanie danych sprzedaży w punkcie sprzedaży (POS): możliwość pobierania danych sprzedażowych od sprzedawcy detalicznego/e-commerce nt. sprzedaży przez importerów/dystrybutorów w celu analizy i odpowiedniego skalowania popytu;
- śledzenie dostaw: obliczanie i śledzenie czasów;
- wielkości produkcji: uwzględnianie minimalnych ilości zamówienia (minimalne serie produkcyjne) produktów, minimalnych wartości itp.;
- zamawianie kontenerów: składając nowe zamówienia w fabryce, wypełniamy cały kontener bez marnowania miejsca;
- monitoring produkcji oraz portal dostawcy: możliwość monitorowania zamówienia od momentu wyprodukowania/przesłania do dostawcy/fabryki, aż po dostarczenie towarów do magazynu odbiorcy; portal cyfrowy zapewniający informacje zwrotne i aktualizacje w czasie rzeczywistym.

Menedżerowie łańcucha dostaw oczekują też automatyzacji pomiędzy systemami, które mają tendencję do tworzenia wąskich gardeł (np. systemami CAD, konfiguratorami lub stronami internetowymi), aby szybciej uzyskać precyzyjne rzeczywiste dane dotyczące zamówień i zestawu komponentów dla pozostałej części łańcucha dostaw. Są również zainteresowani funkcjami pozwalającymi wychwycić ruch produktów, wspierającymi kontrolę zapasów (np. kody kreskowe, czujniki IoT).

Posiadanie wyżej wymienionych informacji wspomaga firmy w pokonywaniu wyzwań dzięki możliwościom dokonywania szybkich zmian i adaptacji. Cyfryzacja i automatyzacja zachęci firmy do tworzenia zapasów magazynowych i zapasów bezpieczeństwa.

- SKALOWALNOŚĆ I ELASTYCZNOŚĆ

Skalowalne i elastyczne rozwiązania przynoszą korzyści także menedżerom łańcucha dostaw. Przykładowo rozwiązania w chmurze pozwalają użytkownikom na dostęp do systemów wszędzie tam, gdzie mają połączenie z Internetem, z rozwiązaniami opartymi na przeglądarce internetowej dostępnymi na urządzeniach mobilnych lub podczas pracy zdalnej, co stało się sprawą kluczową w obliczu pandemii COVID-19. Dzięki możliwościom dostosowanym do wymagań biznesowych wyspecjalizowana oferta SaaS może rozwijać się wraz z prowadzoną działalnością, gwarantując, że produkcja nie będzie utrudniona przez rozwiązania mające na celu zwiększenie wydajności oraz ponowne skalowanie zapasów do sezonowych lub sytuacyjnych zmian popytu.

- UPROSZCZENIE ŁAŃCUCHÓW DOSTAW

Pandemia koronawirusa ujawniła istotne słabości w strukturze i organizacji sieci. Globalne źródło dostaw będzie bez wątpienia istniało, ale ze względu na krytyczne znaczenie komponentów, które mają zostać dostarczone, decyzja za lub przeciw konkretnemu łańcuchowi dostaw będzie podejmowana na podstawie wielu przesłanek. W celu uniknięcia zakłóceń odczuwanych w związku z COVID-19 przedsiębiorstwa będą musiały uprościć łańcuchy dostaw, ponieważ z doświadczeń wynika, że im bardziej złożony łańcuch dostaw, tym większe ryzyko jego awarii.

AI I ANALITYKA PREDYKCYJNA USPRAWNIAJĄ ZARZĄDZANIE ŁAŃCUCHEM DOSTAW

Sztuczna inteligencja (AI) ma wiele do zaoferowania menedżerom łańcucha dostaw, ale jej wykorzystanie jeszcze nie jest powszechne. Tylko 12% specjalistów biorących udział w ankiecie przygotowywanej w ramach rocznego raportu branżowego MHI wykorzystuje AI w swoich działaniach, 60% przewiduje jej zastosowanie w ciągu najbliższych pięciu lat. Z kolei z analityki predykcyjnej korzysta 28% respondentów. Nadal istnieje duża luka pomiędzy tymi, którzy korzystają z tych narzędzi, a tymi, którzy ich nie używają.

- INTELIGENTNIEJSZE ZARZĄDZANIE DZIĘKI AI

Zdaniem ekspertów duże korzyści ze stosowania sztucznej inteligencji w łańcuchu dostaw można osiągać wtedy, gdy jest ona oparta na solidnych podstawach uwzględniających zróżnicowany i dynamiczny charakter współczesnych łańcuchów dostaw.

Szeroko pojęta sztuczna inteligencja, a dokładniej uczenie maszynowe, ma ogromny potencjał w proaktywnym zarządzaniu łańcuchem dostaw. Testujemy wiele takich rozwiązań – potwierdził Per Ädelroth z Axis Communications.

Rozwiązania wspierane sztuczną inteligencją pozwalają zredukować koszty transportu oraz skrócić czas poświęcany na dokonywanie analiz i wysyłkę. Podejmowanie decyzji przebiega sprawniej, a dzięki danym otrzymywanym w czasie rzeczywistym przyspiesza się procesy i sprawniej zarządza terminowością dostaw.

Jedną z możliwych przeszkód dla rozwiązań AI jest jednak dostęp do danych. Dla wielu firm dostęp do „dobrego" strumienia danych nie jest łatwy. Aby optymalnie oszacować ryzyko w zarządzaniu łańcuchem dostaw, rozwiązanie AI stawia określone warunki wstępne – jednym z nich jest dostęp w czasie rzeczywistym do danych wewnątrz i na zewnątrz firmy (oraz zgoda na ich wykorzystanie). To właśnie gromadzenie i interpretacja (przetwarzanie) właściwych danych w sieci dostaw jest kluczowym czynnikiem umożliwiającym skuteczne zarządzanie ryzykiem w łańcuchu dostaw.

WYKORZYSTANIE SZTUCZNEJ INTELIGENCJI I ANALITYKI PREDYKCYJNEJ W ZARZĄDZANIU ŁAŃCUCHEM DOSTAW MA WIELE ZALET – OD POMOCY W OPTYMALIZACJI POZIOMU ZAPASÓW PO BARDZIEJ AKTYWNE ZARZĄDZANIE

- PROAKTYWNOŚĆ DZIĘKI ANALITYCE DANYCH I PREDYKCYJNEJ

Zdolność do bycia proaktywnym i wiedza o tym, co ma nastąpić, może uchronić firmy przed katastrofą w ciągłości dostaw. Właśnie dlatego analityka predykcyjna ma tak wiele do zaoferowania menedżerom łańcucha dostaw. Analityka danych i funkcje (oceny) prognostyczne pomagają w rozumieniu trendów oraz znalezieniu sposobu na przetworzenie ogromnej ilości danych, aby wychwycić to, co może być trudne do zauważenia bez zastosowania narzędzi analityki i przewidywania. Mogą również wspierać menedżerów łańcucha dostaw w analizowaniu popytu klientów czy zamówień, przewidywanego popytu, historii sprzedaży i wysyłek, towarów przychodzących i trendów konsumenckich.

Te technologie mogą połączyć wszystkie te dane w proste widoki, obszary wymagające uwagi (np. popyt przekroczy podaż w tygodniu X lub miesiącu Y) lub wskazać, kiedy popyt konsumencki zmienia się (rośnie lub spada), by można było skupić się na elementach czy liniach produktów, które mogą mieć problemy, zanim te się pojawią.

Dla producentów takich jak Axis Communications dane i analiza danych są kluczowym elementem motta firmy „Wiedzieć szybciej, działać szybciej":

Nieustannie szukamy możliwości lepszej przejrzystości zarówno na dole łańcucha dostaw, jak i na poziomie wyższym dla naszych partnerów i dystrybutorów, by wiedzieć, jakie stany magazynowe posiadają. Dane te wykorzystujemy również do modelowania scenariuszy dotyczących potencjalnych zakłóceń i wzrostu popytu, co pomaga w zidentyfikowaniu i wyeliminowaniu potencjalnego wąskiego gardła w dostawach kluczowych podzespołów – podsumowała Ulrika Magnusson.

Narzędzia te mają krytyczne znaczenie szczególnie w okresach zakłóceń. Umożliwiając proaktywność, pomagają firmom skoncentrować uwagę na określonych obszarach, by móc jak najwcześniej przygotować się na ryzyka związane z łańcuchem dostaw i łagodzić skutki potencjalnych zaniedbań.

3) Offshore – przeniesienie wybranych procesów przedsiębiorstwa za granicę.
4) Onshore – przeniesienie wybranych procesów przedsiębiorstwa do firm działających w pobliżu.

5) https://www.mhi.org/publications/report

5G usprawni zarządzanie flotą pojazdów

Nikogo nie trzeba przekonywać, że flota odgrywa kluczową rolę w sprawnym działaniu łańcucha dostaw. Od tego, jak się nią zarządza, w dużym stopniu zależy terminowość dostaw półproduktów i towarów. Menedżerowie są zatem zainteresowani zaawansowanymi rozwiązaniami, które usprawnią śledzenie przesyłek, monitorowanie pracy kierowców i kontrolę stanu floty.

William Pao

a&s International

Obecnie rozwiązania do zarządzania flotą korzystają głównie z technologii sieci komórkowych 3G/4G. Dzięki coraz szerzej dostępnej technologii piątej generacji, oferującej masową łączność, ogromne szybkości i niewielkie opóźnienia, menedżerowie mogą wykonywać swoje zadania efektywniej. Przyjrzyjmy się zarządzaniu flotą w technologii 5G i temu, jakie korzyści może ona przynieść zarówno operatorom, jak i kierowcom.

EFEKTYWNE ZARZĄDZANIE FLOTĄ W 5G

Producenci i usługodawcy muszą korzystać z flot, żeby na czas dostarczać towary do odbiorcy. W skład flot mogą wchodzić różne pojazdy – ciężarówki i autobusy, a nawet statki i samoloty. Do rynków wertykalnych, które w największym stopniu opierają się na flotach do transportu towarów, należą przetwórstwo ropy i gazu, górnictwo, budownictwo, handel detaliczny, usługi komunalne i gospodarka odpadami.

Firmy obsługujące floty borykają się z licznymi problemami i wyzwaniami. Transportowane towary i aktywa są narażone na uszkodzenia i kradzieże, straty mogą być poważne. Innym wyzwaniem są koszty paliwa – wybranie złej trasy często oznacza nadmierne zużycie paliwa. Trudno również w porę reagować, gdy kierowca jedzie nieostrożnie lub zbyt wolno. Menedżerowie flot chętnie więc sięgają po zaawansowane technologie, aby stawić czoła wszystkim wyzwaniom i skuteczniej monitorować pojazdy. Rozwój Internetu Rzeczy umożliwia przesyłanie danych wizyjnych z trasy i danych dotyczących pojazdu do centrum zarządzania, zapewniając tym samym większą świadomość sytuacyjną. Wzrastający popyt na tego typu rozwiązania przyczyni się do ich rozwoju w najbliższym czasie. Według badań analityków z Market Research Future rynek rozwiązań do zarządzania flotą będzie rósł do 2023 r. w tempie 22% rocznie.

ZARZĄDZANIE FLOTĄ POJAZDÓW BAZUJE NA WYMIANIE I ANALIZIE DUŻEJ ILOŚCI INFORMACJI. ABY BYŁO EFEKTYWNE, MENEDŻEROWIE MOGLIBY KORZYSTAĆ ZE WSPARCIA TECHNOLOGII IOT I BIG DATA. SIEĆ ŁĄCZNOŚCI 5G, PRZEZWYCIĘŻAJĄC OGRANICZENIA TECHNOLOGII KOMÓRKOWYCH 4G, POMOŻE TO OSIĄGNĄĆ

Tym, co wyróżnia sieci 5G od powszechnych jeszcze technologii telefonii komórkowej 3G i 4G, jest praca z mniejszymi komórkami i wykorzystanie fal milimetrowych, obsługa dużo większego ruchu komórkowego za pośrednictwem stacji bazowych z wieloma wejściami i wieloma wyjściami (większa przepustowość) oraz uzyskanie pełnego dupleksu, w przeciwieństwie do obecnych stacji bazowych, które w tym samym czasie mogą albo odbierać, albo transmitować sygnały. W rezultacie sieci 5G zapewniają większe prędkości, minimalne opóźnienia i obsługę ogromnej liczby urządzeń. Oznacza to zatem lepszą komunikację, oszczędność energii i kosztów oraz wyższą produktywność.

5G, zasilając ekosystem Internetu Rzeczy, pozwoli usprawnić śledzenie towarów na całej ich drodze w łańcuchu dostaw. Czujniki IoT dostarczają w czasie rzeczywistym informacji o stanie towaru, krytyczne np. dla artykułów wrażliwych na temperaturę, takich jak żywność czy skomplikowana czuła elektronika. Gdy przedmioty są w drodze, bezzwłoczne śledzenie informacji dostarczanych przez urządzenia IoT może np. ułatwić procesy zarządzania przesyłką czy określić liczbę dni potrzebnych na odnalezienie towarów zagubionych – napisano w poście CTIA, amerykańskiego stowarzyszenia branżowego reprezentującego przemysł łączności bezprzewodowej w tym kraju.

Lepszy ogląd sytuacji dzięki stałej łączności z kierowcą, ciężarówką i ładunkiem umożliwia efektywniejsze planowanie i koordynację wysyłek. Ułatwia to pracę i pomaga skrócić czas przestoju kierowców. Operatorzy zarządzający flotą z pewnością skorzystają na dostępie do Internetu szerokopasmowego, łączności z istniejącymi sieciami komunikacyjnymi i wysokim poziomie produktywności. Poprawi się komunikacja pojazd–pojazd oraz pojazd–infrastruktura, co przyniesie oszczędności energii i kosztów, a tym samym wzrost rentowności.

Wykorzystanie sieci 5G znacząco wpłynie na zarządzanie flotą, zwiększając jej wydajność operacyjną i cykl życia. Menedżerom dostarczy danych w czasie rzeczywistym m.in. o zachowaniu kierowców, warunkach i efektywności tras. Te dane można uwzględniać we wskaźnikach wydajności całej organizacji – powiedział Shaurya Singh, analityk branżowy ds. bezpieczeństwa w firmie Frost & Sullivan.

SPOSOBY NA USPRAWNIENIE PRACY MENEDŻERÓW FLOTY

5G ma wiele zalet w zarządzaniu flotą pojazdów. Szybka i masowa łączność bezprzewodowa z Internetem zapewnia transmisję i analizę złożonych danych w czasie rzeczywistym, co pozwala menedżerom monitorować kierowców, sprawdzać stan floty czy planować trasy.

Menedżerowie flot zmagają się z licznymi wyzwaniami i problemami. Kradzieże, zniszczenia ładunków, awarie pojazdów z powodu braku odpowiedniej konserwacji czy wypadki spowodowane nieostrożną jazdą mogą przynieść poważne straty. Zaawansowane rozwiązania do zarządzania flotą stanowią więc realną pomoc w radzeniu sobie z tymi trudnościami.

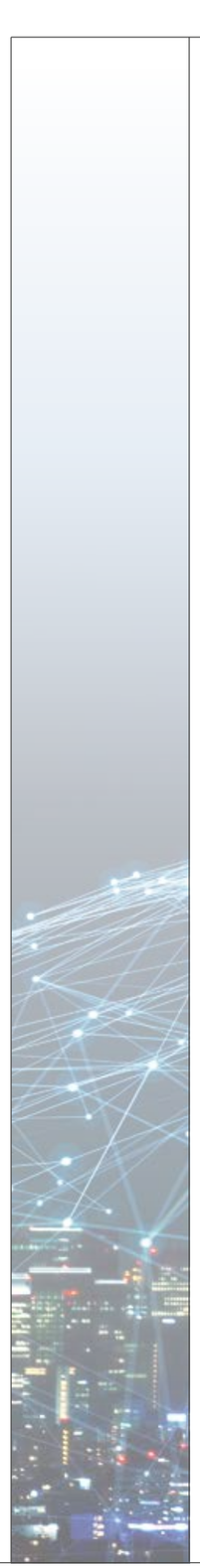
Obecnie rozwiązania do zarządzania flotą wykorzystują głównie technologie komórkowe 3G/4G, które dziś stają się już niewydolne. Ich bariery i ograniczenia może rozwiązać sieć 5. generacji. *Sieci 3G/4G nie dają pełnego oglądu sytuacji, gromadzenie danych jest fragmentaryczne, płytkie analizy nie zwiększają wydajności operacyjnej. Sieć 5G pomoże sprostać tym wyzwaniom dzięki zmniejszeniu opóźnień, co skutkuje zwiększoną reakcją sieci, szybszą transmisją danych w czasie rzeczywistym oraz ulepszoną obsługą czujników i urządzeń IoT* – podkreślił powiedział Shaurya Singh.

Menedżerowie operacyjni za pośrednictwem aplikacji AI *(arttifical intelligence) i* BI *(business intelligence)* będą mogli wykorzystywać i przetwarzać dane w szybszych sieciach i platformach opartych na sztucznej inteligencji. Zastosowanie tych technologii zapewni informacje predykcyjne, a nie mnóstwo danych historycznych. To poprawi wyznaczanie tras i wydajność jazdy oraz załadunku, wraz z przydzielaniem najlepszych pojazdów i kierowców do określonego zadania na podstawie kosztów, konserwacji i niezawodności.

Ogólnie 5G może pomóc menedżerom flot osiągnąć lepszą wydajność na różne sposoby. Są one rozwiązane w następujący sposób.

• MONITOROWANIE STANU POJAZDU I OPŁAT

Nie ma nic bardziej niepożądanego niż posiadanie awaryjnych ciężarówek lub pojazdów, których naprawa może być kosztowna. Monitorowanie stanu pojazdu jest zatem ważnym aspektem zarządzania flotą, które może być wsparte przez sieć 5G gwarantującą duże prędkości i mniejsze opóźnienia. Stosując czujniki i zaawansowane analizy, menedżerowie flot i kierowcy uzyskają informacje nt. stanu urządzeń i terminów obsługi pojazdów, dokładnej lokalizacji poruszających się pojazdów, zużycia paliwa oraz powiadomienia o kolizjach. Ponadto 5G pozwoli skutecznie śledzić i monitorować ładunki, które mogą być przedmiotem kradzieży i uszkodzeń. Zmniejszy to ryzyko zniszczenia ładunku i sprawi, że precyzyjne planowanie tras ciężarówek i koordynacja wysyłek będzie łatwiejsze.



• OSZCZĘDNOŚCI DZIĘKI OPTYMALIZACJI TRASY

Dzięki 5G stała łączność w czasie rzeczywistym między pojazdami a centrum operacyjnym może oznaczać błyskawiczne planowanie optymalnych tras. Sieci 5G poprawią efektywność przejazdu, ostrzegając o korkach i kolizjach, poprowadzą kierowców z ominięciem dróg zatłoczonych lub niebezpiecznych. Pozwoli to skrócić czas podróży i zużyć mniej paliwa.

• MONITOROWANIE KIEROWCY

Menedżerowie flot mogą również stosować 5G do prewencyjnego monitorowania kierowców. Szybka transmisja danych przełoży się na wzrost efektywności operacyjnej. Czujniki i analiza danych dostarczą informacji nt. zachowania kierowców, takich jak niebezpieczna jazda, gwałtowne hamowanie, czas pracy na biegu jałowym, przekroczenie prędkości, niezapięcie pasów bezpieczeństwa czy „senna" jazda. Operatorzy flot, korzystając ze zgromadzonych danych, mogą w tym zakresie szkolić kierowców.

TECHNOLOGIE, KTÓRE DZIĘKI 5G LEPIEJ CHRONIĄ KIEROWCÓW CIĘŻARÓWEK

Kierowcy ciężarówek i innych typów pojazdów są cennym atutem firmy. Zapewnienie im bezpiecznej i wygodnej pracy jest nadrzędne w zarządzaniu flotą. W tym aspekcie 5G może pomóc kierowcom zachować bezpieczeństwo i wydajność na drodze. Nie zawsze jednak wszystko przebiega płynnie. Pokazują to następujące statystyki:

- system raportowania i analiz ofiar śmiertelnych Departamentu Transportu USA podaje, że w 2017 r. we wrakach ciężarówek zginęło 4102 osoby (wzrost o 52% od 2009 r.);
- wg badania przeprowadzonego przez Federalną Administrację Bezpieczeństwa Przewoźnika Samochodowego USA najczęstszymi przyczynami wypadków ciężarówek są uszkodzenia mechaniczne (najczęściej opon), nowe trasy i zmęczenie kierowcy;
- amerykańskie centrum kontroli i zapobiegania chorobom podaje, że 24% kierowców przyznaje się, iż „często" kontynuuje jazdę pomimo zmęczenia, złej pogody lub dużego ruchu, natomiast 47% wyznało, że nadal jeździ w takich warunkach „czasami". Co najmniej jeden wypadek w pracy zawodowej zgłosiło 35% kierowców.

Kierowcy coraz chętniej sięgają po urządzenia IoT i generowane przez nie dane, z których wszystkie mogą posiłkować się 5G. Są technologie, które skutecznie chronią kierowców dzięki zastosowaniu 5G. Oto one:

Telematyka. Coraz częściej ciężarówki są wyposażone w telematykę i czujniki, które kontrolują stan pojazdu i wykrywają nieregularności wzorców jazdy. *Kierowcy będą proaktywnie korzystać z technologii i czujników obsługujących sieci 5G, pomocnych w wyborze trasy, unikaniu kolizji, jeździe zgodnie z ograniczeniami prędkości, a także dostarczających w czasie rzeczywistym informacji o stanie trasy, powiadomień o pracy urządzeń oraz pozwalających kontaktować się ze służbami ratunkowymi w razie wypadku* – wyjaśnił S. Singh z Frost & Sullivan.

V2X. Dzięki 5G można usprawnić pracę czujników w pojeździe i jednostkach pokładowych, które mogą komunikować się z innymi pojazdami i urządzeniami w ramach schematów pojazd–pojazd (V2V) oraz pojazd–wszystko (V2X). Sieci 5G wspomogą kierowców w poruszaniu się w zatłoczonych miejscach, udostępnią wgląd w informacje o korkach, wspomogą jazdę przy słabej widoczności, ulepszą ostrzeżenia przed kolizjami czy o zbyt bliskiej odległości między pojazdami. Dzięki szybszej komunikacji czujników kierowcy zwiększą swoje możliwości unikania kolizji.

Wideo. Kamery dozorowe mogą być oczami ciężarówki. Dzięki 5G transmisja wizji będzie szybsza i płynniejsza. Ze względów bezpieczeństwa systemy kamer coraz częściej stosuje się w kabinie ciężarówki. Sieć 5G umożliwi częstsze oglądanie treści wideo niż tradycyjne nagrania przechowywane w kamerze jako kopia zapasowa. Za pomocą 5G można w czasie rzeczywistym zobaczyć, co robi kierowca, i zweryfikować jego deklaracje.

WYZWANIA

Chociaż sieć 5G ma wiele zalet dla zarządzających flotą pojazdów, nadal różne bariery powodują wahania wśród użytkowników. Dotyczą one infrastruktury 5G, kosztów i cyberbezpieczeństwa.

Obecnie głównym nurtem telefonii komórkowej jest nadal technologia 4G. Chociaż popularność 5G rośnie, jej infrastruktura nie jest jeszcze dojrzała. Jej zasięg będzie różny w zależności od kraju, a także w obszarach miejskich i wiejskich. 5G opiera się na wykorzystaniu wielkich częstotliwości, co sprawia, że jest szczególnie przydatna na obszarach o dużym zagęszczeniu, natomiast nie jest dobrze przystosowana do obszarów wiejskich lub terenów rozległych. To z kolei może wpłynąć na wydajność rozwiązań wykorzystywanych w zarządzaniu flotą przy użyciu 5G. Istnieją ogromne różnice pod względem dojrzałości infrastruktury 5G, nawet w USA czy Kanadzie.

Zasięg sieci 5G szybko rośnie, ale w najlepszym przypadku jest nadal nierówny, zwłaszcza poza centrami miejskimi, co poważnie ogranicza jej praktyczną użyteczność w rozwiązaniach do zarządzania flotą. Wprawdzie korzyści wynikające z małego poboru mocy 5G są fascynujące, jednak słaby zasięg na obszarach wiejskich i oddalonych jest ich główną wadą.

• WĄTPLIWOŚCI ZWIĄZANE Z MIGRACJĄ DO 5G

Migracja do 5G może być ogromnym przedsięwzięciem dla operatorów flot, którzy nadal korzystają z technologii komórkowych 3G i 4G. Będzie musiała wiązać się z opłatami za nowy sprzęt, urządzenia i usługi. *Większość flot wykorzystuje sieci 3G i 4G w urządzeniach komunikacyjnych, elektronicznych urządzeniach rejestrujących i systemach śledzenia, a przejście na 5G zajmie im dużo czasu i będzie wymagało inwestycji. Uaktualnianie starszej technologii w całej flocie to doniosłe zadanie, dlatego menedżerowie flot powinni ściśle współpracować z dostawcami technologii i konsultantami ds. bezpieczeństwa, aby zapewnić płynne i bezpieczne przejście oraz uniknąć przerw w świadczeniu usług* – stwierdził S. Singh. – *Ale prawdziwe pytania brzmią: jaki będzie tego koszt? Czy te usługi są godne uwagi czy niezbędne? Czy pozostaną niszowe, jeśli niewiele flot będzie je subskrybować, ponieważ to dodatkowo zwiększy opłatę za usługę?*

Wyzwaniami dla operatorów flot będą koszty, dostępność sprzętu, bieżąca oczekiwana żywotność sprzętu i zasięg. Rozważania skupią się też na doświadczeniu użytkownika – jak przejść z sieci o niższej szybkości i jak dostosowują się do tego aplikacje. Zgodnie z historycznymi trendami, konsekwencje kosztowe przyjęcia 5G spowodują na początku powolny ich wzrost. Obejmą niezbędny sprzęt do obsługi rozwiązań 5G, a także koszty danych. Wraz z rozwojem i upowszechnieniem koszty spadną do poziomów komercyjnie akceptowalnych przez operatorów.

• BEZPIECZEŃSTWO CYBERNETYCZNE

Kolejnym wyzwaniem dla operatorów flot, którzy będą chcieli wdrożyć 5G, jest cyberbezpieczeństwo. Bez odpowiedniej ochrony urządzenia stosowane w zarządzaniu flotą mogą być narażone na cyberataki lub przejęcie przez wrogie podmioty, które wykorzystają je jako drogę do dalszych ataków, zagrażając flotom i, co gorsza, życiu kierowców.

Ataki takie jak DoS/DDoS, zdalny dostęp czy przejęcie kontroli nad pojazdem w celu przeprowadzenia ataku, awaria infrastruktury 5G spowodowana włamaniem prowadzącym do zatorów w ruchu i atak na bazę danych będą szkodzić flocie i całej sieci transportowej kraju. Operatorzy flot powinni mieć na uwadze cyberbezpieczeństwo. Odegra zasadniczą rolę w utrzymaniu bezpieczeństwa flot i nie będzie przyciągać negatywnej uwagi mediów – powiedział S. Singh. – *Środkami, jakie można zastosować, są ochrona punktów końcowych, wzmacnianie sieci 5G, inwestowanie w technologie cyberbezpieczeństwa, szyfrowanie oprogramowania, a także przestrzeganie najlepszych praktyk.*

WSPOMNIENIE

Na początku grudnia 2020 r. dotarła do mnie ogromnie smutna wiadomość. Oszedł mój „techniczny" przyjaciel, nieoceniony mentor i wzór, a czasem „techniczny przeciwnik", Kazimierz Palutkiewicz, osoba, która współtworzyła zręby automatyki w Polsce, autor genialnej strony internetowej wspierającej wszystkich, którzy „dotykają" automatyki.

To ogromna strata dla Najbliższych, którym niniejszym składam kolejny raz kondolencje, ale również dla mnie osobiście i dla całej branży teletechnicznej. Każdy, kto spotkał Kazimierza na swojej drodze, wie, o czym piszę. Kto Go nie spotkał, niech żałuje. Ja poznałem Kazimierza 4 lata temu i wywarł ogromny wpływ na kształtowanie mojego podejścia do pracy.

Piszę o tym do Czytelników A&S Polska, gdyż Kazimierz był pierwszym recenzentem wszystkich moich publikacji. Jeżeli moje teksty zyskują uznanie, jest to również Jego zasługą. Chciałbym, żebyście o tym wiedzieli. Spoczywaj w spokoju, Przyjacielu. Dziękuję Ci za to, jaki byłeś.

Bezpiecznych lotów!

Terminal pasażerski lotniska sprawia wrażenie obiektu podobnego do innych budynków użyteczności publicznej, takich jak dworce kolejowe czy centra handlowe. Obsługa techniczna, obsługa pasażerów, tłumy odwiedzających i podróżnych, administracja, sklepy, okienka obsługi – na pierwszy rzut oka podobnie. Ale jest podstawowa różnica, która wynika z faktu, że to granica państwa wewnątrz państwa. Ten fakt sprawia, że jest to obiekt wyjątkowy, o wyjątkowych potrzebach, wymagający wyjątkowych rozwiązań zabezpieczających, a popełnione błędy – czy to projektowe, czy uruchomieniowe – mogą być tragiczne w skutkach.

Michał Zalewski

Żeby uświadomić wszystkim wagę problemów projektowo-uruchomieniowych, przytoczę krótką historyjkę. Pasażer nie wszedł na pokład samolotu, ale bagaż na niego zarejestrowany już znalazł się w luku bagażowym. Można powiedzieć: trudno, bagaż poleci, pasażer nie... Okazuje się jednak, że to ogromny problem. Obowiązuje bowiem ścisła kontrola bagażu transportowanego do luku bagażowego i powiązanie go z konkretnym pasażerem. Chodzi nie tylko o to, by pasażer leciał tym samym samolotem co jego bagaż. Jest drugi ważny powód: bezpieczeństwo pozostałych pasażerów. Jeżeli bagaż jest w luku, a pasażera nie ma na pokładzie, samolot nie może polecieć. Dlaczego? Pozostawiam czytelnika chwilowo bez odpowiedzi, chociaż jest ona raczej oczywista.

Teraz już chyba wszyscy rozumiemy, że terminal lotniczy to obiekt niepodobny do innych. Fakt, iż to granica wewnętrzna państwa, obiekt o specyficznym charakterze, rzutuje na zmianę podejścia do projektowania wielu systemów zabezpieczeń.

Na obszarze terminala i całego lotniska operują różne służby odpowiedzialne za różne aspekty bezpieczeństwa: Lotniskowa Straż Pożarna, Służba Ochrony Lotniska, Urząd Celny, Straż Graniczna czy wreszcie policja. Zrozumienie potrzeb tych służb jest kluczowe, by zaprojektowane systemy zabezpieczeń były efektywne. Czasami te potrzeby się dublują, a czasami wręcz wykluczają. Dlatego moim zdaniem projektant systemów już na etapie przygotowania rozwiązań jest zobowiązany rozpoznać te potrzeby i gruntownie je przeanalizować pod kątem oczekiwań poszczególnych służb. Co ważne, projektant systemów zabezpieczeń jest zobligowany do wsparcia głównego projektanta obiektu. Pisałem o tym wielokrotnie.

W przypadku terminala pasażerskiego lotniska ten aspekt jest szczególnie wrażliwy. Bez odpowiedniego wsparcia wielobranżowego projektant obiektu może popełnić błędy, które spowodują gigantyczne konsekwencje. „Nieszczelne" strefy dostępowe, nieodpowiednio dobrana armatura drzwiowa powodująca awarie umożliwiające dostęp osób niepowołanych do zastrzeżonych stref to tylko jedne z wielu wcześniej opisywanych przeze mnie aspektów projektowania systemu kontroli dostępu, które dla lotniska nabierają szczególnej rangi. Odpowiedzialność projektantów, zarówno głównego, jak i projektanta teletechniki, jest tutaj ogromna. Ich współpraca nabiera w takim obiekcie innego znaczenia, powinna wspiąć się na wyżyny precyzji.

Są również uwarunkowania, które sprawiają, że projektowanie staje się trochę łatwiejsze. Wspomniałem, że na lotnisku rezyduje na stałe Lotniskowa Straż Pożarna wyposażona w urządzenia zapewniające błyskawiczną komunikację. To może ułatwić projektowanie systemu oddymiania. Krótki czas przyjazdu pojazdów akcji gaśniczej może posłużyć np. do zmniejszenia wydajności systemu oddymiania, natomiast inaczej niż w innych budynkach należy projektować np. lokalizację przeciwpożarowego wyłącznika prądu.

Z kolei projektant systemów mo-

TO ZADANIE DLA WYKONAWCY TELETECHNIKI, INŻYNIERA URUCHOMIENIOWEGO, ABY CZAS NA URUCHOMIENIA ZAPLANOWAŁ I WYWALCZYŁ W HARMONOGRAMIE

nitoringu wizyjnego musi pamiętać, że różne służby mają odmienne potrzeby dotyczące zakresu rejestrowanego obrazu. Zdarzyło mi się „walczyć" z problemem, gdy celnicy i Straż Graniczna wymagali zupełnie innej lokalizacji dla konkretnej kamery. I tutaj w zasadzie nie ma innego rozwiązania, jak dublowanie kamer monitorujących konkretne obszary obiektu, godzące te „rozbieżne" oczekiwania służb. Pokrycie danego obszaru jedną kamerą, typowe w zwykłych budynkach, dla funkcjonalności na lotnisku może być błędem. Zapis w projekcie: „kamerę ustawić na etapie realizacji zgodnie z życzeniem użytkownika" może być pułapką dla wykonawcy. Podobnie jest z archiwizacją danych oraz możliwością ich przeglądania i analizy.

W dobie cyfrowej telewizji IP współdzielenie strumieni i niezależne rejestratory pozwalają na bardziej elastyczne podejście do tematu. Można de facto zbudować system CCTV, który będzie zapewniał możliwość równoległego, niezależnego archiwizowania danych, jednak podstawą jest identyfikacja potrzeb i, co ważne, musi to być identyfikacja aktywna. Wspominałem na łamach „A&S" wielokrotnie, jak wielkie znaczenie ma aktywna postawa projektanta przy definiowaniu oczekiwać klienta. Na lotnisku nabiera szczególnego znaczenia.

System DSO i jego funkcja wspomagania informacji pasażerskiej to kolejne ważne zadanie dla projektanta. Lotnisko, obsługując wielu pasażerów, musi być wyposażone w interfejs spinający System Informacji Pasażerskiej z DSO. To funkcja niezmiernie istotna. Przypominam historyjkę z zagubionym pasażerem i jego bagażem w samolocie. Niewłaściwe zdefiniowanie stref rozgłaszania w DSO, zarówno automatyczne, jak i z poziomu mikrofonu komercyjnego przy każdym biurku stanowiska Gate, może spowodować błąd w rozgłaszaniu i... gotowe problemy: lot wstrzymany, trzeba rozładować luk bagażowy i odnaleźć bagaż. Błąd konfiguracyjny to mały problem, gorzej, gdy projektant nie weźmie tych potrzeb pod uwagę przy doborze producenta systemu DSO i wystąpią problemy z wydajnością systemu. Komutowanie odpowiednich komunikatów do odpowiednich stref rozgłaszania nie jest zadaniem łatwym, a niewłaściwy dobór urządzeń będzie miał ogromne konsekwencje dla funkcjonowania lotniska.

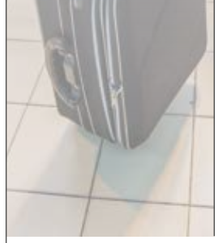
W systemach kontroli dostępu z kolei problemem jest bezpieczeństwo baz danych, zarówno danych dostępowych, jak i identyfikatorów, często biometrycznych, np. linie papilarne. Obwarowania RODO oraz „zwykłe" bezpieczeństwo baz danych to aspekty konieczne do uwzględnienia przez projektanta.

To tylko przykładowe problemy, jakie napotykamy podczas realizacji. Uważam, że terminal pasażerski lotniska międzynarodowego to obiekt najtrudniejszy do zaprojektowania. Nie byłbym oczywiście sobą, gdybym nie poruszył aspektów uruchomieniowych. Tutaj szczególnie ważne jest odpowiednie planowanie uruchomień. Wspomniałem o aspekcie regulacji obrazu z kamer stacjonarnych. Nie można założyć prostej procedury regulacyjnej, gdyż trzeba tego dokonać z uwzględnieniem różnych potrzeb wielu użytkowników. To wymaga czasu.

Podobnie jest z systemem DSO i jego skomplikowaną funkcjonalnością podziału stref rozgłaszania. Uruchomienie i przetestowanie systemu zajmuje tu wielokrotnie więcej czasu niż w budynku z 5–6 strefami. Kontrola dostępu wymaga zebrania wielkiej ilości danych o użytkownikach, konieczna jest weryfikacja poprawności pracy systemu, od której nawet może zależeć życie wielu osób. Wszystko trzeba zaplanować, zadbać, by w harmonogramie realizacji odpowiednio wcześnie zarezerwować czas na sprawdzenie również elementów wykonawczych systemu KD (sztaby, rygle elektryczne, elektrozamki) czy prawidłowości działania drzwi. To zadanie dla wykonawcy teletechniki, inżyniera uruchomieniowego, aby ten czas na uruchomienia zaplanował i wywalczył w harmonogramie.

A dlaczego trzeba zaplanować? Odpowiedź na to pytanie jest taka sama, jak odpowiedź na pytanie dlaczego bagaż nie może lecieć samolotem, gdy jego właściciela nie ma na pokładzie – dlatego że to stwarza zagrożenie związane z atakiem terrorystycznym. Podobnie jak każda dysfunkcja systemów bezpieczeństwa – techniczna czy też operacyjna – otwiera furtkę do ingerencji osób niebezpiecznych.

Z okazji Nowego Roku chciałbym życzyć wszystkim Czytelnikom przede wszystkim zdrowia, a także wielu bezpiecznych lotów w odległe, piękne lub ważne miejsca, do czego mam nadzieję przyczynią się projektanci, wykonawcy i inżynierowie uruchomieniowi systemów lotniskowych.



MICHAŁ ZALEWSKI

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

Skuteczny sposób na parkingowe bolączki

Wiarygodne rozpoznawanie numerów tablic rejestracyjnych (LPR – *license plate recognition)* było dość kosztowne i przydawało się w niewielu sytuacjach. Ogromny postęp technologiczny w dziedzinie kamer IP umożliwia obecnie wykorzystywanie LPR w większej liczbie zastosowań. W zależności od tego, jakie funkcje ma ono spełniać, identyfikacja tablic rejestracyjnych może pomóc zwiększyć wydajność, poziom świadczonych usług oraz bezpieczeństwo.

Automatyczne rozpoznawanie numerów tablic rejestracyjnych znajduje wiele zastosowań, takich jak:

- zarządzanie parkingami (usprawnienie lub automatyzacja płatności, wjazdu i wyjazdu);
- usprawnienie przepływu ruchu przy bramkach na drogach płatnych;
- zarządzanie ruchem na lotniskach (dostęp wyłącznie autoryzowanych pojazdów do pasów ruchu dla taksówek, pojazdów komunikacji publicznej);
- kontrola dostępu (otwieranie bramy wyłącznie autoryzowanym pojazdom i automatyczna rejestracja każdego pojazdu wjeżdżającego na teren obiektu);
- powiadomienia dotyczące pojazdów (automatyczne przekazanie informacji o pojawieniu się pojazdu z listy).

PARKOWANIE W MIEŚCIE

Według danych GUS, w Polsce jest już blisko 25 mln aut osobowych. Choć ta liczba nieustannie rośnie, w wielu miejscach wciąż brakuje odpowiedniej infrastruktury, w szczególności wystarczającej liczby miejsc parkingowych. W jaki zatem sposób ułatwić mieszkańcom żmudny proces poszukiwania przestrzeni do parkowania? Pomocna może okazać się technologia, i to taka, jaką dysponuje już większość polskich miast i miasteczek.
Czy to w dużym mieście, czy np. w kurorcie w środku sezonu turystycznego każdy z nas doskonale poznał problem poszukiwania miejsca parkingowego. Każdego dnia tracimy od kilku do nawet kilkudziesięciu minut na krążenie pomiędzy ulicami, licząc, że jedno z zaparkowanych aut wyjedzie akurat tuż przed nami.

MAŁO MIEJSC = ROSNĄCY PROBLEM

Niestety, zestresowani kierowcy coraz częściej postanawiają parkować w miejscach niedozwolonych. Z informacji udostępnionych przez warszawską Straż Miejską wynika, że stołeczni strażnicy dziennie przyjmują ponad tysiąc zgłoszeń dotyczących nieprawidłowego parkowania. Ulice blokowane przez źle zaparkowane pojazdy mogą okazać się problemem dla służb ratowniczych. Jeśli miasta nie spróbują szybko zaradzić tej sytuacji, kłopoty będą się pogłębiać. Prognozuje się bowiem, że do 2050 roku w miastach na całym świecie będzie mieszkało ponad 6,4 mld osób, a w rezultacie liczba aut wciąż będzie dynamicznie rosła. W Polsce w ubiegłym roku zarejestrowano ich ponad pół miliona.
Nieodpowiednie zarządzanie parkingami ma również negatywny wpływ na środowisko. Samochody poruszające się bardzo wolno po ulicach powodują dodatkowe korki i wypadki drogowe. Włączając do tego także auta dostawcze, których kierowcy pozostawiają uruchomione silniki podczas nielegalnego postoju, mamy rosnącą skalę problemów związanych z zanieczyszczeniem powietrza i poziomem hałasu.
Okazuje się jednak, że korzystne rozwiązania są bliżej, niż nam się wydaje. Wiele miast dysponuje już bowiem infrastrukturą dozoru wizyjnego, którą można wykorzystać w znacznie szerszym zakresie niż dotąd.

PRZEPIS NA PARKINGOWY SUKCES

W prawdziwym *smart city* wiele systemów można połączyć we wspólną sieć, tak aby efektywniej zarządzać tkanką miejską. Tym samym poprawa dostępności miejsc parkingowych niekoniecznie musi wymagać od miast zainwestowania ogromnych sum pieniędzy w zupełnie nową technologię. Można bowiem wykorzystać istniejące systemy dozoru wizyjnego do nowych funkcjonalności, np. rozwiązywania problemów z parkowaniem.
Sieciowe kamery monitoringu – często te, które są już wdrożone w wielu polskich miastach – można dodatkowo wesprzeć specjalnymi aplikacjami analitycznymi, aby móc zarówno alarmować funkcjonariuszy o naruszeniach na parkingach, jak i kierować ruch aut do wolnych miejsc. Wcześniej zdefiniowane strefy dozoru mogą zostać wyposażone w system ostrzeżeń, które będą automatycznie generowane, jeśli nieupoważniony pojazd zatrzyma się w którejś z nich na zbyt długi czas.
– *Takie ostrzeżenia są wysyłane bezpośrednio z kamery do odpowiednich służb, aby mogły one zweryfikować incydent i zareagować w potencjalnie niebezpiecznych sytuacjach. Przykładowo, jeśli auto zastawia drogę dojazdową do szpitala czy dla straży pożarnej, policja lub straż miejska mogą zostać natychmiast poinformowane i szybko interweniować. Kamery nie tylko wykrywają więc naruszenia, ale także pomagają zapobiegać zatorom drogowym i wypadkom* – podkreśla Konrad Badowski z Axis Communications.
Integracja kamer z odpowiednimi narzędziami analitycznymi może także służyć do identyfikacji wolnych miejsc parkingowych, a dodatkowo, po połączeniu z aplikacją nawigacyjną, skutecznie kierować do nich kierowców. Oszczędza to ich czas, zmniejsza korki i wpływa na podniesienie jakości życia zarówno mieszkańców, jak i turystów. Zintegrowane systemy mogą dodatkowo usprawnić czynności operacyjne związane z parkowaniem, np. pobieranie opłat. Kamery z funkcją rozpoznawania numerów tablic rejestracyjnych, połączone z aplikacjami płatniczymi, automatyzują regulowanie opłat parkingowych. Pozwala to również na oszczędność czasu i wpływa na usprawnienie całego procesu płatności, co jest niezwykle istotne np. w garażach wielopoziomowych.
Automatyczne rozpoznawanie tablic rejestracyjnych ma jeszcze jedną zaletę – ułatwia wykrywanie aut, które nie dysponują odpowiednim zezwoleniem na wjazd lub parkowanie w danej strefie. Przy założeniu, że pozwolenia te łączą się z konkretnym autem i jego rejestracją, system mógłby samodzielnie wysyłać informację do służb, tak by mogły szybko interweniować.

ZINTEGROWANE ZARZĄDZANIE

Analiza danych w czasie rzeczywistym i zestawianie ich z danymi historycznymi dają włodarzom miast jeszcze jedną istotną korzyść. Mogą dzięki niej przewidywać godziny szczytu w wybranych obszarach i w związku z tym dobrze się do nich przygotowywać.
Przykładowo, wybrane parkingi mogłyby być otwierane w określonym czasie, a kierowcy informowani o ich dostępności za pomocą szeregu interaktywnych drogowskazów na terenie objętym monitoringiem. W ten sposób rozmieszczenie aut mogłoby być lepiej kontrolowane, a ich użytkownicy nie musieliby kierować się na wybrane parkingi tylko po to, by dowiedzieć się, że nie ma tam wolnych miejsc.
– *Skuteczne zarządzanie parkingami staje się niezbędne w coraz bardziej zatłoczonych miastach. Pomaga zmniejszyć liczbę wypadków drogowych i wykroczeń, prowadzi do zwiększenia bezpieczeństwa mieszkańców, zmniejsza ich stres i poprawia stan środowiska. Wszystkie te czynniki mają wpływ na poprawę jakości życia. Dla miast, które już dysponują znaczną częścią infrastruktury, w postaci monitoringu wizyjnego, to cel w zasięgu ręki* – podsumowuje Konrad Badowski.

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

Kamery Hikvision

w transporcie

Firma Hikvision ma obecnie bardzo mocną pozycję na rynku transportu, a z roku na rok przybywa jej wdrożeń w Polsce i na świecie, co potwierdza wysoką jakość produktów marki.

KAMERY MOBILNE

Mobilne systemy pokładowe oferowane przez Hikvision poszerzają obszar tradycyjnych zastosowań dozoru wizyjny o bezprzewodowe środowiska transportowe. Dostępne są rozwiązania zarówno analogowe, jak i IP oraz szeroka gama wybranych produktów dopasowanych do konkretnych potrzeb. Zaprojektowane z myślą o trudnych warunkach środowiskowych (wibracje, kurz, zmienne temperatury) systemy te charakteryzują się sprawdzoną na rynku wydajnością, a jakość nagrań pozwala na ich wykorzystane jako materiał dowodowy w takich sytuacjach, jak kradzieże kieszonkowe czy wypadki drogowe.
W momencie zgłoszenia incydentu, który wymaga przeprowadzenia dochodzenia, operatorzy systemu mogą uzyskać bezprzewodowy dostęp do materiału filmowego za pośrednictwem sieci komórkowej, bezpośrednio z mobilnych sieciowych rejestratorów wideo, i natychmiast obejrzeć zarejestrowany materiał w centrum monitoringu. Nagrania mogą być również eksportowane do organów ścigania prowadzących dalsze dochodzenie. Hikvision wykracza poza zapisy i dowody, wyposażając swoje produkty mobilne w inteligentne aplikacje, takie jak rozpoznawanie twarzy i liczenie osób, które przetwarzają i analizują potężne ilości danych wizyjnych.

RÓŻNORODNOŚĆ OFERTY

Hikvision ma w ofercie duży wybór modeli kamer dedykowanych do zastosowań transportowych. Wśród nich są modele pokładowe, które doskonale sprawdzają się zarówno wewnątrz pojazdu, monitorując pasażerów, jak i w obserwacji szlaków i sytuacji na zewnątrz. Dostępne są również kamery zewnętrzne, tzw. lusterkowe, instalowane po prawej i lewej stronie kierowcy do obserwacji tego, co dzieje się po obu stronach autobusu lub pociągu. Ponadto dostępny jest odrębny moduł cofania montowany na autobusach.

NIEZAWODNOŚĆ

Kolejnym argumentem przemawiającym za wyborem kamer Hikvision jest ich wysoka niezawodność. Jest to szczególnie ważne we wdrożeniach transportowych. Po pierwsze dlatego, że konieczność serwisowania urządzeń w pojeździe znajdującym się często na drugim końcu kraju jest kosztowne i czasochłonne. Po drugie, by nie utracić zaufania klienta, który chce mieć sprawny tabor.

CERTYFIKATY

Na rynku transportowym bardzo istotne są specjalistyczne certyfikaty stosowanych urządzeń. Kamery Hikvision mają wszystkie wymagane homologacje do zastosowań *automotive*, a na rynku kolejowym certyfikaty na zgodność z normą *PN-EN 50155:2017 Zastosowania kolejowe*. Wyposażenie elektroniczne stosowane w taborze i normą EN 45545 dotyczącą ochrony przeciwpożarowej, co ma gwarantować bezpieczeństwo osób i urządzeń stosowanych w kolejnictwie.

W tym segmencie rynku bardzo istotne jest wsparcie partnerów na wszystkich etapach wdrożenia, od projektu, przez instalację, po obsługę posprzedażową. Dbamy o ciągły rozwój oferowanych produktów, jesteśmy otwarci na współpracę z klientami, aby dostosować parametry kamer do ich określonych wymagań. I właśnie to oraz elastyczność i niezawodność naszych rozwiązań uczyniło nas liderem rynku w sektorze zabezpieczeń w transporcie – mówi Piotr Świder, Business Development Manager w Hikvision Polska.

OPTYMALIZACJA RUCHU DROGOWEGO

Druga grupa produktów bezpośrednio powiązanych z rynkiem transportowym jest odpowiedzią na problemy związane ze wzrostem liczby użytkowanych samochodów, w czego efekcie infrastruktura drogowa staje się coraz bardziej obciążona. Większa liczba pojazdów przyczynia się do powstawania zatorów, frustracji kierowców i opóźnień, co z kolei prowadzi do łamania przepisów ruchu drogowego, a nawet podnosi wskaźniki wypadków. Wszystko to stanowi złożone wyzwanie dla służb, które muszą zaprowadzić porządek w tym chaosie, m.in. planistów miejskich, zespołów monitorujących drogi i służb ratowniczych. Potrzebne są rozwiązania, które podnoszą świadomość, eliminują złożoność i zmniejszają nakład pracy.
Kluczowe cele pozostają te same – utrzymanie bezpiecznego odpowiedzialnego ruchu na drodze, optymalizacja wykorzystania dostępnych zasobów transportowych i jak najszybsze reagowanie na zdarzenia drogowe.
Inteligentny system ruchu drogowego firmy Hikvision pozwala usunąć wąskie gardła – które od dawna stanowią problem dla użytkowników dróg i władz samorządowych w ich dążeniu do utrzymania płynności ruchu – i pomóc ludziom w dotarciu do celu w bardziej inteligentny i płynny sposób.

AUTOMATYCZNE WYKRYWANIE ZDARZEŃ DROGOWYCH

Hikvision oferuje kompleksowe profesjonalne rozwiązanie do automatycznego wykrywania incydentów w takich krytycznych obszarach, jak autostrady, tunele i mosty, bazujące na inteligentnym przetwarzaniu materiału wizyjnego. Może szybko zaalarmować operatorów o incydentach, niezwłocznie wysyłając powiadomienia o zdarzeniach do platformy programowej Hikvision i systemów firm trzecich, jednocześnie automatycznie archiwizując klipy wideo ze zdarzeń. Oznacza to, że rozwiązanie to może przyczynić się do zmniejszenia liczby wypadków.

OPTYMALIZACJA PRZEPŁYWU RUCHU

Inteligentne sterowanie sygnalizacją świetlną jest pomocne zarówno w zapobieganiu niepotrzebnemu spowalnianiu ruchu, jak i rozładowywaniu zatorów. Gdy na skrzyżowaniu tworzy się zator, kamery drogowe zliczają pojazdy przejeżdżające przez skrzyżowanie i oszacowują długość kolejek pojazdów w czasie rzeczywistym. Dzięki tym danym system może dostosować czas trwania zielonego i czerwonego światła, przywracając płynność ruchu we wszystkich kierunkach.
Systemy Traffic Flow zbierają informacje o natężeniu ruchu drogowego na najważniejszych skrzyżowaniach i autostradach i na tej podstawie dostarczają statystyki dotyczące przepływu ruchu, odstępów czasowych i przestrzennych, typów pojazdów i długości kolejek.

ANALIZA RUCHU DROGOWEGO

Centrum zarządzania ruchem jest miejscem, w którym gromadzone są wszystkie dane. Na ich podstawie zespoły zarządzające ruchem monitorują zdarzenia w czasie rzeczywistym. Inteligentna natura rozwiązania oznacza, że mogą być rozpoznawane takie cechy dotyczące pojazdu, jak tablica rejestracyjna, marka, model, kolor i rodzaj. Synchronizacja wszystkich danych oznacza maksymalne wykorzystanie ich potencjału w realizacji scenariuszy ruchu drogowego, dzięki czemu pojazdy mogą poruszać się sprawniej i bezpieczniej.
Urządzenia, oprogramowanie i integracja systemów Hikvision pozwalają podejmować istotne decyzje. Wiedza, działanie i bezpieczeństwo są na wyciągnięcie ręki.

WYKRYWANIE NARUSZEŃ PRZEPISÓW RUCHU DROGOWEGO

Ogromny ruch uliczny jest często uznawany za jeden z największych problemów współczesności. Jest powodem stresu, opóźnień, kolizji i wypadków. Z powodu utrudnień kierowcy często lekceważą przepisy drogowe, co pogłębia ogólne problemy.
Oferowane obecnie produkty Hikvision umożliwiają wykrywanie wszelkich naruszeń drogowych. Za każdym razem, gdy pojazd przejeżdża przez punkt kontrolny, kamera rejestruje jego obraz i charakterystyczne cechy. Dzięki temu można w porę podjąć niezbędne środki ostrożności. Sprawdzone w praktyce rozwiązanie Hikvision Intelligent Traffic Solution zapewni wszystkim użytkownikom dróg bezpieczniejszą, spokojną podróż.

OBSERWUJ NAS NA:
LinkedIn @Hikvision Poland
Facebook @HikvisionPoland
Webiste www.hikvision.com/pl/
Napisz do nas info.pl@hikvision.com

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

Rozwiązywanie problemów

z kontrolą dostępu w obiektach obsługi transportu publicznego

Porty lotnicze i morskie, dworce kolejowe lub autobusowe nie tylko przyciągają dużą liczbę pasażerów, lecz często stanowią też podstawę infrastruktury i gospodarki danego kraju. Ze względu na specyfikę, wymagają zapewnienia odpowiednich standardów bezpieczeństwa także zlokalizowanym tam firmom związanym z obsługą transportu publicznego. Ważną rolę spełniają w tym systemy kontroli dostępu.

Wyzwaniem dla systemu KD w obiektach firm działających w sektorze transportu publicznego jest nie tylko konieczność zapewnienia wymaganego poziomu bezpieczeństwa. Ponieważ korzysta z nich duża liczba pracowników i klientów, systemy KD muszą być łatwe w obsłudze, wydajne i zdolne do działania na dużą skalę. Często konieczne jest scentralizowanie wielu lokalizacji w celu jednolitego centralnego monitorowania i zarządzania nimi, przy jednoczesnym dostosowaniu do zmieniających się zagrożeń i potrzeb.

KONTROLA DOSTĘPU NA DZIŚ I NA PRZYSZŁOŚĆ

Z powodu pandemii koronawirusa firmy muszą podejmować odpowiednie kroki zapobiegające rozprzestrzenianiu się zakażenia, świadcząc jednocześnie swoje usługi. Z pomocą mogą przyjść systemy KD, które uniemożliwią wejście zbyt dużej liczbie osób do tego samego obszaru w tym samym czasie. Integruje się też je z kamerami termowizyjnymi, a dostęp jest przyznawany wyłącznie osobom, których temperatura ciała mieści się w dozwolonym zakresie.

POKONYWANIE OGRANICZEŃ FINANSOWYCH

Kolejnym wyzwaniem jest skromny budżet organizacji samorządowych, którym transport publiczny podlega. W efekcie istniejące systemy są często przestarzałe, nieefektywne i nie gwarantują odpowiedniego stopnia zabezpieczenia. Ale inwestowanie w nowe rozwiązania to proces mozolny. System KD firmy Nedap – AEOS – został wdrożony w wielu różnych obiektach z sektora transportu publicznego na całym świecie. Zintegrowany z systemami innych dostawców, realizuje szeroki zakres funkcji – od sterowania bramami i szlabanami, po wyrywkowe kontrole, przepływy pracy wykonawców, weryfikację biometryczną czy zarządzanie szafkami.

ZNACZNIE WIĘKSZY POZIOM BEZPIECZEŃSTWA

AEOS spełnia wysokie standardy bezpieczeństwa wymagane w transporcie publicznym, w tym RODO. Dzięki takim funkcjom, jak definiowanie poziomów bezpieczeństwa, silnik reguł i kontrola dostępu oparta na rolach, system AEOS umożliwia dostosowanie zabezpieczeń do konkretnych potrzeb. Umożliwia również wstępne zdefiniowanie ustawień w różnych sytuacjach awaryjnych i ich natychmiastowe wdrożenie.

Obecnie firmy dostarczające infrastrukturę techniczną muszą stawiać czoła coraz większej liczbie cyberzagrożeń, które mogą obejmować również systemy kontroli dostępu. Kompleksowy system bezpieczeństwa AEOS łączy w sobie informatyczne zasady szyfrowania z silnym poziomem uwierzytelniania, aby zapewnić skuteczną ochronę przed zagrożeniami fizycznymi i cybernetycznymi. Umożliwia również bezpieczną aktualizację kluczy kart bez konieczności fizycznego dostępu do każdego z czytników.

OSZCZĘDNOŚĆ CZASU I PIENIĘDZY

Funkcje takie, jak zaawansowane raportowanie, integracja zarządzania przepływem pracy i ich ustawienia jednym kliknięciem sprawiają, że system jest łatwy w obsłudze, a użytkownicy mogą skupić się na innych zadaniach.

CENTRALNE ZARZĄDZANIE

Kolejnym sposobem, w jaki AEOS poprawia wydajność, jest ujednolicenie systemów w wielu lokalizacjach i możliwość ich centralnego monitorowania i zarządzania nimi. Ma to kluczowe znaczenie, ponieważ organizacje działające w sektorze transportu publicznego często mają siedziby rozproszone lub rozległe lokalizacje obejmujące duży obszar. Oznacza to również, że wszelkie nieprawidłowości techniczne urządzeń zainstalowanych przy drzwiach mogą być zdalnie wykrywane i często zdalnie usuwane.

DOSTOSOWANIE DO ZMIENIAJĄCYCH SIĘ WYMAGAŃ

Ochraniając duże zakłady lub grupy osób, istotne jest, aby szybko dostosować system KD do konkretnych wymagań danej lokalizacji – zarówno teraz, jak i w przyszłości. System AEOS, którego oprogramowanie jest oparte na otwartej architekturze, umożliwia łatwą rozbudowę i dostosowanie systemu do zmieniających się potrzeb użytkownika. AEOS można zintegrować z urządzeniami różnych producentów, w tym z bezprzewodowymi zamkami online i offline oraz systemami biometrycznymi. Liczne konfiguracje pozwalają z łatwością zrealizować złożone scenariusze bezpieczeństwa, takie jak śluzy z dwoma lub większą liczbą drzwi. Można również stosować różne identyfikatory i uwierzytelniania, od zwykłych kart i kodów PIN, po kody QR i biometrię twarzy. Dzięki AEOS można nadal korzystać z zainstalowanego sprzętu i z łatwością integrować systemy innych dostawców. Dla niektórych organizacji sektora transportu publicznego kluczową rolę odgrywa m.in. możliwość połączenia na jednej platformie systemu KD z systemem sygnalizacji włamania i napadu.

WYBRANE REALIZACJE

AEOS dba o wysoki poziom bezpieczeństwa w **porcie lotniczym Schiphol,** który jest jednym z najbardziej ruchliwych lotnisk w Europie. System zapewnia łatwe zarządzanie

węzłem komunikacyjnym wielu innych zintegrowanych z nim aplikacji, od identyfikacji biometrycznej personelu wchodzącego na płytę postojową, po gromadzenie cennych danych wykorzystywanych w takich aplikacjach, jak obsługa alarmów i monitoring.

Dzięki systemowi AEOS **firma Lufthansa Technik** wdrożyła wysokie standardy bezpieczeństwa, utrzymując jednocześnie poczucie swobody przemieszczania się swoich pracowników i osób odwiedzających firmę. System zainstalowano pilotażowo w zakładzie w Hamburgu, gdzie zatrudnionych jest 10 tys. pracowników, a następnie wdrożono go w czterech kolejnych oddziałach. AEOS zintegrował systemy innych firm oraz umożliwił dodanie takich funkcji, jak zarządzanie szafkami na klucze oraz gośćmi.

W **porcie lotniczym Weeze** w Niemczech wdrożono system AEOS w celu aktualizacji i wzmocnienia środków bezpieczeństwa. Głównym celem było zwiększenie bezpieczeństwa przy przejściu, którym pasażerowie opuszczają strefę odprawy celnej, i uniemożliwienie osobom czekającym na zewnątrz wejście do obszaru chronionego. W tym celu zainstalowano radar nad drzwiami przesuwnymi i zintegrowano go z systemem AEOS, aby alarm się uruchamiał w momencie, gdy jakaś osoba porusza się w niedozwolonym kierunku.

Firma DHL zdecydowała się na system AEOS w celu centralizacji i poprawy poziomu bezpieczeństwa, przy jednoczesnym zapewnieniu większej wygody dostępu dla osób i pojazdów na lotniskach Jeddah i Riyadh. Po przetestowaniu systemu kontroli dostępu i SSWiN AEOS firma DHL wdrożyła go w 60 lokalizacjach w Wielkiej Brytanii i zintegrowała z systemem do zarządzania materiałem wizyjnym Milestone.

W największym **porcie morskim w Antwerpii** (Belgia) do zarządzania kompleksem 47 budynków zastosowano system AEOS, który z biegiem czasu rozszerzono i zintegrowano z innymi systemami. Zwiększono jeszcze bardziej wydajność m.in. poprzez integrację systemu przepływu pracy z AEOS w celu zarządzania dostępem dla wykonawców.

System AEOS chroni liczne **zakłady firmy ProRail,** która obsługuje holenderską krajową infrastrukturę kolejową. Firma potrzebowała systemu umożliwiającego wykonawcom i podwykonawcom potwierdzenie ich kwalifikacji do wykonywania prac na torach. W rezultacie wdrożono cyfrowy paszport bezpieczeństwa składający się z trzech elementów: portalu połączonego z AEOS, przepustki fizycznej i aplikacji ScanApp. Nowy system przyczynił się do poprawy poziomów bezpieczeństwa na torach.

Monitoruj i usprawniaj

swoje procesy w łańcuchu dostaw

Jeżeli istnieje sposób, by zrobić coś lepiej, znajdź go.
Thomas Edison

Monika Kołodziejczyk

Systemy monitoringu wizyjnego i kontroli dostępu kojarzą się przede wszystkim z poprawą bezpieczeństwa w obiekcie. Stają się również ważnym elementem automatyzacji i kontroli produkcji oraz procesów w logistyce magazynowej. Chęć optymalizacji procesów, zwiększenia kontroli nad przepływem towarów i osób, dążenie do ograniczenia do minimum liczby reklamacji i wyeliminowania źródeł błędów w łańcuchu dostaw oraz wysokie koszty pracy ludzi są przejawem coraz wyraźniejszej tendencji do odchodzenia od pracy wykonywanej przez personel i potrzeby automatyzacji tych procesów.

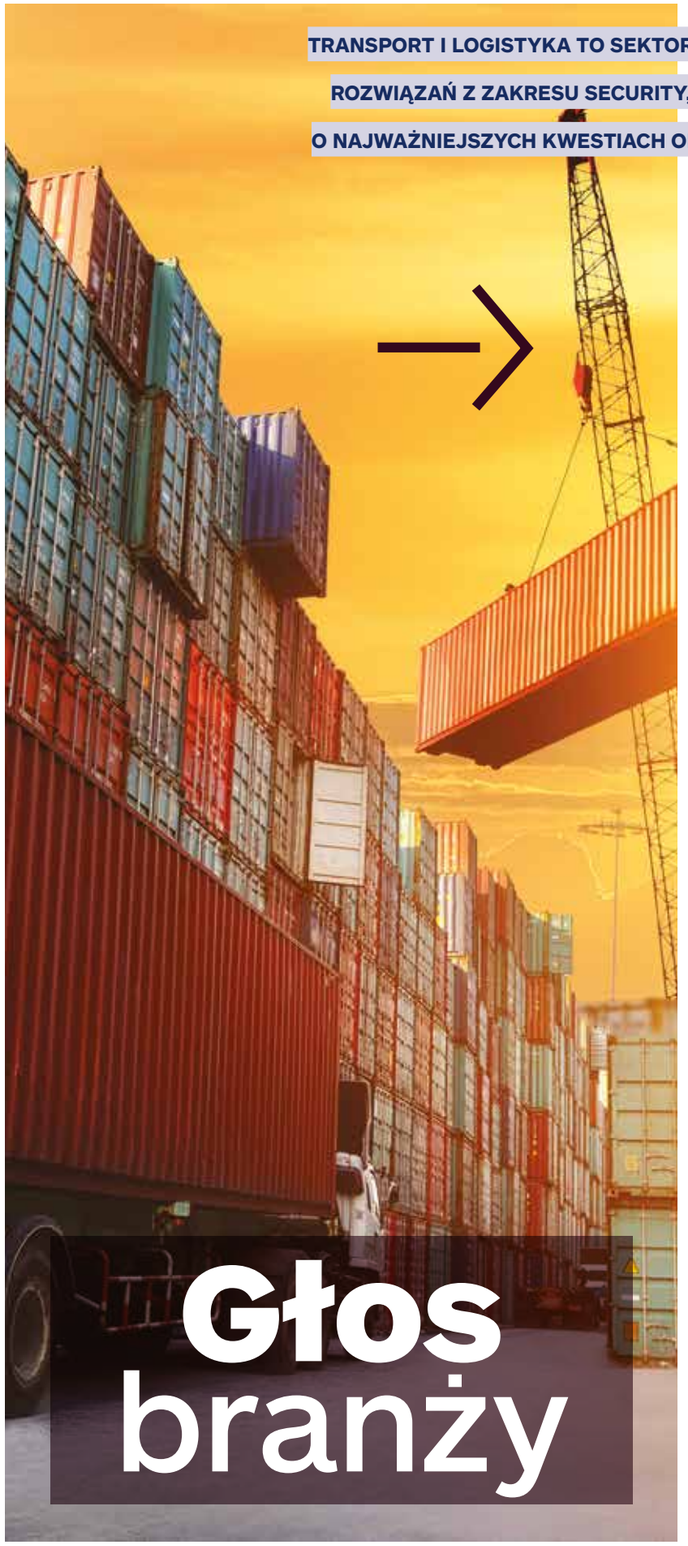
OBNIŻ KOSZTY I PODNIEŚ ZYSKI DZIĘKI INTEGRACJI

Rozwiązania proponowane przez C-AIM można zaliczyć do nowej kategorii *machine vision*. Istniejące technologie integruje się na nowe sposoby i stosuje do rozwiązywania rzeczywistych problemów. W tym przypadku łączymy obrazy z informacjami z wewnętrznych systemów magazynowych, takich jak WMS *(Warehouse Management System)*, skanery kodów kreskowych, RFID, wagi itd.
Każde skanowanie lub inne działanie w procesie to zdarzenie, które zostaje powiązane z obrazami z kamer i dokumentowane w bazie danych. Pozwala to na pełne monitorowanie procesów w łańcuchu dostaw, a także na szybkie wyszukiwanie nagrań nie tylko wg czasu, ale także po dowolnym określonym przez klienta znaczniku. Może nim być numer EAN produktu, numer faktury czy zamówienia itd. W łatwy sposób uzyskujemy dowód, że towary zostały dostarczone w komplecie i bez uszkodzeń lub że było inaczej. To szersze i indywidualne spojrzenie na wykorzystanie systemów zabezpieczeń do zaspokojenia potrzeb klienta w tym obszarze.
Rozwiązania można zastosować na różnych etapach procesów magazynowych: począwszy od wjazdów i wyjazdów, gdzie wykorzystujemy integrację z systemem kontroli dostępu i kamerami ANPR, poprzez procesy kompletacyjne, skończywszy na foliowaniu palet. Dzięki modułowości i elastyczności klient może wybrać obszar, w którym widzi potencjał do zastosowania rozwiązania. Później rozbudowa jest możliwa w dowolnym momencie.

KOMPLETACJA W OKU KAMERY

Kompletacja towarów jest uważana za podstawowe, ale i najbardziej pracochłonne oraz najdroższe działanie w logistyce wewnętrznej. Nie dziwi więc, że większość klientów zaczyna od wykorzystania rozwiązań C-AIM w tym obszarze. W zakresie obsługi towarów przychodzących, w procesie kompletowania i pakowania towarów wychodzących klient otrzymuje najszybciej wymierne korzyści. Rozwiązania znajdują zastosowanie w procesach wykonywanych zarówno ręcznie, jak i automatycznie.
C-AIM.forklifts to propozycja dla klientów, którzy chcą ograniczać miejsce kompletacyjne i optymalizować proces dzięki kompletacji na wózkach. Koncepcja systemu monitorowana procesów logistycznych dedykowanych dla wózków kompletacyjnych opiera się na zainstalowaniu kamer wizyjnych w wykonaniu mobilnym o zwiększonej odporności na wstrząsy i uszkodzenia wraz z systemem zasilania i system komunikacji Wi-Fi.
Końcowym etapem jest foliowanie palet, na którego monitorowanie decyduje się wielu klientów. Proponujemy tu integrację obrazu, systemów zarządzania magazynem i automatyki foliowania.
Przykłady zastosowania można by mnożyć. Efektem końcowym jest kompletny materiał z całego przepływu towaru, a to niepodważalny dowód poprawności przebiegu procesu lub wskazujący jego błędy. Nagranie może być dowodem w przypadku reklamacji czy narzędziem w trakcie inwentaryzacji lub służyć do optymalizacji procesów.
W procesach rejestrowania obrazu należy chronić prywatność pracowników, zasłaniając wizerunek osób za pomocą maskowania lub pikselizacji obrazu danej osoby.

C-AIM
ul. Przejazdowa 2B,
02-496 Warszawa
https://c-aim.pl/
monika.kolodziejczyk@c-aim.pl



Głos branży

TRANSPORT I LOGISTYKA TO SEKTORY WYMAGAJĄCE SZCZEGÓLNYCH ROZWIĄZAŃ Z ZAKRESU SECURITY, ZWŁASZCZA W DOBIE PANDEMII. O NAJWAŻNIEJSZYCH KWESTIACH OPOWIEDZIELI NAM UŻYTKOWNICY SYSTEMÓW I ICH OFERENCI.

Karol Dominiczak

Axis Communications

Smart transport na miarę 2021 r.

Jak wynika z badania Transportowe zwyczaje Polaków, aż 89 proc. z nas korzysta z komunikacji publicznej, a mimo to co dziewiąty ma auto lub planuje jego zakup. Wskazuje to, jak wielka jest skala wyzwań związanych z transportem, przede wszystkim w szybko rozrastających się miastach. Aglomeracje borykają się z wieloma utrudnieniami drogowymi: zmiana infrastruktury, budowa, remonty i rosnąca liczba pojazdów powodują opóźnienia w ruchu i zwiększają kolizyjność. Sprawiają także, że transport jest nieekonomiczny. Naprzeciw tym wyzwaniom wychodzą inteligentne systemy monitoringu wizyjnego.

Kamery sieciowe z oprogramowaniem, używane jako inteligentne czujniki, które zbierają dane o ruchu w czasie rzeczywistym, mogą pokazywać służbom, a dalej także pieszym, pasażerom i kierowcom miejsca, gdzie przepustowość jest najwyższa. Systemy monitoringu wizyjnego rozładowują w ten sposób przeciążone arterie. Nie tylko zliczają pojazdy, ale także zauważają wypadki i zatory, które wpływają na płynność ruchu drogowego.

Obserwacja w czasie rzeczywistym oraz automatyczne powiadomienia o zdarzeniach wysyłane do centrali przez inteligentny system monitoringu są cenną pomocą dla służb w szybkiej ocenie sytuacji na drodze. Technologie wizyjne, dzięki analityce, pomagają w optymalizacji cyklu świateł na skrzyżowaniach i samodzielnie alarmują służby mundurowe. Pomocnym rozwiązaniem jest identyfikacja numerów tablic rejestracyjnych pojazdów, również będących w ruchu, nawet przy prędkości znacznie przekraczających 100 km/h. W efekcie przyczynia się to do zmniejszenia liczby wypadków, kolizji czy przypadków łamania przepisów oraz poprawia płynność ruchu.

W skali makro systemy monitoringu mogą w czasie rzeczywistym analizować obraz z kamer pod kątem zrozumienia zachowania wszystkich uczestników ruchu, kanałów przepustowości, godzin i miejsc szczytów komunikacyjnych. Pozwala to na precyzyjne dopasowanie liczby autobusów czy wielkości składów pociągów do bieżących potrzeb i tworzenie szczegółowych planów urbanistycznych, włącznie z parkingami. Inteligentny system zauważy wolne miejsca parkingowe i poinformuje o nich uczestników ruchu, co zapewnia zarówno oszczędność czasu, jak i realnych kosztów związanych m.in. z przejazdami pustych autobusów czy zakupem paliwa.

Wykorzystanie technologii monitoringu wizyjnego w transporcie jest ograniczone wyłącznie ludzką wyobraźnią. Kamery wyposażone we własne procesory i aplikacje nie są już tylko prostymi urządzeniami, ale rozwiązaniami na problemy transportowe współczesnych miast. Połączone w sieci pozwolą budować logistykę transportu na miarę miast przyszłości – gotowych na kolejną dekadę XXI wieku.

Wojciech Andziak

DHL Parcel

Konieczna jest automatyzacja zadań ochrony

W dobie pandemii szczególną uwagę należy zwracać na zapewnienie bezpieczeństwa sanitarnego pracownikom i kierowcom. To obszar, który trzeba na bieżąco monitorować, ponieważ od tego zależy ich praca, a tym samym zdolność operacyjna firmy. Innym aspektem jest egzekwowanie nowych standardów i rozwiązań, które nie zawsze są przyjmowane ze zrozumieniem. To kwestia budowania świadomości i odpowiedzialności za bezpieczeństwo nie tylko swoje, ale także innych.

Aby podnieść poziom bezpieczeństwa pracowników i zapewnić ciągłość dostaw towarów, pracujemy nad automatyzacją zadań ochrony. Tam, gdzie jest to możliwe, automatyzujemy procesy dotychczas obsługiwane przez pracowników ochrony fizycznej. Pozwala to obniżyć koszty i ograniczyć kontakty osobiste, które mogą powodować zagrożenie epidemiczne w dobie pandemii.

Ważne jest, aby nie podejmować pochopnie decyzji, każda musi być przedyskutowana w zespołach i dogłębnie przemyślana. Należy wybrać rozwiązanie, które nie obniży poziomu bezpieczeństwa, ale wręcz ten poziom podniesie. Tutaj najważniejsze są dobry plan i rozpoznanie możliwości, jakie oferuje branża zabezpieczeń technicznych.

Adam Sawicki

DSV International Shared Services

Zmiany w procesach wymuszone pandemią

W dobie pandemii szczególną uwagę należy zwracać na bezpieczeństwo ludzi i przestrzeganie zasad epidemicznych podczas ich bezpośredniego kontaktu. Coś, co wcześniej wydawało się bezpieczne, dzisiaj niekoniecznie już takie jest... Wiele z wprowadzonych obostrzeń sanitarnych w sposób pośredni lub bezpośredni wymusiło zmiany w procesach logistycznych, a w efekcie wydłużyło czas ich realizacji. Często kosztem bezpieczeństwa, które w branży sektora TSL jest jednym z najwyższych priorytetów.

W naszej firmie zmieniliśmy procedury dotyczące kierowców podczas załadunku i rozładunku - ograniczyliśmy kontakt z nimi tylko do przekazania dokumentów. W zdecydowanej większości punktów kontrolnych wprowadziliśmy pomiary temperatury z wykorzystaniem systemu kamer termowizyjnych z black body, które charakteryzują się najlepszą dokładnością pomiaru. Ograniczyliśmy wizyty gości do niezbędnego minimum.

W obszarach magazynowych rozdzieliliśmy czas zmiany załogi – wprowadziliśmy minimum 15-minutową przerwę pomiędzy zmianą kończącą pracę a rozpoczynającą. Doskonale sprawdziła się tutaj funkcja anti passback systemu kontroli dostępu.

W częściach biurowych przygotowaliśmy i wdrożyliśmy systematyczne dezynfekcję (zamgławianie) dróg komunikacyjnych i stref socjalnych. Poza tym, aby maksymalnie ograniczyć kontakty pomiędzy załogą magazynu a działem administracji magazynowej, wdrożyliśmy również system poczty pneumatycznej dla dystrybucji dokumentów. Skonfigurowaliśmy system kontroli dostępu w taki sposób, aby każda zmiana miała wydzieloną część socjalną, oraz wytypowaliśmy drogi przejścia pomiędzy magazynem a częścią socjalną tak, by się nie krzyżowały.

Ponadto wprowadziliśmy aktywne monitorowanie pojazdów za pomocą plomb elektronicznych z nadajnikami GPS, wdrożyliśmy systemy spinające dane z innych aplikacji, by mieć informacje, czy (i ewentualnie kiedy) kierowca miał bliski kontakt z osobą zakażoną. Dla każdego magazynu mamy przygotowany plan na wypadek pojawienia się ogniska COVID-19. Przeszkolono dodatkową grupę pracowników spoza danego oddziału, która na wypadek wprowadzenia kwarantanny przejęłaby obowiązki zawieszonych pracowników. W ten sposób zachowujemy ciągłość operacyjną.

Tomasz Siwicki

GEFCO

Priorytetem jest bezpieczeństwo

Najważniejszym aspektem bezpieczeństwa w dobie pandemii jest zapewnienie pracownikom bezpiecznych warunków pracy. Dotyczy to szczególnie

tej grupy osób, która ze względu na charakter wykonywanych zadań nie może przejść na system pracy zdalnej, dlatego kluczowym aspektem jest stworzenie i egzekwowanie procedur bezpieczeństwa oraz zapewnienie pracownikom niezbędnych środków ochrony indywidualnej.
Wychodząc z założenia, że nawet najlepsze procedury nie zadziałają, jeżeli pracownik nie będzie się do nich stosował, należy więcej uwagi poświęcić na komunikację z załogą. Każda osoba musi wiedzieć, dlaczego wprowadzane są różnego rodzaju środki bezpieczeństwa, oraz działać w przeświadczeniu, że wszystkie zmiany procedur mają na celu ochronę zdrowia i dobro pracownika.
GEFCO należy do tej grupy firm, dla których bezpieczeństwo jest priorytetem, a nasze systemy zabezpieczeń technicznych są wystarczające, aby zapewnić odpowiedni poziom ochrony pracowników oraz ciągłość łańcucha dostaw. Pandemia wyraźnie przyspieszyła rozwój systemów zabezpieczeń technicznych, które dotychczas były mało popularne lub po prostu zbyt drogie.
Dobrym przykładem są kamery i urządzenia do monitorowania temperatury ciała. Nowoczesne systemy CCTV potrafią nawet zweryfikować, czy osoba wchodząca na teren zakładu ma nałożoną maseczkę ochroną. Taki system, w połączeniu z kontrolą dostępu, umożliwia zablokowanie wejścia osobom potencjalnie chorym, których obecność mogłaby skutkować wstrzymaniem pracy na wiele godzin, np. w celu dezynfekcji pomieszczeń.
Z uwagą śledzę zmiany na rynku i jestem ciekaw nowych rozwiązań z zakresu zabezpieczeń technicznych, które pojawią się w 2021 roku. Liczę, że ich dostawcy zaskoczą nas nowościami, które będą poprawiać bezpieczeństwo w transporcie i logistyce.

Piotr Świder

Hikvision Poland

Konieczne inwestycje w technologie przyszłości

Dynamiczny rozwój rynku transportu i logistyki w ostatnich latach zmienił podejście również do systemów monitoringu wizyjnego – od czasów, kiedy kamery w środkach transportu publicznego (komunikacja miejska czy kolej) były rzadkością, do dzisiejszej rzeczywistości, kiedy stało się to normą, a wręcz wymogiem.
Na rozwój tej gałęzi rynku wpłynął nie tylko fakt, że kamery stały się podstawowym wyposażeniem pojazdów. Dużą rolę odegrały obowiązujące ściśle określone prawem normy i wymagania względem systemów monitoringu wizyjnego montowanych w pojazdach. Hikvision, jako lider branży, planuje certyfikację swoich urządzeń już na etapie ich projektowania, aby spełnić wszystkie wymogi, np. normy EN50155:2017.

Rok 2020 był szczególny i wymagał od rynku transportu dostosowania się do sytuacji wywołanej przez pandemię. Transport publiczny to rynek, który niestety bardzo ucierpiał w obecnych realiach. Znacząco zostały ograniczone ruch lotniczy i turystyka. Firmy działające w branży musiały szukać oszczędności w sytuacji spadku obrotów. Niemniej systemy wizyjne – jako element bezpieczeństwa – cieszyły się ciągle sporym zainteresowaniem.
W mojej opinii nadchodzące lata przyniosą stopniowe wdrażanie technologii, o których jeszcze niedawno mówiliśmy jako o „technologiach przyszłości".

Adam Laskowski

PKP Intercity

Pociągi PKP Intercity zapewniają bezpieczną podróż

Pandemia i związane z nią ograniczenia w sferze publicznej niemal z dnia na dzień diametralnie zmieniły zapotrzebowanie na podróżowanie, a jednocześnie pociągnęły za sobą konieczność modyfikacji procedur bezpieczeństwa, co ważne, z uwzględnieniem sytuacji, która dotychczas nie miała miejsca nie tylko na kolei, lecz także w skali globalnej. PKP Intercity już na samym początku opracowało i wdrożyło plany zapewniające ciągłość działania spółki i realizacji przewozów oraz wysoki poziom bezpieczeństwa pasażerów i pracowników spółki.
PKP Intercity cały czas funkcjonuje w reżimie sanitarnym, dążąc do zapewnienia bezpieczeństwa podróżnym i pracownikom. Maksymalnie bezpieczne korzystanie z pociągów zapewniają zaostrzone i restrykcyjnie przestrzegane procedury związane z codzienną obsługą taboru. Wprowadzono dezynfekowanie kluczowych miejsc i elementów wyposażenia wagonów, z którymi podróżny mają bezpośredni kontakt, m.in. klamek, poręczy, uchwytów, przycisków sterowania drzwiami czy toalet. Proces czyszczenia i dezynfekcji składów prowadzą wszystkie zakłady spółki, dzięki temu każdy pociąg jest odpowiednio przygotowywany przed i po każdym kursie. Od marca do grudnia 2020 r. wykonano w sumie ponad 335 tys. dezynfekcji lokomotyw, wagonów i członów EZT (elektrycznych zespołów trakcyjnych) oraz ponad 6 tys. dezynfekcji wagonów i członów EZT metodą zamgławiania.
Kierownicy pociągów i konduktorzy są wyposażeni w środki ochrony indywidualnej i utrzymania higieny osobistej: maseczki i rękawiczki ochronne oraz żele do mycia i dezynfekcji rąk. Ich kontakt z podróżnymi podczas kontroli biletów odbywa się z zachowaniem bezpiecznego dystansu dzięki wykorzystaniu nowoczesnych terminali zbliżeniowych.
Wprowadzone procedury i procesy bezpieczeństwa w związku z epidemią koronawirusa doceniają pasażerowie – wyniki przeprowadzonych badań satysfakcji pokazują, że 83% pasażerów ocenia pozytywnie bezpieczeństwo w pociągu (to najlepszy wynik od 2013 r., w którym PKP Intercity rozpoczęło prowadzenie cyklicznych badań satysfakcji). Tak ważne w czasie epidemii bezpieczeństwo sanitarne jest jednym z obszarów działań w ramach ogólnospołecznego programu #bezpiecznakolej, którego inicjatorami są PKP Intercity oraz Polska Izba Producentów Urządzeń i Usług na Rzecz Kolei. Jego celem jest wypracowanie najwyższych standardów bezpieczeństwa dla branży kolejowej.
Pociągi typu EZT (Pendolino, Darty, Flirty) są wyposażone w kamery do monitoringu wizyjnego, które gwarantują pasażerom poczucie bezpieczeństwa. Nie było konieczności wprowadzania żadnych nowych rozwiązań w tym zakresie w ostatnich miesiącach trwania pandemii.

Jakub Sobek

Linc Polska

Transport w chmurze

Zachowanie ciągłości łańcucha dostaw to jedno z największych wyzwań dla wielu przedsiębiorstw. Z powodu wielu czynników zabezpieczenie transportu jest zadaniem dość złożonym. Obecnie na firmy transportowe wywierana jest coraz większa presja, aby modernizowały techniki zabezpieczeń i gwarantowały jeszcze większe bezpieczeństwo dostaw. Specyficzne uwarunkowania instalacyjne stanowią jednak pewien problem techniczny dla wielu systemów w takich zastosowaniach.
Rejestratory i kamery w publicznych środkach transportu nie są niczym nowym. Spotykamy je w tramwajach, autobusach i miejscach obsługi podróżnych. Jednym z największych wyzwań dla tego typu technologii w pojazdach jest ich mobilność. W systemach stacjonarnych dostęp do sieci, z wyjątkiem awarii, jest stały i nieprzerwany. Poruszający się pojazd musi przełączać się pomiędzy sieciami i robić to w sposób maksymalnie bezawaryjny. Nie wszystkie rozwiązania poradzą sobie z takimi uwarunkowaniami. Ponadto sprzęt cały czas jest narażony na wibracje, dlatego należy wybierać urządzenia dobrej jakości.

Do tej pory zarejestrowany materiał był zgrywany po przyjeździe pojazdu do zajezdni, portu czy na stację. Obecnie takie podejście już się nie sprawdza, nikt nie oczekuje bowiem tylko działania po fakcie. Coraz bardziej złożone i wymagające operacje tranzytowe wymagają możliwości prowadzenia ciągłego monitoringu w czasie rzeczywistym. Ponadto istotne jest powiązanie nagrań z precyzyjnie zsynchronizowanym czasem oraz bieżącą lokalizacją pojazdu. Tylko taka ewidencja pozwala na precyzyjną rekonstrukcję wszystkich zdarzeń.
Co zrobić, jeśli nie chcemy martwić się przesyłaniem nagrań i mieć dostęp do wszystkich danych w czasie rzeczywistym? Najlepiej wybrać rozwiązania hybrydowe pozwalające na lokalną rejestrację danych oraz zapis w chmurze, wraz z backupem danych lokalnych, zawsze kiedy będzie dostęp do sieci. To gwarancja bezpieczeństwa i łatwości użytkowania. Oprogramowanie w chmurze wykonuje całą pracę związaną z właściwą archiwizacją danych i zachowaniem ich pełnej integralności. Wszystko jest bardzo łatwe w zarządzaniu dzięki aplikacji webowej.
Nowoczesny monitoring transportu właśnie tego wymaga.

Anna Bartoń

rzecznik Metra Warszawskiego

Reorganizacja i dystans społeczny

Zapewnienie bezpieczeństwa w ruchu pasażerskim zawsze było priorytetem dla Metra Warszawskiego. Niezależnie od rodzaju zagrożeń działania spółki opierają na zabezpieczeniu infrastruktury, zapewnieniu obsługi oraz odpowiedniej komunikacji z pasażerami. Nie bez znaczenia pozostaje stały kontakt i współpraca z zewnętrznymi instytucjami odpowiedzialnymi za bezpieczeństwo. Odpowiednia koordynacja tych procesów pozwoliła na stabilne funkcjonowanie metra w czasie pandemii i zapewnienie bezpieczeństwa na wysokim poziomie.
Dynamicznie zmieniająca się sytuacja epidemiologiczna wymusiła natychmiastowe i zdecydowane działania wewnątrz spółki. Należało ocenić zdolność poszczególnych struktur organizacji do radzenia sobie ze zmianami wywołanymi COVID-19 oraz określić procesy mające na celu zapewnienie ciągłości obsługi.
Zostały wyznaczone progi krytyczne absencji w poszczególnych grupach zawodowych, prowadziliśmy ich codzienną aktualizację. Wprowadziliśmy dywersyfikację zatrudniania, wdrażając zmianowość i pracę zdalną. Określiliśmy zasady przemieszczania się pracowników w obszarze firmy, zasady kontaktów z firmami zewnętrznymi oraz elektroniczny obieg dokumentów. Doposażyliśmy pracowników w sprzęt pozwalający na większą mobilność pracy. Zarówno cały obszar firmy, jak i pracowników, wyposażyliśmy w środki ochrony. W 261 newralgicznych miejscach zamontowaliśmy dozowniki płynu dezynfekującego, a pracownicy otrzymali maseczki jednorazowe i płyny do dezynfekcji. Wszystko to ograniczyło transmisję wirusa na terenie zakładu pracy.
Oprócz zabezpieczenia obsługi przewozów podjęliśmy również szereg działań profilaktycznych. Systematyczna dezynfekcja infrastruktury i taboru, komunikaty głosowe przypominające o obowiązku zakrywania ust i nosa, informacje o liczbie osób mogących podróżować w jednym wagonie – wszystko to uzupełniliśmy procedurami działania w przypadku podejrzenia lub potwierdzenia zakażenia COVID-19 u pasażera lub pracowników. Wszystkie wytyczne

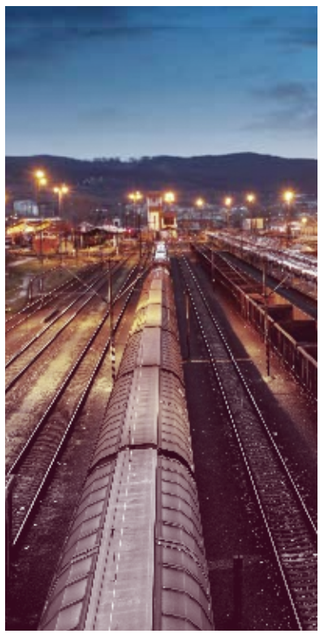
wielokrotnie weryfikowaliśmy. Zależało nam, aby pracownicy wiedzieli, jak postępować w sytuacjach kryzysowych, gdzie szukać informacji, porad, wsparcia. Po pierwszej fali epidemii i zniesieniu przez Radę Ministrów części ograniczeń Zarząd Spółki przeprowadził ocenę wprowadzonych rozwiązań i postanowił utrzymać dotychczasowe rygory. Działania skoncentrowały się na monitorowaniu sytuacji epidemiologicznej, zmianach w przepisach, ich implementacji i dostosowaniu do wymogów wewnętrznych. We wrześniu ponownie przeprowadziliśmy analizę rozwiązań i postanowiliśmy skupić uwagę na identyfikowaniu potencjalnych zagrożeń.
Dotychczasowe działania miały charakter indywidulanego dostosowywania się organizacji do zmieniającej się sytuacji ze względu na charakterystyczne warunki. Podjęcie niewłaściwej albo spóźnionej decyzji mogło doprowadzić do znacznego ograniczenia zdolności przewozowej, co w konsekwencji ma wpływ na zapewnienie przestrzeni dla pasażerów w czasie podróży. Dzięki strategii zapobiegania negatywnym skutkom kryzysu było możliwe podjęcie szybkich decyzji i działań je ograniczających. Uwzględniały one czynnik ludzki oraz procesowy i technologiczny. Przewozy pasażerskie z zachowaniem wszelkich zasad bezpieczeństwa na poziomie zgodnym z zamówieniem ZTM są i były realizowane w szczytowych okresach epidemii.

Łukasz Lubera

PKP CARGO

Zapewnienie maksymalnego bezpieczeństwa

W dobie pandemii przewoźnicy kolejowi powinni zwracać szczególną uwagę na zabezpieczenie personelu niezbędnego do zapewnienia ciągłości działania przedsiębiorstwa, przede wszystkim pracowników odpowiedzialnych za realizację procesu głównego, jakim jest transport towarów bądź pasażerów. Chodzi szczególnie o stanowiska bezpośrednio związane z zestawianiem składów pociągów i przygotowaniem ich do jazdy, a także o osoby odpowiedzialne za prowadzenie i bezpieczeństwo ruchu kolejowego (tj. maszyniści, obsługa pociągów oraz osoby zajmujące się organizacją i sterowaniem ruchem kolejowym).
Nie bez znaczenia dla realizacji bezpiecznych przewozów kolejowych pozostaje również personel odpowiedzialny za realizację procesów wspomagających, np. załoga, na której barkach spoczywa przygotowanie niezbędnych zasobów taborowych i utrzymywanie ich sprawności technicznej według najwyższych, ściśle określonych standardów (pracownicy warsztatów zaplecza technicznego).
Dla zapewnienia maksymalnego bezpieczeństwa personelu, a co za tym idzie sprawnego funkcjonowania przedsiębiorstwa, niezbędne jest podejmowanie działań w oparciu o wyznaczone standardy, w tym wyposażenie pracowników w środki ochrony indywidualnej (płyny do odkażania, rękawice jednorazowe, maseczki lub przyłbice). Jednocześnie należy ograniczać bezpośrednie kontakty pomiędzy pracownikami, tworząc stałe zespoły, bez możliwości rotowania ich składem (poza sytuacjami wyjątkowymi). Dzięki temu w przypadku zakażenia minimalizujemy liczbę osób, które muszą zostać objęte ewentualną kwarantanną, a tym samym ograniczamy zagrożenia związane z potencjalnym brakiem obsady kluczowych stanowisk.
Możliwe jest również rozszerzanie uprawnień personelu dla podobnych stanowisk, pamiętając przy tym, że zarówno szkolenie, jak i doskonalenie pracowników należy realizować z zachowaniem najwyższych standardów sanitarno-epidemiologicznych. Ponadto tam, gdzie to możliwe, należy prowadzić je w formie zdalnej (wykorzystując do tego urządzenia multimedialne, tj. laptopy, tablety lub smartfony i komunikatory internetowe) lub w formie hybrydowej, w ściśle określonych zespołach, bez zmiany ich składów osobowych. Tego typu działania pozwalają ograniczać ryzyko zachorowania i zapewnić ciągłość dostaw towarów.



Andrzej Żochowski

niezależny ekspert

Najważniejsze jest utrzymanie ciągłości działania

W dobie pandemii COVID-19 szczególne znaczenie dla biznesu związanego z logistyką kontraktową, spedycją i łańcuchem dostaw ma utrzymanie ciągłości pracy oraz zapewnienie sprawnej i nieprzerwanej obsługi klientów. Niestety pandemia ma także wpływ na wzrost zagrożeń bezpieczeństwa tego biznesu, takich jak kradzieże towarów, wyłudzenia kredytów od banków, telefonów komórkowych od operatorów telefonii komórkowej, wyłudzeń towarów od operatorów logistycznych przez tzw. fałszywe firmy transportowe.
Jednym z powodów wyraźnego zwiększenia wszystkich tych zagrożeń jest ograniczenie osobistych kontaktów klienta z firmą kurierską, logistyczną oraz innymi dostawcami wspomnianych usług (banki, operatorzy telefonii). Potencjalni oszuści wykorzystują ułatwienia dotyczące składania zleceń i zamówień na usługi, towar czy kredyt drogą telefoniczną lub za pośrednictwem poczty elektronicznej z użyciem m.in. skanów dokumentów tożsamości, zleceń itp.
W celu zredukowania powyższych zagrożeń w firmach zostały dopracowane i wdrożone m.in. oceny ryzyka biznesu/plany ciągłości działania dotyczące zagrożeń związanych z pandemią i emisją wirusa wśród pracowników. Kierownictwo reaguje szybciej na podejrzenia zakażenia pracowników, a tam, gdzie specyfika poszczególnych działów na to pozwala, stosowany jest model pracy w trybie home office. Najczęściej połowa personelu pracuje stacjonarnie, a połowa w domu, w tzw. trybie rotacyjnym. Wdrożono obowiązek noszenia maseczek ochronnych czy przyłbic dla wszystkich pracowników w opcji pracy stacjonarnej i obsługi klientów.
Standardem w miejscach pracy stały się płyny do dezynfekcji rąk oraz utrzymywanie dystansu, zakazano podróży służbowych z wyjątkiem tzw. sytuacji krytycznych. Zastosowano kamery termowizyjne do monitorowania temperatury osób wchodzących na teren obiektów, zarówno pracowników firmy, jak i klientów.

Błażej Ożga

Nedap Security Management

Kluczowa rola kontroli dostępu

Branża logistyczna i transportowa zetknęła się na początku zeszłego roku z wieloma problemami wywołanymi epidemią w kraju i na świecie. Wiele firm nagle znalazło się w sytuacji, która zmusiła je do zapewnienia ciągłości działania i bezpieczeństwa zarówno swoim pracownikom, jak i kontrahentom. Wymagało to reorganizacji zasad bezpieczeństwa wewnątrz tych podmiotów.
Menedżerowie ds. bezpieczeństwa zaczęli poszukiwać rozwiązań, które w zaistniałej sytuacji pozwoliłyby zarówno spełnić wymagania stawiane przez sanepid, jak i przyspieszyć lub wręcz usprawnić procesy. Najważniejszym zadaniem było maksymalne ograniczenie możliwości wejścia na teren zakładu osobie podejrzewanej o zakażenie koronawirusem. Kluczową rolę w tym procesie ma system kontroli dostępu. To on właśnie odpowiada za decyzje o przyznaniu dostępu lub niewpuszczeniu danej osoby.
Ostatni rok pokazał, jak szybko są w stanie zareagować producenci systemów zabezpieczeń na potrzeby rynku, powiększając swoje portfolio o całkowicie nowe urządzenia, umożliwiające np. bezstykowe mierzenie temperatury. Z kolei integracja systemu KD ze stacją odkażania rąk uniemożliwia wejście do strefy chronionej, jeżeli osoba autoryzowana nie użyje tego urządzenia.
Niektórzy producenci wybierają inną drogę - nie wprowadzają na rynek dedykowanych rozwiązań, natomiast podpowiadają swoim klientom, w jaki sposób mogą wykorzystać istniejące zasoby oprogramowania systemu kontroli dostępu, by ten mógł służyć w nowej roli. Jedną z najczęściej wykorzystywanych funkcjonalności jest opcja zliczania osób w poszczególnych obszarach budynku, uniemożliwiająca wejście większej liczby osób niż zaprogramowano. Kolejnym przykładem jest wdrożenie scenariuszy bezpieczeństwa, które jednym kliknięciem odcinają „skażoną" część budynku, uniemożliwiając wejście do tej strefy osobom postronnym, z wyjątkiem uprawnionych służb.
Jedno jest pewne, takie rozwiązania będą potrzebne przez najbliższe lata. Tylko lepsze, bardziej zaawansowane systemy KD nie wymagają wymiany czy inwestowania w dodatkowe moduły, a jedynie odpowiedniego ich skonfigurowania w samym oprogramowaniu. To z kolei przekłada się na wymierne oszczędności wdrażania takich rozwiązań teraz i w przyszłości.

Marcin Walczuk

BCS

Nowe zastosowania systemów zabezpieczeń

Ze względu na panującą od roku pandemię koronawirusa wiele sfer naszego życia uległo zmianie. Nie inaczej sytuacja wygląda w branży transportowej. Zdecydowanie bardziej odczuł to segment przewozów pasażerskich. Oczywiście pomijając sytuacje, w których takie połączenia międzynarodowe zostały zupełnie zawieszone, te lokalne w dalszym ciągu muszą spełniać swoją funkcję, by zapewnić podróżnym możliwość dotarcia chociażby do pracy.
Do standardowych celów do tej pory stawianych przed systemami zabezpieczającymi dworce kolejowe i autobusowe, lotniska czy same środki transportu doszły kolejne związane z koniecznością ochrony podróżnych przed zakażeniem i zahamowania rozprzestrzeniania się wirusa.
Wprowadzone ograniczenie liczby podróżnych wiązało się z koniecznością zamontowania systemów sprawdzających liczbę pasażerów w danym pociągu czy autobusie. Trudno jednak wyobrazić sobie pracownika, który będzie siedział i liczył wsiadających i wysiadających pasażerów. Do takiego zadania można z powodzeniem zaadaptować kamery CCTV, już i tak szeroko wykorzystywane w transporcie. Najnowsze kamery BCS z funkcjami analizy wideo, w których skład wchodzi również algorytm zliczania ludzi, mogą monitorować kilka wejść jednocześnie, tworząc wspólny licznik pasażerów przebywających w pojeździe. W wypadku zbliżania się lub przekroczenia przewidzianego limitu pasażerów może zostać wygenerowany alarm przekazany do kierującego pojazdem.
BCS - korzystając z długoletniego doświadczenia przy zabezpieczaniu obiektów kolejowych, takich jak chociażby dostawy urządzeń do zabezpieczenia przejazdów kolejowych czy współpraca przy projektach Innowacyjnych Dworców Systemowych - może być świetną platformą dla nowych rozwiązań zabezpieczeń stosowanych w walce z COVID-19. Na pewno dodatkowym atutem będzie spełnianie przez nasze urządzenia wytycznych IPI-4 dotyczących projektowania i budowy systemów monitoringu wizyjnego w obiektach obsługi pasażerskiej, a także wytycznych dotyczących dobrych praktyk w inwestycjach dworców kolejowych PKP SA. Dzięki temu można wykorzystać nasze systemy do pomiaru temperatury ludzkiego ciała oparte na kamerach termowizyjnych, pomagające wskazać osoby, które mogą stanowić potencjalne zagrożenie dla innych podróżnych

Wyznaczamy standardy w ochronie przeciwpożarowej

Centrala sygnalizacji pożarowej i sterowania urządzeniami przeciwpożarowymi Schrack Seconet – Integral IP MX

System sygnalizacji pożarowej i sterowania urządzeniami przeciwpożarowymi zgodnie z obowiązującymi przepisami musi spełniać szereg wymagań technicznych i formalnych, żeby w pełni realizować założenia koncepcji bezpieczeństwa pożarowego chronionego obiektu, w szczególności wdrożenia wytycznych zawartych w scenariuszu pożarowym.

Od początku istnienia firmy Schrack Seconet koncentrujemy nasze działania nie tylko na wprowadzaniu do oferty urządzeń, które spełniają wymagania obowiązujących norm, przepisów i wytycznych, ale także na wdrażaniu produktów i rozwiązań, znacznie je przewyższających. Dzięki temu niezmiennie wyznaczamy nowe standardy w zakresie ochrony przeciwpożarowej. Dla potwierdzenia formalnego spełnienia obowiązujących wymagań w zakresie sterowania urządzeniami przeciwpożarowymi centrala sygnalizacji pożarowej, centrala sterowania urządzeniami przeciwpożarowymi (CSP/CSUP) Integral IP MX **jako jedyna na rynku przeszła specjalne badania atestacyjne w CNBOP-PIB w zakresie sterowania urządzeniami przeciwpożarowymi** i uzyskała następujące dokumenty certyfikacyjne:

- krajowy certyfikat stałości właściwości użytkowych nr 063-UWB-0304 wydany na podstawie uzyskanej Krajowej Oceny Technicznej CNBOP-PIB nr CNBOP-PIB-KOT-2020/0228-1009 dla wyrobu budowlanego „Urządzenie sterujące i sygnalizujące w systemach kontroli rozprzestrzeniania dymu i ciepła oraz sterowania gaszeniem – Centrala sterująca urządzeniami przeciwpożarowymi typu Integral IP MX”,
- certyfikat stałości właściwości użytkowych nr 1438-CPR-0743 zgodnie z EN 12101-10:2005 dla wyrobu budowlanego „Zasilacz do systemów kontroli rozprzestrzeniania dymu i ciepła typu Integral IP MX”,
- świadectwo dopuszczenia CNBOP-PIB nr 4192/2020 spełniające wymagania pkt 12.1, pkt 12.2 załącznika do rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 20 czerwca 2007 r. w sprawie wykazu wyrobów służących zapewnieniu bezpieczeństwa publicznego lub ochronie zdrowia i życia oraz mienia, a także zasad wydawania dopuszczenia tych wyrobów do użytkowania (Dz.U. nr 143 poz. 1002; zm.: Dz.U. z 2020 r. nr 85, poz. 553 oraz z 2018 r. poz. 984) dla wyrobu „Centrala sterująca urządzeniami przeciwpożarowymi oraz zasilacza urządzeń przeciwpożarowych typu Integral IP MX”.

Uwzględniając wydane wcześniej certyfikaty, centrala Integral IP MX może spełniać jednocześnie następujące funkcje w ramach instalacji bezpieczeństwa pożarowego:

- centrala sygnalizacji pożarowej zgodnie z PN-EN 54-2:1997+A1:2006,
- centrala sterująca urządzeniami przeciwpożarowymi w systemach kontroli rozprzestrzeniania dymu i ciepła zgodnie z KOT (prEN 12101-9),
- zasilacz do systemów kontroli rozprzestrzeniania dymu i ciepła zgodnie z PN-EN 12101-10:2005,
- zasilacz urządzeń przeciwpożarowych zgodnie z PN-EN 54-4:1997+A1:2002+A2:2006,
- centrala sterująca stałymi urządzeniami gaśniczymi gazowymi zgodnie z PN-EN 12094-1:2003,
- centrala sterująca stałymi urządzeniami gaśniczymi wodnymi, pianowymi, aerozolowymi zgodnie z KOT,
- centrala sterująca i nadzorująca w ramach instalacji wodociągowych i przeciwpożarowych zgodnie z KOT.

Sterowanie i nadzorowanie urządzeń przeciwpożarowych zgodnie z ww. dokumentami odniesienia jest realizowane przez następujące elementy wchodzące w skład CSP/CSUP Integral IP MX:

- karty sterujące wejścia/wyjścia central Integral IP MX,
- moduły wejścia/wyjścia pracujące na liniach pętlowych techniki X-LINE,
- moduły wejścia/wyjścia SF-CONTROL.

CSP/CSUP Integral IP MX może pracować w sieci central w układzie równorzędnym lub hierarchicznym z wykorzystaniem połączeń wykonanych przewodami miedzianymi lub światłowodowymi i zastosowaniem sieci o topologii magistrali, pierścienia lub sieci kratowej *(mesh network)*. Oferowana technologia sieciowa Integral LAN/Integral WAN charakteryzuje się bardzo dużą elastycznością i niezawodnością działania – przy zastosowaniu zdublowanych torów komunikacyjnych w sieci o topologii pierścienia system jest odporny na 3 jednoczesne uszkodzenia połączeń sieciowych, a w przypadku sieci kratowej zapewniona jest odporność nawet na 7 takich uszkodzeń.

Funkcje centrali sygnalizacji pożarowej i sterowania urządzeniami przeciwpożarowymi mogą być wykonywane jednocześnie przez wszystkie centrale pracujące w sieci. Funkcje detekcji i sterowania mogą być podzielone na poszczególne centrale lub realizowane w ramach oddzielnych podsystemów sieciowych w zależności od wymagań technicznych i organizacyjnych danego obiektu.

CSP/CSUP Integral IP MX, ze względu na zastosowaną konstrukcję i technologię opartą na pełnej redundancji platformy sprzętowej i oprogramowania systemowego, zapewnia niezawodne działanie i realizację funkcji sterujących przy wystąpieniu uszkodzenia systemowego – w przypadku awarii następuje bezzwłoczne przełączenie ze strony aktywnej na stronę zapasową pracującą w układzie gorącej rezerwy *(hot standby)*. Dzięki tej technologii centrala może sterować wielostrefowymi systemami gaszenia czy realizować sterowania urządzeniami przeciwpożarowymi w ramach wielu stref pożarowych. Ponadto wyjścia sterujące mają programowaną pozycję *fail-safe* pozwalającą na przełączenie wyjść sterujących w pozycję pożarową np. przy utracie komunikacji modułu pętlowego z centralą.

CSP/CSUP Integral IP może w praktyce realizować najbardziej skomplikowane procedury sterowania zawarte w scenariuszu pożarowym dzięki dostępnym specjalnym funkcjom oprogramowania:

- możliwości tworzenia dowolnych algorytmów sterowania dla wyjść sterujących na bazie szerokiej bazy operatorów logiki Boole'a,
- nadzór ciągłości przewodów zasilająco-sterujących urządzenia ppoż. (np. klapy odcinające wentylacji pożarowej),
- możliwości równoległego stosowania kilku kryteriów sterujących z konfigurowanymi priorytetami wykonywania w zależności od stanu pracy obiektu,
- sterowania wyjść w trybie ciągłym lub impulsowym,
- sterowania grupowe urządzeń (np. klapy ppoż.) do 8 A,
- sterowania cyfrowego klapami wyposażonymi w siłowniki w standardzie MP-BUS,
- sterowania z funkcją potwierdzenia zwrotnego,
- możliwości realizacji funkcji prewencyjnego sterowania wybranych urządzeń przeciwpożarowych podczas prowadzenia prac serwisowych (stan odłączenia systemu).
- sterowania ręczne umożliwiające przesterowanie wyjść uruchomionych przez algorytmy automatyczne,
- blokowania (zatrzaskiwania) stanów wysterowania w zależności od stanu pracy systemu.

Podczas przygotowywania konfiguracji centrali instalator czy programista mają możliwość weryfikacji stworzonych algorytmów sterujących poszczególnymi wyjściami za pomocą wbudowanego symulatora/testera stanów logicznych. Dodatkowo Integral IP umożliwia na etapie uruchamiania systemu blokowanie (zamrażanie) wyjść sterujących w celu testowania działania całego scenariusza pożarowego, bez fizycznego uaktywnienia urządzeń. Zapewnia to duży komfort i bezpieczeństwo podczas wdrażania systemu oraz późniejszego prowadzenia prac modernizacyjnych i serwisowych w obiekcie.

System Integral IP ściśle współpracuje z certyfikowanym systemem integrującym urządzenia przeciwpożarowe SIS-FIRE z wykorzystaniem systemowego protokołu komunikacyjnego ISP-IP. Zapewnia realizację zaawansowanych funkcji detekcji pożaru z możliwością np. odczytu wartości analogowych (temperatura, CO i inne) czujek interaktywnych serii CUBUS oraz sterowania urządzeniami przeciwpożarowymi w ramach spójnego i kompleksowego systemu zarządzania bezpieczeństwem pożarowym obiektu oraz nadzorowanie ich. Istotną cechą systemu zarządzania bezpieczeństwem pożarowym SIS-FIRE jest jego wysoka elastyczność działania i możliwość spełnienia niemal nieograniczonej liczby zadań i funkcji logicznych.

Opisane funkcje systemowe zapewniają bezpieczne i elastyczne zastosowanie CSP/CSUP Integral IP MX w dowolnym typie obiektu oraz wdrożenie praktycznie dowolnej koncepcji bezpieczeństwa.

SCHRACK SECONET POLSKA

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

Cyberbezpieczeństwo w firmach branży S&S[1]

CZ. 1

USTAWA Z 5 LIPCA 2018 R. O KRAJOWYM SYSTEMIE CYBERBEZPIECZEŃSTWA (I WYDANE NA JEJ PODSTAWIE ROZPORZĄDZENIA WYKONAWCZE) OBOWIĄZUJE OD 25 SIERPNIA 2020 R.

1. Ustawa z 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2020 r., poz. 1369 tekst jednolity). Obowiązuje od 25 sierpnia 2020 r.
2. Rozporządzenie Rady Ministrów z 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych (Dz.U. z 2018 r., poz. 1806). Obowiązuje od 22 września 2018 r.
3. Rozporządzenie Rady Ministrów z 2 października 2018 r. w sprawie zakresu działania oraz trybu pracy Kolegium do Spraw Cyberbezpieczeństwa (Dz.U. z 2018 r., poz. 1952). Obowiązuje od 13 października 2018 r.
4. Rozporządzenie Ministra Cyfryzacji z 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U. z 2018 r., poz. 1999). Obowiązuje od 19 października 2018 r.
5. Rozporządzenie Rady Ministrów z 16 października 2018 r. w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej (Dz.U. z 2018 r., poz. 2080). Obowiązuje od 31 października 2018 r.
6. Rozporządzenie Rady Ministrów z 31 października 2018 r. w sprawie progów uznania incydentu za poważny (Dz.U. z 2018 r., poz. 2180). Obowiązuje od 22 listopada 2018 r.
7. Rozporządzenie Ministra Cyfryzacji z 4 grudnia 2019 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo (Dz.U. z 2019 r., poz. 2479). Obowiązuje od 7 stycznia 2020 r.

Nie było zapewne najlepiej w państwach członkowskich Unii Europejskiej z cyberbezpieczeństwem[2], skoro w 2016 r. wprowadzono do europejskiego zbioru aktów prawa powszechnego dyrektywę[3], której celem jest poprawa istniejącej w tym zakresie sytuacji. Dyrektywa zaleca ujednolicenie i zintensyfikowanie działań poprawiających zabezpieczenia przed cyberatakami ważnych unijnych i krajowych sieci LAN (o zasięgu lokalnym) i WAN (o zasięgu ponadlokalnym), a także ważnych[4] autonomicznych systemów teleinformatycznych, połączonych lub niepołączonych z Internetem.

1) Safety & security (bezpieczeństwo i ochrona). Branża S&S grupuje firmy ochrony osób i mienia, firmy zabezpieczenia technicznego, a także wywiadownie gospodarcze i firmy świadczące usługi detektywistyczne.
2) Definicję terminu „cyberbezpieczeństwo" zawiera art. 2, pkt 4 Ustawy z 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa
3) Dyrektywa PE i Rady (UE) 2016/1148 z 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.Urz. UE L 194 z 19.07.2016).
4) Kryteria ważności określa ustawa przywołana w artykule pod pozycją [1].

Marek Ryszkowski

Dyrektywa zobligowała państwa UE do inkorporacji wielu jej przepisów do krajowych aktów prawa powszechnego, a także powołania organów i instytucji władzy publicznej, zapewniających wdrożenie tych regulacji oraz przekazywanie do organów i instytucji unijnych – w ściśle określonym trybie – informacji o stanie cyberbezpieczeństwa w ich narodowych cyberprzestrzeniach. Dla ułatwienia dalszych rozważań problemu cyberbezpieczeństwa przywołam ustawową definicję tego terminu:

cyberbezpieczeństwo – odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy.

Praktykujący sztukę zarządzania dobrze wiedzą, że jeżeli pojawia się jakiś poważny problem do uregulowania, to najskuteczniejszym sposobem dokonania tego jest – po wykonaniu niezbędnych analiz i syntez takiego problemu – zastosowanie metod teorii systemów. Zatem, trywializując nieco, można stwierdzić, że dla zapewnienia bezpieczeństwa danym przetwarzanym w systemach teleinformatycznych oraz sieciach LAN i WAN najlepiej zorganizować – na bazie teorii systemów – system cyberbezpieczeństwa składający się z trzech podsystemów: sterującego, wykonawczego i alimentacyjnego. Ich nazwy jednoznacznie mówią, do jakich zadań zostaną powołane. Wprowadzona dyrektywa unijna niedwuznacznie zaleca powołanie takiego systemu, którego celem będzie zapewnienie wymaganego poziomu cyberbezpieczeństwa w unijnej i krajów członkowskich cyberprzestrzeniach. Określa także w sposób ramowy, jak tego dokonać na szczeblu unijnym i poszczególnych krajów członkowskich UE.

Zapewnienie bezpieczeństwa danych (aktywom informacyjnym) podlegających obligatoryjnej lub fakultatywnej ochronie w polskim systemie prawnym, przetwarzanych w systemach i sieciach teleinformatycznych jest obowiązkiem nie tylko decydentów unijnych i krajowych, lecz także zarządców podmiotów prawa handlowego i podmiotów o innym statusie prawnym, działających w polskiej, zatem także unijnej przestrzeni prawnej.

O podsystemie sterującym (część normatywno-prawna) systemu cyberbezpieczeństwa w naszej cyberprzestrzeni pomyśleli już polscy prawodawcy, wprowadzając do systemu prawa powszechnego RP ustawę o krajowym systemie cyberbezpieczeństwa i – na podstawie jej dyspozycji – kilka rozporządzeń wykonawczych. Zarządcy podmiotów prawa handlowego, także z branży S&S, jeżeli są do tego zobowiązani lub zamierzają (dla rozwoju rynkowego kierowanego przez siebie podmiotu) zorganizować systemy cyberbezpieczeństwa w swoich firmach, powinni zacząć od przestudiowania wspomnianej ustawy i wydanych na podstawie jej dyspozycji aktów wykonawczych – rozporządzeń. W ramce obok podajemy ich pełne nazwy i dane o sposobie opublikowania w Dzienniku Ustaw RP.

Ten zestaw aktów prawa powszechnego, stanowiący istotną część podsystemu sterującego systemu cyberbezpieczeństwa w polskiej cyberprzestrzeni, nie jest lekturą lekką ani łatwą dla osób podejmujących trud ich przestudiowania. Zatem przed podjęciem decyzji o przystąpieniu do organizowania firmowego systemu cyberbezpieczeństwa siłami własnymi firmy warto się zastanowić, czy nie będzie lepiej zaangażować do wykonania tego zadania (tzn. analizy i syntezy, o których była mowa wyżej) wyspecjalizowanej firmy zewnętrznej, która ma doświadczenie w tego rodzaju zleceniach i może okazać wiarygodne listy polecające od innych zleceniodawców, potwierdzających ich autentyczność.

Ponadto warto wiedzieć, że Urząd Dozoru Technicznego[5], który otrzymał niemałe kompetencje ustawowe do działania w polskim systemie cyberbezpieczeństwa, w tym prawo do prowadzenia audytu cyberbezpieczeństwa w tzw. podmiotach – operatorach usług kluczowych, opracował innowacyjną metodykę Framework UDTCyber[6]. Metodyka ta ma być lub już jest wykorzystywana do prowadzenia wspomnianych audytów.

Definicję pojęcia usługa kluczowa zawiera ww. ustawa w art. 2, pkt 16 i brzmi ona następująco:
Usługa kluczowa – [oznacza] usługę, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej, wymienioną w wykazie usług kluczowych.

Natomiast definicję terminu operator usługi kluczowej zawiera art. 5, ust. 1 wspomnianej ustawy i ma ona brzmienie:

5) Urząd Dozoru Technicznego wymieniony został w art. 4 pkt 11 ww. ustawy jako istotny składnik polskiego Krajowego Systemu Cyberbezpieczeństwa.
6) O metodyce tej szerzej w Biuletynie Urzędu Dozoru Technicznego INSPEKTOR – TECHNIKA I BEZPIECZEŃSTWO, nr 2/2020, s. 7-8. Metodykę tę umieszczono w całości na stronie internetowej www.udt.gov.pl. Jej pobranie w całości przez zainteresowane osoby opatrzone jest warunkami, których akceptacja może być dla niektórych trudna do przyjęcia.

Operatorem usługi kluczowej jest podmiot, o którym mowa w załączniku nr 1 do ustawy, posiadający jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej, wobec którego organ właściwy do spraw cyberbezpieczeństwa wydał decyzję o uznaniu za operatora usługi kluczowej.

Przywołana ustawa zawiera (w art. 17, ust. 1) także definicję terminu dostawca usług cyfrowych:
Dostawcą usługi cyfrowej jest osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej, mająca siedzibę lub zarząd na terytorium Rzeczypospolitej Polskiej albo przedstawiciela mającego jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej, świadczącą usługę cyfrową, z wyjątkiem mikroprzedsiębiorców i małych przedsiębiorców, o których mowa w art. 7 ust. 1 pkt 1 i 2 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców (Dz.U. poz. 646 i 1479). Rodzaje usług cyfrowych określa załącznik nr 2 do ustawy.

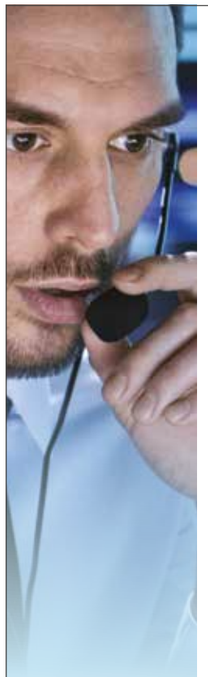
Z kolei wykaz rodzajów usług kluczowych znajduje się w załączniku do rozporządzenia, które wyszczególniono wyżej pod poz. [2]. Wykaz ten powinien uważnie przestudiować zarządca każdego podmiotu, także ten, który świadczy usługi z zakresu ochrony osób i mienia. Świadcząc bowiem te usługi podmiotowi, który został uznany za operatora usług kluczowych lub dostawcę usług cyfrowych w rozumieniu przywołanej ustawy, może być uznany za część systemu cyberbezpieczeństwa tego operatora albo dostawcy, co nie pozostanie bez konsekwencji, np. ekonomicznych, sprzętowych czy organizacyjnych dla takiej firmy z branży S&S.

Wiedza o tym, co zawierają ww. akty prawa powszechnego i co zapisał UDT w swojej metodyce audytowania stanu cyberbezpieczeństwa podmiotów – operatorów usług kluczowych i dostawców usług cyfrowych, jest zatem niezbędna głównie zarządcom podmiotu audytowanego, a niewątpliwie będzie potrzebna także zarządcom jego kooperantów i outsourcingowców. Jak to zwykle przebiega, wiedzą wszyscy, którzy podlegali już różnego rodzaju audytom, certyfikacjom lub np. postępowaniu bezpieczeństwa przemysłowego. Znajomość metodyki wykonywania czynności w ramach tych przedsięwzięć przez inspektorów, audytorów czy kontrolerów (co mogą, a czego nie), zwłaszcza przez zarządców i pracowników objętych tymi czynnościami podmiotów, może okazać się istotnym czynnikiem do uzyskania pozytywnego dla podmiotu audytowanego (kontrolowanego) zakończenia tych czynności.

Kluczowy dla każdego podmiotu prawa handlowego, a także dla firm o innym statusie prawnym, jest wynik analizy i syntezy problemu, jak zapewnić wymagany poziom cyberbezpieczeństwa w cyberprzestrzeni firmy własnej i firmy ochranianej. Dla firm z branży S&S głównie, brak należytego poziomu cyberbezpieczeństwa w firmie tej branży zwykle może bowiem mieć negatywny wpływ na poziom cyberbezpieczeństwa w ochranianej firmie – zwłaszcza gdy jest ona operatorem lub dostawcą, o których była już mowa. Jakie zatem mogą być wyniki takiej analizy i syntezy wspomnianego problemu? Oto one:

1. Nie zajmować się w firmie cyberbezpieczeństwem, gdyż ze względu na specyfikę i profil jej działalności biznesowej nie ma ona takiego obowiązku wynikającego z postanowień przywołanych wyżej (unijnego i krajowych) aktów prawa powszechnego. Może to dotyczyć tylko mikro- i miniprzedsiębiorstw, także tych z branży S&S. Firmy te powinny trzymać się z daleka od np. ofert ochrony fizycznej, wysyłanych do nich przez podmioty prawa handlowego i wszystkie inne, którym nadano status prawny ww. operatorów

BRAK NALEŻYTEGO POZIOMU CYBERBEZPIECZEŃSTWA W FIRMACH BRANŻY SAFETY AND SECURITY MOŻE MIEĆ NEGATYWNY WPŁYW NA POZIOM CYBERBEZPIECZEŃSTWA W OCHRANIANEJ FIRMIE, ZWŁASZCZA GDY JEST ONA OPERATOREM LUB DOSTAWCĄ USŁUG KRYTYCZNYCH



lub dostawców. „Zlekceważenie" cyberbezpieczeństwa w tych firmach nie oznacza oczywiście, że są one zwolnione z zapewnienia ochrony informacjom podlegającym obligatoryjnej lub fakultatywnej ochronie w unijnej i/lub polskiej przestrzeni prawnej przed dostępem osób nieuprawnionych.

2. Kondycja ekonomiczna firmy i/lub perspektywa wzrostu pozycji rynkowej w sektorze jej działalności rynkowej mogą być zachwiane po poniesieniu kosztów budowy w niej systemu cyberbezpieczeństwa, chociaż nie można wykluczyć, że w sprzyjającej koniunkturze może być odwrotnie. W tym przypadku decyzja kierownictwa firmy – wchodzimy w to lub nie wchodzimy – może być trudna. Menedżerowie firm, które na budowę systemu ochrony informacji niejawnych i uzyskanie świadectwa bezpieczeństwa przemysłowego poniosły duże koszty, a które nigdy im się nie zwróciły finansowo, mogą coś na ten temat powiedzieć.
3. Budowa systemu cyberbezpieczeństwa w firmie może – z dużym niekiedy prawdopodobieństwem – korzystnie wpłynąć na jej pozycję rynkową i rynkowy wizerunek. Może to dotyczyć zwłaszcza dużych firm, także tych z branży S&S, które udźwignął finansowo koszty tego przedsięwzięcia i – co ważne – już ochraniają lub są outsourcingowcami firm, które uzyskały status ww. operatorów lub dostawców.

Dla zarządców firm, które uzyskały wyniki analizy i syntezy problemu cyberbezpieczeństwa wyszczególnione w punktach 2 i 3, poza zbudowaniem jak najmniejszym kosztem systemu cyberbezpieczeństwa, ważne jest uzyskanie jego akredytacji przez UDT. Budując ten system, warto więc wiedzieć, wg jakiej metodyki audytorzy UDT będą działać i co sprawdzać w procesie jego akredytacji. Zatem dogłębna znajomość metodyki Framework UDTCyber jest dla zarządców tych firm bezcenna.

Czym jest wspomniana wyżej metodyka UDT, co zawiera i jakie problemy cyberbezpieczeństwa audytowanej firmy obejmą audytorzy UDTCert audytem zostanie przedstawione w drugiej części tego artykułu.

MAREK RYSZKOWSKI

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

Bezpieczeństwo informacji z perspektywy praktyka

Gdy myślimy o bezpieczeństwie informacji, uwagę skupiamy na systemach informatycznych i zagrożeniach tam ulokowanych. I słusznie – IT jest dziś miejscem o niespotykanej kumulacji zagrożeń. Wraz z rozwojem technologii będzie miało jeszcze większe znaczenie, tym samym liczba i nasilenie zagrożeń także będzie w trendzie wzrostowym. Jednak informacje, także te wrażliwe, a niekiedy nawet krytyczne dla bytu przedsiębiorstwa, też znajdują się poza tymi systemami. Niekiedy są na wyciągnięcie ręki: na kartce, ekranie komputera widocznym dla osoby postronnej, można je także skopiować bez włamywania się do systemu.

Jacek Grzechowiak

PERSPEKTYWA 1.
ZŁODZIEJ PRZYCHODZI DO NAS

Pierwszą reakcją osób, z którymi mam kontakt podczas szkoleń czy dyskusji nt. ochrony informacji, gdy przedstawiam klasyczny przykład insidera, jest zdumienie i komentarz, że przecież szpiegostwo dotyczy struktur państwowych i czasów wojennych. Przytoczę komentarz z jednej z dyskusji w serwisie społecznościowym sprzed miesiąca: ***Kret to taka stara metoda działania sowieckiego GRU. Ciekawe, że to funkcjonuje też w biznesie. Pewnie starzy towarzysze mogą mieć w tym doświadczenie.*** Takie podejście nie jest wyjątkiem. Nie jest też – przynajmniej częściowo – błędne. Powodem jest najczęściej formalna definicja szpiegostwa, skierowana na działalność obcego wywiadu i przekazywanie informacji właśnie jemu. To dość mocne i niesłuszne zawężenie problematyki kradzieży informacji. Nie od dziś też wiadomo, że służby specjalne działają na korzyść biznesu swojego kraju, dlatego trzeba przyjąć, że szpiegostwo, obecne na poziomie państwowym, istnieje także w biznesie, ale już nie tylko w formie oddziaływania struktur państwowych. Co istotne, dotyczy to także osób młodych, nie koncentrujmy się więc na „starych towarzyszach", oczywiście nie lekceważąc ich, kierując się jedną z refleksji, jaką zawarłem w artykule *Różne oblicza bezpieczeństwa wartości pieniężnych*[1]. Ochrona informacji jest od strony formalnoprawnej realizowana przede wszystkim na podstawie kodeksu karnego lub ustawy o zwalczaniu nieuczciwej konkurencji. Praktyczne przykłady obrazujące tę problematykę można znaleźć w wielu publikacjach, przy czym o ile od strony procesowej jest to dość proste z wykorzystaniem otwartych źródeł (np. System Analizy Orzeczeń Sądowych SAOS[2] lub System Informacji Prawnej LEX[3]), o tyle bardziej dokładne opisy incydentów trudniej znaleźć – przykładem może być syntetyczny opis m.in. na stronie internetowej wielkopolskiej policji[4]. Z przedstawionego tam obrazu wynika, że osoba zatrudniona na stanowisku analityka przez kilka miesięcy przekazywała informacje osobie pracującej w konkurencyjnym przedsiębiorstwie: dane o zakupie surowca, odbiorcach, szczegółach procesu produkcji, detalach finansowych. To przykład wręcz podręcznikowy, a ponieważ wydarzył się niedawno, skłania do refleksji nad procesem ochrony informacji, w którym procedura ochrony tajemnicy przedsiębiorstwa, zasada wiedzy koniecznej i procesowa dywersyfikacja dostępu do informacji są tak ważne. **Procedura, zasada wiedzy koniecznej oraz dywersyfikacja dostępu** – wielokrotnie zwracam na to uwagę.

Gdyby to było tak proste, to życie byłoby zbyt łatwe, a być może nawet nudne. Niestety to też nie jest wystarczające. Sama procedura, nawet precyzyjnie i rzetelnie realizowana, może nie wystarczyć, jeśli chronione informacje będą zabezpieczane jedynie od strony proceduralnej. Praktycy wiedzą, jak trudno udowodnić, że dana informacja jest tajemnicą przedsiębiorstwa. Powszechnie wiadomo, że przy danych tabelarycznych zawierających układ tabeli, wartości liczbowe i formuły mamy szereg informacji, które pozwalają na wiarygodne zbudowanie tezy o prawach własności tych danych, ale zapewne wielu czytelników spotkało się z argumentem *...mój klient po prostu podchodzi do tworzenia tych dokumentów w ten sposób, ponieważ zapoznał się z nim podczas studiów na tej uczelni; jest to więc wiedza powszechna.*

W dokumentach tekstowych jest jeszcze trudniej. W obu przypadkach z pomocą przychodzą różne techniki dotyczące ciągu następujących po sobie wyrazów, formatowania tekstu, a nawet operatorów graficznych. Wymagają one jednak tak samo skrupulatnego podejścia, jak definiowanie tajemnicy przedsiębiorstwa.

PERSPEKTYWA 2.
ZŁODZIEJ JEST U NAS

Najczęściej pracownicy wykorzystują swoje stanowisko do czerpania własnych korzyści, choć oczywiście nie tylko w tym celu. Zwykle to typowa korupcja, ale niestety, zdarza się, że pracownicy utrzymują swoje relatywnie niezbyt dobrze płatne zatrudnienie np. w celu stałego przysparzania sobie dochodów w przedsiębiorstwach własnych, rodzinnych bądź będących w relacji przyjacielskiej. Liczne przykłady tego typu procederów są dostępne publicznie, choćby w Systemie Analizy Orzeczeń Sądowych.

Jednym z ciekawszych jest zdarzenie, które dotyczyło wykorzystania informacji stanowiących tajemnicę przedsiębiorcy przygotowującego ofertę przetargową. ***Wbrew ciążącemu na niej obowiązkowi***

1) https://aspolska.pl/rozne-oblicza-bezpieczenstwa-wartosci-pienieznych/ (dostęp: 17.01.2021)
2) https://www.saos.org.pl/
3) https://sip.lex.pl/orzeczenia-i-pisma-urzedowe/orzeczenia-sadow/1
4) http://wielkopolska.policja.gov.pl/wlk/aktualnosci/171591,Jarocin-Zarzuty-za-ujawnienie-tajemnicy.html (dostęp: 17.01.2021)

w stosunku do przedsiębiorcy (…) wykorzystała we własnej działalności gospodarczej informacje stanowiące tajemnice przedsiębiorstwa w ten sposób, że po uzyskaniu od pokrzywdzonego istotnych informacji na temat przetargu (…) wzięła udział w przetargu, wygrywając go…[5]

Osoba, która w efekcie wygrała przetarg, będąc pracownikiem, miała dostęp do całości prac nad ofertą przetargową, w wyniku czego mogła przygotować ofertę „najkorzystniejszą" dla siebie.

Podobne incydenty dotyczą np. wykorzystania danych o kosztach utrzymania ciągu technologicznego i ofert składanych przez konkurentów obecnego dostawcy tej usługi, aby przygotować ofertę korzystniejszą, choć jedynie pozornie, precyzyjnie przygotowany wzrost niektórych składników kosztowych spowodował bowiem, iż już po roku faktyczne koszty tej usługi były większe. Mechanizm ten można niestety zastosować także w innych obszarach, np. zakup komponentów produkcyjnych czy sprzedaż wyrobów gotowych, a dotyczy on w takim samym zakresie wyrobów i usług.

Inny przykład. Ostatnimi czasy w serwisie społecznościowym rozgorzała dyskusja na temat nieuczciwych spedytorów przechodzących do konkurencji wraz z bazą klientów, a nawet – o zgrozo – praktyk niektórych firm transportowych, propagujących ten model działania i praktycznie wspierających pracowników w ich niecnym procederze[6]. Z moich doświadczeń – przede wszystkim w branży ochrony, ale nie tylko – wynika, że transfer informacji o klientach i warunkach współpracy z nimi jest niestety praktyką powszechną.

Złodziej „na pokładzie" to sytuacja trudna do zarządzania, gdyż taka osoba potrafi wysyłać komunikaty maskujące prawdziwy problem, a znając przedsiębiorstwo od środka, tworzyć obraz trudny do odszyfrowania, bo opierający się na znajomości nie tylko operacji, finansów i procedur, ale także relacji interpersonalnych, kiedy *wystarczy odpowiednią informację przekazać w odpowiedni sposób odpowiedniej osobie, aby osiągnąć odpowiedni skutek.* Czyli mówiąc wprost – wysłać impuls, kierując się znajomością sympatii i antypatii, i w ten sposób wykreować akceptację bądź odrzucenie oferty. Wydawałoby się, że w świecie wszechobecnych procedur takie działanie jest niemożliwe, ale niestety procedury są tworzone i realizowane przez ludzi, a oni wciąż nie są wolni od emocji. I nigdy nie będą wolni od ułomności. Procedury pomagają więc zabezpieczyć się przed złodziejem wewnętrznym, zmniejszając ryzyko związane z jego działalnością, ale go nie eliminują. Co należy zrobić? Połączyć procedury z zasadą wiedzy koniecznej i dywersyfikacją dostępu do informacji.

PERSPEKTYWA 3.
ZŁODZIEJ ODCHODZI OD NAS

Zdarza się również, że pracownik przygotowuje sobie „mocny start" u nowego pracodawcy i w tym celu kopiuje różne informacje, najczęściej *know-how,* ale też procedury, umowy, kalkulacje kosztów, plany marketingowe itp. To zjawisko nasila się wraz z negatywnym odbiorem swojej sytuacji przez pracownika bądź w czasach niepewności. Ostatnie **Badanie Nadużyć Gospodarczych** (EY) pokazuje, że w czasach kryzysowych (obecny kryzys COVID-19, doświadczenia z lat 2007–2008) nadużycia zdarzają się znacznie częściej[7]. W obszarze bezpieczeństwa informacji niezmiernie ważne jest zrozumienie istoty i wartości chronionego zasobu. Termin *know-how* jest tak pojemny, że dość często prowadzi do stanów skrajnych, które w praktyce już same w sobie mogą zagrażać bezpieczeństwu informacji. Można spotykać się np. ze skrajnym podejściem: *U nas tylko TO jest tajemnicą*. A bardzo często wystarczy przejrzeć kosze, wyciągnąć z nich kilka wadliwych wydruków i zadać sobie pytania: *Za ile kupiłaby to konkurencja?* albo *Czy takie informacje z konkurencyjnej firmy przydałyby się panu?,* aby dojść do wniosku, że tych tajemnic jest więcej. Drugim skrajnym, ale nie mniej groźnym stanem jest kwalifikowanie wszystkiego jako tajemnicy najwyższej rangi, co pracownicy często uważają za obsesję. W efekcie symulują ochronę informacji i z czasem proces ten zanika, ale bez świadomości kierownictwa, które jest święcie przekonane, że ochrona informacji cały czas jest na najwyższym poziomie. Dlatego tak istotne jest dobre zrozumienie wartości chronionych informacji i dobranie środków ochronnych adekwatnych do wartości. Dotyczy to rozwiązań zarówno fizycznych, technicznych i proceduralnych, jak i budujących świadomość pracowników. Ciekawym przykładem jest historia z województwa podlaskiego, pokazana w postaci wyciągu z wyroku.

W okresie od marca 2008 r. do 31 stycznia 2011 r. (…), działając w celu osiągnięcia korzyści majątkowej w postaci zatrudnienia w konkurencyjnym przedsiębiorstwie, poprzez wielokrotne kopiowanie na nośniki USB, uzyskała program komputerowy w postaci plików formatu E (Excel – przyp. autora) z zapisem równań służących do optymalizacji mieszanek paszowych[8]…

Jak widać, arkusz Excel, którego wiele osób nie identyfikuje jako *know-how,* może być zasobem wysokiej wartości, a nade wszystko bazą dającą przedsiębiorcy przewagę konkurencyjną. Zrozumienie tego mechanizmu jest kluczowe w tworzeniu efektywnego systemu ochrony informacji. Samo zrozumienie jednak nie wystarczy, potrzebne są procedura, zasada wiedzy koniecznej i dywersyfikacja dostępu do informacji.

PERSPEKTYWA 4.
TYLKO DO WASZEJ WIADOMOŚCI

Do pochylania się nad tym przykładem skłonił mnie post zamieszczony w jednym z serwisów społecznościowych. Przytaczam go w wersji nieco okrojonej, aby nie koncentrować uwagi na firmie czy miejscu zdarzenia, a jedynie na problemie, jakim jest nieświadomy i niekontrolowany ulot informacji.

Nie wiem, czy są tu pracownicy biura w (…), ale dzisiaj byłem w stanie bez większego problemu, stojąc na podwórku, przeczytać wasze maile i dokumenty z (…), które ktoś wyświetlał na ścianie naprzeciwko okna.

Pojęcie „ulot informacji" zaczerpnąłem z dziedziny kompatybilności elektromagnetycznej, ponieważ prace nad wykorzystaniem promieniowania elektromagnetycznego do uzyskiwania informacji z tych systemów już wiele lat temu doprowadziły do stworzenia urządzeń pozwalających zapoznać się z informacjami przetwarzanymi w de facto podsłuchiwanym systemie[9]. Efektem tych prac było także opracowanie standardu sprzętu odpornego na podsłuch elektromagnetyczny (Tempest) oraz różnego rodzaju kabin i wykładzin ekranujących pole elektromagnetyczne, chroniących przed ulotem informacji. Historia ulotu elektromagnetycznego powinna skłonić nas do myślenia o ulocie nieelektromagnetycznym. Bezpieczeństwo IT będzie bowiem bezużyteczne, jeśli wrażliwą treść wyświetlimy na ekranie, który osoba postronna będzie widziała, np. przez okno. Taki ulot informacji mamy też w wielu miejscach. Któż z nas nie widział osób pracujących na komputerze podczas podróży samolotem czy pociągiem, podczas pobytu w restauracji, poczekalni lotniskowej czy kolejowej, a nawet w miejscach publicznych.

Dotyczy to nie tylko informacji przetwarzanych w urządzeniach, ale także wydruków i rozmów, które w dobie IT security są często lekceważone. Kiedyś byłem świadkiem rozmowy dwóch grup, które omawiały swoje projekty. W pewnym momencie jeden z uczestników zorientował się, że sąsiedzi rozmawiają o tym samym przetargu: cenie, sposobie jej negocjacji, informacjach o konkurencji. Ulot informacji w pełnym wydaniu. Obie grupy szybko się przeniosły w bardziej odległe od siebie miejsca, nie zwracając uwagi na mnie, chociaż wciąż pozostawali w zasięgu mojego wzroku. A gdybym to ja był konkurentem obu grup albo osobą działającą na zlecenie innego konkurenta? Podjęte środki ochronne były niewystarczające zarówno przed ujawnieniem problemu, jak i po ujawnieniu. Wyposażony w mikrofon dobrej jakości uzyskałbym cenne informacje bez potrzeby zmiany miejsca. Co gorsza, dowiedziałbym się rzeczy z pewnością jeszcze bardziej wrażliwych, bo uczestnicy sądzili, że problem został rozwiązany, a to usypia czujność.

Ochrona informacji ma wiele wymiarów, często niewidocznych lub nieoczywistych, bo ukrytych w dźwięku, obrazie, kształcie, a nawet kolorze. To, co piszemy, rysujemy i mówimy, jest równie ważne, jak to, gdzie i jak to robimy, bo wielokrotnie nie trzeba podsłuchów ani specjalistów od szpiegostwa, aby tajemnice trafiły do konkurencji. Wystarczy nieświadomość. Być może prawdopodobieństwo takiej sytuacji jest znikome, ale jest jeszcze coś, o czym warto pamiętać, a co dotyczy każdego obszaru bezpieczeństwa.

PERSPEKTYWA 5.
TEORIA NIEPRZYPADKOWYCH PRZYPADKÓW

W ochronie informacji często spotykamy incydenty, w których przypadek wielokrotnie jest jedynym możliwym wytłumaczeniem wystąpienia zdarzenia. Oczywiście pozornie. Ciekawy incydent został przedstawiony wiele lat temu w artykule *Zaufany człowiek szefa.* Opisano w nim włamanie dotyczące informacji, przy czym skradzione informacje dotyczyły nie tylko operacji przedsiębiorstwa, ale także intymnej sfery prezesa zarządu. A kontekst zdarzenia wskazywał, że właśnie o nie chodziło[10].

I tu poruszamy temat bardzo istotny, gdyż informacje w różny sposób wrażliwe dla kierownictwa przedsiębiorstwa czy kluczowych pracowników także powinny być chronione, mogą bowiem zostać wykorzystane do uzyskania określonego zachowania osób, których te informacje dotyczą. Szantaż bezpośredni lub pośredni (osoba bliska osobie, na którą ktoś chce wpływać) jest w oddziaływaniu na środowiska biznesowe obecny także od dziesięcioleci. Historia IRA czy ETA jest nimi przepełniona. W tym kontekście zakres informacji posiadanych przez tzw. osoby zaufane jest istotny, a najważniejszym narzędziem pozwalającym chronić się przed zagrożeniem z tej strony są: procedura, zasada wiedzy koniecznej i dywersyfikacja dostępu do informacji.

Zarządzanie ryzykiem w ochronie informacji, podobnie jak w ochronie zasobów fizycznych, musi być faktyczne, funkcjonujące i w pełni efektywne. Realizowane zza biurka takie nie jest.

5) https://www.saos.org.pl/judgments/101154 (dostęp: 17.01.2021)
6) http://www.transport-manager.pl/2020/11/19/ukrocic-proceder-podkradania-spedytorow-wraz-z-baza-klientow-czyli-zatrudnie-spedytora-z-baza/ (dostęp: 17.01.2021)
7) https://www.ey.com/pl_pl/news/2020/06/covid-19-utrudnia-prowadzenie-przedsiebiorstwa-w-sposob-etyczny (dostęp: 17.01.2021)
8) https://sip.lex.pl/orzeczenia-i-pisma-urzedowe/orzeczenia-sadow/ii-aka-2-13-wykorzystanie-informacji-jako-znamie-521388419 (dostęp: 17.01.2021)
9) https://www.computerworld.pl/news/Bezpieczenstwo-fizyczne-infrastruktury-teleinformatycznej,320926,3.html (dostęp: 17.01.2021)
10) https://www.computerworld.pl/news/Zaufany-czlowiek-szefa,317266.html?amp=1 (dostęp: 17.01.2021)

JACEK GRZECHOWIAK

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

Nowości firmy Hanwha Techwin

4-kanałowy moduł wizyjny Wisenet ze zdalnymi głowicami kamerowymi

Nowy moduł kamerowy Wisenet PNM-9000QB jest przeznaczony do dyskretnej obserwacji bankomatów, sklepów i innych obiektów, w których niezbędny jest zakamuflowany system do wykrywania oszustw i kradzieży. Moduły wizyjne z obiektywami otworkowymi lub typu „rybie oko" o stałej ogniskowej można ukryć w ciasnych przestrzeniach, takich jak kioski bankomatowe, kabiny wind, narożniki pomieszczeń.

Sercem modułu jest chipset Wisenet7 Hanwha Techwin, który może jednocześnie przetwarzać obrazy z czterech głowic. Wymagany jest tylko jeden port w przełączniku sieciowym i tylko jedna licencja VMS.
Nowa kamera wyposażona w technologię Axis Zipstream z kodowaniem H.264 i H.265 zachowuje wszystkie istotne szczegóły, przy jednoczesnym zmniejszeniu zapotrzebowania na przepustowość i zasoby pamięci masowej. Wbudowane zaawansowane funkcje bezpieczeństwa zapobiegają nieautoryzowanemu dostępowi i chronią cały system. Podpisane oprogramowanie sprzętowe i funkcja „bezpieczny start" gwarantują, że oprogramowanie sprzętowe pozostanie nienaruszone.
Głowice kamerowe są połączone z ukrytym za ścianą modułem wizyjnym za pomocą specjalnych kabli i odseparowane od sieci IP, co jest korzystne dla większości użytkowników końcowych, którzy muszą chronić poufne dane klientów i przeciwdziałać oszustwom. Dodatkowym zabezpieczeniem jest funkcja wykrywania sabotażu (zakrycie obiektyw lub zmiana ustawienie dowolnej głowicy). Ta i inne funkcje, np. wykrywanie braku ostrości obrazu, detekcja ruchu w kadrze są zawarte w pakiecie oprogramowania Intelligent Video Analytics (IVA) wbudowanym w moduł kamerowy.
W chipsecie Wisenet7 zastosowano najnowszą wersję funkcji Extreme WDR 120 dB opracowaną przez Hanwha Techwin. Umożliwia to tworzenie ostrych i wyraźnych obrazów o rozdzielczości 2 Mpix z pełną częstotliwością odświeżania nawet w warunkach kontrastowego oświetlenia. Zastosowanie funkcji WiseStream II znacznie zmniejsza wymagania dotyczące pasma sieciowego podczas przesyłania obrazów do rejestratora. Dzięki temu nie ma potrzeby modernizacji sieci IP w istniejących kioskach bankomatowych.
Moduły PNM-9000QB mają dwa gniazda Micro SD do instalacji kart pamięci SDHC lub SDXC o łącznej pojemności do 512 GB.
Moduł kamerowy PNM-9000QB oferuje pracownikom ochrony bardzo bezpieczny i opłacalny sposób przeglądania bieżących obrazów lub tworzenia materiału wizyjnego dokumentującego przebieg wydarzeń w kioskach bankomatowych zainstalowanych na lotniskach, w bankach, hotelach, obiektach rekreacyjnych lub centrach handlowych – powiedział Uri Guterman, dyrektor ds. produktów i marketingu w Hanwha Techwin Europe.

Nowe sieciowe rejestratory wizyjne

Wielofunkcyjne rejestratory NVR zapisujące obrazy z kamer z szybkością do 400 Mb/s odczytują metadane tworzone przez kamery ze sztuczną inteligencją, dzięki czemu operatorzy systemów dozorowych mogą szybko i precyzyjnie odnajdywać poszukiwane obiekty na podstawie związanych z nimi atrybutów.

Wprowadzony na rynek w tym samym czasie i mający te same funkcje co XRN-6410B4 model XRN-3210B4 obsługuje 32 kanały, a 64-kanałowy rejestrator sieciowy XRN-6410DB4 dodatkowo wyposażono w zasilacz impulsowy SMPS w celu zapewnienia ciągłości rejestracji w systemach o znaczeniu krytycznym. Te trzy NVR-y są kompatybilne ze wszystkimi kamerami Wisenet z funkcjami analizy treści obrazu opartymi na sztucznej inteligencji i głębokim uczeniu.
Funkcje analityczne umożliwiają jednoczesne wykrywanie i klasyfikowanie różnych obiektów, m.in. ludzi, twarzy, pojazdów i tablic rejestracyjnych i są obsługiwane przez algorytmy AI Wisenet. Są one dostępne tylko w produktach Hanwha Techwin i potrafią określać cechy obiektów lub ludzi, m.in. grupę wiekową, płeć czy kolor odzieży. Pozwalają nawet ustalić, czy dana osoba nosi okulary lub trzyma torbę.
Kamery wspierane przez AI w połączeniu z nowymi NVR-ami dają operatorom i personelowi ochrony zaawansowane narzędzie do identyfikacji podejrzanych działań i możliwość szybkiego reagowania. Firmy z sektora detalicznego zyskują możliwość rejestrowania i analizy danych biznesowych, pomocne w określeniu przekroju demograficznego klientów, lepszym zrozumieniu ich zachowania i podniesieniu jakości obsługi.
Algorytmy AI bez problemów analizują dynamicznie zmieniające się obrazy w obiektach o dużym natężeniu ruchu, więc w obiektach handlu detalicznego takie rozwiązanie znacznie lepiej sprawdza się niż tradycyjne systemy analizy treści obrazu.
Nasze kamery ze sztuczną inteligencją, w połączeniu z nowymi rejestratorami sieciowymi, to przyszłościowe rozwiązania w wizyjnych systemach dozorowych, zapewniające funkcjonalność, o jakiej nikomu nie śniło się jeszcze kilka lat temu – mówi Uri Guterman. *Te produkty pomagają klientom wykorzystać wszystkie możliwości wizyjnego systemu dozorowego.*

Nowości od Axis

Kamera PTZ do transmisji na żywo

Wprowadzona na rynek w grudniu 2020 kamera sieciowa AXIS V5925 PTZ to wszechstronne i profesjonalne urządzenie do transmisji na żywo, łączące doskonałą jakość obrazu z płynnym sterowaniem PTZ, w tym trybem sportowym i scenicznym, a także studyjną jakością dźwięku. Idealnie sprawdzi się m.in. w salach lekcyjnych czy podczas halowych wydarzeń sportowych.

AXIS V5925 zapewnia doskonałą jakość obrazu w standardzie HDTV 1080p przy 60 kl./s i 30-krotnym zoomie optycznym, co pozwala z łatwością dostrzec wszystkie szczegóły. Oferuje tryb sceniczny i sportowy, zapewniając operatorowi lepszą kontrolę PTZ w różnych sytuacjach.
Wyjścia HDMI i 3G-SDI umożliwiają podłączenie kamery do większości profesjonalnych przełączników wizyjnych. Dzięki systemowi sterowania opartemu na VISCA RS-232 można ją łatwo zintegrować z istniejącymi już instalacjami audiowizualnymi.
Ponadto funkcja VISCA przez IP pozwala na zdalne sterowanie wieloma kamerami za pośrednictwem połączenia LAN. Dołączona 3-miesięczna licencja próbna aplikacji Camstreamer umożliwia transmisję na żywo do platform streamingowych, takich jak YouTube i Facebook Live, bezpośrednio z kamery przez sieć IP. Można także użyć dowolnego dostępnego oprogramowania do zarządzania materiałem wizyjnym lub po prostu podłączyć przez przeglądarkę internetową.
Nowa kamera wyposażona w technologię Axis Zipstream z kodowaniem H.264 i H.265 zachowuje wszystkie istotne szczegóły, przy jednoczesnym zmniejszeniu zapotrzebowania na przepustowość i zasoby pamięci masowej.
Wbudowane zaawansowane funkcje bezpieczeństwa zapobiegają nieautoryzowanemu dostępowi i chronią cały system. Podpisane oprogramowanie sprzętowe i funkcja „bezpieczny start" gwarantują, że oprogramowanie sprzętowe pozostanie nienaruszone i zostaną zainstalowane tylko aplikacje autoryzowane.

Kompaktowy rejestrator

Axis Communications pod koniec grudnia ub. roku wprowadziło na rynek rejestrator Axis S3008 — łatwe w montażu rozwiązanie do nagrywania obrazu w jakości Ultra HD, które współpracuje z oprogramowaniem do zarządzania materiałem wizyjnym Axis Companion.

Wysoko wydajny rejestrator jest wyposażony w przełącznik PoE obsługujący nawet 8 kamer, dysk twardy spełniający wymogi systemów dozoru wizyjnego i łącze gigabitowe do nagrywania wideo w jakości Ultra HD.
Rozwiązanie poddano intensywnym testom współpracy z szeroką gamą produktów Axis, by można było zapewnić łatwą rozbudowę systemu o dodatkowe urządzenia. Przykładowo, można dołączyć głośniki sieciowe służące do komunikacji z personelem i odstraszania ewentualnych intruzów, a także wideodomofony sieciowe umożliwiające identyfikację audiowizualną i zdalną kontrolę wejść.
Rejestrator AXIS S3008 Recorder zapewnia dostęp do materiałów wideo z dowolnego miejsca na świecie, dzięki zaawansowanej technologii Axis Secure Remote Access.

NAJWAŻNIEJSZE CECHY AXIS S3008 RECORDER:

- Kompaktowy rejestrator z wbudowanym przełącznikiem PoE
- Łatwa instalacja i obsługa
- Dysk twardy spełniający wymogi systemów dozoru
- Port USB do eksportowania materiałów wideo
- Do 5 lat gwarancji

Więcej informacji na stronie: www.axis.com/pl-pl.

VCS

Nowy początek

W WYNIKU ROZWOJU SPÓŁKI LINC POLSKA I STAŁEGO POSZERZANIA OFERTY PRODUKTÓW, A TAKŻE TRANSFORMACJI NA RYNKU ZDECYDOWALIŚMY SIĘ WYODRĘBNIĆ CZĘŚĆ ROZWIĄZAŃ DO ZASTOSOWAŃ MOBILNYCH I STWORZYĆ NOWĄ FIRMĘ, KTÓRA POZWOLI USYSTEMATYZOWAĆ DOTYCHCZASOWĄ AKTYWNOŚĆ I LEPIEJ WSPIERAĆ PAŃSTWA DZIAŁANIA W KAŻDYM ZAKRESIE.

VCS – Virtual CTRL Solutions jest dostawcą rozwiązań z zakresu ochrony technicznej, które mogą być zdalnie monitorowane i kontrolowane. Zdalne zarządzanie odbywa się za pomocą oprogramowania zainstalowanego w chmurze. Jednym z najważniejszych rozwiązań technicznych dostarczanych przez firmę są wieże do monitoringu wizyjnego iTower. Dzięki dużej różnorodności dostępnych rozwiązań możemy zrealizować nawet specyficzne wymagania klienta w zakresie monitoringu wizyjnego.
Wykorzystywana przez nas technologia dozoru wizyjnego pozwala na kontrolę dużych obszarów, takich jak place budowy, farmy fotowoltaiczne, tereny komercyjne czy miejsca organizacji imprez masowych. Obszary trudno dostępne czy częste zmiany lokalizacji dozoru nie stanowią żadnego problemu. Wieże łączą się z wieloma zdalnymi czujnikami, dzięki czemu rejestrują zdarzenia w czasie rzeczywistym. Mogą być wyposażone w panele słoneczne.
Oferujemy również produkty kontroli dostępu dla branży budowlanej, np. kontenery portierskie z kołowrotkami lub same kołowrotki wejściowe. Firmy budowlane mogą uniknąć strat, instalując właściwe ogrodzenia i kołowrotki. W ten sposób nadzorujemy dostęp, pozwalając na wejście tylko jednej upoważnionej osobie naraz, bez ryzyka, że nie zamknie ona drzwi za sobą lub ktoś inny o tym zapomni. Wszystkie wejścia i wyjścia na teren budowy są nadzorowane przez system kontroli dostępu.

Więcej na: www.vcs.pl

Kentix DoorLock

Inteligentny zamek

KENTIX DOORLOCK TO NOWOCZESNY ZAMEK UMOŻLIWIAJĄCY PEŁNĄ KONTROLĘ DOSTĘPU DO POMIESZCZENIA. ELASTYCZNOŚĆ TEGO ROZWIĄZANIA POZWALA STWORZYĆ SYSTEM DOSTOSOWANY DO INDYWIDUALNYCH POTRZEB. DZIĘKI POŁĄCZENIU ZABEZPIECZEŃ Z APLIKACJĄ POPRZEZ CHMURĘ KENTIX360 CLOUD DOSTAJEMY INFORMACJĘ, KTO I O KTÓREJ GODZINIE MA DOSTĘP DO DANEGO POMIESZCZENIA.

Zaletą zastosowania tej technologii jest także łatwe podłączenie do sieci. Modernizacja jest prosta i może być wykonywana bez użycia specjalnych narzędzi i ingerencji w drzwi.
Kentix DoorLock zawiera elementy bezprzewodowe oraz przewodowe, które można połączyć w jeden centralnie zarządzany system. W ten sposób, przy niewielkim nakładzie pracy, można wdrożyć skuteczną kontrolę dostępu.
Za pomocą przeglądarki internetowej można skonfigurować liczbę autoryzowanych użytkowników czy zdalnie odblokować drzwi, mając zawsze pod ręką cały rejestr wejść i wyjść.
Do konfiguracji nie jest wymagane żadne dodatkowe oprogramowanie. Dziennik dostępu pozwala na przeglądanie wszystkich uprawnień, w tym nieudanych prób odblokowania drzwi. Dzięki temu można w każdej chwili sprawdzić, kto wszedł do pomieszczenia. Za pomocą prostych funkcji filtrowania można ograniczyć dostęp do określonych dni, drzwi i użytkowników. To daje maksymalną elastyczność nawet w rozbudowanych systemach.
Można też zintegrować dowolne drzwi z kamerą IP. Wtedy obraz jest rejestrowany przy każdym odblokowywaniu wejścia lub wyjścia.
Materiał wideo jest zapisywany razem z odpowiednimi danymi użytkownika. Nieautoryzowane próby wtargnięcia są natychmiast zgłaszane za pomocą zdarzeń alarmowych lub powiadomień e-mail.

Więcej na: www.smart-i.pl

DS-KIS703-P

Minimum infrastruktury maksimum możliwości

W ofercie Hikvision pojawił się nowy zestaw wideodomofonowy dedykowany do zastosowań w budynkach jednorodzinnych, w których już położone okablowanie nie pozwala na użycie typowych systemów IP.

Zestaw składa się ze stacji bramowej, monitora i zasilacza, a jego instalacja została uproszczona do minimum. Wystarczy podłączyć zasilacz do monitora i połączyć go dwużyłowym kablem ze stacją bramową. Następnie należy uruchomić, z ekranu dotykowego, kreator, który w czterech prostych krokach pozwoli skonfigurować system. *Jednocześnie zestaw oferuje maksimum możliwości w postaci funkcji dostępnych w systemach IP: przekierowanie połączeń na aplikację Hik-Connect oraz podgląd obrazów z kamer IP na monitorze.*
Dużymi atutami stacji bramowej są: wyjście zasilające 12 VDC/1 A pozwalające na zasilanie elektrozamków oraz wbudowane dwa przekaźniki do obsługi furtki i bramy. Uniwersalność zestawu podkreślają dostarczone w komplecie akcesoria do montażu stacji bramowej zarówno natynkowo, jak i podtynkowo.

Więcej informacji znajduje się na na www.hikvision.com/pl

Nowe biuro Genetec w Wiedniu

Firma Genetec, globalny dostawca zunifikowanych technologii i rozwiązań w zakresie zabezpieczeń, bezpieczeństwa publicznego i *business intelligence,* otworzyła w Wiedniu swoje 16. na świecie biuro. Lokalizację tę wybrano, aby rozwijać działalność w Europie Środkowej oraz w krajach DACH. Biuro będzie też wspierać szybko rozwijające się zespoły badawczo-rozwojowe oraz regionalne zespoły sprzedażowe.

Dzięki wielojęzycznej kadrze reprezentującej osiemnaście narodowości austriacki zespół stanowi unikatową mieszankę różnych kultur i pomysłów. Po przejęciu austriackiej firmy KiwiSecurity zajmującej się analizą wizyjną wiedeński zespół badawczo-rozwojowy skoncentruje się na wielu obszarach, w tym na rozwiązaniach do analizy wizyjnej pod kątem prywatności. Umożliwi to klientom zachowanie prywatności przy jednoczesnym zwiększeniu bezpieczeństwa i wydajności operacyjnej.
Nowe biuro w Wiedniu zapewni nam doskonałą platformę do dalszego rozszerzania obecności w Europie Środkowej i utrzymania stałego wzrostu w całej Europie i na świecie – powiedział Cyrille Becker, dyrektor generalny na Europę w Genetec Inc. – *Chociaż w tej chwili wszyscy bezpiecznie pracują z domu, nowe biuro wesprze naszą długoterminową strategię wzrostu, aby lepiej spełniać potrzeby naszych partnerów dystrybucyjnych, użytkowników końcowych i potencjalnych klientów w regionie.*

Centrum kultury na Ursynowie

z kompleksowym systemem oddymiania D+H

Dzielnicowe Centrum Kultury na Ursynowie przyciąga wzrok nieregularną fasadą, przypominającą pogniecioną kartkę. Nowoczesna bryła w połączeniu z przestronnymi jasnymi wnętrzami wprowadza nową jakość do tej kategorii budynków. Jako obiekt użyteczności publicznej, musi posiadać adekwatne zabezpieczenia przeciwpożarowe. Ważną rolę odgrywa system oddymiania.

W DCK na Ursynowie zastosowano kompleksowy system oddymiania D+H. Okna w świetlikach wyposażono w 24 napędy ZA 155/800-HS, dzięki czemu w razie pożaru otwierają się automatycznie i dają ujście dla dymu oraz trujących gazów. Ma to zapewnić bezpieczne drogi ewakuacyjne i ograniczyć rozprzestrzenianie się pożaru. Do napowietrzania wykorzystano okna pionowe uzbrojone w napędy łańcuchowe KA 34/1000. System oddymiania D+H obejmuje także elementy sterujące, m.in. panelowe centrale oddymiania RZN 4316-E9 czy przyciski RT 45 pozwalające na uruchomienie alarmu przez użytkowników obiektu.
System oddymiania jest wykorzystywany nie tylko w razie pożaru. Na co dzień okna wyposażone w napędy mogą być otwierane w celu wentylowania budynku. Odpowiednia cyrkulacja świeżego powietrza i możliwość regulowania temperatury bez obciążania klimatyzacji mechanicznej to podstawowe korzyści takiego rozwiązania.

AJAX

Otrzymuj potwierdzenia alarmów w Hub 2 za pomocą foto weryfikacji w MotionCam

1700 m

Korzysta z komunikacji radiowej

Wykrywa intruza już z 12 m

Po alarmie wysyła animowaną serię zdjęć

Widzi w ciemności

Ignoruje obecność zwierząt

Integracja z

SAFESTAR security cloud

kronos

Darmowe aplikacje dla instalatorów i użytkowników końcowych

www.ajax.systems

macOS | Windows | iOS | Android