CZASOPISMO RYNKU SECURITY

№ 06
2020 (24)
listopad /grudzień

a&S POLSKA

Raport i ranking największych firm security na świecie

WARSAW SECURITY SUMMIT 2020 ONLINE → 14

W nowej formule Content Hub

Kompendium wiedzy o bezpieczeństwie do obejrzenia w dogodnym miejscu i czasie. Filmy, wzorem serwisów VoD, są dostępne bezpłatnie przez rok od dnia premiery (17.11.2020).

RYNEK SECURITY → 48

Normy na systemy kontroli dostępu

Planowanie elektronicznych systemów kontroli dostępu wymaga znajomości szczegółowych wymagań i zasad stosowania według nowych norm. Pierwsza z nich jest już dostępna w wersji polskiej.

BEZPIECZEŃSTWO HOTELI I INSTYTUCJI FINANSOWYCH → 76

Hotele klasy premium

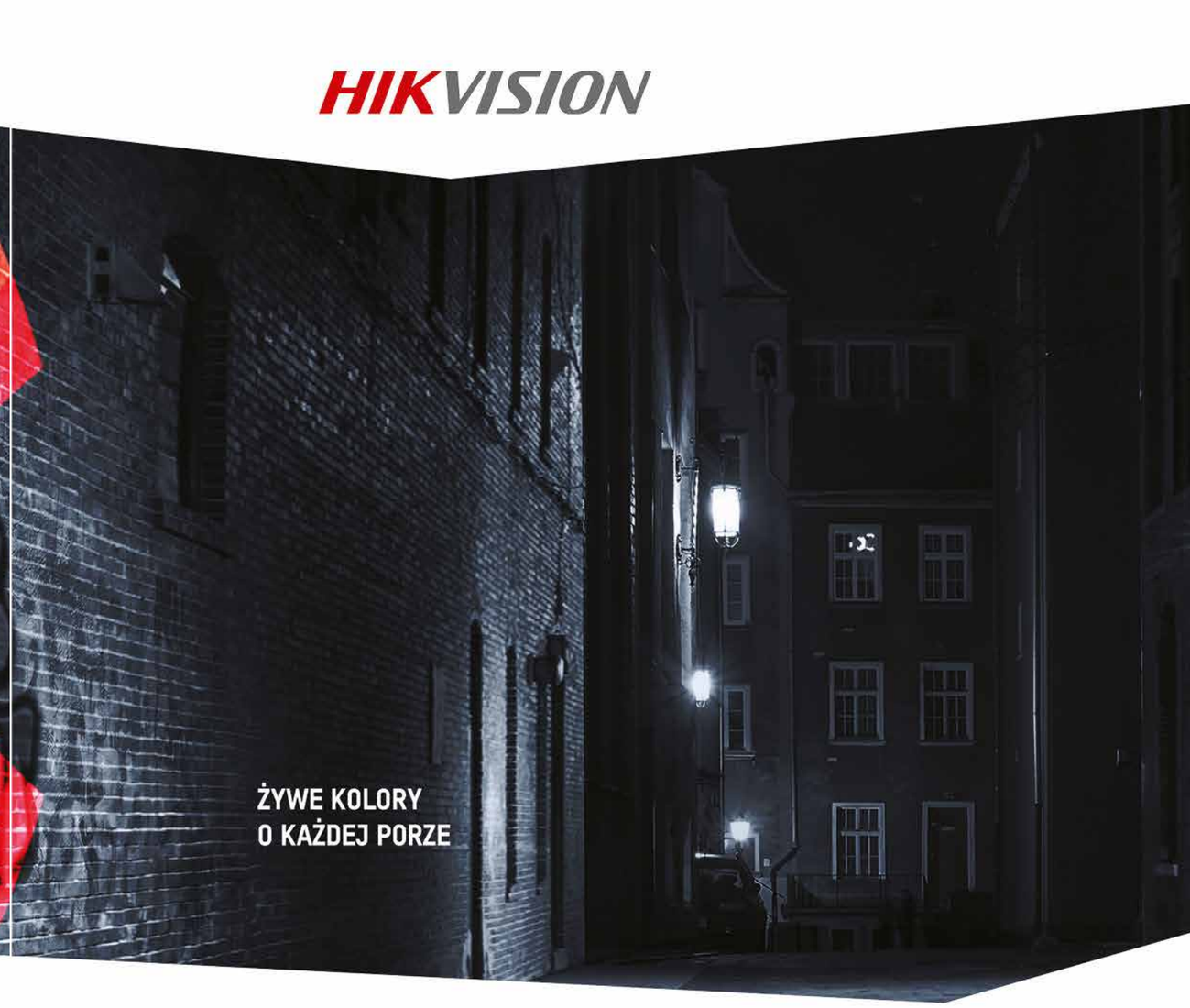
Które hotele przetrwają czas pandemii i wrócą do biznesu? Odpowiedź na to pytanie jest prosta – przede wszystkim bezpieczne! Z certyfikatem jakości i bezpieczeństwa.

15 zł
(w tym 8% VAT)

ISSN 2451-5175
05
9 772451 517703

www.aspolska.pl

HIKVISION



TECHNOLOGIA COLORVU
ŻYWE KOLORY, NAWET W CIEMNOŚCI

Ciesz się żywym, kolorowym obrazem przez całą dobę, dzięki technologii ColorVu

Hikvision to międzynarodowy lider w dostawie produktów i rozwiązań monitoringu wizyjnego. Nowa technologia ColorVu zapewnia jasne, kolorowe obrazy nawet w otoczeniu pozbawionym światła. Lepsze soczewki, bardziej zaawansowane czujniki i dodatkowe miękkie oświetlenie dają obraz świetnej jakości, nawet w ciemności.

ColorVu

DOŁĄCZ DO PROGRAMU PARTNERSKIEGO HIKVISION I UZYSKAJ DOSTĘP DO WIELU KORZYŚCI.
https://partner.hikvision.com/

Hikvision Poland
Żwirki i Wigury 16B
02-092 Warszawa
T +48 22 4600150
info.pl@hikvision.com

@HikvisionPoland
www.hikvision.com/pl/

EDYTORIAL

Drodzy Czytelnicy

W wydaniu listopadowo-grudniowym tradycyjnie już prezentujemy obszerny raport nt. kondycji największych firm branży zabezpieczeń na świecie (s. 18) oraz ranking Security 50 (s. 42). W 2019 r. firmy z tego zestawienia odnotowały średni wzrost o 9,3 proc. w stosunku do 2018 r. Pandemia COVID-19 zakończyła wzrostową krzywą przychodów trwającą całą ostatnią dekadę (s. 20). Teraz branża zabezpieczeń doświadcza czegoś, czego nigdy wcześniej nie notowała – spośród 34 firm z rankingu, które ujawniły swoje przychody za okres od stycznia do czerwca 2020 r., spadki odnotowało aż 27, a tylko siedem firm osiągnęło wzrost. Najbardziej ucierpiały sektory handlu detalicznego, transportu i edukacji. Ale są i takie rynki wertykalne, które radzą sobie stosunkowo dobrze również podczas COVID-19. W dalszym ciągu w zabezpieczenia inwestują segmenty: e-commerce, technologiczny, służba zdrowia, FMCG i produkcja dóbr podstawowych (s. 24). Kamery termowizyjne, bezkontaktowa kontrola dostępu i analityka wizyjna cieszyły się zainteresowaniem większym niż kiedykolwiek (s. 34).
Analiza tegorocznego Security 50 pokazuje, że do końca 2019 r. branża rozwijała się w dobrym tempie. Wojna handlowa między USA a Chinami wywarła negatywny wpływ na chińskie firmy, ale większość skutków zrównoważył silny popyt wewnętrzny w Państwie Środka (s. 44). Sektor dozoru wizyjnego jest cały czas zdominowany przez kilka dużych marek i trend ten powinien się utrzymać (s.38, 46).

Ukazała się w wersji polskiej norma na systemy kontroli dostępu dotycząca ich budowy. Druga jej część – wytyczne stosowania – wkrótce zostanie przetłumaczona. Nowe normy wprowadziły stopnie zabezpieczenia przypisane poszczególnym funkcjonalnościom każdego przejścia kontrolowanego (s. 48). Swoimi doświadczeniami w projektowaniu systemów KD dzieli się doświadczony inżynier uruchomieniowy, omawiając wciąż lekceważone podstawy ich planowania (s. 52).

Tym razem temat bezpieczeństwa instytucji finansowych prezentujemy nieszablonowo, zwracając uwagę na podmioty, które nie mieszczą się ściśle w tym sektorze, a przechowują (przewożą) wartości pieniężne. One także są przedmiotem zainteresowania środowisk przestępczych. Spojrzenie przez pryzmat incydentów kryminalnych jest nie tylko ciekawe, ale też pouczające (s. 68).

Sytuacja epidemiczna zweryfikowała nasze plany związane z organizacją stacjonarnej konferencji Warsaw Security Summit. Dlatego na nowe czasy zaproponowaliśmy jej nową formułę – Content Hub. Wzorem serwisów VoD prelekcje, prezentacje i rozmowy stanowiące kompendium wiedzy o bezpieczeństwie są do obejrzenia na stronie **www.WarsawSecuritySummit.online**. Będą dostępne bezpłatnie przez rok od dnia premiery (17.11.2020). Materiały wideo zostały pogrupowane wg działów tematycznych, można je też oglądać kolejno, wybierając całą playlistę. Cieszy nas, że ta formuła znalazła uznanie wśród oglądających. Już w pierwszym tygodniu stronę odwiedziła rekordowa liczba ponad 1000 gości!

Marta Dynakowska
REDAKTOR NACZELNA

Jan T. Grusznic
Z-CA REDAKTORA NACZELNEGO

Mariusz Kucharski
DYREKTOR ZARZĄDZAJĄCY

A&S POLSKA

www.aspolska.pl

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 marketingu i reklamy
Iwona Krawiec

Dział eventów i konferencji
Jolanta A. Kucharska
Aleksandra Czapska

Projekt graficzny i skład
Kalwala Studio

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

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

Prenumerata
www.aspolska.pl/prenumerata

SPIS TREŚCI

№ 06

2020 (24)

listopad / grudzień

a&S POLSKA

AXIS COMMUNICATIONS

www.axis.com/pl

Pierwsza kamera Axis łącząca AI i *deep learning*

Axis Communications wprowadza na rynek kamerę AXIS Q1615 Mk III z analityką opartą na sztucznej inteligencji, wykorzystującą mechanizmy głębokiego uczenia *(deep learning)*. Ta zaawansowana stałopozycyjna kamera typu box zawiera innowacyjny podwójny chipset, który umożliwia klasyfikację obiektów z dużą dokładnością.

Dzięki chipsetowi – łączącemu procesor **Axis ARTPEC-7** oraz jednostkę przetwarzającą z technologią głębokiego uczenia – kamera udostępnia wyjątkowe, oparte na sztucznej inteligencji funkcje klasyfikacji obiektów. Ponadto fabrycznie zainstalowana aplikacja analityczna **AXIS Object Detector** potrafi rozróżnić takie rodzaje pojazdów, jak rowery, samochody osobowe, autobusy czy samochody ciężarowe.

Analizy mogą być wykonywane bezpośrednio w kamerze, co zwiększa szybkość działania i skalowalność systemu. Przez sieć przesyłany jest tylko niezbędny materiał wizyjny. Ogranicza to zapotrzebowanie na pamięć masową i przepustowość oraz zmniejsza obawy dotyczące prywatności. Inne korzyści: przetwarzanie w czasie rzeczywistym, redukcja kosztów i łatwość obsługi.

Axis wykorzystuje sztuczną inteligencję także w innych swoich rozwiązaniach, np. w aplikacji **AXIS Parking Violation Detection** automatycznie wykrywającej nieprawidłowości w parkowaniu i wysyłającej alarm po każdym wykryciu potencjalnego naruszenia przepisów. Umożliwia to policji lub innym służbom szybkie podejmowanie odpowiednich działań, takich jak odholowanie pojazdu lub wystawienie mandatu.

BCS

www.bcscctv.pl

Autonomiczny terminal do pomiaru temperatury BCS-TKD-AT1

W obecnych czasach coraz częściej poszukiwane są rozwiązania kontroli dostępu umożliwiające otwarcie przejścia metodą bezdotykową. Do tego typu urządzeń należy BCS-TKD-AT1. Jest to autonomiczny terminal kontroli dostępu z wbudowanym czytnikiem kart oraz z autoryzacją biometryczną (rozpoznawanie twarzy).

Oprócz możliwości związanych z kontrolą dostępu terminal realizuje również wiele dodatkowych funkcji, łącząc jednocześnie zalety zarówno wideodomofonu TCP/IP/SIP, jak i kamery monitoringu – obraz z kamery może być nagrywany w rejestratorze. Terminal obsługuje detekcję ruchu, jest zgodny ze standardem Onvif.

Najciekawszą funkcjonalnością jest jednak możliwość pomiaru temperatury osoby wchodzącej za pomocą wbudowanej kamery termowizyjnej, z dokładnością +-0,5°C. Wynik pomiaru jest na bieżąco wyświetlany na wbudowanym zakrzywionym ekranie LCD o przekątnej 7".

Urządzenie wyposażono również w funkcję detekcji maseczki na twarzy i w razie jej braku można, wykorzystując dedykowane do tego wejścia/wyjścia alarmowe i przekaźnikowe, przesłać sygnał do innych systemów. Terminal może być montowany zarówno na ścianie, jak i na biurku lub bezpośrednio na podłodze, z wykorzystaniem specjalnego stojaka. Więcej szczegółów znajduje się na stronie www.bcscctv.pl.

DAHUA TECHNOLOGY POLAND

www.dahuasecurity.com/pl

DSS Pro – VMS do zadań specjalnych

Branża security podlega nieustannym przemianom. Wprawdzie nadal obserwuje się ogromną popularność systemów telewizji dozorowej czy kontroli dostępu, ale też coraz częściej spotykanym wymogiem jest integracja tych systemów. Ma ona na celu zarówno umożliwienie centralnego zarządzania takimi instalacjami, jak i ułatwienie pracy operatorom dzięki np. automatyzacji pewnych procesów czy zdarzeń alarmowych.

Rynek obfituje w różne rozwiązania pozwalające osiągnąć ten cel, jednak integracje realizowane przy użyciu natywnego oprogramowania producenta danych urządzeń niejednokrotnie działają najbardziej przewidywalnie i stabilnie. I taki też zamysł stoi za aplikacją **DSS Pro**.

DSS Pro to zaawansowane oprogramowanie typu **VMS** *(Video Management System)*. Oczywiście umożliwia ono integrację nie tylko systemów wizyjnych – na liście wspieranych rodzin produktów są systemy kontroli dostępu, wideodomofony, ściany wizyjne czy systemy alarmowe. **DSS** pozwala na pracę serwerów w redundantnym trybie **N+M,** co znacznie zwiększa niezawodność i stabilność całej instalacji.

Możliwość obsługi do 2000 kanałów na serwer oraz pokaźne pasmo 600 Mb/s predestynuje to rozwiązanie dla najbardziej wymagających klientów.

System wspiera wszelkie nowoczesne technologie – rozpoznawanie twarzy, odczyt tablic rejestracyjnych, zaawansowaną ochronę perymetryczną, mapy ciepła czy niezwykle ostatnio popularne systemy do pomiaru temperatury ludzkiego ciała. **DSS Pro** to przykład zaawansowanego rozwiązania typu **All-In-One**.

PRODUKT NUMERU

HANWHA www.hanwha-security.eu

Kamery Wisenet X z najnowszym chipsetem Wisenet 7

Firma Hanwha Techwin wprowadziła do oferty serię kamer Wisenet X wyposażonych w najnowszy chipset Wisenet 7.
Nowa seria charakteryzuje się rozdzielczością 6 lub 8 Mpix , w zależności od modelu, oraz zaawansowanymi funkcjami przetwarzania obrazu, które pozwalają na uzyskanie bardzo dobrej jakości obrazu niemal w każdych warunkach oświetleniowych. Wbudowane funkcje, takie jak ***extreme WDR,*** detekcja i kompensacja zamglenia, stabilizacja obrazu na podstawie danych z czujnika żyroskopowego, to jedynie niektóre z opcji. Kamery sieciowe z układem Wisenet 7 są idealnym rozwiązaniem dla obiektów i instytucji, w których szczególny nacisk kładzie się na cyberbezpieczeństwo.
Wisenet 7 wyposażono w zaawansowane mechanizmy chroniące kamerę oraz infrastrukturę sieciową, wśród których wyróżnić można m.in. opcję bezpiecznego uruchomienia kamery, osobny system realizujący funkcje szyfrowania/odszyfrowywania aplikacji czy zabezpieczenie interfejsów JTAG oraz UART. Bezpieczeństwo kamer **Wisenet 7 X** jest potwierdzone certyfikatem UL CAP oraz standardem ***Secured by Default.***
Nowy, wydajny chipset Wisenet 7 daje również większe możliwości w zakresie inteligentnej analizy obrazu. Rozbudowane algorytmy pozwalają na jeszcze skuteczniejszą detekcję osób i stosowanie dodatkowych filtrów, takich jak wejście/wyjście do strefy, przekroczenie linii (z rozpoznaniem kierunku poruszania się) czy automatyczne śledzenie wskazanej osoby w kamerach szybkoobrotowych **PTZ**.

HIKVISION www.hikvision.com/pl

Hikvision Solar Panel Kit

Hikvision wprowadza na rynek zupełnie nowy, przełomowy produkt. Firma zaprezentowała autonomiczny zestaw zawierający wszystko, czego potrzeba, aby uruchomić niezawodny system bezpieczeństwa w dowolnym niemal miejscu – kamerę, panel solarny, baterię, uchwyt oraz akcesoria.
Takie rozwiązanie może być stosowane w miejscach, w których nie można ułożyć sieci kablowych lub w których panują trudne warunki środowiskowe, a urządzeniu stawia się wysokie wymagania stabilności pracy.
System może być używany do monitorowania sieci elektrycznej, wodno-rzecznej, rurociągów naftowych, gospodarstw rolnych czy obszarów leśnych. Może być również stosowany w miejscach wymagających tymczasowego monitoringu, takich jak zawody sportowe, zgromadzenia publiczne, tymczasowa kontrola ruchu czy budowy miejskie.

Całkowicie naładowana bateria zapewnia działanie systemu do siedmiu dni w deszczowe lub pochmurne dni.
Zestaw zawiera **moduł fotowoltaiczny 40W** i akumulator litowy wielokrotnego ładowania **20 Ah**. Użytkownik obsługuje zarządzanie baterią, ma możliwość wyświetlania stanu baterii oraz ochronę baterii przed niską temperaturą.
Ponadto system wykorzystuje bezprzewodową transmisję sieciową **LTE-TDD / LTE-FDD / WCDMA / GSM 4G i obsługuje karty micro SIM**. I co ważne – system jest wodoodporny i pyłoszczelny (**klasa IP67**).

JOHNSON CONTROLS www.jci.com

Nowa platforma SSWiN i automatyki domowej: Qolsys IQ Panel2+

W pierwszym kwartale 2021 roku firma Johnson Controls, właściciel marek DSC i Visonic, wprowadzi na polski rynek nową platformę SSWiN oraz automatyki domowej: Qolsys IQ Panel2+.
Najnowsza technologia radiowa **PowerG**, system popularnej automatyki **Z-Wave**, podwójna łączność **Wi-Fi + LTE**, wbudowana kamera **5 Mpix** oraz czujnik zbicia szkła – to wszystko w nowoczesnej centrali **IQ Panel 2+**, będącej jednocześnie dotykowym ekranem **HD 7".**
Intuicyjna obsługa gestami, jak w smartfonach, oraz dopracowana w najdrobniejszych szczegółach aplikacja mobilna alarm.com pozwalają na wygodną obsługę systemu. Centrala **IQ Panel 2+** będzie miała możliwość podłączenia do zainstalowanego już systemu przewodowego. W tym celu będzie stosowany specjalny moduł wejść przewodowych z transmisją sygnałów **PowerG**. Sterowanie elementami **SMART HOME** będzie się odbywać przy użyciu elementów wykonawczych **Z-Wave**.
Praca inżynierów **Qolsys** pozwoliła na połączenie termostatów, oświetlenia, sterowników bram i drzwi, kamer IP i wideodomofonów z czujnikami **PowerG** w jeden zintegrowany system. Nigdy dotąd nie było tak kompletnego, łatwego w obsłudze panelu. **IQ Panel 2+** to urządzenie, które pozwoli na bezobsługową automatykę, zdalny kontakt z dziećmi, podgląd kamer IP, wideodomofonów czy zdalną rozmowę z kurierem stojącym przed drzwiami. To wszystko będzie możliwe dzięki aplikacji mobilnej alarm.com.
Więcej przedpremierowych informacji na temat **IQPanel2+** można uzyskać, kontaktując się na adres e-mail: **mariusz.banach@jci.com.**

LINC POLSKA www.linc.pl

ADPRO eFT – najwyższa jakość ochrony

ADPRO eFT (eco FastTrace), platforma wideo oparta na systemie operacyjnym XO 4.5 Security+, to nowość w rodzinie rejestratorów ADPRO NVR+ poszerzająca dość obszerną listę funkcji platform NVR+ ADPRO. Jest synonimem wysokiej jakości, stabilności działania i wielu innych usług w jednym rozwiązaniu IP.
System XO 4.5 w powiązaniu z rozwiązaniami **eFT** wspiera od 8 do 16 kanałów IP i do 8 kanałów analityki wizyjnej jednocześnie. Użytkownik może wykorzystać analitykę do detekcji wtargnięć i wałęsania się. Ma też większe możliwości zdalnego zarządzania obiektem.
Dzięki natychmiastowej i wielopoziomowej reakcji obejmującej m.in. dwukierunkową transmisję dźwięku, zdalną obsługę oświetlenia i/lub systemu KD można szybko zareagować i zniwelować zagrożenie.
Jest to pierwsze rozwiązanie technologiczne z inteligentną i dokładną detekcją, o wysokiej niezawodności i atrakcyjnej cenie, skutecznie zwiększające bezpieczeństwo pracownika ochrony. To jedno z niewielu rozwiązań na rynku oferujące w pełni zdalny dostęp do takich funkcji rejestratora, jak uzbrajanie/rozbrajanie, zdjęcia w formacie **QUAD** i wysoką stabilność działania poprzez własny protokół komunikacyjny. Dodatkowo aplikacja mobilna iTrace gwarantuje zdalny dostęp **24/365**, z każdego miejsca na świecie.
Platforma ADPRO eFT optymalizuje wykorzystanie przepustowości łącza w celu uzyskania wysokiej jakości transmisji z wielu kamer. Nowa aplikacja Xchange2 umożliwia łatwe dodawanie licencji analizy wizji do urządzenia.
Więcej szczegółów znajduje się na **www.linc.pl.**

SCHRACK SECONET POLSKA www.schrack-seconet.pl

Integral Remote – narzędzia zdalnego dostępu

Integral Remote to pakiet aplikacji IP pozwalających na zdalne nadzorowanie, zarządzanie oraz obsługę systemów sygnalizacji i pożarowej firmy Schrack Seconet. Jego zalety dostrzegają zarówno inwestorzy, zarządcy, integratorzy, jak i osoby obsługujące i serwisujące instalacje sygnalizacji pożarowej.

Wszystkie dane oraz dostęp do aplikacji są chronione wielopoziomowo, a dodatkowe bezpieczeństwo zapewnia realizowanie wszystkich połączeń w ramach pakietu poprzez połączenia szyfrowane oraz certyfikowane tunele VPN.

W SKŁAD PAKIETU WCHODZĄ:

1. Integral Application Center – pakiet przeznaczony dla programistów i instalatorów systemu Integral IP.
2. Integral Desktop – przeznaczony do obsługi oraz nadzorowania instalacji na komputerach stacjonarnych. Program wyświetla odwzorowany 1:1 panel obsługi centrali sygnalizacji pożarowej Integral IP.
3. Integral Mobile/Integral Browser – aplikacja odwzorowuje panel centrali Integral IP na urządzeniach mobilnych oraz wspiera technologię aktywnych powiadomień *(push notification)*.
4. Integral Message – przeznaczony do zdalnego nadzorowania wielu niezależnych instalacji sygnalizacji pożarowej Integral IP podłączonych do serwera systemu, który wraz ze stanowiskami operatorskimi stanowi centrum nadzoru,
5. Integral Mail – umożliwia wysyłanie e-maili bezpośrednio z centrali SSP, która łącząc się z dedykowanym serwerem pocztowym, wysyła informacje o najważniejszych zdarzeniach w systemie Integral IP.

TP-LINK www.tp-link.com.pl

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

Przełącznik TL-SF1006P został zaprojektowany specjalnie z myślą o systemach monitoringu wizyjnego IP. Dzięki zgodności ze standardem 802.3af/at PoE+ instalacja systemu jest łatwa, bezpieczna i mniej kosztowna. Zastosowanie trybu **Extend** zwiększa zasięg transmisji **PoE** nawet do 250 m, tak więc **TL-SF1006P** jest doskonałym rozwiązaniem w przypadku rozmieszczania kamer IP na dużym obszarze. **TL-SF1006P** oferuje do 30 W mocy na każdym porcie **PoE**. Łączna moc 67 W przełącznika wyposażonego w 6 portów **RJ45 10/100 Mb/s**, w tym **4 porty PoE+** sprawia, że jest to rozwiązanie idealne dla systemów monitoringu wizyjnego małych firm. Gdy całkowity pobór mocy przekracza 67 W, funkcja inteligentnego zarządzania zużyciem energii wyłącza zasilanie portu o najniższym priorytecie, żeby zapewnić zasilanie portów o wyższych priorytetach i tym samym chronić urządzenie przed przeciążeniami.
Portom 1–2 można nadawać wyższe priorytety za pomocą trybu Priority uruchamianego jednym kliknięciem, co gwarantuje wysoką jakość aplikacji wrażliwych na opóźnienia, takich jak rejestracja materiału wideo.

Przełącznik **TL-SF1006P** nie wymaga konfiguracji czy instalacji. Wystarczy wpiąć go do zasilania i podłączyć do niego urządzenia końcowe. Urządzenie jest gotowe do pracy.
Produkt został objęty 5-letnią gwarancją producenta.

Warsaw Security Summit

2020 CONTENT HUB ONLINE

TO WIĘCEJ NIŻ KONFERENCJA!
TO NOWATORSKA FORMUŁA CONTENT HUB

DEBATA EKSPERCKA, PRELEKCJE,
PREZENTACJE, ROZMOWY I WYWIADY
DO OBEJRZENIA W DOGODNYM MIEJSCU I CZASIE.
WZOREM SERWISÓW WIDEO NA ŻĄDANIE (VoD)
FILMY SĄ DOSTĘPNE BEZPŁATNIE I W DOWOLNYM
CZASIE PRZEZ ROK OD DNIA PREMIERY (17.11.2020) .
SAM DECYDUJESZ: CO, KIEDY
I W JAKIEJ KOLEJNOŚCI OBEJRZYSZ...

TEMATYKA

PARTNERZY

PARTNER PLATINUM

AXIS COMMUNICATIONS

PARTNER GOLD

Genetec™

PARTNERZY SILVER

elacompil · Polski Związek Pracodawców Ochrona · SECURITAS · TRUSTMAN www.trustman.pl · VCS

PARTNER MEDIALNY

BANES24

OBEJRZYJ W DOWOLNYM CZASIE

WYBIERZ CO CIĘ INTERESUJE

2020 CONTENT HUB ONLINE

KOMPENDIUM WIEDZY O BEZPIECZEŃSTWIE

BEZPIECZEŃSTWO W CZASACH POST-COVID

**DEBATA EKSPERCKA
WYWIADY
REPORTAŻE**

BEZPŁATNY DOSTĘP ONLINE PRZEZ ROK

ZOBACZ ONLINE

SKANUJ KOD

WarsawSecuritySummit.online

Warsaw Security Summit

















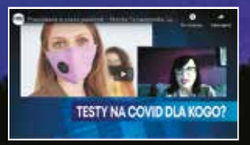


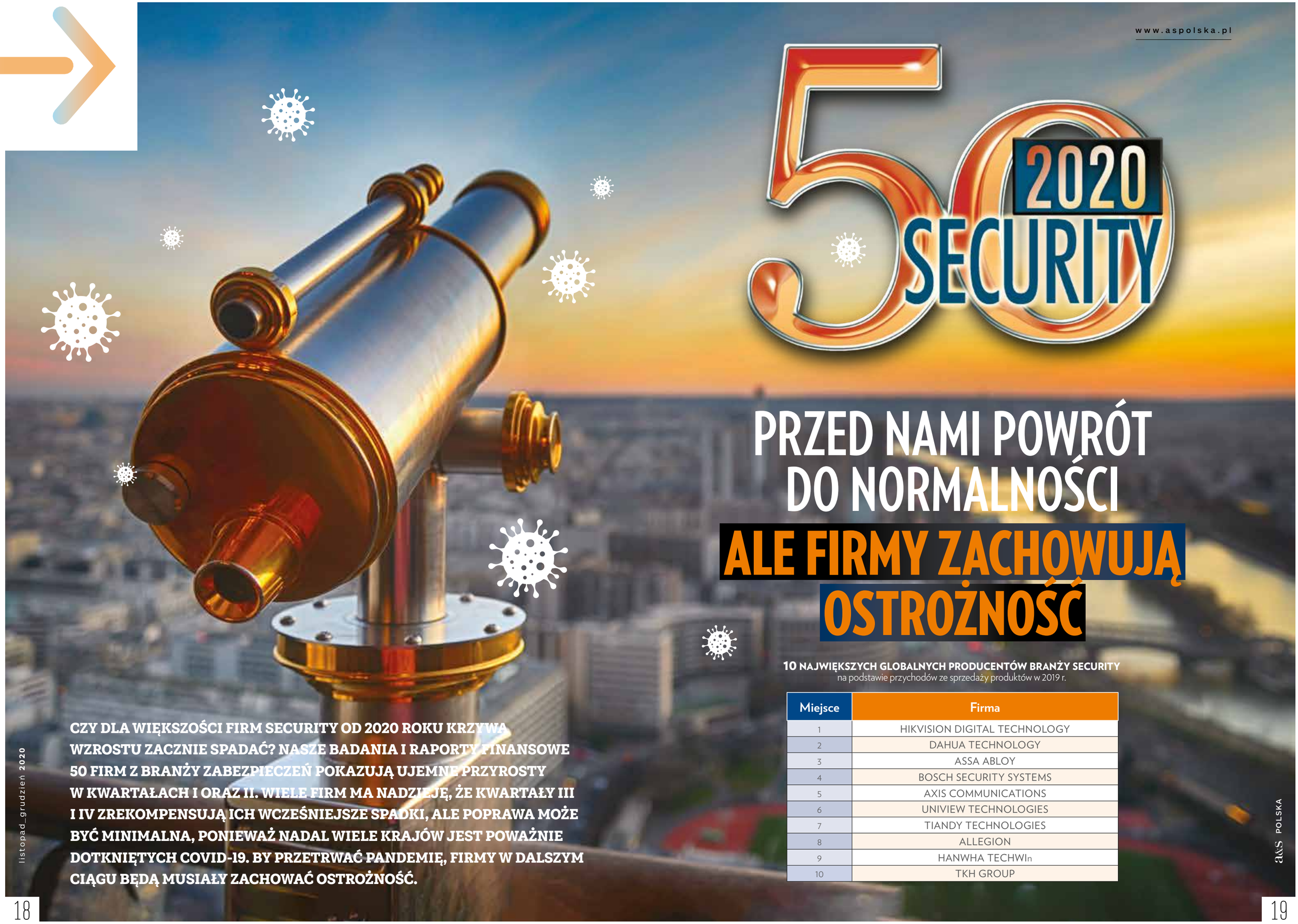








50 2020 SECURITY

PRZED NAMI POWRÓT DO NORMALNOŚCI

ALE FIRMY ZACHOWUJĄ OSTROŻNOŚĆ

CZY DLA WIĘKSZOŚCI FIRM SECURITY OD 2020 ROKU KRZYWA WZROSTU ZACZNIE SPADAĆ? NASZE BADANIA I RAPORTY FINANSOWE 50 FIRM Z BRANŻY ZABEZPIECZEŃ POKAZUJĄ UJEMNE PRZYROSTY W KWARTAŁACH I ORAZ II. WIELE FIRM MA NADZIEJĘ, ŻE KWARTAŁY III I IV ZREKOMPENSUJĄ ICH WCZEŚNIEJSZE SPADKI, ALE POPRAWA MOŻE BYĆ MINIMALNA, PONIEWAŻ NADAL WIELE KRAJÓW JEST POWAŻNIE DOTKNIĘTYCH COVID-19. BY PRZETRWAĆ PANDEMIĘ, FIRMY W DALSZYM CIĄGU BĘDĄ MUSIAŁY ZACHOWAĆ OSTROŻNOŚĆ.

10 NAJWIĘKSZYCH GLOBALNYCH PRODUCENTÓW BRANŻY SECURITY
na podstawie przychodów ze sprzedaży produktów w 2019 r.

Miejsce	Firma
1	HIKVISION DIGITAL TECHNOLOGY
2	DAHUA TECHNOLOGY
3	ASSA ABLOY
4	BOSCH SECURITY SYSTEMS
5	AXIS COMMUNICATIONS
6	UNIVIEW TECHNOLOGIES
7	TIANDY TECHNOLOGIES
8	ALLEGION
9	HANWHA TECHWIN
10	TKH GROUP

www.aspolska.pl

COVID-19 hamuje krzywą wzrostu

obserwowaną w ostatniej dekadzie

W 2019 R. FIRMY Z ZESTAWIENIA SECURITY 50 OSIĄGNĘŁY ŁĄCZNE PRZYCHODY W WYSOKOŚCI 25,84 MLD USD I ODNOTOWAŁY ŚREDNI WZROST O 9,3 PROC. W STOSUNKU DO 2018 R . MIAŁO TO JEDNAK MIEJSCE PRZED PANDEMIĄ COVID-19, KTÓREJ WPŁYW ZAKOŃCZY ZAPEWNE WZROSTOWĄ KRZYWĄ PRZYCHODÓW, JAKĄ FIRMY SECURITY ODNOTOWYWAŁY W CAŁEJ OSTATNIEJ DEKADZIE.

TEKST
William Pao
a&s International

Z oczywistych względów branża zabezpieczeń była w stanie opierać się recesjom. Nawet podczas jednych z najgorszych spadków ostatnich lat, w tym baniek dot.com z początku 2000 r. i kryzysu kredytów hipotecznych subprime z końca 2000 r., wzrost był stały. Zgodnie z badaniami Frost & Sullivan cała branża security miała w ostatniej dekadzie nieprzerwanie dobrą passę, notując wzrosty średnio od 7 do 10 proc.

Pandemia COVID-19, której wpływ jest niszczycielski, może zaburzyć krzywą wzrostu trwającą od dziesięcioleci. Być może najbardziej wyraźną oznaką uderzenia, jaki odczuły firmy security, są ich przychody w pierwszej połowie tego roku w porównaniu z tym samym okresem roku ubiegłego. Spośród 34 firm z Security 50, które ujawniły swoje przychody za okres od stycznia do czerwca br., 27 odnotowało spadki od -39% do -1% rok do roku; tylko siedem odnotowało wzrost w pierwszym półroczu. Te 34 firmy zanotowały w I półroczu spadek średnio o 10 proc. rok do roku.

Na portalu asmag.com została przeprowadzona ankieta, w której wzięło udział 283 specjalistów ds. zabezpieczeń. Wśród nich zdecydowana większość – 77 proc. – wskazała na spadek przychodów w pierwszym półroczu w stosunku do analogicznego okresu poprzedniego roku. Według nich najbardziej ucierpiały sektory handlu detalicznego, transportu i edukacji.

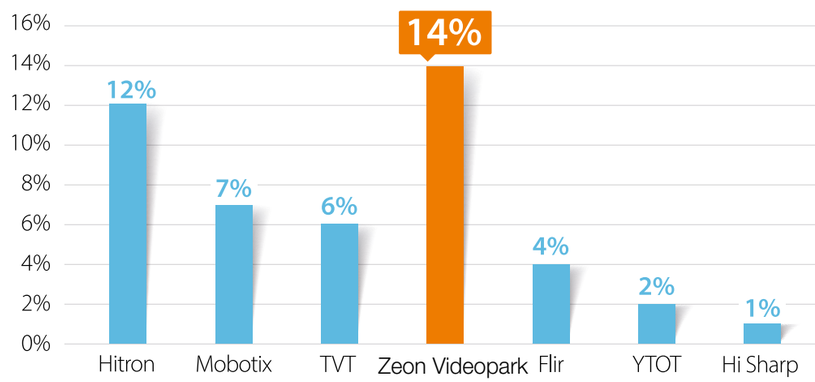
W sektorze transportu szczególnie mocno ucierpiały lotniska. *Z powodu przestojów i opóźnień w ruchu pasażerskim wywołanych lokalnymi lockdownami, które doprowadziły do nakazania obywatelom pozostania w domu i pracy w trybie home office, największe straty odnotują komercyjne i korporacyjne przedsiębiorstwa z branży lotniczej, w tym lotniska* – powiedziała Danielle VanZandt, analityk ds. bezpieczeństwa w firmie Frost & Sullivan. *Nasza działalność polega na rozpoznaniu lokalnych wymagań bezpieczeństwa każdego portu lotniczego poprzez opracowanie planów operacyjnych ConOps (Concept of Operations). Jednak COVID-19 i wynikający z niego chaos gospodarczy zrujnowały sytuację finansową większości lotnisk* – stwierdził Art Kosatka, dyrektor generalny TranSecure.

Spowolnienia w roku 2020, możliwa tendencja spadkowa w 2021 roku

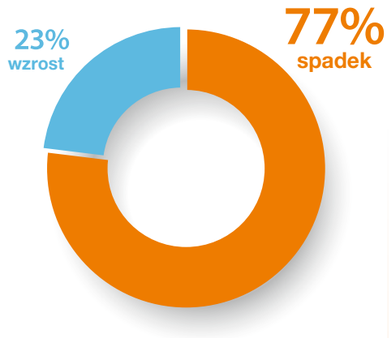
Według Danielle VanZandt w 2020 r. branża zabezpieczeń odnotuje jeszcze niewielki wzrost, ponieważ użytkownicy końcowi zapłacą za już podpisane projekty. *Chociaż tempo wzrostu będzie niższe niż w ciągu ostatniej dekady – 4,47% szacowanego wzrostu w 2020 r. w porównaniu z blisko 7% w 2019 r. – to w 2020 r. firmy nadal będą miały przychody z projektów w toku, które muszą być zakończone i opłacone w całości. Będą też realizowane projekty uzgodnione i częściowo opłacone jeszcze przed pandemią, która po raz pierwszy uderzyła w światową gospodarkę w marcu* – wyjaśniła D. VanZandt.

W 2021 roku sytuacja będzie już inna. Branża może tracić ze względu na ograniczenie wydatków na zabezpieczenia planowane przez użytkowników końcowych. *Rok 2021 będzie rzadkim przypadkiem, kiedy na trajektorii wzrostu nastąpi niewielki spadek przychodów, szacowany na 0,01% w porównaniu z rokiem 2020. Po raz pierwszy od dziesięcioleci rynek zabezpieczeń odnotuje tendencję spadkową, w dużej mierze spowodowaną wolniejszym ożywieniem gospodarczym po pandemii* – powiedziała VanZandt. – *Nawet gdyby wzrosty były widoczne na wszystkich rynkach, łączna suma projektów i funduszy dostępnych w 2021 r. nie zbliży się do tych z okresu przed pandemią.*

Firmy z dodatnim wzrostem przychodów (I połowa 2020 r. – I połowa 2019 r.)



Od stycznia do czerwca 77% respondentów odnotowało spadek przychodów



Pokrywa się to z prognozami przedstawicieli największych firm branży security, przedstawianymi na asmag.com. *Prawie wszystkie prognozy sugerują, że zapewne nigdy więcej nie zobaczymy takiej liczby pasażerów, jaka była w 2019 r. W najlepszym razie może osiągnąć 70% proc., a zyski będą pojawiały się małymi krokami od 2021 r. do 2026 r. lub później* – zaznaczył A. Kosatka.

Uważamy, że skutki gospodarcze pandemii będą odczuwalne przez wiele lat, a to, co teraz widzimy, to tylko wierzchołek góry lodowej. Większość dostawców security nadal wysyła produkty na potrzeby realizacji projektów, które rozpoczęto przed pandemią. Po ich zakończeniu spodziewamy się spadku popytu przez co najmniej kolejne dwa lata. Może tylko kilka firm odnotuje wzrost, ale myślę, że przychody większości znacznie spadną – powiedział Michael A. Silva, dyrektor Silva Consultants.

Gdzie są możliwości

Pandemia gwałtownie zahamowała wzrost przychodów na rynku security. Krótkoterminowy spadek może być nieunikniony. Warto więc obserwować, jak firmy radzą sobie w czasie recesji.

Jednym ze sposobów przezwyciężenia problemów jest poszukiwanie wciąż dostępnych możliwości. *Z powodu skutków pandemii lotniska i sektory komercyjne odnotowują największe spadki wydatków na zabezpieczenia, jednak wiele możliwości wciąż będzie dostępnych, np. fundusze publiczne w takich sektorach, jak organy ścigania, transport publiczny, centra zarządzania kryzysowego, w tym działy zarządzania katastrofami* – stwierdziła D. VanZandt.

Pod względem technologicznym pandemia wywołała wzrost zapotrzebowania na rozwiązania obejmujące walkę z COVID-19, pomocne w ochronie personelu i pracodawców przed zakażeniem, a także wspomagające ich pracę z domu. Obejmują one szyfrowany lub chroniony dostęp do sieci organizacji, bezdotykową kontrolę dostępu, zaawansowaną analitykę i rozwiązania termowizyjne wykrywające podwyższoną temperaturę ciała. Dostarczający te rozwiązania mają większą szansę na pozyskanie zamówień.

Wielu dostawców przygląda się swoim rozwiązaniom, chcąc sprawdzić, czy mogą do nich dodać nowe, specyficzne dla COVID funkcje analityki, takie jak wykrywanie podniesionej temperatury ciała, zarządzanie kolejkami czy zliczanie klientów w sklepie. Dostawcy oprogramowania do rozpoznawania twarzy mogą dodać lub zmienić konfigurację swoich algorytmów, by poprawnie weryfikować tożsamość osób noszących maseczki lub wykrywać, czy dana osoba nosi maseczkę w obiekcie, i zaalarmować w razie jej braku – powiedziała VanZandt.

Analiza kondycji firm, które odnotowały wzrost w I półroczu br., pokazuje, że niektóre z nich zwiększyły swoje przychody dzięki rozwiązaniom termowizyjnym. Należą do nich Mobotix i Flir Systems. „Przychody z technologii termowizyjnych za drugi kwartał wzrosły o 5,5 proc. w porównaniu z tym samym okresem ubiegłego roku. Wzrost przychodów wynikał głównie ze zwiększonego zapotrzebowania na rozwiązania w zakresie wykrywania podwyższonej temperatury ciała" – podano w komunikacie prasowym Flir dotyczącym II kwartału br.

Podsumowując, branża zabezpieczeń doświadcza czegoś, czego nigdy wcześniej nie notowała. Spadek, może niewielki i tymczasowy, jest nieunikniony. Firmy będą mogły prowadzić działalność i przetrwać kryzys dzięki wprowadzaniu rozwiązań niezbędnych zwłaszcza dla tych klientów, którzy zajmują się ochroną przed COVID-19. ▫

www.aspolska.pl

Wpływ pandemii jest ogromny, ale w niektórych sektorach zapotrzebowanie wzrosło

TEKST
William Pao
a&s International

PANDEMIA I ZWIĄZANE Z NIĄ OPÓŹNIENIA WDROŻEŃ ORAZ ODWOŁANIA PROJEKTÓW NA RÓŻNYCH RYNKACH WERTYKALNYCH MIAŁY OGROMNY WPŁYW NA BRANŻĘ SECURITY. SĄ TEŻ SEKTORY, KTÓRE RADZĄ SOBIE LEPIEJ.

Z powodu pandemii różni użytkownicy końcowi zmniejszyli budżety na inwestycje w zabezpieczenia. Spośród 283 ankietowanych przez asmag.com firm z branży security 62 proc. stwierdziła, że ich główni klienci albo zmniejszyli środki na bezpieczeństwo, albo wstrzymywali lub anulowali projekty. Na pytanie, w których sektorach wstrzymano najwięcej inwestycji, 61 proc. wskazało na handel detaliczny, 42 proc. na transport i 31 proc. na edukację.

W branży transportowej np. szczególnie ucierpiały lotniska, ponieważ pandemia zmniejszyła chęć i możliwości podróżowania. Firmy zajmujące się bezpieczeństwem, np. TranSecure, skoncentrowane na projektach lotniskowych, straciły najwięcej. *Lotniska już zamykają nieużywane terminale i sklepy bezcłowe, zwalniają tysiące osób personelu pomocniczego i załóg lotniczych, z których większość nie może czekać dwa, trzy lata na powrót do pracy* – powiedział Art Kosatka. – *Wielu naszych klientów tak zmodyfikowało swoje firmy i życie, aby nie musieć podróżować. Jak długo może to potrwać? Obserwatorzy sugerują, że może minąć nawet sześć do siedmiu lat, zanim gospodarka na tyle się ustabilizuje, aby ją ponownie uruchomić.*

Sektory, które osiągnęły dobre wyniki

Są też takie rynki wertykalne, które dość dobrze radzą sobie również podczas COVID-19. *W dalszym ciągu inwestują następujące segmenty: e-commerce, technologiczne, służba zdrowia, FMCG i produkcja dóbr podstawowych* – wskazał Pawan Desai, współzałożyciel i dyrektor generalny MitKat Advisory Services.

Służba zdrowia

Jak wspomniał P. Desai, segmenty uważane za kluczowe muszą pozostać otwarte nawet w przypadku lockdownu. Są nimi m.in. placówki służby zdrowia, które teraz inwestują w bezpieczeństwo, ponieważ pacjenci wymagają stałej opieki. *Sektor zdrowia się rozwija. Płace podstawowych pracowników medycznych i służb ochrony wzrosły, zapewniono im ubezpieczenie na życie* – powiedział Philip Babajide Edu, dyrektor Corporate Warders.

62% respondentów zredukowało lub zmniejszyło wydatki/siłę roboczą, aby utrzymać biznes w 2020 r.

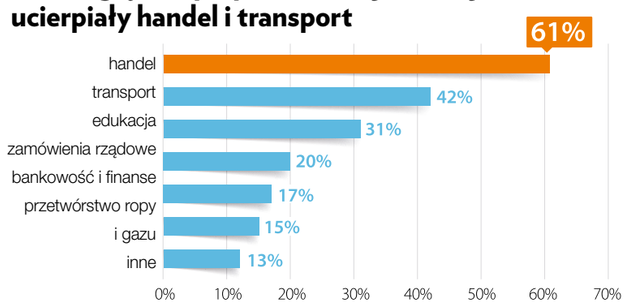
Infrastruktura krytyczna

Innym przykładem jest infrastruktura krytyczna, czyli takie obiekty, jak tamy, reaktory jądrowe czy podstacje energetyczne. *To jedna z branż, które nadal przeznaczają środki na bezpieczeństwo, nawet podczas pandemii, ponieważ zagrożenia nie zniknęły, a nawet mogą być większe* – zauważył Sean Ahrens, lider grupy ds. rynku bezpieczeństwa w Affiliated Engineers.

Banki

Sektor bankowy również radził sobie stosunkowo dobrze. Na pytanie ankieterów asmag.com, „którzy z twoich klientów nadal odnotowują wzrost przychodów", aż 27 proc. respondentów wskazało na bankowość wymagającą zabezpieczeń niezależnie od tego, czy obiekty są otwarte, czy zamknięte. *Banki zainwestowały w tym czasie więcej w poprawę bezpieczeństwa zarówno w domach pracowników, jak i biurach – ze względu na przepisy dotyczące lockdownu i nakaz pracy w trybie home office – by chronić swoje aktywa. Większość oddziałów banków zamknięto, mogły więc stać się łatwym celem dla korzystających z okazji przestępców* – powiedział Munyaradzi Maponga, dyrektor generalny Safeguard Alarms.

Pod względem przychodów najbardziej ucierpiały handel i transport



Podczas pandemii popularność zyskał też sektor centrów danych. Dostawcy rozwiązań wprowadzają coraz więcej ofert w chmurze, które mogą lepiej wspierać pracę mobilną i pomagać w ograniczeniu fizycznej konfiguracji sprzętu, konserwacji czy osobistych wezwań serwisowych. *Centra danych szybko się rozwijają w miarę, jak firmy rozbudowują swoje sieci w chmurze* – zauważył John Torres, prezes Guidepost Solutions. – *Udostępnianie danych w domowych sieciach pracowników stwarza znaczne ryzyko wymagające mocniejszych zapór i zabezpieczeń.*

Zauważyliśmy znaczny wzrost przychodów w sektorze centrów danych, gdyż pandemia wyniosła cyfryzację biznesów i procesów na pierwszy plan. Firmy farmaceutyczne, high-tech oraz internetowe nadal realizują projekty i inwestują w bezpieczeństwo, one także dobrze sobie radzą – powiedział Nicholas Yap, dyrektor operacyjny ICD Security Solutions. ▫

Jak podczas pandemii radzą sobie integratorzy i doradcy

COVID-19 SIEJE SPUSTOSZENIE W BRANŻY OCHRONY I ZABEZPIECZEŃ. W OBLICZU LOCKDOWNU, ZAMKNIĘĆ I NAKAZÓW POZOSTANIA W DOMU. SPRAWDZALIŚMY, JAK RADZĄ SOBIE NAJWIĘKSI GRACZE NA RYNKU SECURITY, BY UTRZYMAĆ SIĘ NA POWIERZCHNI I KONTYNUOWAĆ DZIAŁALNOŚĆ W CZASIE KRYZYSU.

Pandemia odcisnęła piętno na branży security – to fakt. Początkowo większość integratorów systemów i ekspertów spodziewała się dobrego roku 2020. Niestety plany te pokrzyżował koronawirus, tłumiąc wzrost, a nawet powodując spadek przychodów w pierwszej połowie roku.

Przed pandemią dział zabezpieczeń i technologii w firmie Guidepost Solutions działał w rekordowym tempie. Przychody za pierwszy kwartał były najwyższe od siedmiu lat. Gdy wybuchła pandemia, kilka głównych projektów zostało odwołanych lub się opóźniły – powiedział John Torres, prezes Guidepost Solutions.

Mieliśmy w planach zabezpieczenie umów z zamorskimi producentami na specjalistyczny sprzęt i zaproszenie do wizyty w pierwszym kwartale roku. Czekaliśmy na wizy, by przywieźć próbki urządzeń do testów na strzelnicy. Mieliśmy nadzieję na uzyskanie potwierdzonych zamówień w drugim kwartale roku. Jest już czwarty kwartał, a jeszcze nic się nie wydarzyło – stwierdził Philip Babajide Edu, dyrektor ds. ochrony korporacyjnej.

Praca z domu

Pandemia „wysłała" też pracowników do telepracy lub pracy z domu. Żeby móc kontaktować się ze sobą, musieli korzystać ze zdobyczy najnowszych technologii. *Tak, pracowałem w domu i nadal to robię całkiem skutecznie. Osiągnąłem to dzięki wyznaczeniu przestrzeni biurowej w swoim domu i wspomaganiu się technologią kluczową dla tego sukcesu* – zaznaczył Sean Ahrens, lider grupy ds. bezpieczeństwa w firmie Affiliated Engineers.

56% respondentów deklaruje utrzymanie modelu pracy zdalnej do końca 2020 r.

W marcu wszyscy wróciliśmy do domu. Zorganizowaliśmy nasze domowe biura i zmieniliśmy system porozumiewania się, dostosowując go do modelu zdalnego biura. Tylko jedna osoba w tym czasie pracowała w siedzibie firmy, zajmując się wysyłką i odbiorem. Okazało się, że praca z domu nie była taka zła – powiedział Bob Mesnik, prezes Kintronics. – *Jednym z jej efektów jest wrażenie, że czas szybciej mija. Był marzec, a minęło już wiele miesięcy.*

Ćwiczyliśmy pracę z domu jeszcze przed pandemią, dlatego szybko dostosowaliśmy naszą codzienną działalność do nowych warunków. Obecnie monitorujemy sytuację i w razie potrzeby łączymy pracę w biurze z pracą z domu. Nasza wydajność i produktywność nie spadły, ale dystans społeczny obniża jakość życia pracowników. Staramy się więc zapewnić w biurze jak najlepsze warunki pracy – oznajmił Dean Klobucar, dyrektor ds. eksportu w Alarm Automatika.

Nasi koledzy z Indii, Chin, Azji Południowo-Wschodniej, Japonii i Oceanii pracowali w domu na pewnym etapie w 2020 r., a zespoły w Indiach, Oceanii i regionie Morza Południowego nadal tak pracują. Jednak nasi inżynierowie mogli kontynuować prace projektowe i konserwacyjne na miejscu przez cały ten okres, mając niezbędne pozwolenia w każdym regionie – powiedział Nicholas Yap, dyrektor operacyjny ICD Security Solutions. – *Praca z domu jest wyzwaniem zarówno w przypadku wykonywania prac wewnątrz pomieszczenia, jak i w jego przestrzeni zewnętrznej, ale dysponujemy technologią i narzędziami zapewniającymi skuteczną współpracę i komunikację na odległość.*

Dla niektórych firm security blokada była przeżyciem traumatycznym. Zamknięcie było samo w sobie półwięzieniem. *Tylko w wyznaczone dni można było wyjść na zakupy na targu i uzupełnić zapasy żywności* – przypomniał Philip Babajide Edu, dodając, że w jeszcze gorszej sytuacji były firmy ochrony fizycznej. – *Dla pracowników ochrony to było piekło. Przebywali w miejscu pracy przez tygodnie, a nawet miesiące lub w domu bez wynagrodzenia. Pełniący dyżur nie mogli znaleźć w tym czasie otwartych restauracji czy lokalnych punktów żywienia, a chleb i sardynki stały się ich codziennym menu. Zniknęły ich posterunki służbowe, nie ma nawet budek wartownika.*

Pomimo zniszczeń, jakie pandemia i lockdown spowodowały w branży zabezpieczeń, integratorzy systemów i konsultanci muszą kontynuować działalność, aby utrzymać ciągłość biznesową. Co w tym pomagało?

Spełnianie potrzeb klientów w zakresie bezpieczeństwa

Przepisy nakazujące lockdown i związana z tym konieczność zamykania lub zawieszania działalności w wielu branżach nie przeszkodziły w pozyskaniu zleceń od użytkowników końcowych na ochronę ich własności podczas zamknięcia. Firmy security dokładają wszelkich starań, aby skorzystać z takich okazji.

Nasi klienci nadal mają problemy z przestępczością i zwracają się do nas o pomoc – powiedział Michael A. Silva, dyrektor Silva Consultants.

Kilku klientów prosiło nas o wzmocnienie zabezpieczenia ich obiektów pod nieobecność pracowników. Zamówienia dotyczyły magazynów, biur korporacji i restauracji, które były tymczasowo zamknięte – powiedział John Torres. – *W związku z niepokojami społecznymi w wielu miastach firmy, oprócz tego, że zostały dotknięte utratą dochodów z powodu zamknięcia lokali, to jeszcze ich budynki zostały uszkodzone podczas protestów.*

Czas zawieszenia działalności i lockdownu użytkownicy końcowi chcą też wykorzystać na modernizację istniejących systemów. *To okazja, by ukończyć projekty budowlane pod nieobecność pracowników, a wiele z tych projektów obejmuje również udoskonalenie systemów zabezpieczeń* – wyjaśnił Michael A. Silva.

Spełnianie zapotrzebowania na rozwiązania wspierające walkę z rozprzestrzenianiem się wirusa

Wielu integratorów i doradców, z którymi rozmawialiśmy, wprowadziło w tym czasie rozwiązania związane z COVID-19 lub dodało elementy zapobiegające rozprzestrzenianiu się wirusa do istniejących produktów.

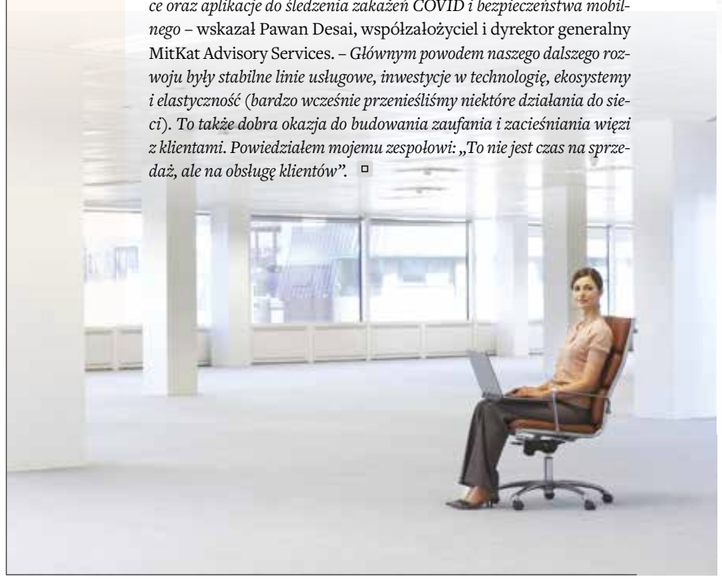
Mamy trzy rozwiązania w zakresie wykrywania maseczki i mierzenia temperatury. Rozwiązania do rozpoznawania twarzy z ekranowaniem temperatury cieszą się popularnością, ale trzeba je również zintegrować z innymi systemami kontroli dostępu, które klienci już posiadają. Dostarczamy rozwiązania niezależnie od rodzaju okablowania – poinformował Bob Mesnik. – *Jest też większe zapotrzebowanie na bezdotykowe systemy domofonowe i rozwiązania do automatycznego śledzenia kontaktów. Śledzenie wszystkich osób w organizacji umożliwiają nasze tagi. Każdy tag zbiera dane o kontaktach i wysyła je do bramki KD, skąd są przesyłane do centralnej bazy danych w chmurze. Jeśli ktoś w firmie zachoruje, informacje z bazy pozwolą natychmiast ustalić wszystkie osoby, z którymi chory miał kontakt.*

Zwiększył się również popyt na systemy zabezpieczeń dla majsterkowiczów, tzw. DIY (*do it yourself*), a dostawcy rozwiązań zintensyfikowali wysiłki, aby mu sprostać. *Zauważyliśmy, że ludzie zaczęli bardziej się interesować bezpieczeństwem swoich domów. W obszarze ochrony i bezpieczeństwa coraz częściej poszukuje się prostych i szybkich rozwiązań dla systemów z segmentu DIY. Ponadto jesteśmy świadkami coraz większej sprzedaży online* – stwierdził D. Klobucar. – *W związku z tym jesienią br. uruchomiliśmy nowy kanał sprzedaży i wprowadzimy na rynek platformę B2C, oferującą właśnie takie rozwiązania. Nasz sklep internetowy Alex oferuje klientom szybkie i proste systemy zabezpieczeń do ich domów.*

Oferowanie potrzebnych usług

Główni gracze security oferują klientom potrzebne im w tym czasie usługi. *W dalszym ciągu świadczymy usługi wdrażania systemów, usługi konserwacji, profesjonalne usługi instalacyjne, usługi konsultingowe i zaawansowane rozwiązania w całym regionie APAC* – powiedział N. Yap.

Wzrasta zapotrzebowanie na następujące usługi: szkolenia online, audyty i oceny centrów danych, cyberbezpieczeństwo, badanie due diligence oraz aplikacje do śledzenia zakażeń COVID i bezpieczeństwa mobilnego – wskazał Pawan Desai, współzałożyciel i dyrektor generalny MitKat Advisory Services. – *Głównym powodem naszego dalszego rozwoju były stabilne linie usługowe, inwestycje w technologię, ekosystemy i elastyczność (bardzo wcześnie przenieśliśmy niektóre działania do sieci). To także dobra okazja do budowania zaufania i zacieśniania więzi z klientami. Powiedziałem mojemu zespołowi: „To nie jest czas na sprzedaż, ale na obsługę klientów”.* □



PODOBNIE JAK W PRZYPADKU WIĘKSZOŚCI GAŁĘZI PRZEMYSŁU NA CAŁYM ŚWIECIE, W BRANŻY SECURITY RÓWNIEŻ WIDOCZNE JEST W 2020 R. ZMNIEJSZENIE AKTYWNOŚCI. PANDEMIA COVID-19 WSTRZYMAŁA BIEŻĄCE PROJEKTY I ODROCZYŁA NOWE.

2020 SECURITY

RAPORT 2020
A&S INTERNATIONAL

W raporcie firmy OMDIA na początku tego roku ostrzegano przed potencjalnym ryzykiem wywołanym pandemią na rynku po tym, jak COVID-19 zakłócił produkcję i łańcuchy dostaw w Chinach, gdzie nadal produkuje się najwięcej kamer. Podczas gdy Chiny w większości podniosły się po pandemii po kilku miesiącach, ryzyko przeniosło się na zmniejszony popyt w innych krajach, w których rządy wprowadziły lockdown i ograniczyły działalność gospodarczą.

W tym artykule redaktorzy A&S International analizują, jak mocno COVID-19 uderzył w głównych dostawców rozwiązań zabezpieczeń, jak radzili sobie z wyzwaniami i czego można się spodziewać w nadchodzącym roku.

www.aspolska.pl

Firmy z rankingu doświadczają wpływu COVID-19

GOSPODARKI SIĘ ZAMKNĘŁY, TRWAJĄCE PROJEKTY ZOSTAŁY WSTRZYMANE, A NOWE PLANY ODROCZONO

COVID-19 wywarł ogromny wpływ na cały rynek zabezpieczeń w 2020 r. Firmy mogą upiększać fakty, ale liczby nie kłamią. Popyt rynkowy, który ostro pikował w pierwszej połowie tego roku, jeszcze nie wrócił do poprzedniego poziomu. Rok 2020 to czas kryzysu dla branży security.

Na tym etapie konieczna jest dokładna analiza wpływu COVID-19 na prowadzoną działalność. W tegorocznym raporcie przedstawiono badanie jakościowe wyników finansowych części spośród największych producentów rozwiązań security, a także badanie ilościowe obejmujące kilka różnych firm.

Zmagania w każdym aspekcie biznesu

Sondaż A&S International dotyczący firm z branży zabezpieczeń pokazuje, że 77 proc. respondentów odnotowało spadek przychodów między styczniem a czerwcem tego roku. W przypadku 35 proc. firm spadek przychodów wyniósł od 25 do 50 proc., w kolejnych 35 proc. firm sprzedaż spadła o 25 proc. Można wskazać konkretne segmenty, które najbardziej odczuły ten spadek, choć tak naprawdę COVID-19 zaszkodził biznesowi w każdym jego aspekcie.

COVID-19 miał wpływ na gospodarkę światową, w tym m.in. na łańcuchy dostaw. Miało to szczególne konsekwencje na nas i naszą branżę, ponieważ jesteśmy zależni od niektórych materiałów i technologii importowanych z krajów na całym świecie – powiedział Ray Mauritsson, prezes Axis Communications. *– Axis odnotował nieco niższą sprzedaż, niż przewidywano przed wybuchem pandemii, ale zaczynamy obserwować stałą poprawę i powrót koniunktury, co pozwoli nam kontynuować wzrost.*

Geograficzne zróżnicowanie wpływu

Badanie A&S International wykazało, że 66 proc. respondentów zauważyło spadek przychodów w sektorze monitoringu wizyjnego, podczas gdy w segmencie kontroli dostępu straty poniosło 19 proc. firm. Keen Yao, wiceprezes Hikvision Digital Technology, zwrócił uwagę, że COVID-19 spowodował, że jego wpływ w niektórych regionach był poważniejszy niż w pozostałych.

Pandemia miała wyraźny wpływ na nasze firmy regionalne, gdzie wprowadzono lockdown, zwłaszcza w tych regionach lub krajach, w których wystąpiła druga fala epidemii – stwierdził K. Yao. *– Zauważyliśmy również, że najbardziej ucierpiały kraje rozwijające się. Większość rządów asygnowała znaczące nadzwyczajne środki finansowe, aby zmniejszyć skutki pandemii. Zatem jednym z globalnych trendów, jakie obserwujemy na rynku zabezpieczeń, jest zmniejszenie liczby projektów rządowych.*

W podobny sposób wypowiada się Joon Jun, prezes Global Business Division w IDIS. Zwrócił on uwagę, że kraje takie, jak Korea Płd., Singapur, Tajwan i Nowa Zelandia, dowiodły, że potrafią kontrolować wirusa. W rezultacie ich PKB i perspektywy gospodarcze w tym i przyszłym roku zapowiadają się korzystniej niż większości krajów Zachodu. Główne ośrodki gospodarcze, takie jak Londyn, Los Angeles, Madryt, Mediolan i Paryż, zostały głęboko dotknięte. Niedawno zostały też zablokowane gospodarki w niektórych rejonach Australii.

Anita Kumar, dyrektor generalna Transition Networks z USA, zgodziła się, że część klientów zdecydowała się opóźnić projekty z powodu niepewnej sytuacji. Jednocześnie wiele amerykańskich miast otrzymało fundusze z CARES Act* na wcześniejsze rozpoczęcie nowych projektów. *Kilku naszych klientów samorządowych wykorzystało ten czas na zaktualizowanie przestarzałej technologii w przestrzeniach publicznych małych miast, aby zapewnić optymalne działanie ich programów bezpieczeństwa i dozoru* – wyjaśniła A. Kumar. *– Nasz międzynarodowy zespół odnotował większą aktywność na początku 2020 r., ponieważ pandemia pojawiła się wcześniej w Azji i Europie.*

Restrykcje działają hamująco mimo zwiększonego popytu lokalnego

Rynek tradycyjnych rozwiązań zabezpieczeń technicznych zwolnił z powodu pandemii, natomiast nastąpił wzrost zapotrzebowania na takie rozwiązania, jak kamery termowizyjne czy bezkontaktowa kontrola dostępu. Ale nawet w tym przypadku wprowadzane rządowe środki zaradcze (lockdown obejmujący kraj czy miasto) ograniczały liczbę projektów, które można było zrealizować.

Wpływ COVID-19 różnił się w zależności od regionu. Na naszą działalność w regionach o przedłużającej się blokadzie wpłynęło to bardziej, gdyż napotykaliśmy fizyczne trudności w prowadzeniu działalności, np. przy instalowaniu systemów czy montażu urządzeń. W innych regionach, w których okres blokady był krótkotrwały, dotknął nas w mniejszym stopniu, a nawet odnotowaliśmy wzrost w porównaniu z rokiem poprzednim. Od trzeciego kwartału obserwujemy ożywienie, ponieważ niektóre kraje łagodzą surowe środki, wznawiają projekty, które zostały przerwane z powodu COVID-19 – oznajmił Young Moon, dyrektor generalny firmy Suprema.

Strategie, które się sprawdziły

Kilku firmom udało się ograniczyć wydatki, aby zrekompensować straty. Jeff Burgess, dyrektor generalny BCD International (USA), potwierdza, że COVID-19 dotknął też jego firmę, która nie odnotuje takiego wzrostu przychodów jak w 2019 r.

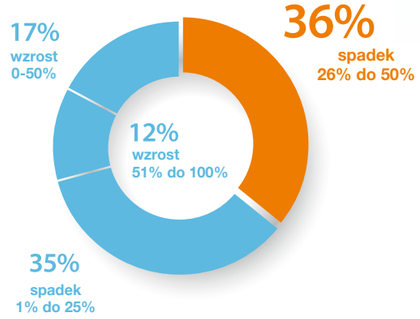
Niezależnie od niewielkiego spadku przychodów nadal osiągamy sukcesy finansowe, częściowo dzięki zmniejszeniu wydatków, np. z powodu odwołania targów i podróży – wyjaśnił J. Burgess.

Kolejną firmą, która poradziła sobie z ograniczenie szkód, jest Špica International. Tone Stanovnik, dyrektor generalny firmy, przypisał to zmianie celu biznesowego firmy jeszcze przed pandemią. *W ciągu ostatnich kilku lat Špica skupiła się na nowym portfolio swoich produktów opartych na technologii Cloud* – powiedział T. Stanovnik. *– Teraz widzimy, że była to świetna wizjonerska decyzja, ponieważ w latach 2019 i 2020 nasz rozwój napędzają przychody z rozwiązań chmurowych. Jednym z kluczowych filarów strategicznych firmy jest wzrost o 20 proc. rok do roku i cieszymy się, że osiągamy ten cel każdego roku. W roku 2019 udało nam się go nawet przekroczyć.*

Zmiany, które mogą trwać dłużej

Pandemia ma na branżę zabezpieczeń katastrofalny wpływ, jednak większość dużych producentów dziś patrzy w przyszłość z ostrożnym optymizmem. Musieli dokonać zmian wielu swoich procedur, aby zapewnić pracownikom możliwość pracy zdalnej i bezpieczeństwo klientom, kontynuując jednocześnie świadczenie usług tak jak wcześniej. Najbliższe miesiące mogą zadecydować, jak te wysiłki wpłyną na branżę. ▫

U 36% respondentów w ciągu pierwszych 6 miesięcy spadek przychodów wyniósł od 26% do 50%



*) *Coronavirus Aid, Relief, and Economic Security Act* – amerykańska ustawa o charakterze specjalnym zawierająca pakiet stymulacyjny wyceniany na 2,2 bln USD, mająca na celu pobudzenie gospodarki amerykańskiej poprzez m.in. wsparcie osób indywidualnych oraz małych i dużych przedsiębiorstw.

www.aspolska.pl

KAMERY TERMOWIZYJNE, BEZKONTAKTOWA KONTROLA DOSTĘPU I ANALITYKA CIESZYŁY SIĘ ZAINTERESOWANIEM WIĘKSZYM NIŻ KIEDYKOLWIEK.

Rozwiązania zapewniające zyski w roku pandemii

Rynek tradycyjnych systemów zabezpieczeń ucierpiał w tym roku. Sprzedający musieli podejmować działania awaryjne, poszukując alternatywnych rozwiązań, które zrekompensowałyby zbliżające się straty. Jak na ironię, problem sam się rozwiązał. Klienci, musząc radzić sobie z COVID-19, zwrócili się ku takim rozwiązaniom, jak kamery termowizyjne, analityka wizyjna czy bezdotykowe systemy kontroli dostępu.

Dostrzegając okazję, wiele firm – choć nie bez problemów – wprowadziło innowacje. Pomimo obaw o dokładność pomiaru kamery termowizyjne stały się produktem popularnym. Funkcje analityczne, takie jak monitorowanie dystansu społecznego, mogą wydawać się zbyt restrykcyjne, ale służą klientom do innych celów. Rozpoznawanie twarzy zyskało popularność, ponieważ nikt nie chciał dotykać czytnika linii papilarnych.

Nowe drogi do przetrwania pandemii

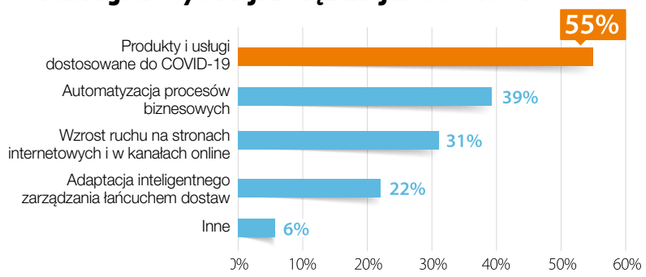
Zmiany preferencji rynku okazały się dla firm sposobem na złagodzenie skutków COVID-19. Christian Morin, wiceprezes ds. usług w chmurze i dyrektor ds. bezpieczeństwa w firmie Genetec, zwrócił uwagę, że wprawdzie pewne obszary rynku znacznie ucierpiały, ale takie sektory, jak handel detaliczny czy podstawowe usługi nadal funkcjonują i wymagają gwarancji bezpieczeństwa. Podobne uwagi przedstawiły inne firmy.

Od momentu lockdownu firma Mobotix zaobserwowała wzrost popytu na rozwiązania do obrazowania termicznego – zauważył Thomas Lausten, dyrektor generalny firmy Mobotix. – *Sporo lotnisk na całym świecie wdrożyło systemy monitorowania temperatury w ramach pakietu środków mających na celu ochronę przed COVID-19 i łagodzenie jej skutków. Kamery termowizyjne, znacznie szybsze i wydajniejsze niż urządzenia ręczne, mogą mierzyć temperaturę, działając trochę jak system wczesnego ostrzegania. Personel może odizolować osobę do dalszego potwierdzenia, czy jest chora, umożliwiając innym kontynuowanie podróży bez przeszkód.*

Duży w ostatnich miesiącach popyt na niezawodne rozwiązania z kamerami termowizyjnymi zadziałał na rozwój firmy Mobotix jak dźwignia. W rocznym raporcie za lata 2019–2020 firma ogłosiła 11-proc. wzrost zysku, spodziewa się też utrzymania tej tendencji w przyszłości. Ray Mauritsson, dyrektor generalny Axis Communications, dodał, że pandemia bez wątpienia doprowadziła do wzrostu zainteresowania rozwiązaniami do zdalnego monitoringu i zapotrzebowania na nie. Oczywistym tego przykładem jest sektor opieki zdrowotnej. Personel podczas pandemii znalazł się pod ogromną presją, musząc radzić sobie z dużą liczbą pacjentów i koniecznością zachowania dystansu.

Tradycyjna technologia dozoru wizyjnego jest wykorzystywana przez lekarzy do zdalnego monitorowania pacjentów, szczególnie w szpitalach tymczasowych. Zdalny monitoring stał się swoistym multiplikatorem sił witalnych pracowników służby zdrowia – powiedział R. Mauritsson. – *W połączeniu z analizą wideo i audio można wykryć oznaki stanu zagrożenia życia pacjenta. Mając dodatkowo urządzenia telemetryczne, które mogą monitorować funkcje życiowe pacjentów, personel uzyskuje niezbędne dane w czasie rzeczywistym i może szybciej reagować, a systemy interkomowe umożliwiają komunikację z pacjentem bez bliskiego kontaktu.*

54% respondentów stara się dostosować produkty i usługi do sytuacji związanej z COVID-19



Szybki wzrost zapotrzebowania na rozwiązania do termowizyjnego monitorowania temperatury ciała przyniósł nowe możliwości również dla Dahua Technology – stwierdził Fu Liquan, prezes Dahua Technology. – *Firma odpowiedziała na zapotrzebowanie rynku, wprowadzając rozwiązania do monitorowania temperatury ciała, w tym kamery termowizyjne i kontrolę dostępu z funkcjami monitorowania temperatury. Rozwiązania te są stosowane m.in. na lotniskach, w węzłach tranzytowych, miejscach biznesowych, instytucjach edukacyjnych na całym świecie.*

Konieczność zachowania elastyczności

Większe korporacje i kadra zarządzająca zdają sobie sprawę, że ich firmy stoją w obliczu bezprecedensowego testu odporności. Żeby zachować ciągłość działania biznesu, potrzebują zdolności do szybkiego reagowania i radzenia sobie z przyszłymi problemami.

Joon Jun, prezes Global Business Division w IDIS, powiedział, że organizacje przyjmują bardziej strategiczne podejście do wdrażania nowych technologii. Rozwiązania te pomagają sprostać wyzwaniom związanym z zachowaniem higieny i dystansu społecznego oraz równoważą wpływ pandemii na przychody i zyski firmy poprzez zwiększanie wydajności operacyjnej i automatyzację procesów, które wcześniej wykonywano ręcznie. Zapewnią elastyczność i skalowalność niezbędne do dostosowania się do nowych warunków.

Podsumowując swoją wypowiedź, Joon Jun dodał, że dla branży zabezpieczeń stwarza to wiele możliwości. Przedsiębiorstwa we wszystkich sektorach stoją przed wieloma takimi samymi wyzwaniami. Wszystkie koncentrują się na ograniczaniu rozprzestrzeniania się COVID-19, starając się jednocześnie zachować ciągłość działania, budować zaufanie klientów i pracowników oraz optymalizować operacje.

Firmy utrzymują spotkania z klientami podczas pandemii

WSZYSCY PRZESZLI NA ONLINE. ALE CZY TO WYSTARCZYŁO?

Pandemia zmusiła firmy do umożliwienia swoim pracownikom pracy z domu. Było to szeroko dyskutowane w mediach jako nowa norma dla firm. Nie było natomiast dyskusji na temat sposobu, w jaki firmy zarządzały spotkaniami z klientami, gdy pandemia COVID-19 wymusiła zamknięcie biur i odwołanie wizyt w terenie. Oczywistą odpowiedzią były działania online. Wiele firm zajmujących się bezpieczeństwem zaczęło oferować webinaria i wirtualne prezentacje produktów.

Tylko w jaki sposób przyciągnąć uwagę klienta i skupić ją przez dłuższy czas w sieci WWW, która jest pełna elementów rozpraszających? Christian Morin, wiceprezes ds. usług w chmurze i dyrektor ds. bezpieczeństwa w firmie Genetec, wyjaśnił, że migracji całości swoich operacji dokonano zdalnie. Od usług po porady inżynierów i certyfikację techniczną – wszystko przeszło do trybu online. Prezentacje i seminaria stacjonarne zostały zastąpione wydarzeniami wirtualnymi.

Pracownicy kluczowi, tak samo klienci

Keen Yao, wiceprezes Hikvision Digital Technology, powiedział, że strategia rynkowa musi wynikać z perspektywy użytkownika, obejmując zwiększone inwestycje w obsługę klienta online.

Aby zrekompensować brak osobistej komunikacji z klientem, która nie była możliwa z powodu epidemii, zorganizowaliśmy kilka seminariów internetowych – wyjaśnił Keen Yao. – *Wprowadziliśmy także pewne aktualizacje produktów lub rozwiązań zgodne z działaniami naszych klientów w zakresie zapobiegania pandemii. Przykładem są kamery termowizyjne z pomiarem temperatury i rozwiązaniami zapewniającymi zachowanie dystansu społecznego, w których wykorzystano technologię sztucznej inteligencji Hikvision.*

Jednocześnie firma dostrzegła nowe możliwości zastosowań w sektorze SMB podczas epidemii. Poprzednie rozwiązania dla małych i średnich firm były związane głównie z wyzwaniami biznesowymi, takimi jak zapobieganie stratom w handlu detalicznym. Teraz dostrzeżono, że większy nacisk należy położyć na bezpieczeństwo pracowników i klientów. Keen Yao uważa, że w przyszłości wymagania dotyczące zapewnienia bezpieczeństwa będą miały jeszcze większe znaczenie.

Tomohiro Tsuji, dyrektor generalny ds. planowania biznesowego i promocji w dziale bezpieczeństwa Optex, dodał, że w firmie również podjęto starania, by zwiększyć kontakt z klientami poprzez seminaria internetowe i wystawy online. *Zapotrzebowanie na technologię lub narzędzia wirtualnej rzeczywistości będzie rosło wraz z upowszechnianiem się takich zdalnych wydarzeń, przed nami jest więc jeszcze wiele możliwości* – podkreślił.

Biznes online

Mimo pandemii wiele firm kontynuowało realizację swojej strategii biznesowej. Thomas Lausten, dyrektor generalny Mobotix, powiedział, że firma stosowała własne produkty i rozwiązania, aby zapobiegać niebezpiecznym sytuacjom wśród swoich pracowników i gości. Oferowała je również swoim klientom.

Przede wszystkim jednak postawiliśmy na dalszy rozwój naszych nowych produktów i rozwiązań – powiedział T. Lausten. – *Co sześć miesięcy prezentujemy innowacje naszym klientom i partnerom, a utrzymanie tego rytmu było dla nas kluczowe. Nie mogliśmy w tym roku zaprosić naszych globalnych partnerów na konferencję, aby zaprezentować nowości, ale dzięki rozwiązaniom technicznym umożliwiającym spotkania online nadal do nich docieramy. Pasjonujące jest obserwowanie, jak zmienił się interfejs użytkownika. Wirtualne targi lub wydarzenia organizowane online zaczynają się teraz rozwijać i osiągają sukcesy.*

Wirtualne targi

Joon Jun, prezes Global Business Division w IDIS, potwierdził – podobnie jak inne firmy – że jego firma także dostosowała sposób pracy do aktualnych warunków. Jednym z głównych celów były wirtualne targi.

Niedawno uruchomiliśmy wirtualną prezentację IDIS. Odtwarza ona w trybie online sposób, w jaki nasi pracownicy oraz partnerzy zajmujący się dystrybucją i integracją systemów oprowadzali klientów po naszych stoiskach na takich targach, jak Intersec, IFSEC czy ISC West. Klienci mogą teraz wziąć udział w wirtualnej wycieczce z przewodnikiem, a odwiedzający mogą po prostu zarejestrować się i przeglądać stoisko w odpowiednim dla nich czasie – wyjaśnił. IDIS współpracuje również z integratorami systemów w celu identyfikacji i zabezpieczenia projektów wideo w prężnych i rozwijających się sektorach, które różnią się w zależności od regionu. W Stanach Zjednoczonych firma nadal dostrzega zwiększoną sprzedaż w sektorach edukacji i logistyki, natomiast wzrost generuje rolnictwo (szczególnie produkcja i sprzedaż konopi) oraz rynek nieruchomości.

Czy te trendy utrzymają się po pandemii?

Przykładowo Axis Communications wskazało, że będzie kontynuować wysiłki online po ustąpieniu COVID-19.

Przeszliśmy z fizycznych do internetowych wydarzeń i targów, które okazały się bardzo udane i po pandemii będą kontynuowane – powiedział Ray Mauritsson. – *Utrzymaliśmy tempo wprowadzania innowacji i zgodnie z harmonogramem wypuściliśmy wszystkie nowe produkty. Cieszymy się, że pandemia nie wpłynęła na naszą zdolność do prowadzenia zrównoważonej działalności biznesowej. Ze względu na ograniczenia w podróżowaniu udało nam się znaleźć nowe, zdalne rozwiązania dla procesów roboczych, które mają mniejszy wpływ na środowisko, i planujemy je kontynuować.*

Mimo to pandemia mogła dać branży tylko krótkoterminowy obraz tego, jak działają te strategie. Większość analiz koncentrowała się bowiem na tym, jak firmy radziły sobie pomimo pracy zdalnej, a nie na jej wpływie na pracowników i klientów w dłuższej perspektywie. Firma może nadal prowadzić hybrydowy model biznesowy, ale jego prawdziwy efekt jeszcze się nie ujawnił.

Wychodząc poza branżę

Pandemia skłoniła niektórych producentów do bardziej przemyślanych działań, które wykraczały poza wysiłki na rzecz zaangażowania klientów w Internecie. Vivotek np. położył duży nacisk na zaangażowanie klientów poprzez udział w webinariach. Ale nie tylko. Kiedy w pierwszych dniach COVID-19 świat walczył o zakup masek ochronnych i potrzebnego sprzętu, firma zdecydowała się wyciągnąć do partnerów pomocną dłoń.

Wiemy, że to trudny czas dla wszystkich, dlatego staraliśmy się okazywać troskę i pomagać naszym partnerom w zachowaniu zdrowia i odporności. Vivotek nie tylko wysłał maseczki do wielu swoich partnerów zagranicznych, gdy świat borykał się z ich niedoborem, ale także wspierał lokalnych dystrybutorów w marketingu regionalnym przy zakupie spersonalizowanych produktów przeciw epidemii, takich jak maseczki, przyłbice i naklejki na podłogę z informacjami o zachowaniu dystansu społecznego – powiedział Peter Chang, dyrektor działu rozwoju produktów w Vivotek.

www.aspolska.pl

Czego branża security może spodziewać się w 2021 r.

PRZEWIDYWANIA, KTÓRE RZUCAJĄ ŚWIATŁO NA POPYT I PODAŻ W NADCHODZĄCYM ROKU.

Rozwój, niezależnie od tego, co wydarzyło się w roku 2020, jest tym, czego oczekuje większość firm branży security. Podstawowym pytaniem jest, co mogłoby ten wzrost pobudzić. Pandemia zakłóciła tradycyjny popyt. Czy zobaczymy powrót popytu sprzed COVID-19, czy też powinniśmy spodziewać się czegoś więcej?

Na podstawie tego, co zaobserwowaliśmy w ciągu ostatnich miesięcy, jesteśmy przekonani, że rynek będzie się nadal rozwijał – stwierdził Ray Mauritsson. – *Ludzie mają fundamentalną potrzebę poczucia bezpieczeństwa, a systemy dozorowe – czy to w kontekście prywatnym, czy publicznym – mogą pomóc w tworzeniu bezpieczniejszego środowiska. Wiele technologii, które podczas pandemii wysunęły się na pierwszy plan – od bezdotykowych rozwiązań kontroli dostępu po technologię zliczania osób w handlu detalicznym – będzie nadal aktualnych i będą zapewniały dodatkową wartość po pandemii.*

Joon Jun podzielił się podobnymi przemyśleniami, spodziewając się dalszego wzrostu w 2021 r. Trudno go jednak precyzyjnie przewidzieć przy tak wielu zmiennych i różnym poziomie ożywienia gospodarczego na świecie, w tym tempa postępu programów szczepień i ich skuteczności.

Więcej funkcji analitycznych

Według J. Jun popyt na tymczasowe rozwiązania specyficzne dla pandemii prawdopodobnie zmniejszy się w nadchodzącym roku. Wzmocnione zabezpieczenia i środki ochronne wdrożone w odpowiedzi na pandemię być może będą jednak miały wpływ na nowe, wyższe standardy we wszystkich typach obiektów.

Potrzeba większej automatyzacji i wydajności będzie miała kluczowe znaczenie dla klientów, którzy nie będą uwzględniać tylko początkowych cen i kosztów cyklu życia swoich rozwiązań. Zastosowanie analityki wspartej głębokim uczeniem zwielokrotni obniżenie kosztów operacyjnych dzięki zmniejszeniu liczby fałszywych alarmów i związanemu z tym zmęczeniu operatora. Już teraz wspomagane przez sztuczną inteligencję powiadomienia o detekcji podejrzanych obiektów czy wałęsania się dają zespołom ochrony większą świadomość sytuacyjną, lepsze wykrywanie i weryfikację, a także szybszą reakcję na zagrożenia i incydenty. Metadane pomagają również radykalnie skrócić czas dochodzenia z godzin do minut – oznajmił J. Jun.

Producenci, z którymi rozmawialiśmy, jasno dali do zrozumienia, że w przyszłości nastąpi szybszy rozwój innowacji. Przykładowo w przyszłym roku firma IDIS wprowadzi funkcję detekcji upadku – rozwiązanie dla sklepów, operatorów centrów handlowych, logistycznych i magazynów. W tych branżach poślizgnięcia, potknięcia i upadki są częste, powodują urazy i utratę możliwości pracy, kosztowne roszczenia ubezpieczeniowe i czasochłonne dochodzenia. J. Jun dodał, że nadal będzie duże zapotrzebowanie na (wielowarstwowe) bezpieczeństwo cybernetyczne w systemach dozoru wizyjnego – obszar, który był już jednym z najważniejszych punktów programu przed pandemią. Będzie on kontynuowany.

Nowe zastosowania dzisiejszych technologii

Czy odkrycie szczepionki mogłoby obniżyć zapotrzebowanie na takie rozwiązania, jak kamery termowizyjne? Firmy nie spodziewają się całkowitego wycofania rozwiązań wprowadzonych w związku z pandemią. Jedyną różnicą byłoby to, że mogą pojawiać się raczej jako część rozbudowanego, zintegrowanego systemu.

Konwergencja będzie kluczowym trendem w 2021 r., który może nadal napędzać rozwój w wielu obszarach. I nie mogę się doczekać, aby zobaczyć, jak nowe technologie i rozwiązania w zakresie wskazań temperatury, detekcji maseczek i monitorowania natężenia ruchu będą tworzyć realną wartość dla klientów końcowych – powiedział Keen Yao. – *Wierzę, że technologie te są niezwykle przydatne dla naszych klientów i mogą wpłynąć na poprawę efektywności operacyjnej. Oczywiście wyzwanie polega teraz na tym, jak zostaną one przyjęte przez rynek, np. przy wdrażaniu do scenariuszy użytkowników, które mogą wymagać oczekiwania na akceptację rynku.*

Yoon Chang-Soo, dyrektor ds. sprzedaży MEA i APAC w Hanwha Techwin, dodał, że COVID-19 zwiększył zapotrzebowanie na sztuczną inteligencję na rynku dozoru wizyjnego i znacząco przyczynił się do wzrostu popularności tej technologii. W czasie pandemii rosną wymagania ze względu na wydajność operacyjną, co przyspieszy rozwój technologii SI w urządzeniach na brzegu sieci (detekcja i klasyfikacja obiektów) oraz specjalistycznych rozwiązań (detekcja masek, aplikacja monitorowania obecności i zajętości).

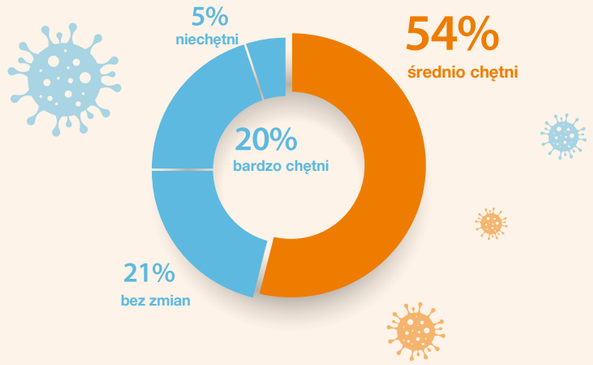
Rozwój technologii 5G umożliwi AIoT (Artificial Intelligence of Things) i przejście od zastosowań zorientowanych na konsumenta do zastosowań na poziomie przemysłowym – ocenił Fu Liquan, prezes Dahua Technology. – *Czujniki, kamery, infrastruktura sieciowa, ogromne ilości danych, chmury obliczeniowe i technologie AI będą kluczowymi i najważniejszymi czynnikami stymulującymi AIoT. W przeszłości dozór wizyjny koncentrował się na podstawowych usługach bezpieczeństwa. Teraz jego zastosowanie może również obniżać koszty i zwiększać wydajność, odgrywając rolę zarządzania w różnych branżach i segmentach.*

Czego firmy mogą najbardziej potrzebować

Firmy na całym świecie przygotowują się na miesiące, a może i lata z COVID-19, ale muszą brać pod uwagę również okres po pandemii. Łatwość przystosowania urządzeń jest sprawą kluczową – stwierdził Thomas Lausten. – *Kluczowe znaczenie ma pewność, że technologie są wystarczająco elastyczne, aby po wygaśnięciu pandemii można je było zastosować w innego rodzaju rozwiązaniach i instalacji w różnych aplikacjach. Dzisiejsze rozwiązanie z zakresu zabezpieczeń jest czymś więcej niż tylko narzędziem dozoru, jest inwestycją w „mądrzejszą przyszłość" i dlatego musi być wystarczająco elastyczne i wszechstronne, aby zaspokajać różne potrzeby, w różnych zastosowaniach, w różnym czasie* – podsumował.

Wprawdzie obecna sytuacja na świecie wymaga głównie instalacji termowizyjnych, to aplikacje te będzie można wykorzystać do celów ochrony przeciwpożarowej, gdyby detekcja podwyższonej temperatury ciała nie była już potrzebna. Co istotne, w zakładach produkcyjnych już korzysta się z inteligentnych kamer termowizyjnych, które potrafią wykryć pożar, zanim spowoduje ogromne szkody. Instalacje termowizyjne są również pomocne w zapobieganiu włamaniom do budynków, z czym zawsze trzeba będzie się mierzyć. Ostatecznie to właśnie elastyczność, która pozwala myśleć o zastosowaniach nieszablonowych, decyduje o wydajności firmy.

54% respondentów twierdzi, że ich klienci są teraz bardziej chętni do korzystania z narzędzi analitycznych lub automatyzacji



Największe firmy liczą na wzrost popytu w 2021 r.

Zbliżamy się już do końca 2020 r., licząc na szczepionkę na COVID-19. W związku z tym branża security patrzy w przyszłość z nadzieją na zwiększenie popytu w sektorach wertykalnych. Rzecz jasna, na początkowym etapie jedne rynki odnotują większe zapotrzebowanie niż inne. Przedstawiamy sektory, w których najwięksi producenci z branży security spodziewają się wzrostu popytu.

Logistyka i magazynowanie

Joon Jun, prezes Global Business Division w IDIS, powiedział, że jego firma dostrzega wzrost obrotów w sektorze logistyki, ponieważ e-handel stale się rozwija, a COVID-19 przyspieszył przejście na dokonywanie zakupów online.

Centra dystrybucyjne i logistyczne musiały utrzymywać i usprawniać swoją działalność, więc prawdopodobnie będą nadal inwestować w rozwiązania zabezpieczające łańcuchy dostaw, pozwalające śledzić towary wchodzące i wychodzące. Będą też wdrażały więcej rozwiązań przeciw zagrożeniom zewnętrznym, takim jak ataki fizyczne czy zorganizowana cyberprzestępczość – stwierdził J. Jun.

Edukacja

Thomas Lausten, dyrektor generalny Mobotix, zwrócił uwagę na duży potencjał w sektorze edukacyjnym. Bezpieczeństwo placówek edukacyjnych jest bardzo ważną kwestią. Niezależnie od tego, czy to przedszkole, szkoła średnia, uniwersytet, prywatne, czy państwowe, efektywne nauczanie wymaga spokojnego i bezpiecznego środowiska.

Wysokiej klasy technologia wizyjna może odegrać zasadniczą rolę w ochronie uczniów przed niebezpiecznymi incydentami. Kluczem są rozwiązania kompleksowe: czy chodzi o zapewnienie, że żaden intruz nie dostanie się do obiektu chronionego systemem rozpoznawania twarzy, czy o zabezpieczanie pomieszczeń i korytarzy, zapobieganie wandalizmowi lub pożarom przy użyciu kamer termowizyjnych, zapotrzebowanie rośnie, a rodzice wymagają coraz lepszej ochrony swoich dzieci i ich danych osobowych. Wszystkie te rozwiązania muszą być również zabezpieczone przed cyberatakami – stwierdził.

www.aspolska.pl

Sektor konopi indyjskich w USA

Według J. Juna również szybko rozwijający się rynek konopi indyjskich w Stanach Zjednoczonych nadal powinien dobrze funkcjonować. Analitycy spodziewają się, że do 2027 r. CAGR utrzyma się na poziomie do 20 proc., co wynika z coraz szerszego zasięgu legalizacji konopi indyjskich przeznaczonych do użytku medycznego i jako środek zwalczający stres dla dorosłych.

Służba zdrowia

T. Lausten dostrzega potencjalny wzrost popytu na usługi w sektorze opieki zdrowotnej, jako że pracownicy służby zdrowia nadal pracują na granicy swoich możliwości.

COVID-19 uwidocznił znaczenia tego sektora. Personel medyczny nawet w normalnych czasach stawał każdego dnia przed wyzwaniami. Wielką szansą na wsparcie w jego obowiązkach i codziennych zadaniach jest technologia. Potrafi np. automatycznie powiadomić personel o tym, że coś się dzieje z pacjentem, by zareagował natychmiast, zanim sytuacja się pogorszy. Ułatwia to wykonywanie stresującej pracy i pozwala nie myśleć o tym, czy pacjent czuje się dobrze i jest bezpieczny – stwierdził T. Lausten.

Praca zdalna

Nowe przepisy umożliwiające przedsiębiorstwom wprowadzenie pracy zdalnej otwierają nowe możliwości dla branży zabezpieczeń.

W USA i Europie, współpracując z integratorami systemów audio-wideo w sektorze mieszkaniowym i małych firm, IDIS dostrzega wzrost zapotrzebowania nie tylko na łatwe zdalne zarządzanie dozorem w celu zwiększenia bezpieczeństwa i ochrony, ale także na wygodę i wydajność dzięki inteligentnym rozwiązaniom automatyzacji, integrującym oświetlenie, strumieniowe przesyłanie muzyki, HVAC oraz urządzenia IoT sterowane zdalnie za pomocą aplikacji mobilnych lub głosem – powiedział J. Jun.

Inne sektory

Branże przemysłowe wymagają dużego wsparcia ze strony techniki ochronnej do zabezpieczenia wszystkich obszarów w swoich zakładach – ochrona obwodowa i kontrola dostępu to tylko jedne z systemów. Zdaniem T. Laustena ważniejsze jest to, że takie rozwiązania, jak inteligentna ochrona przeciwpożarowa, mogą okazać się kluczowe, ponieważ zarówno chronią pracowników, jak i zapobiegają poważniejszym szkodom i stratom przedsiębiorstw.

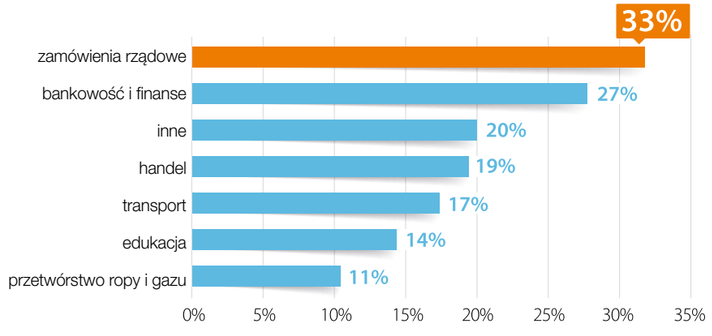
Reagowanie w momencie wybuchu pożaru nie byłoby konieczne, gdybyśmy mogli zapobiegać jego pojawieniu się. Ma to kluczowe znaczenie dla zwrotu z inwestycji, ponieważ pozwala uniknąć nie tylko finansowych, ale także fizycznych szkód dla ludzi i miejsc pracy – dodał T. Lausten.

Nadzieja na powrót inwestycji

Peter Chang, dyrektor Działu Rozwoju Produktu w firmie Vivotek, w tym roku zauważył większe zapotrzebowanie na rozwiązania związane z COVID-19, takie jak systemy kontroli gromadzenia się czy pomiaru temperatury. Ta tendencja może utrzymać się w przyszłym roku.

Spodziewamy się, że w przyszłym roku popyt się utrzyma, choć jego wzrost będzie wolniejszy, ponieważ wiele miejsc i krajów będzie stosować rozwiązania związane z pandemią jako powszechną praktykę – powiedział P. Chang. – *W przypadku projektów większych inwestycji mamy nadzieję na ich powrót, gdy pandemia zostanie opanowana, a projekty te zostaną potraktowane jako czynnik stymulujący ożywienie gospodarcze.*

Podczas pandemii wciąż rosły sektory zamówień rządowych oraz bankowość i finanse



Firmy sektora CCTV

zamierzają stawić czoło zakazowi stosowania chipów HiSilicon

Amerykański zakaz stosowania chipów chińskiej firmy HiSilicon, które były nieodłącznym elementem urządzeń security wielu firm, był prawdopodobnie jedną z najbardziej piorunujących wiadomości w 2019 r. Mimo że kwestia ta w dalszym ciągu pojawia się w nagłówkach gazet, z oskarżeniami w kontekście zarówno politycznym, jak i biznesowym, branża wydaje się powszechnie akceptować fakt, że firmy muszą znaleźć alternatywne rozwiązanie, zgodne z zaleceniem amerykańskiej ustawy NDAA (*National Defense Authorization Act*).

Dzielimy się uwagami niektórych z największych producentów rozwiązań security na temat tego, jak planują poradzić sobie z tą nową zmianą w USA.

Keen Yao, wiceprezes, Hikvision Digital Technology

Zgodnie z polityką firmy ustaloną w momencie jej założenia w trakcie procesu projektowania produktu Hikvision nigdy nie polegał na wyłącznych relacjach z jednym dostawcą. Wobec coraz bardziej niepewnej sytuacji geopolitycznej, która rozpoczęła się w 2018 r., firma skupiła się na alternatywnych planach dostaw znaczących komponentów. Będziemy nadal koncentrować się na ciągłych dostawach wysokiej jakości produktów i usług do naszych partnerów w ramach zrównoważonego globalnego łańcucha dostaw, zgodnego z wymogami firmy.

Joon Jun, prezes Global Business Division, IDIS

W wyniku zarówno sierpniowych zmian w NDAA w USA, jak i rosnącej świadomości oraz wymagań dotyczących bezpieczeństwa cybernetycznego, w połowie 2019 r. zakończył się cenowy „wyścig do dna". Od tego czasu rynek się ustabilizował.

W perspektywie krótkoterminowej producenci z pewnością będą mieli większe możliwości podniesienia cen zestawów zgodnych z zaleceniami NDAA, ale ponieważ wszyscy główni i szanowani gracze są na dobrej drodze do odejścia od chipsetów HiSilicon lub mają układy zgodne z normami, prawdopodobnie będzie to krótkotrwałe. Zapotrzebowanie na kamery i rejestratory zgodne ze standardem NDAA wzrosło nie tylko w Stanach Zjednoczonych, ale także w dużej części Europy, ponieważ duzi użytkownicy końcowi i integratorzy systemów biorą pod uwagę istniejące lub przyszłe inwestycje w Stanach Zjednoczonych. Spodziewamy się, że ta tendencja będzie się utrzymywać.

Yoon Chang-Soo, dyrektor sprzedaży MEA, Hanwha Techwin

Poszerzamy gamę produktów zgodnych z NDAA. Nowe chipsety zastosujemy w kolejnych liniach naszych produktów, od ekonomicznych po zaawansowane. Usuniemy wszelkie bariery w zakupie, jakie mogą napotkać nasi klienci.

Peter Chang, dyrektor działu rozwoju produktów, VIVOTEK

W Vivotek będziemy wybierać różnych dostawców chipsetów, aby sprostać potrzebom klienta. Oprócz cen klientom bardziej zależy na zgodności z NDAA, jakości i wartości dodanej. Spodziewamy się, że w przyszłym roku będzie więcej dostawców procesorów i będziemy mogli zaoferować mocniejszy chipset w przystępniejszej cenie.

Widzimy dwa czynniki, które mogą napędzać wzrost w nadchodzącym roku. Jeden z nich to produkt zgodny z zaleceniami NDAA, a drugi to rozwiązania postpandemiczne. Jeśli chodzi o NDAA, to w roku 2021 będzie bardziej rygorystycznie. Kiedyś HiSilicon był jednym z największych dostawców na rynku dozoru wizyjnego, ale teraz Stany Zjednoczone zakazują sprzedawcom dostarczania produktów i usług tej firmy. To działanie zmusza dostawcę rozwiązań dozoru wizyjnego do przyspieszenia transformacji w celu wybrania alternatywnych opcji zgodnych z NDAA.

Steven Humphreys, CEO, Identiv

Dzisiaj nie odsprzedajemy kamer. Są one jednak dla nas kluczowym elementem integracji, ponieważ wdrażamy na dużą skalę rozwiązania korporacyjne, a nawet mamy mniejsze wdrożenia w chmurze. Oczekujemy, że kamery firm, które nie są objęte zakazem, będą w stanie zaspokoić potrzeby rynku. Choć sytuacja może doprowadzić do niewielkiego wzrostu kosztów, to jednak dodatkowe zapotrzebowanie na zabezpieczenia będą stymulować dalszą sprzedaż i przyszłe wdrożenia.

Uwagi końcowe

Mimo kontrowersji związanych z zakazem w USA wydaje się, że firmy na całym świecie koncentrują się na alternatywnych producentach procesorów, aby uniknąć dalszych zakłóceń swojej działalności. Na etapie, kiedy większość przedsiębiorstw już zmaga się ze skutkami COVID-19 i kryzysem finansowym, jaki po nim nastąpił, jest to decyzja pragmatyczna. Pozostaje jednak pytanie, co okaże się głównym zamiennikiem dla HiSilicon.

NAJWIĘKSZE FIRMY BRANŻY SECURITY NA ŚWIECIE

2019	2018	NAZWA FIRMY	SIEDZIBA	GŁÓWNY OBSZAR DZIAŁANIA	PRZYCHODY W 2019 R. (MLN USD)	PRZYCHODY W 2018 R.	WZROST PRZYCHODÓW 2018-2019
1	1	**HIKVISION DIGITAL TECHNOLOGY** (Telewizja dozorowa)	CHINY	różne	**7702,08**	6806,53	13,16%
2	2	**DAHUA TECHNOLOGY**	CHINY	różne	**3784,29**	3424,85	10,50%
3	3	**ASSA ABLOY** (Zamki elektromechaniczne i elektroniczne)	SZWECJA	kontrola dostępu	**3082,27**	2666,22	15,60%
4	4	**BOSCH SECURITY SYSTEMS**	NIEMCY	różne	**2239,64**	2217,25	1,01%
5	5	**AXIS COMMUNICATIONS**	SZWECJA	różne	**1247,75**	1089,14	14,56%
6	7	**UNIVIEW TECHNOLOGIES**	CHINY	telewizja dozorowa	**714,91**	589,00	21,38%
7	9	**TIANDY TECHNOLOGIES**	CHINY	telewizja dozorowa	**620,01**	521,30	18,94%
8	8	**ALLEGION** (Elektronika i kontrola dostępu)	USA	kontrola dostępu	**599,34**	573,66	4,48%
9	11	**HANWHA TECHWIN**	KOREA	telewizja dozorowa	**497,68**	476,88	4,36%
10	12	**TKH GROUP** (Systemy optyczne i security)	HOLANDIA	różne	**459,94**	434,88	5,76%
11	13	**AIPHONE**	JAPONIA	intercomy	**444,87**	425,08	4,66%
12	14	**INFINOVA**	CHINY	telewizja dozorowa	**394,11**	307,15	28,31%
13	6	**FLIR SYSTEMS** (Handel)	USA	telewizja dozorowa	**354,43**	394,37	-10,13%
14		**ZKTECO**	CHINY	różne	**253,36**	239,49	5,79%
15		**STREAMAX TECHNOLOGY**	CHINY	mobilna telewizja dozorowa	**226,29**	171,15	32,22%
16	18	**VIVOTEK**	TAJWAN	telewizja dozorowa	**203,04**	164,17	23,68%
17	17	**KEDACOM** (Telewizja dozorowa)	CHINY	telewizja dozorowa	**200,74**	168,04	19,46%
18		**DONGGUAN YUTONG OPTICAL TECHNOLOGY**	CHINY	telewizja dozorowa	**178,16**	144,38	23,39%
19	15	**CP PLUS**	INDIE	telewizja dozorowa	**173,21**	223,51	-22,50%
20	16	**NEDAP**	HOLANDIA	różne	**164,60**	172,69	-4,69%
21	21	**MILESTONE SYSTEMS**	NIEMCY	telewizja dozorowa	**153,90**	140,10	9,85%
22	25	**TAMRON** (Handel / Optyka przemysłowa)	JAPONIA	telewizja dozorowa	**131,83**	116,85	12,81%
23	23	**COMMAX**	KOREA	home security i automatyzacja	**122,76**	123,88	-0,90%
24	24	**OPTEX** (Detektory Security)	JAPONIA	sygnalizacja włamania	**121,59**	131,93	-7,84%
25	22	**RAYSHARP**	CHINY	telewizja dozorowa	**121,15**	138,16	-12,31%
26	20	**KOCOM**	KOREA	home security i automatyzacja	**114,87**	140,36	-18,16%
27	32	**WANJIAAN INTERCONNECTED TECHNOLOGY**	CHINY	telewizja dozorowa	**112,58**	63,08	78,46%
28		**BCDVIDEO**	USA	telewizja dozorowa	**93,96**	69,26	35,66%
29		**IDIS**	KOREA	telewizja dozorowa	**92,69**	90,74	2,16%
30	26	**TVT DIGITAL TECHNOLOGY**	CHINY	telewizja dozorowa	**92,05**	88,25	4,30%
31	39	**MAGAL SECURITY SYSTEMS**	IZRAEL	różne	**86,83**	92,60	-6,23%
32		**ZENITEL**	NORWEGIA	intercomy	**85,39**	69,24	23,33%
33	29	**SUPREMA**	KOREA	kontrola dostępu	**84,32**	72,80	15,83%
34		**FUJIAN FORECAM OPTICS/RICOM**	CHINY	telewizja dozorowa (obiektywy)	**83,42**	79,88	4,43%
35	28	**MOBOTIX**	NIEMCY	telewizja dozorowa	**78,28**	74,33	5,31%
36	27	**NAPCO SECURITY SYSTEMS**	USA	różne	**77,31**	85,51	-9,58%
37	31	**IDENTIV**	USA	kontrola dostępu	**76,35**	71,99	6,06%
38	36	**C-PRO ELECTRONICS**	KOREA	telewizja dozorowa	**73,25**	51,05	43,49%
39	30	**FERMAX**	HISZPANIA	kontrola dostępu	**72,02**	70,12	2,71%
40	35	**COSTAR TECHNOLOGIES**	USA	telewizja dozorowa	**69,53**	58,91	18,03%
41	33	**DYNACOLOR**	TAJWAN	telewizja dozorowa	**58,33**	67,06	-13,02%
42	34	**SYNECTICS** (Dział Systemów)	WLK. BRYTANIA	telewizja dozorowa	**51,70**	48,27	7,11%
43	38	**INDIGOVISION** (Motorola Solutions)	WLK. BRYTANIA	telewizja dozorowa	**50,18**	45,96	9,18%
44	37	**GEOVISION**	TAJWAN	telewizja dozorowa	**44,71**	47,92	-6,71%
45	40	**HITRON**	KOREA	telewizja dozorowa	**29,76**	34,97	-14,90%
46	44	**ZEON VIDEOPARK**	CHINY	telewizja dozorowa	**29,24**	20,94	39,64%
47	43	**ITX SECURITY**	KOREA	telewizja dozorowa	**27,33**	23,73	15,16%
48	42	**HI SHARP ELECTRONICS**	TAJWAN	telewizja dozorowa	**26,83**	24,81	8,13%
49		**SPICA INTERNATIONAL**	SŁOWENIA	kontrola dostępu	**17,92**	16,57	8,11%
50	45	**ACTI**	TAJWAN	telewizja dozorowa	**17,41**	18,87	-7,74%

O RAPORCIE

Od 18. lat redakcja a&s International w swoim raporcie „Security 50" przedstawia ranking 50 największych firm w branży zabezpieczeń - takich, które uzyskują najwyższe przychody ze sprzedaży produktów na całym świecie. Ranking obrazuje dynamikę branży na podstawie różnych czynników rynkowych. Jej liderzy zdobywają rynek i podbijają światową gospodarkę, zaspokajając najważniejsze potrzeby klientów, związane z oferowanymi rozwiązaniami.

Ale raport „Security 50" jest czymś więcej niż tylko promocją technologii i produktów. Jego rolą jest także budowanie silniejszych więzi w ramach światowej elity branży security, prezentowanie oryginalnych poglądów dot. zarządzania przedsiębiorstwami, a także kwestii związanych z badaniami i rozwojem, umacnianiem biznesu, budowaniem marki, wyborem partnerów i wiele innych.

Redakcja dokonuje klasyfikacji światowych producentów wyłącznie na podstawie przychodów osiąganych ze sprzedaży produktów, zysku brutto, wielkości marży i zysku netto, ujawnionych w ich publicznych sprawozdaniach finansowych za rok budżetowy 2018. Zestawienie obejmuje zarówno producentów poszczególnych rozwiązań, jak i dostawców całościowych ofert.

W rankingu „Security 50" za rok 2019 mogły wziąć udział następujące firmy:

- Dostawcy elektronicznych urządzeń i systemów opartych na oprogramowaniu z zakresu: dozoru wizyjnego, kontroli dostępu i sygnalizacji włamania, którzy specjalizują się zarówno w kluczowych elementach, jak i wielu segmentach produktowych.
- Przedsiębiorstwa z branży ochrony lub zajmujące się wyłącznie produkcją, posiadające własne produkty, systemy, marki lub rozwiązania.
- Wyłączone zostały przychody z dystrybucji i integracji systemów, z działalności resellerskiej i dealerskiej, instalacji, usług ochrony, ochrony danych (informacji) i zabezpieczania ppoż. oraz inne powiązane.
- Podmioty, które przedstawiły sprawozdania finansowe za rok budżetowy 2018 i rok budżetowy 2017, zbadane i zatwierdzone przez biegłego księgowego lub firmę księgową.
- Publicznie notowane spółki giełdowe, a także niewielka liczba prywatnych, międzynarodowych firm, które wyraziły zgodę na udostępnienie swoich certyfikowanych raportów rocznych. Przed zakwalifikowaniem ich do rankingu są one szczegółowo weryfikowane przez zespół redakcyjny a&s pod kątem rozpoznawalności marki i udziałów w globalnym rynku.

Uwagi do danych finansowych:
a&s nie ponosi odpowiedzialności za informacje finansowe dostarczone przez poszczególne firmy. W celu rzetelnego porównywania walut spoza USA zostały one przeliczone na podstawie średnich rocznych kursów walut podanych przez *Internal Revenue Service*, działający według uchwalonej przez Kongres USA ustawy *Internal Revenue Code*. W rezultacie powstało jak najbardziej obiektywne zestawienie firm gotowych do dzielenia się swoimi wynikami sprzedaży. ▫

Omówienie wyników finansowych za 2019 r. (przed COVID-19)

ANALIZA TEGOROCZNEGO „SECURITY 50” – ZESTAWIENIA 50 NAJWIĘKSZYCH FIRM BRANŻY SECURITY NA ŚWIECIE – WSKAZUJE, ŻE DO KOŃCA 2019 R. BRANŻA ROZWIJAŁA SIĘ W DOBRYM TEMPIE. WOJNA HANDLOWA MIĘDZY USA A CHINAMI WPRAWDZIE WYWARŁA NEGATYWNY WPŁYW NA CHIŃSKIE FIRMY, ALE WIĘKSZOŚĆ SKUTKÓW ZOSTAŁA ZRÓWNOWAŻONA PRZEZ SILNY POPYT WEWNĘTRZNY W CHINACH. SEKTOR DOZORU WIZYJNEGO, TAK JAK W LATACH POPRZEDNICH, BYŁ ZDOMINOWANY PRZEZ KILKA DUŻYCH MAREK. PRAWDOPODOBNIE TREND TEN UTRZYMA SIĘ W NAJBLIŻSZEJ PRZYSZŁOŚCI.

Wzrosty w 2019 r.

Pierwsza dziesiątka bez zasadniczych zmian

W ogólnym ujęciu globalny rynek zabezpieczeń miał dobry rok 2019 (przynajmniej przed COVID-19). Wzrost odnotowało 37 spośród 50 największych firm security. Ich średnia wzrostu 50 firm wyniosła 9,3 proc. w porównaniu z rokiem 2018.

T E K S T
William Pao
a&s International

W pierwszej dziesiątce tegorocznego „Security 50”, wg wielkości przychodów osiągniętych w 2019 r., znalazły się: Hikvision, Dahua, ASSA ABLOY, Bosch Security Systems, Axis Communications, Uniview Technologies, Tiandy Technologies, Allegion, Hanwha Techwin i TKH Group. Nie zanotowano wielu większych zmian w porównaniu z zeszłorocznym rankingiem, z wyjątkiem firmy Flir Systems, która – po spadku przychodów – spadła z 6. pozycji w poprzednim roku na pozycję 13.

Firmy uczestniczące w rankingu „Security 50” w 2019 r. osiągnęły łączny przychód w wysokości 25,84 mld USD i odnotowały wzrost średnio o 9,3% w porównaniu z 2018 r.

Wśród nowicjuszy debiutujących w tym rankingu są firmy: BCD International, Fujian Forecam Optics, Špica International, Streamax Technology, Yutong Optical Technology, Zenitel i ZKTeco. Ich łączny przychód w wysokości ok. 937 mln USD stanowi ok. 3,6 proc. całości dochodu firm ujętych w „Security 50”.

Być może tym, co nas napędza, jest to, że nigdy nie jesteśmy zadowoleni ani nie spoczywamy na laurach. Słuchając naszych klientów i dzieląc się z naszymi dostawcami uwagami na temat filozofii technologii, możemy przesuwać ograniczenia, nazywając to pozytywnym przełomem technologicznym. Ich talent doprowadził do rozwoju własności intelektualnych, takich jak nasze najnowsze DELL iDRAC i VMware zintegrowane z Genetec Security Center. Oba umożliwiają zarządzanie pojedynczym panelem serwera z poziomu komputera stacjonarnego, a nie z serwerowni IT – wyjaśnił Jeff Burgess, dyrektor generalny BCD International. *Špica jest tradycyjnie obecna w regionie Adriatyku, większość naszych dochodów pochodzi z tego obszaru. Ale nasze wyniki w ostatnich latach są napędzane przez rynki międzynarodowe. Jesteśmy obecni w 25 krajach poza Adriatykiem. Po boomie na Bliskim Wschodzie teraz skupiamy się na rozwijających się rynkach w Afryce i regionie Europy Środkowo-Wschodniej, gdzie z sukcesem prowadzimy współpracę z firmą Microsoft* – powiedział Tone Stanovnik, dyrektor generalny Špica International. – *Ponadto nasze rozwiązania chmurowe wchodzą na nowe zachodnie rynki: kraje bałtyckie, Szwecja i USA. W roku 2019 otworzyliśmy biuro w Nowym Jorku.*

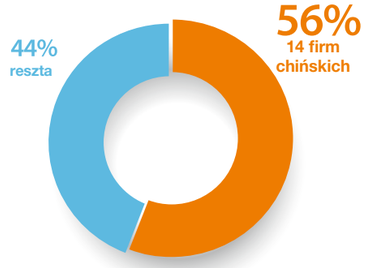
W przeglądzie Security 50 pozycję w pierwszej 10 utrzymało 81% firm

Nowe firmy w zestawieniu 2020 r. (przychody 2019-2018)

Pierwsza dziesiątka firm o największym wzroście (przychody 2019-2018)

www.aspolska.pl

14 chińskich firm generuje 56% całkowitych przychodów z przeglądu Security 50



Wśród pierwszej dziesiątki firm o największym wzroście przychodów w latach 2018–2019 są Wanjiaan, C-PRO Electronics, Videopark, BCD Video, Streamax Technology, Infinova, Vivotek, Yutong Optical Technology, Zenitel i Uniview Technologies.

Silny rynek wewnętrzny w Chinach

W okresie poprzedzającym udostępnienie „Security 50" obserwowaliśmy, czy wojna handlowa między USA a Chinami wpłynie na chińskie firmy security. Na podstawie dokładnej analizy danych możemy stwierdzić, że jej wpływ równoważą dochody, jakie osiągały na rynku krajowym.

Ustawa NDAA (*National Defense Authorization Act*), będąca jednym z powodów wojny handlowej, wprowadziła zakaz korzystania w Stanach Zjednoczonych z urządzeń lub podzespołów security wyprodukowanych przez firmy Hikvision, Dahua i Huawei. Ta ostatnia produkuje chipsety HiSilicon stosowane w większości kamer IP. Mimo to Hikvision i Dahua utrzymały swoje pierwsze i drugie miejsca, z przychodami odpowiednio: 7,7 mld i 3,8 mld USD.

Analiza danych wskazuje, że wzrost obu firm w latach 2018–2019, tj. 13,16% i 10,5%, zmniejszył się w porównaniu z 17,14% i 25,58% w latach 2017 i 2018. Okazało się, że na przychody obu firm miała wpływ konkurencja między USA i Chinami.

Podobnie chińskie firmy, które są wyłącznie lub głównie nastawione na eksport wyrobów finalnych (OEM), ucierpiały bardziej na skutek wojny handlowej. Firma TVT np. odnotowała wzrost przychodów o 4,3 proc. w okresie 2018–2019. W takiej samej sytuacji znalazło się wielu innych średnich i małych dostawców chińskich.

Negatywny wpływ wojny handlowej został zrównoważony przez duży popyt wewnętrzny w Chinach. Podczas konferencji China's Political Consultative w maju i na posiedzeniu Biura Politycznego w lipcu chińscy przywódcy jasno dali do zrozumienia, że motorem napędzającym wzrost w nadchodzących latach będzie popyt wewnętrzny. Polityka ta przyniosła dotychczas dobre wyniki: Chiny odnotowały wzrost PKB o 4,9% rok do roku w III kwartale 2020 r., głównie ze względu na większe zapotrzebowanie w kraju, podczas gdy reszta świata borykała się z COVID-19.

Wysoki popyt wewnętrzny w Chinach znalazł odzwierciedlenie w raporcie „Security 50". Na tegorocznej liście znalazło się w sumie 14 firm chińskich, których łączne przychody wynoszą 14,5 mld USD, co stanowi ponad połowę, a dokładnie 56 proc. łącznych przychodów wszystkich firm z tej listy. Co więcej, w roku 2018 i 2019, w szczytowym okresie wojny handlowej, osiągnęły one średni wzrost o 20 proc. Pomijając Hikvision i Dahua, większość tych firm chińskich, np. Uniview, Kedacom i Tiandy, prowadzi w Państwie Środka spory biznes i realizuje dużą liczbę projektów.

Spośród 14 firm chińskich 13 koncentruje się na dozorze wizyjnym. Nie trzeba dodawać, że technologia dozoru wizyjnego stała się w tym kraju tak zaawansowana ze względu na wsparcie przez rząd i sektor prywatny.

Podsumowując, w 2019 r., zanim pandemia COVID-19 wytrąciła wszystkich z równowagi, na rynku security trwała dobra passa. Warto zauważyć, że ponad połowę wszystkich przychodów osiągały firmy chińskie, a ich rynek krajowy okazał się na tyle silny, że wojna handlowa między USA a Chinami nie miała na to znaczącego wpływu. Ponieważ tylko kilka innych krajów – jeśli nie żaden – jest w stanie osiągnąć tak duży popyt wewnętrzny, produkcję na taką skalę i takie możliwości obniżenia kosztów jak Chiny, możemy spodziewać się, że ich status lidera w dziedzinie zabezpieczeń technicznych w najbliższym czasie pozostanie niezmieniony. □

Dominacja dużych marek
z obszaru dozoru wizyjnego

W tegorocznym rankingu „Security 50" dziesięć największych firm działających w obszarze dozoru wizyjnego generowało lwią część przychodów w tym obszarze. Wskazuje to, że dominacja czołowych marek jest mocno ugruntowana i prawdopodobnie w najbliższej przyszłości się utrzyma.

TEKST
William Pao
a&s International

Dozór wizyjny stanowi największą kategorię produktów w rankingu „Security 50" również w tym roku. W sumie 38 firm jest w całości lub części skoncentrowana na tym obszarze działalności. Razem osiągnęły łączny przychód w wysokości 20,8 mld USD w latach 2018–2019.

Trzeba jednak zauważyć, że chociaż w pierwszej dziesiątce rankingu znalazło się mniej niż jedna trzecia wszystkich firm zajmujących się systemami dozorowymi, przychody tych dwóch trzecich są znacznie mniejsze. Pierwsza dziesiątka firm z rankingu osiągnęła łączne przychody w wysokości ok. 17,76 mld USD, czyli 85,5 proc. łącznego przychodu.

Wśród 10 największych firm dozoru wizyjnego są znane marki, np. Hikvision, Dahua, Bosch, Axis, Uniview, Tiandy, Hanwha Techwin, Infinova, Flir i Vivotek. W ujęciu rok do roku tegoroczna lista Top 10 pozostaje prawie taka sama w porównaniu z 2019 r. Zmieniło się tylko to, że ich przychody wzrosły. Można założyć, że dzięki przychodom, szerokiemu zasięgowi na rynku, ekosystemowi partnerów i możliwościom technologicznym te duże firmy będą w nadchodzących latach nadal dominować w dziedzinie dozoru wizyjnego.

Obiecująca przyszłość dozoru wizyjnego

Było do przewidzenia, że czołowe firmy działające w obszarze dozoru wizyjnego odejdą od sprzedaży pojedynczych produktów. Aby zwiększyć przychody, skupiają się na rozwiązaniach lub projektach dla różnych sektorów rynku, np. zamówień publicznych, inteligentnego miasta czy transportu.

Podobnie firmy dozorowe, które koncentrują się na niszowych i wertykalnych rozwiązaniach, zwykle radzą sobie lepiej niż te, które skupiają się wyłącznie na pojedynczych produktach. Przykładowo firma Streamax Technology z siedzibą w Chinach, nowicjusz zajmujący 15. miejsce w rankingu „Security 50", koncentruje się na rozwiązaniach do mobilnego dozoru wizyjnego. Firma osiągnęła w 2019 r. wzrost przychodów o 32,2 proc. Podobnie Hi Sharp z Tajwanu, również skupiona na mobilnym dozorze wizyjnym, odnotowała wzrost o 8,13 proc. lepszy niż jej konkurenci z Tajwanu.

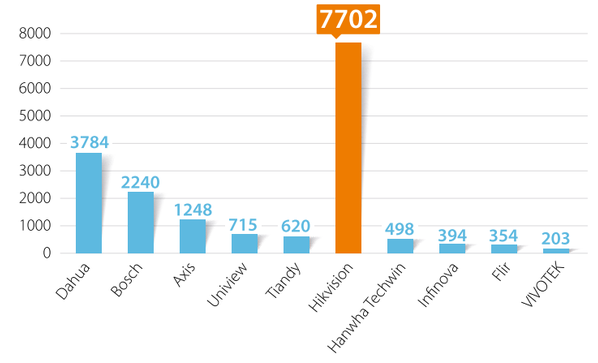
AI i analityka zyskują na znaczeniu w walce z COVID-19

Sztuczna inteligencja i analityka wizyjna odgrywają ważną rolę w dozorze wizyjnym, wspomagając użytkowników końcowych w osiągnięciu celów operacyjnych i dotyczących utrzymania wymogów sanitarnych – wykrywania nietypowego zachowania, rozpoznawania VIP-ów lub wysyłania dodatkowego personelu sklepowego, gdy kolejka do kasy jest zbyt długa. Teraz, podczas pandemii, analityka i sztuczna inteligencja są również pomocne w zapobieganiu i kontrolowaniu rozwoju choroby. Oczekuje się, że taki trend utrzyma się na świecie po pandemii.

To jest nowa normalność. Szkody ekonomiczne i społeczne już wymusiły wydatki rządowe na próby ograniczenia spodziewanej drugiej fali. Powinno to zwiększyć popyt na produkty pomocne w walce z COVID-19 w obiektach publicznych, zwłaszcza w szkołach i na przejściach granicznych – zauważył Munyaradzi Maponga, dyrektor generalny Safeguard Alarms. – *CCTV zintegrowany ze sztuczną inteligencją w celu śledzenia ruchu i zachowania ludzi oraz dostarczania danych w kwestii ryzyka potencjalnego rozprzestrzeniania się zakażenia będzie bardziej powszechny.*

Obecnie pandemia powoduje ponowne zainteresowanie wieloma możliwościami technologicznymi, od monitoringu wizyjnego z analityką po rozwiązania do identyfikacji i zarządzania dostępem, zarówno cyfrowym, jak i fizycznym, zarządzania zdarzeniami czy rozwiązania dla operacyjnego centrum bezpieczeństwa (SOC) – powiedziała Danielle VanZandt, analityk branżowy ds. bezpieczeństwa w firmie Frost & Sullivan. – *Dozór wizyjny, zwłaszcza te systemy, które zawierają zintegrowane rozwiązania analityczne, będą miały kluczowe znaczenie dla umożliwienia klientom ponownego otwarcia ich fizycznych siedzib dla pracowników lub klientów, zapewniając jednocześnie, że procedury dotyczące zachowania dystansu społecznego – odległości lub limitów zajętości – będą mogły być aktywnie monitorowane. Rozwiązania analityczne, które mogą służyć do wielu zastosowań, np. algorytmy zliczające, mierzące odległość i liczbę osób w określonym obszarze, okażą się jednymi z najlepszych do rozważenia rozwiązań, ponieważ zespoły ds. bezpieczeństwa będą zwracać większą uwagę na wybór technologii zabezpieczeń.* □

Przychody ze sprzedaży firm dozoru wizyjnego z pierwszej dziesiątki o największym wzroście (mln USD)



NOWE NORMY Elektroniczne systemy kontroli dostępu

Wymagania systemowe i wytyczne stosowania

Norma europejska (EN) dotycząca budowy elektronicznych systemów kontroli dostępu EACS *(Electronic Access Control Systems)* [1] została przetłumaczona na język polski i jest do nabycia w PKN w formie zarówno papierowej, jak i elektronicznej. Druga jej część [2] – wytyczne stosowania [2] – zostanie przetłumaczona w 2021 r. W normie [1] podano 119 terminów i definicji, znaczna ich część nie była dotychczas powszechnie stosowana, co wymagało wielu uzgodnień tłumaczenia na język polski.

T E K S T
Andrzej Ryczer
Polski Komitet Normalizacyjny, KT 52

W obu normach wymagania funkcjonalne przypisywane urządzeniom kontroli dostępu są określane zgodnie z czterema stopniami zabezpieczenia (*security grades*). Uzyskuje się to na podstawie szczegółowej klasyfikacji funkcjonalności związanych z zabezpieczeniem – kontrolą dostępu, tj. rozpoznanie, aktywacja przejścia kontrolowanego, monitorowanie przejścia, sygnalizacja przymusu i samoochrona systemu (zabezpieczenie przed przypadkowym i/lub przypadkowym sabotowaniem i/lub zakłócaniem działania systemu). Cztery stopnie zabezpieczenia odpowiadają poziomom ryzyka zależnym od przewidywanego zastosowania systemu oraz doświadczenia lub wiedzy atakujących [1].

W klasyfikacji stopni zabezpieczenia zastosowano podobne podejście, jak w „klasycznych" normach z zakresu systemów alarmowych sygnalizacji włamania i napadu – stopień zabezpieczenia zależy od doświadczenia włamywaczy i możliwych do wykorzystania przez nich narzędzi.

Zastosowanie elektronicznych systemów kontroli dostępu wg stopni zabezpieczenia

1. **STOPNIA** powinny być stosowane w aspekcie organizacyjnym i do zabezpieczania zasobów o niskiej wartości (np. w hotelach),
2. **STOPNIA** – w aspektach organizacyjnych i do zabezpieczania zasobów niskiej do średniej wartości (biura, małe przedsiębiorstwa),
3. **STOPNIA** – do zabezpieczania zasobów średniej do wysokiej wartości (przemysł, administracja, finanse),
4. **STOPNIA** – powinny być wykorzystywane w kontroli dostępu do bardzo dużych wartości albo w infrastrukturze krytycznej (np. obiekty wojskowe, rządowe, laboratoria specjalne, produkcja krytyczna) [5], [6].

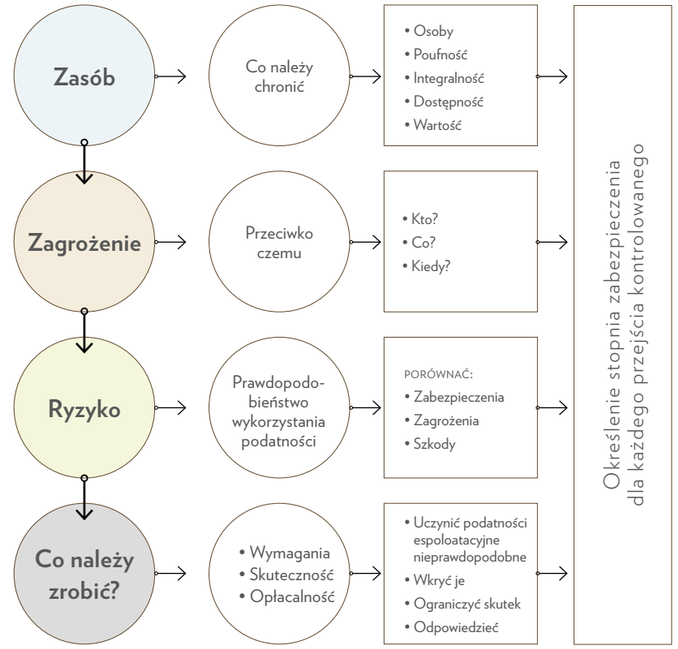
Wymagania normy [1] zostały przedstawione w dziewięciu tablicach, z których najobszerniejsza, dotycząca sygnalizacji i powiadamiania, liczy 47 pozycji. W siedmiu tablicach przedstawiono, zależnie od czterech stopni zabezpieczenia, wymagania dotyczące 140 poszczególnych funkcjonalności:

- interfejsów przejść kontrolowanych,
- sygnalizacji i powiadamiania o zdarzeniach w systemie,
- rozpoznania prowadzącego do przyznania dostępu,
- sygnalizacji przymusu,
- neutralizacji (np. w przypadku pożaru),
- samoochrony systemu,
- zasilania.

Oprócz wymagań norma opisuje szczegółowe procedury badań, które powinny być przeprowadzone w celu potwierdzenia funkcjonalności systemu w odniesieniu do przyporządkowanego funkcjonalnościom stopnia zabezpieczenia.

Norma [1] stawia szczegółowe i liczne wymagania funkcjonalne dotyczące działania czytników i związanych z nimi wskaźników sygnalizujących alarmy i stany przejść (prezentacja informacji dla użytkownika w przejściu i na konsoli monitorującej). Przykładowo w przypadku 4. stopnia zabezpieczenia powinno być spełnionych 47 wymagań związanych np. z wizualizacją poleceń dla użytkownika (sygnalizacja miejscowa i powiadamianie na konsoli obsługi), różnego typu alarmami, utratą łączności, awarią zasilania. Postawiono 27 wymagań związanych z rozpoznaniem – identyfikacją użytkownika. Przykładowo, wskaźnik fałszywych akceptacji FAR w czytnikach z biometrią nie powinien przekraczać 1% (przejście 1. stopnia), 0,3% (przejścia 2. i 3. stopnia) oraz 0,1% (przejście 4. stopnia). W systemie

Rys. 1. Etap planowania



4. stopnia powinna być realizowana sygnalizacja przymusu, a monitorowanie łączności powinno następować odpowiednio co 2 minuty. Czasy podtrzymania zasilania powinny wynosić przy systemach 3. i 4. stopnia odpowiednio: 2 i 4 godz.

Druga z omawianych norm [2] dotyczy wytycznych stosowania. Zwraca się w niej uwagę na tok postępowania włączonego w „cykl życia" systemu, obejmujący etapy: planowania, projektowania, instalowania, uruchamiania, przekazania, działania systemu i jego konserwacji. Ważną częścią wytycznych stosowania są dwa dodatki (normatywny i informacyjny), w których wymieniono dopuszczalne wyjątki – odstępstwa od wymagań normy [1] wymagające uzgodnień między wykonawcą a użytkownikiem końcowym. W dodatku informacyjnym podano zależności liczbowe pozwalające na obliczenie pojemności rezerwowych źródeł zasilania w funkcji średniej spodziewanej liczby aktywacji (otwarć i zamknięć przejść) na godzinę, średniego czasu aktywacji, poboru prądów i wymaganego okresu podtrzymania. W wytycznych stosowania [2] przedstawiono (w sposób graficzny) zarys zalecanego postępowania przy klasyfikacji funkcjonalności systemu opartego na szacowaniu ryzyka *(rys. 1)*. Wyszczególniono też 24 problemy, które należy rozpatrzyć w „cyklu życia" systemu KD, od planowania aż po konserwację.

KLASYFIKACJA STOPNIA ZABEZPIECZENIA

W normach [1] i [2] nie odnosi się stopnia zabezpieczenia do „całego – pełnego systemu", lecz przypisuje się stopnie zabezpieczenia poszczególnym funkcjonalnościom (wymagania z 9 tablic [1] dot. 140 funkcjonalności), zatem etap planowania, w którym określa się poziom ryzyka, powinien dotyczyć **każdego przejścia kontrolowanego,** a nie „całego systemu". Stopnie zabezpieczenia powinny być określane „precyzyjnie" – indywidualnie dla każdego przejścia kontrolowanego, biorąc pod uwagę wymagania dotyczące kontroli wejścia i wyjścia.

W dalszej części artykułu zwrócono uwagę na kilka zalecanych podstawowych zasad projektowania systemu. W tej samej instalacji mogą być stosowane interfejsy przejść kontrolowanych

różnego stopnia zabezpieczenia, pod warunkiem że wspólne elementy systemu zabezpieczające przejścia różnego stopnia zabezpieczenia spełniają co najmniej wymagania dotyczące współpracujących przejść najwyższego stopnia. Zezwala się na systemy oddzielne, gdy instalowanie w jednym systemie przejść o różnych stopniach zabezpieczenia okazuje się niepraktyczne.

Na rys. 1 przedstawiono zarys pełnego postępowania zalecanego na etapie „planowania" (jeszcze przed rozpoczęciem projektowania) prowadzącego do wyznaczenia stopni zabezpieczenia dotyczących funkcjonalności każdego przejścia kontrolowanego [2]. Szacowanie ryzyka (*risk assessment*) otwierające pełny proces stosowania systemu powinno być przeprowadzane w pierwszym etapie – planowanie. Składa się ono z oceny: zasobów – co zabezpieczamy, zagrożeń, ryzyka i tego, „co należy zrobić". W procesie oceny zasobów należy je zinwentaryzować oraz oszacować ich poufność, integralność, dostępność i wartość, wyróżniając zasoby ludzkie. Rozpatrując zagrożenia, należy odpowiedzieć na pytania, przeciwko komu lub czemu, kto, co, kiedy może zagrozić.

Ocena ryzyka polega na ocenie prawdopodobieństwa wykorzystania (przez intruza, hakera) podatności przez porównanie zabezpieczeń, zagrożeń i szkód. W ostatnim etapie postępowania prowadzącym do wyznaczenia stopni zabezpieczenia każdego z przejść kontrolowanych ocenia się skuteczność i opłacalność zastosowanej techniki, minimalizuje podatności eksploatacyjne, wykrywając je i ograniczając ich skutek.

Szczególnie istotne są wymagania dotyczące **samoochrony** systemu [1], które liczą 28 pozycji. Norma określa samoochronę (*self-protection*) systemu jako: *funkcjonalność związaną z zapobieganiem, wykrywaniem i/lub raportowaniem* ***celowego i/lub przypadkowego sabotażu*** *i/lub zakłócania działania systemu,* a **zabezpieczenie przeciwsabotażowe** (*tamper*) jako *metodę wykorzystywaną do zabezpieczenia systemu albo jego części przed celowym zakłócaniem.*

W systemach 3. i 4. stopnia zabezpieczenia przy wykorzystaniu sieci współdzielonych z innymi użytkownikami (np. Internet) wymagane jest szyfrowanie sygnałów między elementami systemu, a informacja przechowywana w identyfikatorze powinna być zabezpieczona przed nieautoryzowaną modyfikacją lub kopiowaniem. Dotyczy to szczególnie systemów kontroli dostępu w inteligentnych budynkach i obiektach infrastruktury krytycznej [5], [6], [7], [8]. W tych obiektach jest wymagane szczególne zabezpieczenie transmisji danych między interfejsami użytkownika (karty, czytniki) a centralami, które można uzyskać, stosując **protokół komunikacyjny OSDP** (*Open Supervised Device Protocol*) [4] do kodowania transmisji wewnątrz systemu.

Kodowana transmisja jest wymagana również w normie [9] dotyczącej łączonych i zintegrowanych systemów alarmowych [9] w przypadku czwartego typu integracji, np. połączenia systemu KD z systemem sterowania oświetleniem budynku.

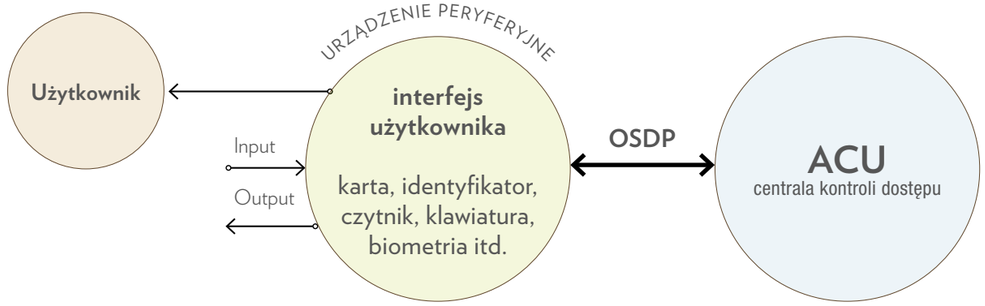
Urządzenia stosowane w systemach KD powinny mieć niezależnie od stopnia zabezpieczenia obudowę o klasie ochrony co najmniej IP4X i odporności mechanicznej IK04. Obudowy powinny być wystarczająco mocne, aby zapobiec niewykrywalnemu (bez widocznych uszkodzeń) dostępowi do elementów wewnętrznych. Obudowy interfejsu użytkownika (np. czytnika, klawiatury itp.) powinny mieć klasę ochrony IP4X. Nie powinno być możliwe uzyskanie dostępu przez wprowadzenie do obudowy 1-mm stalowego próbnika. Alternatywnie jest możliwe wywołanie stanu sabotażu wcześniej, przed dostępem do elementów wewnętrznych.

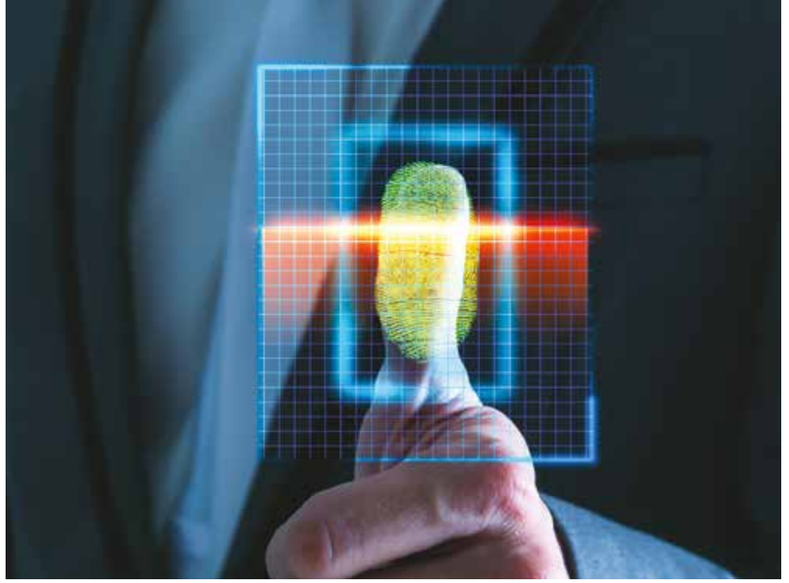
Uwagi końcowe

Ogólna analiza postanowień norm i publikacji podanych w wykazie literatury wskazuje, że ważnym etapem procesu budowy systemów kontroli dostępu jest analiza – szacowanie ryzyka – która powinna być przeprowadzona w pierwszym etapie „planowanie systemu" dla każdego przejścia oddzielnie [2]. Oszacowanie ryzyka prowadzi do wyznaczenia stopnia zabezpieczenia (*security grade*) związanego z funkcjonalnościami poszczególnych przejść, pozwalając następnie na dobór urządzeń i ich parametrów spełniających liczne wymagania szczegółowe [1]. Biorąc pod uwagę, że w [1] określono 140 funkcjonalności, a w [2] 25 dopuszczalnych wyjątków, należy stwierdzić, że proces planowania systemu kontroli dostępu zgodnie z omawianymi normami i wybór parametrów będzie złożony i wymagający precyzyjnej znajomości (interpretacji) wielu szczegółowych wymagań obu tych norm.

Należy podkreślić, że zgodnie z [2] w tym samym systemie mogą być stosowane przejścia kontrolowane o różnych stopniach zabezpieczenia.

Rys 2. Zastosowanie protokołu komunikacyjnego OSDP





Stopnie zabezpieczenia powinny być określone indywidualnie dla każdego przejścia, z uwzględnieniem wymagań dotyczących kontroli wejścia i wyjścia, jednak współpracujące ze sobą elementy powinny spełniać wymagania najwyższego stopnia

Stopnie zabezpieczenia (*security grades*) powinny być określone indywidualnie dla każdego przejścia, z uwzględnieniem wymagań dotyczących kontroli wejścia i wyjścia, jednak kolejno współpracujące ze sobą elementy systemu powinny spełniać wymagania najwyższego stopnia (dotyczy to czytników, central kontroli dostępu/sterowników i konsol obsługi). Oznacza to, że np. czytnik realizujący funkcjonalności 4. stopnia zabezpieczenia powinien być dołączony do centrali z funkcjonalnościami 4. stopnia, a ta również do konsoli obsługi 4. stopnia zabezpieczenia. Dopuszcza się dołączenie czytnika dostępu 1. stopnia do centrali 4. stopnia, ale nie odwrotnie. Takie podejście może mieć wpływ na optymalizację kosztów systemu tam, gdzie oszacowany poziom ryzyka jest niższy, pozwalając na wybranych „drogach dostępu" lub ich odcinkach stosować przejścia o niższym stopniu zabezpieczenia.

Gdy część składowa elektronicznego systemu kontroli dostępu (np. interfejs przejścia kontrolowanego) jest częścią systemu alarmowego (włamania i napadu czy VSS – *Video Surveillance System*), także ona powinna spełniać odpowiednie wymagania norm [1] i [2]. Funkcje dodatkowe (wynikające z integracji) względem funkcji obowiązkowych określonych w [1] mogą być realizowane przez EACS, pod warunkiem że nie przeszkadzają spełnieniu wymagań norm [1], [2].

Omawiane normy dotyczą również systemów KD, gdy są one zintegrowane z innymi aplikacjami poprzez środki rozpoznawania, wykrywania, wyzwalania, połączeń wzajemnych, sterowania, komunikacji, sygnalizacyjnego ostrzegania i zasilania. Wtedy inne aplikacje nie powinny mieć szkodliwego wpływu na działanie systemu kontroli dostępu.

Ze względu na obszerność omawianych norm nową terminologię i powszechne stosowanie systemów kontroli dostępu w nowym budownictwie (systemy łączone i integrowane) byłoby pożądane przeprowadzenie szkoleń – seminariów w zakresie tej tematyki, np. poprzez znanych na rynków dystrybutorów sprzętu albo przez organizacje branżowe. □

LITERATURA:

1. PN-EN 60839-11-1:2013 Systemy alarmowe i elektroniczne systemy zabezpieczeń – Część 11-1: Elektroniczne systemy kontroli dostępu – Wymagania dotyczące systemów i części składowych (IEC 60839-11-1:2013)
2. Pr PN-EN 60839-11-2:2015 Systemy alarmowe i elektroniczne systemy zabezpieczeń – Część 11-2: Elektroniczne systemy kontroli dostępu – Zasady stosowania
3. A. Ryczer, *Stopnie zabezpieczenia i ryzyko w normach Systemy Alarmowe – Systemy dozorowe CCTV i Elektroniczne Systemy Kontroli Dostępu*, „sa" 1/2014 (vol.128)
4. prPN-EN IEC 60839-11-5E Systemy alarmowe i elektroniczne systemy zabezpieczeń – Część 11-5: Elektroniczne systemy kontroli dostępu – Otwarty protokół urządzenia nadzorowanego (OSDP). EN IEC 60839-11-5:2020 (E) Alarm and electronic security systems – Part 11-5: Electronic access control systems – Open Supervised Device Protocol (OSDP)
5. A. Tomczak, *Zwrot w podejściu do systemów kontroli dostępu. Czyżby rewolucja na rynku SKD?*, SEC&AS Security & Alarm System 4/2017(4)
6. A. Tomczak, *Systemy kontroli dostępu w obiektach infrastruktury krytycznej zgodne z Polskimi Normami,* SEC&AS 6/2017(6)
7. P. Piasecka, *Cyberbezpieczeństwo inteligentnych obiektów. Ewolucja oceny zagrożeń w cyberprzestrzeni*, SEC&AS 6/2017(6)
8. B. Ożga, *Systemy kontroli dostępu w obiektach infrastruktury krytycznej,* a&s Polska 2/2018 (8)
9. *EN 50398-1:2017(E) Alarm systems – Combined end integrated systems – Part1: General*

Andrzej Ryczer

Ukończył Wydział Łączności Politechniki Warszawskiej, pracował w Instytucie Telekomunikacji Politechniki Warszawskiej, następnie na Wydziale Transportu, gdzie zajmował się inteligentnymi systemami transportowymi ITS. W Polskim Komitecie Normalizacyjnym jest przewodniczącym Komitetu Technicznego KT52 ds. Systemów alarmowych sygnalizacji włamania i napadu oraz wiceprzewodniczącym KT306 ds. Bezpieczeństwa Powszechnego i Ochrony Ludności, a także członkiem KT323 ds. Usług w Ochronie Osób i Mienia.

JEST WIELE TRENDÓW DOTYCZĄCYCH SYSTEMÓW KONTROLI. JEDNE WYNIKAJĄ Z POTRZEBY INTEGRACJI KONTROLI DOSTĘPU Z INNYMI SYSTEMAMI (WINDOWYMI, SYGNALIZACJI WŁAMANIA, REJESTRACJI CZASU PRACY, EWAKUACYJNYMI), INNE Z CORAZ WIĘKSZEJ ŚWIADOMOŚCI ROSNĄCYCH POTRZEB SŁUŻB BEZPIECZEŃSTWA I ADMINISTRACJI BUDYNKÓW, KOLEJNE SĄ STYMULOWANE SZYBKIM ROZWOJEM TECHNOLOGICZNYM SYSTEMÓW ŁĄCZNOŚCI, ZWIĘKSZAJĄCYM I PRZYSPIESZAJĄCYM MOŻLIWOŚCI WYMIANY DANYCH, NP. POMIĘDZY LOKALIZACJAMI ODDZIAŁÓW FIRMY NA CAŁYM ŚWIECIE.

NOWE TRENDY w systemach kontroli dostępu

TEKST
Michał Zalewski

Problematyka jest obszerna, budzi spore zainteresowanie, jednak proponuję inne podejście do tematu „najnowsze trendy w projektowaniu”. Chciałbym podzielić się swoimi doświadczeniami w projektowaniu systemów KD, omawiając *de facto* podstawy ich planowania, znane wszystkim, ale lekceważone. W zasadzie w każdym projekcie zdarza mi się trafić na jakieś niespodzianki. Z czego mogą wynikać? Nie chcę odpowiadać na pytania o winnych błędów projektowych, ale zgodnie z zasadą *wspieraj, nie oceniaj* spróbuję zaproponować SPPiSPSKD (skrócony podręcznik poprawnego i skoordynowanego projektowania systemu kontroli dostępu). Dotrzymam również obietnicy złożonej w artykule z nr 3/2020 „a&s Polska”* i przedstawię szczegółowo problematykę prawidłowego doboru armatury drzwiowej.

Przystępując do procesu projektowania systemu KD w budynku, należy zacząć od analizy jego funkcji i potrzeb. To dość niewdzięczne zadanie, trudno bowiem znaleźć osoby, które chcą lub są kompetentne odpowiadać na takie pytania. Ale pominięcie tej fazy wiąże się z ryzykiem, że już na początku można popełnić błędy, które później będzie trudno usunąć. W wyniku tych prac musi powstać podział budynku na strefy dostępowe zależnie od funkcji, grupy osób, którym należy zapewnić dostęp do określonych obszarów, zamykając je dla innych.

Polecam metodę zakreślania pomieszczeń na planach różnymi kolorami. Metoda jest znana z wytycznych przeciwpożarowych, w każdym projekcie występuje taki rysunek, nie jest więc żadnym odkryciem. Inżynierowie obawiają się używać kolorowych kredek lub flamastrów, bo to ponoć mało profesjonalne. Ale zapewniam, że skuteczne. Szczególną uwagę trzeba zwracać zwłaszcza na pionowe drogi komunikacyjne, czyli schody i windy. Często te drogi nieoczekiwanie przenikają przez wydzielone strefy dostępowe. Niedawno „wtargnąłem” do zaprzyjaźnionego biura przez ewakuacyjną klatkę schodową, gdy przez przypadek wysiadłem piętro niżej. Wyjście ewakuacyjne było otwarte na kierunku ewakuacji, ale okazało się, że na kierunku przeciwnym, piętro wyżej, również. Pani w recepcji była zdziwiona na mój widok.

Po podziale budynku na strefy dostępowe trzeba się upewnić, czy na wszystkich granicach stref są oddzielenia umożliwiające instalację urządzeń KD, czyli drzwi. Kolejną pułapką, jaką chciałbym zasygnalizować, są przejścia pomiędzy strefami. Dostęp do poszczególnych stref jest wymagany przez strefę komunikacyjną z wolnym dostępem, a jeżeli są konieczne ograniczenia w strefie komunikacyjnej, należy sprawdzić priorytetowość dostępu. Chcę też zwrócić uwagę na wymóg funkcjonalny *antipassback*. Jeżeli taka funkcjonalność jest niezbędna, to wszystkie „kluczowe” drzwi muszą mieć dwustronną kontrolę dostępu. Współpraca z użytkownikiem i projektantem w tej fazie jest naprawdę niezbędna, trzeba o nią zabiegać, ale również jej wymagać.

Gdy już ustalimy przejścia, które muszą zostać objęte kontrolą, trzeba zastanowić się nad doborem armatury

Po podziale budynku na strefy dostępowe trzeba się upewnić, czy na granicach stref są oddzielenia umożliwiające instalację urządzeń KD, czyli drzwi

* https://aspolska.pl/systemy-kd-w-biurowcach-o-koniecznosci-koordynacji-prac-projektowych/

drzwiowej. Określenia tego używam do nazwania wszystkich elementów wykonawczych i zbierających dane, takich jak czujniki, radary wejściowe, elektrozaczepy, elektrorygle, elektrozamki, siłowniki itp. Projektant budynku powinien dostać od nas karty katalogowe proponowanej armatury drzwiowej. Powinniśmy z nim omówić każdy typ drzwi w obiekcie, analizując nie tylko ich mechanikę, ale także funkcje realizowane przez inne systemy, np. sygnalizacji włamania czy oddymiania. Pułapek jest wiele. Kilka przykładów z moich doświadczeń zasygnalizuję poniżej.

- Drzwi wyposażone w trzymacz drzwiowy umożliwiający pozostawienie drzwi otwartych, np. dla transportu wózków towarowych z archiwum czy magazynu. Trzeba mieć świadomość, że ta funkcja uniemożliwia kontrolę niedomkniętych drzwi.
- Konieczność kontroli drzwi w systemie zarówno KD, jak i SSWiN, systemy te nie są zintegrowane, a drzwi (w standardzie) są wyposażone w jeden kontaktron. Rozwiązaniem, chyba jedynym, jest wpięcie wyjścia alarmowego systemu KD do wejścia w systemie SSWiN, to dość łatwe, o ile moduły są zlokalizowane w tym samym pomieszczeniu. Tylko... niepotrzebnie prowadziliśmy przewody do detektora w SSWiN.
- W co wpiąć wyjście sterujące domofonu dla drzwi objętych kontrolą dostępu? To zależy. W przypadku rygla nierewersyjnego to pół biedy, gdy oba systemy mają te same napięcia – wystarczy połączyć masy obu systemów i można próbować. Ale jeżeli domofon ma wyjście 230 V, a system KD 12 lub 24 V? Gdy rygiel jest rewersyjny, KD może przerywać napięcie zasilające rygiel. Alarmowanie sforsowania drzwi lub ich niedomknięcia na pewno zostanie zaburzone!
- Ostatnią niespodzianką, na jaką trafiłem, były drzwi z siłownikiem wypychowym otwierającym drzwi z małym skrzydłem biernym, wyposażone w domofon i kontrolę dostępu. Było spore zamieszanie. Na szczęście udało się dopasować siłownik wyposażony w wyjście napięciowe 24 V do sterowania ryglem. Okazało się również, że potrzebowaliśmy dodatkowego przewodu zasilającego siłownik stałym napięciem pozwalającym na sterowanie ryglem niezależnie od pracy siłownika.

Podobnie jak faza planowania podziału na strefy dostępowe, również faza doboru i koordynacji armatury musi poprzedzać projekt systemu KD. Brak uzgodnienia tych elementów może skończyć się problemami uruchomieniowymi, a nawet skutkować wadami trudnymi do usunięcia. Najsmutniejszy przykład z ostatnich lat: drzwi do sali wyposażone w kontrolę jednostronną, wejście na czytnik, zaplanowane przyciski wyjścia, przyciski typu „zbij szybkę", czujniki kontaktronowe otwarcia i... klamka z obu stron. Oczywiście drzwi bez przeciwrygla i funkcji zamka czy bezwładnej klamki. Projektant po zwróceniu uwagi polecił odpiąć programowo czujniki otwarcia!!! A sal w obiekcie było ok. 50!

Wreszcie wspomnę o – rzadko obecnym w projektach, ale często budzącym spore kontrowersje – problemie koordynacji montażu czytników z innymi elementami zamontowanymi w pobliżu drzwi. Proponuję uzgodnić ich lokalizację wspólnie z projektantem architektury, z uwzględnieniem zarówno rozmieszczenia w pobliżu innych elementów, jak i np. sposobu wykończenia ścian. Nic tak nie podsumowuje braku koordynacji wielobranżowej, jak chaotycznie rozmieszczone elementy przy drzwiach, niezgrane z wykończeniem ścian.

Nie chodzi tylko o uzgodnienia dotyczące koloru i materiału, z jakiego wykonano elementy KD, bo czasem jest to niemożliwe, ale ich posadowienie. Jakże często przechodząc przez atrakcyjne wnętrze, widzę byle jak zainstalowane czytniki czy przyciski. Nie świadczy to dobrze o autorach takich rozwiązań.

Uwagi końcowe

W artykule nie omawiam metod projektowania, instalowania, uruchamiania i programowania samego systemu KD. O wiele lepiej i więcej na ten temat można dowiedzieć się na szkoleniach producentów. Moją intencją jest zwrócenie uwagi na inne aspekty tego zagadnienia. Jest jeszcze jeden powód. Otóż chciałbym, by wzrastała świadomość wagi tych problemów w procesie projektowania. Wtedy będzie szansa, że zauważą je także użytkownik, inwestor, główny projektant, przedstawiciel generalnego wykonawcy.

Oprócz poszukiwania innowacyjnych rozwiązań i nowych funkcji systemów KD nowym (starym) trendem powinno stać się – wydawałoby się oczywiste – staranne projektowanie. To bardzo trudne. Podejmuję wysiłek o zmianę nastawienia, gdyż bliska mi jest opinia Olgi Tokarczuk:

Skoro można pomyśleć, że może być lepiej, to znaczy, że już jest lepiej.

W pogoni za nowatorskimi rozwiązaniami i nowymi funkcjonalnościami systemów kontroli dostępu nie wolno zapominać o ich podstawowej funkcji: umożliwieniu dostępu osobom upoważnionym przy jednoczesnym uniemożliwieniu go intruzom. Bez rzetelnego zadbania o podstawy funkcjonalności nie można myśleć o rozwoju. □

BIO

Michał Zalewski

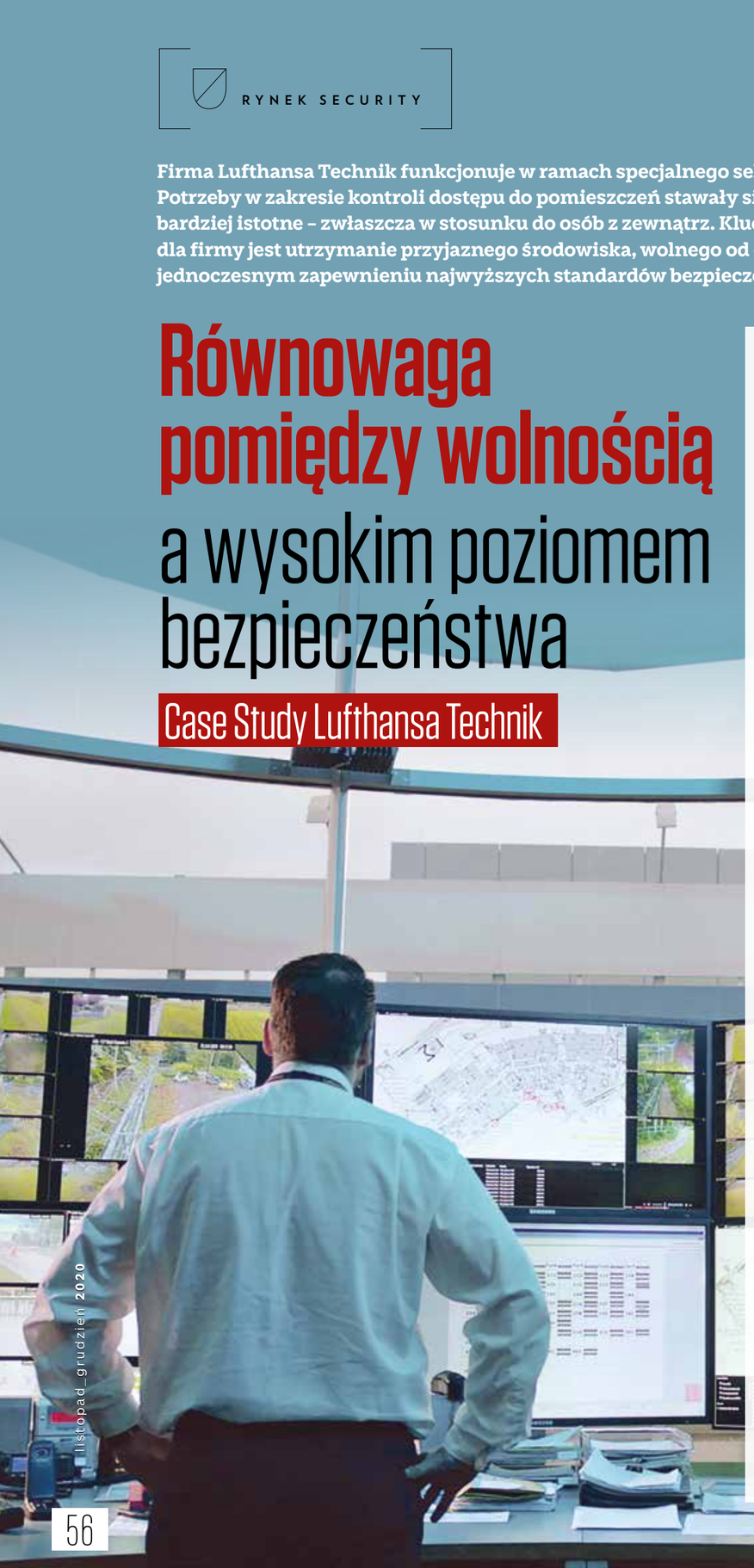
Absolwent Politechniki Gdańskiej i studiów podyplomowych Zarządzania Projektami Politechniki Warszawskiej. W branży od 24 lat, od 12 lat niezależny konsultant, inżynier uruchomieniowy

Oprócz poszukiwania innowacyjnych rozwiązań i nowych funkcji systemów KD nowym (starym) trendem powinno stać się staranne projektowanie

Firma Lufthansa Technik funkcjonuje w ramach specjalnego sektora przemysłu lotniczego. Potrzeby w zakresie kontroli dostępu do pomieszczeń stawały się na przestrzeni lat coraz bardziej istotne – zwłaszcza w stosunku do osób z zewnątrz. Kluczowym wyzwaniem dla firmy jest utrzymanie przyjaznego środowiska, wolnego od ograniczeń, przy jednoczesnym zapewnieniu najwyższych standardów bezpieczeństwa.

Równowaga pomiędzy wolnością a wysokim poziomem bezpieczeństwa

Case Study Lufthansa Technik



Firmie Lufthansa Technik zależy na ograniczeniu możliwości nieupoważnionego wstępu, a przy tym nieutrudnianiu codziennego funkcjonowania swoich pracowników. Znalezienie właściwej równowagi pomiędzy bezpieczeństwem a wygodą, zapewniającej zarówno swobodę poruszania się, jak i poczucie bezpieczeństwa, jest niezwykle istotne. Z kolei pracownicy korzystają z dynamicznego środowiska pracy, które wspomaga ich w optymalnym wykonywaniu swoich obowiązków.

Kontrola dostępu ujednolicona we wszystkich oddziałach

Innym kluczowym celem nowego systemu kontroli dostępu jest jego ujednolicenie. Lufthansa Technik działa w ponad 35 lokalizacjach na świecie, zatrudniając 100 tys. pracowników. W przeszłości każda placówka była odpowiedzialna za swoje bezpieczeństwo. To czasami wymagało zatrudniania specjalistów rozwiązujących jednakowe problemy w różnych miejscach. Firma chciała tego uniknąć i zagwarantować nie tylko te same wysokie standardy bezpieczeństwa, ale również kulturę współdziałania, w ramach której ludzie w dowolnym oddziale będą mogli z łatwością komunikować się ze sobą i współpracować.

Dlatego też nadrzędnym celem firmy Lufthansa Technik jest wspólne korzystanie z jednego systemu kontroli dostępu i przestrzeganie tej samej polityki bezpieczeństwa w każdej placówce. Inną ważną kwestią jest używanie jednego identyfikatora Lufthansa Technik przez wszystkich pracowników przy uzyskiwaniu dostępu do każdego miejsca, po którym mają prawo się poruszać – zarówno w skali lokalnej, jak i międzynarodowej. Zmierzenie się z tym wyzwaniem nie było łatwe, zwłaszcza z powodu kwestii IT związanych z wdrażaniem ujednoliconego systemu KD w wielu miejscach na świecie.

Nedap i ich partnerzy koncentrują się na potrzebach klienta

Firma Lufthansa Technik poszukiwania odpowiedniego systemu kontroli dostępu rozpoczęła od dokładnego badania rynku i organizacji pogłębionego przetargu obejmującego różnych dostawców. Po dokładnych analizach wybrano Nedap.
Melf Westphal, kierownik ds. rozwiązań z zakresu bezpieczeństwa w Lufthansie, wyjaśnia: *Byliśmy naprawdę pod wrażeniem kultury korporacyjnej Nedap, skupienia się na aspektach praktycznych i indywidualnego podejścia. Bardzo starali się znaleźć rozwiązanie idealnie odpowiadające naszym potrzebom. Dlatego zdecydowaliśmy się wdrożyć system Nedap AEOS, który znacząco pomógł nam spełnić nasze kryteria i pozwolił nam stworzyć jednolity system.*

Zapewnienie swobody pozwala ludziom rozwinąć skrzydła

Cele firmy Lufthansa Technik w zakresie kontroli dostępu pokrywają się ze skierowanym na ludzi podejściem Nedap w ramach rozwiązania „Bezpieczeństwo dla życia". Nedap jest przekonany, że systemy bezpieczeństwa należy projektować z myślą o osobach, które będą z nich korzystać, a nie technologii, które będą je obsługiwać.
Podejście „Bezpieczeństwo dla życia" podkreśla aspiracje Nedap do odciążenia personelu w zakresie dbania o kwestie bezpieczeństwa. To z kolei odzwierciedla dążenia firmy Lufthansa Technik do optymalizacji stosunku stopnia ochrony z wygodą:
Za pośrednictwem ich sieci partnerskiej zyskaliśmy możliwość tworzenia spersonalizowanych rozwiązań poprzez integrację z produktami innych firm, które zaspokajają nasze potrzeby dotyczące zabezpieczeń – wyjaśnia Melf Westphal.

Sprostanie wyzwaniom wymaga dużego wsparcia

Początkowo firma Lufthansa Technik uruchomiła projekt pilotażowy w celu wdrożenia systemu AEOS w Hamburgu, gdzie zatrudnionych jest 10 tys. pracowników, a następnie w czterech kolejnych oddziałach. Melf Westphal podkreśla: *Na początku nie wiedzieliśmy, jak się do tego zabrać. Jednak dzięki kompleksowej pomocy Nedap i ich wspaniałych partnerów było nam o wiele łatwiej przebrnąć przez etap wdrażania. Projekt pilotażowy pozwolił nam przezwyciężyć dwie istotne kwestie: jak wdrożyć kontrolę dostępu AEOS w naszej infrastrukturze informatycznej oraz jak zaangażować naszych pracowników.*

Nedap wraz z partnerami wykonali solidną robotę – mówi dalej Melf Westphal. – *To, co nam zaprezentowali, to nie tylko dobre produkty. Dzięki ich wsparciu, a także pomocy ich oddanych partnerów mogliśmy uporać się ze wszystkimi problemami operacyjnymi. Za pośrednictwem ich sieci partnerskiej zyskaliśmy z kolei możliwość tworzenia spersonalizowanych rozwiązań poprzez integrację z produktami innych firm, które zaspokajają nasze potrzeby dotyczące zabezpieczeń. Oznacza to, że zamiast stawiania barier mamy relatywnie dużą wolność poruszania się. Czuję się bardzo bezpiecznie, jednak w razie potrzeby mogę korzystać z mojego identyfikatora, aby udać się w dowolne miejsce. Mamy fantastyczne rozwiązania oraz, co ważne, ten sam identyfikator Lufthansa Technik, który łączy nas wszystkich – niezależnie od naszej lokalizacji.*

Integracja firm trzecich zwiększa elastyczność

Wdrożony przez firmę Lufthansa Technik system kontroli dostępu AEOS to więcej niż tylko ochrona drzwi; zainstalowano również dodatkowe komponenty, takie jak szafy na klucze oraz zarządzanie odwiedzającymi. *AEOS okazał się wielką pomocą w tej kwestii – pozwolił nam na zaangażowanie usługodawców zewnętrznych. Ponieważ filozofią Nedap jest ścisła współpraca z zewnętrznymi partnerami technologicznymi, a AEOS łatwo integruje się z innymi systemami, nie byliśmy ograniczeni tylko do jednego rozwiązania. Zapewniło to nam elastyczność w stworzeniu dokładnie tego, czego oczekiwaliśmy* – powiedział Melf Westphal.

W skutecznych systemach to ludzie są najważniejsi

Dla firmy Lufthansa Technik kluczowym aspektem projektu pilotażowego i następującego po nim wdrożenia jest przekonanie pracowników do pracy z nowym systemem kontroli dostępu. Uważa ona, że nawet najlepszy system KD traci na wartości, jeżeli ludzie z nim pracujący nie mają właściwego podejścia. Z tego powodu Lufthansa Technik poczyniła znaczące inwestycje w szkolenia, komunikację i akcje uświadamiające.
W pierwszej kolejności skupiały się one na zakomunikowaniu pracownikom tego, jak bardzo są cenni, jak ważne jest bezpieczeństwo i dlaczego wprowadza się zmiany w organizacji bezpieczeństwa. Uświadomiły im również znaczenie spodziewanych zagrożeń dotyczących bezpieczeństwa i ich własnej roli w systemie zarządzania bezpieczeństwem firmy Lufthansa Technik.

Każdy pracownik firmy Lufthansa Technik jest teraz zachęcany do brania udziału w tworzeniu bezpiecznego środowiska pracy. Są też szkoleni, jak reagować na alerty i jak zwracać się do nieupoważnionych osób zauważonych w zastrzeżonych miejscach. Co ważne, pracownicy firmy Lufthansa Technik rozumieją, że ich system kontroli dostępu AEOS służy w takim samym stopniu ochronie ich wolności i zapewnieniu im bezpieczeństwa.

Jeżeli chodzi o bezpieczeństwo, moim sloganem jest: Wolimy otwierać drzwi, niż je zamykać. Jest to dla mnie naprawdę ważne – podkreśla Melf Westphal.

Wdrożenie w skali globalnej

Następnym krokiem dla firmy Lufthansa Technik jest kontynuowanie wdrażania AEOS na całym świecie. Melf Westphal wyjaśnia: *Sukces naszego nowego systemu bezpieczeństwa nie pozostał niezauważony. Inne zakłady firmy Lufthansa Technik dostrzegły skuteczność AEOS na przykładzie Hamburga, w zakładzie zatrudniającym 10 tys. pracowników. Widzimy również wzrost zainteresowania podobnymi systemami oddziałów na całym świecie. Naszym obecnym celem jest więc wdrożenie AEOS we wszystkich naszych zakładach, aby uzyskać naprawdę ujednolicony system bezpieczeństwa, który spaja całą rodzinę Lufthansa Technik. System bezpieczeństwa, który pozwala nam otwierać drzwi, a nie je zamykać.* □

Nedap Security Management
Al. Niepodległości 18,
02-653 Warszawa
www.nedapsecurity.com/pl

Jak branża IT postrzega rynek systemów dozoru wizyjnego

Część 2

PRZYSZLI UŻYTKOWNICY SYSTEMÓW DOZORU WIZYJNEGO IP (SZERZEJ – INWESTORZY) WYKONANIE INSTALACJI POD KLUCZ MOGĄ ZAMÓWIĆ U INTEGRATORA Z BRANŻY IT LUB Z BRANŻY ZABEZPIECZEŃ. MOGĄ RÓWNIEŻ WYBRAĆ BARDZIEJ SKOMPLIKOWANY WARIANT PROCESU INWESTYCYJNEGO I POWIERZYĆ WYKONANIE INSTALACJI SYSTEMU DOZORU WIZYJNEGO FIRMIE SPECJALIZUJĄCEJ SIĘ W ZABEZPIECZENIACH, A NIEZBĘDNEJ INFRASTRUKTURY SIECIOWEJ – FIRMIE IT. ANALOGICZNY WYBÓR DROGI POSTĘPOWANIA MAJĄ DO DYSPOZYCJI INTEGRATORZY SYSTEMÓW ZABEZPIECZEŃ, OTRZYMAWSZY ZAMÓWIENIE NA REALIZACJĘ KOMPLETNEJ INSTALACJI SYSTEMU DOZORU WIZYJNEGO IP. MOGĄ OGRANICZYĆ SIĘ DO WYKONANIA SYSTEMU DOZORU WIZYJNEGO, A WYKONANIE INFRASTRUKTURY SIECIOWEJ ZLECIĆ PODWYKONAWCY – INTEGRATOROWI IT. MOGĄ TEŻ SAMI WYKONAĆ INFRASTRUKTURĘ SIECIOWĄ, KUPUJĄC U DOSTAWCÓW IT NIEZBĘDNE URZĄDZENIA.

TEKST
Waldemar Więckowski

We wszystkich wymienionych przypadkach realizacji inwestycji czynnikiem kluczowym dla powodzenia przedsięwzięcia jest przebieg współpracy ze specjalistami z branży IT. W dużej mierze zależy ona od tego, jak branża IT postrzega systemy dozoru wizyjnego.

(Formalny) wstęp do części 2.

Postrzeganie rynku dozoru wizyjnego przez branżę IT omawiam, cytując fragmenty artykułów publikowanych w serwisie crn.pl. Wybrałem opinie i konkluzje, stosując kryterium z kim nie należy wchodzić w relacje biznesowe. Część 1 artykułu opublikowana w nr 4/2020 a&s Polska objęła okres od 2002 do 2011 r. część 2. – lata 2013–2019. (Zachowano ciągłość numeracji w spisie literatury.)

– Mentalność polskich wdrożeniowców ogranicza rozwój systemów CCTV IP

Zdaniem autora powyższej opinii, odnotowanej w czerwcu 2010 r. [8], w krajach zachodnich integratorzy zupełnie inaczej postrzegają rolę systemów CCTV IP niż integratorzy w Polsce, i to właśnie skutkuje ograniczaniem ich rozwoju. *Zachodnie firmy wdrożeniowe planują rozwój systemów monitorujących strategicznie. Kiedy przystępują do realizacji projektu związanego z tworzeniem informatycznego systemu bezpieczeństwa w budynku, system monitoringu traktują jako element większej całości, a nie odrębne przedsięwzięcie. Podobnie firmy wdrożeniowe, które, projektując serwerownię, już na wstępnym etapie uwzględniają to, jaka część zasobów (np. pojemność dysków) zostanie przeznaczona na potrzeby systemu monitorującego. W naszym kraju system monitorowania IP wciąż jest traktowany jak odrębne rozwiązanie.*

Na pytanie, kiedy mentalność polskich wdrożeniowców upodobni się do mentalności ich zachodnich kolegów po fachu, autor powyższej opinii odpowiada, że trudno jednoznacznie powiedzieć, ale raczej nieprędko, gdyż ***w naszym kraju instalowaniem systemów monitoringu zajmują się głównie przedsiębiorstwa niewywodzące się ze świata informatyki, które nie mają globalnej wizji wdrażania takich systemów*** (podkreślenie autora). I nie zmieni tego fakt, że *90 proc. firm specjalizujących się u nas we wdrożeniach systemów monitorowania IP to przedsiębiorstwa wykonujące na co dzień instalacje rozwiązań telewizji przemysłowej, nagłośnienia lub automatyki*. Zatem warunkiem koniecznym i wystarczającym posiadania globalnej wizji wdrażania systemów CCTV IP jest przynależność do świata informatyki, także dlatego że:

– Dozór wizyjny to dodatkowa funkcja systemu informatycznego

Dozór wizyjny jest naturalnym rozszerzeniem zakresu usług firm informatycznych, które układają sieci. Rynek sieciowy jest już bardzo nasycony, stąd coraz więcej integratorów decyduje się rozszerzyć swoją ofertę o monitoring IP. Klientom warto uświadamiać, że może on być częścią sieci komputerowej w przedsiębiorstwie, a kamery tylko jednym z jej elementów. To po prostu ***wzbogacenie obecnie działającego systemu informatycznego o dodatkową funkcję*** (podkreślenie autora). [9]

Takie mylenie istoty zabezpieczeń z narzędziami wspierającymi zabezpieczenia jest charakterystyczne dla „facetów od IT" (*IT guys*). Idą oni nawet dalej, twierdząc, że IT dokonuje transformacji zabezpieczeń fizycznych, gdy w rzeczywistości zabezpieczenia asymilują narzędzia IT, które są dla nich tak samo ważne, jak dla marketingu, finansów itp. Zarządzanie bezpieczeństwem i zabezpieczenia fizyczne to znacznie więcej niż narzędzia, z których korzystają – jest mnóstwo niezbędnych elementów niezwiązanych z technologią. [10]

– Różowo (z zarobkiem) nie jest i jednak trzeba posiąść sporą wiedzę

Opublikowany we wrześniu 2013 r. kolejny artykuł [11] wykazał, że na łatwy zarobek nie mogą liczyć nawet cierpliwi, a brak specjalistycznej wiedzy sytuację wyraźnie utrudnia. Nie jest różowo, ponieważ *szanse resellerów i integratorów IT*

na tym rynku są niewielkie w związku z konkurencją ze strony agencji security. I na dodatek brak wiedzy jednak jest problemem. Przedstawiciele przedsiębiorstw IT, którzy są zainteresowani wdrożeniami z zakresu monitoringu wizyjnego, podkreślają, że zanim zacznie się takie usługi oferować, trzeba posiąść sporą wiedzę.

Druga strona tego medalu jest taka, że ponieważ *technologia IP wymaga od wdrażających system wiedzy z zakresu tworzenia i konfiguracji sieci oraz doboru sprzętu komputerowego do transmisji strumieniowej, więc głównie z tego powodu firmy informatyczne mają pewną szansę na konkurowanie na tym rynku z agencjami ochrony i instalatorami tradycyjnych systemów monitoringu. (...) Obecnie mamy tendencję wzrostową, a typowi gracze (z rynku systemów ochronnych) nie mają odpowiedniej wiedzy ani umiejętności. Gdy uzupełnią braki, to firmy IT zostaną usunięte z tego rynku, bo kamery i rejestratory są dodatkiem do systemów ochrony.*

Jeśli zestawić pogląd wyrażony w ostatnim cytowanym zdaniu (*kamery i rejestratory są dodatkiem do systemów ochrony*) z poglądem cytowanym w poprzednim rozdziale (dozór wizyjny jest dodatkową funkcją systemu informatycznego), to logiczna wydaje się konkluzja, że branża IT jednak nie ma jasnego poglądu na to, czym właściwie jest dozór wizyjny. Ale integrator IT nie musi rozstrzygać takich dylematów i wie swoje: *Dla firm IT branża systemów dozoru wizyjnego to tak naprawdę nic nowego. Układamy sieci, spinamy je z urządzeniami i w tym przypadku jest dokładnie tak samo. Sądzę więc, że dozór wizyjny jest (lub być powinien) naturalnym rozszerzeniem zakresu naszych usług.*

– Tydzień lektury dokumentów kamer

Rok 2014 przyniósł odpowiedź w dyskutowanej przez poprzednie 3 lata kwestii, czy brak specjalistycznej wiedzy umożliwia firmom IT działanie na rynku dozoru wizyjnego, czy też nie: *Reseller, który nie ma dużego doświadczenia we wdrażaniu systemów monitoringu wideo, nie jest na straconej pozycji. Tu nie ma magicznej wiedzy ani konieczności programowania skryptów. **Wystarczy poświęcić tydzień na lekturę dokumentów dostarczanych przez producentów kamer, aby samodzielnie móc zaprojektować niemały system monitoringu*** (podkreślenie autora). [12]

– Kilka dni na nauczenie się podstaw monitoringu; miesiąc przygotowań do pracy na rynku

Rok 2015 przyniósł dwa istotne ustalenia:

1) ***Komuś, kto wdraża sieciówkę, nauczenie się podstaw monitoringu zajmuje kilka dni. Miesiąc przygotowań do pracy na tym rynku w zupełności wystarczy*** (podkreślenie autora).
2) Co ważne, ***wiedza dotycząca tworzenia takiej sieci jest najczęściej nieosiągalna dla tych, którzy dotąd zajmowali się instalowaniem rozwiązań analogowych*** (podkreślenie autora). [14]

Moim zdaniem, zważywszy na fakt, że rok 2015 to – ostrożnie licząc – co najmniej dziesiąty rok obecności IP w dozorze wizyjnym w Polsce, teza o wiedzy nieosiągalnej dla instalatorów analogowych systemów dozoru wizyjnego jest mocno ryzykowna.

– Kompetencje integratorów IP i instalatorów automatyki budynkowej

Trzeba było kolejnych dwóch lat, aby zauważyć, że obraz niezbędnej wiedzy jest jednak bardziej zróżnicowany. *Integratorom z rynku IT potrzebne są kompetencje z zakresu automatyki budynkowej, aby obsługiwać większe kontrakty. Z drugiej strony przedsiębiorstwa, które się w niej specjalizują, muszą uzupełnić wiedzę z obszaru IT. Instalatorzy przyznają, że od pewnego momentu ich działy inżynierskie muszą się wykazywać dobrą znajomością zagadnień informatycznych, po to, aby dobrze porozumiewać się z informatykami pracującymi u klientów końcowych.* [15]

– Nie powinno stanowić problemu...

dołączenie do oferty monitoringu wizyjnego, fizycznej kontroli dostępu i zasilania gwarantowanego dla integratora, który zjadł zęby na budowaniu sieci oraz wdrażaniu aplikacji i systemów. Natomiast kamery IP to dla takiego integratora *po prostu kolejna grupa urządzeń końcowych. Dość specyficzna, bo wymagająca nowych kwalifikacji, chociażby z zakresu optyki.* [16]

– Przewaga integratorów IT nad firmami ochroniarskimi

Duże znaczenie infrastruktury sieciowej w systemach monitoringu sprawia, że rośnie rola kompetentnych firm projektowych, które mają doświadczenie w dziedzinie systemów sieciowych. A to oznacza, że integratorzy IT mają w tym aspekcie przewagę nad firmami ochroniarskimi, którym brakuje wiedzy na temat kompleksowej obsługi informatycznej. Natomiast dla firmy integratorskiej dodanie do oferty systemów monitoringu nie stanowi większego wyzwania. W tym celu wystarczy przede wszystkim poznać kamery i ich możliwości oraz nauczyć się dobierać odpowiednie modele do konkretnych zadań. Należy także wiedzieć, jak obliczyć obciążenie sieci, w której przesyłany będzie obraz z kamer, oraz zasymulować ilość potrzebnej przestrzeni w rejestratorze. [17]

Bardzo trafne spostrzeżenie znalazło się w rozdziale „Jak nie popełniać błędów": *Gdy klient rzuca hasło „zainstalujcie kamery" i nie udaje się z niego wyciągnąć dodatkowych informacji, pojawia się ryzyko, że nie będzie zadowolony z efektów.* Powodów, dla których klient na początku procesu inwestycyjnego nie określa wymagań użytkowych (programu funkcjonalno-użytkowego), może być wiele. Szczególnie niebezpieczne dla dostawcy konsekwencje może mieć sytuacja, w której klient robi to intencjonalnie po to, aby przy odbiorze stwierdzić, że nie tego oczekiwał, i dlatego zapłatę za usługę uwarunkowuje dostawą dodatkowych świadczeń. Po polsku to się nazywa wyłudzanie.

– Wyjście IT ze strefy komfortu i wejście do świata dozoru wizyjnego

*Dla tradycyjnego integratora, który wdraża sieci komputerowe, wejście do świata monitoringu wizyjnego może wydawać się trudne. Kwestie optyki, oświetlenia, doboru kamer, właściwego pokrycia nadzorowanego obszaru itp. **bywają*** (podkreślenie autora) *skomplikowane. Dlatego dla osób, które nie miały dotychczas do czynienia z dozorem wizyjnym, dobrze znane IT pozostaje czymś w rodzaju strefy komfortu. Jednak wyjście z niej okazuje się najczęściej stosunkowo łatwe.* (...) *Dlatego to raczej klasyczni instalatorzy rozwiązań do ochrony, którzy wyrośli na wdrażaniu systemów analogowych, mogą mieć większe problemy z wejściem w świat sieci IP.* [18]

Moim zdaniem kwestie optyki, oświetlenia sceny, doboru kamer, właściwego pokrycia dozorowanego obszaru, kadrowania itp. **są**, a nie tylko **bywają** skomplikowane. Z tego m.in. powodu opracowano europejską normę na systemy dozoru wizyjnego, nie mówiąc już o poradnikach projektowych czy specjalnych oprogramowaniach wspomagających projektowanie pokrycia i kadrowania sceny obserwowanej przez kamerę. Z tego powodu na kursy organizowane przez Polską Izbę Systemów Alarmowych przychodzą kolejni inwestorzy, projektanci, instalatorzy.

– Coraz mniej tajemnic

Ostatni, opublikowany w 2019 r. artykuł nosi tytuł *Monitoring wizyjny: coraz mniej tajemnic.* [19] Interesująca konkluzja 17 lat i 32 artykułów poświęconych dozorowi wizyjnemu.

Najpoważniejszy partner

Prezentując (historyczne) opinie firm z branży IT nt. rynku dozoru wizyjnego, nie chciałbym pominąć reprezentacji tej branży, jaką jest jej samorząd gospodarczy – Polska Izba Informatyki i Telekomunikacji (PIIT). Samorząd jako reprezentant środowiska wypowiada się zazwyczaj w sprawach rangi pierwszorzędnej. Stosowną okolicznością były rozpoczęte w 2014 r. przez MSW prace nad ustawą o monitoringu wizyjnym*. PIIT do swojego wystąpienia o możliwość udziału w pracach ministerstwa (pismo nr PIIT/294/14 z 2014-02-28) dołączyła swoje „CV": *Polska Izba Informatyki i Telekomunikacji (PIIT) istnieje od stycznia 1993 roku, zrzeszając obecnie ponad 140 największych firm sektora teleinformatyki i telekomunikacji. Izba jest więc najpoważniejszym partnerem, zarówno w procesie stanowienia prawa, jak i opiniowania bieżących decyzji administracji rządowej i organów regulacyjnych* (...).

Podzielam pogląd, że samorząd jest (powinien być) partnerem w wymienionych kwestiach, niekoniecznie jednak, że akurat ta izba gospodarcza jest partnerem najpoważniejszym. (Ot i wyższość świata informatyki nad ochroniarskim światem monitoringu). Dominującym wątkiem uwag PIIT do projektu założeń ustawy o monitoringu wizyjnym były – słusznie moim zdaniem – ilość obowiązków nakładanych na administratora systemu oraz ponoszone przez niego koszty na rzecz organów ścigania.

W podsumowaniu (lekko ironicznie)...

Poziom wiedzy branży IT na temat systemów dozoru wizyjnego wzrósł niepomiernie w ciągu tych 17 lat. Firmy IT wiedzą już, że kamery to po prostu kolejna grupa urządzeń końcowych, chociaż dosyć specyficzna, bo wymagająca nowych kwalifikacji, m.in. z zakresu optyki. Ale nie ma co przesadzać z ich zdobywaniem – *wystarczy poświęcić tydzień na lekturę dokumentów dostarczanych przez producentów kamer, aby samodzielnie móc zaprojektować niemały system monitoringu. Przecież komuś, kto wdraża sieciówkę, nauczenie się podstaw monitoringu zajmuje kilka dni. Miesiąc przygotowań do pracy na tym rynku (dozoru wizyjnego) w zupełności wystarczy.*

* Według pisma MSWiA z 24 maja 2016 r. projekt założeń do projektu ustawy o monitoringu wizyjnym został wycofany spod obrad Zespołu ds. Programowania Prac Rządu.

Nie sposób odmówić trafności spostrzeżeniu, że *gdy klient rzuca hasło „zainstalujcie kamery" i nie udaje się z niego wyciągnąć dodatkowych informacji, pojawia się ryzyko, że nie będzie zadowolony z efektów.* Ale nie święci garnki lepią: *dla firm IT branża systemów dozoru wizyjnego to tak naprawdę nic nowego. Układamy sieci, spinamy je z urządzeniami i w tym przypadku jest dokładnie tak samo. To po prostu wzbogacenie obecnie działającego systemu informatycznego o dodatkową funkcję. Dozór wizyjny jest naturalnym rozszerzeniem zakresu usług firm informatycznych, które układają sieci.* I trzeba zająć się tym rozszerzeniem jak najszybciej, bo jak na razie to *w naszym kraju instalowaniem systemów monitoringu zajmują się głównie przedsiębiorstwa niewywodzące się ze świata informatyki, które nie mają globalnej wizji wdrażania takich systemów.*

...(i całkiem serio)

Może się zdarzyć, że w instalacji systemu dozoru wizyjnego IP złożoność infrastruktury sieciowej przewyższy złożoność pozostałych urządzeń – kamer IP, rejestratorów wizji, wyświetlaczy, oprogramowania do zarządzania wizją. Praktyka pokazuje, że nie zawsze można liczyć na należyte wsparcie ze strony firm IT, gdy pojawi się jakiś problem uruchomieniowy lub eksploatacyjny związany ze specyfiką transmisji wizji w sieciach. Powinniśmy unikać relacji biznesowych z tymi firmami IT, które branżę zabezpieczeń traktują jako niewielki rynek zbytu dla swojego produktu. □

Niniejszy artykuł jest zapisem wykładu na kursie „Systemy dozoru wizyjnego wykorzystujące protokół internetowy (IP) do transmisji wizji" organizowanym przez Ośrodek Szkoleniowy Polskiej Izby Systemów Alarmowych.

LITERATURA

[8] Redakcja crn.pl, *Widzę wszystko, wiem wszystko,* 11.06.2010.
[9] Karolina Marszałek, *Cyfrowe oko na fali wznoszącej,* 5.07.2013.
[10] John Honovich, *IT is not transforming Security,* May 3, 2008, ipvm.com.
[11] Karolina Marszałek, *Monitoring IP – różowo nie jest,* 4.09.2013.
[12] Krzysztof Jakubik, *Monitoring wideo: kłopoty z prawem,* 25.06.2014.
[13] Krzysztof Pasławski, *Monitoring wideo: łakomy kąsek dla integratorów,* 10.06.2015.
[14] Tomasz Janoś, *Systemy monitoringu wideo,* 14.10.2015.
[15] Karolina Marszałek, *Monitoring IP: biznes na inteligencji,* 27.09.2017.
[16] Tomasz Janoś, *Monitoring wizyjny, kontrola dostępu i brak przestojów,* 29.05.2018.
[17] Krzysztof Pasławski, *Monitoring potrzebuje infrastruktury,* 8.10.2018.
[18] Tomasz Janoś, *Bezpieczeństwo fizyczne: warto opuścić strefę komfortu,* 28.06.2019.
[19] Wojciech Urbanek, *Monitoring wizyjny: coraz mniej tajemnic,* 11.10.2019.

BIO

Waldemar Więckowski

W branży systemów dozoru wizyjnego od 1984 r. Członek KT 52 w Polskim Komitecie Normalizacyjnym. Doradca Zarządu i pracownik dydaktyczny PISA. Absolwent Politechniki Budapeszteńskiej.

Mądry Polak po szkodzie

O oszczędzaniu na systemach wizyjnych

TEKST
Michał Marciniak

Obecne czasy uczą oszczędności – niepewna sytuacja na rynku pracy, rosnące ceny produktów i koszty usług, inflacja, obniżki stóp procentowych. Wszystko to powoduje, że (prawie) każdy z nas decyduje się na tańsze i niejednokrotnie gorsze rozwiązania, stanowiące kompromis pomiędzy „mieć a chcieć". Czy zatem popełniamy błąd, gdy chcąc wykazać się dozą rozsądku i świadomego wyboru, inwestujemy w sprawdzone rozwiązania bądź aby spełnić minimalne wymagania, wybieramy najtańszą opcję?

Impulsem do napisania tego artykułu jest wszechobecne na naszym rynku poszukiwanie tanich rozwiązań. Żeby była jasność – tanie nie musi oznaczać złe, ale w wielu aspektach wiąże się z gorszymi parametrami, niższą wydajnością i ogólnie marną jakością. Producenci bacznie obserwują rynek i szybko reagują na zachodzące na nim zmiany, wprowadzając coraz tańsze urządzenia z gorszymi podzespołami, szumnie przy tym nadając im nazwy „ECO", „Standard", „Basic" itd. Ma to rozwiać wątpliwości związane z ograniczeniami, jakie wiążą się z ich używaniem. Czy zatem powinniśmy ich unikać i realizować projekty tylko na najwyższych seriach kamer, switchy czy NVR-ów? Odpowiedź jest oczywista: nie. Istotą rzeczy jest znalezienie kompromisu pomiędzy wymaganiami a faktycznymi potrzebami. To trudne zadanie, ale nie jest niemożliwe. Uświadomienie klientowi różnic i korzyści z zastosowania bardziej zaawansowanych rozwiązań jest kluczem do sukcesu i rozbudowy systemu o kolejne komponenty (tym razem nie najtańsze).

Jednym z przykładów, dość często wymuszających zmianę środowiska wizyjnego, jest niska (lub niedostosowana do sceny) jakość rejestrowanego obrazu. Sytuacja taka pojawia się najczęściej tuż po zdarzeniu, które powinno zostać zarejestrowane, a z różnych przyczyn nie można go odtworzyć lub jakość nagrania nie pozwala na jego identyfikację. Oczywiście w pierwszej kolejności należałoby dokonać konserwacji sprzętu (zabrudzenia optyki lub doświetlaczy powodują nierzadko spadek widoczności nawet do 100%) oraz zająć się kwestiami warstwy programowej (aktualizacja systemów, zmiana parametrów kamer, np. niewłączona opcja WDR w prześwietlonych scenach). Wiele problemów może generować niewydajna (lub przeciążona) infrastruktura sieciowa – to kolejny punkt na liście rzeczy do sprawdzenia przed decyzją o wymianie kamer. Jeśli wszystkie te zmiany nie dadzą efektu, należy rozważyć decyzję o wymianie elementów odpowiadających za niską jakość nagrań i być może rozszerzyć projekt o systemy monitorujące działanie poszczególnych elementów.

Przetargi rządzą się swoimi prawami

Nie od dzisiaj wiadomo, jakie kryteria rządzą przetargami publicznymi. W większości na pierwszym miejscu jest cena (najniższa), potem długo, długo nic i dopiero wtedy następuje lista dodatkowych wymagań (rozszerzona gwarancja, opcje serwisowe itp.). Do czego prowadzi takie podejście, również nie jest tajemnicą: kuriozalne dostawy urządzeń wprawdzie zgodnych ze specyfikacją zamówienia, jednak bez uwzględnienia jakości i trwałości wyspecyfikowanych elementów. Ostatecznie (w wielu przypadkach) wiązało się to z brakiem możliwości wykorzystania w pełni pierwotnych założeń i parametrów, funkcji zamawianych podzespołów. Należy również uwzględnić błędy opisowe w trakcie realizacji procesu zamówienia.

Czy tych błędów można uniknąć? Czy zamówienie opisujące kamerę jako „kamera IP 2 Mpix – 40 sztuk" nie jest zbyt ogólne i daje pole do popisu nieuczciwym dostawcom? Absolutnie nie sugeruję stosowania opisów wskazujących na jednego vendora (czego zresztą zakazuje prawo), ale jest wiele parametrów, które pozwolą wybrać urządzenia markowe, z prawdziwym serwisem i wsparciem w postaci aktualizacji zabezpieczeń, tak że z pewnością będzie można liczyć na korzystne rozstrzygnięcie przetargu. Sednem sprawy jest tu proces zapytania ofertowego i dialogu z dostawcami oraz integratorami. Kompromis – to słowo pojawia się dość często, ale ocena konkretnego przypadku przez integratora pozwoli precyzyjnie dobrać parametry urządzeń i zastosować takie podzespoły, które nie spowodują problemów instalacyjnych (np. integracja z istniejącą infrastrukturą sieciową, niedoszacowane miejsce na nagrania, brak istotnych detali sceny w zarejestrowanym materiale itp.).

Prywatnie nie jest lepiej

Czy firmy prywatne i odbiorcy indywidualni działają podobnie? I tak, i nie. Niestety, sfera zarówno ogólnie pojętego IT, jak i systemów zabezpieczeń (wizyjne, KD, alarmowe itd.) jest często kulą u nogi dla wielu inwestorów lub właścicieli. Co ciekawe, wymiana telefonu na nowy model w cenie 5–7 tys. zł dla całej kadry menedżerskiej nie stanowi problemu, gdyż to namacalny produkt, który nie ginie w czeluściach serwerowni, jak nowe switche, routery czy NVR.

Mój poprzedni artykuł w A&S (nr 2/2020) dotykał kwestii bezpieczeństwa i zarządzania ryzykiem w systemach wizyjnych. W tym mamy dokładnie ten sam problem – tanie urządzenia dość szybko tracą aktualizacje producenta, bowiem – w dużym skrócie – nie opłaca się ich wspierać i angażować armii deweloperów, testerów i inżynierów w ramach kolejnych poprawek. Z marketingowego punktu widzenia łatwiej wyprodukować nowy produkt i sprzedawać go jako zupełnie nową wersję. I tu pojawia się problem. W wielu przypadkach proces migracji z jednego urządzenia (lub systemu) na inny, nowy wymaga tygodni, a nawet miesięcy przygotowań. Wiąże się też z kosztami zasobów ludzkich, reorganizacją pracy, oprogramowania i w końcu przyzwyczajeń.

Czy zatem lepiej nic nie zmieniać i iść przetartym szlakiem? Niestety dzisiaj nie jest to możliwe. Systemy ewoluują, kończy się ich wsparcie producenckie (EOL), urządzenia przestają spełniać swoje zadanie (np. rejestratory nie obsługują nowych rozdzielczości, funkcjonalności) i co najważniejsze – pojawia się coraz więcej podatności bezpośrednio wpływających na bezpieczeństwo. To naturalny proces i trzeba się z nim liczyć. Można jednak korzystać z rozwiązań, które umożliwią prosty proces migracji. Warto korzystać z otwartych technologii (a nie prawnie chronionej struktury, która „przykuwa" nas do jednego vendora), by móc liczyć na wsparcie producenta lub integratora nawet w przypadku skomplikowanych projektów aktualizacji środowiska. Takie podejście pozwala budować heterogeniczne środowiska, składające się z różnych podzespołów, które mogą ze sobą współpracować ze względu na jednolity protokół.

> Warto korzystać z otwartych technologii, by móc liczyć na wsparcie producenta lub integratora nawet w przypadku skomplikowanych projektów

TCO i ROI

Jak zatem przekonać inwestora lub też samego siebie do poniesienia większych (pozornie) kosztów początkowych? Najlepiej korzystać z wyliczeń bazujących na wskaźnikach TCO (*Total Cost of Ownership*) i ROI (*Return-on-Investment*), co w ostatecznym rozrachunku pokaże przewagę droższych, ale też bardziej zaawansowanych systemów. W tym zestawieniu bezpieczeństwo stanowi czynnik trudny do zdefiniowania i przełożenia na konkretne kwoty. Czy możemy stać się ofiarą ataku? Czy przechowywane przez nas dane mogą wyciec? Czy ktoś uzyska dostęp do naszych nagrań?

Te pytania powinny pojawiać się w trakcie omawiania nowego lub aktualizacji starego systemu. Sami nie jesteśmy w stanie opracować ich pełnego zestawu, ale korzystając z pomocy dystrybutora, osiągniemy satysfakcjonujący efekt w postaci dokumentu opisującego wszelkie korzyści w kontekście przewidywanych wydatków. Takie podejście da nam obraz planowanej inwestycji nie tylko w ramach samego kosztu zakupu, ale także pokaże całościowe korzyści w perspektywie miesięcy lub nawet lat (koszty wsparcia, serwisu, wymiany, aktualizacji itd.).

Tanio i dobrze?

Czy o tańszych rozwiązaniach powinniśmy zapomnieć i w żadnym razie nie sięgać po nie? Zdecydowanie nie. Głównym wyznacznikiem jest zachowanie zdrowego rozsądku – instalacje redundantne (zarówno dotyczące rejestracji materiału, jak i zasilania) są konieczne np. w obiektach infrastruktury krytycznej, ale nie w przypadku małych lokali użytkowych, gdzie chroniona wartość jest dużo mniejsza. Chociaż i tutaj należy rozważyć kilka wariantów i zastosować kamery spełniające konkretny cel, np. kamera nad kasą, której rozdzielczość pozwoli identyfikować przepływ gotówki pomiędzy kasjerem a klientem, lub też użyć rejestratora POS zbierającego dane z kas fiskalnych i powiązania ich z konkretnym wydarzeniem. Podobnie w przypadku prostych systemów do ochrony prywatnych posesji – rejestrowanie danych na kartach SD, korzystanie z połączeń Wi-Fi w kamerach nie jest tu krytyczne i z perspektywy prywatnego użytkownika w pełni akceptowalne.

Kluczową dla klienta sprawą jest sprawdzony dostawca, integrator, na którym można polegać, który zadba o profesjonalne wdrożenie i serwis. Przekłada się to na długofalową współpracę, w dłuższej perspektywie generującą stabilne zyski. □

BIO

Michał Marciniak

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

Technologia głębokiego uczenia w monitoringu wizyjnym – urządzenia na miarę 5G

TEKST
Konrad Badowski

Technologie 5G związane z najnowszą generacją sieci komórkowych otwierają nowe możliwości w dozorze wizyjnym. Cechująca się nieporównywalną z dotychczasowymi sieciami przepustowością sieć nowej generacji udźwignie do 1 miliona urządzeń na kilometr kwadratowy, komunikujących się ze sobą w czasie rzeczywistym. Raport Digital Poland *5G szanse, zagrożenia, wyzwania* nie pozostawia wątpliwości – urządzenia będą się komunikowały szybciej i sprawniej, w zasadzie bez opóźnień (do 1 ms!), nawet będąc w ruchu, i to przy prędkościach do 500 km/h.

Biorąc pod uwagę tendencję do przenoszenia całej mocy obliczeniowej do urządzeń na brzegu sieci, a więc bezpośrednio do urządzeń końcowych, kamery będą w najbliższej przyszłości analizowały obraz oraz komunikowały się między sobą i z pozostałymi urządzeniami Internetu rzeczy (IoT) w dowolnych zastosowaniach, zarówno *smart city*, jak i przemysłowych, w ochronie zdrowia czy infrastrukturze krytycznej.

Raport Omdia *Video Surveillance & Analytics Intelligence Service*, opublikowany w lipcu 2020 r. wskazuje, że kluczowym trendem, który będzie kształtował rynek zastosowań wbudowanej analityki wizji, jest możliwość przeprowadzania podstawowych analiz właśnie w urządzeniach na brzegu sieci. Ze względu na rosnącą ilość danych, a także coraz wyższą jakość obrazów Omdia prognozuje, że całkowita moc obliczeniowa będzie się przesuwać w kierunku rozwiązań brzegowych.

To nie wszystko. Aby w pełni wykorzystać potencjał monitoringu wizyjnego w sieci 5G, budowanej z wykorzystaniem transmisji bezprzewodowej, wymagana jest adaptacja najnowszych dostępnych technologii. Kamery wyposażone w oprogramowanie analityczne będą korzystać z uczenia maszynowego, a przede wszystkim tzw. uczenia głębokiego (*deep learning*) z wykorzystaniem sieci neuronowych. We wspomnianym raporcie Omdia prognozuje się, że odsetek inteligentnych kamer z analizą głębokiego uczenia wzrośnie z ok. 8% w 2019 r. do ponad 58% w 2024 r.

W ramach programu Axis Application Development Partner[1] wspierającego integrację oprogramowania firm trzecich z otwartą platformą AXIS Camera Application Platform, powstało już pierwsze rozwiązanie tej klasy. Procesor działający na zasadzie głębokiego uczenia (*DLPU – Deep Learning Processing Unit*) został opracowany pod kątem umożliwienia kompleksowej analizy obrazu przez firmę BriefCam[2] (światowego lidera rozwiązań do analizy wizji), która wykorzystała najnowszą kamerę wyposażoną w dedykowany układ DLPU[3], aby przetwarzać metadane bezpośrednio w kamerze, czyli na brzegu sieci. Dzięki temu wyszukiwanie informacji w zapisanym materiale wizyjnym może być dużo szybsze i wymagać znacznie mniejszej mocy obliczeniowej po stronie serwera. Dzięki temu rozwiązaniu w niedalekiej przyszłości monitoring wizyjny będzie tańszy i prostszy, mniejsze też będą wymagania dotyczące przepustowości sieci. We wdrożeniach na większą skalę elastyczność i efektywność będą nieporównywalne z rozwiązaniami opartymi na analizie serwerowej.

Takie rozwiązania w dozorze wizyjnym zapewniają przydatne informacje z zakresu bezpieczeństwa i ochrony oraz szerszą wiedzę biznesową. Ponadto dzięki analizie obrazu realizowanej w urządzeniach brzegowych znika ograniczenie budowy lub rozbudowy systemu wynikające z przepustowości sieci. Nawet dla dużych systemów rozwiązania oparte na chmurze obliczeniowej stają się dostępne i uzasadnione ekonomicznie. Uczenie maszynowe, a zwłaszcza uczenie głębokie w dozorze wizyjnym otwiera przestrzeń dla niemal niezliczonych zastosowań – wielu z nich jeszcze nie znamy. System oparty na analizie realizowanej na brzegu sieci będzie też mógł reagować znacznie szybciej i bardziej precyzyjnie na wykryte incydenty.

System monitoringu wizyjnego, który na podstawie gromadzonych danych potrafi przewidzieć wybryki chuligańskie czy decyzje zakupowe albo ocenić atrakcyjność punktu handlowego w oparciu na zachowaniach grup lub pojedynczych osób, który podpowiada służbom, zarządom miejskim czy właścicielom sklepów, co się wydarzy – jest w zasięgu ręki. Technologia *deep learning*, wsparcie niezliczonych urządzeń IoT poprzez sieć 5G oraz otwarte, łatwo integrowalne z dowolnym oprogramowaniem systemy monitoringu otwierają świat wyobraźni i potrzeb na namacalną rzeczywistość.

1) https://www.axis.com/pl-pl/partners/adp-partner-program
2) BriefCam Video Content Analytics
3) Pierwszą taką kamerą jest AXIS Q1615 Mk III z podwójnym chipsetem ARTPEC-7

AXIS Q16 15 Mk III z podwójnym chipsetem ARTPEC-7

Nowości SATEL – jesień 2020

Nowe centrale alarmowe, moduły komunikacyjne i czujki bezprzewodowe – to główne pozycje, które z początkiem października znalazły się w ofercie SATEL. Ich funkcjonalności i oferowane możliwości zastosowania odpowiadają zmieniającym się potrzebom rynku i oczekiwaniom klientów.

Centrale alarmowe PERFECTA-IP

Rodzina PERFECTA powiększyła się o modele PERFECTA-IP 32 oraz PERFECTA-IP 32-WRL wyposażone w ethernetowy moduł komunikacyjny. Umożliwia on zdalną konfigurację systemu z użyciem programu PERFECTA Soft, przesyłanie kodów zdarzeń do stacji monitorujących, a także zdalne sterowanie i wgląd w stan systemu z aplikacji mobilnej PERFECTA CONTROL. Użytkownicy aplikacji mogą być powiadamiani o wybranych zdarzeniach komunikatami PUSH oraz wyświetlać obraz z kamer rozmieszczonych w nadzorowanym obiekcie.

Moduł komunikacyjny INT-GSM LTE

INT-GSM LTE to moduł umożliwiający centralom INTEGRA i INTEGRA Plus komunikację przez sieci komórkowe 4G, 3G lub 2G. Może on realizować monitoring zdarzeń i wysyłać powiadomienia. Systemem, w którego ramach pracuje, można sterować zdalnie za pomocą SMS, CLIP, programu GUARDX oraz aplikacji INTEGRA CONTROL. Jego atutem jest możliwość współpracy z modułem ethernetowym ETHM-1 Plus – sieć komórkowa stanowi wówczas zapasowy tor łączności dla Ethernetu. Razem mogą realizować monitoring dwutorowy (*Dual Path Reporting*) zgodnie z normą EN 50136.

Moduł telefoniczny GSM-X-PSTN

GSM-X-PSTN to urządzenie przeznaczone do pracy z GSM-X LTE i GSM-X – uniwersalnymi modułami komunikacyjnymi. Po podłączeniu GSM-X-PSTN mogą one wysyłać kody zdarzeń do stacji monitorującej za pośrednictwem sieci telefonicznej PSTN (nawet w sytuacji, gdy działają autonomicznie – nie współpracują z centralą alarmową wyposażoną w dialer). Kanał ten może być używany równolegle lub wymiennie z transmisją danych przez sieć komórkową.

Czujka zmierzchu i temperatury ADD-200

Zewnętrzna bezprzewodowa czujka ADD-200 rozszerza rodzinę urządzeń dwukierunkowego systemu bezprzewodowego ABAX 2 (868 MHz). Wbudowany czujnik zmierzchu umożliwia pomiar natężenia światła od 2 lx do 250 lx. Możliwy jest wybór jednego z 16 progów zadziałania – czujka informuje o spadku natężenia światła poniżej progu (alarm) i powrocie powyżej progu (koniec alarmu). Czujka jest odporna na krótkotrwałe (<3 min) lub przypadkowe zmiany oświetlenia.

Temperatura jest mierzona w zakresie -30°C...70°C. Jej wartości są na bieżąco przesyłane do kontrolera systemu bezprzewodowego. Czujka może też reagować na przekroczenie zadanego progu temperatury – górnego lub dolnego. ADD-200 idealnie sprawdzi się przy realizacji funkcji automatyki budynkowej.

Czujka uniwersalna MXD-300

Do urządzeń bezprzewodowego systemu MICRA (433 MHz) dołączyła wielofunkcyjna czujka MXD-300. Podczas konfigurowania można zdecydować, czy będzie pracować jako czujka:

- magnetyczna,
- magnetyczna z wejściem roletowym,
- wstrząsowa,
- wstrząsowa i magnetyczna,
- zalania wodą (wymaga dodatkowej sondy FPX-1).

Może współpracować z centralami alarmowymi PERFECTA WRL, kontrolerami VERSA-MCU i MTX-300, a także modułem alarmowym MICRA.

Tester sygnału radiowego ABAX 2

ARF-200 pozwala sprawdzić poziom szumu radiowego w paśmie częstotliwości używanym przez urządzenia systemu ABAX 2, a także poziom sygnału odbieranego i wysyłanego przez te urządzenia. Dzięki temu można szybko ocenić, czy w danym miejscu panują warunki sprzyjające poprawnej komunikacji między kontrolerem a innym urządzeniem radiowym (np. czujką) jeszcze przed jego zamontowaniem.

Więcej informacji na temat nowości znajduje się na www.satel.pl

SATEL

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

Różne oblicza bezpieczeństwa

wartości pieniężnych

Zarządzanie ryzykiem musi być faktyczne, funkcjonujące i w pełni efektywne. Realizowane zza biurka takim nie jest

Gdy myślimy o instytucjach finansowych, pierwszym skojarzeniem są banki. Sektor finansowy jest jednak obszerniejszy i należy go postrzegać nie tylko przez pryzmat pieniędzy, ale także wartości pieniężnych w ich szerokim rozumieniu. Brak legalnej definicji „pieniądza" może wynikać z trudności sformułowania jego jednoznacznej definicji ze względu na złożoność tego pojęcia w rozumieniu zarówno prawnym, jak i ekonomicznym[1]. Dlatego dla wielu osób te pojęcia są tożsame.

TEKST
Jacek Grzechowiak

Pomocą w zrozumieniu pojęcia pieniądza służy prawodawstwo, w szczególności wydane na podstawie Ustawy o ochronie osób i mienia [2] *Rozporządzenie w sprawie wymagań, jakim powinna odpowiadać ochrona wartości pieniężnych przechowywanych i transportowanych przez przedsiębiorców i inne jednostki organizacyjne* [3]. Zgodnie z nim pod pojęciem „wartości pieniężne" rozumie się nie tylko pieniądze – czyli krajowe i zagraniczne znaki pieniężne, jak to określono w rozporządzeniu – ale także:

1. czeki, z wyjątkiem czeków zakreślonych, skasowanych lub opatrzonych indosem pełnomocniczym, zawierającym wzmiankę „wartość do inkasa", „należność do inkasa" lub inną o podobnym charakterze;
2. weksle, z wyjątkiem weksli opatrzonych indosem pełnomocniczym zawierającym wzmiankę „wartość do inkasa" lub inną o podobnym charakterze;
3. inne dokumenty zastępujące w obrocie gotówkę;
4. złoto, srebro i wyroby z tych metali, kamienie szlachetne i perły, a także platynę i inne metale z grupy platynowców, z wyjątkiem przedmiotów będących muzealiami.

Jak widać, nasze prawodawstwo uznało, że wartości pieniężne są pojęciem znacznie szerszym, wprowadzając niemonetarne kategorie tej kategorii chronionego mienia. To ściśle wiąże się z szerszym spectrum zagrożeń charakterystycznych dla nich. Zanim przyjrzymy się temu bliżej, warto przypomnieć, iż wartości pieniężne są najbliższe wartości pieniądza, co oznacza, że w nielegalnym obiegu (wprowadzane do obiegu mienie pochodzące z czynów zabronionych, zwane potocznie „praniem") przynoszą największy zysk. I to jest podstawowa przyczyna tak dużego zainteresowania środowisk przestępczych.

Należałoby także przyjrzeć się temu mieniu z perspektywy operacyjnej, dotyczącej nie tylko działań ochronnych, ale także ciągłości biznesu. W grupie wartości pieniężnych mamy bowiem metale z grupy platynowców, które obecnie znajdują coraz więcej zastosowań w motoryzacji, medycynie i elektronice, a to tylko przykładowe branże [4]. Obecnie są one traktowane jako dobro podlegające szczególnemu zainteresowaniu środowisk przestępczych, a jednocześnie incydenty z nimi związane mają z reguły bardzo wysoką wartość strat. Przykładami mogą być napad i kradzież palladu na kwotę 300 tys. dolarów z zakładów 3V Sigma w Georgetown [5]. Metale te są podatne na kradzież tak bardzo, że złodzieje kradną też wyroby je zawierające, w celu odzyskania tych metali, np. katalizatory samochodowe, kradzione nie tylko z zakładów produkcyjnych czy centrów logistycznych, ale także bezpośrednio z pojazdów [6]. Jak widać, wartości pieniężne mogą przybierać nieoczekiwaną postać i – podobnie jak techniki kradzieży – ewoluują adekwatnie do naszego rozwoju.

Przykład metali z grupy platynowców ma jedynie zobrazować, że zbliżoną (a czasem nawet przekraczającą) wartość do złota mogą mieć inne metale lub substancje, jeśli tylko wartość jednostkowa zawierających je wyrobów jest odpowiednio wysoka, a potencjalny zbyt istnieje. To powinno nas skłaniać do nieszablonowego myślenia i niezawężania pojęć, a ich rozszerzania – nie tylko w wyniku znajomości prawa, prawo nigdy bowiem nie nadążało za rozwojem cywilizacyjnym.

Tak więc to na zarządzających bezpieczeństwem spoczywa obowiązek odpowiedniej oceny zasobów chronionych. Drugi ważny wniosek, jaki wynika z podanych przykładów, dotyczy miejsc przechowywania wartości pieniężnych. Jak widać, są to nie tylko instytucje finansowe, ale też zakłady przemysłowe, sklepy czy centra logistyczne. To samo dotyczy ich transportowania. Choć widząc codzienną praktykę (i nie mam na myśli wyłącznie Polski), wydaje się dalekie od efektywności. Temat jest obszerny i ciekawy, powinien zainteresować specjalistów ds. bezpieczeństwa.

Dość powszechną praktyką jest sprowadzanie instytucji finansowych do banków lub instytucji operujących pieniędzmi. Ma to pewne uzasadnienie, jednak pamiętając przytoczoną już definicję wartości pieniężnych, trzeba zwrócić uwagę również na inne instytucje, które nie mieszczą się ściśle w sektorze finansowym, a przechowują w swoich obiektach wartości pieniężne. One także są przedmiotem zainteresowania środowisk przestępczych, a tym samym występują tam różnego rodzaju incydenty kryminalne.

Spojrzenie przez pryzmat incydentów będzie nie tylko ciekawe, ale także inspirujące do szerszego postrzegania tej grupy instytucji. Jednocześnie ze względu na cechy incydentów, do jakich doszło, i kreatywność środowisk przestępczych, powinno znaleźć odzwierciedlenie w tak samo kreatywnym, a byłoby idealnie – bardziej kreatywnym myśle-

niu struktur bezpieczeństwa. Przytoczone trzy przykłady są szczególnie interesujące.

Hatton Garden

Jest kwiecień 2015. W londyńskiej dzielnicy Hatton Garden znajduje się przedsiębiorstwo zajmujące się przechowywaniem diamentów. Podziemny magazyn ma wiele skrytek depozytowych. Uznawany za bardzo bezpieczny, jest wykorzystywany przez pobliskich jubilerów do przechowywania swoich zapasów kamieni szlachetnych, głównie diamentów. Są przekonani, że sami nie są w stanie zapewnić takiego poziomu bezpieczeństwa, jak wyspecjalizowana firma. Skarbiec ten stał się obiektem zainteresowania kilku starszych panów – doświadczonych złodziei, uznawanych nawet przez policję za niegroźnych już emerytów. **Tu pierwsza refleksja:** *osoby wydawałoby się już poza obiegiem potrafią stawić czoło nowoczesnym rozwiązaniom w systemie bezpieczeństwa – wszak skarbiec musi być zabezpieczony w sposób nowoczesny. Nie należy więc ich lekceważyć.*

Złodziejski zespół kierowany przez 73-latka zaplanował atak w czasie długiego weekendu. Zaopatrzony w przemysłową wiertnicę wszedł przez szyb windowy, po czym przewiercił trzykrotnie 50-centymetrową betonową ścianę. **Tu pojawia się druga refleksja:** *nie lekceważ emerytów, zwłaszcza tych pozornych. Ich doświadczenie przynosi, jak widać, ciekawe i – co ważniejsze – skuteczne pomysły.*

Złodzieje dostali się do wnętrza, otwierając 73 z 999 [7] skrytek depozytowych i kradnąc diamenty o wartości 200 mln funtów [8]. Jak widać, potencjał był dużo większy, choć i tak wartość strat jest gigantyczna. Co prawda złodzieje popełnili wiele błędów, w czego wyniku zostali szybko ujęci, ale to nie uchroniło w żaden sposób reputacji skarbca, który pół roku później musiał zostać zlikwidowany. W przypadku Hatton Garden osoby korzystające z usług bezpiecznego przechowywania wartości pieniężnych utraciły zaufanie w sposób jednoznaczny i trwały. Najbardziej wymownym dowodem jest pewne zdjęcie, gdzie na szyldzie widać przyklejoną kartkę z jedynie dwiema literami „UN", zmieniającymi słowo *safe*, znajdujące się w nazwie, na *unsafe*. Wymowa druzgocząca.

Kamienie szlachetne były, są i będą obiektem pożądania, także przez złodziei. Można by dawać inne przykłady, stare, jak z londyńskiej Baker Street (1971 r.), i nowsze, z Amsterdamu (2003 r.) czy lotniska Schiphol (2005 r.). Wartość strat jest wysoka i ma negatywny wpływ na wizerunek. Czasem tak krytyczny, jak w przypadku Hatton Garden. **Stąd refleksja trzecia:** *wartość chronionego mienia jest ważną determinantą środków ochronnych, ale zarówno w analizach bezpieczeństwa, jak i w doborze rozwiązań ochronnych reputacja zawsze powinna być traktowana jako jeden z najważniejszych zasobów chronionych* [9].

Napad na G4S w Sztokholmie

Jest 23 września 2009 r. Zapowiada się słoneczny i całkiem ciepły jak na Szwecję dzień, niezwiastujący żadnych spektakularnych zdarzeń. Centrum obsługi gotówki największej światowej firmy ochrony położone w południowej sztokholmskiej dzielnicy Västberga pracuje jak zwykle, choć ze względu na porę wszyscy są już znużeni, a więc i mniej czujni. Budynek – jak przystało na jego profil – zabezpieczony na wysokim poziomie, ale... Tuż po godz. 5:15 na jego dachu ląduje śmigłowiec, z którego wychodzą napastnicy, rozbijają szyby w świetlikach. Szyby są wzmocnione, ale napastnicy mają młot kowalski. Jest wystarczająco ciężki, więc szybko je rozbijają i wchodzą do wnętrza. Zaskoczona 20-osobowa obsługa nie zdążyła właściwie nic zrobić. Akcja jak z hollywoodzkiego filmu – szybko, sprawnie, skutecznie. Rzecznik sztokholmskiej policji powie później „Nigdy czegoś takiego nie doświadczyłem" [10]. **Pierwsza refleksja:** *żaden scenariusz ataku nie jest absurdalny. A przynajmniej nie powinien być.*

Wszystko wskazuje na to, że procedury zadziałały, bo policja przybywa jeszcze przed ucieczką złodziei, którzy zadbali o zablokowanie dróg wokół budynku, by uniemożliwić dojazd radiowozów policyjnych. Mimo to policja dojeżdża, ale nie interweniuje, bo ma informację o użyciu broni maszynowej. Czekają na „specjalsów". Złodzieje zyskali wystarczająco dużo czasu, by ukraść 39 mln koron (równowartość około 5,3 mln dolarów) [11] i kilka minut później odlecieć nieniepokojeni i nieścigani, bo – tu kolejna ciekawostka – policyjne śmigłowce zostały unieruchomione atrapami bomb. Policja jest bezradna. Złodzieje uciekają, a ich śmigłowiec zostaje znaleziony dopiero 3 godziny później. Wygląda to niesamowicie: kradzież śmigłowca – wylądowanie na dachu – blokada dróg – unieruchomienie pościgu na lotnisku policyjnym...

Późniejsze spekulacje mówią jeszcze o tym, że użyty przez napastników śmigłowiec nie był przypadkowy. Inne nie mieściłyby się na dachu, ten jeden – tak. Ktoś najwyraźniej znał wymiary dachu. **Refleksja druga:** *w bezpieczeństwie nie ma informacji nieważnych. Wymiar dachu też może być ważny – trzeba „tylko" wyobrazić sobie incydent.*

Napad ten ma tak wiele wymiarów, że wciąż rozpala umysły analityków. Ilość i zakres informacji potrzebnych do jego zaplanowania jest zdumiewająca. Przywodzi na myśl operacje wojskowe. I słusznie, bo wiele wskazuje, że wśród napastników znajdował się były żołnierz sił specjalnych. Do tego dochodzi liczba miejsc „zaatakowanych" jeszcze przed napadem, a szczególnie lotnisko policyjne, na którym za pomocą atrap bomb unieruchomiono śmigłowce, umożliwiając złodziejom w ten sposób ucieczkę, a przynajmniej wydłużając ich czas dyspozycyjny. Wreszcie działania podjęte wokół budynku, a utrudniające policji dojazd na miejsce zdarzenia. **To skłania do refleksji trzeciej**: *jeśli twoje mienie jest tego warte, złodzieje, aby zabezpieczyć swoją główną operację, nie zawahają się przed zaatakowaniem obiektów zewnętrznych, a nawet służb państwowych.*

Nasz napad stulecia

Polacy nie są „gorsi". I my również mamy ciekawy, a nade wszystko pouczający przykład, jakim jest dokonana w 2015 r. w Swarzędzu kradzież pieniędzy z bankowozu. Jej scenariusz można by wykorzystać w filmie. Pojawia się w nim człowiek zrekrutowany do wykonania operacji, posiadający nie tylko zmienione dane personalne, ale także farmakologicznie zmienioną fizjonomię [12]. Człowiek ulokowany w miejscu, gdzie jest nowy i nikt go nie zna, nie utrzymuje z nikim kontaktów, co nie dziwi nikogo. Na dodatek to swego rodzaju dziwak: chodzi wciąż w rękawiczkach, różne czynności wykonuje biodrami. Jest jakaś wiarygodna wymówka o chorobie skóry. To wszystko jednak pojawi się dopiero po incydencie. Ponadto – także po tym wydarzeniu – okazuje się, że nie zostawił żadnych śladów: pusta szafka ubraniowa, zero śladów biologicznych. To samo w samochodzie. Wydawałoby się idealny wykonawca.

Refleksja pierwsza: *odmienność też może być symptomem, a relacje interpersonalne narzędziem zmniejszającym ryzyko zagrożeń wewnętrznych.*

W napadzie skradziono 7 mln zł, praktycznie bez pozostawienia śladów, skutecznie neutralizując monitoring bankowozu, czyli pojazdu wymagającego najwyższego poziomu zabezpieczenia. Już w trakcie dochodzenia zaczynają się pojawiać niepokojące informacje dotyczące fałszywych dokumentów, także uprawnień pracownika ochrony. Jednak nade wszystko pojawia się drugie, poważniejsze ryzyko w postaci potencjalnych powiązań sprawcy z członkiem najwyższego kierownictwa spółki. Od razu występuje też porównanie z innym napadem, też w Swarzędzu w roku 1993, kiedy uzbrojeni napastnicy podający się za pracowników agencji ochrony dokonali napadu, rabując 5 mln zł (wartość z 1993 r.), choć był on zupełnie inny w swej formie [13].

Z biegiem czasu dowiadywaliśmy się coraz więcej zarówno o przygotowaniach, jak i przebiegu samego incydentu, coraz wyraźniej widząc, jak duży potencjał ryzyka tkwi w pracownikach właściwie na każdym poziomie organizacji. Domniemany przywódca ulokowany na najwyższym poziomie, potrafiący zorganizować wszystkie, personalne i organizacyjne, szczegóły incydentu. Do tego niewielka czujność współpracowników, współistniejąca z gruntownie przemyślanym planem, realizowanym precyzyjnie (nie wszędzie, ale w zdecydowanej większości), przyniosły efekt w postaci wystąpienia incydentu, a dodatkowo zaskoczenia właściwie wszystkich poziomów organizacji.

To skłania do refleksji drugiej: *działania ochronne muszą mieć zdywersyfikowany dostęp do informacji o nich, aby cały proces był maksymalnie chroniony. Zasada wiedzy koniecznej, funkcjonująca od lat w ochronie informacji niejawnych, jest tu zdecydowanie zalecana.*

Incydent ten ma jeszcze jeden ważny aspekt dotyczący pokrycia ubezpieczeniowego. W tym przypadku ubezpieczyciel odmówił wypłaty odszkodowania, wskazując, iż agencja ochrony naruszyła przepisy dotyczące ochrony osób i mienia. Co ważniejsze, ubezpieczyciel był w stanie obronić swoje stanowisko przed sądem [14]. Nie mając pełnej wiedzy w tym zakresie, trudno ocenić, jak ta sprawa się skończy. Należy jednak pamiętać o tej kwestii zarówno podczas wyboru agencji ochrony, jak i w trakcie realizacji przez nią usług.

To samo zresztą dotyczy agencji ochrony, które niekiedy nie analizują swojego modelu operacyjnego, a nawet nie weryfikują zaleceń organów kontrolnych, które przecież nie muszą być nieomylne. Niezmiernie ważne jest to, że incydent, zwłaszcza duży, w przypadku braku pokrycia ubezpieczeniowego może skutkować problemami nie tylko agencji ochrony, ale także instytucji finansowej. Ryzyko niewypłacalności obu stron jest tu realne.

Stąd refleksja trzecia: *zarządzanie ryzykiem nie jest procesem dedykowanym dużym firmom, ale wszystkim, bo każda działalność jest związana z podejmowaniem ryzyka.* I jeszcze jedno. Zarządzanie ryzykiem musi być faktyczne, funkcjonujące i w pełni efektywne. Realizowane zza biurka takim nie jest. □

1) Nowak-Far A. (red.) (2011), *Finanse publiczne i prawo finansowe*, wyd. C.H. BECK, Warszawa.
2) Dz.U. z 2020 r., poz. 838.
3) Dz.U. z 2016 r., poz. 793.
4) https://www.naukowiec.org/wiedza/chemia/metale-z-grupy-platyny_3178.html [dostęp: 10.11.2020]
5) https://www.postandcourier.com/news/experienced-thieves-steal-300-000-worth-of-precious-metal-in-overnight-heist-on-sc-river/article_9f07676a-baa0-11e9-842d-7b45828cf22e.html [dostęp: 10.11.2020]
6) https://qz.com/1536731/thieves-are-breaking-into-u-hauls-to-steal-catalytic-converters-for-palladium/ [dostęp: 10.11.2020].
7) https://www.bbc.com/news/uk-england-london-32414531?ocid=socialflow_twitter [dostep:10.11.2020]
8) https://en.wikipedia.org/wiki/Hatton_Garden_safe_deposit_burglary [dostęp: 10.11.2020]
9) https://www.dailystar.co.uk/news/latest-news/hatton-garden-safe-deposit-ltd-17335030 [dostęp: 10.11.2020].
10) https://www.theguardian.com/world/2009/sep/23/swedish-cash-depot-helicopter-raid [dostęp: 10.11.2020]
11) https://www.thelocal.se/20101007/29474 [dostęp: 10.11.2020].
12) https://wiadomosci.wp.pl/skok-stulecia-falszywy-konwojent-ukradl-prawie-8-milionow-jest-wyrok-6389412386276993a [dostęp: 10.11.2020].
13) https://pl.wikipedia.org/wiki/Napad_na_konw%C3%B3j_pieni%C4%99dzy_Swarz%C4%99dzkiej_Fabryki_Mebli [dostęp: 10.11.2020].
14) https://businessinsider.com.pl/wiadomosci/napad-stulecia-firma-ochroniarska-servo-nie-dostanie-odszkodowania/qlf6g6h [dostęp: 10.11.2020].

BIO

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.

ProtegeGX – zintegrowany system bezpieczeństwa dla obiektów sektora finansowego

Banki i inne instytucje finansowe mają wyjątkowo wysokie wymagania dotyczące bezpieczeństwa. Klienci muszą być pewni, że zdeponowane aktywa i inwestycje są dobrze chronione, a ich bezpieczeństwo jest na najwyższym poziomie.

ICT ProtegeGX

Napady i oszustwa w sektorze finansowym to zagrożenia o dużym poziomie ryzyka, dlatego szczególną uwagę należy zwracać na wybór systemu zabezpieczenia chroniącego nie tylko budynki, ale także szczególne obiekty, np. bankomaty czy skarbce. Dostęp do nich – zarówno klientów, jak i personelu – musi być ściśle kontrolowany, mieć wiele poziomów zabezpieczeń, aby instytucje mogły sprawnie działać 24 godz./dobę, 7 dni w tygodniu, 365 dni w roku.
Rozwiązaniem dla wielu tych specyficznych wymagań jest Zintegrowany System Bezpieczeństwa ProtegeGX, oferujący bardzo rozbudowaną funkcjonalność oraz integrację systemów KD, SWiN, CCTV i automatyki, a także innych systemów technicznych funkcjonujących w obiekcie. Pomimo tak rozbudowanej funkcjonalności ProtegeGX został zaprojektowany z myślą o użytkowniku – przyjazny interfejs z graficznymi mapami wizualizacji oraz wysoce funkcjonalnymi stronami statusów pozwalają na sprawne i szybkie zarządzanie systemem oraz kontrolowanie jego stanu.

Kluczowe dla instytucji finansowych rozwiązania ICT:

- **JEDEN SYSTEM DLA WIELU LOKALIZACJI.** ProtegeGX tworzy spójny system zabezpieczeń, łatwy do zarządzania i kontrolowania organizacji rozproszonych, takich jak siedziba banku i wszystkie jego filie.
- **PODWÓJNE UWIERZYTELNIANIE.** Funkcja ta wymaga podania poświadczeń tożsamości dwóch upoważnionych użytkowników w celu otwarcia drzwi i/lub uzyskania dostępu do strefy alarmowej – idealne rozwiązanie w przypadku pomieszczeń najwyższego poziomu zabezpieczenia.
- **UWIERZYTELNIANIE DWUSKŁADNIKOWE.** To, co masz (karta), i to, co znasz (PIN) – dwuelementowa autoryzacja zapobiega wykorzystaniu zgubionych lub skradzionych identyfikatorów w celu uzyskania nieautoryzowanego dostępu. Tę funkcję można rozszerzyć o biometrykę i inne dane identyfikacyjne.
- **ANTI-PASSBACK.** Globalna i lokalna funkcja anti-passback kontroluje prawidłowość przemieszczania się osób w strefach i zapobiega użyciu karty „podanej do tyłu" drugiej osobie.
- **OPÓŹNIENIE ROZBROJENIA.** Po wykonaniu procedury rozbrojenia strefy odliczany jest zaprogramowany czas, zanim ostatecznie uzyska się do niej dostęp. Nawet gdy użytkownik rozbroi strefę pod przymusem, system i tak odczeka zaprogramowany czas, zanim pozwoli wejść do środka.
- **AUTOMATYCZNE PONOWNE UZBROJENIE.** Automatyczne uzbrojenie obszaru po jego uprzednim rozbrojeniu następuje po określonym czasie, w jakim użytkownik może w nim przebywać.
- **ZŁOŻONOŚĆ KODÓW KONTROLOWANA PRZEZ SYSTEM.** System ProtegeGX może kontrolować, czy kody użytkowników nie są zbyt proste – sprawdza liczbę takich samych cyfr oraz ich sekwencje, wymaga odpowiedniej długości kodu PIN oraz wymusza konieczność jego zmiany po upływie określonego czasu.
- **RAPORTOWANIE I INFORMACJA.** ProtegeGX ma imponujące możliwości raportowania i pozyskiwania potrzebnych informacji. Wydajne filtrowanie i elastyczne opcje raportowania umożliwiają szybkie i łatwe uzyskanie szczegółowych informacji o istotnych zdarzeniach w systemie, nawet w bardzo rozbudowanych instalacjach z setkami tysięcy zdarzeń dziennie. Pozyskiwanie ważnych informacji w zakresie bezpieczeństwa nigdy nie było łatwiejsze.

Całości dopełniają rozbudowane interfejsy integracyjne, pozwalające na sprawne współdziałanie systemu bezpieczeństwa z innymi systemami organizacji. System ProtegeGX spełnia najwyższe wymogi normy EN50131 potwierdzone certyfikatem GRADE 4. □

Miwi Urmet

ul. Pojezierska 90A,
91-341 Łódź
tel. 42 616 21 00
miwi@miwiurmet.pl
www.miwiurmet.pl

Dzisiejszy świat bardzo szybko ulega przemianom cyfrowym. Prym wiedzie branża finansowa, a szczególnie banki. Coraz mniej transakcji ma charakter gotówkowy, co wynika m.in. z regulacji prawnych, ale też z wygody „nienoszenia" portfela. Konsekwencją tego jest zmniejszenie liczby okienek kasowych w oddziałach, nieraz likwidacja placówek. Napady na banki są niezwykłą rzadkością.

Rozwiązania pewne jak w banku

T E K S T
Konrad Szadkowski
ASSA ABLOY Opening Solutions Poland

Czy to oznacza, że ochrona życia i mienia w bankach może zejść na drugi plan, a departament odpowiadający za bezpieczeństwo fizyczne w banku ma coraz mniej pracy?
Moim zdaniem odpowiedź jest jednoznaczna: zakres obowiązków osób odpowiedzialnych za bezpieczeństwo instytucji finansowej wręcz się rozszerza. Oprócz opieki nad skarbcem, biurami, placówkami obsługującymi klientów, bankomatami i przewozami gotówki pojawiają się aspekty związane z ochroną danych wrażliwych, ochroną informacji niejawnych, zabezpieczeniem centrów przetwarzania danych oraz pojedynczych szaf serwerowych i komputerów. Zmusza to osoby odpowiedzialne do ciągłego kreowania polityki bezpieczeństwa od nowa, do poszukiwania rozwiązań, które będą służyły długo, będą wszechstronne, pozwolą na ujednolicanie systemów, a przede wszystkim będą „pewne jak w banku".
Należy pamiętać, że system bezpieczeństwa nie jest tylko kosztem. Jest inwestycją w pewność i spokój, jest narzędziem pracy, od którego zależy dobre imię banku.
Abloy, fińska marka należąca do największego na świecie producenta systemów zamknięć i zabezpieczeń oraz kontroli dostępu – Assa Abloy, postawiła na dostarczanie rozwiązań będących odpowiedzią na potrzeby związane z bezpieczeństwem instytucji o kluczowym dla społeczeństwa i kraju znaczeniu. Używając słowa bezpieczeństwo, mam na myśli życie i zdrowie, mienie, informację oraz procesy.

Abloy w swoich systemach klucza generalnego (*Master Key*) od ponad 100 lat rozwija technologię dyskową, która na obecnym poziomie, w odróżnieniu od klasycznej zastawkowo-sprężynowej, jest odporna na wszystkie manipulacyjne metody otwierania. Unikatową zaletą ABLOY PROTEC2 jest brak możliwości kopiowania klucza (ścisły nadzór fabryki nad surówkami kluczy). W kluczu znajduje się element ruchomy (kulka) współpracujący z kulkami umieszczonymi w zamknięciu – rozwiązanie jest chronione patentem do 2030 r. Zadaniem kulki jest ponadto uniemożliwienie wykonania kopii klucza na drukarce 3D. Tak zabezpieczony klucz możemy bez obaw powierzyć pracownikom i podwykonawcom, wiedząc, że po jego zwrocie nie dostaną się oni do obiektów bez naszej wiedzy.
ABLOY PROTEC2 to szeroki wachlarz zamknięć: wkładki do drzwi, kłódki, zamki przemysłowe, zamki meblowe, sta-

Przypadek: budynek bankowy

STREFY DOSTĘPU
- Strefa komercyjna
- Strefa socjalna
- Pokoje
- Obszar High Security

PRODUKTY
- Zamki Elektryczne
- Samozamykacze
- Automaty drzwiowe
- Wkładki C LIQ
- Zamki typu Cam-lock mechanical
- Zamki typu Cam-lock CLIQ
- Zamki meblowe
- Zamki specjalne

cyjki do sterowania procesami. Jednym systemem klucza można objąć budynki i pomieszczenia, bankomaty, wrzutnie, tuby depozytowe, pojemniki do przewozu wartości, skrytki depozytowe, pomieszczenia skarbcowe, szafy do przechowywania akt oraz szafy serwerowe.
Współczesne systemy bezpieczeństwa, podobnie jak banki, skręciły mocno w stronę rozwiązań elektronicznych. Kamery, czujniki i różnego rodzaju sprzęt elektroniczny spotykamy na każdym kroku. Abloy nie tylko dotrzymuje kroku w cyfrowym wyścigu, ale nadaje ton, tworząc innowacyjne rozwiązania. Przykładem tego może być system podwójnej kontroli dostępu – ABLOY PROTEC2 CLIQ. Wszystkie wymienione wyżej zamknięcia mogą łączyć w sobie pewność zabezpieczenia mechanicznego obracających się dysków (PROTEC2) z wygodą, jaką zapewnia elektroniczna kontrola dostępu (CLIQ). Zamknięcia, mimo że wykorzystują dwie różne technologie, na pierwszy rzut oka są takie same. Co ciekawe – nie wymagają żadnego zasilania! Klucze w tym rozwiązaniu mają, oprócz klasycznego brzeszczotu, własną elektronikę z wymienną baterią – wprowadzony klucz jest dla zamknięcia źródłem zasilania. W kluczu są zapisane prawa dostępu do określonych obiektów, pomieszczeń, w określonych dniach i godzinach.
Zamknięcia mogą mieć funkcję skrytki bankowej, czyli otworzą się pod warunkiem sekwencyjnego włożenia dwóch kluczy. Każde zamknięcie i każdy klucz elektroniczny ma rejestr zdarzeń. Dzięki temu wiemy kto, kiedy i jak długo przebywał w określonej lokalizacji lub miał dostęp do określonego zasobu. Prawa dostępu dla użytkownika klucza można nadawać zdalnie, a w przypadku zagubienia klucza łatwo go dezaktywować. Decydując się na ABLOY PROTEC2 CLIQ, można elastycznie korzystać z zamknięć elektronicznych (do obiektów wrażliwych) i mechanicznych (mniej istotnych). Zamknięcia można swobodnie przenosić między lokalizacjami, aby jeszcze lepiej dopasowywać się do zachodzących dynamicznych zmian. Czy możliwe jest zapewnienie dostępu do ważnych pomieszczeń z zachowaniem pewności zamknięcia na klucz i wygody użycia karty dostępowej?
Najczęściej stosowane elementy wykonawcze w klasycznych systemach kontroli dostępu to elektrozaczep i zwora magnetyczna. Oba są bardzo podatne na manipulacje i wrażliwe na niewłaściwy montaż. Tego typu elementy mogą być stosowane wyłącznie w miejscu, gdzie kontrola dostępu ma jedynie charakter porządkowy. Wszędzie tam, gdzie kontrola ma mieć charakter ścisły, powinny być użyte zamki elektryczne.
Podstawową cechą zamków elektrycznych jest ich samoryglowanie. Oznacza to, że drzwi, które są w ościeżnicy, na pewno mają wysunięty rygiel. Na sygnał z systemu KD typu „dostęp dozwolony" rygiel może być chowany elektrycznie (zamki elektromotoryczne) lub sprzęgnięty z klamką – w momencie naciśnięcia klamki rygiel chowa się (zamki z kontrolą klamki). Z zamka można wydobyć wiele cennych informacji, np. czy drzwi są zamknięte, w jakiej pozycji jest rygiel, czy użytkownik autoryzował się w SKD, czy użył klucza. Zamki mogą pracować jako jedno- i dwustronna kontrola dostępu. Klasycznym przykładem przejść, gdzie powinny być stosowane zamki elektryczne (w tym przypadku wieloryglowe) są drzwi o podwyższonej klasie odporności na włamanie wg PN-EN 1627:2012. Takie drzwi objęte klasycznym systemem kontroli dostępu (ze zworą lub elektrozaczepem) najczęściej są użytkowane w ten sposób, że rano pierwsza osoba, która wchodzi do pomieszczenia, otwiera drzwi kluczem, pozostałe zaś korzystając już tylko z urządzeń SKD (klawiatura PIN, czytnik kart lub inny). Pod koniec dnia pracy drzwi są ponownie zamykane kluczem. Należy pamiętać, że tylko drzwi zaryglowane mają klasę podwyższonej odporności na włamanie. Zatem w ciągu dnia pracy drzwi są klasycznym przejściem bez odporności na włamanie!

Systemy klucza Master Key, zamki elektryczne, depozytory kluczy, samozamykacze i inne rozwiązania dostarczane przez Abloy od wielu lat spotykają się z uznaniem banków w Polsce i na świecie. Być zaufanym doradcą w kluczowych dla bezpieczeństwa sprawach to cel, jaki stawia przed sobą Abloy. Zbieranie doświadczeń ze wszystkich zakątków świata oraz cykliczna wymiana informacji pozwalają na dostarczanie efektywnych rozwiązań.
Abloy prowadzi szkolenia z zakresu zabezpieczeń mechanicznych i elektronicznych oraz kontroli dostępu. Szkolenia mają formę warsztatów, podczas których uczestnicy mogą sprawdzić różne rodzaje zabezpieczeń, poznają złe i dobre praktyki inżynierskie, mogą też spróbować swoich sił w manipulowaniu systemami bezpieczeństwa. Szkolenia odbywają się również w formie webinarów. Zapraszamy do skorzystania z naszych doświadczeń.
Abloy For Trust

ASSA ABLOY Opening Solutions Poland
ul. Magazynowa 4, 64-100 Leszno
www.assaabloyopeningsolutions.pl
konrad.szadkowski@abloy.pl

KTÓRE HOTELE PRZETRWAJĄ CZAS PANDEMII I WRÓCĄ DO BIZNESU? ODPOWIEDŹ NA TO PYTANIE JEST PROSTA – BEZPIECZNE! NA TYM ARCYKRÓTKIM PODSUMOWANIU TEKST MÓGŁBY SIĘ ZAKOŃCZYĆ.

My hotel is my castle

T E K S T
Jacek Tyburek

Rząd ogłosił właśnie kolejny etap obostrzeń, które obejmują również hotele. Obecnie z ich usług będą mogły korzystać tylko osoby w podróży służbowej. Co to oznacza dla hoteli z punktu widzenia biznesu, można sobie wyobrazić. Komunikaty na temat kondycji branży hotelarskiej – od kwietnia mniej lub bardziej katastroficzne – zmieniają się dynamicznie. Jeszcze we wrześniu można było przeczytać, że branża hotelarska zaczyna odrabiać straty, a już w listopadzie znowu większość Europy pozostaje w coraz bardziej restrykcyjnym lockdownie.

W tym miejscu chciałbym nawiązać do osobistych doświadczeń związanych z bezpieczeństwem w branży hotelarskiej. W latach 2011 i 2012 miałem zaszczyt i przyjemność pracować dla lokalnej organizacji UEFA, w spółce UEFA Euro 2012. Jako menedżer ds. miejsc oficjalnych byłem odpowiedzialny za zorganizowanie i skoordynowanie przygotowań w zakresie bezpieczeństwa zgodnie ze standardami UEFA i oczekiwaniami drużyn uczestniczących w turnieju. Praca ta była wspaniałą zawodową przygodą, ale jednocześnie wielką odpowiedzialnością. Kibiców piłki nożnej nie trzeba uświadamiać, jak ważnym elementem życia topowej drużyny narodowej było bezpieczeństwo zawodników. Bezpieczeństwo rozumiane również jako wolność od zbyt natarczywych kibiców, którzy swoich idoli na przemian kochali lub nienawidzili. Kategorią bezpieczeństwa był też tzw. święty spokój, do którego zawodnicy mieli prawo i wręcz obowiązek. Nie bez znaczenia w takich imprezach jest przeciwdziałanie natrętnym dziennikarzom, paparazzi i pozostałym gotowym na wszystko przedstawicielom mediów. A to przecież nic innego, jak zapobieganie swoistemu „szpiegostwu przemysłowemu".

W przypadku piłkarzy mówimy o bardzo poważnym potencjale biznesowym. Według CIES (Międzynarodowe Centrum Badań nad Sportem), aby wyliczyć wartość rynkową piłkarza, bierze się pod uwagę wiele danych, takich jak wiek, pozycja, rola w reprezentacji, potencjał marketingowy i wiele więcej. Rokrocznie publikowana jest lista najdroższych piłkarzy. W 2019 r. Robert Lewandowski zajął 21. miejsce z kwotą, uwaga, 107,5 mln euro! Nie oznacza to jeszcze, że jakiś klub będzie chętny tyle zapłacić, ale pokazuje, z jakimi kwotami mamy tutaj do czynienia. Do pierwszego miejsca dużo zabrakło, gdyż Neymar był wyceniany na 213 mln euro! W tym samym rankingu zdobywca pięciu Złotych Piłek Cristiano Ronaldo został wyceniony na „jedyne" 80,4 mln euro. Dla przykładu łączna wartość kontraktów zawodników Portugalii wynosi obecnie 709 mln euro. Zbudowanie systemu bezpieczeństwa w hotelach właśnie dla reprezentacji narodowych jest więc zadaniem trudnym. Bezpieczny hotel jest bardzo ważnym elementem tego systemu.

Świat sportu to nie tylko piłka nożna. Futbol jest przykładem najbardziej jaskrawym, gdyż żadna inna dyscyplina sportowa nie przyciąga takiej publiczności, żadna inna nie kumuluje wokół siebie takich budżetów i zysków. Nawet igrzyska olimpijskie, letnie czy zimowe, które są imprezami organizacyjnie większymi, nie mają poważniejszego wydźwięku biznesowego.

Dlaczego o tym wszystkim piszę? Ponieważ pandemia koronawirusa pokrzyżowała plany całemu sportowemu światu. Lista wielkich imprez, które miały odbyć się w 2020 r., a zostały odwołane lub przesunięte na inny termin, jest imponująca i bardzo smutna jednocześnie. W przeszłości tylko wojna światowa miała podobne reperkusje. Najbardziej spektakularne przykłady: zawody Formuły 1 w Australii, GP Bahrajnu, mistrzostwa świata w hokeju na lodzie w Kanadzie, przerwanie rozgrywek ligi hokejowej NHL oraz rozgrywek ligi koszykówki NBA, odwołanie zawodów lekkoatletycznych diamentowej ligi w Szanghaju czy przeniesienie letnich igrzysk olimpijskich w Tokio 2020 oraz mistrzostw Europy w piłce nożnej Euro 2020, które mają się odbyć w 2021 r.

Przykłady można by mnożyć, gdyż nie ma dyscypliny sportu, która nie zostałaby dotknięta tym problemem. Dla branży hotelarskiej w miejscowościach zaangażowanych w wielkie imprezy sportowe to tragedia. Straty finansowe – z powodu braku kibiców, którzy są świetnymi, niezbyt oszczędnymi klientami, oraz z punktu widzenia budowania prestiżu marki hotelu, w którym mieszkają i odpoczywają gwiazdy sportu – są ogromne.

Piszę na temat standardów bezpieczeństwa stosowanych w przypadku gwiazd sportu, ponieważ żyjemy w czasach, gdy szczególnie w hotelach klasy wielogwiazdkowej każdy klient będzie swoistym VIP-em. Niestety będzie to kosztowało, tanie hotele o wysokim standardzie przestaną mieć rację bytu. Poziom bezpieczeństwa, łatwy do zweryfikowania przez rozpoznawalny certyfikat, stanie się jednym z podstawowych kryteriów wyboru pobytu w danym hotelu w ogóle. Być może hotelarstwo będzie pierwszą branżą, dla której poziom bezpieczeństwa stanie się podstawowym czynnikiem sukcesu biznesowego.

Są jednak dwa warunki, bez których spełnienia ten sukces żadnemu hotelowi się nie uda – konieczne inwestycje w infrastrukturę związane z bezpieczeństwem oraz przeorganizowa-

nie funkcjonowania obiektu i pracy personelu. Większość wytycznych dotyczy zagwarantowania podstawowych zaleceń sanitarnych stanowiących możliwie skuteczne zabezpieczenie przed rozprzestrzenianiem się wirusa. Przykładowo, amerykańskie towarzystwo hotelarskie American Hotel & Lodging Association (AHLA) wdrożyło wytyczne dotyczące bezpiecznego pobytu, które uzgodniono z głównymi markami, takimi jak Wyndham, Hilton, Marriott i Best Western, w celu ujednolicenia standardów czystości. Wiele z tych rekomendacji stosuje się już powszechnie: dozowniki z płynem odkażającym, informacja o myciu rąk, ograniczony do minimum kontakt klienta z obsługą. AHLA wydała poradnik w formie prostych standardów, dostępny na stronie internetowej: www.ahla.com.

Z ciekawością śledzę dyskusję dotyczącą funkcjonowania hoteli po pandemii i zmian, jakie już pozostaną. Znakiem rozpoznawczym nowych czasów będą zasady „Do widzenia bufetom śniadaniowym i obsłudze hotelowej. Witamy kontrolę temperatury i odprawę bez kluczy". W hotelach na całym świecie wciąż opracowuje się zasady obowiązujące w czasach pandemii i bez wątpienia goście dostrzegą duże zmiany, gdy następnym razem się zameldują.

W dającej się przewidzieć przyszłości – do czasu, gdy dostępna będzie szczepionka, szeroko skuteczne leczenie lub natychmiastowe testy na koronawirusa – pobyty w hotelach będą prawdopodobnie ograniczone, również ze względu na cenę. Szczególnie dotyczy to obiektów z tzw. wyższej półki, w których spersonalizowana obsługa i udogodnienia od dawna są testowane. Wcześniej z przyczyn głównie ekonomicznych, bo przecież personel kosztuje, teraz z zupełnej konieczności.

Goście będą woleli bezkluczykowe zameldowanie z zachowanie dystansu społecznego i wymeldowanie oraz kilka spersonalizowanych interakcji. Każda usługa, którą będzie można przenieść w świat aplikacji mobilnych, zostanie tam przeniesiona! W niektórych obszarach koszty funkcjonowania hoteli wzrosną, ale koszty osobowe z pewnością znacząco spadną.

„Będę chciał po prostu wejść do hotelu, wjechać windą na górę, bez konieczności dotykania czegokolwiek wejść do mojego pokoju, który usługodawca całkowicie zdezynfekował przed moim przyjazdem, poczuć się bezpiecznie".

Jedną z podstawowych praktyk w wykryw waniu możliwej infekcji stanie się kontrola temperatury gości i pracowników, ale nie jest jeszcze jasne, na jak szeroką skalę zostanie wdrożona w hotelach. Z pewnością rozwinie się też nieformalna sieć rebeliantów hotelarstwa, którzy w imię swoiście pojmowanej wolności osobistej będą unikali wdrożenia większości regulacji.

Hotele na całym świecie dokładają wszelkich starań, aby uspokoić gości. Jak szybko to zaufanie wróci, dopiero się okaże.

W hotelu Venetian w Las Vegas skanery termowizyjne pojawią się w każdym punkcie dostępu do obiektu, „umożliwiając dyskretny i nieinwazyjny pomiar temperatury" personelu i gości, zgodnie z nowymi zasadami Venetian Clean. W Singapurze ogólnokrajowa kampania o nazwie SG Clean została przeprowadzona w różnych branżach, „tam, gdzie jest to wykonalne i ma zastosowanie". Obejmuje zestaw standardów również dla hoteli, w tym kontrolę temperatury gości. Z kolei Four Seasons w Nowym Jorku przestrzega niewiarygodnie surowego pakietu tymczasowych protokołów, odkąd zaczął przyjmować pracowników służby zdrowia na początku kwietnia br.

I nie ma też pewności, czy takie usługi, jak bufety – hotelowe bary śniadaniowe czy przekąskowe – kiedykolwiek wrócą do serwisu. Nasza świadomość transmisji zakażeń wzrośnie teraz na tyle, że nawet jeśli coś jest bezpieczne i nie powinno powodować strachu przed pandemią, z psychologicznego punktu widzenia może nie być już atrakcyjne. Możliwe, że do listy rozwiązań w najbliższej przyszłości trzeba będzie dopisać serwowanie wyłącznie dań przygotowanych wcześniej i zapakowanych w bezpieczny sposób.

Miejsca ogólnodostępne o dużej liczbie osób jednocześnie tam przebywających, gdzie trudno zachować dystans społeczny – spa czy sale gimnastyczne, z wieloma klamkami i miejscami wymagającymi starannej dezynfekcji – stanowią duże ryzyko transmisji wirusa. Jednak nie wszystkie hotele rezygnują z tych usług. Gdyby kontakt społeczny stał się jeszcze rzadszy, uzdrowiska takie będą mogły stanowić „wyjątkową przystań, w której ludzie doświadczają bliskości innych w czystym i bezpiecznym środowisku".

Podsumowując, przed nami prawdopodobnie era hoteli nafaszerowanych techniką ochronną, kontroli dostępu, monitorowania incydentów i poprawności działania systemów. Przypominam, że piszemy o hotelach klasy premium dla wymagających klientów, dla których luksus jest wartością samą w sobie, ale w nowych warunkach również analiza ryzyka i weryfikowalne przestrzeganie standardów będą stanowić kryterium wyboru. Oznacza to oczywiście niezbędne inwestycje w branży hotelarskiej. Nie da się ich uniknąć, walcząc o cennego w tych nowych warunkach klienta. Koronawirus zabiera spontaniczność i przemiły kontakt z obsługą hotelu, delektowanie się daniami z karty w restauracji hotelowej przyrządzanymi prawie na oczach klienta przez szefa kuchni. W zamian oddaje zupełnie nowy segment hotelarstwa. Taka niestety będzie cena przetrwania. Do hoteli bez najwyższego standardu bezpieczeństwa nie przyjadą światowej klasy sportowcy, gdy już wszystkie imprezy wrócą do kalendarza. Nie zawitają zapewne goście korporacyjni, bo im firmy nie pozwolą mieszkać w miejscach innych niż certyfikowane.

Dochodzimy zatem do kwestii kluczowych dla skutecznej reanimacji hotelarstwa: są to standaryzacja oraz rozpoznawalny znak jakości i bezpieczeństwa. Takie powinno być przesłanie tego potencjalnego certyfikatu – wiemy, czego się możemy spodziewać, i na pewno to dostaniemy.

Stworzenie certyfikatu bezpieczeństwa hotelu jako systemu wytycznych organizacyjnych i zastosowanych narzędzi technicznych powinno być zadaniem dla branży security. Nikt tego równie dobrze nie zrobi. Nie bardzo można liczyć na graczy instytucjonalnych, gdyż oni z natury rzeczy będą działać wolniej i nie mają tak głębokiej znajomości rynku, trendów technologicznych i możliwości. Zadanie zdaje się karkołomne, ale odpowiednio zakomunikowane branży zarówno security, jak i hotelarskiej oraz jej klientów, jest osiągalne.

Pamiętajmy o obiecującym segmencie wsparcia operacyjnego „centrum monitorowania" i monitoringu wizyjnym oraz systemach zarządzania budynkami. Bo to, że pracowników nie będzie widać, nie oznacza, że ich nie będzie w ogóle. Będą funkcjonowali w warunkach centrów monitoringu, shared serwisów, tak aby ograniczyć kontakt z klientem, który dalej będzie mógł liczyć na wsparcie hotelu w każdej sprawie, jak wcześniej. A może dzięki technologiom komunikacyjnym nawet bardziej. Wdrożenie gamy narzędzi i rozwiązań technologicznych czy proceduralnych będzie musiało mieć swoje weryfikowalne podstawy. Za bezpieczeństwo klient zapłaci tak samo jak za luksus, hotel to bezpieczeństwo zagwarantuje, więc weźmie na siebie odpowiedzialność również prawną, gdyby coś poszło nie tak, gdyby w tym naszym przykładowym superzabezpieczonym hotelu klient zgłosił, że np. zaraził się tą czy inną chorobą. Jedynym ratunkiem dla zachowania reputacji hotelu i jego stawki ubezpieczeniowej jest możliwość udowodnienia, że posiada system weryfikacji oraz kontroli procesów i może to pokazać.

Interesującym eksperymentem i jednocześnie testem powrotu do pełnej operacyjności są statki wycieczkowe, typowe cruisery, które są niczym innym jak ekskluzywnymi hotelami w wielkiej skali. Obecnie trwa test powrotu do uruchomienia rejsów dla zamożniejszych mieszkańców Singapuru. Szukają oni odskoczni od życia w stresie w państwie-mieście, szukają oderwania się od tej rzeczywistości. Kwestią absolutnie kluczową jest bezpieczeństwo. Rygorystyczne warunku są obecnie testowane. Aby ułatwić wznowienie rejsów rozpoczynających się w piątek (6 listopada), w Marina Bay Cruise Centre Singapore utworzono ośrodek testowy Covid-19. Stanowisko testowe na trzecim piętrze parkingu centrum wycieczkowego ma odprawiać 125 pasażerów co 30 minut. Rzecznik centrum powiedział, że budowa obiektu (projekt infrastruktury, budowa, planowanie trasy przepływu oraz testy i operacje wykonawcze) zajęła nieco ponad dwa tygodnie.

Blisko 1700 gości, którzy dołączyli do pierwszego rejsu Genting Cruise Lines w piątek, przejdzie szybki test antygenu w centrum rejsowym przed wejściem na pokład statku „World Dream". Wyniki będą dostępne w ciągu godziny. Prezes Dream Cruises i szef sprzedaży międzynarodowej w Genting Cruise Lines, powiedział, że każdy gość, który nie przejdzie kontroli zdrowia lub testów COVID-19, będzie miał zakaz odprawy i kontynuowania rejsu. Będzie musiał udać się na dalsze badania i testy do wyznaczonych ośrodków medycznych wskazanych przez ministerstwo zdrowia. Testy dla osób wchodzących na pokład „World Dream" rozpoczną się o godz. 9.00 w dniu rejsu, a pasażerowie wejdą na pokład od godz. 14.00, mając „wystarczająco dużo czasu na cieszenie się statkiem". Wszyscy zaokrętowani otrzymają wyznaczony przedział czasowy na przystąpienie do testu COVID-19, aby upewnić się, że zostaną przetestowani przed wypłynięciem statku o godz. 21.00.

Dyrektor zarządzająca ds. Azji i Pacyfiku w Royal Caribbean International powiedziała, że rezerwacje rejsowe dokonane w październiku były sześciokrotnie wyższe niż w tym samym okresie ub. roku – pierwsza, 1 grudnia, została wyprzedana. Na naszych oczach powstaje świetnie prosperująca usługa oparta na standardach bezpieczeństwa. Sukces zostanie jednak osiągnięty tylko wówczas, gdy system będzie skutecznie i bezwzględnie kontrolowany. To wielkie wyzwanie dla dyrektora ds. bezpieczeństwa.

Wracając do sportu i potrzeb, jakie kreują związki sportowe, szczególnie w wysokobudżetowych imprezach, które są dobrym punktem odniesienia, hotelarze muszą się przygotować na to, że wymagania organizatorów imprez będą coraz większe.

Ten, kto ich nie spełni lub da się przyłapać na tym, że próbuje je obchodzić, nie zrobi interesu w hotelarstwie nowych czasów.

Dla branży security, szczególnie jej części technologicznej, to bardzo dobra wiadomość. Ale to sama branża musi sobie wypracować możliwości.

Rok 2021 będzie pod tym względem przełomowy, wskaże bowiem hotelom, przemysłowi rozrywki czy ekskluzywnych podróży kierunki „powrotu do gry" po wygranej wojnie z pandemią. ▫

BIO

Jacek Tyburek

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

Terminal do zadań specjalnych

Banki są instytucjami wymagającymi zaawansowanych technicznie rozwiązań ochronnych, które gwarantują bezpieczeństwo pracowników i klientów oraz przechowywanych tam aktywów.

Cieszy fakt, że w ostatnich latach przy wyborze systemu zabezpieczeń banki większą uwagę zwracają na jakość systemu, nie kierują się już tylko jego ceną. Zazwyczaj są tworzone od podstaw, specjalnie pod wymogi określonej placówki. Regułą stają się rozwiązania idące w kierunku jak największej automatycznej analizy danych, odbywającej się na podstawie zarejestrowanych zdarzeń – powiedział Piotr Świder, Business Development Manager w Hikvision Polska. Mimo że w systemach bankowych wiele operacji można dziś wykonać online, niektóre transakcje wymagają fizycznej wizyty w placówce, chociażby po to, aby na dokumentach złożyć odręczny podpis. Dlatego w czasach pandemii COVID-19 banki muszą zapewnić ochronę przed możliwością zakażenia się wirusem SARS-CoV-2 zarówno swoim pracownikom, jak i klientom. Do tego celu można wykorzystać terminale Hikvision – urządzenia wykonujące kilka różnych funkcji. Pomagają w przestrzeganiu wymogów sanitarnych, wykrywając m.in. osoby z gorączką czy niezasłaniające nosa i ust maseczką.

Początkowo nasi klienci z instytucji finansowych do pomiaru temperatury stosowali głównie kamery termowizyjne i moduły blackbody. To bardzo wygodne rozwiązanie, ponieważ nie trzeba wytyczać specjalnych torów podejścia osoby, której temperaturę chce się zmierzyć. Każdy klient wchodzący do oddziału jest automatycznie monitorowany, może nawet tego faktu nie zauważyć. Obecnie widzimy większe zainteresowanie naszymi terminalami termograficznymi. W tym przypadku klienci są wcześniej informowani o pomiarze temperatury, co sprawia, że wchodząc do placówki, mają poczucie przebywania w bezpiecznym otoczeniu – zauważa Piotr Świder.

Terminal składa się z trzech podstawowych elementów:

1. Kamera światła widzialnego, która po wykryciu twarzy w polu detekcji przesyła sygnał do kamery termowizyjnej w celu dokonania pomiaru temperatury. Dzięki takiemu rozwiązaniu systemu nie można oszukać np. przez umieszczenie w polu widzenia kubka z gorącą zawartością. Aby pomiar był dokonany, musi być najpierw wykryta twarz.
2. Kamera termowizyjna mierząca temperaturę ciała z dokładnością od 0,3 do 0,5°.
3. Elementy kontroli dostępu, w tym czytniki kart Mifare, możliwość wgrania do bazy zdjęć osób uprawnionych do wejścia w określoną strefę.

Terminal może współpracować z systemami zabezpieczeń innych producentów. *Integrację terminalu można przeprowadzić na kilka sposobów: za pomocą oprogramowania HikCentral lub naszych rejestratorów, do których można podłączyć kamery różnych producentów. Terminal jest łatwy w instalacji i konfiguracji. Wszystko metodą plug&play* – dodaje Piotr Świder.

Korzystając z wyjść alarmowych, terminal można połączyć z bramkami kontroli dostępu. Jeśli u osoby wykryje się gorączkę (próg temperatury można ustalić, najczęściej jest to 38°), przejście przez bramki zostanie zablokowane, osoba nie będzie wpuszczona dalej, a odpowiednie służby zostaną poinformowane o konieczności podjęcia określonych działań. Terminal można również zastosować do wykrywania osób wchodzących bez maseczki. W takim przypadku także można zablokować otwarcie bramek kontroli dostępu.

Weryfikacja osoby może odbyć się wg czterech kryteriów:

1. pomiar temperatury,
2. detekcji twarzy,
3. odczyt karty dostępu,
4. wykrycie maseczki.

W tej chwili zdecydowanie największym zainteresowaniem banków i instytucji finansowych cieszą się nasze terminale. Te instytucje myślą kompleksowo o zapewnieniu bezpieczeństwa i ochronie zdrowia swoich pracowników i klientów. Nasze terminale, łączące w sobie wiele funkcji, sprawdzają się tu znakomicie – dodaje Piotr Świder. □

Hikvision Poland

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

TP-LINK OMADA SDN – rozwiązanie chmurowe dla sieci hotelowych

EAP265 HD – pracujący w standardzie AC1750 sufitowy punkt dostępowy może obsłużyć aż 500 urządzeń klienckich jednocześnie, dzięki czemu świetnie sprawdzi się w salach konferencyjnych

Firma TP-Link poleca serię centralnie zarządzanych punktów dostępowych Wi-Fi z serii Omada. W portfolio znajdują się punkty dostępowe zarówno montowane na suficie, jak i naścienne (montowane w standardowej puszce elektrycznej) oraz zewnętrzne odporne na warunki atmosferyczne.

EAP225-WALL – dyskretny access point AC1200 przeznaczony do montażu w pokojach hotelowych. Dzięki portowi Ethernet PoE Out z urządzenia można zasilić np. telefon VoiP

Możliwość utworzenia nawet 16 odseparowanych sieci bezprzewodowych i autoryzacji gości przez stronę powitalną, Facebooka, SMS-em czy jednorazowym kodem dostępu sprawia, że urządzenia są z powodzeniem stosowane przy budowie hotelowej infrastruktury sieciowej. Co istotne, wszystkie punkty dostępowe z serii TP-Link Omada są zasilane poprzez standard PoE, który umożliwia wykorzystanie kabla Ethernet do jednoczesnego zasilenia urządzenia i transmisji danych.

Wychodząc naprzeciw oczekiwaniom administratorów sieciowych, TP-Link rozbudowuje swoją ofertę urządzeń zarządzanych centralnie poprzez chmurę i wprowadza platformę Omada SDN. Do oferty producenta trafiają nowe bramy sieciowe, przełączniki i kontrolery, a oferowane już wcześniej punkty dostępowe otrzymały aktualizację oprogramowania. TP-Link Omada SDN umożliwia utworzenie wysoce skalowalnych sieci LAN i WLAN – w pełni kontrolowanych za pomocą jednego interfejsu. Przekłada się to na płynne połączenia przewodowe i bezprzewodowe niezbędne m.in. w hotelach, szkołach, biurach czy urzędach.

Dzięki rozwiązaniu Omada SDN administratorzy będą mogli łatwo i kompleksowo zarządzać centralnie całą siecią, także rozproszoną pomiędzy placówkami – z dowolnego miejsca i o dowolnej porze. Instalatorzy mają do wyboru dwie możliwości implementacji systemu: poprzez kontrolery sprzętowe OC200/OC300, które eliminują konieczność korzystania z komputerów i serwerów, lub przez oprogramowanie Omada Controller instalowane na komputerze w sieci lokalnej.

Do oferty dołączy też kontroler Omada Cloud w modelu subskrypcyjnym, całkowicie oparty na chmurze, który nie wymaga stosowania kontrolera sprzętowego ani programowego. W każdym przypadku jest zapewniona identyczna funkcjonalność, a dzięki takiemu zróżnicowaniu administrator ma wybór platformy, która najbardziej mu odpowiada. Wbudowana w kontroler sztuczna inteligencja zapewnia skuteczniejsze działanie i bardziej intuicyjną kontrolę sieci Wi-Fi niż w przypadku infrastruktury tradycyjnej. Automatycznie analizuje potencjalne problemy i wysyła sugestie dotyczące optymalizacji sieci i zwiększenia jej wydajności. Pomaga też lokalizować źródła zakłóceń i przeciwdziałać im, automatycznie dostosowując ustawienia kanału i moc transmisji sąsiednich punktów dostępowych w ramach tej samej sieci. O wszystkich problemach są informowani administratorzy, dzięki czemu mogą dokonywać zmian mających na celu poprawę bezpieczeństwa.

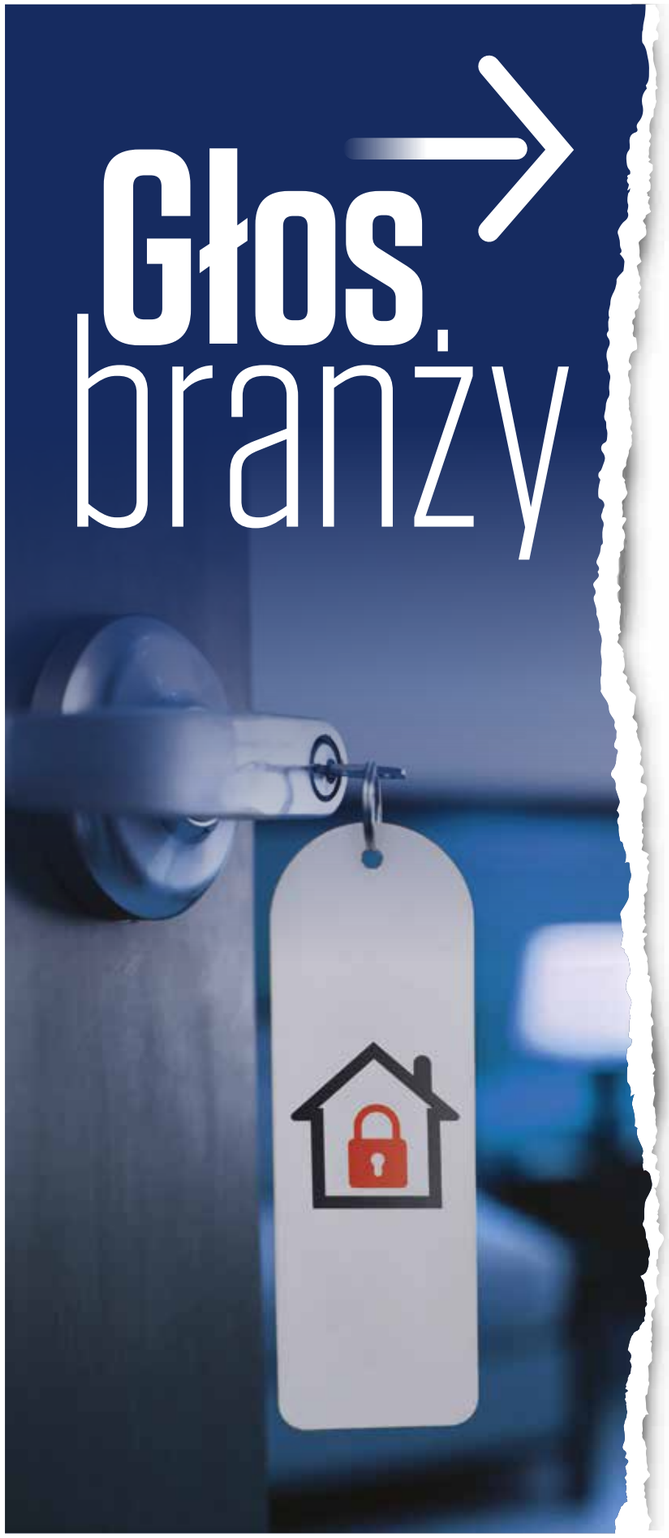
System Omada SDN umożliwia przydzielanie administratorom różnych uprawnień i w efekcie wieloosobowe, wielopoziomowe zarządzanie siecią z zachowaniem najwyższego poziomu bezpieczeństwa. Ponadto system oddziela zasoby dotyczące zarządzania siecią od wrażliwych danych użytkowników, dzięki czemu ruch generowany przez nich nie jest przetwarzany w chmurze, co zapewnia lepszą ochronę ich prywatności. Sprawdzanie poziomu wykorzystania przepustowości i natężenia ruchu, uzyskiwanie dostępu do dzienników ze statystykami, otrzymywanie powiadomień i ostrzeżeń oraz śledzenie kluczowych dla rozwoju firmy danych nigdy nie było tak proste. □

EAP225-OUTDOOR – punkt dostępowy AC1200 zaprojektowany z myślą o użytku na zewnątrz budynków. Obudowa z certyfikacją IP65 zapewnia odporność na warunki atmosferyczne

TP-Link Polska

ul. Ożarowska 40/42,
05-850 Duchnice
www.tp-link.com.pl
robert.gawronski@tp-link.com

Głos branży



HOTELE I INSTYTUCJE FINANSOWE SĄ OBIEKTAMI WYMAGAJĄCYMI SZCZEGÓLNEJ OCHRONY, ZWŁASZCZA TERAZ W DOBIE PANDEMII COVID-19. ZARZĄDZAJĄCY NIMI MUSZĄ DBAĆ O BEZPIECZEŃSTWO ZARÓWNO GOŚCI, JAK I PRACOWNIKÓW.

Marcin Walczuk

BCS

Bezpieczeństwo w hotelu

Branża hotelarska w czasie pandemii koronawirusa zdecydowanie nie ma lekko. W tych trudnych dla niej czasach hotele muszą zwracać uwagę na zapewnienie szeroko pojętej ochrony mienia, zdrowia i życia swoich gości, a szczególnie ich ochrony przed możliwością zakażenia.

Sprowadza się to m.in. do przestrzegania rygorystycznych wymogów sanitarnych i minimalizowania zagrożeń związanych z rozprzestrzenianiem się koronawirusa. Świetnie sprawdzają się np. bezdotykowe systemy kontroli dostępu do pokojów gościnnych czy systemy telewizji dozorowej z funkcjami pomiaru temperatury ludzkiego ciała oraz analityką obrazu.

BCS, jako producent systemów telewizji dozorowej, ma w ofercie pełną gamę urządzeń, które idealnie sprawdzają się w sprawnym i skutecznym zabezpieczeniu nawet największych obiektów tego typu. Rejestratory 128-kanałowe pozwolą na monitorowanie średnich hoteli. Nic natomiast nie stoi na przeszkodzie, aby przy użyciu aplikacji BCS Manager połączyć więcej tego typu urządzeń i cały system obsługiwać z poziomu jednej stacji roboczej. W takim przypadku ograniczeniem będzie tylko moc wspomnianej stacji, żeby wyświetlić obrazy z odpowiedniej liczby kanałów.

Osoby korzystające z usług hotelowych oczekują pełnego bezpieczeństwa. Ze względu na zróżnicowane potrzeby wymagających (zwłaszcza teraz) gości BCS proponuje rozwiązania, które spełnią oczekiwania hoteli. Kamery specjalnego przeznaczenia, np. kamery termowizyjne służące do pomiaru temperatury ciała, pozwolą szybko i automatycznie sprawdzić, czy dana osoba nie ma podwyższonej temperatury, i w razie potrzeby postępować zgodnie z procedurami. Taka kamera może również wykryć, czy osoby mają założoną maseczkę ochronną, aby w przypadku jej braku bezzwłocznie zwrócić na to uwagę.

Rozpoznawanie i identyfikacja twarzy osób przebywających na terenie hotelu pozwolą na porównanie z bazą danych gości lub pracowników i wychwytywanie osób nieuprawnionych do pobytu w obiekcie lub w niedostępnych dla nich miejscach. Kamery z funkcjami zliczania ludzi sprawdzą, czy liczba osób odpowiada aktualnemu limitowi przewidzianemu dla danego hotelu albo, w przypadku ewakuacji, czy wszyscy opuścili obiekt.

Najnowsza seria kamer BCS z algorytmami AI pozwala systemowi CCTV reagować na zdarzenia szczególnego typu, takie jak przekroczenie linii, wtargnięcie lub zbyt długie przebywanie w strefie bądź monitorowanie pozostawionych lub skradzionych przedmiotów. Przy monitorowaniu parkingu nieodzowna będzie kamera do rozpoznawania tablic rejestracyjnych, która w połączeniu z BCS Managerem pozwoli też przyznawać dostęp autom o właściwych numerach rejestracyjnych. Wszystkie te funkcjonalności będzie można wykorzystać znacznie szerzej po całkowitym otwarciu hoteli.

Andrzej Berecki

Orbis Hotel Group

Poszukiwanie ekonomicznych metod zarządzania

Wszystkie systemy bezpieczeństwa zainstalowane i obsługiwane w hotelach przed pandemią nadal działają i są obsługiwane. Pracownicy wykonują te same obowiązki. Nie zauważyłem, aby w branży hotelarskiej na masową skalę wykorzystywano np. systemy wizyjne wykrywające podwyższoną temperaturę ciała.

Możliwe jest natomiast zmierzenie temperatury na życzenie gościa lub pracownika, np. termometrem.

Oprócz firm oferujących systemy termowizyjne pojawiły się firmy oferujące bramki dezynfekcyjne. Spotkałem się z ofertą wykorzystania dedykowanej dla hoteli aplikacji gromadzącej dane o gościach w kontekście zagrożenia COVID-19. Na pewno są to rozwiązania mogące mieć pozytywny wpływ na wzmocnienie poczucia bezpieczeństwa, ale moim zdaniem przed zastosowaniem niektórych z nich w hotelu należy przeanalizować zagrożenia dotyczące ochrony danych osobowych, w tym np. medycznych.

Najważniejszą zmianą, jaka nastąpiła w hotelach, jest wprowadzenie restrykcyjnych protokołów postępowania związanych z zapewnieniem bezpieczeństwa gościom i pracownikom. Mam tu na myśli dezynfekcję pokoi i innych przestrzeni hotelu, używanie maseczek, utrzymywanie dystansu, odpowiednią aranżację elementów wyposażenia itp. Hotele są przygotowane na wypadek konieczności postępowania z osobą, u której podejrzewa się zakażenie, i ściśle współpracują w tym zakresie z instytucjami ochrony zdrowia.

Pewne rodzaje prac w hotelu są wykonywane przez pracowników osobiście, i tego nie zmienimy. Niektóre jednak mogą odbywać się zdalnie, np. w dziale rezerwacji. Nie jest to związane *stricte* z instalacjami bezpieczeństwa fizycznego, ale w szeroko rozumianym ujęciu branża bezpieczeństwa, szczególnie IT, musi zapewnić i odpowiednio zabezpieczyć możliwość pracy zdalnej.

Obecna sytuacja wymusza także poszukiwanie sposobów dotyczących automatyzacji niektórych procesów lub zastosowanie zdalnych metod, np. monitoringu hoteli. Przykład: zamiast pracownika parkingu można zastosować zautomatyzowane systemy parkingowe, co w dłuższej perspektywie pozwoli na optymalizację kosztów.

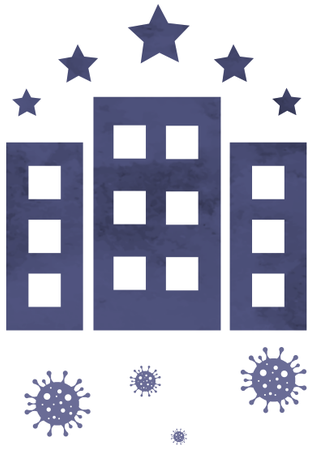
Chodzi o poszukiwanie optymalnych ekonomicznie metod zarządzania bezpieczeństwem w tym trudnym ekonomicznie czasie. Nie twierdzę, że w każdym hotelu należy zrezygnować z ochrony fizycznej, a wykorzystać np. zdalny monitoring i wsparcie grupy interwencyjnej, gdyż ktoś musi zweryfikować na miejscu powód wzbudzenia alarmu pożarowego. Konieczne jest jednak zwiększenie efektywności pracowników ochrony w hotelach, aby – oprócz będących zawsze priorytetem obowiązków w zakresie zapewnienia bezpieczeństwa – mogli wykonywać inne zadania.

Piotr Świder

Hikvision

Jak przetrwać kryzys w branży hotelarskiej

Obecny rok to dla branży hotelarskiej zdecydowanie najgorszy sezon w XXI wieku. Wiele branż ucierpiało, ale chyba najbardziej obecny kryzys związany z pandemią COVID-19 dotknął właśnie hotelarzy, restauratorów czy transportu. Jako że często podróżuję (służbowo i prywatnie), zauważyłem, że hotele, walcząc o gości, znacząco obniżyły ceny pobytu za dobę. W ten sposób próbu-



ją zdobyć klienta, nawet te topowe hotele 4- i 5-gwiazdkowe w najlepszych lokalizacjach. Mimo to według różnych raportów średnia frekwencja spadła znacząco poniżej 30 procent. Jeszcze w zeszłym roku hotele współorganizowały setki eventów dla różnych branż w postaci kongresów, szkoleń, spotkań itp., które przynosiły wysokomarżowe profity.

Obecnie tego typu wydarzenia przeniosły się do sieci i coraz częściej uczestniczymy w spotkaniach online. Kryzys jest już zauważalny w momencie składania rezerwacji. Przed pandemią musiałem rezerwować miejsce z dużym wyprzedzeniem, obecnie nie ma problemu z rezerwacją nawet w dniu przyjazdu. Niestety prognozy nie są optymistyczne i zakładają, że część hoteli nie przetrwa bez znaczących cięć kosztów (kadry i usług) lub pomocy rządowej.

Dlatego obecnie właściciele próbują wypracować strategię działania na następne lata, ograniczają inwestycje, ale jednocześnie próbują zagwarantować swoim gościom atrakcyjną ofertę połączoną z poczuciem bezpieczeństwa. W tym celu doposażają obiekty w specjalistyczne środki ochrony osobistej, urządzenia sanitarne do dezynfekcji czy systemy do pomiaru temperatury gości i pracowników.

Według mnie jest to niezbędne działanie w dobie pandemii, ponieważ gość przy wyborze hotelu nie będzie się już kierował jedynie ceną, położeniem czy standardem, ale także podjętymi działaniami zapewniającymi bezpieczeństwo. Część obiektów ma już działające systemy automatycznego pomiaru temperatury oparte na kamerach termowizyjnych lub terminalach. To dobry kierunek.

Liczę, że uda nam się opanować kryzys i sytuacja zacznie wracać do normy, czego życzę nam wszystkim.

Barbara Podwysocka

Polski Holding Hotelowy

Bezpieczeństwo w hotelach w dobie pandemii

Pandemia znacząco zmieniła spojrzenie na kwestie bezpieczeństwa we wszystkich aspektach funkcjonowania obiektów hotelarskich. Gość przyjeżdżający do obiektu liczy na to, że będzie się w nim czuł bezpiecznie, wręcz tego wymaga bez względu na charakter podróży oraz standard hotelu. To fundamentalne prawo było zawsze zapewnione. Przez wiele lat udało się wypracować wysoki poziom bezpieczeństwa fizycznego, a także bezpieczeństwa teleinformatycznego przy jednoczesnym zachowaniu najwyższych standardów jakościowych.

Wybuch pandemii spowodował, iż goście rozpoczynają pobyt w hotelu od swoistej analizy ryzyka. COVID-19 zmienił ich optykę na bezpieczeństwo w obiekcie. Obecnie potrzebują przede wszystkim bezpieczeństwa sanitarnego. Zwracają uwagę na certyfikaty higieniczne, wręcz wymagają, aby przestrzegano wszystkich niezbędnych procedur bezpieczeństwa. Już nie wystarczy zapewnienie sieci, iż obiekt spełnia wymagania. Obecnie chcą to zobaczyć na własne oczy i mieć pewność, że będą mogli skorzystać ze środków dezynfekujących, a w razie potrzeby otrzymają maseczkę czy rękawiczki.

Nastawienie gości zmienia się w różnych fazach pandemii. Natomiast statystyki wzrostu zachorowań sprawiają, że stają się coraz bardziej świadomi, oczekują znacznie większych, dodatkowych standardów bezpieczeństwa. Teraz konieczność zwiększenia dystansu jest bardziej zrozumiała. Zamawianie usług przez środki telekomunikacji, takich jak telefon czy Internet, stało się naturalne, a korzystanie z aplikacji nie stanowi już problemu.

Wiele usług przeszło do świata wirtualnego – również w Internecie klient chce się czuć bezpiecznie. Zdecydowanie woli przebywać w swoim pokoju niż w częściach ogólnodostępnych. Ponieważ spędza w nim większość czasu, chce mieć pewność, że jego pokój jest czysty, np. ozonowany (zdezynfekowany) specjalnie dla niego. Korzystając z przestrzeni wspólnej, również zwraca uwagę na środki bezpieczeństwa. Nie chce już, tak jak kiedyś, „niewidocznego poczucia bezpieczeństwa".

Obecnie, aby móc poczuć się bezpiecznie, musi, mówiąc wprost, to bezpieczeństwo zobaczyć. Z tego powodu teraz najważniejszymi rozwiązaniami są te obejmujące systemy dozowania środków do dezynfekcji, a także urządzenia służące do usuwania drobnoustrojów, takie jak sprzęt do ozonowania, lampy do dezynfekcji czy systemy zamgławiania. W całej tej dbałości o bezpieczeństwo higieniczne nie możemy jednak zapomnieć o bezpieczeństwie fizycznym gościa oraz o bezpieczeństwie infrastruktury w trosce o usługi.

Niezmiernie ważnym aspektem w zakresie zapewnienia bezpieczeństwa jest świetnie przygotowany, przeszkolony i poinformowany pracownik. Przygotowana załoga wie, co należy robić w razie pojawienia się przypadku COVID-19 na terenie hotelu. Zna numery telefonów do stacji sanitarno-epidemiologicznej i do najbliższej pomocy medycznej. Potrafi udzielić pomocy nawet w przypadku pojawienia się objawów COVID-u u gości.

Kadra hotelu doskonale zna procedury i wie, że przestrzegając ich, zapewnia bezpieczeństwo sobie, gościom i współpracownikom. Dbanie o bezpieczeństwo w tak trudnym dla branży momencie staje się jednym z filarów jej dalszego funkcjonowania. Zapewnienie tej podstawowej zasady, choć obecnie inaczej rozumianej, sprawi, iż goście wrócą do hoteli.

Jesteśmy w drugiej fali pandemii i na razie trudno przewidzieć wszelkie scenariusze. Sytuacja jest skomplikowana. Niemniej pewna elastyczność w działaniu i otwartość na nowe technologie pomogą każdej branży w przetrwaniu tego kryzysu.

Pamiętajmy, iż gość hotelowy potrzebuje teraz innego poczucia bezpieczeństwa niż tego z początku roku, a nawet z pierwszej fali pandemii. Minione miesiące uświadomiły nam, iż przestrzeganie nakazów, zakazów i procedur wpływa pozytywnie na losy wszystkich. Tylko od nas zależy, jak szybko będziemy w stanie wrócić do z pewnością odmienionego środowiska hotelarskiego.

Adam Latek

Latek Hotels, Polska Izba Hotelarzy

Zarządzanie w przypadku wykrycia choroby

Wielu właścicieli obiektów hotelowych w dzisiejszych czasach zastanawiało się, jak będą zabezpieczane pokoje hotelowe przed koronawirusem. Na rynku pojawiły się ozonatory i sterylizatory. Hotelarze przeanalizowali koszty i skupili się na bezpieczeństwie gości. Okazało się, że ozonatory nie były do końca bezpieczne dla zdrowia. Sterylizacja powietrza ma na celu zniszczenie zarazków, które mogły pozostać po pobycie poprzedniego gościa. Hotelarze bardzo szybko opracowali standardy i procedury dostosowane do wytycznych Głównego Inspektoratu Sanitarnego.

Bezpieczeństwo higieniczne w obiektach hotelarskich zawsze było na wysokim poziomie. Zabezpieczanie pokoi i po każdy sprzątnięciu pieczętowanie naklejką „Specjalnie dla Ciebie pokój sterylizowany" ma na celu zagwarantowanie bezpieczeństwa pobytu. W czasach, gdy mogą przyjmować jedynie gości będących w podróży służbowej, większość hoteli zrezygnowała z bufetów śniadaniowych, a tylko serwuje do stołu wyporcjowane jedzenie przykryte jednorazową folią spożywczą. W kuchniach hotelowych wytyczono nowe procedury HACCP.

Chciałbym zaprezentować jeden z punktów zarządzania kryzysowego na wypadek wykrycia choroby epidemicznej w hotelu.

CHOROBA EPIDEMICZNA LUB ZAKAŹNA (np. COVID-19, wirus ebola)

Działania priorytetowe w tej sytuacji:

Podnieś alarm - zapewnij pełne zaangażowanie władz lokalnych

Ratuj życie - zminimalizuj rozprzestrzenianie się infekcji w hotelu

Zachowaj spokój

Uwaga:

Używaj środków ochrony osobistej (PPE) – maski na twarz, gogle, rękawice lateksowe

PROCEDURA

• W przypadku wyraźnych oznak choroby COVID-19 (uporczywy kaszel, złe samopoczucie, trudności w oddychaniu) gość nie powinien być wpuszczony do hotelu. Powinien zostać poinstruowany, aby jak najszybciej zgłosił się do najbliższego szpitala zakaźnego, jadąc tam własnym transportem. To samo dotyczy pracownika hotelu, u którego widoczne są ww. objawy.

• W przypadku zgłoszenia choroby przez gościa zbierz wszelkie możliwe informacje (od kiedy złe samopoczucie, jakie są objawy itp.).

• Zadzwoń do lokalnej stacji sanitarno-epidemiologicznej oraz pogotowia ratunkowego (112, 999).

• Jak najszybciej odizoluj zarażonego, jeśli to możliwe, ogranicz dalsze rozprzestrzenianie się choroby poprzez izolację osób, które mogły mieć z nim ewentualny kontakt.

• W przypadku COVID-19 – zorientuj się, z kim zainfekowana osoba (osoby) miała kontakt i zlokalizuj ich; postępuj zgodnie z instrukcjami GIS dostępnymi na https://www.gov.pl/web/koronawirus/ i https://gis.gov.pl/.

• W przypadku niepokojących objawów sugerujących zakażenie koronawirusem wśród pracowników należy natychmiast odsunąć ich od pracy i wysłać do domu indywidualnym transportem. Konieczne jest zawieszenie przyjmowania gości oraz powiadomienie sanepidu.

• COVID-19 – należy niezwłocznie przeprowadzić właściwe czyszczenie i dezynfekcję wszystkich obszarów odwiedzanych przez zarażoną osobę (w szczególności klamek, poręczy, uchwytów).

• Należy powiadomić dyrektora gneralnego oraz kierownika działu, aby zminimalizować ryzyko.

• Należy zawiesić przyjmowanie innych gości i ściśle przestrzegać instrukcji sanepidu.

• Należy przygotować się na ewentualną izolację w hotelu (sprawdzić zapas żywności i wody).

• W przypadku ewakuacji postępuj zgodnie z procedurą.

• Podkreśl potrzebę maksymalnej dyskrecji. Minimalizuj i kontroluj uwagę mediów.

Andrzej Krasowski

Schrack Seconet

Wyzwania w zapewnieniu bezpieczeństwa w hotelach

Komfort pobytu gości jest bez wątpienia jednym z priorytetów właściciela czy menedżera każdego obiektu hotelowego. Dobrze wyposażone pokoje, wygodne łóżka, doskonała lokalizacja, wyśmienita kuchnia to czynniki ważne z punktu użytkowego. Należy pamiętać, że równie istotne jest zapewnienie odpowiedniego bezpieczeństwa pobytu i wynikającej stąd konieczności ochrony życia i zdrowia zarówno gości, jak i personelu. To z pewnością proces niezauważalny z punktu widzenia gościa, ale powinien być jednym z krytycznych dla osób odpowiedzialnych za bezpieczeństwo.

Analiza zagrożeń, na które są narażone obiekty hotelowe, nakazuje patrzeć na ich bezpieczeństwo wielowymiarowo. Należy brać pod uwagę czynniki wewnętrzne i zewnętrzne. Mogą to być zarówno zachowania chuligańskie, akty wandalizmu, ataki terrorystyczne, jak i różnego rodzaju zagrożenia pożarowe. Ich przyczyny wynikają z zaniedbań personelu lub gości hotelowych, ale mogą być także konsekwencją wadliwej pracy urządzeń technicznych.

W każdej takiej sytuacji krytyczne jest sprawne i pewne współdziałanie wielu systemów, które na ogół w niewidoczny i nieodczuwalny dla otoczenia sposób czuwają nieprzerwanie nad bezpieczeństwem obiektu.

Warto zaufać tym, których wiedza, zaawansowane technicznie urządzenia oraz wielokrotnie wdrożone i sprawdzone rozwiązania dają najwyższą gwarancję niezawodności. Takim sprawdzonym partnerem jest bez wątpienia firma Schrack Seconet Polska, od lat dostarczająca najbardziej zaawansowane technicznie rozwiązania stoso-

wane w detekcji pożaru, sterowaniu automatyką pożarową i kompleksowym zarządzaniu bezpieczeństwem pożarowym.
SIUP SIS-Fire realizuje funkcje nadzoru, sterowania i zarządzania systemami bezpieczeństwa pożarowego oraz innymi urządzeniami i systemami mającymi wpływ na bezpieczeństwo pożarowe obiektu. System zarządza sprawnym przepływem informacji, automatyzuje i koordynuje procesy obsługi i sterowania, dzięki czemu jest narzędziem wspierającym personel ochrony obiektu i pozwala na skuteczne zarządzanie ewakuacją w przypadku alarmu pożarowego lub innego zdarzenia kryzysowego.
Warto powierzyć życie gości, mienie i bezpieczeństwo obiektu w ręce ekspertów, a pobyt w hotelu pozostanie zapamiętany wyłącznie jako niezwykle atrakcyjny, mile spędzony czas.

Bogumił Szymanek

Axis Communications

Bezpieczeństwo placówek bankowych w dobie pandemii

Przez stulecia oddziały bankowe były utożsamiane z najwyższym poziomem bezpieczeństwa. Wzrost znaczenia cyfrowych usług bankowych wymusza dziś dynamiczną ewolucję placówek, które teraz coraz częściej służą przede wszystkim za centra doradztwa. Za tymi przemianami idzie także zmiana definicji bezpieczeństwa w oddziałach, szczególnie w czasach COVID-19.
Mówiąc o technologii wspierającej bezpieczeństwo w czasach pandemii, mamy na myśli przede wszystkim te rozwiązania, które pozwalają zachować odpowiedni dystans społeczny. Przykładem mogą być systemy monitoringu wizyjnego, które samodzielnie zliczają osoby wchodzące do placówki bankowej. Po osiągnięciu określonego limitu na ekranie zainstalowanym przed wejściem automatycznie pojawi się informacja z prośbą o zaczekanie, aż ktoś opuści oddział.
To niejedyna „automatyzacja", która może pomóc w zachowywaniu obecnych norm sanitarnych. Innym przykładem jest system kamer wzbogacony o tor audio, który po wykryciu przekroczenia limitu osób na metr kwadratowy bądź braku maseczki na twarzy odwiedzającego nadadzą automatyczny komunikat głosowy, np. z prośbą o zachowanie dystansu społecznego. Tego typu rozwiązania przydadzą się nie tylko w czasach pandemii, w przyszłości mogą nadawać np. komunikat powitalny lub muzykę, wzbogacając tym samym doświadczenie klienta placówki.
Kwestie bezpieczeństwa dotyczą nie tylko klientów, ale także pracowników. System audio funkcjonujący poza miejscami dostępnymi dla klientów może regularnie przypominać o potrzebie mycia rąk czy zachowywaniu odpowiedniego dystansu. Ponadto wejście do strefy pracowniczej można wyposażyć w bezdotykowy system dostępu bazujący np. na aplikacji mobilnej lub kodach QR. Dzięki temu pracownicy nie będą narażeni na dotykanie takich elementów, jak klamki czy klawiatury dostępowe.
Tego typu rozwiązania z pewnością pozytywnie wpłyną na poczucie bezpieczeństwa nie tylko klientów, ale także pracowników, wspierając placówki bankowe również po zakończeniu pandemii.

Jakub Sobek

Linc Polska

Z sejfu do serwera, czyli najlepsza lokata bankowa

Coraz więcej państw rozważa lub planuje w przyszłości całkowitą rezygnację z tradycyjnych środków płatniczych. Choć perspektywa czasowa dla tych założeń w poszczególnych krajach jest różna, to mówi się o tym coraz częściej np. w Szwecji, Danii, Norwegii czy Korei Południowej. W Ekwadorze już w 2015 r. uruchomiono państwowy system pieniądza elektronicznego, dzięki czemu jest to pierwszy kraj z cyfrowym systemem płatności krajowych. To naturalny kierunek rozwoju, który dodatkowo jest napędzany przez kryptowaluty.
Napady na bank w westernowym stylu odejdą w zapomnienie. Co mielibyśmy chronić w banku, jeśli za parę lat nie będzie tam gotówki? Po co w instytucjach finansowych instalować kamery lub inne systemy zabezpieczenia technicznego?
Cyfrowa gotówka jest także wartością, która będzie wymagała ochrony i to w znacznie nowocześniejszy sposób, niż to było do tej pory. Cyfryzacja wartości pieniężnych sprawia, że gotówka z sejfów przenosi się na serwery. To właśnie centra danych i wszelkie kanały dostępowe będą wymagały szczególnej ochrony. W serwerowniach systemy kamer, kontroli dostępu oraz wczesnej detekcji pożarów z pewnością będą podnosić poziom jakości i skuteczności działania. Wszystko dzięki postępującej integracji systemów i ich wsparcia automatycznym dozorem wizyjnym wykorzystującym nowe rozwiązania AI.
Liczba klasycznych oddziałów bankowych z pewnością będzie się zmniejszać, to efekt przejścia na bankowość internetową lub kolejne rozwiązania wprowadzane przez segment fintech. W tych placówkach, które pozostaną, kamery udostępnią jednak zupełnie nowe funkcjonalności. Można za ich pomocą analizować zachowania klientów w poszczególnych oddziałach, np. czas oczekiwania na obsługę, lub monitorować zajętość poszczególnych stanowisk. Część firm na podstawie informacji z kamer oferuje także rozwiązania typu „tajemniczy klient" – w określonych przedziałach czasowych, łącząc się z kamerami i sprawdzając np. porządek na biurkach pracowników, odpowiednie oświetlenie lub inne elementy wystroju banku.
Transformacja sektora bankowego będzie wymuszać transformację branży ochrony. Bez wiedzy informatycznej i znajomości nowych technologii firmy nie będą dla banków partnerami do rozmowy. Zatem inwestycja w wiedzę jest i będzie najlepszą „lokatą bankową". □

Nowoczesne sterowanie urządzeniami biorącymi udział w scenariuszu pożarowym

Obecne rozwiązania techniczne umożliwiają pełną kontrolę nad algorytmami sterującymi, realizującymi coraz bardziej skomplikowane scenariusze pożarowe. Dzięki temu eksploatowanie obiektu jest nie tylko bezpieczne dla użytkowników, lecz także nie sprawia problemów.

Nowoczesne budownictwo musi spełniać coraz bardziej wyśrubowane standardy bezpieczeństwa pożarowego, wprowadzane przez branżowych specjalistów i potwierdzane w nowelizowanych przepisach, rozporządzeniach i prawie budowlanym. Nowo projektowany obiekt należy wyposażyć w większą liczbę urządzeń technicznych zapewniających odpowiednie standardy ochrony ppoż. Wszystkie muszą właściwie zadziałać w przypadku wykrycia zagrożenia. Sposób ochrony budynku opisuje dokument nazwany scenariuszem pożarowym.

Zasadniczym i najczęstszym problemem w trakcie realizacji scenariusza pożarowego jest synchronizacja działania urządzeń budynkowych z systemami ppoż. Prawidłowo zaprojektowany scenariusz musi zapewniać warunki bezpiecznej ewakuacji oraz wydzielenie strefy objętej pożarem. Umożliwia to przede wszystkim odpowiednie sterowanie urządzeniami i systemami ppoż.
Na podstawie dotychczasowych realizacji projektanci uważają, że system automatyki pożarowej należy podzielić na detekcyjny oraz sterująco-monitorujący, które wymieniają między sobą niezbędne informacje, ale fizycznie są rozdzielone w obszarach instalacyjnych, konfiguracyjnych i sprzętowo-programowych. Takie rozwiązanie znacząco wpływa na prawidłowość realizacji przyjętego scenariusza pożarowego bez ryzyka zablokowania się systemu SSP, którego podstawową rolą jest wykrycie zagrożenia i poinformowanie o tym.
Wszystkie funkcje sterujące i kontrolne przejmuje więc odrębny system zbudowany z wykorzystaniem centrali sterująco-monitorującej, odciążający z tego zakresu centrale sygnalizacji pożarowej zgodnie z zasadą, że funkcje detekcyjne nie powinny być zakłócane przez coraz bardziej skomplikowane programy sterujące i coraz większą liczbę sygnałów monitorujących (*feedback*).

Rolą SSP, zgodnie z normą PN-EN 54-1, jest wykrycie pożaru i podanie słyszalnych i/lub widzialnych sygnałów użytkownikom budynku, którzy mogą być zagrożeni pożarem. Oddzielenie obszaru detekcji od obszaru sterująco-monitorującego znacząco wpływa na jego niezawodność. Centrala sterująco-monitorująca stanowi warstwę pomiędzy systemem SSP a urządzeniami i systemami wykonawczymi. Umożliwia implementację scenariuszy pożarowych ze wszystkimi wymaganiami czasowymi i zależnościami logicznymi.
Każde urządzenie może mieć indywidualnie ustawiony czas zarówno wysterowania w reakcji na alarm pożarowy, jak i przejścia do stanu spoczynku w odpowiedzi na reset pożarowy; czasy te mogą być różne w każdej ze stref. Pozwala to na optymalne dostosowanie sterowań do warunków w obiekcie (z uwzględnieniem strefy, w której wykryto pożar), scenariusza ewakuacji ludzi z obiektu oraz innych czynników, np. wymagań technologicznych dot. zastosowanych urządzeń. Rozdzielenie funkcji detekcyjnej od sterującej ma także istotny wpływ na przebieg procesu instalacyjno-uruchomieniowego. System SSP można instalować niezależnie od systemu sterującego i prowadzić próby odcinkowe oraz testy współdziałania.

Branża security w obszarze ppoż. napotyka wiele wyzwań. Nadchodzące zmiany w prawie budowlanym, brak interakcji między systemami, rosnące koszty ochrony fizycznej to tylko niektóre z nich. W trakcie eksploatacji obiektu gromadzone są wszelkie informacje o stanie zintegrowanych, sterowanych i monitorowanych systemów, analizowane słabe punkty, by móc natychmiast informować o wykrytych awariach i usterkach. Gromadzone dane można przetwarzać na wiele sposobów i przedstawiać w najbardziej czytelnej formie.
W Ela-compil powstał **FPM+, czyli Fire Protection Manager** – nowoczesne środowisko zapewniające sterowanie wszystkimi urządzeniami ppoż. i pozostałymi urządzeniami uwzględnianymi w scenariuszu pożarowym.

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

Zasilacze urządzeń przeciwpożarowych 230 V napięcia przemiennego

TEKST
Dariusz Cygankiewicz

Założenia budowy rezerwowego zasilania 230 V dla instalacji bezpieczeństwa w systemach ochrony ppoż.

Potrzeba i idea zasilania elektrycznego o wysokiej niezawodności urządzeń systemów przeciwpożarowych jest sprecyzowana w najnowszym wydaniu normy [1]. Nadrzędny cel niezawodności instalacji ppoż., będącej w całości lub w części instalacją bezpieczeństwa, narzuca w p. 560.6.1 tej normy stosowanie następujących rozwiązań zasilania systemu (poza podstawową linią zasilania):

1. akumulatory,
2. ogniwa galwaniczne,
3. zespoły prądotwórcze niezależne od normalnego źródła zasilania,
4. oddzielne przyłącze sieci zasilającej, które jest skutecznie uniezależnione od normalnego przyłącza.

Pierwsze z przedstawionych rozwiązań umożliwia wykorzystanie:

- napięcia baterii 24 V wprost jako wyjściowego źródła bardzo niskiego napięcia stałego (ELV wg normy [2]),
- baterii akumulatorów 24 V jako rezerwowego źródła napięcia stałego,
- napięcia tej samej baterii 24 V jako źródła zasilania przetwornicy DC/AC generującej niskie napięcie przemienne 230 V (LV wg [2]).

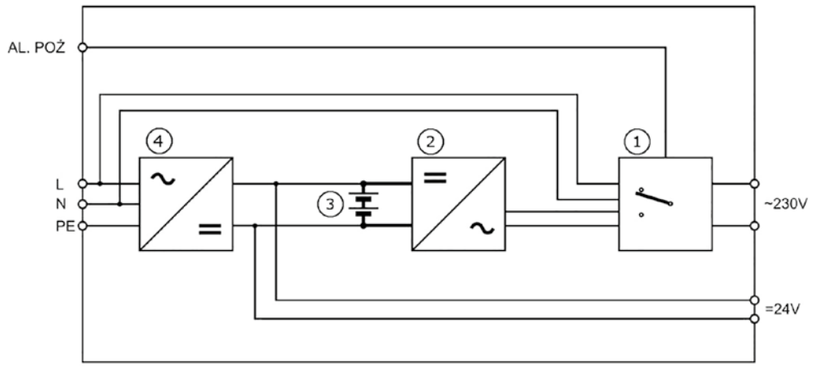
Zasilacz zbudowany zgodnie z przedstawionymi zasadami jest źródłem gwarantowanego napięcia przemiennego 230 V i napięcia stałego 24 V. W takim zasilaczu po zaniku zasilania podstawowego wyjście przetwornicy – będącej rezerwowym źródłem zasilania 230 V – jest automatycznie i prawie bezprzerwowo przyłączane na określony czas do urządzeń odbiorczych prądu przemiennego.
Cechą charakterystyczną większości urządzeń systemów kontroli rozprzestrzeniania dymu i ciepła (SKRDiC – grupa norm PN-EN 12101) zasilanych napięciem 230 V jest brak poboru mocy w trakcie dozoru, kiedy te urządzenia pozostają na ogół w bezruchu. Przy uwzględnieniu tej właściwości zasilacz pracuje w trybie dozoru przez 72 godz. po zaniku sieci podstawowej i po upływie tego czasu jest zdolny dostarczyć pełną moc napięcia zarówno przemiennego 230 V, jak i stałego 24 V do zasilania urządzenia (urządzeń) w trakcie alarmu pożarowego przez czas wymagany dla alarmu zgodnie z normami [2] i [3].

W p. 560.3.16 normy [1] są wymienione m.in. następujące systemy bezpieczeństwa:

- alarmowe (np. pożarowe),
- ewakuacyjne,
- wyciągów dymu.

Funkcje specjalne zasilacza

1. W trakcie długotrwałego zaniku zasilania podstawowego zasilacz 230 V (wyłączony w celu oszczędzania energii) musi zareagować na sygnał alarmu pożarowego i w efekcie udostępnić napięcie 230 V. Powinno się to odbywać tylko w tym czasie, w jakim wymagane jest dostarczenie energii do zasilanego urządzenia.
2. Po zakończeniu działania urządzeń podczas dalszego zaniku sieci podstawowej zasilacz przechodzi w stan czuwania – wtedy przetwornica będąca źródłem rezerwowym 230 V zostanie ponownie wyłączona.



Rys. 1. Schemat blokowy zasilacza gwarantowanego napięcia przemiennego 230 V i stałego 24 V:
1 - główny blok rozdziału zasilania 230 V,
2 - przetwornica 24 V DC/230 V AC,
3 - bateria akumulatorów 24 V,
4 - zasilacz AC/DC, którego podstawową funkcją jest ładowanie, nadzór nad baterią akumulatorów, dostarczanie prądu do wyjścia 24 V DC oraz zasilanie układów elektronicznych bloku rozdziału zasilania 230 V.

UWAGI:
1) pozycja przełącznika na rysunku odpowiada zasilaniu podstawowemu z sieci elektroenergetycznej,
2) zanik zasilania podstawowego 230 V powoduje zmianę położenia przełącznika, co umożliwia zasilanie urządzeń odbiorczych ze źródła rezerwowego 230 V.

Na rys. 1. przedstawiono schemat blokowy zasilacza obrazujący opisaną ideę jego działania.

Ciągłość funkcjonowania a ciągłość dostawy energii dla instalacji bezpieczeństwa

Ciągłość funkcjonowania systemów ppoż. zależy od ciągłości dostawy energii do poszczególnych urządzeń systemu. W przypadku systemów zasilanych prądem przemiennym ciągłość dostawy energii jest zagadnieniem bardziej skomplikowanym (niż przy prądzie stałym) i nie musi być interpretowana w dosłownym znaczeniu słowa „ciągłość".
Zależnie od konstrukcji, cech funkcjonalnych i przeznaczenia urządzenia może ono działać w sposób ciągły zgodnie z potrzebami systemu ppoż., przy określonych przerwach w ciągłości zasilania. Przerwy te mogą powstać np. w trakcie przełączenia z zasilania podstawowego na zasilanie rezerwowe lub odwrotnie – z zasilania rezerwowego na zasilanie podstawowe.
Dla zasilaczy urządzeń ppoż. zgodnie z normą [2] czas przerwy w zasilaniu musi być zdeklarowany przez producenta w specyfikacji technicznej zasilacza (instrukcji obsługi) i na tabliczce znamionowej. Znajomość charakteru pracy zasilanych urządzeń i ich reakcji na określoną przerwę w zasilaniu jest podstawą do deklarowania przez producenta przewidywanych zastosowań zasilaczy.
Z punktu widzenia bezpieczeństwa obiektu oraz jego użytkowników zasilacze powinny charakteryzować się możliwie najkrótszą przerwą.
Najlepiej, gdy zgodnie z normą [1] (p. 560.4.1) zasilacze napięcia gwarantowanego 230 V pracują w trybie samoczynnym, o bardzo krótkiej przerwie (klasa B), przy której automatyczne przełączenie zasilania następuje w czasie 0,15 s lub nieco krótszym. Czas przerwy można dostosować w zależności od typu zasilanego urządzenia i zasady jego działania. Należy przy tym mieć na względzie minimalizację ryzyka braku zasilania urządzeń w czasie pożaru, gdyż nadmierne skracanie przerwy może zmniejszyć niezawodność i pewność działania zasilacza.
Bardzo ważne, aby podczas doboru czasu przerwy mieć na uwadze zapobieżenie zresetowaniu się sterownika zasilanego urządzenia. Przy stosunkowo krótkiej przerwie w zasilaniu uzyska się ciągłość w funkcjonowaniu urządzenia, a przerwa w zasilaniu będzie praktycznie niezauważalna wizualnie.

Czas pracy urządzeń stosowanych w ochronie ppoż.

W artykule przedmiotem końcowych rozważań będą zasilacze gwarantowanego napięcia przemiennego, wykorzystujące energię zgromadzoną w baterii akumulatorów. Energia akumulatorów służy do wytworzenia rezerwowego napięcia 230 V, które po zaniku sieci podstawowej zasila urządzenia odbiorcze. Niezbędny czas działania urządzeń (np. siłowników klap odcinających wentylacji pożarowej, napędów bram napowietrzających) wynika ze specyfiki ich działania i na ogół nie przekracza 1 minuty.
Odmiennym zagadnieniem jest czas pracy wentylatorów stosowanych w ochronie przeciwpożarowej. Dla wentylatorów napowietrzających lub oddymiających czas działania wynika głównie ze scenariusza pożarowego i na ogół wynosi 30 minut. Przy takim zróżnicowaniu czasów pracy konstrukcja zasilaczy powinna uwzględniać możliwość ich nastaw, choćby ze względu na oszczędność energii.

Podsumowanie

Na podstawie założeń sprecyzowanych w normach [1], [2], [3] opracowano i wdrożono do produkcji rodzinę zasilaczy ZUP-230V predestynowaną do zastosowań w instalacjach bezpieczeństwa w charakterze „czynnych" urządzeń ochrony przeciwpożarowej.
Zasilacze mają certyfikat stałości właściwości użytkowych CPR i świadectwo dopuszczenia do użytkowania, a ponadto uzyskały Złoty Medal 2020 w Konkursie Międzynarodowych Targów Poznańskich. □

BIBLIOGRAFIA

[1] PN-HD 60364-5-56: 2019-01 Instalacje elektryczne niskiego napięcia. Część 5-56: Dobór i montaż wyposażenia elektrycznego. Instalacje bezpieczeństwa
[2] PN-EN 12101-10:2007 Systemy kontroli rozprzestrzeniania dymu i ciepła. Część 10: Zasilacze
[3] PN-EN 54-4: 2001 +A1: 2004 +A2: 2007 Systemy sygnalizacji pożarowej. Część 4: Zasilacze

MERAWEX
ul. Toruńska 8
44-122 Gliwice
merawex@merawex.com.pl
https://merawex.com.pl/

W trosce o środowisko

ZRÓWNOWAŻONY ROZWÓJ I TECHNOLOGIE PRZYJAZNE DLA ŚRODOWISKA SĄ TERAZ TEMATAMI MODNYMI. WSZYSCY MÓWIĄ O ZMIANACH KLIMATYCZNYCH, NIEKTÓRZY UWAŻAJĄ, ŻE KLIMAT ZAWSZE SIĘ ZMIENIAŁ, I MAJĄ RACJĘ. DZIEŃ DŁUGU EKOLOGICZNEGO (*Earth Overshoot Day*) KAŻDEGO ROKU NADCHODZI JEDNAK WCZEŚNIEJ. CZY MNIEJ OZNACZAŁOBY WIĘCEJ?

W latach 80. ub. wieku świat podjął działania na rzecz ochrony warstwy ozonowej. Substancją, której stosowanie zostało wówczas zakazane, był halon powodujący zubożenie atmosfery ziemskiej. Wycofanie z użytku tego środka gaśniczego pozostawiło w ochronie przeciwpożarowej lukę, którą wypełniła mgła wodna.

Co sprawia, że mgła wodna jest przyjazna dla środowiska?

Systemy gaszące mgłą wodną zużywają do 85% mniej wody niż tradycyjne instalacje tryskaczowe i mogą być podłączane do sieci wodociągowej lub małego zbiornika. W obu przypadkach nie wymagają dużego metrażu. Mówimy więc o oszczędności miejsca i materiałów, a co za tym idzie – o mniejszych kosztach.

Możliwość korzystania z sieci wodociągowej sprawia, że systemy mgły wodnej są atrakcyjne dla właścicieli domów i budynków. Otrzymują system gaszenia, który chroni obiekt i podnosi poziom bezpieczeństwa bez użycia szkodliwych substancji. Instalacja jest szybka, system można łatwo zmodernizować.

W wielu przypadkach problem stanowi brak miejsca na zbiornik. Rozwiązaniem jest wykorzystanie jednego systemu do ochrony kilku budynków. Jest to również bardzo przydatne w obiektach zabytkowych, gdzie integracja systemu ochrony ppoż. może być skomplikowana. Brak konieczności instalowania zbiornika i stosowanie rur o mniejszej średnicy sprawia, że system mgły wodnej jest najlepszym rozwiązaniem.

Z myślą o środowisku

Stowarzyszenie IWMA (International Water Mist Association) zaleca, aby wszystkie elementy mające kontakt z wodą były wykonane ze stali nierdzewnej! Nie jest to obowiązkowe, ale Michael Bindreiter, szef działu sprzedaży globalnej w Aquasys, zwraca uwagę, że *zastosowanie elementów z wysokiej jakości stali nierdzewnej odpornej na korozję zapobiega zanieczyszczeniom i wspiera wysoki standard higieny.*

Mówiąc o „zanieczyszczeniu" i „higienie", mamy na myśli również konieczność usuwania pozostałości po pożarach w obszarach szczególnego przeznaczenia. Tam pożar może spowodować uwolnienie wielu różnych toksyn i chemikaliów. Luciano Nigro, prezes Jensen Hughes Con. Europa – Mediolan, wyjaśnia: *Na obszarach o specjalnym przeznaczeniu woda gaśnicza musi być zbierana i usuwana, co jest trudnym zadaniem, ale tym łatwiejszym, im mniej wody trzeba zebrać. Ilość wody zużywanej przez system mgły wodnej jest najmniejsza, a zatem łatwiejsza do zatrzymania i znacznie tańsza w utylizacji.* Ponadto dzięki mniejszej ilości odprowadzanej wody mniejsze są ogólne uszkodzenia. To oznacza kolejną oszczędność kosztów, ponieważ firma ma mniej przestojów i mniej zanieczyszczeń do usunięcia.

Inną kwestią jest efekt wypełnienia środkiem gaśniczym całego pomieszczenia: ze względu na wielkość kropel mgła wodna jest dobrze rozprowadzana, wypełnia wszelkie zakamarki i szczeliny w ciągu kilku sekund od aktywacji. Jest też stale doprowadzana, dzięki czemu obszar jest zasilany nowymi drobnymi kroplami. Większość z nich może bezpośrednio oddziaływać na źródło ognia, co prowadzi do silnego efektu chłodzenia, który zapobiega ponownemu zapłonowi, a w konsekwencji do ugaszenia ognia.

Przykłady zastosowań

W budynkach projektowanych z myślą o ochronie środowiska coraz więcej klientów końcowych wybiera systemy ppoż. na mgłę wodną.

• Green Pea w Turynie we Włoszech

To czteropiętrowe centrum wielofunkcyjne chce koncentrować się na przyjaznym dla środowiska handlu detalicznym i gastronomii. Powstaje z uwzględnieniem zasady zrównoważonej architektury przy minimalnym wpływie na środowisko. Firma VID Fire-Kill weźmie udział w ponownym zagospodarowaniu budynku. – *W tym przypadku przyjazny dla środowiska system gaszenia pożarów spełnia wymogi zrównoważonej architektury, ponieważ celem jest jak najmniejszy wpływ na środowisko* – powiedział Alex Palle, dyrektor generalny VID Fire-Kill.

Budynek Green Pea jest pokryty panelami drewnianymi, a część kompozycji stanowi roślinność. Zastosowanie naturalnych materiałów w projekcie wymaga unikalnej, skutecznej strategii ochrony ppoż., wkomponowanej w otoczenie. Ponieważ założeniem był jak najmniejszy wpływ na środowisko, klient szukał odpowiedniego systemu gaszenia pożaru. A. Palle wyjaśnia: *Klient końcowy wiedział, że nasz system mgły wodnej charakteryzuje się niskim zużyciem wody i energii, a także niewidoczną strukturą. To doskonale spełnia jego wymagania.*

• Hotel Alsik w Sønderborg w Danii

Hotel otwarto na początku 2019 r. Już na etapie projektu wieżowiec odgrywał szczególną rolę w mieście, które ma aspiracje bycia jednym z najbardziej przyjaznych dla środowiska miejsc w Danii. Celem była optymalizacja dostaw, wykorzystania energii, wody i materiałów oraz zapewnienie, że działalność hotelu będzie przyjazna dla środowiska.

Aby zachować zgodność z wizją zrównoważonego rozwoju budynku i miasta, starannie wybrano dostawców, a firmie Danfoss Fire Safety powierzono zadanie wdrożenia systemu ppoż. – *Jesteśmy dumni z tego, że zostaliśmy wybrani na dostawcę systemu ochrony przeciwpożarowej i stanowimy część projektu wdrażania czystych technologii* – stwierdził Henrik Bygbjerg, Global Director R&D, Service, EHS & Q w Danfoss Fire Safety.

W hotelu zainstalowano 2500 dysz w przestrzeniach o średnim zagrożeniu pożarowym OH1, OH3 i OH4, takich jak biura, pokoje hotelowe, restauracje, sale konferencyjne, spa, siłownia, atrium i magazyny.

Wizualizacja hotelu Alsik w Sønderborg w Danii

Hotel Alsik w Sønderborg w Danii

• Państwowe Laboratorium Berlin Brandenburg w Niemczech

Jedno to być w harmonii ze środowiskiem, drugie to je chronić. Ważnym aspektem jest tutaj ochrona wrażliwych obszarów i zaawansowanych technicznie urządzeń w szczególnych warunkach środowiskowych przy jednoczesnym zmniejszeniu ryzyka zanieczyszczenia. To duże wyzwanie dla operatorów laboratoriów, centrów danych czy szpitali.

– *Zapobieganie korozji rurociągów, możliwość stosowania zdemineralizowanej wody w połączeniu z wysokiej jakości stalą nierdzewną, a co za tym idzie możliwość obniżenia ryzyka zanieczyszczenia zapewnia spełnienie najwyższych wymagań w zakresie czystości* – zauważa M. Bindreiter z Aquasys.

Państwowe Laboratorium Berlin Brandenburg było pierwszą międzynarodową instytucją badawczą w Niemczech, zajmującą się szerokim zakresem badań w obszarach ochrony konsumentów, ochrony przed promieniowaniem, kontroli chorób zwierząt i katastrof. W 4-kondygnacyjnym budynku na powierzchni 249 m² działają laboratoria o trzecim poziomie bezpieczeństwa chronione systemem mgły wodnej firmy Aquasys.

• Elektrownia w Carmignano di Brenta we Włoszech

W roku 2016 firma Marioff dostarczyła system ochrony ppoż. do maszynowni elektrowni wykorzystującej energię odnawialną, zarządzaną przez Onenergy srl. Celem było zainstalowanie systemu gaszenia zgodnego z ideą zrównoważonego rozwoju i zapewniającego ochronę ppoż. bez ryzyka zanieczyszczenia środowiska pracy.

Massimo Ferretti, regionalny kierownik sprzedaży w Marioff, wyjaśnia: *Klient zdecydował się na system mgły wodnej, ponieważ nie jest ona szkodliwa dla ludzi, a jej wpływ na zakład w przypadku sytuacji awaryjnej jest minimalny, gdyż jest ona obojętna dla środowiska. Nie ma też kosztów utylizacji środka gaśniczego, więc system jako całość chroni personel, zakład i środowisko.*

Dobry projekt sprzyja środowisku

Globalna zmiana klimatu została uznana za jedno z najważniejszych – jeśli nie najważniejsze – wyzwań środowiskowych, przed którymi stoi ludzkość w XXI wieku. COVID-19 spowodował zmniejszenie śladu węglowego, jednak prawdziwy zrównoważony rozwój powinien być osiągany poprzez dobry projekt, a nie pod wpływem sytuacji kryzysowych. □

International Water Mist Association

Poststraße 33,
D-20354 Hamburg, Niemcy
tel. + 49 (0) 40 35085-215
www.iwma.net

1) Dzień Długu Ekologicznego to dzień, w którym ludzkość wykorzystała limit dostępnych na dany rok zasobów naturalnych Ziemi.

RAZEM, nawet zdalnie, możemy wszystko!

W DRUGIEJ POŁOWIE UB. ROKU SCHRACK SECONET POLSKA INFORMOWAŁA O PLANOWYCH W FIRMIE ZMIANACH. NOWYM PREZESEM ZARZĄDU SPÓŁKI OD 1 MAJA 2020 R. JEST MICHAŁ SIDOR, ZWIĄZANY Z ORGANIZACJĄ OD PONAD 11 LAT. DO KOŃCA KWIETNIA PEŁNIŁ FUNKCJĘ DYREKTORA HANDLOWEGO W POLSCE. POSTANOWILIŚMY ZAPYTAĆ, JAK ODNAJDUJE SIĘ W NOWEJ ROLI. JAK RADZI SOBIE W NIEZWYKLE TRUDNEJ DZIŚ SYTUACJI.

GRATULUJEMY AWANSU NA STANOWISKO PREZESA SCHRACK SECONET POLSKA. JAK CZUJE SIĘ PAN W NOWEJ ROLI?

Wspaniale! A zupełnie poważnie, bardzo dziękuję za zaproszenie do rozmowy i gratulacje. Jestem związany z firmą od wielu lat, znam dobrze branżę i ludzi, z którymi współpracujemy, mam koleżeńskie relacje z zespołem, dlatego dość naturalnie odnalazłem się w nowej roli. Oczywiście perspektywa współpracy jest dziś zupełnie inna, muszę patrzeć zdecydowanie szerzej zarówno na firmę i współpracowników, jak i na potrzeby firm partnerskich i klientów oraz relacje z nimi.

JAKĄ MA PAN WIZJĘ ROZWOJU FIRMY? JAKIEŚ SZCZEGÓLNE PRZEDSIĘWZIĘCIA?

Zdecydowanie zamierzam kontynuować dotychczasową politykę firmy, niezmienne pozostaną strategia i zasady naszych działań rynkowych. Planujemy i wdrażamy stopniowo nowe produkty i rozwiązania, spójne z dotychczasowymi kierunkami rozwoju firmy. Musimy jednak pamiętać, że dziś funkcjonujemy w zupełnie nowej rzeczywistości, znacznie zmienionej przez pandemię. Dość trudna sytuacja w kraju i na świecie, związana z COVID-19, niesie ze sobą ryzyko konieczności korygowania zaplanowanych działań. Mam jednak nadzieję, że już w pierwszym kwartale przyszłego roku będziemy mogli podzielić się z Państwem szczegółami dotyczącymi planowanych przez nas przedsięwzięć.

MÓWI PAN O NOWYCH POMYSŁACH, CZY JUŻ DZIŚ MOŻE PAN ZDRADZIĆ CZYTELNIKOM, CZEGO KONKRETNIE DOTYCZĄ?

Na ten moment mogę zdradzić tylko tyle, że wśród kluczowych nowości w ofercie Schrack Seconet znajdzie się m.in. produkt związany ze sterowaniem i zasilaniem pożarowym, który umożliwi nam zaoferowanie partnerom kompleksowego rozwiązania: od detekcji, poprzez sterowanie i zasilanie urządzeniami przeciwpożarowymi, na certyfikowanym systemie integrującym skończywszy.

CZYLI W NAJBLIŻSZYM CZASIE MOŻNA SPODZIEWAĆ SIĘ WIĘCEJ NOWOŚCI W PAŃSTWA OFERCIE?

Zdecydowanie tak. Wspólnie z naszymi kolegami z Austrii przygotowujemy się do wprowadzenia na rynek kolejnej generacji systemu sygnalizacji pożarowej. Jak zwykle do takich istotnych zmian w ofercie przygotowujemy się z ogromną starannością. Do dzisiaj nazwy nowego systemu jeszcze nie ujawniliśmy, więc jeśli powiem, że będzie to **Integral EvoxX** zdecydowanie możemy stwierdzić, że na łamach czasopisma „a&s Polska" rozpoczynamy premierę naszego nowego rozwiązania. Więcej o samym systemie, jego funkcjonalnościach i oprogramowaniu będziemy mogli Państwu przekazać wraz z rozpoczęciem kampanii marketingowej w 2021 r.

JAKIE SĄ PRIORYTETOWE OBSZARY DZIAŁANIA SCHRACK SECONET, NA KTÓRYCH CHCIAŁBY SIĘ PAN SKUPIĆ W NAJBLIŻSZYCH LATACH? KTÓRE OBSZARY CHCE PAN ROZWIJAĆ?

Odpowiedź na te pytania wynika bezpośrednio z naszych działań okołoproduktowych.

Wiele miesięcy temu rozpoczęliśmy prace nad rozwiązaniami, o których wspominałem wcześniej. Rynek związany z systemami bezpieczeństwa pożarowego jest dziś mocno skupiony 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. Oczywiście naszym core biznesem pozostanie niezmiennie stale udoskonalany system sygnalizacji pożarowej.

JAKIE WYZWANIA STOJĄ PRZED PANEM ORAZ FIRMĄ SCHRACK SECONET W NAJBLIŻSZYM CZASIE?

Największym wyzwaniem dla nas wszystkich będzie w dalszym ciągu mierzenie się z tym, co dzieje się na świecie. Pandemia i jej skutki będą miały ogromny wpływ na to, jak w ciągu najbliższych kilku lat będzie funkcjonował rynek. Musimy przewidywać możliwe spowolnienie, jednak nadal utrzymując realizację naszych celów i zobowiązań na tym samym wysokim poziomie. W roku 2020, mimo nie najlepszej sytuacji rynkowej, udaje nam się osiągać wszystkie postawione cele, a plany sprzedażowe nawet przekraczać. Wyzwaniem na rok 2021 jest przede wszystkim utrzymanie firmy w jak najlepszej kondycji, a samego wyniku na poziomie nie gorszym niż w roku bieżącym.

JAK ZBUDOWANY JEST OBECNIE MODEL BIZNESOWY SPÓŁKI?

Model biznesowy firmy jest od wielu lat niezmienny i taki pozostanie. Przewiduję jedynie drobne udoskonalenia w obszarze specjalizacji produktowych wśród firm partnerskich. Schrack Seconet, jako producent wysokiej klasy systemów bezpieczeństwa pożarowego, od samego początku swojej działalności w Polsce skoncentrował się na budowie sieci Autoryzowanych Partnerów. Początkowo wszystkie firmy z nami współpracujące (po przejściu procesu autoryzacji) uzyskiwały certyfikat autoryzacji uwiarygadniający na rynku zakres ich kompetencji. Od początku 2019 r. wprowadziliśmy kilka zmian definicyjnych oraz nowe wzory certyfikatów. Podstawowa struktura firm partnerskich Schrack Seconet Polska wyróżnia teraz trzy grupy kompetencyjne: Autoryzowanych Partnerów Wiodących, Autoryzowanych Partnerów oraz Partnerów Pre-autoryzowanych. Kończący się rok 2020 wiąże się

z weryfikacją firm partnerskich i aktualizacją uprawnień dla specjalistów reprezentujących te przedsiębiorstwa.

JAK OCENIA PAN POTENCJAŁ ROZWOJU RYNKU BUDOWLANEGO W NADCHODZĄCYM ROKU?

Obawiam się, że należy spodziewać się dalszego jego spowolnienia, możliwe jest też ograniczenie lub wstrzymanie realizowanych inwestycji czy przesunięcia w terminach rozpoczęcia nowych. Dziś można rozmawiać 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. Ja jestem przekonany, że nasza firma, mająca ponad 30-letnie doświadczenie na rynku polskim, wspierana przez najlepszych w branży partnerów, poradzi sobie nawet w tym najtrudniejszym okresie.

CO ZATEM MOŻE BYĆ RECEPTĄ NA SUKCES W NIEPEWNYCH GOSPODARCZO CZASACH?

Przede wszystkim ludzie i zaufanie. Zespół, silni i doświadczeni partnerzy biznesowi, relacje oparte na wieloletniej współpracy, zadowoleni klienci i ich wspieranie również po zakończeniu inwestycji. Konieczne jest też dostosowanie działań do zmieniających się warunków w tych specyficznych i nieprzewidywalnych czasach.

JAKIE SEKTORY SĄ DZISIAJ KLUCZOWYMI ODBIORCAMI ROZWIĄZAŃ SCHRACK SECONET?

Od wielu lat inwestycje biurowe zajmują pierwsze miejsca na naszej liście referencyjnej. Do tych obiektów dostarczyliśmy najwięcej systemów sygnalizacji pożarowej, DSO czy zarządzania bezpieczeństwem pożarowym SIS FIRE. Bardzo ważnym obszarem naszej działalności jest też sektor obiektów przemysłowych, niezwykle specyficzny, wymagający bardziej zaawansowanych rozwiązań z obszaru bezpieczeństwa, specjalnych certyfikatów i uprawień. Jesteśmy aktywni we wszystkich obszarach, zabezpieczamy obiekty historyczne, muzealne, wojskowe i szpitalne, do których dostarczamy również systemy przyzywowe i komunikacji. W każdym z tych sektorów działamy od wielu lat, dlatego możemy stale rozwijać i udoskonalać nasze systemy, by jak najlepiej spełnić oczekiwania wymagających klientów.

JAKA JEST DZIŚ POZYCJA SCHRACK SECONET NA RYNKU?

Schrack Seconet jest zdecydowanym liderem w branży systemów sygnalizacji i zarządzania bezpieczeństwem pożarowym oraz jednym z wiodących dostawców systemów przyzywowych i komunikacji szpitalnej. Zarówno system sygnalizacji pożarowej INTEGRAL IP, jak i system zarządzania bezpieczeństwem pożarowym SIS-Fire cieszą się bardzo dużym zainteresowaniem, zadowoleniem i uznaniem naszych klientów. Z sukcesami pojawiamy się w kolejnych technologicznie skomplikowanych inwestycjach w całym kraju. Z każdym rokiem zdobywamy też coraz większy udział w rynku dźwiękowych systemów ostrzegawczych (DSO), realizując z naszymi partnerami kolejne projekty. Jako producent nie pozwalamy o sobie zapomnieć w obszarze systemów przyzywowych i komunikacji szpitalnej, wyposażając w nasze systemy duże, skomplikowane obiekty, a ostatnio także szpitale COVID-owe.

SCHRACK SECONET FUNKCJONUJE Z POWODZENIEM NA RYNKU JUŻ PONAD 30 LAT. CO DECYDUJE O SUKCESIE I WIELOLETNIM ROZWOJU?

O sukcesie firmy zawsze decydują ludzie, w naszym przypadku także. Tworzymy zgrany, kreatywny zespół doświadczonych specjalistów, których cechuje nieustanny rozwój i zaangażowanie, co owocuje świetnymi relacjami z naszymi partnerami

biznesowymi. Sukces to także strategia działania, niezmienna, ale udoskonalana i dająca stabilizację. To również wieloletnia współpraca z silnymi partnerami, która buduje zaufanie i zadowolenie klientów końcowych. Niezwykle ważnymi aspektami są też stabilna polityka cenowa i oferowana przez nas technologia, ciesząca się bardzo dużym uznaniem.

JAK KSZTAŁTUJE SIĘ KONKURENCJA NA RYNKU, NA KTÓRYM SPÓŁKA PROWADZI DZIAŁALNOŚĆ? CO WYRÓŻNIA PAŃSTWA NA TLE INNYCH PRODUCENTÓW?

Na polskim rynku jest wielu producentów oferujących swoje rozwiązania w obszarze systemów bezpieczeństwa pożarowego, a to zdecydowanie wpływa na jakość dostępnych i nieustannie rozwijanych produktów. Nas, jako producenta, na pewno wyróżnia stabilny, wysokiej jakości produkt, klarowne zasady jego dystrybucji i bezpośrednie wsparcie posprzedażowe, czego dowodem jest nasz kilkunastoosobowy zespół wsparcia technicznego i realizacja szkoleń technicznych dla ponad 1000 specjalistów rocznie. Oferowane przez nas systemy są wybierane na potrzeby realizacji największych inwestycji w Polsce zdecydowanie częściej niż produkty i rozwiązania naszej konkurencji.

A CO PAN OSOBIŚCIE UWAŻA ZA NAJWIĘKSZY SUKCES FIRMY?

Zdecydowanie Zespół! Mam świadomość, że się powtarzam. Uważam jednak, że każdy sukces współtworzą ludzie, a nie jeden człowiek, chociaż miałby najlepsze na świecie pomysły. Tylko razem, wspierając siebie we wszystkich działaniach, ufając tym, którzy podejmują kluczowe decyzje, i wierząc, że robimy to wszystko w konkretnym, spójnym celu, możemy naprawdę wszystko.

JAKIE DZIAŁANIA PODJĘŁA FIRMA W CZASIE PANDEMII?

Już w pierwszych dniach po pojawieniu się w Polsce pierwszego potwierdzonego przypadku zakażenia podjęliśmy decyzję o uruchomieniu szkoleń online. Każdego roku szkolimy ponad tysiąc specjalistów, musieliśmy szybko przygotować się do tego, żeby przy wprowadzonych ograniczeniach móc szkolić wszystkich zainteresowanych naszymi rozwiązaniami i aktualizacją wiedzy. Od połowy marca do października przeszkoliliśmy online ponad 500 osób, co ze względu na ograniczenia związane z COVID-19 jest wynikiem, z którego naprawdę jesteśmy dumni. Na początku pandemii przygotowaliśmy dla naszych klientów specjalną ofertę na narzędzia zdalnego dostępu do systemów sygnalizacji pożarowej INTEGRAL IP umożliwiające korzystanie online ze wszystkich najważniejszych funkcji systemu. Niezależnie od tego, które z rozwiązań wchodzących w skład pakietu wybierzemy, zyskujemy gwarancję kontroli obiektu przez 24 godziny na dobę bez konieczności dojazdu na miejsce oraz możliwość zdiagnozowania i rozwiązania problemu online. W maju br. przygotowaliśmy specjalny materiał dotyczący tych rozwiązań, zachęcam raz jeszcze do zapoznania się z jego treścią w wydaniu specjalnym „a&s Polska”*.

Ze względu na nadal ogromne zagrożenie zdrowia pracowników, klientów i naszych rodzin pracujemy hybrydowo, ograniczamy kontakty do minimum – jeśli to możliwe. Od wielu miesięcy także bieżące spotkania biznesowe prowadzimy online. Niezmiennie dbamy o bezpieczeństwo, higienę miejsc pracy i sprzętu.

Duże wydarzenia branżowe przesuwamy o kolejne miesiące, mając nadzieję, że nie będą to lata.

Naszą maksymą na 2021 r. jest ***Remote with Schrack Seconet***. RAZEM, nawet zdalnie, możemy wszystko!

CZEGO MOŻEMY PANU ŻYCZYĆ Z OKAZJI OBJĘCIA FUNKCJI PREZESA?

Zdrowia. Biorąc pod uwagę aktualną sytuację, to słowo ciśnie się na usta jako pierwsze. Tak naprawdę, jeśli miałbym sobie czegoś życzyć, to przede wszystkim zaufania, które pozwoli dalej rozwijać zespół, firmę i relacje z naszymi partnerami i klientami. Redakcji, Czytelnikom A&S i wszystkim uczestnikom rynku budowlanego w Polsce chcę życzyć bezpiecznego i stabilnego 2021 roku. Niech zbliżające się święta Bożego Narodzenia będą spokojne, pełne wytchnienia i rodzinne, nawet jeśli będziemy musieli z najbliższymi spotkać się zdalnie, korzystając z urządzeń mobilnych. Takie doświadczenia uczą nas doceniać przede wszystkim drugiego człowieka, jego obecność i zaangażowanie.

JESZCZE RAZ GRATULUJEMY I ŻYCZYMY POWODZENIA!

* https://aspolska.pl/bezpieczenstwo-w-czasach-pandemii/

Nowa kamera stałopozycyjna Axis – znakomita jakość obrazu w miejscach o dużym natężeniu ruchu

Axis Communications właśnie wprowadził na rynek sieciową kamerę P1455-LE, typu bullet, oferującą wiele funkcji i rozdzielczość HDTV 1080p przy szybkości do 60 klatek/s. Jest to idealne urządzenie do wielu zastosowań związanych z dozorem wizyjnym, szczególnie w miejscach o dużym natężeniu ruchu.

Nowa kamera zewnętrzna, dzięki funkcji Axis Forensic WDR, rejestruje wysokiej jakości obraz nawet wtedy, gdy obserwowana scena zawiera zarówno ciemne, jak i jasne partie. Technologia Axis Lightfinder 2.0 zapewnia znakomity obraz nawet przy bardzo słabym oświetleniu, a Axis OptimizedIR umożliwia dozór na odległość do 40 m w całkowitej ciemności.
Funkcja przystosowywania czasu ekspozycji do natężenia ruchu w kamerze znacznie zmniejsza rozmycia obrazu powodowane przez zbliżające się lub blisko położone obiekty.
Ponadto dzięki technologii edge-to-edge kamera umożliwia inteligentne łączenie w pary urządzeń sieciowych Axis, które mogą ze sobą współpracować, np. przy dwukierunkowej transmisji audio za pośrednictwem głośników sieciowych Axis. Wszystko to pozwala spełniać indywidualne wymagania klientów.
Kamera AXIS P1455-LE realizuje także funkcję Axis Edge Vault, która chroni przypisany kamerze identyfikator urządzenia Axis i upraszcza uwierzytelnianie produktów Axis w sieci. Ponadto technologia Axis Zipstream z obsługą formatów H.264 i H.265 znacznie zmniejsza zapotrzebowanie na przepustowość i pamięć masową. □

Więcej informacji jest dostępnych na www.axis.com/pl-pl

Najważniejsze cechy

- Lightfinder 2.0, Forensic WDR i OptimizedIR
- Technologia edge-to-edge
- Przystosowywanie czasu ekspozycji do natężenia ruchu
- Udoskonalone funkcje zabezpieczeń
- Technologia Zipstream z obsługą formatów H.264 i H.265

Powrót marki Aritech

Aritech™, globalna marka rozwiązań z zakresu systemów alarmowych sygnalizacji włamania i napadu oraz dozoru wizyjnego, powraca na rynek z ofertą zintegrowanych i niezawodnych rozwiązań przeznaczonych do domów, budynków mieszkalnych i instytucji. Zastępuje markę Interlogix w komercyjnych i konsumenckich rozwiązaniach z zakresu systemów alarmowych oraz zintegrowanej kontroli dostępu, a także dozoru wizyjnego. Będzie obecna w nowych regionach świata, m.in. w Australii i Nowej Zelandii, Ameryce Łacińskiej oraz w niektórych krajach azjatyckich.

Aritech, wiodący producent rozwiązań z zakresu elektronicznych systemów zabezpieczeń, jest częścią firmy Carrier Global Corporation, czołowego światowego dostawcy rozwiązań służących do ochrony zdrowia, zapewnienia bezpieczeństwa i na potrzeby sektora budownictwa ekologicznego. Carrier jest także niekwestionowanym liderem w branży HVAC.
Aritech jednoznacznie kojarzy się z niezawodnością, innowacyjnością i koncentracją na klientach. Z dumą ogłaszamy powrót na rynek produktów Aritech – oznajmiła Stéphane Baudena, dyrektor zarządzający, Fire & Security Products EMEA, Carrier. – *Kontynuujemy wprowadzanie*

innowacji i dostarczanie zintegrowanych rozwiązań z zakresu zabezpieczeń, które wykraczają poza tradycyjne granice postrzegania systemów alarmowych, kontroli dostępu oraz dozoru wizyjnego.
W segmencie komercyjnym Aritech oferuje rozwiązania zintegrowane, które pozwalają klientom zarządzać swoimi potrzebami z zakresu bezpieczeństwa. Te zaawansowane produkty umożliwiają zarządzanie systemami zabezpieczeń budynków oraz dbanie o bezpieczeństwo pracowników i gości, począwszy od wykrywania włamań po kontrolę dostępu i dozór wizyjny. Innowacyjne rozwiązanie w chmurze UltraSync® gwarantuje bezpieczeństwo transmisji dzięki wykorzystaniu kompleksowej komunikacji z zastosowaniem pełnego szyfrowania i technologii VPN.
Innowacyjne rozwiązania Aritech oferuje również klientom detalicznym. Stosując rozwiązanie chmurowe UltraSync w połączeniu z platformą ZeroWire™, użytkownik może samodzielnie stworzyć bezprzewodowy system inteligentnego domu i w ten sposób zadbać o bezpieczeństwo rodziny i swojego dobytku, kontrolując sytuację na bieżąco z poziomu tabletu lub smartfonu.
Firma Aritech oferowała rozwiązania z zakresu security na rynku europejskim od momentu założenia w 1980 r., aż do zmiany marki na Interlogix, która nastąpiła w 2010 r. □

Więcej informacji na stronie https://pl.firesecurityproducts.com

Kasa na Nowy Rok od Hikvision

Koniec roku to czas podsumowań i podziękowań. Z tej okazji wiele firm decyduje się rozdawać prezenty swoim klientom.

Hikvision wystartowało zatem z promocją – Kasa na Nowy Rok! Robiąc zakupy u Autoryzowanych Dystrybutorów Hikvision, masz szansę odebrać voucher do jednej z popularnych sieci handlowych o wartości nawet 400 zł. Ile musisz wydać? Tylko 1000 zł netto, by „załapać się" na najniższy próg i odebrać 100 zł.
Szczegóły promocji znajdziesz na https://content.hikvision.com/kasananowyrok.
Zapraszamy do udziału w Promocji!
A korzystając z okazji firma Hikvision życzy czytelnikom A&S Polska i wszystkim swoim klientom Zdrowych Świąt i samych sukcesów w nadchodzącym Nowym Roku! □

AI trafia pod strzechy **Dahua XVR5216A-I2**

Model XVR5216A-I2 należy do nowości Dahua. To jeden z najprostszych rejestratorów HDCVI wyposażonych w algorytmy sztucznej inteligencji, które na podstawie rozpoznania obiektów potrafią odróżnić osoby i pojazdy od pozostałych elementów kadru, takich jak zwierzęta, roślinność, zmiany oświetlenia czy zjawiska pogodowe.

Wpływa to na zdecydowaną poprawę skuteczności działania algorytmów detekcji ruchu, przekroczenia linii oraz wejścia w strefę. Operator jest w ten sposób alarmowany tylko w przypadku wykrycia realnego zdarzenia. Dodatkowo ułatwia to przeszukiwanie nagrań, ponieważ na osi czasu są zaznaczone tylko prawdziwe alarmy.
XVR5216A-I2 pozwala na ustawienie inteligentnej detekcji ruchu na 16 kanałach lub detekcji IVS (przekroczenie linii, wejście w strefę) na dwóch kanałach. Alternatywnie można skorzystać z rozpoznawania twarzy na maks. dwóch kanałach.
Oprócz tego rejestrator jest kompatybilny z rozwiązaniami AHD, TVI, CVBS oraz IP, co pozwala wykorzystać już zainstalowane kamery albo wykonać płynną migrację np. z systemu analogowego. □

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

Linc Polska
nadszedł czas na zmiany...

Z radością informujemy, że w związku z rozwojem firmy już niebawem zmieniamy lokalizację. Przenosimy się w miejsce, które pozwoli nam lepiej wspierać Państwa działania w każdym zakresie.

Od 1 stycznia 2021r. znajdziecie nas Państwo pod nowym adresem:

Linc Polska Sp. z o.o.
ul. Czarnowska 22,
60-415 Poznań

Dotychczasowe numery telefonów oraz adresy e-mail pozostają bez zmian. Prosimy o zaktualizowanie danych w swoich bazach informacyjnych oraz kierowanie bieżącej korespondencji pod nowy adres spółki.
Serdecznie wszystkich Państwa zapraszamy do nowej, przyjaznej i przestronniejszej siedziby. Chętnie porozmawiamy przy dobrej kawie. □

Więcej na: www.linc.pl


2020
CONTENT
HUB ONLINE
Warsaw
Security
Summit
KOMPENDIUM WIEDZY O BEZPIECZEŃSTWIE
W CZASACH POST-COVID
a&S
POLSKA
OGLĄDAJ BEZPŁATNIE NA
www.WarsawSecuritySummit.online