



Inwestycje hotelowe

20 zł
(w tym 8% VAT)



Raport z rynku hoteli

Zmienia się sposób, w jaki klienci korzystają z usług hotelowych. Branża stara się nadążyć, potykając się o inflacyjne progi. Czy osiągnie sukces?

Security w hotelarstwie

Goście mają się czuć komfortowo, a fakt, że ktoś dba o ich bezpieczeństwo, ma być niezauważalny. O tym, jak to pogodzić, opowiadają security managerowie.

Czy jesteśmy bezpieczni?

Jeśli chcemy mieć pewność, że poradzi-
my sobie w sytuacji kryzysowej, musimy
wcześniej ją przeciwżyć. Szkolenie to
podstawa bezpieczeństwa.

check. create. manage.



Checly

the best startup 2023

checly.app



Co zaprzęta myśli branży hotelarskiej?

Nie będzie zapewne dla nikogo zaskakujące, jeśli na tytułowe pytanie odpowiemy wprost: pieniądze, a dokładnie inflacja. Wprawdzie przedstawiciele branży chwalą się kolejnymi inwestycjami, to wyzwaniem okazuje się utrzymanie rentowności obiektów w sytuacji sporej gospodarczej niepewności.

Owszem, inwestycji w branży nie brakuje. Mapę najciekawszych publikujemy na str. 68. A jak czytamy w *Raporcie z rynku hoteli* (str. 22) w najbliższych latach planowane jest uruchomienie aż 98 obiektów w samych tylko dużych miastach (Warszawa, Kraków, Poznań, Gdańsk, Wrocław, Łódź), a drugie tyle w miejscowościach turystycznych. Potrzeba rozwoju jest, bo do tej pory spory był też popyt na usługi noclegowe, ale... apetyt na skalowanie biznesu studzi nieco malejąca wartość pieniądza. Zarządcy tradycyjnych hoteli, pensjonatów czy obiektów wczasowych planują i budżetują na wiele miesięcy, o ile nie lat, do przodu. Rosnąca inflacja długoterminowemu planowaniu nie sprzyja. Gdy oddajemy ten numer do druku, NBP podał najnowsze prognozy dotyczące inflacji. Średnioroczna w 2023 r. wyniesie ma 11,9%, by spaść do 5,2% w roku przyszłym. Niestety, ekonomiści banku centralnego nie wykluczają, że jeszcze w tym roku będzie na poziomie ok. 14%.

Co to oznacza dla branży security? Ni mniej, ni więcej konieczność przygotowania się na fakt, że zarządcy nowych obiektów, ewentualnie tylko remontowanych bądź modernizowanych jeszcze uważniej będą oglądać każdą złotówkę, nim ją wydadzą. Gdzie w takim razie szukać kontraktów? Nie ma wątpliwości, że najłatwiej prowadzi się rozmowy w obiektach zarządzanych przez firmy rodzinne. W artykule *Rodziny hotel – bezpieczny i dyskretny* piszemy wprost, że próba wejścia do hoteli międzynarodowych działających globalnie sieci może nie tyle jest z góry skazana na porażkę dla polskich firm z branży security, co jednak obciążona dużym ryzykiem niepowodzenia. Lepszym rozwiązaniem jest postawienie na współpracę z rodzimym biznesem. Niezależnie jednak od tego, czy mowa o przytulnym pensjonacie, czy o obiekcie przeznaczonym dla kilkuset osób, najważniejsze jest bezpieczeństwo gości. Potwierdzają to słowa security managerów, cytowanych w artykule *Security w hotelarstwie* (str. 38). I choć każda z pytanych przez nas osób mówiła o różnego rodzaju praktykach i procedurach, jakie stosują, by ich obiekty były bezpieczne, to ich praca ma wspólny mianownik: miarą sukcesu nie jest niewielka liczba zdarzeń, ale to, jak wielu z nich udaje się zapobiec. W podobnym tonie wypowiadają się eksperci z branży security (*Głos branży*, str. 44).

Dla branży hotelarskiej czerwiec to początek sezonu, czas bardzo intensywny. Dokładnie taki sam był dla naszej redakcji. Za nami bowiem pierwszy w tym roku Security BootCamp, utrzymany w klimacie PRL (fotorelacja na str. 88) oraz już siódme spotkanie w ramach Warsaw Security Summit (więcej na temat na str. 14). Tym naszym Czytelnikom, którzy w konferencji nie mogli wziąć udziału, polecamy wideorelację umieszczoną na stronie aspolska.pl. Podobnie, jak lekturę tego, już 40. wydania czasopisma „a&s Polska”.

Redakcja

ZŁOTY PARTNER A&S POLSKA



SREBRNY PARTNER A&S POLSKA



SPIS TREŚCI



Inwestycje hotelowe

PRODUKTY NUMERU

- 8 Najnowsze rozwiązania firm: Axis Communications, BCS, Hikvision, Linc Polska, Nedap Security Management, Schrack Seconet Polska, TP-Link, W2, ZKTeco

WYDARZENIA

- 14 Warsaw Security Summit za nami

BEZPIECZNE HOTELE

- 22 Raport z rynku hoteli
Adela Prochyra
- 30 Rodzinny hotel – dyskretny i bezpieczny
Jacek Tyburek
- 34 Rozważania o bezpieczeństwie
Hubert Zak
- 38 Security w hotelarstwie
Adela Prochyra
- 44 Głos branży
- 50 Monitoring wizyjny kluczem do utrzymania konkurencyjności
Krzysztof Mika, Hikvision Poland
- 52 Bezprzewodowy system zarządzania zamkami hotelowymi ZKTeco
ZKTeco Europe
- 54 Kompletna infrastruktura sieciowa w hotelu
TP-link
- 56 Systemy do bezobsługowych obiektów hotelowych
Global Security Partner
- 58 Współczesne hotele: pełen komfort i dyskretna ochrona
Jan T. Grusznic
- 64 Rozwiązania polecane dla sektora hotelowego
Materiały partnerów

REDAKCJA

ADRES REDAKCJI

a&s Polska
ul. M. Rodziewiczówny 1 lok. 801
04-187 Warszawa
info@aspolska.pl
www.aspolska.pl

PREZES ZARZĄDU

Mariusz Kucharski

REDAKTOR NACZELNA

Marta Dynakowska

Z-CA RED. NACZELNEGO

Jan T. Grusznic

REDAKCJA

Monika Żuber-Mamakis
Adela Prochyra

DZIAŁ REKLAMY

Iwona Krawiec

DZIAŁ PROJEKTÓW SPECJALNYCH

Jolanta A. Kucharska
Aleksandra Czapska
Michalina Nowak

CENTRUM KOMPETENCJI

Jacek Grzechowiak

KOREKTA

Jolanta Kucharska

PROJEKT GRAFICZNY I SKŁAD

Bogusław Kálwala

WYDAWCA

SENS Group Sp. z o.o.
ul. Rondo ONZ 1
00-124 Warszawa
www.sensgroup.pl

Redakcja zastrzega sobie prawo skracania i redagowania nadesłanych tekstów. Tytuły i śródtytuły pochodzą od Redakcji. Opinie autorów nie muszą być tożsame z poglądami Redakcji. Za treść reklam i artykułów partnerów Redakcja nie odpowiada. Przedruki tekstów bez zgody Wydawcy są niedozwolone.

© Copyright by a&s Polska



REJESTRATORY 4K

- REJESTRATORY BCS LINE 4K I 8K
- OBSŁUGA KAMER IP DO 32MPX
- PASMO PRZYCHODZĄCE DO 1024MBPS
- ANALIZA WIDEO Z POZIOMU REJESTRATORA



www.bcs.pl
www.facebook.com/bcspl

» Więcej przeczytasz na stronie 8



SPIS TREŚCI

RYNEK SECURITY

- 68 Mapa inwestycji
opr. Adela Prochyra
- 70 Wraz ze świadomością rośnie i zmienia się rynek
Wywiad z Tomaszem Grzelakiem
- 72 Access AtWork® – usługa kontroli dostępu w chmurze
Nedap Security Management
- 74 Kody QR uzupełnieniem systemów kontroli dostępu
Axis Communications
- 76 EchoPoint OPTEX – technologia światłowodowa
z zasięgiem do 100 km
Optex

CYBERBEZPIECZEŃSTWO

- 77 Cyberataki wymierzone w pracowników
Fortinet

SYGNALIZACJA POŻAROWA

- 78 Bezpieczna ewakuacja
Rafał Kował, Schrack Seconet Polska

BEZPIECZEŃSTWO BIZNESU

- 82 Udajemy, że jesteśmy bezpieczni
Wywiad z płk. Krzysztofem Przepiórką

SERWIS INFORMACYJNY

- 85 Nowości produktowe/informacje firmowe
- 88 Security BootCamp 2023 w klimacie PRL
- 92 Centrum Kompetencji: Gdzie się podziało nasze ptasie
mleczko?
Monika Żuber-Mamak

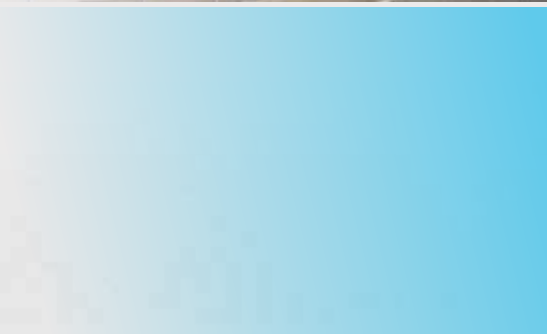


RACS 5 v2 Polska platforma kontroli dostępu, bezpieczeństwa i automatyki klasy *Enterprise*

roger

Intelligence for Building

- Obsługa systemów rozproszonych terytorialnie
- Integracja z systemami SSP, SSWiN, CCTV
- Zarządzanie systemami bezpieczeństwa w module VISO SMS
- Integracje z platformami BMS, VMS, SMS, PSIM i aplikacjami do zarządzania biurowcem
- Integracja z usługą Active Directory
- Integracja z serwerowymi systemami windowymi firm KONE, Schindler i innych





AXIS COMMUNICATIONS

Pierwsza na świecie kamera przeciwwybuchowa do stosowania w ekstremalnych warunkach Division 2

Kamera AXIS P1468-XLE wykorzystuje metodę ochrony „Ex e”, czyli podejście do ochrony przeciwwybuchowej określane jako „zwiększone bezpieczeństwo” lub „niewybuchowość”.

Metoda ta zapewnia, że łuki elektryczne i iskry nie mogą wystąpić, a nadmierne przegrzanie nie pojawia się podczas normalnej pracy urządzeń elektrycznych. W rezultacie urządzenia elektryczne z ochroną „Ex e” nie powodują zapalenia się gazu lub pyłu w otaczającym je potencjalnie wysoce łatwopalnym środowisku.

AXIS P1468-XLE wyposażono w najnowszy system on chip – ARTPEC-8. Dzięki modułowi

przetwarzania danych z funkcją głębokiego uczenia, kamera może analizować, przechowywać i przetwarzać jeszcze większe niż poprzednio ilości danych. AXIS Object Analytics pozwala na obserwację parkingu, przeprowadzenie kontroli prędkości, sprawdzenie poprawności parkowania według typów pojazdów oraz – w połączeniu z głośnikiem sieciowym Axis – zbieranie informacji audio, a także emitowanie zaprogramowanego



ostrzeżenia. Kamera została wyposażona także w OptimizedIR, co umożliwia dozór w całkowitej ciemności aż do 40 m.

Ta wielofunkcyjna kamera oferuje liczne korzyści w obszarach dbania o zdrowie i bezpieczeństwo oraz podnoszenia efektywności operacyjnej. Może służyć do monitorowania i dostosowywania procesów w czasie rzeczywistym z myślą o maksymalizacji wydajności. Ponadto ekstrakcja oraz wysyłanie danych przyda się w monitorowaniu trendów i konserwacji predykcyjnej.

Więcej na: www.axis.com/pl-pl



HIKVISION

Inteligentne switche zarządzalne Hikvision

Inteligentne switche zarządzalne Hikvision pomagają realizować centralne zarządzanie wszystkimi urządzeniami sieciowymi.



Wyróżniają się doskonałą integracją z oprogramowaniem Hikvision, zapewniając kompleksowe możliwości obsługi i konserwacji w oparciu o ujednoczoną topologię.

Topologia systemu, status stanu sieci i urządzeń oraz powiadomienia o alarmach mogą być wyświetlane i zarządzane w sposób wizualny, przyczyniając się do inteligentnego zarządzania i zwiększonej wydajności operacyjnej.

Powiadomienie o alarmie w czasie rzeczywistym będzie wyświetlane wizualnie z zaznaczeniem miejsca zdarzenia. W przypadku awarii sieci lub urządzenia przyczyni się to do szybszej naprawy i konserwacji.

Nieodłączną korzyścią jest możliwość podłączenia aplikacji Hik-Connect oraz Hik-PartnerPro, dzięki którym można w prosty sposób przejrzeć statystyki oraz stan switcha, a także zarządzać jego ustawieniami. Aplikacja umożliwia łatwe sterowanie urządzeniami systemu dozoru, podgląd na żywo oraz powiadomienia o alarmach w czasie rzeczywistym.

Więcej na: www.hikvision.com/pl

BCS

Nowa rodzina rejestratorów BCS Line

W szerokiej gamie produktów BCS Line pojawiły się nowe rejestratory sieciowe – modele L-NVR-4K i L-NVR-8K-Ai. Pierwszy z nich jest dostępny w wersjach 8-, 16-, 32- i 64-kanalowych z możliwością montażu 2, 4 lub 8 dysków twardych o pojemności do 16 TB każdy. Wśród rejestratorów L-NVR-8K-Ai są modele 32-, 64- lub 128-kanalowe, ale tylko w wersji 8 dyskowej.

Podstawową różnicą w porównaniu do modeli dotychczas dostępnych jest obsługa kamer o zdecydowanie wyższej rozdzielczości. Poprzednie współpracowały z kamerami o maksymalnej rozdzielczości 12 Mpix, nowe modele nie będą miały problemu z kamerami o rozdzielczości nawet 32 Mpix.

Kolejną wartą odnotowania zmianą jest poprawa przepływności danych w obu typach rejestratorów. O ile w rejestratorach L-NVR-4K wynosi od 320 Mb/s do 384 Mb/s, o tyle w rejestratorach L-NVR-8K-Ai pasmo przychodzące na poziomie 1024 Mb/s zdecydowanie już robi wrażenie.

Rejestratory L-NVR-8K-Ai są wyposażone w moduł sztucznej inteligencji pozwalający na uruchomienie funkcji zaawansowanej analizy wideo bez względu na to, czy podłączona do niego kamera jest kompatybilna z protokołem Onvif. Rejestrator może realizować funkcje inteligentnej detekcji ruchu (SMD), rozpoznawania twarzy, ochrony perymetrycznej czy gromadzenia metadanych. W połączeniu z kamerami BCS Line oferuje również wsparcie dla zliczania osób czy funkcji rozpoznawania tablic rejestracyjnych (ANPR). Również rejestratory L-NVR-4K są w taki moduł wyposażone, a różnica dotyczy liczby kanałów, na których analiza z poziomu rejestratora może zostać uruchomiona.



Więcej na: www.bcs.pl



ALNET
SYSTEMS

Polskie profesjonalne
zintegrowane rozwiązania
VMS

Ponad 200 000 instalacji
na całym świecie

Jesteśmy z Wami od
2003 roku



www.alnetsystems.com



LINC POLSKA

Wideoanalityka Camect – wygoda i bezpieczeństwo w innowacyjnym wydaniu

Camect Smart Hub to małe urządzenie o wielkich możliwościach. Z jednej strony oferuje maksymalną wygodę użytkownikowi, dostarczając alarmy na czas w przystępnej formie powiadomień w aplikacji lub/i w formie maila.

Połączenie chmurowe umożliwia szybki przegląd zdarzeń z 24 godzin w 60 sekund, a dzięki monitorowaniu sieci urządzenia można uzbroić całkowicie automatycznie, bez interakcji użytkownika.

Z drugiej zaś strony rozwiązanie to oferuje ciągłe nagrywanie lokalne, analizę wideo AI na urządzeniu, bezpośrednie połączenie ze stacją monitorowania i pełną prywatność danych użytkownika. Konfiguracja urządzenia nie zajmuje więcej niż 5 minut, po których można mieć pełny dostęp do systemu. Dzięki harmonogramom i strefom definiuje się tylko wybrane rejony.

Gdy dodamy do tego wykrywanie i różnicowanie ponad 30 różnych obiektów, takich jak ludzie, pojazdy czy zwierzęta z poprawnością detekcji wynoszącą 99,67%, uzyskujemy niespotykane dotąd możliwości. Nie



jest to zwykły rejestrator wideo, a hybryda łącząca zalety chmury, analizy AI, sieci neuronowych i błyskawicznych alertów w niewielkim urządzeniu.

Jest to po prostu Camect Smart Hub, którego warto przetestować!

Więcej na: www.linc.pl

NEDAP SECURITY MANAGEMENT

Access AtWork®. Kontrola dostępu w modelu chmurowym



Nedap Security Management wprowadził na rynek nowe rozwiązanie Access AtWork® – systemu kontroli dostępu nowej generacji.

- **Access AtWork® rewolucjonizuje tradycyjnie skomplikowany proces zarządzania kontrolą dostępu**, czyniąc go prostym, intuicyjnym i wydajnym. Koniec ze zmaganiem się z listwami drzwi i szablonami.
- **Access AtWork® to natywne rozwiązanie chmurowe**, oferujące zdalny dostęp, regularne aktualizacje i upgrade'y.
- **Access AtWork® to system zgodny z rygorystycznymi protokołami i standardami bezpieczeństwa.**
- **Access AtWork® działa na naszych sprawdzonych kontrolerach AEOS Blue** i płynnie integruje się z istniejącymi czytnikami, dzięki temu migracja na nasz system jest prostsza niż kiedykolwiek.
- **Access AtWork® to kontrola dostępu jako usługa (ACaaS) oferująca niższe koszty początkowe**, przewidywalne regularne opłaty, automatyczne aktualizacje i mniejsze obciążenia związane z konserwacją.

Rozwiązania kontroli dostępu Nedap są stosowane przez ponad 25% czołowych europejskich marek. Niezależnie od tego, czy chodzi o wysokie wymagania w zakresie bezpieczeństwa infrastruktury krytycznej, czy też o bezproblemową i łatwą w zarządzaniu kontrolę dostępu dla organizacji, dzięki 46-letniemu doświadczeniu mamy wszystko pod kontrolą.

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

SCHRACK SECONET POLSKA

SIS-POWER – wielofunkcyjna centrala sterująco-zasilająca urządzenia ppoż.

Centrala SIS-POWER wraz z zasilaczem urządzeń ppoż. S-POWER jest przeznaczona do sterowania i zasilania napięciem niskim i bardzo niskim (maks. 1000 VAC, 1500 VDC) urządzeń wchodzących w skład systemów kontroli rozprzestrzeniania dymu i ciepła, SUG wodnych i innych urządzeń ppoż. Dzięki układom SZR (samoczynne załączenie rezerwy) CSZUP SIS-POWER lub S-POWER można też stosować jako główne rozdzielnice pożarowe budynku.

SIS-POWER jest dostępna w różnych wersjach, zależnie od zastosowanego modułu kontrolno-sterującego S-CONTROL.

SIS-POWER/S-POWER może współpracować (protokół cyfrowy) z systemem sygnalizacji pożarowej i sterowania urządzeniami ppoż. Integral EvoxX oraz systemem integrującym urządzenia ppoż. SIS-FIRE.

Pozwala to zbudować kompleksowy, w pełni zintegrowany system bezpieczeństwa pożarowego (detekcja, sterowanie, zasilanie i zarządzanie urządzeniami ppoż. i innymi urządzeniami technicznymi obiektu).

SIS-POWER, zgodnie z dokumentami certyfikacyjnymi CNBOP-PIB, umożliwia sterowanie

i kontrolę urządzeń oddymiania mechanicznego (kanatowego i bezkanatowego) i grawitacyjnego (ze stałym/zmiennym nawiewem kompensacyjnym), systemami oczyszczania z dymu, a także zasilanie komponentów systemu różnicowania ciśnień (wentylatory pożarowe, kłapy ppoż. i dymowe, okna oddymiające, drzwi kompensacyjne, przepustnice powietrza kompensacyjnego, bramy, kurtyny dymowe, wyrzutnie dymu, elektromechaniczne i elektromagnetyczne urządzenia ryglujące).





CAMECT SMART HUB

NOWY WYMIAR **BEZPIECZEŃSTWA**
WYŻSZY **KOMFORT UŻYTKOWANIA**

Niezasadnione alarmy generują zbyt duże koszty?

Wyobraź sobie system, który eliminuje **fałszywe zgłoszenia**, bo rozróżnia **ludzi, owady i deszcz**.

Taki właśnie jest Camect Smart Hub - **rejestrator z Analizą AI** do wykrywania **intruzów** w oparciu o sieci neuronowe.

- **Szybka instalacja** - tylko 5 minut na uruchomienie systemu
- Wygodna **aplikacja mobilna** i natychmiastowe powiadomienia
- **Skuteczność filtrowania** niezasadnionych alarmów do **99,67%**
- Obsługa stacji monitorowania Safestar i innych po DC09 (SIA)





TP-Link

TP-Link VIGI NVR4032H 32-kanalowy sieciowy rejestrator wideo

W ofercie TP-Link pojawił się nowy rejestrator VIGI NVR4032H, do którego można podłączyć do 32 kamery. Urządzenie idealnie sprawdzi się w systemie monitoringu wizyjnego w dużych instalacjach firmowych.

VIGI NVR4032H umożliwia przechowywanie materiału wizyjnego z kamer na dyskach SATA. Można zamontować nawet 4 dyski o pojemności do 10 TB każdy, co gwarantuje bezpieczeństwo lokalnego przechowywania danych. Wbudowane wyjście HDMI wspiera rozdzielczość 4K oraz VGA.

Rejestrator może dekodować do 16 strumieni wizyjnych o rozdzielczości 2 Mpix każdy. Wysoka przepustowość zapewnia zarządzanie maks. 32 kamerami HD. Wbudowany głośnik pozwoli odsłuchiwać także dźwięk z nagrań. Dwa gigabitowe porty Ethernet zapewniają większą stabilność sieci i nieprzerwaną pracę urządzenia. Standard kompresji H.265+ ogranicza nadmierne wykorzystanie przepustowości sieci i zapewnia optymalne wykorzystanie przestrzeni dyskowej.

VIGI NVR4032H działa w trybie plug&play – automatycznie wykrywa kamery VIGI i je konfiguruje. Rejestrator uzupełnia system monitoringu wizyjnego od TP-Link, w którego skład wchodzi m.in. wewnętrzne kamery typu turret (np. VIGI C440) oraz zewnętrzne typu bullet (np. VIGI C340). Jest także w pełni zgodny ze standardem ONVIF, dzięki czemu współpracuje z kamerami różnych producentów. VIGI NVR4032H pozwala na monitorowanie zdalne P2P, dzięki czemu TP-Link ID i mobilnej aplikacji VIGI dostępnej na urządzenia mobilne z systemami iOS i Android. Rejestrator VIGI objęty jest 36-miesięczną gwarancją producenta.

Więcej na: www.tp-link.com/pl



w2

Nowa seria sygnalizatorów pożarowych P8

W ofercie W2 pojawiła się nowa seria sygnalizatorów pożarowych P8, w której skład wchodzi urządzenia typu SA-P8, SO-P8, SAO-P8. Sygnalizatory te zastępują znane od lat wyroby SA-K5N, SO-Pd13, SA-K7N.

Seria P8 to zupełnie nowy projekt usprawniający dotychczas wykorzystywane rozwiązania z zastosowaniem pewnych innowacji. Wśród nich należy wymienić nową bryłę optyczną 12 m (SO-P8, SAO-P8), która pozwala uzyskać nawet do 70% większy promień obszaru pokrycia. Bardzo przydatne są również opcja wyboru bryły optycznej (SO-P8, SAO-P8) w obrębie jednego urządzenia czy możliwość wyboru częstotliwości błysku (SO-P8). Ponadto cała seria P8 została wyposażona w ogranicznik prądu rozruchowego, synchronizację za pomocą dodatkowej żyły oraz solidną obudowę o wytrzymałości mechanicznej IK07.

Seria P8 to również mnogość dostępnych modeli. Sygnalizatory występują w obudowie białej lub czerwonej. Oprócz tego sygnalizatory z członem optycznym (SO-P8, SAO-P8) występują w odmianach generujących światło czerwone, białe lub czerwone i białe naprzemiennie. Klosz członu optycznego jest matowy, co poprawia ogólny wygląd oraz estetykę.

Sygnalizator SO-P8 jest certyfikowany jako zewnętrzny (może pracować w temperaturach -25...70°C, ma klasę ochrony IP54). Seria P8 jest objęta aktualnymi dokumentami CNBOP-PIB, tj. Certyfikatami Stałości Właściwości Użytkowych (obowiązują dla wszystkich odmian) oraz Świadectwami Dopuszczenia (obowiązują dla odmian SA-P8/C, SA-P8/B, SO-P8/CC, SAO-P8/CC).

Więcej na: www.w2.com.pl



ZKTeco

Inteligentne zamki ML200 i ML300 firmy ZKTeco

Zamki do drzwi ML200 i ML300 to wyjątkowe połączenie techniki kontroli dostępu z wysoką funkcjonalnością.



Oba zamki wyposażono w podświetlaną klawiaturę numeryczną, a zamek ML300 w czytnik linii papilarnych.

Instalacja zamka jest bardzo łatwa i nie wymaga wiercenia otworów. Wystarczy zastąpić nim klamkę z pojedynczym otworem. Zamki pasują do drzwi lewych i prawych. Dzięki dwustronnej konstrukcji są chronione przed ich demontażem przez nieupoważnione osoby. Ze względu na wodoodporność zamek ML200 można montować w drzwiach zewnętrznych.

Konfiguracja zamka zajmuje zaledwie kilka minut. Oba można otworzyć za pomocą kodu, a ML300 przez zeskanowanie linii papilarnych. Połączona z zamkiem bezprzewodowo bramka Bluetooth umożliwia odblokowanie go za pomocą komputera lub smartfonu z dowolnego miejsca.

Za pośrednictwem aplikacji można udostępnić użytkownikowi tymczasowe kody do otwarcia drzwi, sprawdzić historię logowań, zarządzać użytkownikami czy otrzymywać na bieżąco komunikaty, w tym o rozładowanej baterii czy nielegalnych próbach sforsowania drzwi.

Zamek można też uruchomić za pomocą poleceń głosowych, po zsynchronizowaniu go z urządzeniem Amazon Alexa lub Asystentem Google. W ten sposób można jednocześnie obsługiwać do 128 zamków, łącząc je w sieć.

Komunikacja z zamkami jest bezpieczna dzięki 128-bitowemu szyfrowaniu. Zamki ML200 i ML300 polecane są do prywatnych domów, apartamentów i mają szerokie zastosowanie w wynajmie krótkoterminowym lokali.

Więcej na: <https://zkteco.eu/>



dobrze zaprojektowane BEZPIECZEŃSTWO

KOMPLEKSOWE SYSTEMY SYGNALIZACJI POŻAROWEJ

- PRODUKCJA • SERWIS • SZKOLENIA
- WSPARCIE TECHNICZNE I PROJEKTOWE

AUTOMATYKA POŻAROWA



WARSAW SECURITY SUMMIT

Konferencję otworzył
Krzysztof Ibisz.

O tym, czy naprawdę jest się
czego bać, mówił dr Maciej
Kawecki, prezes Instytutu Lema,
prorektor ds. innowacji Wyższej
Szkoły Bankowej w Warszawie,

Wystąpienia, które pokazały szerokie spojrzenie na kwestie bezpieczeństwa. Prelekcje, dzięki którym zrozumienie technologicznych wyzwań stojących nie tylko przed branżą, ale także przed ludzkością – stało się proste, jak nigdy dotąd – taka była 7. edycja Warsaw Security Summit. Konferencja przyciągnęła jak zawsze rzesze zainteresowanych, dla których w tym roku przygotowaliśmy wraz z partnerami nieco inną formułę i zupełnie inne miejsce.





Gości powitał Mariusz Kucharski, prezes a&s Polska.

Warsaw Security Summit za nami

Konferencję otworzył Krzysztof Ibis – jak sam o sobie powiedział – najmłodszy prezynter w Polsce. Następnie licznie zgromadzonych w hotelowej auli gości powitał prezes a&s Polska Mariusz Kucharski. Choć spotkanie nie było stricte branżowe, jako że uczestniczyli w nim przede wszystkim security managerowie, specjaliści do spraw bezpieczeństwa, instalatorzy, projektanci, nie obyło się bez poruszenia tematu numer jeden chyba w każdej branży, czyli sztucznej inteligencji. Prezynter, zapowiadając wystąpienie pierwszego gościa, powołał się na badania IBRIS dla Radia Zet, według których 9,2% zdecydowanie upatruje w niej szansę dla ludzkości, 36% raczej szansę, a aż 27,7% respondentów uważa ją raczej za zagrożenie.

O tym, czy naprawdę jest się czego bać, mówił dr Maciej Kawecki, prezes Instytutu Lema, prorektor ds. innowacji Wyższej Szkoły Bankowej w Warszawie, który wystąpił jako pierwszy prelegent. W swoim wystąpieniu odniósł się do popularnej tezy, jakoby AI miała wkrótce zastąpić ludzi i zreplikować mózg człowieka. „*To mit, clickbait, bo do dziś nie wiemy, jak działa ludzki mózg, więc tym bardziej nie jesteśmy w stanie napisać formuły matematycznej, która go zastąpi*” – stwierdził. Co nie znaczy, że nie jesteśmy w momencie przełomowym. Stworzyliśmy nowy byt, który ma własny wewnętrzny świat, nie do końca dla nas zrozumiały. Sztynny podział na rzeczywistość fizyczną i wirtualną przestał obowiązywać. Możemy już mówić o rzeczywistości mieszanej.

Z dobrych wiadomości – o ile Polska nie ma cennych złóż, tak jak kraje Bliskiego Wschodu, architektury, jak Włochy, ani potencjału turystycznego Grecji, o tyle kapitał programistyczny mamy wielki. Maciej Kawecki użył względem Polski określenia „potentat”.

Na rynkach międzynarodowych wygrywamy dobrą edukacją informatyczną, wysoko ocenianą w badaniach edukacyjnych PISA, dobrą znajomością języka angielskiego i dobrym przygotowaniem polskich pracowników. Powstają u nas wysoko zaawansowane technologie medyczne, np. algorytm diagnozujący raka piersi czy kapsułka endoskopowa stworzona przez wrocławski start-up BioCam. Wojciech Paprota, CEO start-upu Walletmor, stworzył pierwszy na świecie implant zbliżeniowy. Polska jest też liderem medycyny predykcyjnej, która daje nadzieję na odciążenie służby zdrowia. Sukces OpenAI, czyli producenta Chatu GPT, również zawiera duży polski komponent. Jednym ze współzałożycieli spółki jest Wojciech Zaremba z Kluczborka. To on optował za stworzeniem symulacji dialogu, dzięki czemu powstało coś, co odpowiadało na potrzeby człowieka. Maciej Kawecki przekonywał, że rozwój AI nie przebiega wbrew woli człowieka, ale jest zgodny z tym, czego chcemy i potrzebujemy.

Na obecnym etapie nie da się zatrzymać rozwoju sztucznej inteligencji ani jej kontrolować. Problem polega na tym, że nie wiemy, jak działa element losowy. My kierujemy podpowiedź, która jest rozkładana na czynniki pierwsze, czyli słowa. Algorytm losowo wychwytuje powtarzalności w ogromnym zasobie danych i z nich tworzy rozwiązanie. Jest to algorytm preuczony, czyli napełniony do pewnego momentu dawką wiedzy. Teraz jego źródłem są użytkownicy. O ile rozumiemy same algorytmy, o tyle nie pojmujemy mechanizmu predykcyjnego. Dominująca obecnie teoria dotycząca AI to teoria ciemieniowo-skroniowa, czyli podkreślająca funkcję części mózgu odpowiadającą za kontrolę, którą staramy się odzwierciedlić w algorytmach. Najbardziej realne zagrożenie to instrumentalne wykorzystanie AI do manipulacji politycznych.

Po dyskusji, która rozgorzała po wystąpieniu Macieja Kaweciego, pałeczkę przejął pułkownik Andrzej Kruczyński, były oficer GROM, wieloletni szef bezpieczeństwa Stadionu Narodowego w Warszawie z wystąpieniem „Co nowego w bezpieczeństwie? Trendy na 2023”. Dzięki wyjątkowemu i bogatemu doświadczeniu przemowę zilustrował trafiającymi do wyobraźni przykładami. Większość z nich dotyczyła okresu pracy pułkownika przy otwarciu Stadionu Narodowego (obecnie PGE Narodowy). Obiekt tej klasy powinien być zabezpieczony szczególnie starannie i to już na etapie rozpoczęcia budowy, praktyka jednak pokazuje, że często o bezpieczeństwie myśli się dopiero na ostatnim etapie realizacji. Dlatego jeszcze przed otwarciem bram stadionu zgłosił się do organizatorów i zaproponował swoje usługi w zakresie zorganizowania całego systemu bezpieczeństwa. „Procedury trzeba stworzyć odpowiednio wcześniej i je przetestować” – podkreślał wielokrotnie. Najgorszy scenariusz to ten, kiedy dochodzi do paniki, ponieważ nad rozhisteryzowanym tłumem nie sposób zapanować. Tymczasem wiele sytuacji można przewidzieć i tu prelegent upatruje najważniejsze zadanie bezpieczeństwa. Terrorysty mogą wziąć za cel zarówno infrastrukturę, jak i cele miękkie. O ile budynki można zabezpieczyć, dziś zwłaszcza mamy do dyspozycji wysoko zaawansowane technologie, o tyle ochrona ludzi wymaga przećwiczenia dziesiątków wariantów, i tu także największą sztuką jest przewidywanie. Jak głosi propagowana przez pułkownika A. Kruczyńskiego Procedura 4U – uważaj, uciekaj, ukryj się, udaremnij atak.

Profilaktyka i przewidywanie były hasłami przewodnimi wystąpienia Jacka Grzechowiaka, dyrektora Centrum Kompetencji AS, menedżera zarządzania ryzykiem i bezpieczeństwem, „Nic tak nie

daje do myślenia jak przykład”. Na dziesiątkach przykładów z życia wziętych pokazał nieraz rażące błędy i niedociągnięcia współczesnej branży security. Jako audytor bezpieczeństwa wielokrotnie obserwował firmy ochroniarskie w działaniu czy raczej jego braku. Wśród przytoczonych przykładów nieprawidłowości znalazły się takie zdumiewające przypadki jak pracownicy ochrony pełniący dyżur w kłapkach, klucze czy karty master zamknięte na atrapy plomb i wcale nie tak rzadko spotykany wymóg posiadania orzeczenia o niepełnosprawności w rekrutacji na stanowisko pracownika ochrony.

Przytoczył też przykład konferencji, która odbyła się w Akademii Koźmińskiego w 2015 r. Grupa studentek zaprezentowała wówczas wyniki audytu, który polegał na tym, że z kilkunastu obiektów zebrały plany ochrony. Łatwość dostępności planów bezpieczeństwa poszczególnych miast poruszał kolejny prelegent.

Kamil Barański z Megavision Technology zaprezentował film na temat produktu Venom – rozwiązania klasy PSIM. Praca nad nim trwała 12 lat. Ogranicza on ryzyko błędu człowieka, a najczęstsze zastosowanie to obiekty infrastruktury krytycznej i przemysłowe.

Następnie Jarosław Stelmach, ekspert ds. antyterrorystycznego i bezpieczeństwa obiektów użyteczności publicznej Safety Project, przybliżył założenia dyrektywy CER, która ma wejść w życie w ciągu najbliższego roku, dwóch lat. Podkreślił też zalety Narodowego Programu Ochrony Infrastruktury Krytycznej: zwiększenie faktycznej liczby podmiotów krytycznych oraz ustanowienie minimalnych standardów ochrony. Zazaczył, że ma on też minusy. Wśród dobrych praktyk wymienił zastosowanie podejścia scenariuszowego, prakseologię i weryfikację wprowadzonych rozwiązań. Jako wzory podał NATO, Interpol i Safety Project. →

Pułkownik Andrzej Kruczyński, były oficer GROM, wieloletni szef bezpieczeństwa Stadionu Narodowego w Warszawie, z wystąpieniem „Co nowego w bezpieczeństwie? Trendy na 2023”.



Profilaktyka i przewidywanie były hasłami przewodnimi wystąpienia Jacka Grzechowiaka, dyrektora Centrum Kompetencji A&S, menedżera zarządzania ryzykiem i bezpieczeństwem, „Nic tak nie daje do myślenia jak przykład”.

Jarosław Stelmach, ekspert ds. antyterrorystyki i bezpieczeństwa obiektów użyteczności publicznej Safety Project, przybliżył założenia dyrektywy CER, która wkrótce ma wejść w życie.



Stoisko firmy Genetec



Kamil Barański z Megavision Technology zaprezentował film na temat produktu Venom – rozwiązania klasy PSIM.



Stoisko firmy Hikvision



Stoisko firmy Megavision Technology





Jakub Kozak i Kay Oshe z Genetec przedstawili prezentację pt. „Unifikacja zabezpieczeń w obiektach Infrastruktury Krytycznej”.

DEBATA:
Bezpieczeństwo
w transporcie
i logistyce



Stoisko firmy Roger

Stoisko firmy Assa Abloy



Kamery Hikvision



System kontroli dostępu Roger



Jakie rekomendacje mieli dla branży Jakub Kozak i Kay Oshe z Genetec? Tytuł ich wystąpienia to „Unifikacja zabezpieczeń w obiektach Infrastruktury Krytycznej”. „Technologia może pomóc w zarządzaniu bezpieczeństwem, ale nasi wrogowie używają tej samej technologii. Kto będzie szybszy?” – pytali. Trwa wyścig między agresorem a broniącym się, co oznacza, że nieraz trzeba podejmować decyzje dotyczące nieznannej przyszłości. „Moja rekomendacja: idź z global playerem, bo on ma globalne doświadczenie” – zachęcał Jakub Kozak.

Podstawą wszelkiego bezpieczeństwa jest obecnie bezpieczeństwo cybernetyczne. Dopiero w dalszej kolejności bezpieczeństwo prawne, fizyczne, teleinformatyczne i audyt. Dlatego warto korzystać z rozwiązań otwartych umożliwiających zachowanie elastyczności w kwestii zabezpieczania danych.

Ostatni w tym bloku Thorsten Neuman z TAPA wystąpił za pomocą nagrania „Resilience in Risk” (odporność na ryzyko). Zaczął od tego, że obecnie właściwie nie ma czarnego rynku. Wszystkie informacje są dostępne wszędzie i dla wszystkich! Następnie podkreślił, jak ważne są szkolenia i certyfikacja TAPA na rynku przewoźników europejskich. Bądźcie aktywni!

Panel dyskusyjny kończący główną część Warsaw Security Summit moderowała Viktoria Moroz z DHL Supply Chain. Gośćmi byli: Paweł Kański z Procter&Gamble, Jacek Tyburek z DHL Supply Chain, Daniel Kamiński z Alertcontrol, Krzysztof Łazor z Fides i Norbert Bogucki, konsultant TAPA. Paweł Kański poruszył kwestię nieuczciwych podwykonawców, znikających transportów oraz napaści na kierowców na parkingach. Pewną gwarancję daje certyfikat TAPA u podwykonawcy, gdyż wymusza na nim dotrzymanie procedur bezpieczeństwa. Jacek Tyburek podkreślił, że DHL Supply Chain zdecydowało się na certyfikację TAPA z powodów praktycznych. Klienci i partnerzy biznesowi coraz częściej pytają o ten standard. Ma to więc uzasadnienie biznesowe. TAPA nie jest jedynym systemem certyfikacji w Europie, jest zbiorem najlepszych praktyk tworzonych przez ekspertów. Mamy obecnie do czynienia z sytuacją, gdy już nie tylko drogi sprzęt elektroniczny jest atrakcyjny dla złodziei, ale także artykuły codziennego użytku, w tym spożywcze, wszelkie zabezpieczenia transportów są więc w cenie. Samo monitorowanie pojazdów to standard, jak podkreślił Daniel Kamiński, ale kierowcy muszą także przestrzegać podstawowych procedur bezpieczeństwa. Niedopuszczalne jest np. publikowanie trasy w social mediach. Niektóre firmy zapobiegają tego rodzaju uchybieniom, wymagając od swoich pracowników, aby zdali prywatne telefony przed wyruszeniem w trasę. Przestrzegali także przed tym, że przestępcy mogą wykorzystać słabości pracownika, np. hazard, alkoholizm. Pracodawcy powinni sprawdzać przeszłość pracownika 5 lat wstecz, tym bardziej że mają taki obowiązek. Krzysztof Łazor, przedstawiciel branży ubezpieczeniowej, potwierdził konieczność uszczelniania systemu bezpieczeństwa. Powinny się na niego składać procedury, systemy, a także nakłady. Certyfikat TAPA może być argumentem za obniżeniem rachunku u ubezpieczyciela, ale ostatecznie ryzyko szacowane jest z uwzględnieniem wielu zmiennych. Norbert Bogucki podkreślił tę korzyść z udziału w TAPA, że uzyskanie certyfikatu zapewnia dostęp do ogromnej globalnej bazy firm, które wymagają określonych standardów. W Polsce certyfikatów jest 20. Dla porównania w Holandii – ok. 400.



Stoisko firmy Checly



Andrzej Kruczyński promował swoją książkę.



Był też czas na lekturę czasopisma.



Spotkanie zakończył Mateusz Biliński z Niebezpiecznik.pl, który podczas wystąpienia „Cyberbezpieczeństwo w biznesie – jak ustrzec się przed wyciekiem danych firmowych?” opowiedział o tym, jak zabezpieczyć się przed wyciekiem danych firmowych. Absolutną podstawą jest wybór narzędzi telekomunikacyjnych dla firmy. Niektóre z nich, jak WhatsApp, gromadzą różne dane i udostępniają je wewnątrz korporacji Meta będącej właścicielem np. Facebooka. Inne, np. Signal, zbierają jedynie dane podstawowe – numer telefonu i datę rejestracji. Podobnie należy uważać na otwarte narzędzia, np. do przechowywania dokumentów, jak chociażby docer.pl, gdyż inni użytkownicy za pomocą zwykłego hasła „umowa” wpisanego w okno wyszukiwarki mogą zyskać dostęp do setek poufnych, zdawałoby się, dokumentów.

Kolejny elementarny błąd, na który wskazał prelegent, to dobrowolne udostępnianie wrażliwych danych osobowych w mediach społecznościowych. Posłużył się przykładem fanów jednego z humorystycznych profili, którzy w odpowiedzi na post autorki opublikowali setki prywatnych zrzutów ekranu z zabawnymi tytułami przelewów. Przy okazji „pochwalili się” też imionami, nazwiskami, numerami kont i tym, w jakich bankach trzymają pieniądze. Ślady zostawiamy po sobie zresztą na wiele innych, z pozoru niewinnych sposobów, np. dane geolokalizacyjne za pomocą aplikacji sportowych, rozmów z Siri czy innymi inteligentnymi asystentami osobistymi.

Nie zawsze jednak wyciek danych jest spowodowany tzw. błędem ludzkim. Dane wyciekają też z dużych firm i platform internetowych, z których choć raz korzystał niemal każdy, ale też z aplikacji do kupowania biletów w kinie. „Wektorów ataku jest mnóstwo” – mówił M. Biliński. Od przypadku po wycelowany atak. Może się zdarzyć, że nasza firma padnie ofiarą takiego ataku. Kluczowa jest wtedy prawidłowa reakcja na incydent, czyli to, aby każdy pracownik znał protokół postępowania w takiej sytuacji i by każde zgłoszenie dotyczące bezpieczeństwa traktować poważnie. Zdarzają się bowiem sytuacje, jak wyciek danych z Tauronu, kiedy osoba, która brzmi jakby robiła sobie żarty lub była pod wpływem, mówi prawdę i faktycznie posiada ważne informacje.

Dane wypływają w różny sposób i z różnych przyczyn. Oprócz standardowych sposobów ochrony, wskazanych powyżej, należy sprawdzać wyrywkowo, czy nasze dane nie padły ofiarą hakera – można to zrobić za pomocą strony haveibeenpwned.com. Na niej ustawić alert na konkretny adres e-mail i numer telefonu. Warto także korzystać z dwustopniowego systemu uwierzytelniania haseł. ●

Frekwencja dopisała. Na konferencję zapisało się ponad 700 osób.



PRYWATNOŚĆ POUFNOŚĆ



Mateusz Biliński z Niebezpiecznik.pl podczas wystąpienia „Cyberbezpieczeństwo w biznesie – jak ustrzec się przed wyciekami danych firmowych?”.

Stoisko firm: AB i Seagate



Stoisko firmy STid



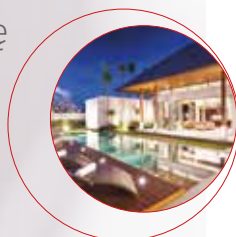
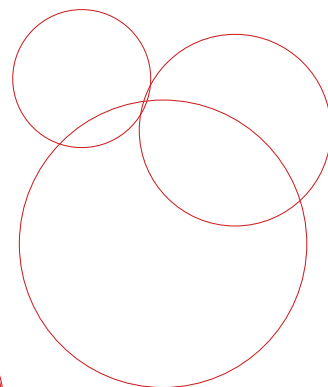
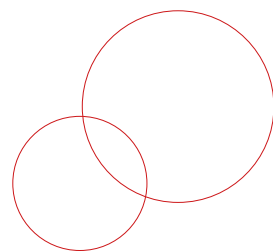
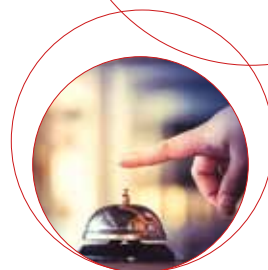
Partnerami wydarzenia były firmy:
AB S.A., ASSA ABLOY, Checkly, DHL Polska,
Genetec Inc., Hikvision, Megavision Technology,
Roger, Seagate, STid oraz TAPA.



Raport z rynku hoteli

Nie bezpieczeństwo, ale inflacja stanowi dziś największe wyzwanie dla branży hotelarskiej. Jej przedstawiciele są powściągliwi w ocenie perspektyw dla rynku, choć nie ukrywają, że jest to rynek bardzo ciekawy. W dużej mierze już korzysta on z najnowocześniejszych rozwiązań technologicznych opartych m.in. na AI. I nie znaczy to wcale, że zamiast recepcjonistów, concierge'ów czy szefów kuchni, w hotelowym lobby powszechnie spotyka się roboty. Sztuczna inteligencja w większości znajduje się bowiem na razie na zapleczu.

Adela Prochyra





Temat wojny w Ukrainie – do niedawna numer jeden wszędzie – rozpatrywany jest w tej branży pod specyficznym kątem. Polska, jako państwo ościennie, jest niezbyt korzystnie postrzegana przez turystów z zagranicy. Wielu potencjalnych gości obawia się bliskiego położenia kraju, w którym toczą się walki, a także, co może dziwić, obecności uchodźców. Co zatem w hotelarstwie dyskutowane jest przede wszystkim? Pieniądze. Gościnności (*hospitality*) dotyczą te same bolączki co inne branże, czyli przede wszystkim inflacja. W dalszej kolejności są to: sztuczna inteligencja, ekologia i system condo.

Jeśli nie wiadomo, o co chodzi, to chodzi o...

W Polsce wciąż otwiera się wiele hoteli. Powstają w miastach chętnie odwiedzanych przez turystów, jak Kraków, Świnoujście czy Karpacz, po miasta uważane za mniej atrakcyjne, jak Radom czy Kielce. W najbliższych latach planowane jest otwarcie 98 obiektów w samych tylko dużych miastach (Warszawa, Kraków, Poznań, Gdańsk, Wrocław, Łódź), a drugie tyle w miejscowościach turystycznych. Hotelarze mówią o niesłabnącym apetycie na rozwój. Podkreślają, że rynek polski jest nadal chłonny i atrakcyjny dla międzynarodowych inwestorów. Zmiany w tym obszarze, które dokonały się w ciągu ostatnich trzech lat, obrazują poniższe liczby.

Hotele w naszym kraju od początku 2023 r. zauważalnie zwiększają liczbę gości, co potwierdza najnowsza comiesięczna ankieta Izby Gospodarczej Hotelarstwa Polskiego dotycząca sytuacji w branży. W trakcie długiego majowego weekendu aż 65% badanych hoteli odnotowało obłożenie przekraczające 50%. Szczególnie imponujące wyniki odnotowano w hotelach wycieczkowych, gdzie aż 91% obiektów było zapelnionych w ponad połowie swojej pojemności.

Jeśli chodzi o Europę, to średnia obłożenia w 2023 r. wynosi 94% wyniku z roku 2019. Wśród dużych miast i stolic Starego Kontynentu Warszawa ma wręcz najlepsze wskaźniki obłożenia w odniesieniu do 2019 r., jak podkreślił podczas swojego wystąpienia na Forum Hotel Investment Trends Poland&CEE w sierpniu 2022 r. Aleksander Robinson, dyrektor, Industry Partner w STR. Wrócił ruch korporacyjny, czyli konferencje i podróże służbowe, znów dozwolone są wyjazdy integracyjne i inne wydarzenia grupowe, a to przede wszystkim na rynku biznesowym i przyjmowaniu gości z zagranicy był oparty rynek warszawski – przed pandemią najmocniejszy w Polsce, po pandemii właśnie z tego powodu długo podnoszący się po zapaści. Podobnie było w Krakowie, choć to miasto częściej odwiedzane jest w celach turystycznych, także przez Polaków. Obłożenie to jednak tylko połowa sukcesu. Równie ważna jest rentowność, z którą jest gorzej.

W roku 2019 hotele warszawskie miały średnioroczne obłożenie na poziomie 73%, średni dzienny dochód z zajmowanego pokoju (*Average Daily Rate*, ADR) wynosił 320 zł, a przychód na jeden dostępny pokój (*Revenue per Available Room*, RevPAR) – 265 zł. Dwa lata później obłożenie wynosiło niecałe 37%, co przełożyło się na obniżenie średniego ADR do 265 zł, w związku z czym RevPAR spadł do 97 zł. To właśnie ten wskaźnik, mimo jego niedoskonałości (nie uwzględnia informacji o kosztach uzyskania przychodu!), dobrze obrazuje faktyczne spadki rentowności hoteli. Obłożenie w większości z nich jest na powrót wysokie, ale przychody właściwie wszędzie spadły dwu-, a nawet niemal trzykrotnie (por. RevPAR krakowski: 238,70 zł w 2019 r. i 81,70 zł w 2021).

Powód jest prozaiczny, co nie dziwi przy wysokiej inflacji. Znacznie zwiększyły się ceny gazu, energii elektrycznej, żywności, materiałów budowlanych itp., w wyniku czego wzrosła wysokość stawki hotelowej. W całej Europie w kwietniu br. średnio były one wyższe o 23% w porównaniu z 2019 r.

Wybuch wojny był kolejną zmienną, która na moment zachwiała rynkiem. Szacuje się, że od 24 lutego 2022 r. do Polski wjechało 2,5 mln Ukraińców. Część z nich zatrzymała się w hotelach i płaciła ceny „z lady”, czyli bez rezerwacji, stąd stosunkowo niezłe wyniki. Trudno jednak było opierać na tym jakiekolwiek przewidywania. Inna zmienna, która „zaburzyła” statystyki, to bon turystyczny, który obowiązywał od 1 sierpnia 2020 do 31 marca 2023 r. Najwięcej zarobili na nim przedsiębiorcy z Małopolski (łącznie 647 mln zł), a przede wszystkim Zakopane, gdzie z bonów wpłynęło 262 mln zł. Rekordzistą krajowym był park rozrywki Energylandia w Zatorze (116 mln zł).

Rynek hotelarski dotykają te same bolączki co inne branże, czyli przede wszystkim inflacja. W dalszej kolejności są to: sztuczna inteligencja, ekologia i system condo.

Hoteli przybywa jak grzybów po deszczu

Potrzeba noclegu w innym mieście czy chęć wycieczki i rozrywki nie znikają mimo wielu (niekorzystnych) zmian globalnych. Widać to na przykładzie Trójmiasta, które okazało się poniekąd odporne na pandemię, wojnę i inne trendy. Dzięki nadmorskiemu położeniu był to jeden z najlepszych rynków w pandemii w całej Europie (44% obłożenia), a i po pandemii nie odstraszały chętnych ani wysokie ceny (średnio 466 zł – dane za sierpień 2022 r.), ani tłumy przyjezdnych (85% obłożenia – dane jw.). Także wskaźnik RevPAR kształtował się w 2023 r. znakomicie (400 zł) i był wyższy niż w sierpniu przed pandemią (380 zł).

„Podróże to siła nie do powstrzymania” – mówił podczas Hotel Investment Trends Poland&CEE 2023 Michael Collini, wiceprezes ds. rozwoju sieci Hilton. Potwierdził to Christian Michel, wiceprezes ds. rozwoju na Europę z Wyndham: „Polska oraz cała

LICZBA OBIEKTÓW HOTELOWYCH W POLSCE

Liczba miejsc noclegowych
obiektów hotelarskich ogółem:

280 671

Liczba obiektów
hotelarskich ogółem:

3427



Liczba obiektów hotelarskich z podziałem na rodzaj:



hotel

2826



282

pensjonat



119

kemping



81

motel



55

schronisko
młodzieżowe



49

schronisko



15

dom
wycieczkowy



LICZBA HOTELI WEDŁUG KATEGORII

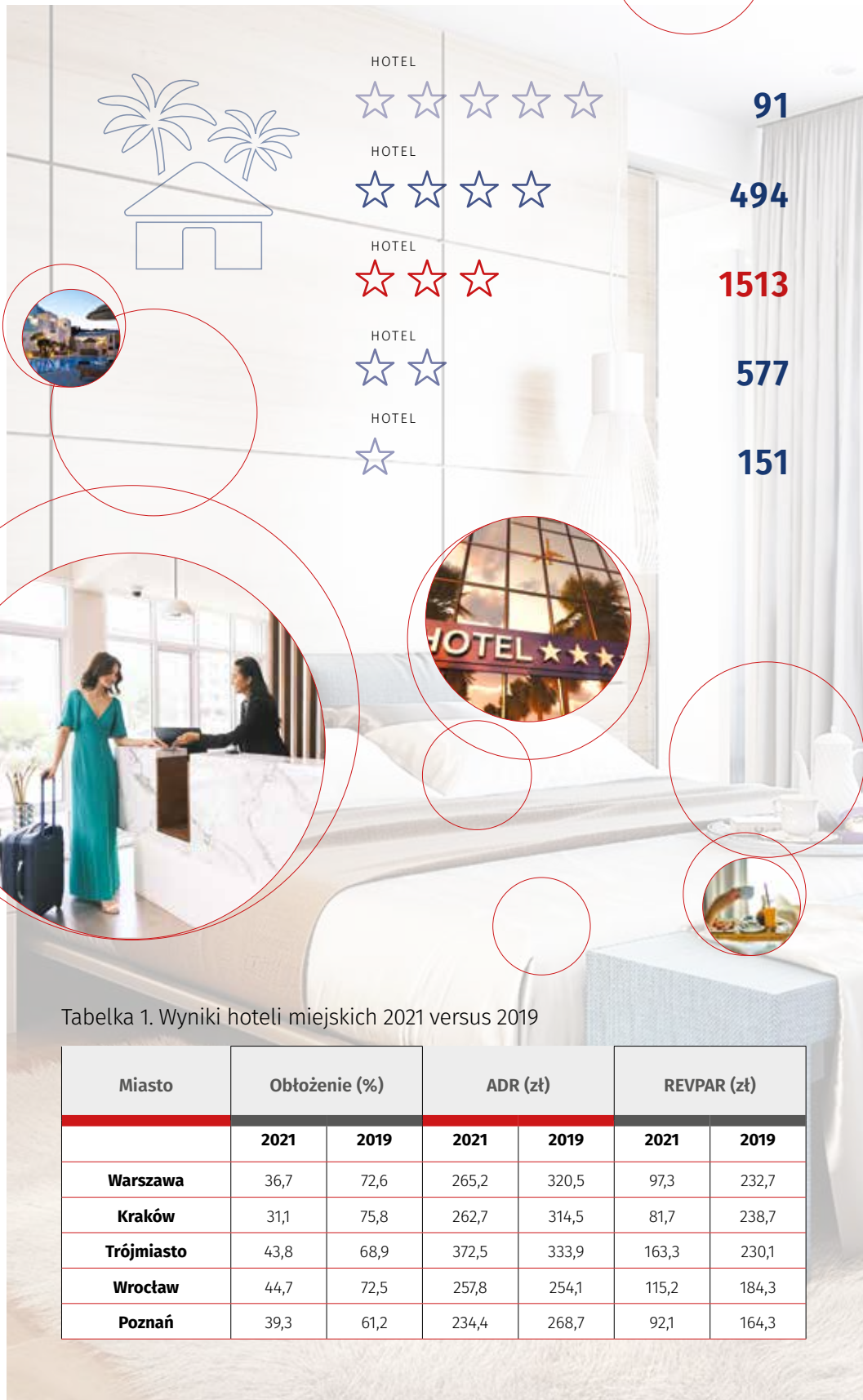


Tabela 1. Wyniki hoteli miejskich 2021 versus 2019

Miasto	Obłożenie (%)		ADR (zł)		REVPAR (zł)	
	2021	2019	2021	2019	2021	2019
Warszawa	36,7	72,6	265,2	320,5	97,3	232,7
Kraków	31,1	75,8	262,7	314,5	81,7	238,7
Trójmiasto	43,8	68,9	372,5	333,9	163,3	230,1
Wrocław	44,7	72,5	257,8	254,1	115,2	184,3
Poznań	39,3	61,2	234,4	268,7	92,1	164,3

Źródło: System Rejestrów Publicznych w Turystyce, turystyka.gov.pl. Stan na 2 czerwca 2023

region kwitnie i to dobre miejsce do inwestowania”. Pod względem liczby projektów w pipeline Polska zajmuje piąte miejsce w Europie. Potwierdzają to poniekąd raporty inwestycji pokazujące, jak baza noclegowa w Polsce powiększyła się w ciągu ostatnich trzech lat o tysiące nowych pokoi. Tylko w Warszawie od wybuchu pandemii pojawiło się 13 hoteli z ponad 2,5 tys. pokoi. W Krakowie – 10 hoteli, w których mieści się ponad 1,5 tys. pokoi. Gdańsk, Poznań, Wrocław, Kielce, Radom, Szczecin, Łódź powitają w bieżącym roku co prawda zaledwie po jednym nowym obiekcie. Prace są na różnych etapach – od braku rozpoczęcia działań budowlanych (Mövenpick w Poznaniu) po oddanie do użytku (B&B Kielce). Inaczej sytuacja przedstawia się w regionach turystycznych. W Karpaczu, Szklarskiej Porębie, Szczyrku, Szczawnicy, Pobierowie, Mielnie, Kołobrzegu, Międzyzdrojach, Międzywodziu, Darłowie i w całym pasie nadmorskim rynek jest rozgrzany do czerwoności. Trwają budowy obiektów mających pomieścić dziesiątki tysięcy pokoi. Otwierane są obiekty 300-pokojowe (Aqua Resort w Międzyzdrojach), 500-pokojowe (Crystal Mountain w Wiśle), a nawet 1000-pokojowe (hotel Gołębiowski w Pobierowie). Na marginesie zaznaczmy, że wiele z nich jest realizowanych w systemie condo. Do tego jeszcze wrócimy.

Skoro Polska jest tak chłonnym i pożądanym przez zagranicznych inwestorów rynkiem hotelarskim, dlaczego polscy przedsiębiorcy wypowiadają się o nim sceptycznie? Szymon Wróblewski, współwłaściciel Zdrojowa Invest&Hotels, mówi: „Największym problemem jest koszt kapitału i dostępność kapitału. Hotele muszą być teraz znacznie bardziej opłacalne niż dotąd”. Swoją wątpiący głos dokłada Rafał Abramczyk, prezes firmy doradczej hotelAG: „Nie widzę tego boomu budowlanego. W Warszawie powstają raptem trzy hotele – Puro, Campanille i Hampton by Hilton na Towarowej. Gdzie ten pipeline? Dostajemy mnóstwo zapytań od inwestorów, ale potem nic z nich nie wynika. To się nie przekłada na rozpoczęcie projektów”.

Faktycznie, inwestycje w Warszawie czy Krakowie, o których była mowa, toczą się siłą przedpandemicznego rozpędu. To projekty rozpoczęte w latach 2019–2020 lub wcześniej, które teraz są domykane. Na nowe bardzo trudno zdobyć fundusze. Obecna na HIT 2023 dyrektor w Banku Peak Izabela Kuszner powiedziała na otwarciu panelu finansowego, że w inwestycjach hotelowych minimalna wartość wkładu własnego wymagana obecnie przez banki to 50%. Inaczej model finansowy się nie domyka. Nietrudno zgadnąć, że dla wielu graczy to bariera nie do pokonania. Do tego należy doliczyć znacznie wyższe niż do niedawna ceny materiałów budowlanych, mediów i wykonawstwa. Finansowanie sektora bankowego, dotąd i tak ostrożnie dobierającego

projekty hotelarskie do swoich portfolio, teraz stało się dla inwestorów niemal nieosiągalne.

Tę lukę wypełniły projekty condo, czyli hotele finansowane przez właścicieli prywatnych. Wykupują oni poszczególne pokoje, którymi w zamian za czynsz zarządza operator. Poza strukturą własności, z punktu widzenia klienta, niczym nie różnią się one od tradycyjnych hoteli. Mają recepcję, restaurację, strefę SPA, siłownię, pralnię i inne hotelowe przestrzenie. Chyba że... nie mają. Kontrowersje związane z tymi projektami biorą się z niebotycznych jak na możliwości dzisiejszej gospodarki obietnic zysku – rzędu 8% rocznie – oraz licznych przypadków niedotrzymania umowy przez inwestora polegających na niewyposażeniu hotelu we wszystko, co stanowi o byciu takim obiektem. Stąd biorą się problemy: brak rentowności, rotacja operatorów, którzy nie są w stanie jej zapewnić, i koło się zamyka. Niektóre z projektów condo są obliczone wręcz na zysk jedynie z działań deweloperskich, więc nie mogą generować przychodu jako inwestycja długofalowa.

Jednocześnie przedstawiciele wielkich sieci – Hiltona, Marriotta, Radissona, IHG, Accor Group – opowiadają o planach dalszej rozbudowy w najbliższych latach. Zamierzają wybudować i otworzyć pod różnymi markami po kilka, kilkanaście obiektów każdy. Jak zaawansowane są te plany, tego podczas majowej konferencji nie ujawniono.

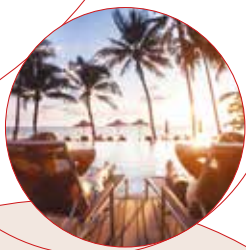
AI odpowiedzą na wszystkie bolączki?

Gdzie w tym wszystkim jest security? Bezpieczeństwo rozumiane w tradycyjny sposób nie spędza snu z powiek hotelarzom w takim stopniu jak kwestia finansów. Znacznie istotniejsze może niebawem okazać się bezpieczeństwo cyfrowe i ochrona wszelkich danych zarówno klientów, jak i samego hotelu. Hotele już teraz przetwarzają ogromne ilości

danych dotyczących np. preferencji klientów (programy lojalnościowe!) oraz tzw. *big data*, czyli informacje na temat dynamicznego poziomu cen na podstawie popytu i obłożenia. O dynamicznej digitalizacji (*dynamic digitalisation*) mówiono w branży już kilka lat temu, a część obiektów już jest naszpikowana technologią. Teraz otwiera się nowy rozdział tej opowieści – szeroką ławą wchodzi do codziennego użytku sztuczna inteligencja (AI). Wchodzi jeszcze śmieiej, należałoby dodać, ponieważ w wybranych segmentach rynku jest obecna od dawna, choćby w *revenue management*, czyli optymalizacji przychodów hotelu.

Branża zastanawia się, w jakich obszarach gościnności, opartej bądź co bądź na kontakcie i relacji z drugim człowiekiem, mogą sprawdzić się inteligentne maszyny. Pomysły wahają się od dość bezpiecznych i często stosowanych, takich jak klucze cyfrowe, chatboty, inteligentny, personalizowany marketing i social media,

»
Branża
zastanawia się,
w jakich obszarach
hotelarstwa, opartego bądź
co bądź na kontakcie i relacji
z drugim człowiekiem,
mogą sprawdzić się
inteligentne maszyny.
«



Przewidywania dla branży są różne dla różnych kategorii. Aglomeracje, w których branża była oparta na ruchu biznesowym i turystach zagranicznych, muszą liczyć się z nadpodażą.



działalność operacyjna – automatyzacja rezerwacji, zameldowania i wymeldowania, obsługa prostych potrzeb, np. zamówienie stolika w restauracji lub taksówki na lotnisko, po bardziej śmiało, jak zaawansowany system „niewidocznej” obsługi, czyli automatyzacja zarządzania hotelem. Połączenie systemu informacji o zameldowaniach i wymeldowaniach z serwisem sprzątającym, aby efektywnie wykorzystać jego moce i skierować najpierw do tych pokoi, które zostaną zajęte najszybciej, wykorzystanie czujników obecności do zaplanowania serwisu pobytowego, połączenie czujników ruchu sterujących nocnym oświetleniem na korytarzach z automatycznym przywołaniem windy na dane piętro, usprawnienie algorytmu zarządzającego hotelowym obłożeniem tak, aby było ono równomierne na wszystkich piętrach, wykorzystanie dźwigu było optymalne, a pokoje zużywały się w miarę jednakowo, czy wykrywanie przez AI potencjalnych zagrożeń, co zwiększy ochronę i bezpieczeństwo. Wszystko po to, aby doświadczenie gościa hotelowego było jak najlepsze. Jeśli to możliwe – szyte na miarę.

Co na to eko?

Ostatni na liście gorących tematów może rzucić ciekawe światło na bolączki hotelowej branży. Prowadzenie hotelowego biznesu ekologicznie jest dziś traktowane jako oczywistość, ale wielu menedżerów rozumie ją pobieżnie. „Od lat jesteśmy siecią wolną od jednorazowego plastiku”, „Ten dywan jest wykonany z wełny, jest ognioodporny i leży tu od dekady”, „W naszym hotelu nie drukujemy materiałów informacyjnych dla gości, tylko udostępniamy je online” – tego typu deklaracje, rzucane lekko, podawali goście podczas każdego panelu HIT 2023.

Temat jest obecny, ale można odnieść wrażenie, że mimo solennych zapewnień liderów o wadze ekologii branża w rzeczywistości traktuje ją po macoszemu. W nieodległej przyszłości może się to okazać sporym przeoczeniem, jako że stan środowiska naturalnego będzie definiował każdą sferę. Dlatego chciałabym zwrócić uwagę Czytelników na interesującą rzecz, którą podczas panelu liderów rynku powiedział Frank Reul, wiceprezes sieci Accor. Podniósł on kwestię traktowania przestrzeni: „Dziś skupiamy się na tym, żeby nasze hotele były wolne od plastiku, ale wkrótce będziemy budować nowe na zielonych dziewiczych terenach. Może należałoby się zastanowić nad konwersją już istniejących przestrzeni?”. Wspomniał również o standardach, które być może nie są już aktualne: „Aby hotel spełniał standardy 4- czy 5-gwiazdkowe, kluczowa jest odpowiednia wielkość pokoi, które muszą zająć określoną przestrzeń. Może zamiast zajmować coraz więcej przestrzeni, zmieńmy standardy?”.

W obliczu rozchwianej gospodarki, galopującej inflacji, toczącej się za naszą granicą wojny, gwałtownych zmian klimatu i powszechnej drożyzny XX-wieczne standardy w hotelarstwie mogą okazać się nie do obronienia. Mówiąc wprost, możemy nie poradzić sobie z utrzymaniem ogromnych powierzchni i wielu dodatkowych atrakcji.

Perspektywy

Przewidywania dla branży są różne dla różnych kategorii. Aglomeracje, w których branża była oparta na ruchu biznesowym i turystach zagranicznych, czyli głównie Warszawa i Kraków – gdzie w ostatnim czasie przybyły tysiące miejsc noclegowych



– muszą liczyć się z nadpodażą. Po pandemii ożywił się rynek MICE, ale jest to ruch słabszy niż przed 2020 r. Organizatorzy dużych międzynarodowych konferencji raczej nie będą brali pod uwagę naszego kraju ze względu na sąsiedztwo Ukrainy i związane z wojną podwyższone ryzyko. Na ile polski biznes wypełni tę lukę? Jak długo potrwa ten stan?

Co prawda także w regionach turystycznych, głównie w górach i nad morzem, buduje się bardzo wiele nowych hoteli, a dziesiątki niedawno otwarto. Chętnych do wypoczynku nie brakuje, ale czy portfele potencjalnych turystów wytrzymają ceny, które już równe są cenom w europejskich kurortach? Zmienia się struktura klientów – ruch zagraniczny jest mniejszy, większy generują rodzimi turyści. Zmieniają się preferencje podróżnych. Nowy wymiar wprowadzają także powszechna już praca zdalna i coraz powszechniejszy koncept *workation*, czyli pracy z miejsc turystycznego. I wreszcie AI – tu pytań jest więcej niż odpowiedzi. Czy zwiększy oszczędność, wydajność i przychody, czy zabierze miejsca pracy, skazując podróżnych na hotele bezobsługowe? Podniesie poziom bezpieczeństwa, czy wzmocni kontrolę i zacznie nami sterować? Eksperti w długofalowych przewidywaniach są raczej optymistyczni, jeśli chodzi o rozwój hotelarstwa w Polsce. Krótkofalowo – znaleźliśmy się w ciekawym momencie historycznym. ●

W hotelu Hilton McLean w Wirginii funkcję hotelowego concierge pełni robot Connie wykorzystujący sztuczną inteligencję IBM Watson AI i kognitywną technologię komputerową WayBlazer. Odpowiada na pytania gości hotelowych dotyczące lokalnych atrakcji turystycznych. Imię otrzymał na pamiątkę założyciela sieci Conrada Hiltona.

Choć pracownicy branży twierdzą, że stosunkowo łatwo można zrobić w niej karierę, tylko w 2020 r. odeszło z niej ok. 100 tys. ludzi. Brak rąk do pracy to problem wielu gałęzi gospodarki, zwłaszcza jeśli chodzi o proste, powtarzalne zadania, które łatwo zautomatyzować. AI nie zastąpi człowieka w tej branży, ale może znacząco podnieść jej wydajność, przejmując żmudne zadania oraz analizując różne dane.



Rodzinny hotel dyskretny i bezpieczny

Branża hotelarska to biznes niezwykle wrażliwy. Z jednej strony musi sprostać żądaniom klientów oczekujących zazwyczaj wysokiego standardu, dyskrecji i bezpieczeństwa, z drugiej – musi radzić sobie z wieloma aspektami hotelowego życia niewidocznymi dla gości.

Jacek Tyburek

ak podaje Główny Urząd Statystyczny, w końcu lipca 2021 r. w Polsce działalność prowadziły łącznie 9942 turystyczne obiekty noclegowe. Najwięcej było hoteli (2521), następnie pokoi gościnnych (2007), innych obiektów hotelowych (957) oraz ośrodków wczasowych (947). Hoteli 5- i 4-gwiazdkowych jest w Polsce około 500, a 3-gwiazdkowych ponad 1300. To liczby z pewnością interesujące dla branży zabezpieczeń. Uzyskanie i późniejsze utrzymanie gwiazdek oznacza spełnienie wyśrubowanych niejednokrotnie wymagań. To jednak inwestycja przekładająca się na rentowność obiektu. Dla branży security ważne jest to, by goście hotelowi, niezależnie od tego, czy zarezerwowali miejsce w 5-gwiazdkowym hotelu, czy w małym pensjonacie, mieli zapewnione bezpieczeństwo osobiste i ochronę swojej własności. Oczywiście nie można zamykać oczu na fakt, że inne możliwości ochrony ma hotel wysokiej klasy, a inne mały obiekt prowadzony przez osobę fizyczną. Oba powinny o tym pamiętać.

Gość w dom

Hotelarstwo jest branżą o tyle specyficzną, że nawet duże międzynarodowe sieci hotelarskie mają swoje korzenie w rodzinnym biznesie. Najstarszą działającą bez przerw firmą rodzinną świata jest hotel Hōshi Ryokan funkcjonujący od 718 r. w Komatus (Japonia). Słynne gorące źródła należące do hotelu uzdrawiają gości od 1291 r. Od 1300 lat należy do jednej rodziny. Zarządzało nim



»» *Polskie hotele będące własnością biznesowych rodzin wyróżniają się fantazją, ciekawym designem, pomysłową adaptacją bazy, na której zbudowano hotel. Mówiąc wprost, są dalekie od korporacyjnej unifikacji.* «

w tym czasie 46 pokoleń. Przez wieki istnienia budynki były wielokrotnie niszczone, jednak za każdym razem rodzina je odbudowywała. Niektóre części hotelu i ogród mają ponad 400 lat.

W Polsce ze względów oczywistych aż tak spektakularnych przykładów nie ma, ale wiele rodzimych obiektów jest biznesami rodzinnymi. Najbardziej znane to sieć hoteli Gołębiowski, butikowe hotele rodziny Likus czy inwestycje firmy Arche należącej do Władysława Grochowskiego. Niektóre firmy rodzinne nie inwestują jednak w sieć, a jedynie w pojedyncze obiekty, traktując je jako rodzaj wizytówki. Mowa m.in. o hotelu Narvil koło Serocka, należącym do właścicieli firmy farmaceutycznej Adamed, czy Blow Up Hall 50/50 będący własnością Grażyny Kulczyk oraz Hotelu Spa Dr Irena Eris.

Wszystkie powyżej wspomniane należą do obiektów klasy premium, w których odbywa się wiele imprez różnego charakteru. W czasie EURO 2012 aż dwa hotele należące do rodziny Likus gościły drużyny uczestniczące w imprezie sportowej.

Co różni wymienione hotele i ośrodki hotelowo-konferencyjne od należących do międzynarodowych sieci o podobnej klasie? Nie można oprzeć się wrażeniu, że polskie hotele będące własnością biznesowych rodzin wyróżniają się fantazją, ciekawym designem, pomysłową adaptacją bazy, na której zbudowano hotel. Mówiąc wprost, są dalekie od korporacyjnej unifikacji.

Przykładem jest Hotel Stary w Krakowie (Likus Hotele), który był bazą pobytową reprezentacji Anglii w czasie EURO 2012. Jego wnętrza mają przywoływać skojarzenia ze średnio-wiecznym zamkiem, czemu służy nieoczywisty system korytarzy i przejść. Za wrażenie luksusu odpowiadają użyte w pomieszczeniach materiały, w tym skóra, drewno egzotyczne, orientalne dywany. Na niebanalne rozwiązania stawiają także hotele Arche, można je znaleźć szczególnie we flagowych obiektach tej sieci: Cukrowni Żnin i Folwarku Łochów. W obu przypadkach to kompleksy hotelowo-konferencyjno-wypoczynkowe z rozbudowaną strukturą obiektów tworzących te miejsca. Poza wyglądem istotna jest jeszcze jedna ich cecha, tak ważna dla branży security: łatwiejsza współpraca z zarządem takiego obiektu.

Elementarz bezpieczeństwa hotelowego

O jakich zabezpieczeniach, systemach i procedurach powinien zatem pamiętać zarząd hotelu, aby zapewnić gościom dyskrecję i bezpieczeństwo? Przede wszystkim powinny to być:

- kontrola dostępu zarówno do pokoi, jak i wszystkich kluczowych pomieszczeń hotelowych pozwalająca na tworzenie stref dostępu dla klientów zgodnie z potrzebami;
- zapewnienie bezpieczeństwa pojazdów gości wraz z możliwością odtworzenia zdarzeń w przypadku incydentów z ich udziałem;





Warto wiedzieć

- Polskie prawo nie dysponuje definicją firmy rodzinnej. Nie znaczy to jednak, że ich nie ma. Polska Agencja Rozwoju Przedsiębiorczości przyjęła zatem, że przedsiębiorstwo rodzinne to podmiot gospodarczy, w którym pracuje co najmniej dwóch członków rodziny właścicieli lub osób z nią spokrewnionych i zarazem przynajmniej jedna z nich ma wpływ na zarządzanie przedsiębiorstwem, i również do rodziny lub osób z nią spokrewnionych należy ponad 50% udziałów przedsiębiorstwa.
- Nie ma więc znaczenia, czy będziemy mieć do czynienia z jednoosobową działalnością gospodarczą, czy sp. z o.o., by była to jednocześnie firma rodzinna, o ile jeden z powyższych warunków zostanie spełniony. A przecież hotelarstwo ma to do siebie, że w obsłudze gości zaangażowana jest cała rodzina. Dotyczy to zwłaszcza różnego rodzaju pensjonatów czy moteli.



» *Polska należy do krajów, w których zgłoszenie swojego hotelu do kontroli i otrzymanie kategorii wyrażanej gwiazdkami (lub ku zgrozie gości ich całkowitym brakiem) jest obowiązkowe i sankcjonowane prawnie.* «

- systemy przywoływania pomocy;
- systemy do zarządzania bieżącą konserwacją urządzeń infrastruktury security hotelu zarówno elektronicznych, jak i mechanicznych;
- monitorowanie dostępu i używania kluczy mechanicznych. Rekomendowane jest stosowanie mechaniczno-elektronicznych rozwiązań gromadzących dane o ich użyciu;
- monitoring wizyjny – w zależności od skali obiektu monitorowanie powinno się odbywać w trybie prewencyjnym i online;
- zastosowanie procedur oraz rozwiązań dotyczących gromadzenia i przekazywania gotówki, zorganizowanie systemu minimalizujące ilość gotówki;
- stosowanie systemów antynapadowych dla personelu hotelu na wypadek ataków kryminalnych lub terrorystycznych;
- stosowanie szaf i sejfów do przechowywania przedmiotów wysokiej wartości oraz dużego znaczenia lub wydzielenie specjalnego pomieszczenia do przechowania wartościowych przedmiotów klientów;
- korzystanie z usług wyspecjalizowanych w zapewnianiu bezpieczeństwa firm ochrony, zarówno pracowników ochrony fizycznej, operatorów monitoringu, jak i detektywów hotelowych;
- przygotowanie procedur alarmowych i awaryjnych bazujących na analizie ryzyka dla różnych scenariuszy;
- ochrona systemów IT przed cyberprzestępczością wymierzonych w hotel oraz jego gości.

Powyższa lista to elementarz bezpieczeństwa dla dobrze zorganizowanego ośrodka, a przede wszystkim takiego, którego właścicielem zależy nie tylko na wysokiej kategorii, ale także na dobrych opiniach w Internecie.

Komu gwiazdkę, komu?

Należy pamiętać, że aby obiekt mógł się ubiegać o gwiazdki oznaczające jakość usług, musi gwarantować określony poziom wyposażenia hotelu oraz jakości usług w nim stosowanych. W naszym kraju system kategoryzacji hoteli został wprowadzony na podstawie Ustawy z 29 sierpnia 1997 roku o usługach hotelarskich oraz usługach pilotów wycieczek i przewodników turystycznych. Konkretnie wymagania związane z przyznawaniem gwiazdek znajdują się w rozporządzeniu Ministra Sportu i Turystyki z 16 listopada 2011 r. Aby świadczyć usługi hotelarskie, należy spełnić określone ustawowe wymagania, a przedsiębiorca jest zobowiązany uzyskać kategoryzację (art. 39 wspomnianej ustawy). Polska należy do krajów, w których zgłoszenie swojego hotelu do kontroli i otrzymanie kategorii wyrażanej gwiazdkami (lub ku zgrozie gości ich całkowitym brakiem) jest obowiązkowe i sankcjonowane prawnie. Do tej grupy państw należą również m.in. Holandia, Belgia, Węgry, Włochy czy Hiszpania. Są jednak takie kraje, gdzie procedura ta jest dobrowolna i polega na chęci właściciela obiektu (np. we Francji, w Niemczech czy Wielkiej Brytanii).

O zaszeregowaniu obiektu hotelarskiego do jednego z poszczególnych rodzajów (a jest ich w sumie osiem) oraz przyznaniu konkretnej kategorii (wyrażanej gwiazdkami) decyduje właściwy terytorialnie marszałek województwa. I zazwyczaj jest to procedura złożona. Marszałkowie powołują specjalną komisję złożoną ze specjalistów z dziedzin hotelarstwa. W jej skład wchodzi często również przedstawiciele sanepidu oraz straży pożarnej.

Wbrew powszechnemu przekonaniu nie tylko hotele mają gwiazdki. Przyznawane są one także motelom, pensjonatom, a nawet kempingom. A im więcej gwiazdek, tym bardziej wyśrubowane wymagania, także dotyczące bezpieczeństwa. W zamian za to rośnie cena noclegu.

Gdzie są konfitury?

Hotele sieciowych globalnych marek branży hotelarskich, takich jak Marriott, Sheraton, Hilton, Holiday Inn czy Accor, mają własne wyśrubowane standardy bezpieczeństwa. Słowo „własne” jest w tym przypadku kluczowe. Z własnymi standardami wiążą się bowiem bardzo często własne firmy wykonawcze lub globalnie wybrane firmy dostawcze, w tym usługowe. Moje doświadczenie podpowiada, że „wejście” do takiego obiektu z ofertą security to dla polskiej branży twardy orzech do zgryzienia. Jednocześnie z perspektywy branży największymi potencjalnymi klientami są właśnie obiekty 4- i 5-gwiazdkowe. Jak to pogodzić? Kierując uwagę na obiekty prowadzone przez firmy rodzinne.

W Polsce prestiżowych hoteli nie brakuje, wiele pozostałych obiektów oferuje warunki więcej niż przyzwoite. I choć hotele 5-gwiazdkowe od 3-gwiazdkowych pensjonatów dzieli jakościowa przepaść, to często mają one wspólny mianownik – są prowadzone przez firmę rodzinną. Z moich doświadczeń wynika, że ta cecha ułatwia współpracę. Polski właściciel, od podszewki znający swój biznes, bardzo często jednoosobowo nim zarządzający oznacza, że proces decyzyjny jest krótszy w porównaniu z obiektami pozostającymi w gestii dużych firm. Łatwiejsze są też ustalenia dotyczące zabezpieczeń, a firmy rodzinne, choć bardzo często oglądające uważnie każdą wydawaną złotówkę, są pod różnymi względami bardziej elastyczne niż korporacje międzynarodowe.

Powodów tej elastyczności jest kilka. Pierwszym i najważniejszym jest brak wyznaczonego globalnie standardu bezpieczeństwa sprowadzającego się do listy urządzeń pochodzących od wyznaczonych przez działy inwestycji i zakupów. W przypadku krajowego biznesu branża ma zdecydowanie większe pole do popisu. Nie jest też, proponując rozwiązania, ograniczana narzucanymi standardami. Polscy właściciele nie boją się też nowinek i chętnie przyjmują nieszablonowe pomysły.

Pewnym wyzwaniem dla kreatywności dostawców rozwiązań są obiekty o charakterze butikowym. Jednocześnie to w nich dostawca może wprowadzić rozwiązania autorskie, nieszablonowe, szyte na miarę danego budynku. Ważne jest to, że w mniejszych obiektach prowadzonych rodzinnie brak eksperta security. Dla branży to szansa, gdyż taki obiekt potrzebuje najpierw doradztwa i projektu, a potem stałego wsparcia zgodnie z potrzebami hotelu. •

R E K L A M A



Produkty i Rozwiązania zgodne z NDAA

Bezpieczeństwo cybernetyczne,
któremu możesz zaufać



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*. Obecnie związany z Black Onion Resilience Community.





Rozważania o bezpieczeństwie w hotelach

Bezpieczeństwo gości – to o nim myślimy w pierwszej kolejności, gdy pytamy o systemy stosowane w hotelarstwie. Klienci mają odczuwać spokój i komfortowo spędzić czas w obiekcie. Nie ukrywamy jednak, że często stosuje się również zabezpieczenia, które dbają nie o wygodę gości, ale o interes gospodarza.

Hubert Żak

Kluczowe systemy stosowane w obiektach hotelowych można podzielić na dwie kategorie. Pierwsze wymagane przepisami, czyli m.in. systemy sygnalizacji pożarowej (SSP) i dźwiękowe systemy ostrzegawcze (DSO), oraz dodatkowe, dobrowolnie już instalowane systemy telewizji dozorowej, kontroli dostępu czy zamki hotelowe. Bez tych pierwszych obiekt nie może działać. Jeśli kontrola wykaże, że są wadliwe lub niesprawne, zarząd hotelu musi liczyć się ze wstrzymaniem działalności do czasu usunięcia problemu. W przypadku tych drugich zarówno zamawiający, jak i wykonawca muszą uwzględnić przepisy RODO.

Dobór systemów zabezpieczeń w dużej mierze zależy od procedur obowiązujących w obiekcie i od tego, czy pozwolą gromadzić dane przydatne w działalności biznesowej. Wówczas to ich wartość dodana.

Na to, jakie zostaną ostatecznie zastosowane zabezpieczenia, wpływa przede wszystkim rodzaj prowadzonej działalności. W przypadku hotelu należy brać pod uwagę nie tylko obsługę gości, ale także ewentualne postępowanie odszkodowawcze czy współpracę ze służbami.

„Czy ja byłem z pieskiem, czy bez pieska?”

Strefy wjazdu i wyjazdu z parkingu hotelowego powinny być monitorowane kamerami wysokiej rozdzielczości rozlokowanymi tak, aby możliwa była rejestracja nie tylko tego, co dzieje się na parkingu, ale też tego, w jakim stanie są pojazdy wjeżdżające. Jednocześnie należy pamiętać o wystarczająco długim przechowywaniu zapisu, gdyż roszczenia niejednokrotnie pojawiają się po dłuższym czasie od opuszczenia przez gościa hotelu.



W jednym z hoteli gość powiadał recepcję o tym, że jego auto zostało uszkodzone na przynależącym do budynku parkingu. Odtworzenie nagrania z dnia przybycia tej osoby zarejestrowanego przez kamery umieszczone w strefie wjazdu dowiodło, iż już wtedy samochód był uszkodzony.





Bywa też, że goście hotelowi zgłaszają, że okradziono ich pokój. Nie zawsze jest to próba wyłudzenia. Niekiedy to zwykłe roztargnienie lub niedopatrzenie gościa. Monitoring wizyjny pozwala wyjaśnić sytuację, o ile wtedy, gdy miała nastąpić kradzież, nikt do pokoju hotelowego nie wchodził. Jeśli zaś wszedł ktoś z obsługi, monitoring ułatwia poprowadzenie dalszego postępowania. Ważne, aby wejście do pokoju były nadzorowane w ten sposób, by nagranie nie pozostawiało pola do dowolnej interpretacji. Dlatego przydatnym uzupełnieniem telewizji dozorowej jest możliwość zbierania informacji z użycia zamków hotelowych.

Płacić czy nie płacić

Kolejnym obszarem wymagającym szczególnej uwagi i zastosowania odpowiednich rozwiązań są systemy transakcyjno-płatnicze. Odpowiednio zaprojektowane i wdrożone pozwalają od razu rozwiać wątpliwości co do tego, czy gość uiścił rachunek, jak twierdzi, czy też nie. Zdarza się niekiedy, że w tej kwestii dochodzi do sporu pomiędzy obsługą a klientem. Pojawiają się też próby posługiwania się fałszywymi pieniędzmi lub płatność cudzą kartą. Należy zawsze mieć na względzie, że przepisy szczegółowo określają, jakie dane dotyczące osób płacących inaczej niż gotówką mogą być gromadzone i jak długo mogą być one przechowywane.

Czy leci z nami pilot?

Nadzorowanie obiektu bez zaawansowanych systemów jest wyzwaniem nawet dla najbardziej doświadczonych menedżerów hotelowych. Urządzenia i aplikacje realizujące zadania kontroli dostępu oraz systemy zamków hotelowych stanowią w zasadzie najważniejsze narzędzia pozwalające zapanować nad tym, co się dzieje w budynku, chroniąc magazyny i umożliwiając wydzielenie stref z ograniczonym dostępem.

Dobrze zorganizowana kontrola dostępu, z podziałem na strefy i rejestracją wydarzeń, takich jak użycie zamka, ogranicza kradzież i nadużycia wewnętrzne zarówno przez pracowników własnych, jak i firmy zewnętrzne. Zastosowanie CCTV daje efekt synergii, wzmacniając ochronę i minimalizując ryzyko do zaledwie kilku procent.

Wydzielenie stref zapewnia płynną kontrolę i ograniczenie dostępu osobom nieupoważnionym. Jest również ważne ze względu na bezpieczeństwo ogólne w zakresie kradzieży, zewnętrznych zagrożeń atakami terrorystycznymi i innymi incydentami, w przypadku których uwarunkowania architektoniczne nie pozwalają na stałe odcięcie ciągu komunikacyjnego. Sprawdzi się wówczas kontrola dostępu pozwalająca na płynną kontrolę różnych przestrzeni.

Bardzo ważne, jeśli nie najważniejsze, są systemy ewakuacyjne i rozwiązania je wspomagające. Od tego, czy zostaną dobrze zaprojektowane i właściwie zainstalowane, może zależeć zdrowie i życie ludzi. Same systemy to zbyt mało, ważne są także szkolenia, przede wszystkim personelu, który musi być gotów do przeprowadzenia sprawnej ewakuacji (więcej na ten temat w wywiadzie na str. 82 – przyp. red.)



Na podziemnym parkingu hotelowym doszło do samozapłonu instalacji i pożaru. System sygnalizacji pożarowej zareagował błyskawicznie, uruchamiając drugi poziom alarmu. Ze względu na zadymienie, do którego doszło pomimo automatycznego otwarcia kłap i uruchomienia oddymiania, obsługa

natychmiast przystąpiła do ewakuacji. Ponad 300 gości oraz personel sprawnie opuściło budynek m.in. za sprawą właściwego oświetlenia ewakuacyjnego i komunikatów akustycznych. Cała ewakuacja przebiegła sprawnie, bez paniki, nikt nie został poszkodowany dzięki temu, że zadziałał bardzo dobrze zaprojektowany i skonfigurowany system pożarowy wraz z DSO oraz sensowne procedury wewnętrzne.

W obiektach wyposażonych w odpowiednie, właściwie dobrane i umiejętnie obsługiwane systemy zabezpieczeń liczba roszczeń wysuwanych przez gości i wysokość odszkodowań wypłacanych w związku z nimi jest znacznie niższa niż w obiektach takich systemów pozbawionych.



W świetnie usytuowanym hotelu cieszącym się dużą popularnością roczny koszt wypłacanych gościom odszkodowań w ostatnich latach przed pandemią wahał się od 500 tys. do nawet 1,2 mln zł. Po zainstalowaniu odpowiednich urządzeń kontroli dostępu i telewizji dozorowej kwoty odszkodowań

zostały znacząco zredukowane, co wpłynęło na zmniejszenie szkodowości hotelu, a wraz z nią składek ubezpieczeniowych. Obiekt odnotował aż 10-krotny spadek wartości wypłat.

Dbanie o bezpieczeństwo gości i pracowników nie może być postrzegane wyłącznie jako koszt. Jest to też inwestycja w zdrowie i życie gości oraz pracowników, własną reputację, a ostatecznie także w mniejsze składki ubezpieczeniowe. Doświadczeni hotelarze wiedzą bowiem, że wiele prawdy jest w angielskim powiedzeniu „Liczbę na najlepsze, lecz bądź przygotowany na najgorsze”. ●

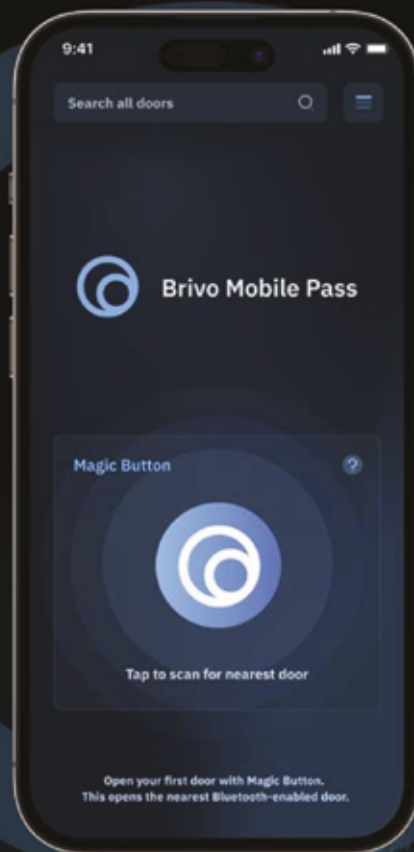
Hubert Żak

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



DOSTĘP JEST PRZYSZŁOŚCIĄ INTELIGENTNYCH BIUR

ZOPTYMALIZUJ
SWOJE NIERUCHOMOŚCI
DZIĘKI KONTROLI
DOSTĘPU BRIVO



Technologia
zabezpieczeń klasy
korporacyjnej dla
każdego rodzaju obiektu

60+
KRAJÓW NA
CAŁYM ŚWIECIE



Kontrola dostępu i dane
video, dzięki którym Twoje
budynki staną się bardziej
inteligentne

90+
TYSIĄCE
WDROŻEŃ



Możliwości integracji,
aby połączyć istniejące
inwestycje
technologiczne

450Mkw
NIERUCHOMOŚCI W
ZARZĄDZANIU



Security w hotelarstwie

W hotelach dochodzi do różnych incydentów, ale miarą sukcesu ich działań bezpieczeństwa nie jest niewielka liczba zdarzeń, ale to, jak wielu z nich udaje się zapobiec. Ułatwiają to liczne procedury oraz programy bezpieczeństwa i ochrony, które są stosowane zarówno przez wielkie sieci, jak i pojedyncze obiekty. Gdy wszystko jest w porządku, wszyscy są zadowoleni, ale ze względu na specyfikę branży opartej na gościnności, hotele muszą być przygotowane na wydarzenia niepożądane. Jak się do tego przygotowują i jakie narzędzia stosują? Adela Prochyra zapytała o to security managerów Radissona, Orbisu, Polskiego Holdingu Hotelowego i Marriotta.

Hotele muszą przestrzegać przepisów BHP, prawa budowlanego i przeciwpożarowego, jak również zasad zdrowego rozsądku, ale poza tym przepisy nie określają szczególnych środków, jakie hotele muszą powziąć, aby zapewnić swoim gościom bezpieczeństwo pobytu. Pamiętajmy, że większość obiektów hotelowych jest otwarta dla różnych ludzi przez całą dobę. Może wejść każdy, a to zawsze niesie ryzyko. Jeśli są to duże przestrzenie, czuwanie nad bezpieczeństwem klientów staje się jeszcze trudniejsze. A zdarzyć się mogą różne rzeczy – od pospolitych kradzieży po wtargnięcia osób niepożądanych czy pożary. Generalnie hotele spełniają wysokie standardy, jeśli chodzi o bezpieczeństwo gości. Stosują szereg zabezpieczeń i reguł, a ponadto zrzeszają się w sieciach, współpracują ze służbami porządkowymi i ze sobą nawzajem, korzystają z nowoczesnego sprzętu. Zobaczmy, jak się przygotowują na niespodziewane.



» W biznesie i działalności 24/7 wszystko może się zdarzyć w dowolnym momencie, począwszy od protestów poza hotelem, domniemanej kradzieży, klęsk żywiołowych, pożarów, zagrożeń bombowych itp. «

Geert Coremans

Director Corporate Safety & Security,
Radisson Hotel Group

Czym różni się branża hotelarska od innych branż pod względem bezpieczeństwa?

Hotele działają w systemie ochrony 24 godziny na dobę, 7 dni w tygodniu. W niektórych lokalizacjach na świecie są uznawane za miejsca narażone na większe zagrożenia, więc musimy się upewnić, że mamy odpowiednie środki, aby chronić członków naszego zespołu i gości.

Jakie procedury, systemy lub praktyki bezpieczeństwa są ważne w hotelu?

Opracowaliśmy kompleksowe procedury i wdrożyliśmy systemy zabezpieczeń, które chronią członków naszego zespołu oraz gości i o nich dbają. Korzystamy z naszego globalnego programu S&S TRICS, aby upewnić się, że wszystkie potrzeby są zaspokojone. W celu zapewnienia bezpieczeństwa stosujemy formułę $T + R + I + C = S$ (*Threat Assessment + Risk Mitigation + Incident Response + Crisis Management = Safe & Secure Hotels*). To podejście oznacza ocenę zagrożeń, ograniczanie ryzyka, reagowanie na incydenty i zarządzanie kryzysowe, dzięki czemu przy ciągłości komunikacji hotel jest bezpieczny.

Co jest najważniejsze, jeśli chodzi o bezpieczeństwo?

Najważniejsze, aby goście hotelowi i członkowie zespołu byli bezpieczni i czuli się zaopiekowani. Ścisłe współpracujemy z Safehotels, która certyfikuje nasze obiekty według własnego, niezależnego globalnego standardu bezpieczeństwa hoteli (*Global Hotel Security Standard*). Kryteria certyfikacji uzyskane przez hotel składają się z ponad 230 indywidualnie ocenianych na miejscu elementów związanych z bezpieczeństwem (w tym pożarowym), zarządzaniem kryzysowym oraz zdrowiem. Obecnie 141 naszych placówek posiada certyfikat Safehotels.

W jaki sposób opracowywane są procedury bezpieczeństwa?

Stosowane przez nas procedury bezpieczeństwa powstały na bazie połączenia podejścia odgórnego i oddolnego, aby jak najlepiej wykorzystać wspólną wiedzę. Standardowe procedury operacyjne (SOP) różnią się w zależności od lokalizacji, są dostosowywane do bieżących sytuacji na podstawie incydentów, których doświadczyliśmy jako grupa hotelowa. Na przykład w ramach naszych kwartalnych wizyt SSA (*Social Security Administration*) po strzelaninie w Mandalay Bay w Las Vegas zdecydowaliśmy o wzmocnieniu wytycznych, szkoleń, procedur i zabezpieczeń.

Z jakimi sytuacjami i incydentami najczęściej spotykają się hotele i jak sobie z nimi radzą?

W biznesie i działalności 24/7 wszystko może się zdarzyć w dowolnym momencie, począwszy od protestów poza hotelem, poprzez domniemaną kradzież, klęski żywiołowe, pożary, skończywszy na atakach terrorystycznych. Zasadniczym elementem jest umożliwienie zespołom hotelowym działania poprzez reagowanie na incydent. Niekoniecznie musi być to 500-stronicowy podręcznik z SOP opisujący każdą potencjalną sytuację. Mamy solidny i jasny proces zarządzania kryzysowego z poziomami brązowym, srebrnym i złotym, ustalonymi na podstawie wagi incydentu. Nasze zespoły hotelowe znają podstawowe działania, jakie muszą podjąć w takich sytuacjach. Wiedzą, jak utworzyć lokalny zespół zarządzania kryzysowego, kiedy powiadomić kierownictwo wyższego szczebla i jak zwiększyć swoją gotowość do radzenia sobie z incydentami.

Jakie rozwiązania w zakresie bezpieczeństwa są obecnie interesujące z perspektywy branży hotelarskiej?

Jesteśmy firmą opartą na ludziach, a nasi pracownicy są naszym najważniejszym zasobem. Współpracujemy z ekspertami zewnętrznymi w zakresie doradztwa strategicznego i taktycznego, wskazówek dotyczących wdrażania projektów bezpieczeństwa oraz systemów zabezpieczeń technicznych w niektórych lokalizacjach o wyższym zagrożeniu.



Andrzej Berecki

Kierownik ds. Bezpieczeństwa,
Orbis S.A./AccorInvest Europa
Wschodnia

Czym różni się branża hotelarska od innych branż pod względem security?

Istotnym aspektem jest dla mnie stosowanie standardów sieciowych. Połączenie zewnętrznych przepisów i wytycznych sieci pozwala stworzyć solidny system bezpieczeństwa. W ramach standardów sieciowych przeprowadzane są regularne i szczegółowe audyty pod kątem stanu bezpieczeństwa, nie tylko fizycznego. Ważną kwestią jest również współpraca pomiędzy hotelami w grupie i wymiana wiedzy, dobrych praktyk oraz doświadczeń. Niedawno spotkałem się z moim odpowiednikiem zatrudnionym w Wielkiej Brytanii. Wymieniliśmy doświadczenia, omówiliśmy najlepsze praktyki, a przede wszystkim upewniliśmy się, że nasze systemy i organizacja są na wysokim poziomie.

Jakie procedury, systemy czy praktyki bezpieczeństwa są istotne w hotelu?

Bezpieczeństwo hotelu jest obszarem o szerokim zakresie i obejmuje wiele elementów. W branży hotelarskiej można zastosować wiele podstawowych środków bezpieczeństwa w celu ochrony zarówno gości, pracowników, jak i mienia hotelowego. Przykładowo systemy monitoringu wizyjnego (CCTV), kontroli dostępu





» W moim przekonaniu priorytetowym elementem jest system sygnalizacji pożaru i zadymienia. «

oraz systemy parkingowe funkcjonują w celu zapobiegania nieuprawnionemu dostępowi czy wykrywania osób przebywających w niedozwolonych obszarach. Rolą sprawnie działających systemów jest także minimalizacja strat. W moim przekonaniu elementem priorytetowym jest system sygnalizacji pożaru. Dlatego niezwykle ważne są niezawodność i prawidłowe funkcjonowanie tego systemu, a także innych urządzeń oraz systemów ochrony przeciwpożarowej.

Znajomość obsługi centrali pożarowej oraz dźwiękowego systemu ostrzegania jest kluczowa dla zapewnienia bezpieczeństwa gości, pracowników oraz mienia. W związku z tym szczególną wagę przykładamy do szkolenia pracowników w tym obszarze. Odpowiedzialność za zarządzanie ewakuacją w przypadku zagrożenia spoczywa na zespołach recepcji. Dlatego organizujemy ćwiczenia praktyczne dla wszystkich pracowników, ale ze szczególnym uwzględnieniem zespołów recepcji, obejmujące uruchomienie wszystkich systemów i urządzeń ochrony przeciwpożarowej w hotelu oraz DSO. Regularnie współpracujemy również z państwową strażą pożarną. Przykładem tego jest niedawne ćwiczenie, w którym za pomocą wysięgnika ewakuowaliśmy ludzi z jedenastego piętra jednego z naszych hoteli. W pierwszej połowie 2023 r. przeszkoliłem już ponad tysiąc naszych pracowników w Polsce w zakresie bezpieczeństwa pożarowego.

Co jest najistotniejsze, jeśli chodzi o bezpieczeństwo?

Uważam, że bardzo ważni w kontekście bezpieczeństwa są wszyscy pracownicy hotelu, nie tylko pracownicy ochrony. Ich spostrzegawczość, zdrowy rozsądek, pewność siebie, odpowiednie przeszkolenie w zakresie rozpoznawania sytuacji zagrożeń, świadomość bezpieczeństwa oraz wiedza, kogo i kiedy powiadomić, są kluczowe dla minimalizacji lub wyeliminowania zagrożeń. Właściwe przeszkolenie pracowników w zakresie bezpieczeństwa pozwala im reagować skutecznie i szybko w przypadku wystąpienia incydentów. Warto również polegać na świadomych gościach, od których możemy również dowiedzieć się o nietypowych sytuacjach.

Jak powstają procedury bezpieczeństwa w państwa hotelach?

AccorInvest jest operatorem i właścicielem hoteli w Europie, obecnym również w Ameryce Łacińskiej i Azji. Grupa działa w dwudziestu sześciu krajach i ma blisko osiemset obiektów. W Polsce jest właścicielem Orbisu, który dysponuje ponad czterdziestoma hotelami. W Polsce i pozostałych krajach zarządza nimi Accor, który przygotował kompleksowy zestaw wskazówek dotyczących bezpieczeństwa w celu ułatwienia zarządzania incydentami i sytuacjami kryzysowymi na poziomie hotelu. Stosujemy je, a w razie potrzeby modyfikujemy, aby były jeszcze bardziej efektywne – w zależności od lokalizacji, wielkości hotelu oraz rodzaju występujących zagrożeń. Na poziomie zarówno hoteli, jak i biur zarządu istnieją komitety kryzysowe odpowiedzialne za reagowanie na sytuacje kryzysowe i udzielanie wsparcia w zarządzaniu nimi. Bezpieczeństwo pracowników i gości jest naszym priorytetem, dlatego podejmujemy

wszelkie niezbędne środki, aby minimalizować ryzyko oraz skutki incydentów czy sytuacji kryzysowych.

Z jakimi sytuacjami i incydentami najczęściej spotykają się hotele i jak sobie z nimi radzą?

Pracuję w branży hotelarskiej od 2001 roku, m.in. w hotelach pięciogwiazdkowych w Warszawie. Przez ten czas spotkałem się z wieloma incydentami i sytuacjami kryzysowymi, które wymagały natychmiastowej reakcji i skutecznego zarządzania. Charakter pracy w obszarze bezpieczeństwa tych obiektów wiąże się z ciągłą dostępnością, osoby związane z tą dziedziną wiedzą, jak istotne jest to zobowiązanie. Bezpieczeństwo gości i personelu zawsze było dla nas najwyższym priorytetem, dlatego stale doskonalimy swoje umiejętności i pozostajemy czujni na wszelkie potencjalne zagrożenia.

Jakie rozwiązania z obszaru bezpieczeństwa są interesujące z perspektywy hotelarstwa?

W przypadku hotelowych technicznych systemów bezpieczeństwa moim zdaniem niczego rewolucyjnego już nie odkrywamy. Wspomniane wcześniej rozwiązania, takie jak m.in. monitoring CCTV, analityka, systemy przeciwpożarowe, systemy kontroli dostępu, depozytory kluczy, klucze gościnne oparte na smartfonach, stanowią duże wsparcie. Większość technicznych rozwiązań już mamy. Ważne jest podejmowanie działań organizacyjnych i komunikacyjnych, aby pracownicy współpracowali efektywnie, potrafili skutecznie wykorzystać istniejące systemy bezpieczeństwa, dlatego kluczowym elementem są szkolenia. W naszej grupie regularnie je przeprowadzamy. Obejmują one m.in. szkolenia dotyczące obsługi systemów, zagadnienia BHP, pierwszej pomocy, obsługi defibrylatora AED czy obsługę gaśnic. Ponadto wprowadziliśmy szkolenia dotyczące rozwiązywania sytuacji trudnych i kryzysowych, uwzględniające m.in. sieciowe wskazówki postępowania w przypadku zagrożeń ALERT.

Pamiętajmy, że bezpieczeństwo w hotelu to nie tylko kwestia terroryzmu i podobnych zagrożeń. Niezwykle ważne są inne obszary m.in. to, jak postępować w przypadku zaginionego dziecka lub podejrzenia wykorzystywania seksualnego nieletnich. Czy wolno przechowywać leki lub broń, jak interpretować sygnały alarmowe z centrali pożarowej dotyczące np. czujników przepływu w instalacji tryskaczowej. Czy pracownicy hotelu mogą i powinni opiekować się dziećmi gości. Jak postępować podczas wizyt Vipów. Jak postępować w przypadku osoby nieprzytomnej w zablokowanej windzie itp. To tylko niektóre obszary dotyczące szeroko rozumianego bezpieczeństwa działalności hotelowej.



Barbara Podwysocka

dyrektor Pionu Jakości i Bezpieczeństwa
Polski Holding Hotelowy

» *Procedury bezpieczeństwa zawsze muszą być poprzedzone analizą zewnętrznymi i wewnętrznymi uwarunkowań danego obiektu hotelarskiego. Tylko tak przygotowane procedury są adekwatne do danego obiektu. «*

Jakie procedury, systemy czy praktyki bezpieczeństwa są istotne w hotelu?

Branża hotelarska to jedna z najszybciej i najlepiej rozwijających się gałęzi gospodarczych, dlatego utrzymanie odpowiedniego poziomu bezpieczeństwa jest tu szczególnie istotne.

Wielowymiarowość i interdyscyplinarny charakter terminu „bezpieczeństwo” sprawia, że na jego strukturę należy patrzeć na wielu płaszczyznach, a jednocześnie rozpatrywać zagrożenia i ryzyka na etapach działania przedsiębiorstwa. Takie podejście do systemu bezpieczeństwa należy przyjąć jako priorytet.

Czym branża hotelarska różni się od innych branż pod względem security?

Branża hotelarska jest szczególnie wrażliwa na zmiany gospodarcze, w związku z powyższym, projektując system bezpieczeństwa bądź zarządzając nim, należy brać pod uwagę szerokie spektrum działania. Czynniki zewnętrzne i wewnętrzne organizacji oraz zagrożenia powinny być analizowane na bieżąco.

Co jest najistotniejsze, jeśli chodzi o bezpieczeństwo?

Poczucie bezpieczeństwa jest wartością samą w sobie, a gość przyjeżdżający do obiektu hotelarskiego powinien czuć się bezpiecznie pod każdym względem. W całym systemie bezpieczeństwa obiektów hotelarskich dbamy zatem o bezpieczeństwo gości, zapewniając ochronę fizyczną, cyberbezpieczeństwo czy bezpieczeństwo żywności, jednak przy całym procesie należy pamiętać, iż istotne jest zapewnienie bezpieczeństwa pracownikom i obiektom.

Jak powstają procedury bezpieczeństwa w państwach hotelach?

Procedury bezpieczeństwa muszą być poprzedzone analizą zewnętrznymi i wewnętrznymi uwarunkowań danego obiektu hotelarskiego. Tylko tak przygotowane są adekwatne do danego obiektu.

Jakie sytuacje i incydenty występują najczęściej w państwach hotelach i jak sobie z nimi radzicie?

Zagrożenia występujące w obiektach zmieniają się w czasie. Nie można przyjąć, iż ich występowanie jest stałe, czy też przewidzieć każdą sytuację, niemniej jednak należy się przygotować, czyli szkolić załogę tak, aby była w stanie reagować na sytuacje niestandardowe, stresujące i niebezpieczne.

Jakie rozwiązania z obszaru bezpieczeństwa są interesujące z perspektywy hotelarstwa?

Tematy z obszaru bezpieczeństwa zawsze aktualne to bezpieczeństwo fizyczne gościa czy cyberbezpieczeństwo, biorąc pod uwagę zmieniający się zakres usług informatycznych. Z uwagi na sezon letni nie bez znaczenia jest zwrócenie szczególnej uwagi na bezpieczeństwo żywności.



Iwona Kawecka

Director of Loss Prevention
Warsaw Marriott Hotel

Czym branża hotelarska różni się od innych branż pod względem security?

Nie możemy się zamknąć. Są branże przemysłowe, biznesowe, które są bardzo newralgiczne, bo np. przetwarzają dane osobowe czy produkują niebezpieczny sprzęt. Jeśli nie chcą, aby ktokolwiek postronny miał do nich dostęp, wprowadzają kontrolę dostępu, zatrudniają ochronę, która pilnuje wejścia i nie pozwala osobom z zewnątrz wchodzić do środka. U nas nie ma takiej możliwości. W bardzo dużym stopniu jesteśmy otwarci, do nas może wejść dosłownie każdy z ulicy. Staramy się to ograniczać w rozsądnym stopniu. Poza gośćmi hotelowymi zapraszamy też ludzi do naszych lokali gastronomicznych, które są otwarte. Osoby z zewnątrz, niebędące gośćmi hotelowymi, organizują u nas imprezy, nieraz bardzo duże, na setki czy tysiące osób. Mamy



» Konkurujemy ze sobą na poziomie rezerwacji i sprzedaży, ale jeśli chodzi o bezpieczeństwo, hotele współpracują. «

ogromną przestrzeń konferencyjną, kasyno, bar na czterdziestym piętrze otwarty do późnych godzin, gdzie przychodzi mnóstwo osób. Funkcjonujemy przez całą dobę i jesteśmy cały czas otwarci. To jest główne wyzwanie dla security w branży hotelarskiej.

Jakie procedury, systemy czy praktyki bezpieczeństwa są istotne w hotelu?

Jeśli chodzi o tworzenie procedur, dla każdego hotelu czy dla każdej marki, są one podobne. Bardzo ważne jest to, w jaki sposób meldujemy gości w hotelu, na jakich zasadach osoba ta otrzyma dodatkowy klucz. Mamy klucze, które umożliwiają dostęp do całego budynku, wszystkich pokoi gości. Wiadomo, że dział sprzątający, dział techniczny, room service mają dostęp do pokoi gości. Ważne, na jakich zasadach wydajemy klucze i kto może z nich korzystać, w jaki sposób do nas później wracają i jak są te osoby rozliczane, kto może wejść, kto nie może wejść do pokoju, czy gość może np. w pewnym momencie swojego pobytu powiedzieć: „Od teraz nie życzę sobie, żeby ktokolwiek wchodził do mojego pokoju” i jakie to ma reperkusje. Mamy procedurę podaną przez korporację, ale kluczowy jest też zdrowy rozsądek.

Co jest najistotniejsze, jeśli chodzi o bezpieczeństwo?

Obserwujemy miejsca najbardziej dla nas kluczowe, gdzie, jak wynika z naszego doświadczenia, dochodzi do różnych incydentów. Bar otwarty do późnych godzin nocnych, gdzie jest spożywany alkohol, lobby hotelowe, ogródek, recepcja. Zatrudniamy dodatkową osobę i mamy dodatkowe kamery, które obserwują te przestrzenie, żebyśmy mogli jak najszybciej zareagować na incydenty, które mogą tam się pojawić. Zainstalowaliśmy przyciski alarmowe, za pomocą których recepcjonista może dyskretnie wezwać osobę z ochrony. Ogródek zewnętrzny, przez który mamy styczność z dworcem centralnym i z centrum miasta, gdzie przechodzą ludzie we wszystkich możliwych kierunkach i często są to osoby niekoniecznie pożądane wewnątrz hotelu. Mamy teraz rozszerzoną ochronę, która zna już z widzenia te osoby. Staramy się ograniczać ich wejścia po to, by nasi goście mogli się czuć bezpiecznie i swobodnie korzystać z tego, co im oferujemy.

Jak powstają procedury bezpieczeństwa w państwa hotelach?

Każdy obiekt ma specyficzne wymagania, ale mamy możliwość dopasowywania się do specyfiki w zależności od tego, kogo obsługujemy i w jakim miejscu na świecie się znajdujemy. Inaczej będą wyglądały względy bezpieczeństwa w naszym hotelu, który jest czterdziestotrzypiętrowym budynkiem w centrum Warszawy, a inaczej na obrzeżach Warszawy czy w mniejszej miejscowości. Pewne rzeczy są takie same dla wszystkich. Marka Marriott narzuca nam pewne zasady i są to bardzo mądre zasady, ale bardzo ogólne. My mamy możliwość rozbudowy albo dopasowywania konkretnie do naszych warunków – do tego, ile mamy wejść, w jak wysokim budynku znajduje się hotel, ilu gości przyjmujemy dziennie, jak szeroką mamy przestrzeń konferencyjną, czy jesteśmy powiązani też z czymś innym, np. w naszym budynku mamy nie tylko hotel, ale też część biurową i centrum medyczne.

Jakie sytuacje i incydenty występują najczęściej w państwa hotelach i jak sobie z nimi radzicie?

Najczęstsze incydenty, które się zdarzają, to wtargnięcia, np. na piętra hotelowe osób niepowołanych, spoza hotelu – nie tylko na piętra dla gości, ale również konferencyjne. Pojawiają się osoby, które próbują dokonać kradzieży, niekoniecznie na szkodę gości, ale na szkodę hotelu, np. wejść na nasze zaplecza. Staramy się to ograniczać na tyle, na ile to możliwe. Zainstalowaliśmy kontrolę dostępu w windach hotelowych, czyli windę można włączyć wyłącznie za pomocą karty do pokoju. Zdarza się, że osoba z zewnątrz wchodzi do windy razem z grupą gości hotelowych. Nie od razu jesteśmy w stanie to wychwycić. Mamy oczywiście odpowiednio zaprogramowane zamki, z których możemy wykonać odczyty, mamy monitoring w windach i kamery na pierwszym planie, razem z lobby hotelowym, kamerami zewnętrznymi i w recepcjach. Te przestrzenie są kluczowe i cały czas je obserwujemy. Jeżeli widzimy, że ktoś często np. zjeżdża windą z piętra na piętro, jesteśmy w stanie to wychwycić.

Istotna jest dla nas liczba incydentów, których udało nam się uniknąć dzięki temu, że obserwujemy bacznie przestrzeń, wychytujemy zagrożenia i działamy prewencyjnie. Czasami można nie zauważyć, że interweniowaliśmy. Ścisłe współpracujemy z innymi sieciami hoteli. Konkurencja jest na poziomie działu sprzedaży i działu rezerwacji, natomiast na poziomie security wyłącznie współpracujemy. Współpracujemy też ze służbami – polską policją, ale też z zagranicznymi, m.in. z ambasadą amerykańską.

Jakie rozwiązania z obszaru bezpieczeństwa są interesujące z perspektywy hotelarstwa?

Zdecydowanie doskonalenie monitoringu. Monitoring IP daje dużo więcej możliwości niż analogowy. Odtwarzając wstecznie nagrania, możemy za jego pomocą zrobić zbliżenie i np. przeczytać z gościem gazetę. Podkreślę, że działamy na zasadzie prewencji i chociaż nikt tego nie widzi, jej sukcesem jest to, że udaje się wyeliminować niepożądane zdarzenia.

Wprowadzamy też inne rozwiązania, takie jak kontrola dostępu na naszych zapleczach hotelowych. Kiedyś hotel był znacznie bardziej otwartą przestrzenią, teraz tylko pracownicy albo osoby, którym towarzyszymy albo którym udzielimy rejestrowanego dostępu, mogą tam wejść. W naszych rozwiązaniach mamy tzw. *mobile checkin*, za pomocą którego gość jest w stanie, jadąc z lotniska, zameldować się w hotelu za pośrednictwem Internetu i pobrać klucz do pokoju czy zarezerwować stół w naszej restauracji, też całkowicie zdalnie. Warunkiem jest przystąpienie do naszych programów lojalnościowych, a więc jest to rozwiązanie dla wybranej grupy osób. Taka osoba musi być zarejestrowana od pewnego czasu, udzielić nam wirtualnego dostępu do swojej karty kredytowej. ●

Megavision Technology ogłasza premierę na polskim rynku
nowej linii produktowej profesjonalnych
kamer wysokich rozdzielczości
NEXUS iPRO

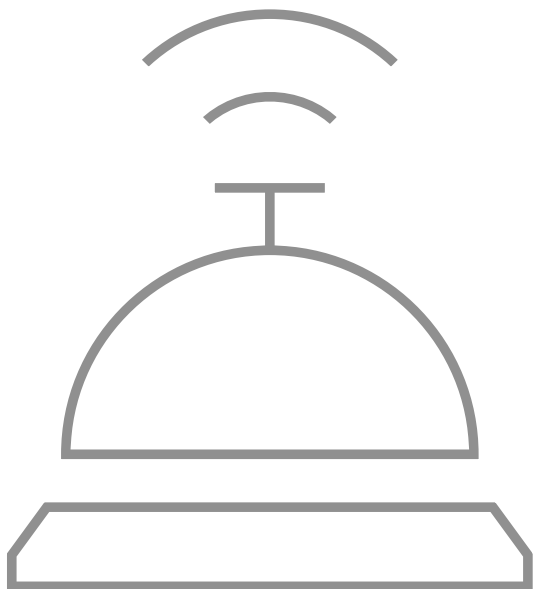
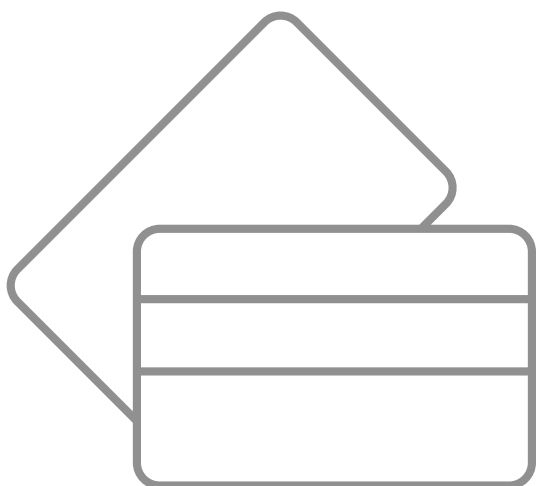


Kamery produkowane są w Korei Południowej zgodnie z wymogami NDAA oraz TAA
zapewniając tym samym najwyższy poziom bezpieczeństwa dla użytkowników



głos branży

Zapewnienie bezpieczeństwa obiektów użyteczności publicznej – banków, hoteli i szkół – stanowi ogromne wyzwanie dla security managerów. W odróżnieniu od wielu budynków IK czy przemysłowych, nie mamy tu wyłącznie świadomej i przeszkolonej załogi, ale wiele zupełnie przypadkowych osób.



Tomasz Krzysztański
NOVOTEL POZNAŃ CENTRUM

Okiem menedżera

Wraz z cyfryzacją i rozwojem techniki XXI wiek przynosi systematyczny wzrost liczby zagrożeń stojących przed zarządzającymi hotelami, a przede wszystkim przed osobami odpowiedzialnymi za bezpieczeństwo obiektów. Mówiąc o bezpieczeństwie, należy brać pod uwagę nie tylko bezpieczeństwo gości hotelowych (konferencyjnych) i pracowników, dostawców towarów oraz usług, ale także bliskiego sąsiedztwa obiektu. Ponosimy odpowiedzialność prawną z zakresu ochrony pożarowej, prawa budowlanego, przetwarzania i ochrony danych osobowych, ale też bezpieczeństwa fizycznego osób przebywających na terenie i dokoła naszego obiektu.

Moje 17-letnie doświadczenie w branży hotelarskiej wskazuje na olbrzymie znaczenie posiadania oraz efektywnego wykorzystywania systemów zabezpieczeń technicznych. W pierwszej

kolejności należy wymienić wszystkie systemy zabezpieczeń technicznych (system sygnalizacji pożarowej SSP, dźwiękowy system ostrzegawczy, system detekcji ulatniania się gazów, system oddymiania, oświetlenie awaryjne z wizualizacją i autotestem, przeciwpożarowy wyłącznik prądu), awaryjne źródła i systemy energii. Ważne jest połączenie tych systemów z zewnętrznymi organami wsparcia ratowniczego (monitoring pożarowy, alarmy napadowe), przy czym sygnały alarmowe o konieczności wsparcia przekazywane są w sposób automatyczny. Muszą one być wspierane przez zdalne monitorowanie poprawności działania przez serwisy specjalistyczne z możliwością interwencji, bez konieczności przyjazdu do obiektu. Coraz częściej jest stosowana okresowa weryfikacja prawidłowości wykonywania czynności obsługowych i konserwacji tych systemów przez zewnętrzne centrum monitorowania, dodatkowo wspierające obiekt.

Bardzo ważne są elementy zabezpieczeń biernych, np. stosowanie odpowiednich materiałów i urządzeń, dodatkowe zabezpieczenie przeciwpożarowe elementów konstrukcyjnych i wyposażenia przy użyciu materiałów odpornych na ogień i działanie wysokich temperatur, wydzielenie stref w obiekcie, tworzenie bariery dla dymu i ognia na terenie dróg ewakuacyjnych itd. Mówimy tutaj o realizacji zobowiązań wynikających z Ustawy o ochronie przeciwpożarowej z 26.08.1991, gdzie w myśl art. 3 ust. 1 tej ustawy właściciele korzystający ze środowiska, budynku, obiektu lub terenu są obowiązani zabezpieczyć je przed zagrożeniem pożarowym lub innym miejscowym zagrożeniem. Równolegle jesteśmy zobowiązani do wypełnienia zobowiązań wynikających z Rozporządzenia Ministra Infrastruktury w sprawie warunków technicznych, jakim powinny odpowiadać budynki i ich usytuowanie z dnia 12.04.2022 (Dz.U. nr 75, poz. 690).

W zakresie realizacji zobowiązań budowlanych warto zgłębić ustawę Prawo budowlane z dnia 7.07.1994, rozdz. 6 *Utrzymanie*. W myśl art. 62 naszym obowiązkiem jest regularne kontrolowanie budynku i jego wyposażenia. Tutaj też warto rozważyć zastosowanie systemów, które pomogą nie tylko przygotować się do kontroli, ale też zapewnić bezpieczeństwo na co dzień.

Szczególnie istotną kwestią dla zapewnienia bezpieczeństwa obiektu jest posiadanie profesjonalnego systemu telewizji dozorowej (CCTV), który przesyła obraz z kamer do wyznaczonego zestawu monitorów i rejestratorów obrazu o właściwych parametrach. Ważne, moim zdaniem, jest zadbanie o odpowiedni dobór kamer (umożliwiających czytelność obrazu w każdych warunkach, w tym zadymienia), ich należytą liczbę oraz właściwą lokalizację i odpowiednie parametry, rejestratory o wystarczająco dużej pamięci i odpowiednim poziomie zapisu w celu archiwizacji obrazu. Bardzo ważne jest bezpieczeństwo i pewność rejestracji, w tym zapewnienie odpowiedniego zasilania w energię oraz przeciwdziałanie możliwości sabotażu. Im dłuższa archiwizacja, tym lepiej (na podstawie Kodeksu pracy nie może jednak być dłuższa niż 3 miesiące) zarówno dla nas, jako zarządcy obiektu, jak i służb, np. policji, które często korzystają z zapisów monitoringu wizyjnego dla weryfikacji zdarzeń mających miejsce dookoła hotelu (zwłaszcza w centrach miast). W parze z posiadanym systemem CCTV rekomenduję zaopatrzenie obiektu i pracowników w tzw. przyciski napadowe, które w przypadku zagrożenia pozwalają szybko uzyskać wsparcie fizyczne. Niejednokrotnie zdecydowanie szybciej aniżeli reakcja służb mundurowych.



Wskazane jest stosowanie kamer i systemów CCTV w windach (zasłabnięcie, działania przestępcze). Ważne jest również monitorowanie ewakuacji osób niepełnosprawnych w sytuacji pożaru lub innego zagrożenia.

Niestety poziom zabezpieczeń często bywa przestarzały, poszczególne systemy działają w sposób niedostatecznie ze sobą skoordynowany. Dlatego w większych obiektach zlokalizowane są centra monitorowania bezpieczeństwa i ratownictwa wyposażone w systemy zbierające informacje ze wszystkich instalacji, a w sytuacji alarmu lub zagrożenia wyodrębniające sektor zagrożenia i pracę systemu zabezpieczeń. Monitoruje również pracę systemów ochrony przeciwpożarowej (zapas wody pożarowej, gotowość lub działanie maszynowni oraz instalacji systemów bezpieczeństwa i wentylacji pożarowej, gotowość źródeł awaryjnych, wyłączenia, awarie i odstawienia). To znacznie zwiększa bezpieczeństwo obiektu. Brakuje odpowiednich norm i polskich przepisów regulujących zabezpieczanie hoteli, musimy implementować normy europejskie.

Podsumowując, pragnę podkreślić znaczenie posiadania systemów zapewniających bezpieczeństwo na wymaganych prawem polach. To niełatwa inwestycja, ale istotna, ponieważ pozwoli skupić się na działalności operacyjnej prowadzonego obiektu. Umożliwia wcześniejszą reakcję zapobiegającą, co znacznie ogranicza zagrożenia i ich skutki.



Radosław Suchodoła
GLOBAL SECURITY PARTNER

Nowoczesne technologie w zarządzaniu hotelami i apartamentowcami

W dzisiejszych czasach skuteczniejsze zarządzanie, lepsze decyzje, większa efektywność i niższe koszty stanowią priorytety w utrzymaniu hoteli i apartamentowców. Wyobraź sobie sytuację, w której gość w hotelu może samodzielnie się zameldować i wymeldować, a bramy lub szlabany otwierają się automatycznie.





Nie musisz już martwić się o włączoną klimatyzację czy otwarte okno w pokoju hotelowym. Klient zostawiający włączone urządzenia elektryczne czy oświetlenie również nie stanowi problemu. To nie musi być tylko wyobraźnia, wszystko to już istnieje. Odpowiednio zaprojektowane systemy zabezpieczeń, automatyka budynkowa oraz nowoczesne technologie hotelowe wspomagają zarządzanie takimi obiektami i pomagają zapomnieć o wielu problemach.

Dzięki tym rozwiązaniom goście mogą cieszyć się samodzielnym meldowaniem i wymeldowaniem, a bramy oraz szlabany otwierają się automatycznie, zapewniając wygodę i swobodę. Kontrola klimatyzacji czy otwartych okien w pokojach staje się sprawą zautomatyzowaną, eliminującą niepotrzebne obawy. Dodatkowo, systemy bezpieczeństwa zapobiegają zostawieniu włączonych urządzeń elektrycznych i oświetlenia przez klientów.

Właściwie wdrożone systemy zabezpieczeń, zintegrowane z automatyką budynkową umożliwiają minimalizację problemów związanych z funkcjonowaniem hotelu. Nowoczesne technologie hotelowe nie tylko poprawiają wydajność i efektywność zarządzania, ale również przyczyniają się do zwiększenia satysfakcji gości. Dzięki nim wszelkie problemy związane z zarządzaniem i utrzymaniem obiektów są skutecznie rozwiązywane, a personel może skoncentrować się na zapewnieniu najwyższej jakości obsługi.



BOGUMIŁ SZYMANEK
AXIS COMMUNICATIONS

Dyskretnie, ale bezpiecznie

Systemy zabezpieczeń odgrywają niezwykle istotną rolę we wszystkich obiektach, gdzie przebywa duża liczba ludzi. W takich miejscach jak hotele, szkoły, uczelnie codziennie pojawiają się pracownicy danej instytucji, pracownicy firm zewnętrznych, goście,

dostawcy, uczniowie, studenci itd. Otwarta formuła sprawia, że potencjalnie zwiększa się ryzyko wystąpienia aktów wandalizmu, kradzieży, niewłaściwego zachowania czy nieautoryzowanego dostępu.

Jednocześnie systemy służące do dozoru nie powinny negatywnie wpływać na poczucie prywatności i komfortu osób.

Osoby odpowiedzialne za bezpieczeństwo stoją przed trudnym zadaniem zabezpieczenia obiektu systemem kamer i kontroli dostępu. Dobierane urządzenia powinny być dyskretne, estetycznie wtapiać się w wystrój wnętrza, a jednocześnie widoczne, aby pełniły funkcję prewencyjną i zwiększały poczucie bezpieczeństwa gości obiektu.

Bardzo często klienci doceniają możliwości nowoczesnych sieciowych systemów audio od Axis. Są one idealnym uzupełnieniem systemów zabezpieczeń, gdyż pozwalają na zdalną komunikację głosową do miejsca zdarzenia oraz wywoływanie automatycznych komunikatów po wykryciu zdarzenia, np. przez kamery z analizą obrazu.

Elastyczność instalacyjna oparta na transmisji IP sprawia, że można łatwo budować systemy kilkuset głośników podzielnym na wiele stref. Rozwiązanie to może zapewnić przyjemny klimat jako źródło muzyki w tle oraz nadawać komunikaty informacyjne i reklamowe wg ustalonych reguł i harmonogramu. W razie potrzeby menedżer może przywołać pracownika albo przekazać bieżące komunikaty. Dodatkową korzyścią jest możliwość zarządzania wieloma, nawet rozproszonymi systemami audio z poziomu jednego interfejsu, np. w przypadku sieci hoteli, wydziałów uczelni, oddziałów szkoły.



Marcin Walczuk
BCS

Zapewnienie bezpieczeństwa w hotelu

W celu zapewnienia wysokiego poziomu ochrony hotele stosują różne systemy zabezpieczeń technicznych, które mają za zadanie wykrywać zagrożenia takie jak kradzieże, sabotaże czy pożary i zapobiegać im. Systemy te są często zintegrowane i współpracują ze sobą, tworząc wielopoziomową i wieloaspektową platformę bezpieczeństwa.

Jednymi z podstawowych systemów zabezpieczeń w hotelach są systemy telewizji dozorowej i kontroli dostępu. Pierwszy pozwala na monitorowanie wszystkich obszarów hotelu za pomocą kamer, z których obraz i ewentualnie dźwięk są zapisywane na rejestratorach. Drugi natomiast umożliwia dostęp do konkretnych pomieszczeń tylko osobom uprawnionym, wykorzystując do tego czytelniki kart, linii papilarnych lub wprowadzenie kodu PIN, które zastępują tradycyjne klucze do pokoi gościnnych.

Kolejnym ważnym ogniwem zabezpieczenia hotelu jest system sygnalizacji pożarowej wraz z systemem oddymiania, DSO oraz oświetleniem ewakuacyjnym i awaryjnym. Całość ma za zadanie samoczynnie wykryć pożar, ostrzec o zagrożeniu i umożliwić szybką ewakuację osób ze strefy zagrożenia.

Niezbędny przy prawidłowym zabezpieczeniu takiego obiektu jak hotel jest system alarmowy antywłamaniowy, ale może nawet bardziej antynapadowy. Takie zabezpieczenie pozwoli reagować na próby włamania lub napadu na recepcję lub inne miejsca w hotelu, wysyłając sygnał do ochrony lub służb ratunkowych. Alarm może być aktywowany przez czujki ruchu, magnetyczne lub po zbitciu szyby albo zostać wywołany ręcznie przy użyciu pilotów lub przycisków napadowych.

Ciekawym uzupełnieniem jest system parkingowy, który kontroluje ruch pojazdów na terenie. Składa się ze szlabanów, bram lub innego typu barier i kamery do rozpoznawania numerów tablic rejestracyjnych. Jego głównym zadaniem jest zapewnienie bezpiecznego ruchu na parkingu, prowadzi również analizę dostępnych miejsc parkingowych oraz zapobiega nieuprawnionemu parkowaniu.

Najlepiej jeśli wszystkie wymienione powyżej systemy zabezpieczeń są kontrolowane i zintegrowane z nadrzędnym systemem typu BMS (*Building Management System*), który wizualizuje wszystkie dane i sygnały związane z bezpieczeństwem.



Krzysztof Mika
HIKVISION POLSKA

Monitorujemy nie tylko bezpieczeństwo

Branża turystyczna i hotelarska, mimo powrotu do normalności po okresie pandemii, wciąż staje przed wieloma trudnościami. W sprostaniu tym wyzwaniom i zapewnieniu najwyższej jakości obsługi coraz większą rolę odgrywają nowoczesne systemy zabezpieczeń. Systemy monitoringu wizyjnego nie tylko podnoszą poziom bezpieczeństwa gości i personelu, ale także mają istotny wpływ na efektywność pracy całego obiektu. Urządzenia, wykorzystując sztuczną inteligencję, potrafią identyfikować obiekty, sygnalizując jedynie istotne zdarzenia dla obsługi hotelowej. Dzięki temu operatorzy mogą skutecznie reagować na sytuacje wymagające natychmiastowej interwencji. Nowoczesne kamery umożliwiają m.in. odczytywanie tablic rejestracyjnych pojazdów, co eliminuje konieczność stosowania tradycyjnych kart parkingowych i zapewnia wygodę gościom.

Systemy monitoringu wizyjnego dostarczają dane przydatne w innych obszarach działalności hotelowej. Kamery pozwalają na śledzenie liczby gości i zapewniają bezpieczeństwo poprzez wykrywanie porzuconego bagażu oraz wtargnięcie osób niepowołanych do strefy tylko dla personelu. Dzięki inteligentnym

funkcjom, np. automatycznej kontroli kolejek, kamery dostarczają cennych informacji dla zarządcy hotelu, ułatwiających podejmowanie działań zarządczych, decyzji marketingowych oraz podnoszących jakość obsługi gości.

Innowacyjne technologie monitoringu wizyjnego przynoszą liczne korzyści dla branży hotelarskiej, zapewniając bezpieczeństwo, wygodę i doskonałą obsługę gości. Systemy monitoringu nie tylko minimalizują fałszywe alarmy, ale także generują cenne dane analityczne. Dzięki temu hotele mogą skutecznie reagować na sytuacje kryzysowe i optymalizować procesy zarządzania.



Błażej Ożga
NEDAP SECURITY MANAGEMENT

Trendy w kontroli dostępu

Żyjemy w świecie ciągle zmieniających się trendów. Spośród setek z nich widać te wyraźnie wyłaniające się, jak (AI), i te, które już straciły nieco na popularności (3D). Jedno jest pewne – powinniśmy trzymać rękę na pulsie, ponieważ dużo się dzieje również w naszej branży. Przyjrzyjmy się zatem temu, co najczęściej pojawia się w prognozach.

Potencjał AI: Dane generowane przez systemy zabezpieczeń, w tym przez KD, stają się coraz ważniejsze. AI może wzmocnić automatyzację poprzez wykorzystanie tego, co oferują nam te dane z potencjalnym zastosowaniem we wszystkich formach kontroli dostępu, zarządzania budynkami, bezpieczeństwa IT, jak również procesów biznesowych. Generowanie raportów czy też wykrywanie anomalii to jedno z nielicznych możliwych zastosowań.

Automatyzacja i integracja: Automatyzacja może nie tylko poprawić reakcję na incydenty i reaktywność systemu, ale także pomóc zaoszczędzić na kosztach. W połączeniu z nowymi technologiami, takimi jak AI i zaawansowana biometria, firmy mogą skuteczniej zabezpieczać obiekty, a dane mogą być gromadzone i wykorzystywane w celu poprawy optymalizacji i budowania większej odporności systemu. Automatyzacja może być kluczowa dla firm, które koncentrują się na cyberbezpieczeństwie i zintegrowanych systemach IT.

On-Premises czy ACaaS (*Access Control as a service*): Współcześni pracownicy oczekują i wymagają większej elastyczności, dlatego nowoczesne miejsce pracy musi być na to gotowe. Modułowa kontrola dostępu jako SaaS może elastycznie dostosowywać się do zmieniających się potrzeb firm, czyniąc je łatwiejszymi w implementacji, proaktywnymi i zorientowanymi na przyszłość. W niektórych przypadkach organizacje mogą wdrożyć połączenie rozwiązań lokalnych i ACaaS. Kluczem do przyszłości bezpieczeństwa w organizacjach jest jednak elastyczność przyjętych rozwiązań.

Potęga chmury: Potęgą technologii chmurowych i natywnej infrastruktury chmurowej doprowadziła do wielu innowacji





w ciągu ostatniej dekady. Coraz częściej platformy dostępne w chmurze oferują firmom korzyści, które mogą mieć wpływ na budżet, wydajność operacyjną i zgodność z przepisami. Elastyczność i zdolność adaptacji będą kluczowe w nadchodzących latach. Firmy mogą podejmować lepsze, skuteczniejsze decyzje dzięki danym osiąganym w czasie rzeczywistym. Ponadto utrzymanie takich systemów jest łatwiejsze, a aktualizacje i dodatki są wdrażane bez przestojów, co jest niezbędne we współczesnych systemach kontroli dostępu.

Biometria: Biometria zagościła w naszym życiu dzięki używaniu urządzeń mobilnych. W połączeniu z coraz większą akceptacją interakcji bezdotykowych oznacza to, że technologie biometryczne, takie jak rozpoznawanie twarzy i głosu lub bezdotykowe czytniki odcisków palców, stają się coraz bardziej realistyczne i skuteczne w systemach kontroli dostępu. Choć z biometrią wiążą się istotne kwestie dotyczące prywatności, to jednak ta technologia ma ogromny potencjał do uproszczenia i optymalizacji systemów KD w przyszłości.



Daniel Kamiński

SMART-I

Wygoda użytkownika wyznacza kierunek KD

Trzy lata po najbardziej znaczącym odejściu od tradycyjnych środowisk pracy pracownicy zaczęli wracać do biur, ale dynamika ich powrotów uległa zmianie. Kiedyś musieli być cały czas na miejscu w biurze, teraz oczekują elastycznych godzin pracy,



środowisk hybrydowych i większej liczby udogodnień. Oczekiwania, które nie podlegały negocjacom, są dzisiaj zaktualizowanymi zasadami, procedurami i procesami zapewniającymi pracownikom, najemcom i mieszkańcom większą wygodę.

Nigdzie ta zmiana nie jest bardziej widoczna, jak w kontroli dostępu. Szczególnie jeśli chodzi o wygodę otwierania drzwi. Z badania przeprowadzonego przez Brivo wśród użytkowników kontroli dostępu wynika, że za najwygodniejsze uznano uwierzytelnianie za pomocą twarzy (51%). Odblokowywanie telefonem (22%) zajęło drugie miejsce, a korzystanie z karty dostępu trzecie (12%).

Respondenci badania wyraźnie podkreślili wygodę jako główną wartość dodaną rozwijającego się mobilnego cyfrowego rozwiązania kontroli dostępu. Mobilna kontrola dostępu została oceniona znacznie wyżej niż w przypadku tradycyjnych kart plastikowych lub breloczków: dwie najczęstsze odpowiedzi odzwierciedlały znaczenie doświadczenia użytkownika.

Wygoda użytkownika jest istotnym trendem nie tylko w dziedzinie bezpieczeństwa, ale także w innych obszarach. Przekłada się to na różne dziedziny życia, korzystanie z kont bankowych, zamawianie biletów na koncerty, korzystanie z opłat drogowych na autostradach czy otrzymywanie recept. Użytkownicy oczekują podobnej wygody w miejscach pracy, dlatego mobilna kontrola dostępu szybko się rozwija.

Aplikacje mobilne dla najemców to kolejny rosnący trend w sektorach przedsiębiorstw i nieruchomości komercyjnych. Pozwalają one pracownikom rezerwować sale na spotkania i prezentacje, zmieniać temperaturę i oświetlenie, poruszać się po dużych budynkach, zgłaszać potrzebę konserwacji, zapisywać się na wydarzenia, a nawet korzystać z rynku usług, takich jak posiłki, dostawa jedzenia i wysyłka paczek.

Wygodna przestrzeń biurowa zachęca użytkowników do powrotów do pracy, dlatego pracodawcy szybko dostosowują swoje biura, aby sprostać nowym wymaganiom pracowników i ich oczekiwaniom w zakresie wygody i dostępności usług mobilnych.

Temat wygody dotyczy również specjalistów ds. bezpieczeństwa. Dzięki mobilnemu dostępowi mogą szybko reagować na incydenty i pytania ze strony biznesu. Na pytanie, jakie problemy chcieliby rozwiązać za pomocą aplikacji, specjaliści ds. bezpieczeństwa wymienili kilka, które ułatwiają im pracę. Należą do nich w szczególności: zdalne zarządzanie drzwiami, natychmiastowe tworzenie, modyfikacja i unieważnianie poświadczeń oraz outsourcing zarządzania i nadzoru nad systemem kontroli dostępu.

Dostęp mobilny dla pracodawcy oznacza niższe koszty związane z dystrybucją kart kontroli dostępu. Spada liczba zagubionych kart, ponieważ personel pilnuje swoich telefonów i ich nie pożycza, co przekłada się na wzrost bezpieczeństwa. Korzystanie z telefonów umożliwia wprowadzenie wieloskładnikowego uwierzytelniania przy użyciu danych biometrycznych (np. rozpoznawanie twarzy i odciski palców), co również zwiększa bezpieczeństwo. Administratorzy nie muszą przebywać w biurze, aby wystawić fizyczną przepustkę, mogą łatwiej zarządzać dostępem i poświadczeniami z dowolnego miejsca. Mobilne systemy kontroli dostępu to teraźniejszość i przyszłość.



Marcin Kamieniorz

ING BANK ŚLĄSKI

Bezpieczeństwo instytucji finansowych

W instytucjach finansowych utrzymywany jest wysoki poziom zabezpieczeń technicznych, co wynika z wielu powodów. Przede wszystkim minimalne wymagania i normatywy znajdują się bezpośrednio w Ustawie o ochronie osób i mienia z dnia 22 sierpnia 1997 r. oraz powiązanych rozporządzeniach MSWiA, a także w regulacji Prawa bankowego oraz rozporządzeniach Prezesa NBP i rekomendacji tzw. regulatorów, m.in. KNE, EBA. Te regulacje określają wymagane obowiązki oraz konieczny dla stosowania minimalny poziom środków i sposobów organizacji bezpieczeństwa fizycznego, co już kwalifikuje te środki na istotnym poziomie jakości i skuteczności.

Kolejnym istotnym czynnikiem wpływającym na wysoki poziom zabezpieczeń technicznych jest wysoka dojrzałość instytucji finansowych w zarządzaniu ryzykiem niefinansowym wynikająca z kilku powodów.

Jednym z najistotniejszych jest przyjęty koszt ryzyka rozumiany jako koszt potencjalnej lub realnej straty finansowej. W analizie biznesowej przyjęty koszt inwestycji w środki dla obniżenia tego ryzyka jest często dużo niższy niż możliwa strata finansowa. Powoduje to konieczność ciągłej analizy stosowanych środków technicznych oraz ich rozwoju, gdyż istotne w tym sektorze jest utrzymanie wysokiej jakości opinii rynkowej, przez co strata wizerunkowa instytucji finansowej jest niepożądana.

Nie mniej ważnym czynnikiem jest dostępny budżet do inwestowania w ten obszar ryzyka. Instytucje finansowe z natury swojej działalności w naturalny sposób inwestują w „narzędzia”, a obszar ryzyka jest nieodłącznym zakresem takiej działalności. Mając na uwadze wysoką wrażliwość w tym obszarze, stosowane środki są niebanalne, a bardzo często zastosowane rozwiązania są na bardzo wysokim poziomie technologicznym i jakościowym.

Dotychczas stosowane techniki i rozwiązania w takich obszarach jak wykrywanie naruszeń dozorowanych powierzchni (detekcja PIR), monitorowanie wizyjne (CCTV), kontrola dostępu są znane już od kilkudziesięciu lat i nadal z powodzeniem są stosowane. Warto podkreślić, że jakość stosowanych czujek, kamer oraz czytników/kart wraz z rozwojem technologii niewątpliwie wzrosła, jednak nie ma i nie spodziewam się istotnej rewolucji w tym obszarze.

W obszarze zabezpieczenia wartości pieniężnych rozwiązania mechaniczne zostały uzupełnione o elementy elektroniczne, które z powodzeniem mapują obszar dostępu (zamki elektroniczne), rejestrują operacje na/w urządzeniu czy wykrywają niepożądane czynności. W tym obszarze również nie spodziewam się istotnego progressu rozwoju tych technologii.

Natomiast warto zwrócić uwagę na kilka kwestii. Zauważam niewykorzystany potencjał biometrii w powszechnych zastosowaniach w obszarze bezpieczeństwa fizycznego. Zastanawiają mnie wciąż występujące obawy i brak akceptacji w systemach kontroli dostępu oraz sygnalizacji włamania, metod autentykacji opartych na biometrii, a jednocześnie zachwywanie się biometrią szeroko stosowaną w smartfonach, które obecnie są naszym „oknem na świat”, portfelem, sejfem, pocztą, pamiętnikiem itp.

Kolejnym obszarem wymagającym, w mojej opinii, uwagi jest bezpieczeństwo danych. Mam tu na myśli urządzenia i systemy stosowane w obszarze zabezpieczeń technicznych. Dotyczy to danych przesyłanych i przetwarzanych przez te systemy i urządzenia – dane spoczynku oraz dane w tranzycie. Z pewnym niepokojem zauważam stosowane systemy kontroli dostępu oparte na jawnych danych na kartach czy protokół Wieganda w transmisji pomiędzy czytnikiem a kontrolerem. Jednocześnie nie należy zapominać, że do systemów kontroli dostępu mamy dedykowane rozwiązania, np. standard OSDP2, który jest skuteczną propozycją dla zabezpieczenia danych w tranzycie.

Podobnie dużym wyzwaniem jest obszar bezpieczeństwa danych wideo w systemach monitoringu wizyjnego (CCTV). Mając na uwadze rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych... (RODO), wizerunek osoby jest daną wrażliwą, a takie dane powinniśmy chronić. Co więcej, ochrona tych danych powinna być zapewniona nie tylko w urządzeniu rejestrującym (DVR/NVR), ale także w czasie transmisji tych danych do oraz z tego urządzenia. Ponadto takie dane skopiowane na nośnik zewnętrzny również podlegają ochronie.

Intryguje mnie także duży potencjał w rozwiązaniach integracji lokalnych systemów zabezpieczeń technicznych, gdzie w naturalny sposób migrujemy te systemy do narzędzi z obszaru IT. Takie rozwiązania pozwalają istotnie zautomatyzować zarządzanie rozproszonymi systemami zabezpieczeń i zapewniają automatyzację pomiędzy nimi, np. sterowanie uzbrojeniem stref alarmowych z systemu kontroli dostępu itp.

Ponadto, jeśli poprawnie zaprojektujemy architekturę takiej integracji oraz zastosujemy wydajne rozwiązania sprzętowe i programowe, uzyskamy również wysoki poziom bezpieczeństwa w transmisji danych przetwarzanych przez systemy zintegrowane. Należy nadmienić, że szeroko rozumiany obszar IT posiada już wysokie standardy i normy bezpieczeństwa, co pozwoli w czasie takiej integracji zastosować wysoko skuteczne rozwiązania w obszarze bezpieczeństwa danych. ●





Monitoring wizyjny kluczem do utrzymania konkurencyjności

Turystyka i hotelarstwo to niezwykle dynamiczny sektor polskiej gospodarki. I choć firmy z tego sektora wróciły do swobodnego funkcjonowania po trudnym okresie pandemii, wciąż mierzą się z wieloma problemami. Wzrost inflacji, niedobory kadrowe oraz zmieniające się preferencje i oczekiwania klientów, to tylko niektóre. Nowoczesne systemy zabezpieczeń pozwalają sprostać wyzwaniom, pomagając przy tym w zachowaniu jak najwyższej jakości obsługi.

Krzysztof Mika

Monitoring wizyjny jest standardem w obiektach hotelowych. Systemy te nie tylko podnoszą poziom bezpieczeństwa gości i personelu, ale także mają znaczący wpływ na efektywność pracy całego obiektu.

Wraz z postępem technologicznym kamery nauczyły się „rozumieć” obrazy, które rejestrują. Za sprawą sztucznej inteligencji kamery Hikvision są w stanie rozróżniać ludzi i pojazdy od innych obiektów, reagując jedynie na zdarzenia istotne dla obsługi hotelowej. Ta umiejętność w znacznym stopniu usprawnia pracę operatorów, z jednej strony ograniczając liczbę fałszywych alarmów, z drugiej – umożliwiając skuteczną reakcję na sytuacje wymagające natychmiastowej interwencji.

Możliwości nowoczesnych kamer wychodzą daleko poza zwykły monitoring wizyjny. W branży hotelowej zastosowanie rozszerzonej analizy obrazu spotkało się z entuzjastycznym przyjęciem. Przykładem takiej analizy jest odczytywanie przez kamery tablic rejestracyjnych pojazdów. Gość, podając numer rejestracyjny podczas rezerwacji, może wjeżdżać na parking hotelowy i wyjeżdżać z niego przez cały okres pobytu, bez konieczności angażowania obsługi lub stosowania tradycyjnych kart parkingowych. Ponadto nowoczesne systemy monitoringu wizyjnego mają możliwość monitorowania stanu zajętości miejsc zarówno na parkingach zewnętrznych, jak i wewnętrznych. Mogą też wyświetlać informacje o lokalizacji zaparkowanego pojazdu, co jest dużym udogodnieniem dla gości i obsługi. Zarejestrowany obraz z kamer może również stanowić niepodważalny materiał dowodowy w przypadku zarysowania lub uszkodzenia pojazdu.

Kolejną innowacją, która zdobyła uznanie branży hotelarskiej, jest możliwość obserwacji kolorowego obrazu nie tylko w ciągu dnia, ale również w nocy, bez względu na warunki pogodowe i oświetleniowe. Firma Hikvision wprowadziła na rynek technologię ColorVu, która zrewolucjonizowała rynek telewizji dozorowej. Tradycyjne kamery, korzystając w nocy z oświetlaczy podczerwieni, mogły transmitować jedynie czarno-białe obrazy, przez co rozpoznawanie szczegółów, zwłaszcza podczas opadów deszczu czy mgły, było utrudnione. Dzięki wprowadzeniu zaawansowanych przetworników obrazu



o wysokiej czułości i szerokiej aperturze kamery ColorVu dostarczają kolorowy obraz przez całą dobę, nawet w trudnych warunkach oświetleniowych.

Technologie dozoru wizyjnego stosowane we współczesnych hotelach mają również zastosowanie w wielu innych obszarach działalności. Na przykład automatyczna kontrola kolejek informuje menedżerów, że liczba oczekujących osób przekracza ustalony limit, sygnalizując potrzebę oddelegowania dodatkowych osób do obsługi recepcji. Kamery monitorujące pozwalają dyskretnie kontrolować, ile osób przebywa w budynku, poza gośćmi hotelowymi, co ma ogromne znaczenie w przypadku przymusowej ewakuacji.

Dla pracowników ochrony, oprócz redukcji fałszywych alarmów dzięki technologii AcuSense, istotne są takie funkcje, jak wykrywanie porzuconych bagaży po określonym czasie, alarmowanie w przypadku dostępu osób niepowołanych do strefy tylko dla personelu, a także ochrona obiektów za pomocą termowizji. Pozwala to skutecznie reagować na obecność osób nieuprawnionych. Kamery, dzięki funkcjom rozpoznawania twarzy, rozróżniają pracowników i pozwalają im swobodnie poruszać się w odpowiednich strefach bez reakcji systemu. Wejście do pomieszczeń ochrony możliwe jest dopiero po weryfikacji uprawnień zapisanych na karcie za pomocą odcisku palca osoby uprawnionej, kodu dostępu lub po rozpoznaniu twarzy.

Nowoczesne systemy monitoringu wizyjnego są również źródłem cennych dla zarządu danych, takich jak informacje demograficzne

dotyczące gości czy też o najczęściej odwiedzanych częściach obiektu, a nawet o preferowanych przez gości atrakcjach. Te statystyki umożliwiają ciągłe doskonalenie działalności hotelu w kontekście zarządzania, marketingu i podnoszenia jakości obsługi gości.

Bezpieczeństwo, wygoda i doskonała obsługa gości są niezwykle ważne dla hoteli, a zastosowanie innowacyjnych rozwiązań pozwala na skuteczne osiągnięcie tych celów. Dzięki postępowi technicznemu kamery są bardziej inteligentne, potrafią rozpoznawać i analizować obrazy, co prowadzi do ograniczenia do minimum liczby fałszywych alarmów i skuteczniejszej reakcji na sytuacje wymagające interwencji. Systemy telewizji dozorowej nie tylko zapewniają bezpieczeństwo, ale także umożliwiają optymalizację procesów zarządzania, poprawę jakości obsługi oraz generowanie cennych danych do analizy i podjęcia odpowiednich decyzji. Nagrania rejestrowane przez telewizję dozorową okazują się też przydatne, gdy na terenie obiektu dojdzie do złamania prawa. W dobie dynamicznego rozwoju branży hotelarskiej oraz specyficznych wyzwań inwestycja w nowoczesne technologie monitoringu wizyjnego jest kluczowa dla utrzymania konkurencyjności i zapewnienia obsługi najwyższej jakości. ●



Hikvision Poland

ul. Żwirki i Wigury 16B, 02-092 Warszawa

michal.swoboda@hikvision.com

<https://www.hikvision.com/europe/>



Bezprzewodowy system zarządzania zamkami hotelowymi ZKTeco

Bezpieczeństwo, wydajność i eleganckie wzornictwo zawsze miały kluczowe znaczenie dla branży hotelarskiej. Aby zaspokoić potrzeby tych użytkowników, firma ZKTeco oferuje rozwiązanie składające się z bezprzewodowego zamka hotelowego i specjalistycznego oprogramowania. Dzięki niemu smartfon gościa może stać się cyfrowym kluczem do hotelowego pokoju.

Bezprzewodowy zamek do drzwi nie wymaga okablowania i wzajemnych połączeń między elementami systemu, co znacznie ułatwia jego instalację oraz sterowanie nim. Komunikacja i przesyłanie danych między zamkami a kontrolerami odbywa się za pomocą protokołu Zigbee HA. Jeden kontroler ZigBee obsługuje do 6 zamków drzwiowych, których w systemie może być nieograniczona liczba. Jeden serwer może obsłużyć 2000 wejść, a połączenie kilku serwerów pozwoli obsłużyć ich aż 8000. Jest to więc rozwiązanie idealne dla bardzo dużych

obiektów. Po podłączeniu zamka do systemu i ustawieniu jego parametrów goście hotelowi do otwarcia drzwi mogą używać zarejestrowanych kart bądź smartfonu.

Oprogramowanie hotelowe

Zamki hotelowe ZKTeco współpracują z oprogramowaniem ZKBioHLMS będącym modyfikacją znanego w kontroli dostępu oprogramowania ZKBioSecurity. Umożliwia ono przyznawanie gościom hotelowym prawa dostępu do pokoi oraz wind w określonym

przez recepcję przedziale czasowym. Natomiast personel hotelu może bezpośrednio w programie sprawdzić poziom zasilania zamków drzwiowych, dyspozycje gości typu „Nie przeszkadzać” bądź to, czy aktywny jest status „Drzwi otwarte”. Dzięki temu obsługa gości jest bardziej dyskretna. ZKTeco umożliwia administratorom systemu rejestrację wszystkich rezerwacji, na ich bazie generując informacje statystyczne o liczbie zameldowanych i wymeldowanych danego dnia gości, stanie obłożenia hotelu, a także wybrane informacje finansowe. Oprogramowanie zapewnia bezpieczne przesyłanie danych, wykorzystując do tego protokół HTTPS.

Obsługa za pomocą smartfona

ZKTeco wykorzystuje technologię opartą na chmurze, stosując do komunikacji z serwerem standard HTML5. Dzięki temu goście mogą poprzez przeglądarkę internetową na własnym urządzeniu mobilnym zdalnie otwierać drzwi do swoich pokoi hotelowych oraz bezpłatnie korzystać z dostępnych w aplikacji funkcji.

Po rejestracji goście otrzymują od hotelu wiadomość SMS lub e-mail powitalny, szczegóły dotyczące rezerwacji oraz link służący do otwarcia drzwi. Mogą też skorzystać z Mobilnego Asystenta Obsługi Pokoju, by np. skontaktować się z recepcją. Kliknięcie na link rejestracyjny pozwala sprawdzić lokalizację hotelu za pomocą GPS.

Hotel może łatwo dostosować aplikację do swoich wymagań, umieszczając w niej swoje logo, zdjęcia obiektu czy dane kontaktowe. Te nowoczesne, a zarazem proste rozwiązania są dobrze odbierane przez potencjalnego klienta.

Inne cechy systemu

- Zamki hotelowe ZKTeco obsługują karty dostępowe RFID Mifare.
- Rozwiązanie „jedna karta” zapewnia gościom możliwość wejścia za pomocą tej samej karty do wszystkich udostępnianych im pomieszczeń, np. sali konferencyjnej, fitness, SPA i na parking.
- Personel hotelowy, programując dostęp do wind, może ograniczyć możliwość wyjścia z windy tylko do pięter, do których dana osoba ma przyznany dostęp.
- ZKTeco oferuje API do integracji swojego oprogramowania z aplikacjami innych firm. ●



ZKTeco Europe

Carretera Fuencarral 44, Edificio 1,
Planta 2, 28108 Alcobendas, Madryt
marek.piotrowski@zkteco.eu
www.zkteco.eu



NOWOCZESNE ROZWIĄZANIE HOTELOWE

System On Line obsługi inteligentnych zamków hotelowych



Kompatybilny z oprogramowaniem
ZKBioHLMS



Oprogramowanie hotelowe

TCP/IP



Bramka ZigBee

ZigBee



Bezprzewodowy zamek hotelowy

Rozwiązanie ZKTeco Smart Lock nie wymaga stosowania okablowania łączącego elementy systemu co znacznie ułatwia i obniża koszty instalacji sieci kontrolującej stany zamków drzwiowych stosowanych w biurach i hotelach. Bezprzewodowa komunikacja i przepływ danych pomiędzy zamkami a oprogramowaniem ZKBio HLMS realizowana jest za pomocą protokołu Zigbee.

Oprogramowanie to umożliwia podgląd stanu zasilania dowolnego zamka. Dzięki wbudowanemu modułowi windy personel może również nadawać gościom prawa dostępu do wind.

ZAMKI

ZL500



ZL600



ZL700





Kompletna infrastruktura sieciowa w hotelu

Zapewnienie stabilnego i szybkiego połączenia sieciowego to obecnie jedno z głównych wyzwań, przed jakim stają administratorzy takich miejsc, jak hotele, restauracje i kawiarnie, by sprostać rosnącym wymaganiom i utrzymać wysoki poziom satysfakcji gości. Nowo powstały Focus Hotel Premium Warszawa postanowił całą infrastrukturę sieciową zbudować z wykorzystaniem rozwiązań oferowanych przez TP-Link.

Rozwiązanie

Zdecydowano się na wdrożenie kompleksowego systemu Omada SDN od TP-Link. Celem wdrożenia było stworzenie wydajnej sieci przewodowej oraz Wi-Fi na terenie całego obiektu dla gości hotelowych, a także do obsługi systemu POS, terminali płatniczych oraz na potrzeby biurowo-administracyjne. Dodatkowym założeniem było także stworzenie infrastruktury niezbędnej do prawidłowego funkcjonowania kamer CCTV i telewizji hotelowej IPTV.

Wyzwanie

Ze względu na dużą powierzchnię budynku oraz 13 kondygnacji, włącznie z garażem podziemnym, zdecydowano się na rozmieszczenie lokalnych punktów dystrybucyjnych na każdym piętrze połączonych z główną serwerownią.

Szkielet sieci stanowią dwa 8-portowe switchy SFP+ 10G TL-SX3008F znajdujące się w głównym punkcie dystrybucyjnym. Dzięki zastosowaniu połączeń światłowodowych i wkładek 10G TL-SM5110-LR uzyskano bardzo szybkie połączenia pomiędzy wszystkimi 11 lokalnymi punktami dystrybucyjnymi znajdującymi się na każdym z 11 pięter budynku.

W lokalnych punktach dystrybucyjnych zastosowano dwa rodzaje urządzeń. W większych punktach dystrybucyjnych oprócz przełączników PoE TL-SG3428XMP oraz dostępowych TL-SG3452 wykorzystano również przełącznik agregujący TL-SX3008F, którego zadaniem jest umożliwienie szybkiego połączenia 10G bez tworzenia „wąskich gardeł” w sieci lokalnej. Trzy większe punkty dystrybucyjne odpowiadają za podłączenie nie tylko punktów dostępowych, ale także obecnych w obiektach kamer IP i zapewnienie dostępu do sieci przewodowej.

Osiem mniejszych punktów dystrybucyjnych wyposażono w przełączniki TL-SG3428XMP mające 24-gigabitowe porty RJ45 PoE+ służące do zasilania i zapewnienia komunikacji z punktami dostępowymi EAP615-Wall. Ponadto ten model przełącznika posiada 4 złącza SFP+ 10G, które zostały wykorzystane do połączenia z serwerownią oraz pozostałymi znajdującymi się tam przełącznikami.



łącznie wykorzystano 20 przełączników PoE TL-SG3428XMP, 10 przełączników TL-SG3452 oraz 3 switchy TL-SG3428X, które zapewniają dostęp do sieci lokalnej i Internetu zarówno przewodowo, jak i bezprzewodowo za pomocą zastosowanych punktów dostępowych Omada.

Dostęp do sieci Wi-Fi odbywa się za pomocą 174 punktów dostępowych z serii Omada. W częściach wspólnych obiektu zamontowano łącznie 24 urządzenia. W salach konferencyjnych zastosowano 5 sufitowych punktów dostępowych EAP620 HD przeznaczonych do pracy w najbardziej obciążonych miejscach, gdzie z Internetem łączy się wielu użytkowników jednocześnie. W pozostałych miejscach użyto 19 sufitowych Access Pointów EAP610. Oba modele pracują w najnowszym standardzie Wi-Fi 6.

Z kolei za dostęp do sieci bezprzewodowej w pokojach hotelowych odpowiada 150 kompaktowych punktów dostępowych Wi-Fi 6 EAP615-Wall. Urządzenia te zostały zamontowane w co drugim pokoju, w puszkach elektrycznych w konstrukcji biurka, dzięki czemu są niewidoczne.

Wszystkie urządzenia w sieci są zarządzane za pomocą kontrolera sprzętowego Omada OC300. Na kontrolerze skonfigurowano osobne SSID powiązane z VLAN. Dzięki takiemu rozwiązaniu hotel posiada



Focus Hotel Premium Warszawa

Focus Hotel Premium Warszawa to nowoczesny, 4-gwiazdkowy obiekt charakteryzujący się oryginalnym designem, doskonałą lokalizacją oraz świetną ofertą konferencyjną. W nowo otwartym budynku znajdują się 234 przestronne komfortowe pokoje. Hotel dysponuje 1370 m² nowoczesnej powierzchni konferencyjnej. W jej skład wchodzi m.in. sala balowa o powierzchni 637 m², 8 sal konferencyjnych – każda o powierzchni 55 m² – oraz foyer o powierzchni 310 m². Do dyspozycji gości oddano przestronną restaurację, która pomieści do 200 osób.



osobną sieć bezprzewodową dla gości oraz osobną sieć przewodową i bezprzewodową dla pracowników hotelu.

Rezultaty

Montaż i instalacja urządzeń przebiegła sprawnie, bez najmniejszych problemów. Dzięki wdrożeniu goście zyskali dostęp do sieci Wi-Fi o wysokiej przepustowości na terenie całego obiektu. Również systemy CCTV i telewizji hotelowej działają zgodnie z przyjętymi założeniami.

– Sieć bazująca na urządzeniach TP-Link działa stabilnie, goście zyskali możliwość korzystania z bezprzewodowego Internetu na terenie całego obiektu. Bezproblemowego działania systemu dowodzą też opinie na popularnym portalu booking.com. Obiekt może się pochwalić bardzo wysoką średnią ocen w kategorii Bezpłatne Wi-Fi 9,3/10 przy blisko 200 opublikowanych opiniach – mówi Daniel Dzierba, dyrektor generalny, Focus Hotel Premium Warszawa. ●



TP-Link Polska

ul. Ożarowska 40/42, 05-850 Duchnice

www.tp-link.com.pl

robert.gawronski@tp-link.com



Systemy do bezobsługowych obiektów hotelowych

Rynek branży hotelowej po licznych kryzysach się skurczył. Odczuwalne są też trudności w pozyskaniu pracowników z odpowiednimi kwalifikacjami. Dlatego ważnym elementem jest dobór narzędzi umożliwiających bezobsługową pracę obiektu hotelowego i skupienie się na obsłudze gości pod kątem ich komfortowego pobytu w obiekcie i poza nim.

Na potrzeby obiektów bezobsługowych najdogodniejsze będzie wdrożenie systemów umożliwiających zdalne zarządzanie kontrolą dostępu oraz temperaturą w apartamentach, a także automatycznym zarządzaniem energią elektryczną zależnie od obecności gości w apartamencie. Dodatkowym rozwiązaniem jest system awizacji pojazdów oraz automatycznej kontroli wjazdu na parking i wyjazdu z niego.

Kontrola dostępu – zamki apartamentowe SmartLock

Zamki apartamentowe SmartLock występują w wersji nakładkowej (zamiast sztyldów) i są montowane do istniejących drzwi bez ingerencji w ich konstrukcję. Źródłem zasilania zamków są baterie 4 x AAA pozwalające na rok pracy przy 24 cyklach otwarć dziennie.

W Global Security Partner zajmujemy się projektowaniem, dystrybucją i kompleksową dostawą najnowocześniejszych rozwiązań dla budownictwa oraz elektronicznych systemów zabezpieczeń. Bogate doświadczenie pozwala nam odczytywać potrzeby klientów i wprowadzać na rynek produkty, które spełniają ich oczekiwania. Razem z naszymi partnerami, firmą SALUS Controls, z którą projektujemy automatykę budynkową dla branży grzewczej i firmą Premnet jesteśmy w stanie zaprojektować i wykonać instalacje na obszarze całego kraju.

Zamki SmartLock mają trzy interfejsy:

- **Bluetooth** – zarządzanie chmurowe, programowanie, otwieranie lokalne i zdalne;
- **PIN-kod** – przypisywanie kodów PIN spersonalizowanych dla gości na określony czas (od dnia ... do dnia, od godziny ... do godziny);
- **RFID** – programowanie stałe, czasowe i cykliczne kart zbliżeniowych RFID przypisanych do apartamentu.

Zamki są obsługiwane za pomocą aplikacji chmurowej TLock instalowanej na smartfonach lub przez dowolną przeglądarkę WWW. Do zarządzania zamkami online służy bramka komunikacyjna, która z zamkami łączy się przez Bluetooth, a z Internetem przez Wi-Fi. Zamki SmartLock występują w wersji z wbudowaną bramką komunikacyjną Bluetooth/Wi-Fi.

Dostępne są warianty do montażu w drzwiach oraz do sterowania elektrozaczepem, bramą, szlabanem parkingowym i dowolną automatyką.

Salus Controls – system sterowania temperaturą

Komfortową temperaturę w pokojach zapewni gościom system Salus Controls umożliwiając sterowanie temperaturą i klimatyzacją w pomieszczeniach. Sterowanie może odbywać się lokalnie, zdalnie oraz automatycznie wg harmonogramów i scenariuszy.

Podstawowymi elementami systemu są regulatory ściennie z czujnikami temperatury i wilgotności sterujące inteligentnymi głowicami w grzejnikach bądź siłownikami w głowicach rozdzielczych ogrzewania wodnego. Wszystkie urządzenia działają w technologii bezprzewodowej ZigBee i za pośrednictwem bramki komunikacyjnej umożliwiają zdalną regulację temperatury oraz harmonogramów.

SaveKey PIR – bezkartowe włączniki prądowe

Idealne rozwiązanie, które nie utrudnia gościom pobytu, a jednocześnie dba o oszczędzanie energii w czasie ich nieobecności, to włączniki prądowe SaveKey PIR. Pracują one w dwóch trybach:

- **„gość w pokoju”** – po rozłączeniu kontaktronu w drzwiach i wykryciu ruchu włącza strefy zasilania (światło, gniazda 230 V, inne urządzenia);
- **„brak gościa w pokoju”** – po rozłączeniu kontaktronu w drzwiach i braku ruchu włącza strefy zasilania (światło, gniazda 230 V, inne urządzenia).

Zmiana trybu pracy następuje po otwarciu drzwi i rozłączeniu kontaktronu. Czujka PIR wykrywa ruch lub jego brak i przekazuje sygnał do stycznika w rozdzielni elektrycznej, który włącza lub wyłącza obwody energetyczne. Dodatkowym atutem włącznika jest możliwość podłączenia go do regulatora temperatury Salus i automatyczne sterowanie temperaturą w zależności od obecności gości w apartamencie. ●



Global Security Partner

ul. Lęborska 3b, 80-286 Gdańsk
www.gspartner.pl
gk@gspartner.pl



NOVUS
MANAGEMENT
SYSTEM



INTELIGENTNY NADZÓR WIZYJNY OBIEKTU

NOWOŚĆ

Novus Management System VSS umożliwia połączenie wielu systemów monitoringu wideo w jednym oprogramowaniu. Daje możliwość podglądu i rejestracji nieograniczonej programowo liczby strumieni wideo. Novus Management System VSS łączy systemy analogowe oraz IP, daje również wszelkie narzędzia wspomagające pracę administratora, operatora i użytkownika.



JAK TO DZIAŁA?

NMSVSS.AAT.PL

NOVUS MANAGEMENT SYSTEM VSS to profesjonalne rozwiązanie dla systemów dozoru wizyjnego

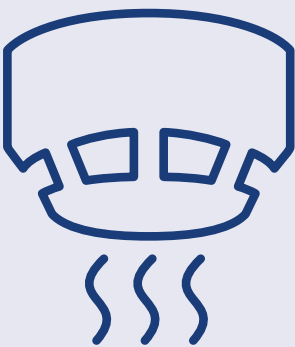
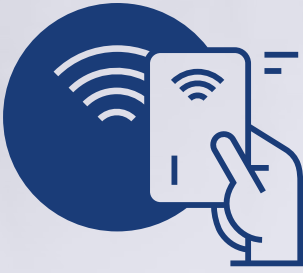
Do nabycia u najlepszych instalatorów!

AAT SYSTEMY BEZPIECZEŃSTWA

PRODUCENT I DOSTAWCA ELEKTRONICZNYCH SYSTEMÓW ZABEZPIECZENIA MIENIA
www.aat.pl



BEZPIECZNE HOTELE



Współczesne hotele: pełen komfort i dyskretna ochrona

Kontrola dostępu, telewizja dozorowa, sygnalizacja pożarowa, dźwiękowy system ostrzegawczy czy system parkingowy odgrywają ważną rolę w codziennym zarządzaniu hotelem. Dostarczenie pakietu „wszystko w jednym”, współgrającego z posiadanymi systemami do zarządzania usługą, jest kolejnym wyzwaniem dla branży zabezpieczeń. Jednak jest to wyzwanie, które opłaca się podjąć.

Jan T. Grusznic





» Popyt na kontrolę dostępu w różnych sektorach, w tym w hotelarstwie, stale rośnie w tempie 8,7% rocznie. Firmy z branży nieustannie poszukują sposobów na ulepszenie poprzednich technologii w celu poprawy wydajności, bezpieczeństwa klientów i jakości usług.«

Bezpieczeństwo w hotelu zaczyna się od kontroli dostępu

Hotele dysponujące niewielką liczbą pokoi na ogół wykorzystują tradycyjne rozwiązania kontroli dostępu w postaci kluczy fizycznych. W przypadku zgubienia lub przypadkowego zabrania klucza przez gościa trzeba dorobić nowy, a bywa, że konieczna jest wymiana wkładki lub jej prze-programowanie. Aby zmniejszyć to ryzyko (i związane z nim koszty), do hotelowych kluczy dodawane są nieporęczne breloki. Gdy proceder gubienia kluczy jest nagminny, pozostaje tylko wprowadzenie elektronicznego systemu kontroli dostępu.

Najbardziej popularne w tym względzie są karty-klucze RFID ze względu na ich niską cenę i łatwość obsługi. Choć karty równie łatwo zabrać lub zgubić, jak klucze, to jednak ich zablokowanie i wydanie duplikatu jest szybsze, tańsze i łatwiejsze. Rozwiązanie to może mieć charakter samodzielnego systemu kontroli dostępu (zwanego także systemem offline), który sprawdza się w mniejszych obiektach i który można szybko wdrożyć bez dużych nakładów finansowych. Wymagane jest tylko podstawowe sterowanie: czytnik lub klawiatura (najczęściej zintegrowane z szyldem zamka), brelok lub karta zbliżeniowa oraz zasilanie (najczęściej jest to bateria montowana w szyldzie od strony pokoju). Każde drzwi można odblokować tylko za pomocą karty-klucza, który został wydany upoważnionemu użytkownikowi. Ograniczeniem tego rozwiązania jest brak centralnego zarządzania i kontrolowania drzwi. Nie zawsze istnieje też możliwość weryfikacji historii użycia zamka. Każdy klucz elektroniczny jest ręcznie dodawany do każdego indywidualnego kontrolera drzwi, czyli inaczej niż w przypadku kontroli dostępu online, która umożliwia centralną zmianę i aktualizację uprawnień.

System kontroli dostępu online pozwala monitorować przemieszczanie się wszystkich osób na terenie całego obiektu w czasie rzeczywistym. Prawidłowo skonfigurowany zapewnia dostęp określonym osobom do wybranych obszarów w różnym czasie. Na przykład gościom hotelowym można przyznać dostęp do piętra, na którym jest ich pokój, windy, basenu hotelowego czy do restauracji, ale uniemożliwić np. wjazd na inne piętro. Coraz częściej stosowany w hotelach jest system kontroli dostępu właśnie do windy. Zapewnia to bezpieczeństwo gościom, gdyż zapobiega jej nieautoryzowanemu użyciu. W windy hotelowe stanowią niewralgiczny punkt łączący część ogólnodostępną ze wszystkimi piętrami hotelu, dlatego warto zadbać o to, aby nie korzystały z nich osoby postronne.

Kontrola dostępu do pokoju hotelowego nie ogranicza się wyłącznie do otwarcia drzwi. Może być wykorzystana również do włączenia zasilania w pokojach, czyli włączenia telewizora, światła lub dostępu do wyposażenia pokoju hotelowego, np. minibaru. Klucze szyfrowe na karcie są przypisane do poszczególnych pomieszczeń lub stref (m.in. parking, SPA), które są dobierane na podstawie rezerwacji, umożliwiając gościom korzystanie z atrakcji znajdujących się w obiekcie.

Według raportu MarketsandMarkets Reserach Private Ltd. *Access Control Market Industry Report Size, Share, Growth Drivers, Trends, Opportunities, 2030* popyt na kontrolę dostępu w różnych sektorach, w tym w hotelarstwie, stale rośnie w tempie 8,7% rocznie. Firmy z branży nieustannie poszukują sposobów na ulepszenie poprzednich technologii (kart dostępu, czytników kart itp.) w celu poprawy wydajności, bezpieczeństwa klientów i jakości usług.

Jedną z najbezpieczniejszych metod kontroli dostępu jest biometria, która wielokrotnie sprawdziła się w miejscach, w których konieczne jest zapobieganie nieautoryzowanemu wejściu i zagwarantowanie, że tylko upoważniony personel może do nich wejść. Rozwiązania dostępu biometrycznego są jednak drogie i obwarowane wieloma legislacyjnymi obostrzeniami, dlatego nie można ich swobodnie stosować w takich obiektach, jak hotele. Ich użycie ogranicza się zatem do sejfów instalowanych w pokojach hotelowych. Choć większość jest wyposażona w tradycyjny zamek szyfrowy, to coraz popularniejsze stają się zamki wykorzystujące właśnie biometrię, np. odciski palców.

Zapewnienie nowego poziomu doświadczeń związanych z korzystaniem z usług hotelowych jest możliwe przez wykorzystanie coraz popularniejszych, także mobilnych, systemów dostępu. Wykorzystanie smartfonu gościa do przeprowadzenia procesu meldunku, uczynienie z niego karty dostępu do pokoju i umożliwienie za pomocą telefonu zakupu dodatkowych usług staje się trendem w hotelach „bezobsługowych” oraz obiektach wynajmujących apartamenty na krótki okres. To rozwiązanie wykorzystuje łączność przez Bluetooth Low Energy (BLE), zapewniającą wysoką efektywność energetyczną i wydajność (urządzenia wykorzystujące BLE mogą pracować miesiącami bez konieczności wymiany baterii) do śledzenia zasobów, kontroli dostępu, nawigacji w pomieszczeniach i wyświetlania ukierunkowanych treści.

Nawet mały pożar to duży kłopot

W maju br. w jednym z hoteli w Nałęczowie wybuchł pożar. Dzięki przeprowadzonej przez pracowników akcji ewakuacyjnej nikt nie ucierpiał. W akcji gaśniczej brało udział 40 zastępów z PSP i OSP oraz ok. 160 strażaków, sama akcja gaśnicza trwała 12 godzin. Hotel obecnie nie funkcjonuje, a straty oszacowano na miliony złotych. To tylko jedno z takich zdarzeń. W roku 2022 w Polsce odnotowano 410 pożarów przy ponad 9766 obiektach hotelowych i noclegowych działających w kraju. To oznacza, że do pożaru doszło w niemal 4% obiektów. Większość z nich nie miała tak niszczycielskiego przebiegu jak ten w nałęczowskim hotelu. Były to pożary małe, obejmujące niewielką powierzchnię do 70 m², co można zinterpretować jako spalanie się pojedynczego pokoju hotelowego.

Niezależnie jednak od wielkości pożaru zawsze należy poinformować wszystkich użytkowników o zagrożeniu i szybko przeprowadzić ewakuację. Do alarmowania i ewakuacji osób w obiektach hotelowych najczęściej są stosowane systemy sygnalizacji pożarowej (SSP) i dźwiękowe systemy ostrzegawcze (DSO). Jednak nie w każdym przypadku. Na podstawie obowiązujących przepisów dotyczących wymogu korzystania z urządzeń ppoż. systemy sygnalizacji pożarowej należy stosować w obiektach hotelowych oferujących więcej niż 50 miejsc noclegowych. Te mniejsze muszą być wyposażone jedynie w stałe elementy gaśnicze, plany ewakuacji, oświetlenie awaryjne, główny wyłącznik zasilania energią i instrukcję bezpieczeństwa pożarowego.

Tymczasem wczesna detekcja pożaru dzięki zastosowaniu wielokryterialnych czujek pożarowych, pozwala na niezwłoczne zaalarmowanie osób przebywających w obiekcie. Podstawowym źródłem alarmu są przede wszystkim sygnalizatory akustyczne uzupełnione o sygnalizatory optyczne. Instalacja tych ostatnich jest szczególnie ważna dla osób niesłyszących, a także w pomieszczeniach, w których ze względu na panujące warunki sygnalizatory akustyczne byłyby nieskuteczne. Ciekawym rozwiązaniem są sygnalizatory adresowalne, które w przypadku wykrycia pożaru mogą być uruchomione w konkretnym pokoju hotelowym. Jest to bardzo wygodne, ponieważ najpierw są powiadamiane osoby w zagrożonym pomieszczeniu. Dopiero po weryfikacji i potwierdzeniu pożaru alarm jest uruchamiany w całej strefie. Projektanci chętnie sięgają też po sygnalizatory adresowalne akustyczno-głosowe, gdyż w hotelach, w których nie ma obowiązku stosowania dźwiękowego systemu ostrzegawczego, znacznie przyspieszają ewakuację. Na rynku są dostępne urządzenia, które mogą mieć wgrywane komunikaty w różnych językach oraz programowalne sekwencje sygnałów akustycznych i głosowych. Jest w nich programowalny także poziom natężenia emitowanego dźwięku czy synchronizacja.

W obiektach hotelowych powyżej 200 miejsc noclegowych konieczny jest dźwiękowy system ostrzegawczy. Jego zadaniem jest m.in. zapewnienie możliwości rozgłaszania sygnałów ostrzegawczych i komunikatów głosowych. Właściwe informacje przekazywane w komunikatach decydują o prawidłowym zachowaniu się osób przebywających w obiekcie. Komunikaty muszą zawierać istotne wytyczne wskazujące konkretne postępowanie. Pozwala to uniknąć paniki i niepożądanych reakcji, a tym samym usprawnia i przyspiesza ewakuację.

Zastosowania DSO nie ogranicza się jedynie do alarmowania w przypadku zagrożeń, chociaż to bez wątpienia ich podstawowa funkcjonalność. Można je wykorzystywać również na wiele innych sposobów, np.

- jako radiowęzeł,
- do nadawania komunikatów reklamowych,
- w celu zapewnienia tła muzycznego w obiektach.

DSO można również integrować z innymi systemami, np. audio-wizualnymi, co pozwala na wspólne korzystanie z instalacji i głośników DSO. Tak obszerny wachlarz dodatkowych funkcji systemów DSO pozwala połączyć kilka systemów nagłośnienia w jednym.

Hotel to nie tylko pokoje dla gości. Zazwyczaj mieszczą się w nim restauracja, bar, sale konferencyjne, siłownia, basen czy SPA. W każdym z takich miejsc gość powinien się czuć komfortowo. To priorytet. W każdej z tych stref inwestor może potrzebować odrębnego nagłośnienia, by emitować odpowiednie tło muzyczne lub nadawać komunikaty informacyjne, co właśnie może zapewnić system DSO.






Bezpieczeństwo już od progu

O zadowolenie i bezpieczeństwo gościa hotelowego należy zadbać, gdy tylko przekracza próg obiektu, a w wielu przypadkach jest nim... hotelowy parking. Istotna jest więc wygoda wjazdu i wyjazdu, odpowiednio duże miejsca parkingowe, a dla obsługi – kontrola obłożenia. Kluczowym elementem nowoczesnych systemów parkingowych są kamery ANPR (*Automatic Number Plate Recognition*), które przechwytyują numery tablic rejestracyjnych wjeżdżających i wyjeżdżających pojazdów. Numery te stają się identyfikatorami połączonymi z kontem gościa. Takie rozwiązanie

zwiększa poziom bezpieczeństwa. Rejestracja pojazdów na podstawie tablic rejestracyjnych daje obsłudze zawsze aktualne informacje o tym, które pojazdy znajdują się na parkingu, a które go opuściły i kiedy. Tradycyjne nadzorowanie miejsc parkingowych wymaga dużych nakładów i jest nieekonomiczne. Dzięki rozwiązaniom identyfikującym pojazdy można je zautomatyzować. System natychmiast poinformuje obsługę, że np. konkretny pojazd przekroczył czas parkowania lub został postawiony na miejscu przysługującym innemu gościowi (więcej o systemach ANPR w artykule *Odczyt tablic rejestracyjnych – przegląd rozwiązań* opublikowanym w „A&S Polska” 1/2023).



» Tradycyjne nadzorowanie miejsc parkingowych wymaga dużych nakładów i jest nieekonomiczne. Dzięki rozwiązaniom identyfikującym pojazdy można je zautomatyzować. «

Kamery – im mniej widoczne, tym lepiej

Dobrze zaprojektowane i, co ważne, poprawnie wdrożone nowoczesne systemy dozoru wizyjnego okazują się bardzo skutecznym narzędziem zarządzania hotelem czy ośrodkiem wypoczynkowym. Zapewniają zespołom zarządzającym na miejscu analizę niezbędną, by usprawnić świadczenie usług. Systemy obecne na rynku, w tym kamery, zostały wyposażone w zaawansowane analizy zawartości obrazu, często bazujące na algorytmach uczenia maszynowego bądź sztucznej inteligencji. Analiza wideo przeprowadzana przez AI dowiodła swojej wartości w wielu aplikacjach, umożliwiając szybkie wykrywanie zagrożeń, weryfikację i reakcję.

Dzięki zastosowaniu rozwiązań sieciowych osoby obsługujące system kamer dozorowych w hotelach nie muszą już tkwić godzinami przed monitorami, aby nadzorować całą nieruchomość. Zamiast tego, dzięki zdalnemu dostępowi, mogą mieć dostęp, np. na smartfonie, do obrazu z kamer w czasie rzeczywistym z dowolnego miejsca. Dzięki sztucznej inteligencji i bezpiecznemu połączeniu internetowemu możliwe jest zwiększenie efektywności i przeglądanie materiału ze zdarzenia zaraz po otrzymaniu informacji o nim. To właśnie w tym obszarze zdalnego monitoringu i usług wirtualnej ochrony AI okazuje się szczególnie korzystna dla hoteli. Usługi zdalnego dozoru obsługiwane przez sztuczną inteligencję, w tym nadzór operacji biznesowych, rozszerzają możliwości systemu dozoru wizyjnego, wykorzystując algorytmy AI do wykonywania pracochłonnych i kosztownych zadań związanych z ochroną i monitorowaniem na miejscu. Odciażają hotelowe zespoły ochrony, a jednocześnie zapewniają użytkownikom całodobowy dostęp do monitoringu. Ten rodzaj wirtualnej ochrony pozwala hotelom zaoszczędzić na kosztach związanych z zatrudnianiem pracowników ochrony.

Systemy zabezpieczeń powinny być jednak dyskretne, aby goście nie czuli się inwigilowani. Na szczęście producenci rozumieją ten aspekt i obiektom, takim jak pensjonaty czy hotele, oferują rozwiązana praktycznie dla gości niedostrzegalne, a jednocześnie zapewniające niezawodną ochronę.

W wysocze konkurencyjnej branży hotelarsko-gastronomicznej niezbędne jest zbieranie i przechowywanie informacji o tym, co dzieje się w budynku i jego otoczeniu. Dane gromadzone z urządzeń monitoringu pozwalają obsłudze na bieżąco reagować na różne wydarzenia, ale także umożliwiają planowanie przyszłości.

Oprogramowanie do analizy obrazów z kamer dozorowych może agregować dane gromadzone przez długi czas, dzięki czemu marketing, operacje i inne działy mogą generować raporty i oceniać trendy zachowań gości. Dane prezentowane w formie graficznej ułatwiają ich analizę, pozwalając ich operatorom wychwycić kluczowe wzorce i normy. Po zdefiniowaniu norm mogą oni skonfigurować logikę zdarzeń w celu wyzwalania alarmów w przypadku wykrycia nietypowych zdarzeń.

Warto jednak pamiętać, że nowoczesne technologie niosą nowe zagrożenia, gdyż mogą być celem cyberataków. Przykładem może być atak hakerów na austriacki Seehotel Jägerwirt, w 2017 r. Za pomocą *ransomware'u* hakerzy zablokowali zamki hotelowe, a następnie zażądali okupu. Z kolei w 2018 r. eksperci z F-Secure znaleźli poważną lukę w systemie inteligentnych zamków jednego z uznanych producentów, która umożliwiła utworzenie karty master na podstawie dowolnej karty dostępu.



» Należy zadbać nie tylko o instalację inteligentnych systemów zabezpieczeń, ale przede wszystkim o to, by one same były chronione przed niepożądanym dostępem. «

Te przykłady pokazują, że należy zadbać nie tylko o instalację inteligentnych systemów zabezpieczeń, ale przede wszystkim o to, by one same były chronione przed niepożądanym dostępem. Nikt nieproszony nie powinien kręcić się po hotelowym korytarzu i nikt obcy nie powinien buszować w systemach chroniących gości. •



Funkcja AcuPick do szybkiego przeszukiwania nagrań

Sukces biznesowy obiektu hotelowego zależy od umiejętności zapewnienia gościom jak najlepszych wrażeń z pobytu. Bezpieczeństwo jest priorytetem dla każdego hotelu, dlatego inwestycji w tym obszarze nie brakuje. Systemy monitoringu wizyjnego oparte na najnowszych technologiach odgrywają kluczową rolę w zapewnianiu bezpieczeństwa oraz doskonałej obsługi gości w hotelach.

Kamery umieszczone w strategicznych miejscach, takich jak hol, korytarze, klatki schodowe, parkingi czy wejścia pomagają w zapobieganiu kradzieżom, włamaniami i innym incydentom. Otwarte środowisko hotelu, z dużą liczbą gości

i personelu sprawia, że w razie potrzeby odtworzenia przebiegu zdarzeń na podstawie zarejestrowanych obrazów trzeba przeanalizować ogromną ich ilość. Z myślą o ułatwieniu tego zadania Dahua Technology wprowadziła w kamerach

i rejestratorach funkcję AcuPick. Jej działanie polega na tym, że wizerunek każdej osoby i pojazdu pojawiających się w obszarze obserwowanym przez kamery jest analizowany i opisywany w postaci metadanych.

Za pomocą AcuPick wystarczy na obrazie na żywo lub zapisanym zaznaczyć osobę albo pojazd, a system przeszuka nagrania ze wszystkich kamer w obiekcie oraz wskaże, kiedy i gdzie przebywała dana osoba. Dzięki temu odtworzenie przebiegu zdarzeń jest możliwe za pomocą tylko dwóch kliknięć.

Zastosowanie tej funkcji zapewnia menedżerom i osobom odpowiedzialnym za bezpieczeństwo w obiekcie lepszą świadomość sytuacyjną przy minimalnym ich zaangażowaniu.

Funkcja AcuPick jest dostępna w kamerach IPC S(5-S3) i SD5A/6AL oraz rejestratorach NVR5-EI.

Więcej informacji na temat AcuPick znajduje się na stronie internetowej Dahua Technology. Pomoc przy wyborze modeli można uzyskać u Autoryzowanych Partnerów Sprzedaży.



Więcej na

<https://www.dahuasecurity.com>



TNV-7011RC – kamera do montażu narożnego z szerokim polem widzenia

Hanwha Vision wprowadza na rynek model TNV-7011RC – nowoczesną, wyróżniającą się na rynku, kompaktową kamerę narożną. Urządzenie to oferuje szerokie pole widzenia (FOV) w rozdzielczości 3 Mpix i częstotliwości 30 kl./s. TNV-7011RC to najświeższa propozycja z cenionej serii Wisenet T, przystosowana do pracy nawet w najbardziej wymagających warunkach środowiskowych.

Kamera TNV-7011RC o eleganckim i praktycznym designie została stworzona z myślą o montażu w narożnikach pomieszczeń i wind. Jej unikalna kon-

strukcja nie tylko świetnie komponuje się z przestrzenią, ale także utrudnia zasłanianie obiektywu oraz próby oderwania kamery od ściany.

TNV-7011RC jest wyposażona w funkcję trybu korytarzowego, która umożliwia efektywne monitorowanie wysokich i wąskich przestrzeni. Uzupełnieniem tej funkcjonalności jest technologia Dark IR 940 nm, zapewniająca zasięg do 10 m i umożliwiającą obserwację nawet bardzo ciemnych obszarów.

Kamery z serii Wisenet T odznaczają się szerokim zakresem dynamiki (WDR).

TNV-7011RC generuje obraz stworzony z czterech klatek rejestrowanych przy różnych poziomach ekspozycji, co przekłada się na uzyskanie pełnego, jasnego obrazu, nawet w miejscach o silnym kontraście oświetlenia.

TNV-7011RC to też kamera z inteligentnymi funkcjami analizy obrazu wspieranymi przez AI. Dzięki temu operatorzy mogą szybko wykrywać różnorodne zdarzenia, od detekcji intruza po wałęsanie się. Kamera jest zdolna do wykrywania dźwięków, co pozwala na identyfikację potencjalnych incydentów, takich jak krzyki czy tłuczone szkło. Wykorzystuje technologię kompresji WiseStream II i kodek H.265, dzięki czemu zmniejsza zapotrzebowanie na pamięć masową i przepustowość o 75% w porównaniu do standardowej kompresji H.264.

TNV-7011RC jest idealnym rozwiązaniem dla sektora hotelowego łączącym zaawansowane funkcje z dyskretnym designem. Praktycznie niewidoczna dla gości kamera zapewnia im wysoki poziom bezpieczeństwa, nie naruszając ich prywatności.

Więcej na

<https://hanwhavision.eu/pl/>





ASSA ABLOY



TESA Hotel – system kontroli dostępu dostosowany do rosnącego zapotrzebowania branży hotelowej

TESA ASSA ABLOY, wchodząca w skład Grupy ASSA ABLOY, światowego lidera w zakresie rozwiązań kontroli dostępu, nieprzerwanie pracuje nad rozwiązaniami dla sektora hotelowego, czego efektem jest system kontroli dostępu TESA Hotel.

Dzięki systemowi z wieloma dedykowanymi elementami wykonawczymi można zredukować kolejki przy rejestracji, korzystając z dostępu przyznanemu na urządzenie mobilne lub kodu PIN, które gość otrzymuje przed przybyciem do hotelu. Inteligencja i niezawodność kryją się w każdym drzwiach – elementy są autonomiczne i nie wymagają okablowania, a plan otwarcia jest zapisany indywidualnie w pamięci każdego urządzenia: okucia, zamka, cylindra, czytnika, zamka szafkowego, sejfów.

System TESA Hotel zabezpiecza obiekt przed dostępem niepowołanych osób, a jednocześnie – dzięki zastosowaniu przerywacza prądu redukującego pobór energii elektrycznej – staje się częścią planu optymalizacji kosztów. Inteligentny przerywacz w połączeniu z kartą hotelową będzie odporny na manipulowanie, np. metodą „na wizytówkę”. Skalowalność systemu pozwala na dostosowanie rodzaju licencji do rosnących

potrzeb obiektu. Dostępne są następujące tryby pracy:

Read&Write – tryb standardowy, z kartą jako bezprzewodowym nośnikiem danych o dostępie,

Openow – rozbudowuje poprzednią licencję o dostęp mobilny (dostępy mogą być przyznawane również na urządzenia mobilne z systemami iOS lub Android), *Wireless Online* – uruchamia bezprzewodową komunikację online elementów wykonawczych z systemem poprzez huby komunikacyjne rozlokowane w obiekcie.

Dodatkową funkcjonalnością jest nadrzędne zarządzanie systemem z jednego punktu.

Ostatni poziom licencji to *Checkin PIN* – tryb, który pozwoli na ustanowienie kodu PIN do drzwi oraz dystrybucję kodu przez e-mail. Rozwiązanie to jest szczególnie przydatne, gdy recepcja nie funkcjonuje 24 godziny na dobę.

Więcej na

<https://www.assaabloy.com/pl/>



VCN

VRent i VnetLPR Hotel – automatyzacja i kontrola dostępu dla hoteli

Zarządzający hotelami doceniają rozwiązanie VnetLPR Hotel za poprawę jakości obsługi gości i usprawnienie procesu zameldowania i wjazdów. Dysponują zawsze aktualną informacją w czasie rzeczywistym o tym, kto przebywa na terenie obiektu. Dzięki zastosowanym rozwiązaniom personel hotelowy ma więcej czasu na inne zadania, a goście mogą cieszyć się bezproblemowym wypoczynkiem, bez konieczności częstego odwiedzania recepcji.

W celu usprawnienia działania hotelu można zastosować:

- System VnetLPR sterujący szlabanem na wjeździe na teren obiektu. Szlaban otworzy się automatycznie (bezobsługowo) po zidentyfikowaniu tablicy rejestracyjnej auta przyjeżdżającego gościa. Po zakończonym pobycie
- awizacje na wjazd i wyjazd automatycznie wygasają.
- Portal do awizacji dla gości dostępny przez przeglądarkę www. Pozwala na samodzielne rezerwowanie pobytu z dowolnego miejsca bez angażowania pracowników hotelu. Goście mogą też zaznaczyć usługi, z których chcą korzystać.



System automatyzacji i kontroli dostępu do hoteli

- System VRent – portal do rezerwacji usług dodatkowych (kortów, SPA, fitness itp.). Po dokonanej rezerwacji klient otrzymuje kody dostępowe przez e-mail czy SMS-em.
- Hotelowe zamki elektroniczne zapewniające bezpieczny i wygodny sposób dostępu tylko osobom upoważnionym.
- Integrację z systemami hotelowymi, co eliminuje papierowe ankiety i ręczne wprowadzanie danych niezbędnych do meldunku.
- Telefon z aplikacją do kontroli, czy dany pojazd ma prawo pobytu na parkingu hotelowym.

Dzięki VnetLPR Hotel zarządzający hotelami zyskują m.in. przyspieszenie procesu obsługi gości i zmniejszenie kolejek na wjeździe na teren obiektu. System sterowania szlabanem i automatyzacja dostępu do przestrzeni hotelowych tylko dla uprawnionych osób minimalizuje zaangażowanie obsługi hotelowej. Bardzo przydatne jest też narzędzie do sprawniej kontroli prawa pobytu pojazdów i szybki dostęp do bieżącej informacji o pojazdach znajdujących się na terenie hotelu, dające pełny obraz sytuacji.

Więcej na www.vcn.pl



Wysokiej klasy skarbiec hotelowy z najnowszym certyfikatem T2

Podróżujemy coraz częściej, przewożąc nierzadko ważne dokumenty czy cenne przedmioty. Dlatego chcąc kompleksowo zadbać o potrzeby swoich gości, nowoczesny hotel musi zapewnić nie tylko wygodę i atrakcyjność wypoczynku, ale także poczucie bezpieczeństwa.

Doskonałym rozwiązaniem jest utworzenie skarbcza hotelowego, który nie musi być ogromnym pomieszczeniem za ciężkimi drzwiami – zamiast tego może przybrać formę sejfów mieszczących kolumny skrytek depozytowych. W związku z tym warto przywrócić się produktom z nowym atestem T2. W efekcie ostatniej ewaluacji europejskiej normy EN 1143-1 dotyczącej m.in. sejfów i szaf listę narzędzi wykorzystywanych w testach włamaniowych wzbogacono o sekcję T2, a pierwsze produkty z nowym certyfikatem są już dostępne w ofercie Gunnebo. Zgodnie z aktualną wersją atestu sejfy DuoForce T2 oraz TriForce T2 wykazują potwierdzoną rygorystycznymi badaniami odporność na włamanie z użyciem narzędzi o zdecydowanie większej mocy niż narzędzia znane z wcześniejszych testów certyfikacyjnych.



Prezentowane sejfy chronią nie tylko przed atakami mechanicznymi i próbami włamania, ale także przed ogniem. Co więcej, TriForce T2 jest także odporny na działanie materiałów wybuchowych. Ponadto można w nim zastosować ochronę przed przerwieniem wiertłem diamentowym. To pierwszy na rynku sejf, w którym ta opcja nie spowoduje unieważnienia certyfikatu ognioodporności!

Sejfy renomowanej marki Chubb Safes cechują się nie tylko najwyższym poziomem bezpieczeństwa – oba modele oferują też

szeroki wybór wyposażenia wewnętrznego, a szczególnie ciekawe wykorzystanie dostępnej przestrzeni stanowią skrytki depozytowe. Przy ich użyciu nawet w niewielkim pomieszczeniu można utworzyć prawdziwy skarbiec hotelowy. Dzięki temu goście będą mogli cieszyć się spokojem ducha zarówno w dużym ośrodku wypoczynkowym, jak i niewielkim hotelu butikowym.

Więcej na

<https://www.gunnebosafestorage.com/pl-PL/>

Gunnebo



Rozwiązania Bosch gwarancją szybkiej i pewnej detekcji pożaru

Seria urządzeń AVENAR firmy Bosch w każdym obiekcie zapewni możliwie najszybszą i pewną detekcję pożaru. Mogą być montowane z powodzeniem w hotelach w pokojach gościnnych, salach konferencyjnych, na terenie restauracji, a nawet w saunie.

W obiektach hotelowych bardzo ważna jest estetyka. Tu sprawdzi się niewidzialna płaska czujka serii 500, optyczna lub optyczno-chemiczna z wirtualną komorą pomiarową. Zupełnie płaska konstrukcja ogranicza osadzanie się kurzu i umożliwia pracę w trudnych warunkach.

Do obiektów użyteczności publicznej, takich jak hotele czy ośrodki wczasowe firma Bosch poleca czujki serii AVENAR 4000, które zapewniają bardzo precyzyjne i szybkie wykrywanie pożaru. Charakteryzują się one najwyższą odpornością na fałszywe alarmy i reagują na szeroki



zakres pożarów. Wersje z dwoma detektorami optycznymi (dualną detekcją optyczną) są w stanie wykryć najlżejsze oznaki dymu dzięki technologii Dual-Ray. Wersje z czujką termiczną wykrywają pożary o gwałtownym wzroście temperatury lub o maksymalnej temperaturze. Wysoką niezawodność i dokładność uzyskano dzięki technologii inteligentnego przetwarzania sygnałów (ISP). Najnowszy model – czujka punktowa serii FAP-425-DOTCO-R – łączy w sobie czujniki termiczne, dualoptyczne i chemiczne. To nowe urządzenie oprócz funkcji wykrywania ognia i dymu wykrywa tlenek węgla (CO) zgodnie z normami EN54-26, EN54-30, EN54-31. Zapewniając kompatybilność z istniejącą gamą systemów Bosch Avenar, czujka dodatkowo wzmacnia funkcje automatycznych czujek pożarowych z rodziny AVENAR. Systemy FPA/AVENAR i jego elementy składowe spełniają wymagania prawne obowiązujące w Polsce i posiadają stosowne dokumenty potwierdzające możliwość ich zastosowania w ochronie przeciwpożarowej budynków.

Więcej na

<https://www.boschsecurity.com/pl>

Bosch Security System

GEUTEBRÜCK



your individual
security solution

WWW.LEDAVI.TECH

● L E D A V I
● T E C H

Geutebrück
official partner
for Poland, Baltics
and Ukraine



Po raz kolejny przedstawiamy Państwu mapę dużych inwestycji, które są w trakcie realizacji lub dopiero się rozpoczną, a których termin ukończenia nie upływa przed I kwartałem 2024 r. Tym razem prezentujemy przede wszystkim projekty, które związane są z produkcją energii, dostarczaniem gazu i przesyłem informacji. Słowem wyjaśnienia – szykując dla Was ten wybór, nie skupiamy się na żadnej konkretnej dziedzinie przemysłu. Szukamy przede wszystkim dużych inwestycji prowadzonych przez renomowane firmy, w których widzimy szansę na współpracę dla podmiotów sektora security. Jednocześnie polecamy Państwa uwadze dwa poprzednie numery „A&S”, w których zamieściliśmy wiele innych przedsięwzięć o długim czasie realizacji.

Adela Prochyra, a&s Polska

Mapa inwestycji



BUDIMEX

Co: GENERALNA REALIZACJA GAZOCIĄGU WARSZAWSKIEGO

Gdzie: Rembelszczyzna-Mory, na północny zachód od Warszawy

Kiedy: I połowa 2025 1

Co: BUDOWA CENTRUM INFORMATYKI RESORTU FINANSÓW

Gdzie: Radom 2

Kiedy: 2025

ELEKTROTIM S.A.

Co: BUDOWA LINII ŚWIATŁOWODOWYCH POMIĘDZY KOMPLEKSAMI W M. GDYNIA, RUMIA, ŁĘŻYCE, WEJHEROWO, RZUCEWO WRAZ Z UZYSKANIEM NIEZBĘDNYCH ZGÓD, UZGODNIENI, DECYZJI I POZWOLEŃ – UMOWA ZAWARTA ZE SKARBEM PAŃSTWA – CENTRUM ZASOBÓW CYBERPRZESTRZENI SIŁ ZBROJNYCH

Gdzie: Gdynia, Rumia, Łężyce, Wejherowo, Rzucewo

Kiedy: 570 dni od dnia przekazania terenu budowy 3

ENOX SP. Z O.O.

Co: PRZEBUDOWA OCZYSZCZALNI ŚCIEKÓW DLA AGLOMERACJI PIENIĘŻNO

Gdzie: gmina Pięńszyno

Kiedy: 31.10.2024 4

GOSPODARSTWO ROLNE

Co: BUDOWA TARGOWISKA MIEJSKIEGO WRAZ Z INFRASTRUKTURĄ

Gdzie: gmina Kolbuszowa

Kiedy: sierpień 2025 5

MIRBUD

Co: SZKOŁA PODSTAWOWA WRAZ Z SALĄ GIMNASTYCZNĄ

Gdzie: Szczepne, gmina Grodzisk Mazowiecki

Kiedy: 450 dni od daty zawarcia umowy 04.07.2023 6

MOSTOSTAL PŁOCK

Co: NOWY ZBIORNIK DO MAGAZYNOWANIA ROPY NAFTOWEJ DLA PKN ORLEN WRAZ Z INFRASTRUKTURĄ TOWARZYSZĄCĄ

Gdzie: Płock

Kiedy: 27 miesięcy od daty przekazania terenu budowy 7

Co: PREFABRYKACJA I MONTAŻ 4 ZBIORNIKÓW W RAMACH PROJEKTU HYDROKRAKINGU OLEJÓW BAZOWYCH LOTOS OIL

Gdzie: Gdańsk

Kiedy: 29 tygodni od daty przekazania fundamentu ostatniego zbiornika, co powinno nastąpić nie później niż 20.04.2023 r. 8

NEXEN TECHNOLOGY

Co: PRZEBUDOWA I ROZBUDOWA STACJI UZDATNIANIA WODY W ZAWONIU

Gdzie: Gmina Zawonia

Kiedy: 26.12.2023 9

POLIMEX MOSTOSTAL

Co: BUDOWA INSTALACJI FOTOWOLTAICZNYCH WRAZ Z INFRASTRUKTURĄ TOWARZYSZĄCĄ I WYPROWADZENIEM MOCY – PV ŻÓŁTAŃCE 1 (MOC DO 5 MW), ŻÓŁTAŃCE 2 (MOC DO 5 MW), ŻÓŁTAŃCE 3 (MOC DO 5 MW)

Gdzie: Żółtańce, woj. lubelskie

Kiedy: 31.07.2024 10

UNIBEP

Co: ZABUDOWA UKŁADU KONDENSACJI SPALIN ZA KOTŁEM K1 W ELEKTROCIĘPŁOWNI SIEKIERKI W WARSZAWIE

Gdzie: Warszawa

Kiedy: IV kwartał 2025 11



Wraz ze świadomością rośnie i zmienia się rynek

Zewnętrzny wandal i wewnętrzny szpieg gospodarczy, złodziej albo sabotażysta – to dopiero początek długiej listy zagrożeń, na jakie muszą być przygotowane niemal wszystkie obiekty w Polsce. Coraz częściej model zarządzania budynkiem oparty jest na bliskiej współpracy facility managera z profesjonalnym operatorem zewnętrznym. Jak wygląda branża zarządzania nieruchomościami? – o tym Aleksandra Czapska rozmawia z Tomaszem Grzelakiem, CEO w Stay Safe Poland, Security Inspektorem w DPD Polska, przewodniczącym grupy ds. bezpieczeństwa w Polskiej Radzie Facility Managementu.

Od stycznia 2023 r. w branży usług zarządzania nieruchomościami widać pewne ożywienie. Czy jest ono również zauważalne w inwestycjach w bezpieczeństwo?

To prawda, po chwilowej stagnacji na rynku rok 2023 przyniósł niewątpliwie wzrost zainteresowania usługami firm specjalizujących się w zarządzaniu nieruchomościami. Takie ożywienie ma oczywiście dobrą stronę, pozytywnie wpływając na rentowność firmy zajmujących się tego typu usługami, ale też widzę pewne zagrożenia. Ożywienie w branży zarządzania nieruchomościami to skutek m.in. większej świadomości klientów na temat zagrożeń oraz związanej z nimi potrzeby wprowadzenia odpowiednich środków ochronnych. A to oczywiście poprawia bezpieczeństwo obiektów. Firmy zarządzające nieruchomościami zaczynają zwracać większą uwagę na szkolenie pracowników, audyty bezpieczeństwa, wdrażanie odpowiednich standardów i procedur. Niestety, większe zainteresowanie usługami zarządzania nieruchomościami ma też pewien negatywny aspekt, ponieważ może skutkować brakami kadrowymi, niedostatecznym szkoleniem personelu z zakresu bezpieczeństwa, niedostateczną kontrolą podczas budowy czy też zwiększonym ryzykiem zagrożeń zewnętrznych.

Aby zapewnić odpowiednio wysoki poziom bezpieczeństwa facility managerowie powinni m.in. dokonywać szczegółowej analizy ryzyka przeprowadzanej osobno dla każdego obiektu, chcąc zidentyfikować i ocenić potencjalne ryzyko związane z bezpieczeństwem. Na podstawie takiej analizy powinni następująco:

- wdrożyć nowe procedury lub zmodyfikować obowiązujące, by uwzględniały wykryte zagrożenia, wytyczne i sposoby przeciwdziałania nim oraz środki zapewniające skuteczną ochronę;
- wprowadzić regularne szkolenia personelu; firmy zarządzające nieruchomościami muszą inwestować w szkolenia pracowników, aby potrafili odnaleźć się w każdej sytuacji kryzysowej;

- rozważyć współpracę z profesjonalistami ds. bezpieczeństwa, choćby po to, by przeprowadzili audyt bezpieczeństwa, doradzili w zakresie nowoczesnych rozwiązań technicznych i pomogli w opracowaniu skutecznych strategii bezpieczeństwa;
- stale monitorować sytuację na rynku; bezpieczeństwo obiektów powinno być regularnie kontrolowane i oceniane, skutkując dokonywaną na bieżąco modernizacją środków ochronnych, by w ten sposób zapewnić odpowiedni poziom ochrony nieruchomości.

Po pandemii może nie wszyscy, ale z pewnością wielu pracownicy wróciło do pracy stacjonarnej. Firmy zachęcają ludzi do tego kroku, ale czy równie chętnie inwestują w systemy bezpieczeństwa lub ich modernizację?

Owszem, organizacje inwestują w różnego rodzaju nowe rozwiązania, choćby dlatego, że część pracowników została przyjęta do pracy w trakcie pandemii lub tuż po zniesieniu obostrzeń. Bywa więc, że współpracownicy nie znają się osobiście. Spore zainteresowanie dotyczy urządzeń bezdotykowych minimalizujących konieczność fizycznego kontaktu. Powodzeniem cieszą się czytniki zbliżeniowe i systemy rozpoznawania twarzy.

Dodam, że inwestycje w systemy bezpieczeństwa nie ograniczają się tylko do biurów. Wiele przedsiębiorstw, co mnie bardzo cieszy, ma świadomość zagrożeń i rozszerza wdrażanie systemów również w innych rodzajach nieruchomości, takich jak centra handlowe, szkoły, hotele, aby zapewnić bezpieczne warunki pracownikom i klientom.

Jakie wyzwania stoją przed działami security w budynkach?

Zapewnienie bezpiecznego środowiska pracy jest najważniejszym zadaniem działów zajmujących się bezpieczeństwem danego obiektu przy czym zadanie to dotyczy aspektu bezpieczeństwa zarówno fizycznego, jak i technicznego. Ważna jest nie tylko ochrona przed włamaniami i napadami, ale też szybkie i skuteczne reagowanie na incydenty, takie jak pożary, wypadki, ataki terrorystyczne lub inne zagrożenia życia i mienia. Działy security muszą być odpowiednio przygotowane, aby zarządzać tego typu sytuacjami. Muszą mieć wypracowane procedury ewakuacyjne, alarmowe, a także współpracować z odpowiednimi służbami ratunkowymi i organizować cykliczne szkolenia dla personelu w zakresie reagowania na kryzysy. Zapewnienie odpowiedniego poziomu bezpieczeństwa nie jest możliwe bez skutecznych systemów, dlatego kolejnym wyzwaniem jest odpowiedni wybór, wdrożenie oraz późniejszy nadzór nad zabezpieczeniami technicznymi, opracowanie skutecznych strategii, instrukcji użytkowania i ich aktualizacja.

I na koniec wyzwanie, o którym mało się mówi, ale które jest jednym z największych wyzwań dla działów security, a mianowicie zapobieganie działaniom przestępczym ze strony pracowników. Mogą to być kradzieże, szpiegostwo przemysłowe, sabotaż, wandalizm lub przestępstwa finansowe. Konieczne jest zatem zadbanie o wdrożenie środków minimalizujących ryzyko takich incydentów, np. systemów monitoringu wizyjnego, kontroli dostępu, procedur audytowych i szkoleń.

Jakie perspektywy widzi Pan dla rozwoju tego segmentu? Czy facility management rozwija się głównie w dużych miastach, czy dotyczy też nieruchomości usytuowanych w mniejszych miejscowościach?

Na rynku usług zarządzania nieruchomościami kształtuje się tendencja do wzrostu znaczenia profesjonalnego zarządzania nieruchomościami.

» Wraz ze wzrostem świadomości wśród zarządców nieruchomości oraz rosnącym zapotrzebowaniem na profesjonalne usługi można oczekiwać dalszego rozwoju tej branży w Polsce. «

Ludzie są coraz bardziej świadomi korzyści z efektywnego zarządzania obiektami, wdrożeń innowacyjnych technologii i mają coraz większą świadomość ekologiczną, co przyczynia się do zwiększonego zapotrzebowania na profesjonalne usługi facility managementu w różnych lokalizacjach.

Należy podkreślić, iż rozwój gospodarki, a wraz z tym infrastruktury w naszym kraju spowodował, że wiele firm buduje obecnie swoje obiekty poza dużymi aglomeracjami, ponieważ oznacza to np. mniejszy koszt zakupu gruntu, jednocześnie lepszy dostęp do tras szybkiego ruchu czy infrastruktury kolejowej, a w późniejszej perspektywie niższy koszt utrzymania zakładu.

Biorąc pod uwagę fakt, iż często są to duże przedsiębiorstwa mające wdrożone odpowiednie standardy w swoich obiektach rozsiadanych w całym kraju lub na świecie znajdują one korzyści płynące z profesjonalnego zarządzania nieruchomościami. Ponadto skuteczne zarządzanie może przynieść oszczędność kosztów, automatyzację procesów i poprawę efektywności operacyjnej, co zachęca przedsiębiorstwa do skorzystania z profesjonalnych usług facility managementu.

Jak polski segment facility management wygląda na tle Europy i świata?

W porównaniu ze światowym rynkiem facility managementu polski segment ma jeszcze pewien dystans do pokonania w stosunku do najbardziej rozwiniętych krajów, takich jak Stany Zjednoczone czy niektóre kraje Europy Zachodniej. Jednak rozwój polskiego rynku jest widoczny i dynamiczny. Polscy usługodawcy zyskują na znaczeniu.

Na naszym rynku funkcjonują zarówno duże międzynarodowe firmy, jak i lokalne podmioty specjalizujące się w różnych obszarach facility managementu. Wzrasta także liczba polskich firm świadczących wysokiej jakości usługi w tym obszarze, które coraz śmielej ruszają z ekspansją na rynki zagraniczne. Również polscy specjaliści nie mają się czego wstydić, ich wiedza, doświadczenie, umiejętności pozwalają im konkurować z kolegami z innych krajów. Wraz ze wzrostem świadomości wśród zarządców nieruchomości oraz rosnącym zapotrzebowaniem na profesjonalne usługi można oczekiwać dalszego rozwoju tej branży w Polsce. ●

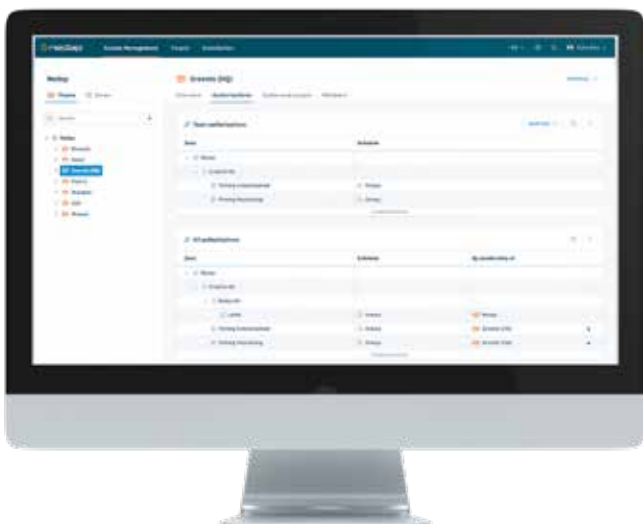


Access AtWork® - usługa kontroli dostępu w chmurze

Trend przechodzenia na usługi chmurowe jest efektem rosnącego popytu klientów pożądanymi rozwiązaniami intuicyjnymi i skalowanymi. Było oczywiste, że kwestią czasu było to, zanim wymyślimy własną kontrolę dostępu w chmurze, wymagającą minimalnego wysiłku ze strony użytkownika (i instalatora).

Wielu producentów tradycyjnych systemów kontroli dostępu nadal nie ma ofercie żadnych usług chmurowych. Tę niszę wykorzystują start-upy. Problem polega na tym, że chociaż ich rozwiązania funkcjonujące w chmurze i modelu SaaS mogą na pierwszy rzut oka wyglądać dobrze, to tym młodym firmom brak doświadczenia w zakresie zabezpieczeń. Wydaje się, że lepiej sobie radzą z zaspokajaniem potrzeb rynku konsumenckiego czy mieszkaniowego.

Powoduje to lukę na rynku, którą wykorzystał Nedap, oferując klientom Access AtWork®. Dlaczego? Ze względu na bardzo dobrą reputację w branży zabezpieczeń, bogate doświadczenie lidera rozwiązań chmurowych (w segmencie opieki zdrowotnej) i silną sieć partnerów. Ale być może przede wszystkim dlatego, że mamy 45 lat doświadczenia związanego z kontrolą dostępu!



Warto wyjaśnić, że najnowsze rozwiązanie Access AtWork® w żadnym wypadku nie zastępuje AEOS. Ze względu na rosnące zagrożenie dla infrastruktury krytycznej z jednej strony, z drugiej – chęć zdobycia przez nas dodatkowego udziału w rynku, widzimy miejsce dla dwóch rozwiązań kontroli dostępu, z których każde ma swój cel i idealny profil klienta (ICP).

- **AEOS:** lokalne rozwiązanie dla tych firm, które muszą kontrolować każdy szczegół swojego systemu i chcą samodzielnie zarządzać aktualizacjami oprogramowania. To najlepszy wybór do sektora infrastruktury krytycznej. AEOS zyskał wszystkie niezbędne certyfikaty, jest wyposażony w zaawansowane funkcje bezpieczeństwa i umożliwia integrację z innymi narzędziami, od aplikacji HR, przez urządzenia biometryczne, aż po Video Management Systems.
- **Access AtWork®:** system kontroli dostępu w chmurze oferowany w modelu SaaS dla tych organizacji, które chcą uzyskać pełen nadzór nad obiektem bez inwestowania w rozbudowę infrastruktury IT. Wprowadzenie tego modelu powoduje, że oprogramowanie jest zawsze aktualne, co uwalnia zespół IT od konieczności czuwania nad tym zadaniem. Access AtWork® idealnie nadaje się do biur wielooddziałowych i zarządzania dynamicznym przepływem osób.

Klienci wybierają Access AtWork®

Jedną z głównych różnic w porównaniu z innymi tego typu systemami chmurowych jest to, że Access AtWork® został wyposażony w najbardziej zaawansowany i najpotężniejszy model autoryzacji. Podjęcie decyzji o tym, jakie osoby potrzebują dostępu do poszczególnych stref, powinno być proste. I teraz jest. Oczywiście dzięki Access AtWork®.

Zastosowanie zaawansowanego modelu autoryzacji powoduje, że administratorzy systemu mogą szybciej niż kiedykolwiek wcześniej konfigurować i modyfikować uprawnienia dostępu i zarządzać

nimi we wszystkich lokalizacjach i budynkach. Skalowanie profesjonalnego systemu KD w wielu lokalizacjach nigdy nie było tak proste.

Użytkownicy, oczywiście w zależności od uprawnień, błyskawicznie otrzymują informacje o tym, kto ma dostęp do jakich pomieszczeń lub stref, w jakich godzinach, a nawet jaki był powód zmiany. Osoba zajmująca się nadawaniem uprawnień może przelatać się na widoki zespołu, strefy lub konto indywidualnego użytkownika. I nie ma już kłopotów po zmianie organizacji stref budynku. Prawa dostępu są automatycznie aktualizowane. Inne opcje to m.in. możliwość tworzenia niestandardowych typów uprawnień, dodawanie pól oraz zakładanie „grup użytkowników”. Inteligentne tabele pozwalają w dowolny sposób ukrywać, sortować i filtrować dane.

To oczywiście nie wszystko. Access AtWork® jest wybierany także z tego powodu, że stoi za nim niezawodność wbudowanych kontrolerów drzwi AEOS Blue. Oznacza to, że z wyjątkiem naszego kontrolera drzwi Access AtWork® jest niezależny od sprzętu. Nie trzeba wymieniać istniejących czytników i zamków. Niezależność od konkretnego producenta okazuje się sporą zaletą, gdy nadchodzi czas na modernizację.

Warto wiedzieć, że nasze solidne kontrolery drzwi działają nawet mimo utraty połączenia z siecią. Ponadto każdy ma własne połączenie

z chmurą, co zapobiega sytuacji, w której awaria jednego kontrolera powoduje awarię całego systemu. W przypadku innych producentów zdarza się, że kierują wszystkie połączenia do pojedynczej bramy, co może sprawić, że cały system będzie podatny na ataki.

Wspólnie z partnerami osiągamy pożądany wynik

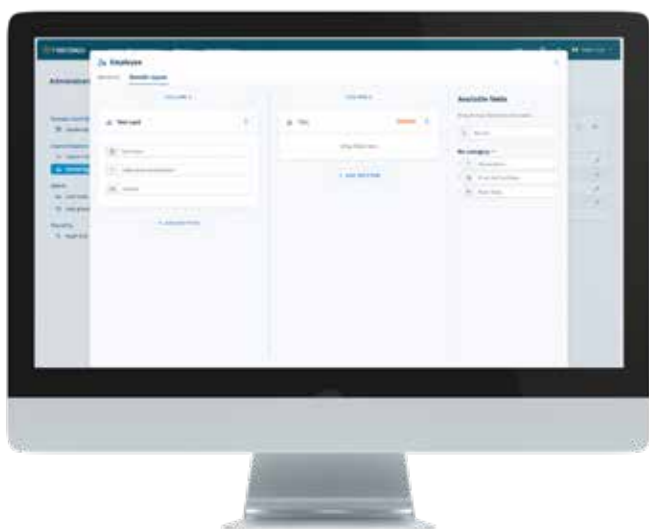
Współpraca z Access AtWork® oferuje szereg korzyści, w tym dostęp do nowych segmentów rynku, łatwość instalacji i konserwacji oraz poprawę rentowności. Rozszerzenie portfolio o nasz system kontroli dostępu w chmurze może przynieść korzyści ze względu na fakt, że rośnie liczba organizacji poszukujących łatwiejszych rozwiązań, elastyczności, jaką daje model SaaS, i braku konieczności inwestowania w zasoby IT. Ważną cechą Access AtWork® jest to, że umożliwia również szybszą i łatwiejszą konfigurację nowych lokalizacji klientów bez konieczności konfigurowania oprogramowania serwerowego. Ponadto Access AtWork® oferuje partnerom atrakcyjny model finansowy, w którym początkowemu zyskowi towarzyszy stały powtarzalny dochód.

Największe korzyści z zastosowania Access AtWork® naszym zdaniem odniosą organizacje rozproszone w wielu lokalizacjach i preferujące usługi typu Software-as-a-Service (SaaS), które odciążają ich zespoły IT.

Sprostanie zadaniu, jakim jest precyzyjna kontrola dostępu, jest niełatwe, a jednocześnie kosztowne w zarządzaniu za pomocą istniejących narzędzi. Dlatego klienci poszukują takich systemów, które pozwolą im nadążyć za rosnącymi wymaganiami, również w zakresie zgodności.

Sektory i branże, które najwięcej zyskują na wprowadzeniu Access AtWork® to organizacje zajmujące się oprogramowaniem i doradztwem IT, FinTechy, międzynarodowe koncerny z licznymi rozproszonymi biurami oraz firmy z branży nieruchomości komercyjnych.

Access AtWork® to produkt oferowany w modelu SaaS, co oznacza, że będzie on regularnie aktualizowany i wzbogacany o nowe funkcje. Jednocześnie Nedap śledzi uważnie wszystkie zagrożenia dla cyberbezpieczeństwa, błyskawicznie wprowadzając aktualizacje chroniące klientów przed zagrożeniem. ●



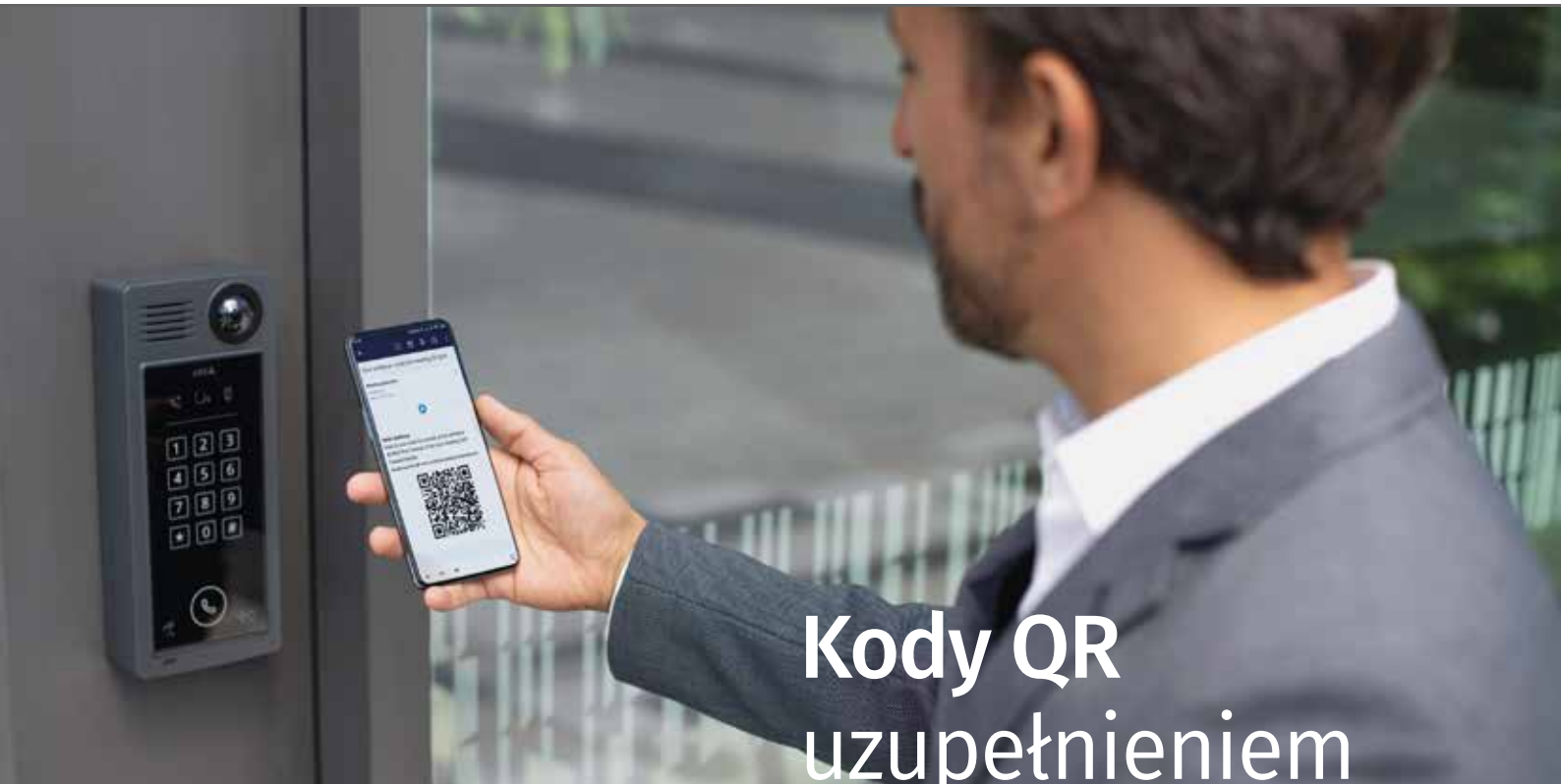
Nedap Security Management

al. Niepodległości 18

02-653 Warszawa

www.nedapsecurity.com/pl/





Kody QR uzupełnieniem systemów kontroli dostępu

Większość z nas niejednokrotnie spotkała się z kodami QR. Często jednak nie zdajemy sobie sprawy z tego, jakie faktycznie dają możliwości. Jedną z nich jest poprawa kontroli dostępu, która wzbogacona o kody QR jest bardziej ekonomiczna, ekologiczna i zoptymalizowana.

Rozwój inteligentnych technologii powoduje, że zarządcy obiektów otrzymali narzędzia zapewniające wysoki poziom zautomatyzowanej kontroli nad całym budynkiem. Możliwość ekonomicznej i stopniowej rozbudowy systemu jest najważniejsza. Rozpoczynając inwestycje w rozwój i zabezpieczenie infrastruktury budynku, warto rozważyć rolę kontroli dostępu i jej podstawową funkcję w ramach inteligentnej infrastruktury budynku.

W tym przypadku kluczem do osiągnięcia zdolności adaptacyjnych jest odejście od systemów zamkniętych, silosowych i inwestowanie w otwarte, elastyczne rozwiązania z łatwą integracją z innymi narzędziami służącymi do ochrony. Dobrze zaprojektowany i elastyczny system kontroli dostępu będzie można w przyszłości zintegrować z nowymi rozwiązaniami lub wzbogacić o nowe funkcje, choćby takie jak... technologia kodów QR.

Przykładem takiej adaptacji i odejścia od systemów zamkniętych jest połączenie kontroli dostępu z systemem rezerwacji gości, co stanowi dodatkowy element wzmacniający bezpieczeństwo. Bardziej zaawansowaną ideą jest przyznanie uprawnień dostępu dla różnego rodzaju dostawców, by wybrane firmy mogły przekazywać dostawy do konkretnych punktów, np. recepcji lub kuchni hotelowej.

Kody QR eliminują też problem przekazywania kart dostępowych osobom nieuprawnionym. Stanowią zatem bezpieczniejszy

i skuteczniejszy sposób kontroli dostępu. Dla firm przywiązujących wagę do dbałości o środowisko ważne zapewne będzie też zmniejszenie zapotrzebowania na karty plastikowe, a nawet ich wyeliminowanie. Ponadto już teraz mamy do dyspozycji dynamiczne kody QR, które m.in. mogą być zabezpieczone hasłem, co dodatkowo wzmacnia poziom bezpieczeństwa tej technologii.

Kody QR w kontroli dostępu

Kody QR nie potrzebują żadnych specjalnych czytników, choć można i takie zastosować. Do odczytania kodu wystarczy kamera smartfona. Jednocześnie kod może zawierać znacznie większą ilość danych niż kod kreskowy. Ta specyfikacja i elastyczność pozwalają na efektywne zarządzanie kontrolą dostępu, gdzie w roli danych uwierzytelniających występuje kod QR.

Zarządzanie kodem, służącym za poświadczenie w systemie KD, jest dość proste w porównaniu z tradycyjnymi kartami. System może szybko i łatwo wygenerować unikalny kod QR dla dowolnej osoby, zapewniając dostęp do budynku np. tylko przez określony czas lub określając maksymalną liczbę jego użycia. Wygenerowany kod QR wysyłany jest pocztą elektroniczną bezpośrednio do odbiorcy, który może go wyświetlić na ekranie smartfona lub wydrukować. Następnie użytkownik skanuje kod za pomocą czytnika umieszczonego w obiekcie.

Zeskanowane dane przekazywane są do systemu kontroli dostępu w celu potwierdzenia praw dostępowych.

– W przypadku kontroli dostępu rozwiązaniem szytym na miarę mogą być dynamiczne kody QR. Eliminują one ryzyko związane z kopiowaniem danych uwierzytelniających, ponieważ kopia ekranowa, fotokopia, a nawet nagranie wideo dynamicznego kodu QR nie zadziała. Połączenie go z rozwiązaniem uwierzytelniania wieloczynnikowego, takim jak PIN wprowadzany w tym samym czasie, w którym skanowany jest dynamiczny kod QR, dodatkowo zwiększy poziom bezpieczeństwa – mówi Bogumił Szymanek z Axis Communications.

Kody QR: efektywne, ekonomiczne i ekologiczne

Korzystanie z kodów QR w zakresie kontroli dostępu ma szereg zalet. Kod QR może być generowany, dystrybuowany, aktualizowany i unieważniany w ciągu kilku sekund, zapewniając wysoko wydajne rozwiązanie do zarządzania całym systemem. Jest on również bardzo wygodny w użyciu, szczególnie dla użytkowników preferujących rozwiązania mobilne.

Typowym zastosowaniem jest przekazanie kodu gościowi, który mając go na swoim smartfonie, może wejść do obiektu lub wjechać na parking bez konieczności osobistego załatwiania formalności w recepcji budynku. Innym typowym scenariuszem jest zarządzanie dostawami odbywającymi się poza ściśle ustalonymi godzinami pracy biura. Dostawca, który ma kod QR na swoim urządzeniu mobilnym, może wyświetlić go przed wideodomofonem lub kamerą, aby otrzymać możliwość wejścia czy wjazdu.

Kody QR stanowią ekonomiczne i przyjazne dla środowiska rozwiązanie niwelujące konieczność zakupu, obsługi, druku i produkcji fizycznych kart oraz instalacji dodatkowej infrastruktury – istniejące już wideodomofony i kamery mogą zostać z powodzeniem wykorzystane jako czytniki kodów QR.

Integracja kodów QR z rozwiązaniami analitycznymi i systemami audio

Połączenie technologii kodów QR z wideodomofonami i interkomami nie jest jedynym sposobem na usprawnienie działania systemów kontroli dostępu. Okazują się również przydatne w zastosowaniach związanych z analizą wizyjną. Połączenie technologii rozpoznawania tablic rejestracyjnych z systemem kodów QR ułatwia np. gościom hotelowym korzystanie z parkingu lub innych pomieszczeń, które zazwyczaj nie są ogólnie dostępne. Podczas rezerwacji pokoju gość hotelowy po podaniu numeru rejestracyjnego swojego samochodu otrzymuje kod QR, który w bezpieczny sposób umożliwi mu dostęp do hotelowego parkingu.

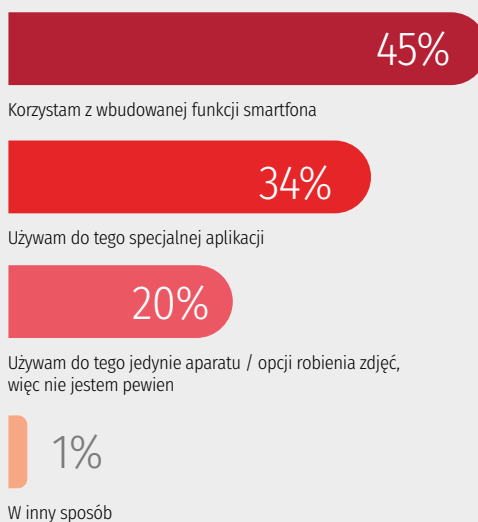
– Dodatkowym usprawnieniem może być również integracja sieciowych systemów audio z kontrolą dostępu. Dzięki systemom audio możliwe jest wygenerowanie komunikatu, np. do kierowcy próbującego dostać się na parking, o tym, że jego kod QR stracił ważność. W razie potrzeby systemy audio mogą wygenerować alarm informujący pracowników ochrony o próbie nieautoryzowanego dostępu, a zintegrowane kamery zarejestrują zajście, stanowiąc ważny materiał dowodowy – wyjaśnia Bogumił Szymanek. ●



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

Technologia kodów QR opracowana w połowie lat 90. XX w. zyskuje na znaczeniu zwłaszcza w branżach rozwijających rozwiązania bezdotykowe. Z ostatniego badania HX Study wynika, że ponad 60% Polaków regularnie korzysta z kodów QR. Jednak w systemach kontroli dostępu wciąż dominującym rozwiązaniem jest korzystanie z tradycyjnych plastikowych kart, mimo że istnieje ryzyko ich zgubienia lub dzielenia się nimi z osobami nieuprawnionymi.

Sposób skanowania QR kodów W jaki sposób najczęściej skanujesz kody QR?



Źródło: QR kody w komunikacji z konsumentem, badanie Starcom (2022 r.)





EchoPoint OPTEX – technologia światłowodowa z zasięgiem do 100 km

Japońska firma OPTEX, która od ponad 40 lat jest światowym liderem detekcji i globalnym dostawcą systemów zapobiegania przestępczości, przedstawiła nowy produkt – serię światłowodowych systemów EchoPoint wykorzystujących technologię Distributed Acoustic Sensing (DAS). To wysoko zaawansowane rozwiązanie do wykrywania włamań nawet w najbardziej rozległych obiektach.

Dzięki najnowocześniejszym algorytmom detekcji i klasyfikacji źródła wystąpienia alarmu systemy EchoPoint niezawodnie wykrywają włamania, identyfikują miejsce naruszenia z dokładnością do ok. 6 m oraz rozpoznają rodzaj naruszenia. System został zaprojektowany do pracy w trudnych, niebezpiecznych środowiskach.

System umożliwia tworzenie wirtualnych stref detekcji, których wielkość może być regulowana w zależności od potrzeb, umożliwiając dopasowanie do rzeczywistych warunków obiektu. Alarmy strefowe mogą być przekazywane do systemów zarządzania sygnałem wizyjnym (VMS) za pośrednictwem protokołu XML/TCP/IP lub za pomocą opcjonalnych modułów wyjść przekaźnikowych.

Ważną cechą systemu jest możliwość jego zdalnej konfiguracji. Zaletą rozwiązania jest także to, że uszkodzenie przewodu nie wpływa na funkcjonalność całego systemu. Podwójne zasilanie i dodatkowe mechanizmy redundancyjne eliminują pojedynczy punkt awarii. W mało prawdopodobnym przypadku awarii procesora drugi procesor automatycznie przejmuje

kontrolę, aby zapewnić ciągłość działania systemu.

Systemy EchoPoint wykorzystują zaawansowany algorytm klasyfikacji źródła wystąpienia alarmu, który pomaga określić rodzaj naruszenia i skutecznie wykrywać wszelkie próby przecięcia siatki, wspinania się na ogrodzenie, czołgania pod nim, a nawet przewiercenia się przez ścianę. W przypadku zastosowania rozwiązania, w którym światłowód jest zakopany, EchoPoint rozpoznaje różnice pomiędzy kopaniem ręcznym, kopaniem maszynowym i ruchem pojazdów.

Systemy EchoPoint są odpowiednie do zaawansowanych aplikacji w dużych obiektach logistycznych, wojskowych i infrastruktury krytycznej, w tym również do zabezpieczania rurociągów i przewodów telekomunikacyjnych. Przewaga ekonomiczna tej technologii jest szczególnie widoczna przy rozległych instalacjach ze względu na jeden punkt montażowy, niską cenę, a także niewielki koszt eksploatacji. ●



OPTEX Security
ul. Sielecka 35, 00-738 Warszawa
optex@optex.com.pl
www.optex.europe.com/pl





Cyberataki wymierzone w pracowników

Ponad 50% zarządzających przedsiębiorstwami wskazuje, że ich pracownikom brakuje odpowiedniej wiedzy dotyczącej bezpieczeństwa. Podkreślają też znaczenie skutecznych szkoleń w zakresie cyfrowej świadomości prowadzonych w celu zmniejszenia poziomu ryzyka przyczyniania się pracowników do powodzenia ataku.

Przedsiębiorstwa zmagają się z coraz bardziej wyrafinowanymi zagrożeniami. W najnowszej edycji raportu *Global Threat Landscape Report*, opracowanego przez ekspertów należącego do firmy Fortinet działu FortiGuard Labs, wykazano, że zagrożenia związane z oprogramowaniem ransomware utrzymują się na szczytowym poziomie i nie ma dowodów na ich spowolnienie w skali globalnej. Jednocześnie przeprowadzone przez Fortinet badanie *2023 Cybersecurity Skills Gap Global Report* wykazało, że 84% przedsiębiorstw doświadczyło jednego lub więcej naruszeń bezpieczeństwa w 2022 r.

Według najnowszych badań ponad 90% liderów uważa, iż zwiększona świadomość pracowników w zakresie cyberbezpieczeństwa pomogłaby zmniejszyć skalę powodzenia ataków. Ponieważ przedsiębiorstwa stają w obliczu rosnącego cyfrowego ryzyka, badania podkreślają ważną rolę pracowników jako pierwszej linii obrony przed cyberprzestępczością.

W ubiegłym roku aż 81% przedsiębiorstw doświadczyło ataków z użyciem złośliwego oprogramowania, phishingu oraz hasła, które były kierowane głównie do użytkowników. Podkreśla to, że mogą być najstarszym ogniwem zabezpieczeń przedsiębiorstwa lub jednym z jego najpotężniejszych mechanizmów obronnych.

Posiadanie skutecznego programu szkoleniowego jest kluczem do zaszczepienia w pracownikach właściwego poziomu cyberhigieny – 85% zarządzających przedsiębiorstwami twierdzi, że został w nich zaimplementowany program szkoleń i podnoszenia świadomości w zakresie bezpieczeństwa, ale ponad 50% uważa, że ich pracownikom nadal brakuje wiedzy na ten temat. Luka ta sugeruje, że programy szkoleniowe nie są tak skuteczne, jak mogłyby być, co skutkuje niespójnością w stosowaniu przez pracowników dobrych praktyk w zakresie cyberbezpieczeństwa, lub tym, że szkolenia nie pokrywają tematyki w wystarczający sposób.

Cyberbezpieczeństwo coraz częściej staje się priorytetem dla zarządców – badanie Fortinet wykazało, że w 93% firm zarząd pyta o kwestie dotyczące cyberbezpieczeństwa oraz strategię firmy w tym zakresie.

– *Nasz raport z globalnego badania 2023 Security Awareness and Training Global Research Brief podkreśla kluczową rolę, jaką pracownicy odgrywają w zapobieganiu cyberatakam. Wskazuje również na istotną potrzebę nadania przez przedsiębiorstwa priorytetu krzewieniu świadomości dotyczącej bezpieczeństwa, m.in. poprzez szkolenia, aby zapewnić, że pracownicy będą stanowić pierwszą linię obrony* – powiedział John Maddison, EVP of Products and CMO Fortinet.

O Fortinet

Firma Fortinet jest czołowym producentem systemów ochronnych i innowatorem rozwiązań zapewniających konwergencję funkcji sieciowych i zabezpieczających środowisko IT. Jej misją jest ochrona ludzi, urządzeń i danych, niezależnie od ich miejsca. Ponad pół miliona klientów zaufało rozwiązaniom Fortinet, które należą do najczęściej wdrażanych, posiadających najwięcej patentów i najlepiej ocenianych w branży. Więcej informacji na stronie <https://www.fortinet.com>. ●



Bezpieczna ewakuacja



W obiektach użyteczności publicznej dźwiękowe systemy ostrzegawcze (DSO) pełnią bardzo ważną funkcję w codziennym życiu. Zazwyczaj instalowane są w budynkach biurowych, galeriach handlowych, szpitalach, hotelach czy akademikach, a także w obiektach infrastruktury krytycznej, zakładach produkcyjnych czy przestrzeniach magazynowych. Odpowiedni dobór rozwiązania i prawidłowo przygotowany do niego projekt może zagwarantować efektywną, a co za tym idzie bezpieczną ewakuację osób z zagrożonych obszarów.

Rafał Kowal

Na rynku jest dostępnych wiele rozwiązań w zakresie DSO, jednak system to nie wszystko. Ważne jest szczegółowe zapoznanie się przez projektanta z poszczególnymi rozwiązaniami i ich możliwościami – funkcjonalnością. Kolejnym istotnym czynnikiem jest świadomość, że może on liczyć na wsparcie techniczne ze strony producenta systemu i co najważniejsze, aby to wsparcie było zapewnione na każdym z etapów związanych z instalacją systemu w obiekcie, począwszy od etapu projektu koncepcyjnego, poprzez etap wykonawczy, skończywszy nawet na pomiarach akustycznych w już zaaranżowanym obiekcie.

Takie podejście od lat stosuje firma Schrack Seconet Polska, co daje pewność zarówno projektantowi, jak i inwestorowi, że skonfigurowany i zainstalowany system w danym obiekcie będzie działał prawidłowo, spełniając wszelkie wymagania przed nim postawione.

Należy zwrócić uwagę, że DSO jest przede wszystkim bezpośrednio sterowany i nadzorowany przez SSP (system sygnalizacji pożarowej) i zastępuje (tam gdzie to wymagane prawnie) sygnalizatory akustyczne. Jego głównym zadaniem jest powiadamianie o powstałym zagrożeniu w danym obszarze i strefie z wykorzystaniem funkcji rozgłaszania komunikatów głosowych (automatycznych lub nadawanych na żywo za pośrednictwem pulpitu mikrofonowego), zazwyczaj poprzedzanych sygnałem dźwiękowym typu gong lub syrenka (najczęściej są to znormalizowane sygnały). Funkcjonalność ta ma na celu w sposób automatyczny, uporządkowany i jednoznaczny wspomóc proces ewakuacji ludzi z zagrożonej strefy. Krótko mówiąc, DSO jest elementem wykonawczym systemu sygnalizacji pożarowej (SSP) zastępującym standardowo stosowane sygnalizatory akustyczne.

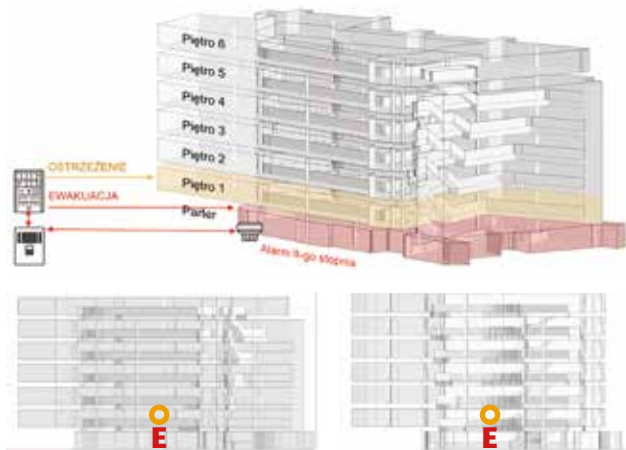
Podstawową przewagą DSO nad wspomnianymi sygnalizatorami jest fakt, że o ile konwencjonalne sygnalizatory akustyczne (bez funkcji komunikatów głosowych) są w stanie wygenerować sygnał o wysokim poziomie SPL (*Sound Pressure Level*), np. 100 dB, który dodatkowo może być modulowany, co ma na celu zwiększyć uwagę osób przebywających w zagrożonej strefie, o tyle to nadal tylko sam sygnał, po którym nie jesteśmy w stanie stwierdzić, z jakiego typu zagrożeniem mamy do czynienia i jak powinniśmy się zachować w danej sytuacji.

W przypadku DSO istnieje możliwość wygenerowania krótkich sygnałów dźwiękowych (np. gong lub syrenka) poprzedzających komunikat słowny, które mają na celu przede wszystkim zwrócić uwagę osób przebywających w danej strefie nagłośnieniowej, a następnie nadanie komunikatu głosowego o konkretnej treści dostosowanej do typu, przeznaczenia obiektu oraz zagrożenia, jakie w nim wystąpiło.

To podstawowa funkcja DSO i bezapelacyjnie pożądana w przypadku potrzeby sprawnego i bezpiecznego przeprowadzenia ewakuacji ludzi z zagrożonej strefy. Dodatkową kwestią jest język, w którym ten komunikat zostanie nadany. Bardzo często w ramach dobrej praktyki inżynierskiej stosuje się komunikaty, np. dwujęzyczne polsko-angielskie lub nawet trójjęzyczne polsko-angielsko-niemieckie/ukraińskie. Komunikaty te są tego samego przeznaczenia, tj. komunikat ostrzegawczy, ewakuacyjny lub odwotujący, i odpowiednio skonstruowane zgodnie z projektem, uwzględniające przeznaczenie obiektu oraz możliwości ewakuacji. Rozgłaszanie tych komunikatów w przypadku systemu APS®-APROSYS może być zrealizowane na różne sposoby w zależności od sposobu ewakuacji, np. jednoetapowa, po potwierdzeniu pożaru i alarmie II stopnia następuje ewakuacja całego budynku w tym samym czasie zgodnie z wymaganiami scenariusza pożarowego, np. kilku-kondygnacyjny hotel, akademik, hala produkcyjna czy supermarket.

Drugim wariantem może być tzw. ewakuacja wieloetapowa z równoczesnym nadawaniem np. dwóch komunikatów: EWAKUACYJNEGO do strefy bezpośrednio zagrożonej i OSTRZEGAWCZEGO do strefy przyległej.

Rys. 1. Przykład ewakuacji wieloetapowej (dwa komunikaty nadawane jednocześnie)



Kolejnym wariantem może być ewakuacja wieloetapowa z podziałem na nadawanie komunikatów w kolejności: 1 EWAKUACYJNEGO, 2 OSTRZEGAWCZEGO w układzie sekwencyjnym (naprzemiennym), gdzie w pierwszej kolejności następuje ewakuacja osób ze strefy zagrożonej oraz klatek schodowych, a następnie po zakończeniu rozgłaszania komunikatu ewakuacyjnego następuje ostrzeżenie stref przyległych (rys. 2).

Rys. 2. Przykład ewakuacji wieloetapowej – sekwencyjnej (rozgłaszanie naprzemiennie)



Odpowiedni dobór rozwiązania w zakresie sposobu ewakuacji to klucz do sukcesu. W niektórych przypadkach może się okazać, że nadawanie więcej niż jednego komunikatu w tym samym czasie może skutkować powstawaniem tzw. kakofonii – braku zrozumienia

i odpowiedniej reakcji poprzez np. nakładające się na siebie komunikaty różnej treści. Takim przykładem może być budynek z „otwartym” atrium przez kilka kondygnacji lub pojawiające się przestłuchy pomiędzy strefami. W tym przypadku ewakuacja (o ile jest taka potrzeba) powinna odbywać się raczej w układzie naprzemiennym, co daje dodatkowo możliwość łatwiejszego porozumiewania się między sobą osób znajdujących się w zagrożonej strefie bez niepotrzebnego „przekrzykiwania się” z komunikatami nadawanymi przez DSO.

W szczególnych przypadkach (np. w szpitalach, portach lotniczych) często stosowane są tzw. komunikaty kodowane przeznaczone dla przeszkolonego personelu. Komunikaty te w przeciwieństwie do komunikatów ostrzegawczych czy ewakuacyjnych powinny być tak skonstruowane, aby przede wszystkim nie wzbudzały paniki lub niepokoju wśród osób przebywających w zagrożonej strefie.

Zastosowanie komunikatów kodowanych ma na celu dyskretne powiadomienie przeszkolonego personelu o wykrytym zagrożeniu (może być to stan, kiedy zagrożenie nie zostało jeszcze potwierdzone – tzw. alarm pożarowy I stopnia) i umożliwienie przygotowania do ewakuacji całego piętra czy strefy.

Dodatkową i bardzo przydatną funkcją w tego typu obiektach (ale nie tylko w nich), jaką można znaleźć w systemie APS®-APROSYS, jest możliwość dodzwonienia się do systemu i zdalnego nadawania komunikatów w czasie rzeczywistym. Przeszkolony personel w sytuacji nadzwyczajnej (np. nagły atak agresji wśród osób przebywających w częściach wspólnych czy próba sabotażu lub ataku terrorystycznego) może bezzwłocznie (bez zbędnej straty czasu na dotarcie do pomieszczenia ochrony, recepcji, gdzie zostały zainstalowane pulpity mikronowe) zawiadomić pozostały personel o zaistniałej sytuacji. Taka funkcjonalność systemu może przyspieszyć podjęcie działań przez ochronę obiektu w zakresie stłumienia lub ograniczenia tego typu zagrożeń lub w sytuacji kryzysowej związanej z niedostępnością do urządzeń obsługi DSO zarządzać ewakuacją obiektu.

Aby zapewnić sprawną i bezpieczną ewakuację z zagrożonej strefy, należy pamiętać, że bardzo ważnym czynnikiem jest klarowność w przekazywanych informacjach o zdarzeniach w obiekcie, co pozwoli na szybszą reakcję i podjęcie ewakuacji lub przygotowanie się do niej osób znajdujących się w zagrożonych obszarach.

W obiektach, które są wyposażone w systemy sygnalizacji pożarowej, dźwiękowe systemy ostrzegawcze, kontroli dostępu, dozoru wizyjnego itp., aby systemy te mogły wesprzeć akcję bezpiecznej ewakuacji z zagrożonej strefy, muszą działać zgodnie ze scenariuszem pożarowym i przygotowaną na jego podstawie matrycą lub tabelą/matrycą sterowań. Niestety zdarza się, że scenariusz lub matryca są przygotowane na końcu etapu budowy i dostosowywane (lub nie) do już zainstalowanego wyposażenia. W efekcie może spowodować to konieczność modernizacji instalacji lub, co gorsza, rozbudowy dopiero co zainstalowanych (zgodnie z projektem) ww. systemów zabezpieczeń. Oczywiście w przypadku rozwiązań Schrack Seconet nie stanowi to technicznego problemu chociażby ze względu na pełną elastyczność oferowanych rozwiązań w zakresie kompleksowego bezpieczeństwa pożarowego, tj. SSP, DSO, systemy sterowania, zasilania i system integrujący urządzenia przeciwpożarowe (SIUP). Należy jednak brać pod uwagę ewentualne dodatkowe koszty przy wymaganej modernizacji instalacji i wynikające z nich uzgodnienia techniczne oraz niepotrzebne zamieszanie wśród osób odpowiadających za wykonanie instalacji, co wpływa na dotrzymanie terminów realizacji i koszt wdrożenia.





Aby zapewnić jak najwyższy poziom bezpieczeństwa, stosowane są systemy integrujące urządzenia przeciwpożarowe (SIUP), które służą do kompleksowego zarządzania urządzeniami przeciwpożarowymi i innymi systemami mającymi wpływ na bezpieczeństwo pożarowe obiektu.

W szczególności rola SIUP jest kluczowa w zakresie zarządzania bezpieczną ewakuacją osób z obiektu, dlatego ważna jest ścisła współpraca oferowanego przez Schrack Seconet Polska SIUP SIS-FIRE z systemem sygnalizacji pożarowej oraz sterowania urządzeniami przeciwpożarowymi Integral EvoX i DSO APS®-APROSYS wraz z nowym kontrolerem APS-9000. Najwięcej funkcji i wartości dodanych w zakresie bezpieczeństwa i komfortu uzyskujemy w momencie wdrożenia pełnej dwukierunkowej komunikacji cyfrowej między tymi systemami. Cyfrowa komunikacja kontrolera APS-9000 z systemami nadrzędnymi: Integral EvoX oraz SIS-FIRE (za pomocą dedykowanych protokołów komunikacyjnych Modbus TCP-IP czy MQTT) udostępnia wiele ciekawych możliwości funkcjonalnych przy integracji tych systemów poprzez komunikację dwukierunkową.

Dzięki integracji DSO z SIUP możliwe jest nadrzędne sterowanie CDSO. System APS®-APROSYS skomunikowany cyfrowo z SIS-FIRE pozwala operatorowi i kierującemu działaniami ratowniczymi na zmianę scenariusza automatycznego i uruchomienie rozgłaszania komunikatów

głosowych w trybie ręcznym do wybranych stref nagłośnieniowych. Takie rozwiązanie zapewnia dynamiczną reakcję personelu ochrony i uniknięcie sytuacji, w której np. jedno z wyjść ewakuacyjnych zostało zablokowane lub został odcięty dostęp do klatki schodowej i osoby ewakuujące się z zagrożonej strefy nie otrzymały odpowiedniego powiadomienia, nie zostały „przekierowane” do innego wyjścia ewakuacyjnego. Zastosowanie zintegrowanego systemu bezpieczeństwa pożarowego w obiekcie zarządzanym przez SIUP można w każdej chwili ingerować i przerwać automatyczne sterowanie, a co za tym idzie w sposób bezpieczny kontynuować ewakuację ludzi z zagrożonej strefy.

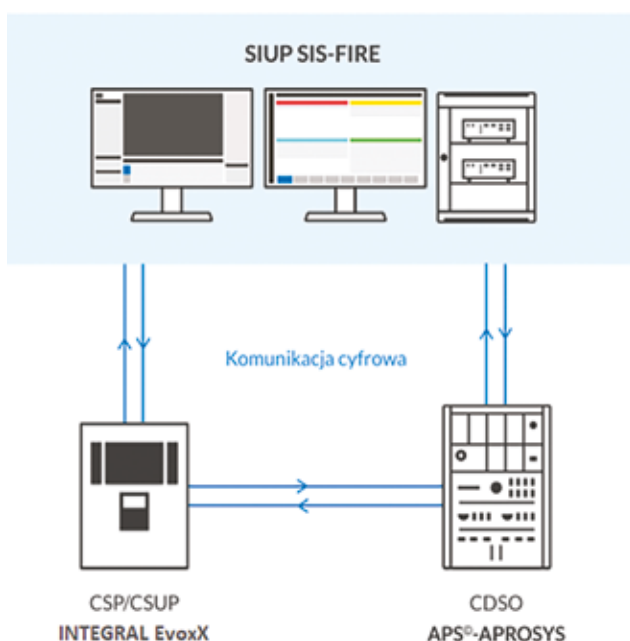
Oczywiście po ustaniu zagrożenia w obiekcie i podjęciu decyzji o zakończeniu ewakuacji ważne jest nadanie komunikatu „odwołującego”, który jednoznacznie poinformuje osoby znajdujące się w budynku, że zagrożenie ustało.

Ponadto SIS-FIRE szczegółowo monitoruje stany działania DSO np. w zakresie zasilania podstawowego, rezerwowego czy połączenia CDSO z pulpitemi mikrofonowymi, łącznie z monitorowaniem usterek poszczególnych linii głośnikowych poprowadzonych w obiekcie.

Ze względu na przeznaczenie, wielkości obiektów, do których dostarczana jest technologia oferowana przez Schrack Seconet Polska, powyższe rozwiązanie jest często stosowane przez partnerów firmy i cenione zarówno przez inwestorów, jak i przez użytkowników końcowych.

Dodatkowo kontroler główny APS-9000 ma wbudowane 4 niezależne odtwarzacze audio umożliwiające nadawanie czterech komunikatów w tym samym czasie. Z kolei wbudowana karta sieciowa zapewnia połączenie dowolnej liczby systemów DSO w sieci LAN oraz transmisję sygnałów audio z wykorzystaniem standardu AES67 do pozostałych central DSO (pracujących w układzie rozproszonym) lub do innych podsystemów wykorzystywanych do celów komercyjnych. Wbudowany procesor DSP zapewnia swobodny routing źródeł dźwięku oraz jego cyfrową obróbkę z zachowaniem jakości, jak to ma miejsce w przypadku profesjonalnych systemów estradowych.

Szczegółowe informacje dotyczące systemu APS®-APROSYS, najnowszych rozwiązań (w tym kontrolera APS-9000) i jego możliwości można uzyskać bezpośrednio podczas organizowanych cyklicznie szkoleń projektowych. Więcej informacji na stronach <https://www.schrack-seconet.com/pl> oraz <https://wydarzenia.schrack-seconet.pl/>



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

CRYSTAL

Megavision Technology

ZŁOTY PARTNER

zaprasza wszystkich profesjonalistów branży
na tegoroczną edycję

21 SPIN

26-27.09.2023

Hotel CRYSTAL MOUNTAIN Wisła



avigilon™

venom

megavision
technology



Udajemy, że jesteśmy bezpieczni



Fot: Daniel Dmitriew/Forum

Szkolenie to podstawa bezpieczeństwa. Zawsze powtarzałem i powtarzać będę: kto nie ćwiczy, ten nie umie – przekonuje **pułkownik Krzysztof Przepiórka**. – Jeśli chcemy mieć pewność, że poradzimy sobie w sytuacji kryzysowej, musimy wcześniej ją przećwiczyć. Ograniczamy się do tego, co niezbędne i wynika z przepisów prawa, a to zbyt mało – zwraca uwagę instruktor technik antyterrorystycznych.

O tym, jak istotne jest szkolenie zarówno kadr w budynkach użyteczności publicznej (szkołach, bankach, hotelach, urzędach), jak i wszystkich obywateli, którzy mogą przypadkiem znaleźć się w zagrożeniu, opowiedział w wywiadzie udzielonym Monice Mamakis.

Czy Polska jest krajem bezpiecznym?

Nie chciałbym być źle zrozumiany, ale co w obecnych czasach znaczy „kraj bezpieczny”? Za naszą wschodnią granicą toczy się wojna, która trwa już ponad półtora roku i jej końca nie widać. Nie wiadomo, jak i kiedy się skończy. To jest realne zagrożenie i powinniśmy być przygotowani, a według mnie nie jesteśmy.

Co w takim razie powinniśmy zrobić?

Tak prywatnie? Choćby spakować plecak ewakuacyjny.

Pan taki ma?

Oczywiście. Stoi zawsze w tym samym miejscu.

I co pan w nim umieścić?

To co najbardziej potrzebne, w tym rzecz jasna dokumenty, by przeżyć pierwsze dni: apteczka, przedmioty higieny osobistej, żywność i woda oraz rzeczy umożliwiające znalezienie bezpiecznego schronienia i komunikację. A pani taki plecak ma?

Nie, ale za to mam w domu dwie gaśnice i wiem, co zabrałabym ze sobą w razie pożaru.

I co by to było?

Poza dzieckiem i psem, co wydaje się oczywiste, byłyby to dokumenty, laptop, zdjęcia rodzinne i miś, którego dostałam od mamy, gdy byłam dzieckiem.

W razie pożaru domu to może i by wystarczyło. Ale gdyby trzeba było dom opuścić na dłużej, tak jak musieli to zrobić nasi sąsiedzi z za wschodniej granicy, to raczej nie bardzo. A co zabrałoby ze sobą pani dziecko i mąż? Też o tym myśleli?

Nie sędzę. Nigdy z nimi nie rozmawiałam na ten temat. Wszyscy czujemy się raczej...

...bezpiecznie? Większość z nas tak się czuje, moim zdaniem nieco bezpodstawnie.

Na swoją obronę przyznam, że wchodząc do miejsca takiego jak galeria handlowa, szczególnie taka, w której jeszcze nie byłam, mam w zwyczaju rozejrzeć się, gdzie są wyjścia ewakuacyjne. To obsesja czy raczej zdrowy odruch?

Żadna obsesja, tak powinniśmy robić. To zwykły zdrowy pragmatyzm. Dla własnego komfortu zawsze trzeba sprawdzić drogi ewakuacyjne i wyjścia awaryjne. W tym względzie nie jesteśmy wyedukowani. Ludzie zazwyczaj uważają, że coś złego spotyka innych, nigdy nas.

Czy uważa pan, że jako społeczeństwo w sytuacji zagrożenia, np. w razie pożaru czy powodzi, poradziłibyśmy sobie?

Uważam, że niewiele potrafimy. I dlatego tak dużo mówię o potrzebie szkoleń prowadzonych od podstaw już w szkołach podstawowych, byśmy z czasem nabrali zdrowych nawyków. Nauka ewakuacji prowadzona jest wyłącznie dlatego, że wymagają tego przepisy przeciwpożarowe. To zdecydowanie za mało. Nie nadążamy jako społeczeństwo za zmieniającym się światem. Pożar to przecież niejedyny zagrożenie, a nawet i w tym przypadku nie potrafimy zachować się prawidłowo.

Prawidłowo, czyli jak?

Posłużę się przykładem. Wyobraźmy sobie pożar w typowej polskiej szkole. Klasycznej „tysiąclatce”, jakich w naszym kraju jest wiele. Ile osób może być w takiej placówce w tym samym momencie?

Nie wiem, może pięćset?

Owszem, a może być nawet osiemset, a w dużym mieście jak Warszawa nawet tysiąc. Przyjmijmy jednak, że będzie to osiemset osób. Dzieci w niej wiedzą, bo powiedziano im, że w przypadku alarmu pożarowego (a zakładamy, że potrafią rozpoznać jego sygnał, co wcale nie jest oczywiste) mają razem z nauczycielem spokojnie udać się na miejsce zbiórki. Ale gdzie zaplanowano zbiórkę?

Zapewne na boisku szkolnym?

Tak, tak jest najczęściej. Proszę sobie wyobrazić osiemset osób, albo i więcej, stojących na stosunkowo niewielkim boisku. Wiemy, że to nie są ćwiczenia, i mamy do czynienia z prawdziwym dużym pożarem. Ogień sięga miejscami ponad dach budynku, nagle wieje wiatr i dym kieruje się w stronę boiska. Co wówczas się dzieje?

Zgaduję, że wszyscy rzucają się w stronę wyjścia?

Właśnie tak. Wyjście może być jedno, jakaś mała furtka. I zamiast sprawnej ewakuacji nieszczęście gotowe. Bo komuś wcześniej zabrakło wyobraźni, a w ostatecznym rozrachunku ludziom, czyli w przypadku tej hipotetycznej szkoły, zabrakło wiedzy kadrze pedagogicznej. Zawsze powtarzałem i powtarzać będę: kto nie ćwiczy, ten nie

umie. W polskich szkołach nie ćwiczy się umiejętności ewakuacji w razie różnego rodzaju zagrożeń. Nie ma też zwyczaju, by zamiast jednego miejsca zbiórki było ich kilka. Jeśli bowiem będzie to atak szaleńca z bronią, to wiele osób zgromadzonych w jednym miejscu jest wymarzone dla takiego przestępcy celem. Opiekunowie znają tylko podstawowe zasady bezpieczeństwa, nie wiedzą, że mogą wykorzystać do pomocy tzw. naturalnych liderów.

Kto jest naturalnym liderem?

Bardzo często jest nim największy łobuz w klasie. Dziecko być może niesforne, ale często odważne i mające posłuch u innych. To w nim nauczyciel może znaleźć wsparcie, pomoże mu opanować osoby, które wpadły w panikę. W razie ataku furii pomoże choćby zablokować drzwi.

Według pana szkoły powinny prowadzić zajęcia dotyczące umiejętności odnalezienia się w różnych sytuacjach zagrożenia, np. w przypadku ataku terrorystycznego. Nie ma pan jednak wrażenia, że to trochę przesada. Po co straszyć dzieci?

Bo takie rzeczy na świecie się dzieją. I nie ma powodu, by nie wystąpiły się w Polsce. Mam wrażenie, że my na dzieci chuchamy i dmuchamy. Trzeba je chronić, to oczywiste, ale trzeba je też przygotować na różnego rodzaju trudne sytuacje. To, czego nauczymy ich za młodu, może im się przydać w dorosłym życiu.

Cały system edukacji powinien przygotowywać do tego, by radzić sobie z takimi przypadkami jak pożar, trzęsienie ziemi czy choćby atak uzbrojonego człowieka. Moim zdaniem co najmniej raz w miesiącu powinny odbywać się zajęcia praktyczne. W szkołach, na uczelniach, w instytucjach użyteczności publicznej – wszędzie tam, gdzie w tym samym czasie przebywa wiele osób.

Wyobraźmy sobie, że ktoś grozi zamachem bombowym w jednym z biurowców, drapaczy chmur, każdy po kilkanaście albo i kilkadziesiąt pięter. Co zrobią ludzie pracujący w takim miejscu? Czy będą potrafili się ewakuować tak, by nawzajem się nie stratować?

To zależy od tego, czy wpadną w panikę, czy też zachowają zimną krew, bo wcześniej przeszli właściwe kursy. To z kolei zależy od tego, na ile świadome są firmy, które tych ludzi zatrudniają, ale też zarządcy budynków, gdzie mieszczą się biura.

Trochę ma też znaczenie pewnego rodzaju odwaga u zarządców takich budynków polegająca na tym, że nie będą się bali prowadzić odpowiednich szkoleń. Nawet mimo marudzenia najemców, że praca, że szkoda czasu, że terminy goniają... Podejmą to wyzwanie. Jest jeszcze jeden ważny aspekt – by takie szkolenia miały sens, muszą być wspólnym działaniem najemcy, firmy fizycznie ochraniającej budynek i zarządcy. Wszystkie tryby muszą wspólnie zadziałać.

Moje doświadczenie pokazuje, że nie umiemy sobie radzić w sytuacjach zagrożenia. Niejednokrotnie podczas szkoleń spotykałem ludzi,

» Dla własnego komfortu zawsze trzeba sprawdzić drogi ewakuacyjne i wyjścia awaryjne. W tym względzie nie jesteśmy wyedukowani. «



którzy wiedzieli, że są prowadzone ćwiczenia, a i tak postępowali chaotycznie, ulegając emocjom. Strach pomyśleć, co się stanie, gdy faktycznie będą musieli się ewakuować, np. z płonącego wieżowca. Kiedy rozmawiam z firmami zainteresowanymi szkoleniem pracowników, powtarzam do znudzenia: jeden kurs nie wystarczy. Trzeba ćwiczyć, powtarzać, trenować. Kiedy czujemy się zagrożeni, jedynie wypracowane w czasie szkoleń nawyki mogą nas uratować. Zresztą widzę to na własne oczy. Każde kolejne szkolenie tych samych ludzi powoduje, że radzą sobie coraz lepiej. I co najważniejsze, ci ludzie muszą znać najważniejszą regułę w sytuacjach, gdy zagrożeniem jest nie żywioł, a inny człowiek.

Jaka to reguła?

By nie zgrywać bohatera. Zasada jest prosta, najpierw uciekamy. Jeśli ucieczka nie jest możliwa, chowamy się. Walkę podejmujemy wtedy, gdy nie możemy ani uciec, ani się ukryć. I tego uczę m.in. na kursach prowadzonych dla firm. Zawsze też zachęcam: robicie spotkanie integracyjne? To zamiast tradycyjnej popijawy, bo nie oszukujemy się często tak wyglądają takie spotkania, zróbcie kurs obrony cywilnej, może być np. z paintballem. I faktycznie są firmy, które tak właśnie robią. To świetna zabawa, ale i nauka. Zajęcia z obrony cywilnej były kiedyś prowadzone w szkołach, teraz ich nie ma. Lepiej, gorzej, ale były. W efekcie ludzie nie potrafią udzielić nawet pierwszej pomocy. Już nie mówię o tym, żeby znali się na medycynie pola walki, ale by chociaż umieli prawidłowo przeprowadzić resuscytację czy zatamować krwotok.

Takie szkolenia czy kursy powinny być rozwiązaniami systemowymi, propagowanymi przez państwo. Tymczasem tak nie jest. Odgórny wymóg systemowy mógłby się też łączyć z przyznawaniem np. odpowiednich certyfikatów. Zarządcy różnego rodzaju budynków, np. biurowców, mogliby otrzymywać certyfikat typu bezpieczny biurowiec, bezpieczna szkoła. To by znaczyło, że ludzie w nich się znajdujący, ale też zarządzający obiektami przeszli odpowiednie szkolenia. Mogłoby się to wówczas przełożyć korzystnie na cenę najmu w przypadku nieruchomości komercyjnych. Uważam też, że taki certyfikat mógłby zniechęcić potencjalnych złoczyńców.

W jaki sposób?

Choćby w taki, że ewentualny napastnik będzie wiedział, że w danym biurowcu pracują ludzie, którzy potrafią działać zamiast bezczynnie się przyglądać z nosem przyklejonym do szyby, nagrywając wszystko na komórkę.

Mówimy o sytuacji, w której wszyscy obecni na miejscu ludzie są nieprzypadkowi. Tymczasem choćby w hotelach czy ośrodkach wypoczynkowych mamy do czynienia z osobami, które znalazły się w nich na przykład po raz pierwszy. Co wówczas, jak zadbać o ich bezpieczeństwo?

Zacznijmy od tego, że gdyby ci ludzie, goście hotelu czy pensjonatu, przeszli szkolenia w swoich firmach, to już byłoby coś. Mieliby świadomość, co mogą zrobić w razie zagrożenia, umieliby opanować

emocje, wchodząc, np. do hotelu, sprawdziliby, gdzie są drogi ewakuacyjne, umieliby pomóc poszkodowanym. Faktem jest jednak, że na to obsługa hotelu liczyć nie może i nie powinna, sama musi być więc wyszkolona.

A jest?

Z tym bywa różnie. Rzecz jednak nie w braku świadomości zarządców hoteli, ale w dużej rotacji kadr wynikającej choćby z sezonowości zatrudnienia. Znam też przykłady budujące, takie jak jeden z dużych hoteli pod Warszawą czy duży kompleks wypoczynkowy w Bieszczadach. Tam szkolimy regularnie. Każdy, kto pracuje w hotelu – od dyrektora najwyższego szczebla, przez kucharzy, po personel sprząający – powinien wiedzieć, co robić w razie ataku terrorystycznego, napadu lub pożaru. Role powinny być podzielone, tak jak to dzieje się na dużych statkach wycieczkowych, gdzie załoga wie, co w którym momencie ma robić. Trudność polega na tym, o czym wcześniej wspominałem: w takich miejscach kadra

często się zmienia, a tu ma znaczenie perfekcyjne opanowanie swojej roli.

» *Każdy, kto pracuje w hotelu – od dyrektora najwyższego szczebla, przez kucharzy, po personel sprząający – powinien wiedzieć, co robić w razie ataku terrorystycznego, napadu lub pożaru.* «

Jakiego rodzaju instytucje w naszym kraju są najlepiej przygotowane na ewentualny atak, np. terrorystyczny lub podobne zagrożenie?

Nie będzie zapewne zaskoczeniem, jeśli powiem, że obiekty infrastruktury krytycznej. Wszelkiego rodzaju stacje uzdatniania wody, instalacje przesyłowe, gazownie, elektrownie itp. Obsługa tego typu obiektów zna procedury, a obiekty są chronione.

A urzędy publiczne czy np. placówki bankowe?

O urzędach trudno mi się wypowiadać, a placówki bankowe mają odpowiednie zabezpieczenia. Pracownicy przebywający w salach operacyjnych są regularnie szkoleni. Wiedzą, jak mają się zachować. Inna rzecz, że napady na banki czy poczty nie zdarzają się w naszym kraju często, choć występują. Ważne jest to, że nie giną w nich ludzie. Ostatnim, w którym doszło do ofiar śmiertelnych, był napad, który miał miejsce ponad 20 lat temu. Tamta sytuacja była jednak nietypowa (mowa o napadzie na Kredyt Bank w marcu 2001 r., którego dokonali pracownicy agencji chroniącej bank – przyp. red.). Pracownicy banków są szkoleni, by nie dyskutować z napastnikiem. Warto wiedzieć, że napad rabunkowy statystycznie trwa 90 sekund, i należy zrobić wszystko, by nie dopuścić do wzięcia zakładników. Dlatego najlepiej nic nie robić. Oddać pieniądze i pozwolić napastnikowi wyjść. W żadnym wypadku nie udawać bohatera. Tego m.in. uczę na moich szkoleniach. ●

Podpułkownik Krzysztof Przepiórka instruktor technik antyterrorystycznych, spadochroniarstwa, strzelectwa, narciarstwa. Absolwent kursu antyterrorystycznego w Stanach Zjednoczonych (Special Training Group) oraz kursu International Bodyguard Association (Wlk. Brytania). Obecnie prowadzi firmę szkoleniową SpecAudy.



SAFETY PROJECT

VI Międzynarodowy Kongres Naukowo-Techniczny SAFE PLACE

Tegoroczna edycja VI Międzynarodowego Kongresu Naukowo-Technicznego SAFE PLACE 2023 Odporność budynków użyteczności publicznej i Infrastruktury Krytycznej wobec zagrożeń wojennych, hybrydowych i terrorystycznych odbędzie się od 20 do 22 listopada 2023 r. w Klubie Wojskowej Akademii Technicznej w Warszawie.

Kongres został objęty honorowym patronatem Dyrektora Rządowego Centrum Bezpieczeństwa, Dyrektora NATO DEEP eAcademy, JM Rektora-Komendanta Wojskowej Akademii Technicznej w Warszawie oraz JM Rektora Wyższej Szkoły Bezpieczeństwa Publicznego i Indywidualnego APEIRON w Krakowie.

Do udziału w kongresie zapraszamy zarządzających bezpieczeństwem w obiektach, ekspertów, przedstawicieli instytucji bezpieczeństwa i administracji publicznej, przedstawicieli świata nauki oraz prywatnego sektora bezpieczeństwa, żołnierzy, funkcjonariuszy i wszystkich zainteresowanych tematyką bezpieczeństwa. Takie grono pozwoli na wypracowanie wspólnych wniosków i rekomendacji oraz zapewni wymianę doświadczeń przydatnych we wzmacnianiu odporności obiektów i instytucji na współczesne zagrożenia.



Obrazy tematyczne tegorocznego kongresu będą skupione wokół następujących zagadnień:

- zagrożenia militarne dla bezpieczeństwa obiektów publicznych i infrastruktury krytycznej,
- przygotowanie obiektów do reagowania na zagrożenia wojenne,
- cyberbezpieczeństwo w dobie zagrożeń wojennych, hybrydowych i terrorystycznych,
- ochrona antyterrorystyczna obiektów i przestrzeni,
- zarządzanie bezpieczeństwem obiektów i instytucji w obliczu współczesnych zagrożeń,
- projektowanie nowoczesnych systemów zabezpieczeń technicznych obiektów i obszarów,
- odporność infrastruktury krytycznej oraz obiektów użyteczności publicznej na zagrożenia wojenne, hybrydowe i terrorystyczne,
- bezpieczeństwo obiektów i obszarów kolejowych, obiektów kultury i dziedzictwa narodowego, obiektów sektora finansowego oraz placówek medycznych i szpitali.

Wszelkie informacje organizacyjne znajdują się na stronie internetowej www.safepace.edu.pl. Z uwagi na ograniczoną do 350 liczbę uczestników obrad o zapisach będzie decydowała kolejność zgłoszeń. Zgłoszenie należy wysłać na adres kongres@safepace.edu.pl ●



AXIS COMMUNICATIONS

Axis Van Roadshow 2023

Axis Communications wraz z dystrybutorami AB, ADI, ARPOL i WESCO-ANIXTER zorganizowali Axis Van Roadshow 2023 – cykl wydarzeń, który odbył się w pięciu polskich miastach. W ramach tego nietypowego roadshow producent prezentował swoje najnowsze technologie z zakresu bezpieczeństwa i monitoringu wizyjnego..



Specjalnie przystosowany samochód wypełniony po brzegi najnowszymi produktami Axis zatrzymywał się w Szczecinie, Poznaniu, Wrocławiu, Warszawie i Krakowie, dając okazję do przetestowania wielu swoich produktów i rozwiązań, w tym analizy wideo, kamer nasobnych z przekazem obrazu na żywo oraz wybranych aplikacji partnera technologicznego CamStreamer wgrzywanych bezpośrednio do urządzeń Axis.

Ten nietypowy sposób promocji jest kontynuacją tournée zapoczątkowanego w zeszłym roku w krajach Beneluksu, Niemiec, Austrii i Szwajcarii. Pomysł jest strzałem w dziesiątkę, sądząc po liczbie uczestników polskiej edycji oraz ich zaangażowaniu zarówno podczas testów sprzętu, jak i podczas prelekcji. Przedstawiciele Axisa podkreślali, że Axis Van Roadshow zostało przygotowane zwłaszcza dla osób, które dotychczas nie korzystały z urządzeń tego producenta.

Oprócz prezentacji produktów omówiono najnowsze trendy w technologiach stosowanych w zabezpieczeniach technicznych, poruszono też kwestię związaną z implementacją dyrektywy NIS2 – nowelizacji dyrektywy NIS, pierwszego europejskiego prawa w zakresie cyberbezpieczeństwa, które zacznie obowiązywać w październiku 2024 r.

To pierwsza edycja wydarzenia w tej formie zorganizowana przez polski zespół Axis Communications, ale – jak zapowiadają organizatorzy – na pewno nie ostatnia. Zatem do zobaczenia. ●



POLSKI ZWIĄZEK PRACODAWCÓW OCHRONA

Nowy Zarząd PZPO

Podczas XXXV Walnego Zgromadzenia Sprawozdawczo-Wyborczego, które odbyło się 19 czerwca 2023 r., Polski Związek Pracodawców Ochrona wybrał nowy zarząd związku. Na nową czteroletnią kadencję na Prezesa Zarządu został wybrany Paweł Korzybski.

W skład Zarządu PZPO weszli: Łukasz Koch, Grzegorz Wojtasik, Grzegorz Sawczak, Mateusz Jaszczuk, Ryszard Kaliński, Ryszard Podgórski, Jarosław Kur, a także Prezesi Regionów: Piotr Jakubowski, Artur Podsiedlik i Jacek Wołk.

Nowy prezes Zarządu Paweł Korzybski jest doświadczonym menedżerem rynku ochrony osób i mienia. Od 2015 r. jest prezesem Zarządu Solid Security. Członek Zarządu PZPO w latach 2015-2019. Zwolennik innowacji i nowoczesnych trendów oraz zrównoważonego rozwoju.

Walne Zgromadzeniu PZPO poprzedziła konferencja, której motywem przewodnim były wyzwania dla sektora ochrony wobec sytuacji na rynku pracy, zmian legislacyjnych uwarunkowanych krajowym planem odbudowy oraz sytuacji makroekonomicznej. Podczas konferencji omówione zostały m.in. trendy i rozwój technologii chmurowych, nowe rozwiązania technologiczne dla sektora ochrony bazujące na LTE, oraz perspektywy rozwoju sztucznej inteligencji w branży CCTV i systemach dozoru wizyjnego. ●



AAT SYSTEMY BEZPIECZEŃSTWA

Wandaloodporna kamera IP NVIP-12F-4201 marki NOVUS z obiektywem „rybie oko” oraz aktywnym odstraszaniem

Charakterystyczną cechą wandaloodpornej kamery IP marki NOVUS z obiektywem „rybie oko” jest możliwość aktywnego odstraszania intruza. Pozwala to osobie monitorującej daną przestrzeń kamerą NVIP-12F-4201 na reakcję za pomocą światła lub komunikatów głosowych w momencie wykrycia potencjalnego zagrożenia lub nieprawidłowego zachowania.



Podnosi to bezpieczeństwo miejsca, które jest monitorowane, zniechęcając intruza do dalszych działań przez odstraszanie go. Nie ma wtedy potrzeby bezpośredniej interwencji pracowników ochrony.

Zastosowanie obiektywu typu „rybie oko” umożliwia obserwację całego pomieszczenia za pomocą jednej kamery. Dzięki takiemu typowi obiektywu nie występują „martwe strefy” i oszczędza się zasoby, ponieważ do monitorowania pomieszczenia wystarczy tylko jedno urządzenie. Ponadto dzięki ultraszerokiemu kątowemu widzenia kamery z obiektywem typu „rybie oko” nie wymagają wielu ustawień i precyzyjnego dobierania miejsca instalacji. Dzięki temu są one proste w użyciu i łatwe w konfiguracji.

Dzięki Smart IR kamera dynamicznie dostosowuje poziom wbudowanego w nią oświetlacza podczerwieni do odległości od obserwowanego obiektu, dzięki czemu obraz nie jest prześwietlony, a obiekty są wyraźne, nawet w bliskiej odległości. ●

LINC POLSKA

WYKRZYCZ TO!

Nieodzownym elementem systemu bezpieczeństwa jest możliwość odstraszenia intruzów za pomocą komunikatów głosowych nadawanych przez stację monitorowania. Dzięki temu intruz dostaje jasną informację, że został wykryty i znajduje się w strefie chronionej.

Taki rodzaj głośnej, spersonalizowanej reakcji sprawia, że większość nieproszonych gości zaprzestaje dalszych działań.

Dzięki najnowszej aktualizacji Camect zyskał kompleksową obsługę audio. Można do niego podpiąć system zarówno analogowy, jak i IP wiodących producentów. Mając takie narzędzie, interwencja jest skuteczniejsza, przez co obiekt staje się bezpieczniejszy.

Jak przystało na Smart Hub, Camect poszedł o krok dalej. Wykorzystując integrację audio z Alexa i Google Home Camect, potrafi werbalnie poinformować użytkownika o tym, że na jego posesji wykryto np. kuriera czy wiewiórkę. Teraz korzystanie z systemu staje się jeszcze wygodniejsze, nawet bez patrzenia na ekran. Camect jest po prostu Smart! ●



ROGER

Moduł VISO SMS i integracje central ppoż. w systemie RACS 5



Wprowadzona do oferty pod koniec zeszłego roku druga edycja oprogramowania zarządzającego systemem kontroli dostępu (VISO v2) oferuje szereg nowych funkcji oraz udoskonaleń, wśród których do najważniejszych należy dodanie modułu VISO SMS oraz integracje z centralami pożarowymi (SSP).

Moduł VISO SMS umożliwia monitorowanie i wizualizację zintegrowanych systemów zabezpieczeń w ramach oprogramowania zarządzającego systemem RACS 5 i w wielu przypadkach z powodzeniem może zastąpić zewnętrzne programy SMS. Integracja systemów SPP jest kolejną ważną grupą funkcjonalności, którą dodaje się do istniejących wcześniej integracji: CCTV, VMS, RCP, SMS, BMS, PSIM, SSWiN, wind serwerowych, depozytorów kluczy oraz bezprzewodowych zamków online. W VISO v2 zintegrowano następujące centrale SSP:

- FPA/AVENAR (Bosch),
- Cerberus PRO (Siemens),
- POLON 4000/6000 (POLON-ALFA),
- Integral EvoX (Schrack Seconet).

Możliwości integracji SSP w module VISO SMS:

- wizualizacja stanów centrali pożarowej na mapach,
- lokalizacja stanów centrali na mapach,
- weryfikacja stanów centrali SSP za pośrednictwem CCTV,
- prezentacja procedur postępowania w sytuacjach alarmowych,
- planowanie i rejestracja prac serwisowych systemu SSP,
- rejestracja działań operatora systemu. ●



ZKTECO

Terminal kontroli dostępu SC800

SC800 to jeden z najnowszych terminali kontroli dostępu RFID firmy ZKTeco przeznaczony do zastosowań zewnętrznych. Jego oprogramowanie jest oparte na systemie Linux.

Elegancka w swojej prostocie konstrukcja skrywa od strony hardware'u i software'u bardzo wyrafinowane rozwiązania. Szkielet obudowy terminala wykonano z metalu, a przedni panel ze szkła hartowanego 2,5D stosowanego w telefonach komórkowych. Dzięki temu zapewniono mu wodoodporność i szczelność na poziomie IP65 oraz wandaloodporność IK04.

Terminal SC800 ma kolorowy ekran o przekątnej 2,4 cala i ukrytą klawiaturę dotykową. Wbudowany wielokartowy moduł RFID pracuje na częstotliwościach 125 kHz i 13,56 MHz. Terminal obsługuje protokół Push i jest kompatybilny z oprogramowaniem ZKBioAccess IVS. Zawiera port wejściowy Wiegand do podłączenia zewnętrznego czytnika zbliżeniowego RFID, a dzięki wbudowanemu wyjściu Wiegand może dla kontrolera działać jako czytnik zewnętrzny.

W zależności od konfiguracji SC800 może pracować jako terminal systemu kontroli dostępu lub rejestracji czasu pracy. Ma wbudowany webserwer do zdalnej konfiguracji. Posiada też zgodność z OSDP (wersja 2.1.7). Oprócz wejść i wyjść Wiegand terminal wyposażono w interfejsy: TCP/IP, RS-485, RS-232 (dla drukarki) i WiFi (opcja). Obsługuje wiele standardów RFID i ponad 100 rodzajów kart (w tym Felica, Legic, DESfire EV1/EV2, HID Prox, HID iClass. ●





SECURITY BOOTCAMP

w klimacie PRL

Pomożecie? Pomożemy! – odpowiedzieli chórem security menedżerowie oraz szefowie bezpieczeństwa z różnych firm i instytucji z całej Polski na starcie kolejnej edycji Security BootCamp. Wiosenne szkolenie odbyło się tym razem w PGR w Koszelewie. Przdownicy pracy znakomicie poradzili sobie z przygotowanymi dla nich zadaniami.



Witamy na BootCampie!



Mariusz Kucharski wita uczestników BootCampu



Konkurencja przygotowana przez firmę CIAS



Konkurencja przygotowana przez firmę Geutebrück



Szkolenie z udzielania pierwszej pomocy przygotowane przez Securitas



Konkurencja przygotowana przez Linc Polska i smart-i polegająca na zapamiętaniu numerów tablic rejestracyjnych



Konkurencja przygotowana przez Schrack Seconet Polska



Konkurencja przygotowana przez Nedap Security Management



Anna Twardowska

Nedap Security Management

Nasze warsztaty podzieliliśmy na cztery części. Pierwsza dotyczyła dyrektywy NIS2, druga programowania kart, a trzecia nowego rozwiązania Nedap Security Atlas, które wspomaga zarządzanie autoryzacjami w organizacji. Czwartą część wypełniały rywalizacja i zabawa. Zorganizowaliśmy quiz, który pozwolił uczestnikom sprawdzić wiedzę zdobytą podczas warsztatu.



Daniel Kamiński

smart-i

Przygotowaliśmy stoisko z rozpoznawaniem tablic rejestracyjnych. Z własnego doświadczenia założyliśmy, że w ciągu minuty można odczytać ok. ośmiu tablic. Rekordziści rozpoznali 20! Udało im się to dlatego, że pracowali zespołowo, podzielili pracę między osoby i jako grupa po prostu wykazali się sprytem.



Paweł Cendrowski

CIAS

Pokazaliśmy nasze urządzenia, które służą do ochrony perymetrycznej: bariery mikrofalowe i system napłotowy. Zadanie polegało na tym, że trzeba było drabinę przystawić do płotu i spróbować wejść na pierwszy szczebel. Rekordzista wszedł na czwarty! Na szkoleniu mieliśmy możliwość porozmawiania z klientami końcowymi i w pewnym sensie uświadamiania im, na co w ochronie perymetrycznej należy zwrócić uwagę.



Artur Koman

Geutebrück

Pół roku od ostatniego Security BootCampu pokazało nam, jak szybko świat się zmienia, ponieważ pół roku temu uczestnicy szukali totalnie innych rozwiązań. Dzisiaj interesują ich urządzenia wyposażone w sztuczną inteligencję, głęboką analizę obrazu, machine learning. Branża zabezpieczeń już wcześniej o tym komunikowała, że to jest przyszłość security. I w tym kierunku będziemy podążać.



Krzysztof Bartuszek

Securitas Polska

Chcieliśmy przede wszystkim pokazać, że najważniejsi w branży są ludzie i ich bezpieczeństwo. Stąd też udzielanie pierwszej pomocy jest kluczowym elementem, z którego szkolimy naszych pracowników. Wykorzystujemy do tego najnowszą technologię, mam tu na myśli technologię VR. Szkolimy naszych pracowników, aby na wypadek wystąpienia pożaru wiedzieli co robić. Praca z goglami VR idealnie uzupełnia ćwiczenia fizyczne w tym zakresie. Pomaga w wypracowaniu automatycznej reakcji chociażby w przypadku pierwszej pomocy czy w przypadku postępowania w sytuacjach kryzysowych, gdzie należy wziąć gaśnicę i najwycyziej zacząć gasić. To są te elementy, w których VR pozwala wielokrotnie użyć tej gaśnicy, niekoniecznie od razu ją odpalając.



Piotr Rodak

Schrack Seconet Polska

Tym razem jesteśmy na terenie PGR-u Koszelew, w obiekcie w klimacie PRL-u, dlatego nasze zagadki też dostosowaliśmy do tego klimatu. Uczestnicy mogli się wykazać znajomością filmów z tamtego okresu, dat historycznych, ale też mieli okazję zapoznać się z naszym sprzętem w nieco inny sposób, m.in. zadymiając czujkę z tamtych lat podłączoną do współczesnej centrali.



Jacek Tyburek

DHL Supply Chain Polska

Szkolenie miało charakter gry decyzyjnej. Chodziło o to, aby pokazać, że żyjemy w czasie, w którym przestępstwa w cargo, czyli w transporcie drogowym, bardzo się intensyfikują. To jest duży wzrost. I chciałem koleżankom i kolegom na spotkaniu pokazać, jak wygląda kwestia zarządzania tym problemem i jak lepiej przygotować się do ryzyka, na które wszyscy możemy być narażeni.



Jak szybko wejdiesz na drabinę, zanim wzbudzisz alarm?



Wirtualne szkolenie z wykorzystaniem gogli VR



Zwycięska grupa Brygadzystów. Gratulujemy!



Ciekawej prezentacji warto posłuchać



Jacek Tyburek prowadzi grę decyzyjną



Ile osób zmieściło się do Malucha?



Dariusz Kluska
Reckitt Benckiser

Staramy się wyciągnąć z tych wszystkich sześciu historii największej i najlepiej, jak tylko możemy, by wykorzystać to w naszej pracy, naszych firmach. Wdrożyć te rozwiązania, które naprawdę mają niesamowite znaczenie z punktu widzenia security i przede wszystkim naszych możliwości.



Viktoria Moroz
DHL Supply Chain

Odkrywcą rzeczą dla mnie było użycie VR. Sama je przetestowałam i naprawdę miałam wrażenie, że faktycznie to się ze mną dzieje. Kiedy musiałam skoczyć z palącego się budynku, to miałam obawy.



Maciej Kornacki
Hill International

Sposób, w jaki zostało to przedstawione, był innowacyjny i ciekawy. Myślę, że stworzyły się przez to grupy, które potrafiły się wymienić swoim doświadczeniem, a także potrzebami.



Mateusz Jasina
PKP PLK

Najważniejsze są elastyczność tych systemów i możliwość rozszerzenia ich funkcjonalności na różne obszary i obiekty. Z jednej strony widzimy centralizację, ale z drugiej rozproszenie.

Gdzie się podziało nasze ptasie mleczko?

Załoga działu kreacji dużego producenta kosmetyków luksusowych miała przyjemny zwyczaj, by codzienne poranne zebrania odbywać w towarzystwie dobrej herbaty i ptasiego mleczka. To ostatnie było szczególnie ważne, jako że wszyscy zgodnie uważali, że ptasie mleczko ma zbawczy wpływ na inwencję i wyobraźnię.

Zebrania organizowano w całkiem sporym gabinecie Joanny Jasnej, szefującej działowi. Joasia uwielbia słodczyce, bez opamiętania zajada się czekoladą i zawsze ma jakiś smakołyk w szufladzie biurka. Od lat kieruje się zasadą „cukru nigdy dość”. Niestety, ku rozgoryczeniu koleżanek, jadała i nie tyła. Życie jest niesprawiedliwe.



– Ktoś pożarł nasze ptasie mleczko. Przejrzałam wszystko. Moja szuflada też jest pusta. Ktoś zjadł też te dobre cukiereczki z kuchni. I maślane ciasteczka, które Janek trzymał na czarną godzinę. Są dwie opcje: albo to ja wszystko zjadłam i tego nie pamiętam, albo to ktoś z was. – W głosie Joanny zabrzmiało poważne oskarżenie, choć słychać było też gorycz i żal.

Szok i niedowierzenie

Tuż przed godziną dziesiątą kolejne osoby mościły się w, jak go zwano, „jasnym pokoju”. Każdy z kubkiem herbaty, nieliczni odszczepieńcy z kawą. Brakowało tylko dyrektor Jasnej, która tuż po 10.00 wkroczyła z widocznym marsem na czole.





Wszyscy zgromadzeni popatrzyli na siebie. Na twarzach malowały się szok i niedowierzenie. Zjeść to jedno. Nie raz i nie dwa przydarzyło się osobie siedzącej w nocy nad projektem kampanii buszować po szufladach w poszukiwaniu kalorii. Jednak nigdy nie doszło do takiej patologii, że delikwent zjadł i zapasu nie uzupełnił. Zdumienie sięgnęło zenitu, ale też nikt się nie przyznał do tego karygodnego czynu.

– *To może ja skoczę do sklepu...?* – zaoferował nieśmiało najmłodszy stażem copywriter Karol, nazywany czule TikTokiem.

– *Nie, nie marnujmy teraz czasu, weźmy się do tej nowej kampanii. Jak wicie mamy przy niej sporo poprawek* – zarządziła ponurym głosem Joanna. – *Najwyżej teraz będziemy pracować o suchym pysku, a potem, Karolu, skoczysz do sklepu.*

– *Olu!* – Dyrektor Jasna zwróciła się do kreatywnej graficzki. – *Jak nam idzie z kampanią? Kiedy ruszamy? Bo musimy się zgrać ze sprzedażą.* Aleksandra Hałas już, już miała przystąpić do wyjaśnień, dlaczego uważa, że przed nimi jeszcze długa droga, gdy powietrze przeszło soczyste:

– *O ty w mordę jeża, widzieliście?!* – Janek, drugi grafik, tuż przed sobą trzymał smartfon. Wszyscy jak zahipnotyzowani zbliżyli się do ekranu.

– *To... nasz... krem, ten słoiczek, sama wybierałam* – wyszeptała Ola Hałas, którą w normalnych warunkach niełatwo było zmusić do szeptu.

– *Ale... jak?* – Głos uwiązł jej w gardle.

– *To moje teksty!?* – Z oburzeniem zapytał, a w zasadzie stwierdził Karol, patrząc, jak na ekranie smartfonu wiję się siedemnastoletnia na oko dziewczuszka zachwalająca krem dla pięćdziesięciolatek, którego reklama już na pierwszy rzut oka była kopią tego, nad czym pracowali. – *Podebrali moje teksty! Przecież to ja wymyśliłem to hasło! To nasz krem!*

– *Pomysł nasz, tylko firma jak widzę nie nasza.* Joanna Jasna nie mogła wyjść ze zdumienia. A potem głosem pełnym zgrozy krzyknęła: – *Ktoś nas szpieguje! I okrada* – dodała ciszej – *z ptasiego mleczka też.* Atmosfera zgęstniała.

– *Kochani, mam wrażenie, że dzieje się tu coś złego.* – Dyrektor Jasna zrozumiała, że bez pomocy bezpiecznika się nie obejdzie.

Co my tu mamy?

– *Pan rozumie, że dla nas to bardzo przykra rzecz.* Joanna Jasna nie kryła zdenerwowania. – *Mamy doskonałe laboratorium, genialne*

produkty, ale siłą rzeczy drogie. Nasze reklamy są więc zawsze prze-myślane do ostatniego szczegółu. Pracujemy nad nimi wiele miesięcy. Tymczasem konkurencja dotarła do pomysłu naszej kampanii i reklamuje swój tandetny badziew naszym hasłem...

Grzegorz Jackowiak, zatrudniony kilka tygodni wcześniej specjalista do spraw ochrony, przerwał dyrektor Jasnej i bezceremonialnie przeszedł do rzeczy:

– *IT coś znalazło?*

– *Nie, i w tym problem. Jakby znaleźli wyciek, to wbrew pozorom czułabym się lepiej. Wie pan, my się tu bardzo lubimy, nie chcę, żeby wyszło, że ktoś jest szpicielem. Firma i tak już dużo straciła, nie chcę jeszcze stracić kogoś z ludzi.*

Jackowiak przeszedł do czynów. Na wszelki wypadek odpytał jeszcze IT. Reguły cyberbezpieczeństwa były jednak tak surowe, że żaden bajt z firmy nie mógł wypłynąć niepostrzeżenie. Nie pozostawało mu więc nic innego, jak przespacerować się po biurze. Załoga ze zdumieniem przypatrywała się, jak młody stażem bezpiecznik buszuje po szufladach, oczywiście pytając wcześniej o pozwolenie, przegląda kuchenne szafki, a nawet zagląda do koszy na śmieci.

Kto nas szpieguje?

Grzegorz Jackowiak nabrał podejrzeń co do tego, kto mógł być kretem, ale podejrzania to za mało. Delikwenta trzeba było złapać za rękę. Dlatego postanowił dyskretnie przyjrzeć się temu, co dzieje się w firmie, gdy pracownicy ją opuszczają. Niewidoczne dla postronnych kamery zostały gęsto rozstawione we wszystkich pomieszczeniach. Obraz z nich był przesyłany bezpośrednio na laptop Jackowiaka. Na ekranie miał całe biuro jak na dłoni. Każdy jego zakamarek.

Nadeszła godzina prawdy. Tuż po 18.00 Jackowiak, razem z całą załogą działu kreacji, zaszyli się w pokoiku z materiałami biurowymi. Ostatnia wcisnęła się Ola Hałas, mocno wciągając brzuch. Zaczęła się obserwacja. Było ciasno, duszno i ekscytująco.

Najpierw przez biuro przeszedł pan Tadeusz, pracownik ochrony z dwunastoletnim stażem. Sprawdzał okna, pogasił światła i... sięgnął do szafki kuchennej, gdzie na wabia postawiono kolejne opakowania słodczy. Przyjrzał się im, a następnie ustawił wg kolorów i wielkości pudełek. Lubił porządek. Potem otworzył zmywarkę, przetaił



blat i podlał kwiaty. Następnie przeszedł do głównego pokoju kreacji, po drodze podnosząc papiery walające się przy drukarce, ułożył je w zgrabnym stosiku na klapie urządzenia i powędrował dalej.

– *Uff, już się bałam, że to on.* Dyrektor Jasnej wyraźnie ulżyło. W dusznym pokoiku czas zaczął się dłużyć. Jednak równo o 20.00 wszystkim skoczyło ciśnienie. Do gabinetu Joanny Jasnej wkroczyła bowiem pewna młoda osoba.

– *Widzicie to? Joasiu, przegrzebuj te swoje szuflady!* – W szepcie Karola zabrzmiało wyraźne oburzenie.

– *I zre ptasie mleczko, które zachomikowałam* – dodała ze smutkiem Joanna.

– *I okrada was w najlepsze. W sposób, jak widać, bardzo analogowy* – dodał Jackowiak. – *Szanowni, za chwilę podejmiemy interwencję. Uprzedzam, nie będzie przyjemnie.*



Opracowała Monika Mamakis na bazie scenariusza Jacka Grzechowiaka

• Kto wynosił pomysły na kampanie marketingowe i co było słabym punktem systemu zabezpieczeń w firmie produkującej kosmetyki klasy premium?

Odpowiedzi na te pytania poznali uczestnicy strategicznych warsztatów Security Forum przeprowadzonych 30 stycznia przez Jacka Grzechowiaka, dyrektora Centrum Kompetencji a&s Polska.

Centrum Kompetencji a&s Polska organizuje szkolenia i warsztaty dla osób odpowiedzialnych za bezpieczeństwo fizyczne, cyfrowe i zabezpieczenia techniczne. Przekonaj się, co o warsztatach sądzą osoby, które wzięły w ich udział.

Aleksandra Zaremba-Rybińska, BNP Paribas
Jak zwykle ze spotkań a&s Polska wyniosłam dużo ciekawych informacji. Odpowiadam za nieruchomości, w tym ich bezpieczeństwo, a temat potężniejszego kwestii administracyjnych z bezpieczeństwem rzadko się podejmuje na szkoleniach. Jest to bardzo cenne, zwłaszcza że zdobytą tu wiedzę będę mogła przekazać swoim współpracownikom.



Patryk Tabor, CBRE
Dla mnie takie warsztaty są rewelacyjną formą przekazywania wiedzy. Prosty sposób budowania świadomości osób, które tak na co dzień nie zajmują się bezpieczeństwem, jak ważna jest współpraca całego zespołu oraz wszystkich ludzi zaangażowanych w budowanie tego bezpieczeństwa. I tak naprawdę uświadomienie też tego, że utrzymanie bezpieczeństwa wewnętrznego na właściwym poziomie nie zależy tylko od osób odpowiedzialnych stricte za bezpieczeństwo w firmie.

Kamil Wachowicz, Impel Facility Service

Ze spotkania wyniosłem cenną wiedzę i ciekawe refleksje. Podobają mi się forma warsztatów. Bardzo obrazowa była praca na konkretnych przykładach. Podczas ich omawiania wywiązywała się ciekawa dyskusja, z której można było wyciągnąć wnioski pomocne w naszej pracy. Poznałem też bardzo ciekawych ludzi, z którymi mogliśmy wymienić się doświadczeniami.



SICUREZZA

INTERNATIONAL SECURITY & FIRE EXHIBITION

15-17 NOVEMBER 2023 fieramilano



IN A WORD, MANY SOLUTIONS.

MIBA

MILAN INTERNATIONAL BUILDING ALLIANCE



ONE PLACE. FOUR EXHIBITIONS

INTERNATIONAL NETWORK



www.exposec.com.br



fireshow.com.br

PARTNER



FIERA MILANO



PulsON
ALARM

Bezpieczeństwo
dostosowane
do **Twojego wnętrza**



www.pulsionalarm.pl
kontakt@pulsionalarm.pl

