a&S POLSKA
www.aspolska.pl

CZASOPISMO RYNKU SECURITY
nr 6/2018 (12)
listopad/grudzień
15 zł (w tym 8% VAT)

Światowi liderzy security

ISSN 2451-5175

BADANIE RYNKU

Ranking TOP 50 Security 2018

Lista największych na świecie producentów zabezpieczeń technicznych i obszerne opracowanie nt. kondycji globalnego rynku security.

str. 20

TEMAT NUMERU

Raport: Bezpieczny hotel

Lista incydentów i oszustw, na jakie są narażeni właściciele, zarządcy i klienci hoteli, jest długa. Pojawiają się też zupełnie nowe zagrożenia.

str. 64

BANKING SECURITY

Bezpieczeństwo instytucji finansowych

Polski sektor finansowy należy do najbardziej zaawansowanych technologicznie na świecie. Czy także w obszarze bezpieczeństwa?

str. 86

HIKVISION

24/7 VIVID COLOR CAMERA

0.0005 Lux

F1.0 Super Aperture

DEEP LEARNING DVR

False Alarm Filter

Quick Target Search

Target Extraction

WIĘCEJ NIŻ MOŻESZ ZOBACZYĆ
TURBO HD 5.0

HIKVISION NR 1 NA ŚWIECIE

Hikvision to światowy lider w dostawie innowacyjnych produktów i rozwiązań do monitoringu wideo. Dzięki najsilniejszej w branży kadrze R&D, firma Hikvision rozwija kluczowe technologie kodowania audio i wideo, przetwarzania obrazu wideo oraz związanego z tym przechowywania danych. Aby uzyskać więcej informacji, odwiedź nas na stronie www.hikvision.com/pl/.

Hikvision Poland
The Park Warsaw
ul. Krakowiaków 50
02-255 Warszawa
T +48 22 4600150
info.pl@hikvision.com

ColorVu

Obrazy w żywych kolorach przez całą dobę

Kamery Hikvision ColorVu zapewniają obrazy w jasnych kolorach przez całą dobę, nawet w warunkach słabego oświetlenia. Dzięki zaawansowanym obiektywom i sensorom o wysokiej czułości doskonale radzą sobie z rejestrowaniem żywych obrazów w różnych, nawet trudnych do monitoringu miejscach.

AcuSense

Inteligentna precyzja

Oparty na algorytmach sztucznej inteligencji DVR AcuSense Turbo HD oferuje znacznie lepszą precyzję VCA.

@HikvisionPoland
www.hikvision.com/pl/

Drodzy Czytelnicy

Koniec roku to tradycyjnie czas podsumowań. U nas ma on wymiar nie tylko symboliczny, ale także rynkowy. Już po raz trzeci prezentujemy polskim Czytelnikom **Ranking TOP 50 Security** (s. 20) wraz z obszernym raportem o światowym rynku zabezpieczeń technicznych. Dział analityczny *a&s International* zestawił notowane firmy z branży security o globalnym zasięgu i porównał ich wyniki finansowe. Powstał w ten sposób pełen przegląd wskazujący **kierunki rozwoju rynku**.
Większość firm ujętych w rankingu odnotowała **wzrosty ze sprzedaży**, które wynikają po części z utrzymującego się popytu na rozwiązania związane z zapewnieniem bezpieczeństwa (s. 30). Analizując raport pod kątem przyszłości, zidentyfikowaliśmy **trendy technologiczne, które napędzają rozwój branży** (s. 34).
Raport TOP 50 Security ma wymiar globalny. Prezentujemy zatem charakterystykę i specyfikę poszczególnych **światowych regionów**, którą opracowali dla nas wiodący integratorzy systemów z całego świata (s. 36), bowiem to właśnie oni mają najpełniejszy obraz rynku. Jak co roku publikujemy także **analizę brytyjskiej firmy badawczej Memoori** (s. 42). Tym razem eksperci nie tylko przeanalizowali wskaźniki ekonomiczne globalnego rynku security, ale także przyjrzeli się dominującemu trendowi – analityce wideo opartej na sztucznej inteligencji. Wygląda na to, że **jesteśmy o krok od przełomu** (s. 46).

Dużo uwagi poświęcamy w tym wydaniu przyszłości. Wielką szansą nie tylko dla branży security w Polsce, ale także dla całej naszej gospodarki będzie **nowa rewolucja technologiczna** (s. 48). Jednym z jej przejawów jest wykorzystanie *machine learning* – polecamy artykuł **o czterech typach uczenia maszynowego** (s. 52). Kolejnym trendem, który będzie w najbliższych latach przybierał na sile, jest **świadczenie usług security w chmurze** (s. 58).
Tematem tego numeru jest **„Bezpieczny hotel"** (s. 64). Coraz bardziej wyrafinowane oszustwa są w tym segmencie rynku dużym problemem, a jednocześnie szansą na rozwój branży zabezpieczeń.
Gorącym tematem jest obecnie **bezpieczeństwo instytucji finansowych** (s. 86), o którym – ze względu na nasilające się cyberataki – mówi się coraz głośniej. Polacy chętnie korzystają z zaawansowanych technologicznie usług finansowych, gorzej jest jednak ze świadomością realnych zagrożeń.

Koniec roku to nie tylko czas podsumowań, ale także planów. Już teraz zapraszamy na kolejną edycję **Warsaw Security Summit 2019** (s. 119). Postaramy się, aby ta największa w Europie Środkowo-Wschodniej konferencja naszej branży była także najciekawsza i najbardziej wartościowa. Wkrótce przedstawimy tematy paneli i prelegentów – zapewniamy, że będzie interesująco! W przyszłym roku zorganizujemy kolejne wydarzenia, jakich do tej pory w branży nie było. Jednym z nich będzie **Security BootCamp** – warsztaty strategiczno-terenowe dla security managerów (s. 118). O kolejnych będziemy informowali na bieżąco.
Obiecujemy wiele pozytywnych zaskoczeń!

Marta Dynakowska
redaktor naczelna

Jan T. Grusznic
z-ca redaktora naczelnego

Mariusz Kucharski
dyrektor zarządzający

www.aspolska.pl

a&S POLSKA

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

Redakcja
ul. A. Branickiego 15
Wilanów Office Park, bud. 1
02-972 Warszawa
e-mail: info@aspolska.pl
www.aspolska.pl

Dyrektor zarządzający
Mariusz Kucharski

Redaktor naczelna
Marta Dynakowska

Z-ca redaktora naczelnego
Jan T. Grusznic

Stały felietonista
Andrzej Popielski

Dział marketingu i reklamy
Iwona Krawiec
Patrycja Sołtysik

Dział eventów i konferencji
Aleksandra Czapska

Kolegium redakcyjne
Norbert Bartkowiak
Edmund Basałyga
Sebastian Błażkiewicz
Janusz Bohdanowicz
Marek Domański
Jacek Grzechowiak
Roman Maksymowicz
Dariusz Mostowski
Przemysław Pierzchała
Janusz Sawicki
Stefan Jerzy Siudalski
Jerzy Sobstel
Paweł Wittich
Waldemar Wnęk
Aleksander M. Woronow

Korekta
Jolanta Kucharska

Projekt graficzny
Sylwester Dmowski

Skład
Dorota Cybulska
Sylwester Dmowski

Prenumerata
www.aspolska.pl/prenumerata

W numerze...

WYBRANE WDROŻENIA

axxonsoft

EXPERIENCE THE NEXT

MIASTO KRAKÓW

- 6 serwerów Axxon Next
- 700 kamer
- 8 stacji operatorskich
- ACCR & LPR - wszystkie kamery
- analityka PTZ

axxonext

- Axxon Next jako platforma optymalizowana dla pracy w środowisku miejskim
- Zaawansowane narzędzia do przeszukiwania zdarzeń
- Przeszukiwanie całej sieci kamer pod kątem twarzy i tablic rejestracyjnych (LPR)
- Multidomenowość
- Zaawansowane narzędzia wsparcia operatorów (ściana wideo, time compressor, autozoom)
- Narzędzia zgodności z RODO
- Skalowalność już od jednego kanału
- Bezpłatne aktualizacje
- Interaktywna praca z mapą miasta wraz z wizualizacją zdarzeń i położeniem kamer aby zrozumieć lokalizację zdarzenia
- Narzędzie Tag&Track do wodzenia za obiektami
- Narzędzia statystyczne dostarczające dane o ruchu pieszym i kołowym w mieście

CLIP

- Architektura systemu:
  - 2 serwery Axxon Intellect
  - 3 serwery Axxon Next
- 250 kamer
- 7 stacji operatorskich
- ACCR & LPR - 9 kamer

axxonext Intellect

- Zintegrowany system bezpieczeństwa Axxon Intellect Enterprise jako wielofunkcyjna, otwarta platforma PSIM
- Axxon Next do rejestracji i zaawansowanej analizy wideo
- Narzędzie Tag&Track do wsparcia współpracy kamer statopozycyjnych i obrotowych
- Rozpoznawanie tablic na wjeździe
- Inteligentne przeszukiwanie archiwum pod kątem zdarzeń, twarzy i tablic rejestracyjnych
- Detekcja pociągu
- Możliwość wizualizowania zdarzeń z innych systemów (takich jak domknięcie elektrozwor, bram itp.)
- Bezpłatne aktualizacje
- Usługa generowania metadanych w czasie rzeczywistym

ORANGE

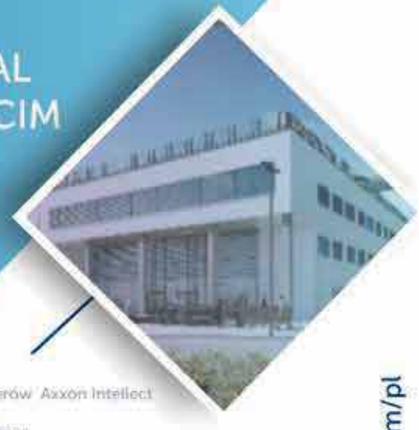
- Zintegrowany system bezpieczeństwa Axxon Intellect Enterprise jako wielofunkcyjna, otwarta platforma PSIM, zoptymalizowana do zarządzania rozbudowaną bazą użytkowników
- Narzędzia zgodności z RODO
- Zaawansowane narzędzia wsparcia operatorów (moduł importu użytkowników, interaktywna mapa zbiorcza, moduł edycji szablonów do identyfikatorów, moduł zarządzania użytkownikami)
- Bezpłatne aktualizacje
- Przeszukiwanie bazy użytkowników z uwzględnieniem dowolnie wybranych atrybutów i przedziałów czasowych
- Zoptymalizowany panel alarmów informujący o aktualnych stanach elementów systemu we wszystkich nadzorowanych obiektach
- Rozbudowane narzędzia do zarządzania obiektami oraz wyszukiwania zdarzeń
- Pełna integralność systemu zapewniająca korzystanie z tej samej bazy użytkowników przez różne moduły
- Interaktywna praca z mapą Polski wraz z wizualizacją zdarzeń oraz rozmieszczeniem elementów systemu na planach poszczególnych budynków.

- Architektura systemu:
  - 1 serwer główny + 1 serwer redundantny
  - 2 serwery LPR
  - 12 stacji operatorskich
- 268 kontrolerów
- 1775 czytników
- 107 obsługiwanych lokalizacji w całej Polsce
- 37006 użytkowników

Intellect NODER

SZPITAL PROKOCIM

- Zintegrowany system bezpieczeństwa Axxon Intellect Enterprise jako wielofunkcyjna, otwarta platforma PSIM
- Wyświetlanie, odtwarzanie i zarządzanie dowolnymi kamerami.
- Tworzenie, zmienianie oraz przeszukiwanie bazy danych systemu KD i zarządzanie przepustkami
- Interaktywna praca z mapą obiektu wraz z wizualizacją zdarzeń oraz rozmieszczeniem elementów systemu na planach poszczególnych budynków.
- Zoptymalizowany panel alarmów informujący o aktualnych stanach elementów systemu we wszystkich nadzorowanych obiektach
- Bezpłatne aktualizacje
- Narzędzia zgodności z RODO
- Przeszukiwanie bazy użytkowników z uwzględnieniem dowolnie wybranych atrybutów i przedziałów czasowych



- 8 serwerów Axxon Intellect
- 750 kamer
- 9 + 54 stacje kliencki
- 1700 czytników
- 415 kontrolerów

Intellect NODER

www.axxonsoft.com/pl

AXIS P3717-PLE – cztery w jednym

AXIS
www.axis.com/pl

Panoramiczna kopułkowa kamera sieciowa AXIS P3717-PLE o rozdzielczości 8 Mpix umożliwia elastyczne pozycjonowanie czterech zmiennoogniskowych modułów optycznych w ramach jednego urządzenia. W efekcie można uzyskać panoramiczny widok 360° lub kombinację 4 podglądów i powiększonych szczegółów obrazu w wysokiej rozdzielczości. Ponadto oświetlenie w podczerwieni (indywidualnie sterowane diody IR LED) umożliwia kalibrację obrazu nawet w ciemności. Innowacyjne technologie Axis – Lightfinder, Forensic WDR i Zipstream – gwarantują wysoką jakość obrazu i umożliwiają dokładną jego analizę za pomocą odpowiednich algorytmów. Kamera „4 w 1" ma jeszcze jedną zaletę – niższy całkowity koszt okablowania i usług instalacyjnych. Dodatkowo w przypadku zerwania połączenia z serwerem kamera może utrzymać ciągłość zapisu, uruchamiając archiwizację na opcjonalnie zainstalowanej karcie pamięci.
Kamery AXIS P3717-PLE w zintegrowanej obudowie mogą być stosowane zarówno w pomieszczeniach zamkniętych, jak i na zewnątrz: w miejscach użyteczności publicznej, w obiektach o rozgałęzionych korytarzach, na narożnikach budynków. Funkcjonalność AXIS P3717-PLE pozwala korzystać z tej kamery w ramach szeroko rozumianych inwestycji budowlanych. Monitoring wizyjny „4 w 1" stanowi wsparcie dla różnych systemów zabezpieczeń, np. KD – stały, 24-godzinny dozór bram wejściowych i wyjściowych oraz sektorów prac krytycznych, ciągów komunikacyjnych, składowisk materiałów, a nawet wind czy dźwigów.

BCS-SFIP21200IR-II z obiektywem *fisheye*

BCS
www.bcscctv.pl

BCS-SFIP21200IR-II to topowy przedstawiciel rodziny kamer z obiektywem typu *fisheye* w ofercie marki BCS. Superczuły 12-megapikselowy przetwornik Sony STARVIS oraz szerokokątny obiektyw o ogniskowej 1,98 mm sprawiają, że ten model kamery stanowi potężne narzędzie monitoringu wizyjnego. Dzięki nim można uzyskać obraz o kącie widzenia 180° tworzący panoramę 360°, bez tzw. martwych stref. Kamera sprawdzi się w dozorze rozległych otwartych przestrzeni, wymagających pełnego pokrycia monitorowanego obszaru – lotnisk, centrów handlowych, banków czy hoteli.
Zastosowanie kamery BCS-SFIP21200IR-II przynosi wiele korzyści, przede wszystkim zapewnia możliwość zastąpienia wielu kamer jedną typu *fisheye*. Obraz transmitowany do rejestratora można rozłożyć (tzw. *dewarping*), tworząc maksymalnie 8 wirtualnych kamer PTZ. Każdą z nich można wykorzystać do dokładniejszej obserwacji interesującej strefy.
Kamera udostępnia funkcje inteligentnej analizy obrazu – przekroczenia linii oraz naruszenia strefy, ale przede wszystkim mapy cieplnej. Za jej pomocą można w graficzny sposób zobrazować strefy o największym natężeniu ruchu, co może stanowić cenne dane analityczne.
Ponadto kamera została wyposażona w promiennik podczerwieni, moduł audio, wandaloodporną obudowę o klasie szczelności IP67 i klasie odporności mechanicznej IK10, dzięki czemu może znaleźć zastosowanie również w monitoringu wizyjnym stref podwyższonego ryzyka, takich jak cele więzienne czy sale przesłuchań.

Systemy RCP oparte na kontrolerach ASA4214F oraz ASA6214F

Dahua Technology Poland
www.dahuasecurity.com/pl

Firma Dahua Technology wprowadziła do sprzedaży nową linię produktów do systemów KD i RCP. Jednymi z ciekawszych urządzeń są dwa bliźniaczo podobne kontrolery ASA4214F oraz ASA6214F. Autoryzację można przeprowadzić na 4 różne sposoby, posługując się hasłem, kartą lub brelokiem, odciskiem palca oraz na podstawie rozpoznawania twarzy. Możliwe są również ich kombinacje.
Pierwszy model ma pamięć „tylko" 1000 wzorów twarzy, wyższy umożliwia zapis nawet do 3 tys. charakterystycznych wzorów twarzy. Oba mogą obsłużyć do 3 tys. odcisków palców oraz 30 tys. kart. Log zdarzeń umożliwia zapamiętanie nawet do 150 tys. rekordów.
W urządzenie wbudowano dwie kamery – jedna pokazuje na wyświetlaczu obraz „na żywo", druga służy do rozpoznawania twarzy, pracując w podczerwieni.
System jest łatwy w programowaniu i obsłudze. Do zaprogramowania obu urządzeń z podwójną biometrią służy ekran dotykowy 4,3" z intuicyjnym menu. Użytkowników można dodać w łatwy sposób, wprowadzając wzory ich twarzy, odciski palca (możliwe po 3 dla każdej osoby), przypisując im kartę lub hasło z klawiatury. Dzięki zaawansowanym technologiom systemu nie można oszukać przez podstawienie zdjęcia lub zapisu wideo z zaprogramowaną uprzednio osobą. Czas rozpoznawania twarzy jest krótszy niż 1 s.
Do generowania raportów rejestracji czasu pracy służy bezpłatne oprogramowanie SmartPSS.
Wyjście z interfejsem Wieganda umożliwia podłączenie do systemów KD innych producentów.

Nowa jakość systemów wideodomofonowych

COMMAX
www.commax.pl

Na rynku wideodomofonowym pojawił się produkt o niespotykanej dotychczas jakości i funkcjonalności. Monitor COMMAX CDV-704MA z panoramicznym 7” ekranem wyświetla obraz z paneli wejściowych wyposażonych w optykę HD 960p (1,3 Mpix), co przekłada się na 3-, a nawet 4-krotnie większą szczegółowość obrazu w porównaniu do standardowych kamer analogowych. Zwiększenie jakości toru wideo nie wymaga dodatkowych zabiegów instalacyjnych – system pracuje poprawnie na standardowym okablowaniu. Na monitorze można również wyświetlać obrazy z dodatkowych kamer obserwacyjnych pracujących również w rozdzielczości AHD 1,3 Mpix. System przeznaczony do zabudowy jednorodzinnej można rozbudować do 4 monitorów, zapewniając selektywną łączność interkomową między nimi. Na wbudowany moduł pamięci (możliwość rozbudowy o karty microSD) zostają zapisane zdjęcia lub filmy podczas wywołania monitora oraz w przypadku wykrycia ruchu na obrazie z wybranej kamery. Obsługę ułatwia ekran dotykowy. Monitor jest dostępny w dwóch wersjach kolorystycznych: klasycznej biało-perłowej oraz designerskiej ciemnoszarej z granatowym akcentem wokół ekranu.
Monitor obsługuje panele wejściowe COMMAX – analogowe oraz z optyką HD 1,3 Mpix. Użytkownik może wybrać modele do montażu na wąskich słupkach (np. DRC-4CPHD) lub klasyczne (np. DRC-41UNHD), wyposażone w czytnik kart/breloków i/lub klawiaturę kodową, umożliwiające otwarcie furtki i bramy za pomocą kodu i/lub transpondera zbliżeniowego (np. DRC-40DKHD).

Genway: Kamera Tiandy 2MP TC-NCL214C

Genway
www.tiandy.pl

Kolejnym przedstawicielem klasy ekonomicznej kamer Tiandy jest model TC-NCL214C. Przy zachowaniu konkurencyjnej ceny znajdziemy tam kodowanie H.265 i analizę obrazu. Całość zamknięto w kompaktowej obudowie w kształcie tuby o wymiarach 208 x 82 x 31 mm.

Budowa kamery
W kamerze zastosowano przetwornik obrazu o wysokiej czułości (0,05 luksa) i rozdzielczości 2 Mpix, który połączono z jasnym szklanym obiektywem o aperturze F1.2. Ogniskowa obiektywu 4 mm umożliwia uzyskanie kąta widzenia 90° w poziomie. Zastosowanie kodeka H.265 pozwala na obniżenie do 50% zajętości pasma sieciowego w porównaniu do H.264, a tym samym oszczędność miejsca na dysku twardym, potrzebnego na zarejestrowanie materiału wizyjnego.

Analiza obrazu
W kamerze zaimplementowano funkcje inteligentnej analizy obrazu IVA: przekroczenia wirtualnej linii i naruszenia obszaru. To znaczne rozszerzenie popularnej detekcji ruchu, która analizuje wyłącznie zmiany kontrastu obrazu. Dzięki IVA kamera analizuje faktyczne obiekty, które naruszą linię lub obszar. Mogą być analizowane również nieprawidłowości wizji i fonii. Kamery są objęte 3-letnią gwarancją.
Więcej na www.tiandy.pl

PNM-9320VQP: PTZ i kamera wielosensorowa w jednym

Hanwha Techwin Europe
www.hanwha-security.eu

Hanwha Techwin wprowadza do oferty nową kamerę hybrydową PNM-9320VQP. Składa się ona z wbudowanej centralnie kamery PTZ full HD z 32x zoomem optycznym oraz czterech modułów kamer stacjonarnych, rozmieszczonych na obwodzie wokół kamery PTZ, mogących pracować z maks. rozdzielczością 20 Mpix. Każdy moduł kamer stacjonarnych może być wyposażony w jeden z wymiennych obiektywów o ogniskowej: 2,4 mm, 2,8 mm, 3,6 mm lub 12 mm w wersji 2 Mpix lub 3,7 mm, 4,6 mm lub 7 mm w wersji 5 Mpix. Kamery obsługują kompresję H.265 i H.264, do 10 niezależnie transmitowanych strumieni danych, WDR o dynamice 150 dB, żyroskopową stabilizację obrazu, przełomową metodę transmisji WiseStream II ograniczającą pasmo do 75% w stosunku do standardowego H.264 oraz bogaty zestaw funkcji analizy obrazu. Całość uzupełnia funkcja wykrywania i korekcji mgły, dwa gniazda kart SD o łącznej pojemności 512 GB oraz funkcja PTZ Handover – automatyczne przekazanie do kamery PTZ pozycji obiektu obserwowanego przez jedną z wbudowanych kamer stacjonarnych (np. wskutek zadziałania analityki obrazu), a następnie uruchomienie automatycznego śledzenia PTZ.
Cyberbezpieczeństwo to mocna strona nowych modeli. Szyfrowane pliki firmware i konfiguracji, brak haseł domyślnych, wymuszanie wysokiej komplikacji haseł, autentykacja SSL i TLS/EAP, filtrowanie adresów IP to niektóre technologie gwarantujące najwyższą jakość zabezpieczeń, o znaczeniu kluczowym w obiektach przemysłowych czy infrastruktury krytycznej.

EasyIP 4.0 – produkty z technologią AcuSense

Hikvision
www.hikvision.com/pl/

Hikvision, czołowy dostawca innowacyjnych produktów i rozwiązań do systemów monitoringu wizyjnego, wprowadza na rynek nową serię kamer i rejestratorów EasyIP 4.0 dla małych i średnich firm. Produkty tej serii korzystają z najnowszej kompresji obrazu H.265+, dzięki czemu zapotrzebowanie na przepustowość sieci i pojemność pamięci jest mniejsze nawet o 50% w porównaniu z H.265. Zapewnia to duże oszczędności w zakresie IT. Seria EasyIP 4.0 wprowadza też szereg innowacji technologicznych, pomocnych w maksymalizacji dozoru i poziomu bezpieczeństwa. Obejmują one m.in. technologię Hikvision AcuSense – oparty na algorytmach AI klasyfikator obiektów.
Implementacja technologii Hikvision AcuSense w kamerach IP i rejestratorach NVR serii EasyIP 4.0 pomaga odfiltrować fałszywe alarmy, umożliwiając szybszą reakcją na rzeczywiste zagrożenia. Jej działanie polega na wykrywaniu i klasyfikowaniu obiektów, z podziałem na ludzi i pojazdy. Dzięki temu potrafi skutecznie odfiltrować fałszywe alarmy wywołane m.in. przez poruszające się na wietrze liście, gałęzie, zwierzęta czy „grę" świateł. Jako rozszerzenie możliwości rejestratory EasyIP 4.0 oferują funkcję szybkiego wyszukiwania celu, która w razie incydentu pozwala operatorom szybko znaleźć materiał pochodzący od konkretnego obiektu. Oszczędza to wiele godzin przy przeszukiwaniu ręcznym.

Hikvision: AXHub DS-PWA32-N

Hikvision
www.hikvision.com/pl/

Firma Hikvision poszerza ofertę o nowatorską centralę alarmową do małych i średnich obiektów, głównie mieszkalnych i biurowych. Centrala AXHub łączy w niedużym urządzeniu system alarmowy obsługujący do 32 czujek bezprzewodowych oraz system wideoweryfikacji zdarzeń na podstawie podglądu z kamer IP Hikvision. System oparto na uznanym dwukierunkowym systemie bezprzewodowym Enforcer firmy Pyronix pracującym na częstotliwości 868 MHz i doświadczeniu Hikvision jako producenta systemów dozoru wizyjnego.
Ważnym atutem AXHub jest dostępność interfejsów komunikacyjnych, umożliwiających rejestrację w chmurze Hik-Connect. Już podstawowa wersja urządzenia jest wyposażona w łączność Ethernet i Wi-Fi, są też wersje z dodatkowym modemem GPRS lub 3G/4G. Wybranym kanałem komunikacji można przekazywać komunikaty Contact ID do stacji monitoringu.
Centralę można obsługiwać za pomocą aplikacji Hik-Connect, która pozwala na sterowanie systemem, odbiór powiadomień o zdarzeniach, a także podgląd zdarzeń (wideoweryfikację). W przypadku wystąpienia zdarzenia powiązanego z kamerą użytkownik może obejrzeć 7-sekundowe nagranie (5 s pre-alarmu oraz 2 s po wystąpieniu zdarzenia). Systemem można sterować również za pomocą jednego z 8 pilotów sterujących Pyronix lub breloków zbliżeniowych Mifare.
Powiadamianie o zdarzeniach w systemie może odbywać się także w klasyczny sposób poprzez jeden z 2 bezprzewodowych sygnalizatorów Pyronix oraz komunikaty głosowe emitowane z urządzenia.
Centralę konfiguruje się poprzez interfejs dostępny przez przeglądarkę www.

Głośnik Q-SC-P620 marki TOA

Linc Polska
www.linc.pl

Klasyczny system monitoringu wizyjnego zapewnia podgląd na żywo i zapis zdarzeń alarmowych. W przypadku zdalnej ochrony obiektów warto mieć narzędzie, które pozwoli zareagować i odstraszyć niepożądane osoby. Dobrym rozwiązaniem jest rozbudowanie ww. systemu o kilka głośników, które przekażą komunikaty głosowe intruzowi. Praktyka pokazuje, że komunikacja audio pełni bardzo ważną funkcję w systemach zabezpieczeń, a reakcja głosowa na zdarzenie często wystarczy, aby wyeliminować zagrożenie.
Głośnik tubowy Q-SC-P620 marki TOA to rozwiązanie przeznaczone do współpracy z systemami monitoringu wizyjnego. Jego instalacja jest prosta, ponieważ większość elementów jest zintegrowana wewnątrz urządzenia. Wystarczy podłączyć zasilanie 12 VDC, sygnał audio z kamery czy z rejestratora i gotowe.
Dzięki zaawansowanej konstrukcji głośnik jest przystosowany do pracy na zewnątrz w wysokiej temperaturze i trudnych warunkach atmosferycznych. Metalowa obudowa i nierdzewny uchwyt zapewniają niezawodną pracę. W głośniku zintegrowano 20-watowy wzmacniacz audio klasy D, gwarantujący wysoką słyszalność odtwarzanych komunikatów, z zachowaną doskonałą jakością dźwięku.
Głośnik tubowy Q-SC-P620 marki TOA to idealny wybór do zastosowań zarówno wewnętrznych, jak i w zabezpieczaniu terenów zewnętrznych, np. centra miast, otwarte magazyny, farmy wiatrowe czy fotowoltaiczne, dworce, lotniska. To doskonałe uzupełnienie systemów zabezpieczeń.

VISOCALL IP System przyzywowy i komunikacji

Schrack Seconet Polska
www.schrack-seconet.pl

Systemy przyzywowe VISOCALL IP umożliwiają osobom potrzebującym pomocy zaalarmowanie personelu w przypadku pojawienia się zagrożenia ich zdrowia lub życia. Oprócz obiektów szpitalnych stosuje się je również w toaletach dla osób niepełnosprawnych w obiektach użyteczności publicznej i hotelach.

Najważniejsze cechy systemu:

- rozproszona architektura oparta na sieci LAN,
- odbieranie przywołań na urządzeniach w różnych lokalizacjach, wskazanych przez inwestora,
- teksty w systemie zgodne z występującymi w obiekcie,
- integracja z telefonami, serwerami sygnałów alarmowych, systemem sygnalizacji pożarowej itp.,
- szeroka gama urządzeń z komunikacją głosową i bez niej,
- możliwość podłączania przycisków zewnętrznych, np. w saunach,
- kasowanie alarmów za pomocą kart RFID lub standardowo przyciskiem kasującym,
- kasowanie zdalne przywołań po nawiązaniu rozmowy,
- możliwość oddelegowania personelu po akceptacji przywołania,
- integracja z systemem BMS w celu przekazywania informacji o uszkodzeniu.

Cechy te umożliwiają dopasowanie systemu do potrzeb użytkownika, zapewnienia najwyższego poziomu bezpieczeństwa i optymalizacji procesów.

Aktem prawnym nakazującym stosowanie systemów przywoławczych w hotelach jest Rozporządzenie Ministra Gospodarki i Pracy z 19 sierpnia 2004 r. w sprawie obiektów hotelarskich i innych obiektów, w których są świadczone usługi hotelarskie (z późn. zm.).

Synology Surveillance Station

Synology
www.synology.com/pl-pl

Synology Surveillance Station to bezpłatne oprogramowanie przeznaczone na serwery sieciowe Synology, które służy do kompleksowej obsługi stacji monitoringu wizyjnego opartej na systemie NAS. Klient, kupując serwer NAS, otrzymuje 2 licencje na urządzenia (kamery IP, głośniki IP lub inne sterowniki). Licencje na kolejne należy dokupić. Surveillance Station oferuje zaawansowane funkcje z zakresu rejestracji, odtwarzania i analizy obrazu oraz zarządzania uprawnieniami użytkowników. Integracja stacji monitoringu z systemem NAS daje ogromne możliwości w zakresie zabezpieczenia nagrań i zapewnienia ciągłości pracy systemu. Wbudowane funkcje kopii bezpieczeństwa, system centralnego zarządzania rejestratorami (CMS) czy możliwość łatwego zapewnienia redundancji zasilania są niewątpliwym atutem, podobnie jak ciągły rozwój i dodawanie nowych funkcji przez producenta.

W wersji 8.2 system zyskał nowe możliwości:

- Obsługa głośników IP – pozwala na planowane transmisje dźwięku.
- Funkcja *Time Leapse* – pozwala sprawnie przeglądać i streszczać długie nagrania.
- Transmisja na żywo do serwisu YouTube, bez potrzeby instalowania dodatkowego oprogramowania.
- Podwójna autoryzacja dostępu do nagrań zapewniająca ochronę prywatności i nagrań.
- Aplikacja LiveCam na smartfony zmieniająca je w kamerę IP.
- Ulepszona aplikacja DS Cam na smartfony do podglądu na żywo, przeszukiwania i oglądania nagrań.
- Narzędzie *Application Center* to nowy styl dodatków – 26 aplikacji i narzędzi dodających kolejne funkcjonalności do systemu.

TP-Link: kontroler Omada Cloud OC200 do centralnego zarządzania siecią

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

TP-Link wzbogaca serię urządzeń biznesowych o kontroler sprzętowy Omada Cloud OC200. Umożliwia on zarządzanie siecią bezprzewodową zbudowaną z punktów dostępowych *(Access Point)* serii Omada przez chmurę z dowolnego miejsca na świecie z dostępem do Internetu. To idealne rozwiązanie sieciowe dla małych i średnich firm do centralnego zarządzania urządzeniami z serii Omada. Monitorowanie statystyk ruchu w czasie rzeczywistym i ich analiza poprzez wbudowane narzędzia wizualizacji danych, uwierzytelnianie gości za pomocą strony powitalnej, aktualizacja i restart systemu oraz łatwe skalowanie sieci to funkcje, które wspomogą rozwój każdej firmy. Wystarczy podłączyć OC200 do sieci LAN – nie jest wymagany komputer lub serwer z oprogramowaniem zarządzającym. Kontrolerem OC200 można zarządzać zdalnie poprzez chmurę zarówno za pośrednictwem aplikacji na urządzenia mobilne z systemem iOS lub Android, jak i przeglądarki WWW.

Zasilanie przez port Micro USB lub w standardzie PoE 802.3af/at znacznie ułatwia instalację i obniża jej koszty. Drugi port USB jest przeznaczony do aktualizacji oprogramowania lub tworzenia kopii zapasowych konfiguracji sieci.

Producent zadbał o jakość i trwałość konstrukcji urządzenia i jego obudowy. Zaawansowany, wydajny chipset pozwala na użytkowanie OC200 nawet w firmach posiadających rozbudowane, wymagające sieci.

Kontroler Omada Cloud jest objęty 5-letnią gwarancją.

ŚNIADANIE EKSPERTÓW

Bezpieczeństwo w handlu

Sztuczna inteligencja, Internet Rzeczy, biometria i roboty – czy tak będzie wyglądał nowoczesny handel? O nowych technologiach w branży retail rozmawiali uczestnicy kolejnego śniadania ekspertów „a&s Polska”. W ożywionej dyskusji wzięli udział przedstawiciele producentów z rynku security i szefowie bezpieczeństwa z firm handlowych.

Czy koniec tradycyjnych sklepów jest bliski? Czy *e-commerce* zdominuje handel? By konkurować z zakupami online, sklepy stacjonarne sięgają po nowe technologie.
Dyskusja przedstawicieli branży zabezpieczeń z odbiorcami i użytkownikami końcowymi systemów security odbyła się 15 października, tradycyjnie w warszawskim hotelu Westin.

Film ze spotkania na:
http://aspolska.pl/sniadanie-handel-2018/

Karol Stec
Polska Izba Handlu i Dystrybucji

Rozmowy dotykały z jednej strony możliwości sprzętu, z drugiej strony – oczekiwań branży handlowej, zderzenia tych dwóch światów, dwóch punktów widzenia, które na tym spotkaniu mogą znaleźć jakąś platformę porozumienia, określenia wzajemnych relacji, oczekiwań i rozwiązań, które mogą być zastosowane w handlu detalicznym.

Maciej Pietrzak
Dahua Technology Poland

Dyskusja oscylowała wokół stosowania analityki wideo w centrach handlowych, współpracy między systemami security a systemami stricte marketingowymi.

Bardzo dobre i bardzo udane spotkanie. Bardzo ciekawy głos ze strony integratorów i firm, które świadczą takie usługi. Oni łączą te dwa światy: producentów i klientów, którzy mają oczekiwania albo czasami mają problem z wyartykułowaniem tych oczekiwań.

Jan Grusznic
a&s Polska

Mirosław Lukowski
Carrefour Polska

Uważam, że dyskusja była bardzo ciekawa, tematyczna, merytoryczna i potrzebna, bo połączenie interesów zarówno dostawców w naszej branży, jak i odbiorców, czyli nas, jest bardzo ważne. Doskonałą okazją spotkania się, porównania naszych problemów z problemami dostawców są takie właśnie spotkania, podczas których na luzie można porozmawiać o wszystkich swoich problemach.

Jacek Wójcik
Optex Security

Jak zwykle najbardziej warte uwagi jest wysłuchanie opinii odbiorców systemów, do których adresujemy nasze rozwiązania. Wysłuchanie tego, czego oni oczekują, żebyśmy wiedzieli, w którym kierunku mamy się rozwijać.

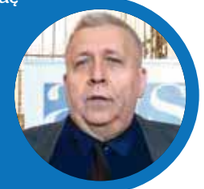
Wiele wniosków może wyciągnąć zarówno jedna, jak i druga strona: w którym kierunku należy się poruszać, jakie rzeczy należy poprawić w produktach...

Artur Nowakowski
Linc Polska

Marcin Walczuk
NSS

Mówiliśmy o możliwościach pozyskiwania nowych informacji z systemów monitoringu, które – jak to było na tym spotkaniu wspomniane – nie są już tylko zwykłą telewizją dozorową, ale mogą dostarczać więcej danych do analizy czy to zachowań ludzi, czy strategii marketingowej tak, aby sieci handlowe mogły się odpowiednio rozwijać.

Nie tylko piszę dla „a&s Polska”, ale również uczestniczę w tych spotkaniach. A rozmowy kuluarowe naprawdę owocne, dziękuję za zaproszenie i polecam.



Michał Czuma
ekspert bezpieczeństwa

Zobaczyłem tu zupełnie inne spojrzenie na sieci handlowe i ich potrzeby niż do tej pory miałem jako producent. Bardzo dziękuję za zaproszenie.

Dawid Jakubiak
Hikvision

Roman Marszycki
Securitas

Warto spotykać się z takimi ludźmi, bo następuje wtedy przepływ informacji. Również ja miałem możliwość uzupełnienia wiedzy.

Nieważne, co myślisz o sztucznej inteligencji nie powinieneś jej ignorować!

RAPORT TOP 50 SECURITY 2018
Dział analityczny a&s International zestawił notowane na giełdzie firmy z branży security o globalnym zasięgu i porównał ich przychody ze sprzedaży produktów zabezpieczeń technicznych w 2017 r.

TOP 10 ŚWIATOWI PRODUCENCI SECURITY

(na podstawie przychodów ze sprzedaży w 2017 r.)

1	HIKVISION DIGITAL TECHNOLOGY	Chiny
2	DAHUA TECHNOLOGY	Chiny
3	ASSA ABLOY	Szwecja
4	BOSCH SECURITY SYSTEMS	Niemcy
5	AXIS COMMUNICATIONS	Szwecja
6	FLIR SYSTEMS	USA
7	ALLEGION	USA
8	HANWHA TECHWIN	Korea Płd.
9	TIANDY TECHNOLOGIES	Chiny
10	AVIGILON	Kanada

Tegoroczna lista a&s TOP 50 Security potwierdza, że branża światowych producentów zabezpieczeń technicznych odnotowuje stały wzrost – ubiegłoroczne przychody większości firm notowanych w zestawieniu wrosły średnio o 4,1 proc. Wśród najważniejszych kierunków rozwoju wyraźnie widocznych w ostatnich 12 miesiącach na pierwszy plan wysuwają się zaawansowane narzędzia analizy, które dają użytkownikom pełniejszy obraz sytuacji biznesowej. Wiele firm sprzedaje swoje rozwiązania pod hasłem „sztucznej inteligencji" (AI – *Artificial Intelligence*), choć są też dostawcy niechętnie używający tego terminu. Bez względu na to, czy rzeczywiście mamy do czynienia z AI, zaawansowane narzędzia analityczne umacniają się na rynku i w najbliższych latach będą miały duży wpływ na zapewnienie bezpieczeństwa.

Raport TOP 50 Security składa się z trzech części. Część pierwsza zawiera dyskusję na temat sztucznej inteligencji oraz prognozy na nadchodzący rok. W części drugiej zostały przytoczone opinie integratorów systemów dotyczące sektorów gospodarki o największym wzroście sprzedaży w ostatnim roku. Trzecią część stanowi podsumowanie rynku i technologii w 2018 r. przeprowadzone przez firmę Memoori, będące jednocześnie kompleksowym przeglądem branży zabezpieczeń technicznych.

AI: przełomowa technologia czy medialny szum?

Jeśli mielibyśmy wskazać najważniejszy trend w branży zabezpieczeń w ciągu ostatnich 12 miesięcy, to byłoby nim z pewnością wykorzystanie zaawansowanych mechanizmów analityki, które często określa się mianem sztucznej inteligencji. W jaki sposób mogą one przyczynić się do poprawy bezpieczeństwa i dlaczego niektórzy rynkowi gracze kwestionują termin „AI"?

Zwolennicy podkreślają zalety AI

W porównaniu do często przereklamowanej analityki obrazu (VCA) sprzed lat w zastosowaniach security, współczesne mechanizmy osiągnęły już pewien poziom dojrzałości i okazały się skuteczne w takich zastosowaniach, jak rozpoznawanie obiektów czy inteligentne wyszukiwanie. Stało się to możliwe dzięki kilku czynnikom, takim jak większa moc obliczeniowa procesorów, bardziej zaawansowane, skuteczniejsze algorytmy, dużo większa dostępność danych, na których systemy mogą się uczyć, oraz zrozumienie potrzeb różnych branż. W efekcie powstają rozwiązania ułatwiające użytkownikom osiąganie większej efektywności i świadomości sytuacyjnej.

Wykorzystanie technologii sztucznej inteligencji wraz z oprogramowaniem do analizy zawartości obrazu znacząco wpływa na rozwój rynku, zapowiadając jednocześnie utrzymanie tego trendu w najbliższej przyszłości. Technologia ta staje się coraz bardziej popularna, pozwalając zwiększyć ogólną efektywność podejmowania decyzji – mówi Saurabh Pradeep Sortee, analityk z Grand View Research. – *Implementacja algorytmów sztucznej inteligencji w systemach security pozwala na stosowanie inteligentnych rozwiązań ochrony obwodowej, z pełną automatyzacją wykrywania intruzów i podejmowania właściwych działań.*

Kenneth Hune Petersen
CMO, Milestone Systems

– AI zdecydowanie zwiększa swój udział w całym rynku zabezpieczeń, ponieważ instalacje są coraz większe, zawierają większą liczbę różnych czujników i kamer. Nie jest możliwe, by człowiek był w stanie monitorować wszystkie napływające informacje – uważa Kenneth Hune Petersen, dyrektor Działu Marketingu w Milestone Systems. – *Aby maksymalnie wykorzystać informacje z zainstalowanych urządzeń, należy użyć sztucznej inteligencji do właściwego interpretowania danych.*

Jednym z przykładów zastosowań jest automatyczne wyszukiwanie obiektu. W tym przypadku użytkownik nie musi już spędzać wielu godzin na żmudnym przeglądaniu zarejestrowanego materiału. Wystarczy wprowadzić pytanie, by szybko otrzymać odpowiedni fragment archiwalnego nagrania. – *Dahua jest liderem branży w zakresie korzystania z technologii AI, zwłaszcza stosowania analizy kognitywnej w wymagających rozwiązaniach security. Przy tysiącach kanałów trudno wyszukiwać i przesyłać strumieniowo dane wideo. Technologia Dahua strukturyzuje te dane na podstawie cech charakterystycznych ludzi lub pojazdów, zapewniając funkcje wyszukiwania i analizę dwustopniową* – podkreśla Gao Jiaqi, Overseas Marketing Director w Dahua Technology.

Taka analiza daleko wykracza poza automatyczne wyszukiwanie. Przykładowo, oparte na AI rozpoznawanie twarzy może być bardzo skuteczne i dokładne w dopasowaniu osoby widocznej na ekranie do zdefiniowanej w bazie danych, nawet jeśli ta osoba ma częściowo zakrytą twarz.

Willem Ryan
wiceprezes, Avigilon

– Liczba kamer i nagrań wideo jest obecnie tak duża, że operatorzy muszą znaleźć sposób, by sobie z nimi radzić. Co więcej, potrafią skupić uwagę na krótko. W rozwiązaniu tego problemu może pomóc sztuczna inteligencja, która przeanalizuje o wiele więcej danych wizyjnych, niż mógłby to zrobić człowiek – twierdzi Willem Ryan, wiceprezes ds. marketingu i komunikacji w Avigilon. – *Wspomagane sztuczną inteligencją oprogramowanie do zarządzania wideo pozwala operatorom zwiększyć wydajność i skuteczność pracy bez potrzeby ciągłego obserwowania obrazów na monitorach. Dzięki automatyzacji wykrywania mogą teraz szybko weryfikować krytyczne zdarzenia i reagować na nie. A to nie tylko przyspiesza działania dochodzeniowo-śledcze, ale także umożliwia reakcję na zdarzenia w czasie rzeczywistym.*

Dror Sharon
prezes Magal Security Systems

– Sztuczna inteligencja i uczenie maszynowe zapowiadają znaczną poprawę wydajności istniejących aplikacji oraz wprowadzenie nowych, zaawansowanych funkcji, które wcześniej były niedostępne – mówi Dror Sharon, dyrektor generalny firmy Magal Security Systems. – *Niezależnie od tego, czy wyzwaniem jest wizyjna detekcja zamaskowanej twarzy ukrytej w tłumie, czy też wyizolowanie charakterystycznej sygnatury naruszenia bezpieczeństwa z tła o wysokim szumie otoczenia, AI ma potencjał zwiększania wydajności w przyszłości.*

AI ułatwia analizę biznesową w różnych branżach

– Oferując analizę kognitywną, Dahua powiększa zakres aplikacji o smart retail, in-

teligentne zarządzanie ruchem czy smart parking. Stosujące je organizacje mogą pracować dużo wydajniej, a to przekłada się na większe zyski – mówi Gao Jiaqi. *Opracowwując nowe strategie mające na celu poprawę wyników finansowych, mogą korzystać z bezcennych informacji uzyskanych z analizy biznesowej. Przykładowo, w centrach handlowych technologia analizy kognitywnej Dahua może posłużyć do identyfikowania ruchu klientów i określania wysokości czynszu pobieranego od sprzedawców za wynajem.*

Kontrowersje wokół AI

Niektórzy dostawcy i konsultanci, z którymi były prowadzone rozmowy, mieli problem z samym pojęciem „sztuczna inteligencja". Według nich stosowane obecnie technologie to w najlepszym przypadku zaawansowana analityka, do sztucznej inteligencji wciąż im daleko.

Pierre Racz
prezes i dyrektor generalny firmy Genetec

– Należy być ostrożnym z określaniem różnych rozwiązań inteligentnymi – ostrzega Pierre Racz z firmy Genetec. *– Obecnie bardzo dużo mówi się o AI, które ma zapewniać ogromne zaawansowanie technologiczne. Prawda jest taka, że ta marketingowa „sztuczna inteligencja" w rzeczywistości nie jest jeszcze w stanie zapewnić nam obiecywanych latających pojazdów czy w pełni inteligentnych autonomicznych samochodów.*

To nie jest jedyny krytyczny głos w dyskusji o sztucznej inteligencji...

Anna Sliwon
Research Analyst, IHS Markit

– AI z impetem wkracza do branży security, ale stosowane na tym rynku rozwiązania są jeszcze ograniczone. Przed nami nadal długa droga do osiągnięcia prawdziwie inteligentnych rozwiązań security, które – bazując na inteligentnych systemach – potrafiłyby podjąć niezbędne decyzje dotyczące wymaganych akcji w określonych przypadkach. Nie chodzi jednak o działanie na bazie wcześniej napisanych algorytmów – tłumaczy Anna Sliwon, Research Analyst w IHS Markit.

– Mamy do czynienia z „zaawansowaną analityką", a nie ze „sztuczną inteligencją". AI jest znacznie szerszym pojęciem i obejmuje możliwości daleko wykraczające poza rozpoznawanie obiektów i ich klasyfikowanie – uważa Alex Ganin, Project Manager w BitRefine Group. *– AI oznacza, że komputer dosłownie „myśli". Aby spowodować to myślenie, należy połączyć wiele złożonych technologii.*

Technologiom brakuje obecnie elementu predykcyjnego, np. zdolności przewidywania, że ktoś ma zamiar zrobić coś złego, ponieważ wykazuje zachowanie nietypowe dla jego profilu.

– Istnieje mnóstwo samouczących się algorytmów. Powstały one jeszcze długo przed obecnymi, bardzo obiecującymi algorytmami opartymi na sieciach neuronowych. Te samouczące się mechanizmy, które są w stanie przechwycić obiekty i porównać ich prędkość ze średnią prędkością obiektów w ich otoczeniu, są w gruncie rzeczy prymitywne. Trudno oczekiwać od nich, że automatycznie rozpoznają podejrzane zachowania danej osoby – twierdzi Alex Ganin. *– Sieci neuronowe potrafią wyjątkowo dobrze rozpoznać wszelkie obiekty statyczne, począwszy od twarzy, skończywszy na obiektach w skanerze rentgenowskim. W ostatnim czasie pojawiły się również konwolucyjne sieci neuronowe 3D. Algorytmy te umożliwiają ocenę złożonego wzorca ruchu w celu klasyfikacji zachowania obiektów. Wciąż jednak pozostaje wiele problemów do rozwiązania, zanim ta technologia będzie mogła zostać w pełni wykorzystana w dostępnych na rynku systemach zabezpieczeń. Gdy tylko to się stanie, będziemy mogli rozpocząć tworzenie prewencyjnych systemów CCTV.*

John Distelzweig
dyrektor generalny i wiceprezes ds. security w firmie FLIR Systems

– Na razie nie zaprezentowano publicznie, że produkty oparte na sztucznej inteligencji są w stanie dokonywać bardziej złożonych rozstrzygnięć, np. czy dana osoba działa w podejrzany sposób lub czy dane działanie jest typowe dla określonej osoby, sceny, środowiska – podkreśla John Distelzweig, dyrektor generalny i wiceprezes ds. bezpieczeństwa w firmie FLIR Systems.

Nie oznacza to jednak, że zaawansowana analityka – bez względu na to, jak się ją nazywa – jest faktycznie pozbawiona wartości. To bardzo złożona i potężna technologia, która otwiera ogromne perspektywy w niemal każdym aspekcie życia. Security jest tylko niewielką częścią możliwych zastosowań.

– Uczenie maszynowe i wnioskowanie statystyczne w programach, które dają iluzję inteligencji, zapewniają naszym użytkownikom końcowym większą użyteczność i funkcjonalność rozwiązań. Z ostatnich osiągnięć w zakresie technologii uczenia maszynowego, w szczególności w głębokich sieciach neuronowych, mogą obecnie korzystać wszyscy. Zastosowaliśmy te techniki do poprawy wydajności niektórych naszych kluczowych rozwiązań, m.in. w automatycznym odczycie tablic rejestracyjnych (ALPR) Genetec AutoVu – podsumowuje Pierre Racz.

WARUNKI UDZIAŁU W RANKINGU TOP50

W rankingu mogą uczestniczyć:

- **dostawcy urządzeń i systemów z branży security, w tym produktów telewizji dozorowej, kontroli dostępu, sygnalizacji włamania i napadu oraz produktów z więcej niż jednego z tych segmentów, produkujący pod własną marką lub na zlecenie innych firm;**
- **firmy notowane na giełdzie** ***(Uwaga: co roku a&s International uwzględnia również niewielką liczbę międzynarodowych firm nienotowanych na giełdzie, które udostępniają swoje poświadczone sprawozdania roczne. Ich udział w rankingu jest dokładnie analizowany pod kątem rozpoznawalności marki oraz udziału firmy w rynku międzynarodowym);***
- **firmy, które dostarczą sprawozdania finansowe za pełny 2016 r., pełny 2017 r. oraz za pierwszą połowę 2018 r. Sprawozdania muszą być sprawdzone lub zatwierdzone przez biegłego rewidenta.**

W rankingu nie są uwzględniani: dystrybutorzy, integratorzy systemów, resellerzy, dealerzy, instalatorzy, agencje ochrony osób i mienia, firmy z branży ochrony informacji i bezpieczeństwa pożarowego. Nie są też uwzględniane przychody powiązane z działalnością w tych obszarach.

a&s nie ponosi odpowiedzialności za dane finansowe udostępnione przez firmy. Dla celów porównawczych kwoty podane w innych walutach niż USD zostały przeliczone na USD wg średniego kursu wymiany z dn. 11.07.2017 r. (notowania XE.com). Udział w rankingu i przekazanie wyników finansowych są bezpłatne i dobrowolne.

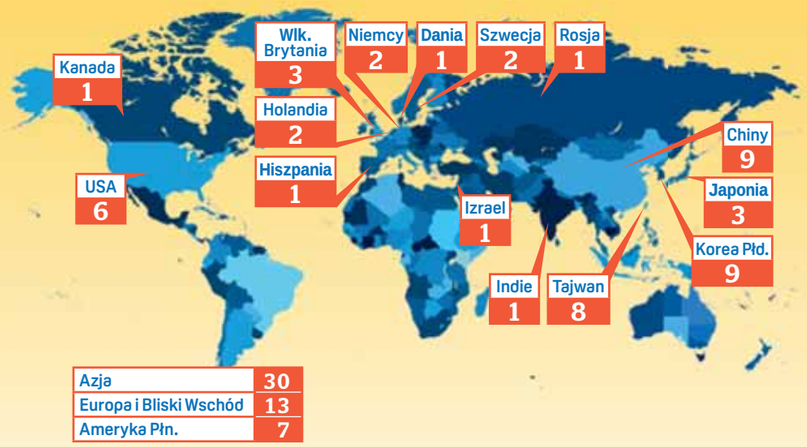
TOP 50 SECURITY 2018

światowi liderzy SECURITY

Ranking 2018	Ranking 2017	NAZWA FIRMY	SIEDZIBA	GŁÓWNY OBSZAR DZIAŁANIA	PRZYCHODY W 2017 (MLN USD)	PRZYCHODY W 2016 (MLN USD)	WZROST PRZYCHODÓW (2016-2017)	ZYSK BRUTTO 2017 (MLN USD)	MARŻA W 2017	ZYSK NETTO 2017 (MLN USD)
1	1	**HIKVISION DIGITAL TECHNOLOGY**	Chiny	różne	5364,08	4242,52	26,4%	1361,09	25,4%	1235,1
2	3	**DAHUA TECHNOLOGY**	Chiny	różne	2680,58	1896,03	41,4%	375,85	14,0%	338,1
3	4	**ASSA ABLOY** (Electromechanical & eletronic locks)	Szwecja	kontrola dostępu	2311,33	2084,12	10,9%			
4	2	**BOSCH SECURITY SYSTEMS**	Niemcy	różne	2087,76	1964,25	6,3%			
5	5	**AXIS COMMUNICATIONS**	Szwecja	różne	967,24	830,41	16,5%	501,33	51,8%	82,7
6	6	**FLIR SYSTEMS** (Surveillance & Security)	USA	telewizja dozorowa	777,21	772,49	0,6%			
7	9	**ALLEGION** (Electronic Products & Access Control)	USA	kontrola dostępu	505,72	447,60	13,0%			
8	8	**HANWHA TECHWIN**	Korea Płd.	telewizja dozorowa	492,64	541,17	-9,0%	214,96	43,6%	
9	11	**TIANDY TECHNOLOGIES**	Chiny	telewizja dozorowa	448,92	344,76	30,2%	172,15	38,3%	
10	12	**AVIGILON**	Kanada	telewizja dozorowa	408,63	353,62	15,6%	211,01	51,6%	28,3
11	10	**AIPHONE**	Japonia	kontrola dostępu	386,68	375,89	2,9%			13,1
12	13	**INFINOVA**	Chiny	telewizja dozorowa	258,39	255,19	1,3%	18,02	7,0%	18,1
13	21	**OPTEX**	Japonia	sygn. włamania i napadu	182,97	170,74	7,2%			29,0
14	16	**VIVOTEK**	Tajwan	telewizja dozorowa	173,79	151,51	14,7%	120,78	69,5%	11,0
15	17	**CP PLUS**	Indie	telewizja dozorowa	170,76	133,67	27,7%	10,62	6,2%	6,6
16	15	**TKH GROUP** (Vision & Security Systems)	Holandia	różne	165,93	163,81	1,3%			
17	14	**NEDAP**	Holandia	różne	163,89	149,30	9,8%			30,4
18	-	**RAYSHARP**	Chiny	telewizja dozorowa	132,48	77,35	71,3%	12,06	9,1%	10,6
19	20	**MILESTONE SYSTEMS**	Dania	telewizja dozorowa	128,35	103,29	24,3%	35,84	27,9%	17,0
20	22	**KEDACOM**	Chiny	telewizja dozorowa	123,62	97,42	26,9%			
21	23	**KOCOM**	Korea Płd.	automatyka domowa	121,41	96,63	25,6%	30,40	25,0%	
22	18	**COMMAX**	Korea Płd.	automatyka domowa	119,00	111,01	7,2%	28,77	24,2%	7,8
23	24	**TAMRON** (Optyka)	Japonia	telewizja dozorowa	101,37	92,05	10,1%			
24	26	**NAPCO SECURITY TECHNOLOGIES**	USA	różne	87,37	82,51	5,9%	29,58	33,9%	5,6
25	19	**IDIS**	Korea Płd.	telewizja dozorowa	79,45	90,54	-12,2%	24,22	30,5%	

Ranking 2018	Ranking 2016	NAZWA FIRMY	SIEDZIBA	GŁÓWNY OBSZAR DZIAŁANIA	PRZYCHODY W 2017 (MLN USD)	PRZYCHODY W 2016 (MLN USD)	WZROST PRZYCHODÓW (2016-2017)	ZYSK BRUTTO 2017 (MLN USD)	MARŻA W 2017	ZYSK NETTO 2017 (MLN USD)
26	27	**TVT DIGITAL TECHNOLOGY**	Chiny	telewizja dozorowa	74,28	74,92	-0,8%	2,76	3,7%	2,9
27	25	**MOBOTIX**	Niemcy	telewizja dozorowa	70,95	86,22	-17,7%			-6,8
28	31	**DYNACOLOR**	Tajwan	telewizja dozorowa	69,82	62,33	12,0%	24,47	35,0%	9,0
29	29	**WANJIAAN INTERCONNECTED TECHNOLOGY**	Chiny	telewizja dozorowa	67,63	64,40	5,0%	8,53	12,6%	7,5
30	30	**SUPREMA**	Korea Płd.	kontrola dostępu	64,22	61,66	4,2%	29,71	46,3%	
31	28	**FERMAX**	Hiszpania	k. dostępu/automatyka dom.	60,97	62,95	-3,1%	34,67	56,9%	34,7
32	33	**SYNECTICS** (System Division)	Wlk. Brytania	telewizja dozorowa	57,01	59,75	-4,6%	5,25	9,2%	
33	34	**IDENTIV**	USA	kontrola dostępu	56,40	52,91	6,6%	22,16	39,3%	
34	32	**GEOVISION**	Tajwan	telewizja dozorowa	50,11	60,14	-16,7%	17,79	35,5%	-6,3
35	36	**ZENO TECHNOLOGY (VIDEOPARK)**	Chiny	telewizja dozorowa	45,99	47,28	-2,7%	3,42	7,4%	3,1
36	40	**COSTAR TECHNOLOGIES**	USA	telewizja dozorowa	44,27	38,56	14,8%	17,84	40,3%	-0,4
37	-	**DSSL (TRASSIR)**	Rosja	telewizja dozorowa	43,78	29,54	48,2%	17,81	40,7%	9,5
38	39	**C-PRO ELECTRONICS**	Korea Płd.	telewizja dozorowa	43,14	41,51	3,9%	7,67	17,8%	0,4
39	38	**INDIGOVISION**	Wlk. Brytania	telewizja dozorowa	42,33	45,92	-7,8%	22,77	53,8%	-2,9
40	46	**INCON** (dawniej Win4NET)	Korea Płd.	telewizja dozorowa	37,34	30,65	21,8%	8,05	21,5%	
41	42	**HITRON SYSTEMS**	Korea Płd.	telewizja dozorowa	31,88	34,90	-8,7%	-0,02	-0,1%	
42	43	**VICON INDUSTRIES**	USA	telewizja dozorowa	26,65	35,76	-25,5%	10,15	38,1%	
43	49	**ITX SECURITY**	Korea Płd.	telewizja dozorowa	26,38	20,80	26,8%	7,06	26,8%	0,4
44	47	**ACTI**	Tajwan	telewizja dozorowa	24,49	30,13	-18,7%	11,53	47,1%	2,1
45	48	**HI SHARP ELECTRONICS**	Tajwan	telewizja dozorowa	23,78	24,07	-1,2%	4,91	20,7%	0,3
46	45	**MAGAL SECURITY SYSTEMS** (Perimeter Products)	Izrael	różne	22,30	32,37	-31,1%	0,24	1,1%	
47	41	**EVERFOCUS ELECTRONICS**	Tajwan	telewizja dozorowa	17,93	36,02	-50,2%	4,94	27,5%	-3,3
48	-	**THRUVISION GROUP** (dawniej Digital Barriers)	Wlk. Brytania	telewizja dozorowa	16,25	30,30	-46,4%	-17,54	-107,9%	
49	37	**AV TECH**	Tajwan	telewizja dozorowa	12,21	21,16	-42,3%	6,20	50,8%	0,5
50	50	**HUNT ELECTRONIC**	Tajwan	telewizja dozorowa	8,61	13,36	-35,6%	1,65	19,1%	-2,1

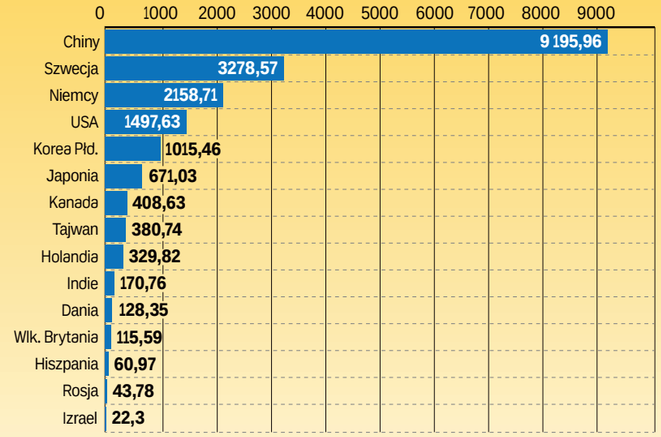
Firmy z Rankingu **TOP 50** na świecie



15 najszybciej rosnących firm

	nazwa	siedziba	Przychody w 2017 (mln USD)	Przychody w 2016 (mln USD)	Wzrost przychodów (2016-2017)
1	**Raysharp**	Chiny	132,48	77,35	**71,3%**
2	**DSSL (Trassir)**	Rosja	43,78	29,54	**48,2%**
3	**Dahua Technology**	Chiny	2680,58	1896,03	**41,4%**
4	**Tiandy Technologies**	Chiny	448,92	344,76	**30,2%**
5	**CP Plus**	Indie	170,76	133,67	**27,7%**
6	**Kedacom**	Chiny	123,62	97,42	**26,9%**
7	**ITX Security**	Korea Płd.	26,38	20,80	**26,8%**
8	**Hikvision Digital Technology**	Chiny	5364,08	4242,52	**26,4%**
9	**KOCOM**	Korea Płd.	121,41	96,63	**25,6%**
10	**Milestone Systems**	Dania	128,35	103,29	**24,3%**
11	**INCON**	Korea Płd.	37,34	30,65	**21,8%**
12	**Axis Communications**	Szwecja	967,24	830,41	**16,5%**
13	**Avigilon**	Kanada	408,63	353,62	**15,6%**
14	**Costar Technologies**	USA	44,27	38,56	**14,8%**
15	**VIVOTEK**	Tajwan	173,79	151,51	**14,7%**

Przychody firm z Rankingu **TOP 50** (mln USD)



Przegląd i prognozy 2018/2019

Większość firm ujętych w Rankingu TOP 50 Security 2018 zanotowała wzrosty ze sprzedaży, które wynikają po części z utrzymującego się popytu różnych branż na rozwiązania związane z zapewnieniem bezpieczeństwa. Wyniki finansowe za pierwsze trzy kwartały 2018 r. wskazują, że kończący się rok również będzie udany. Trend utrzyma się także w 2019 r.

Przeglądając tegoroczne zestawienia TOP 50 Security 2018, nie sposób nie zauważyć, że dwa najwyższe miejsca na podium zajęły firmy Hikvision Digital Technology oraz Dahua Technology, która awansowała na drugą pozycję z trzeciej w roku ubiegłym. Tym samym umocnił się status dwóch spółek chińskich (w branży security określanych często wspólną nazwą – „Hikua") jako największych na świecie producentów zabezpieczeń technicznych. Hikvision utrzymał pozycję lidera, osiągając przychody ze sprzedaży produktów o wartości 5,4 mld USD (wzrost o 26,4 proc. w porównaniu z rokiem 2016 r.). Z kolei Dahua odnotowała w 2017 r. przychód o wartości 2,7 mld USD (wzrost o 41,4 proc. w stosunku do roku poprzedniego!).
W tegorocznym zestawieniu na miejscu 18. zadebiutował inny chiński dostawca rozwiązań z obszaru telewizji dozorowej – Raysharp, osiągając w 2017 r. przychody w wysokości 132 mln USD. Firma zwiększyła sprzedaż o 71,3 proc., zajmując tym wynikiem pierwsze miejsce pod względem wzrostu przychodów!

Lista TOP 10

Niewiele zmieniło się na górze listy w TOP 10 najlepszych firm. Znane marki – ASSA ABLOY, Bosch Security Systems, Axis Communications, FLIR Systems, Allegion, Hanwha Techwin i Tiandy Technologies utrzymały swoje pozycje w pierwszej dziesiątce. Avigilon awansował z zeszłorocznej 12. pozycji na miejsce 10., tym samym zamykając listę TOP 10 w tym roku.
W ubiegłorocznym rankingu według wzrostu przychodów chińskie firmy zajęły pierwszych pięć miejsc. W tym roku są rozproszone w pierwszej piętnastce. Raysharp, Dahua, Tiandy, Kedacom i Hikvision zajęły miejsca – odpowiednio: 1., 3., 4., 6. i 8., a zeszłoroczny zwycięzca w tej kategorii, Wanjiaan Interconnected Technology, wypadł z pierwszej piętnastki.
Czołówka rankingu nadal jest zdominowana przez firmy azjatyckie. Oprócz pięciu wymienionych firm w tej grupie są również: CP Plus, ITX Security, KOCOM, INCOM i VIVOTEK.
Wśród firm spoza Azji rosyjski DSSL – nowy uczestnik rankingu TOP 50 – znalazł się na drugim miejscu zestawienia, odnotowując wzrost przychodów o 48,2 proc. Z kolei Milestone Systems i Axis Communications zajmują w tej kategorii pozycje odpowiednio: 10. i 12.

Hikvision i Axis zajęły dwa pierwsze miejsca pod względem zysku brutto, osiągając w 2017 r. odpowiednio: 1,4 mld oraz 501 mln USD. Firmami o najwyższych marżach zysku brutto są: VIVOTEK, Fermax, IndigoVision, Axis i Avigilon. Z kolei pięć firm o najwyższym zysku netto to: Hikvision, Dahua, Axis, Fermax i Nedap.

Co ciekawe, w TOP 50 Security Security są firmy, które mimo spadku przychodów w 2017 r. okazały się zyskowne. Świadczy to o tym, że ich strategia obniżania kosztów była skuteczna. Należą do nich: Fermax, Hanwha Techwin i IDIS – ich przychody w 2017 r. zmalały odpowiednio o: 3,1%, 9% i 12,2% w porównaniu z 2016 r. Z kolei w kategorii zysku brutto osiągnęły odpowiednio: 34,7 mln, 215 mln i 24,2 mln USD, co dało im w rankingu miejsca 9., 4. i 15.

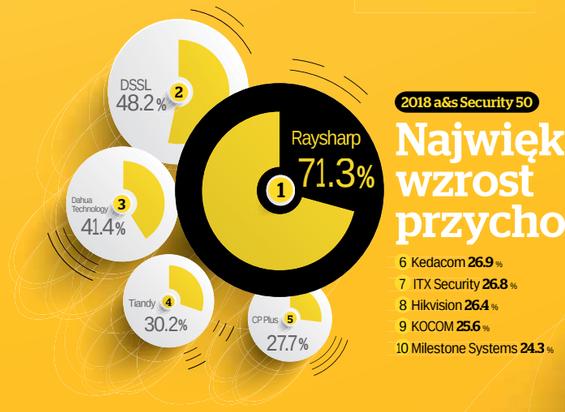
Kontynuacja wzrostu w 2018 r.

Analizując przychody największych producentów, widać wyraźnie, że rynek security się rozwija. Rok 2017 przyniósł wzrost przychodów, a większość dostawców spodziewa się go również w 2018 r. Cały rynek security ma perspektywy rozwoju w 2018 r. Oczekuje się znaczącego zwiększenia sprzedaży, przy globalnej stopie wzrostu przekraczającej 8 proc., liczonej rok do roku. Wzrost napięcia międzynarodowego, coraz większe zagrożenie terroryzmem, zwiększenie liczby ludności na świecie oraz rosnące dochody to czynniki, które powinny sprzyjać rozwojowi.

– Incydenty związane z poważnymi naruszeniami bezpieczeństwa czy ataki terrorystyczne, a także nowe wymogi regulacyjne systematycznie zwiększają zainteresowanie rozwiązaniami zaawansowanymi. A to tylko niektóre z czynników przyczyniających się do rozwoju branży zabezpieczeń. W firmie FLIR obserwujemy zwiększone zapotrzebowanie na nasze rozwiązania. Przychody firmy również z roku na rok są większe – podkreśla John Distelzweig.

– W roku 2018 obserwujemy dobrą koniunkturę zarówno w przypadku zaawansowanych, dużych instalacji, jak i w odniesieniu do mniejszych i średnich. Przekłada się to na pokaźny wzrost i dobre perspektywy dla całego rynku – mówi Kenneth Hune Petersen z Milestone Systems. *– Spodziewamy się dwucyfrowego wzrostu i w tym, i w przyszłym roku. Rynek rozwija się w dobrym kierunku.*

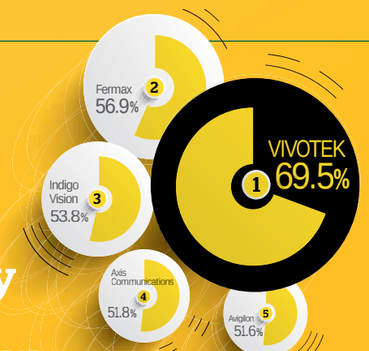
– W skali globalnej rynek zabezpieczeń kontynuuje rozwój dzięki zwiększonemu zapotrzebowaniu na systemy zabezpieczeń w sektorze zarówno publicznym, jak i prywatnym. Popyt na



2018 a&s Security 50

Największy wzrost przychodów

6 Kedacom **26.9** %
7 ITX Security **26.8** %
8 Hikvision **26.4** %
9 KOCOM **25.6** %
10 Milestone Systems **24.3** %



2018 a&s Security 50

Największa marża

6 AV TECH **50.8** %
7 ACTi **47.1** %
8 Suprema **46.3** %
9 Hanwha Techwin **43.6** %
10 DSSL **40.7** %

2018 a&s Security 50

Największy zysk netto

6 Optex (Security Sensors) **29.02**
7 Avigilon **28.26**
8 Infinova **18.07**
9 Milestone Systems **17.05**
10 Aiphone **13.14**

Zestawienie wyników za 2017 r.
przychody, marża, zysk netto

Thomas Schulz
ASSA ABLOY

Fu Liquan
Dahua Technology

produkty zapewniające elastyczność, możliwość adaptacji i współpracy jest motorem napędowym naszej działalności – mówi Pierre Racz z Genetec.

Wzrosty są spodziewane we wszystkich głównych regionach geograficznych, w Ameryce Północnej, EMEA (Europa, Bliski Wschód i Afryka) i APAC (Azja i Pacyfik). – *W Ameryce Północnej przychody przekroczyły prognozowany wzrost na 2018 r. Region ten pozostaje prężnym rynkiem przyjmującym ujednolicone rozwiązania, rozwijającym się po części w wyniku uświadamiania cyberzagrożeń wśród społeczeństw* – twierdzi Pierre Racz. – *Popyt na rynkach wschodzących, takich jak Indie, wręcz eksplodował. Imponujący wzrost w regionie APAC wynika przede wszystkim z realizacji inicjatyw bezpiecznego miasta.*

Rok 2017 Axis Communications ocenia jako dobry. Region EMEA i Ameryka Północna to nasze najlepsze rynki. W pierwszej połowie 2018 r. w regionie EMEA osiągnęliśmy wzrost przychodów o 12 proc. Na nasz rozwój w największym stopniu wpływa powiększanie się rynku i umiejętne czerpanie korzyści z wysokiego tempa wprowadzania rozwiązań innowacyjnych oraz rozwijania naszych produktów – mówi Ray Mauritsson, prezes i dyrektor generalny Axis Communications.

Dobre wyniki ma osiągnąć zwłaszcza region EMEA. Rządy państw europejskich podjęły istotne działania mające na celu zapewnienie bezpieczeństwa w miejscach publicznych. Dotyczą one wdrażania zaawansowanych systemów dozoru wizyjnego i przekazywanie organom ścigania zarejestrowanego materiału lepszej jakości. Dobre wskaźniki wzrostu można również przypisać zwiększonemu popytowi na systemy zabezpieczeń, związanemu ze wzrostem przestępczości. W Europie i na Bliskim Wschodzie coraz więcej kamer telewizji dozorowej jest instalowanych na lotniskach i w miejscach publicznych.

Na Starym Kontynencie zainteresowanie rozwiązaniami zapewniającymi bezpieczeństwo stale rośnie, widoczne są jednak różnice między rynkami rozwiniętymi a rozwijającymi się. Na Bliskim Wschodzie i w Afryce lokomotywą wzrostu są rozwój infrastruktury inteligentnych miast, budownictwo mieszkaniowe i lotniska, co jest zjawiskiem pozytywnym – mówi Paulo Byun, prezes COMMAX.

Rok 2018 kończy się bardzo dobrze dla regionu Europy i Bliskiego Wschodu. Pomimo powolnego startu wynikającego z niepewności na scenie politycznej i wprowadzenia przepisów GDPR, począwszy od drugiego kwartału odnotowaliśmy duży popyt w sektorze zarówno publicznym, jak i prywatnym. Afryka i rynki Bliskiego Wschodu są uzależnione od cen ropy naftowej, co przekłada się na duże inwestycje w przemyśle naftowym i gazowym. Na sytuację w Europie wpływa ponowne ożywienie w gospodarce i obawa przed terroryzmem – uważa Dror Sharon z Magal Security Systems.

Popyt w większości branż

W 2017 r. większość branż inwestowała w bezpieczeństwo, użytkownicy końcowi zaś przeznaczali większe kwoty na zastosowania związane z ochroną osób i mienia oraz niezwiązane z zabezpieczeniami. – *W bezpieczeństwo w 2017 r. zainwestowali przede wszystkim dostawcy mediów użytkowych, przemysł, handel, sektor farmaceutyczny i edukacja. Popyt wynika w dużej mierze z poprawy sytuacji gospodarczej, wzrostu zagrożenia i wdrożenia nowych lub podwyższonych standardów bezpieczeństwa* – mówi Dror Sharon.

Infrastruktura krytyczna, w szczególności stacje elektroenergetyczne, rurociągi i mosty, była jednym z tych segmentów, w których zaobserwowano stały popyt.

Wzrosły również wydatki na zabezpieczenie lotnisk i portów. Obserwujemy też zwiększone zapotrzebowanie ze strony właścicieli stadionów i operatorów dużych obiektów publicznych. Większą uwagę skupiają na ochronie obwodowej, na co wpływ mają doniesienia o wtargnięciach na teren obiektu, napaściach z użyciem broni i aktach terroryzmu. Obiekty IK priorytetowo traktują inwestycje w najnowocześniejsze systemy zabezpieczeń – wyjaśnia John Distelzweig z FLIR Systems.

Również sektor handlu detalicznego, który pod presją handlu online usprawnił obsługę klienta i podniósł poziom jego zadowolenia, jest liczącym się odbiorcą produktów security. Handel detaliczny w dużej mierze przyczynił się do wzrostu przychodów dostawców, ponieważ coraz więcej sprzedawców korzysta z rozwiązań analityki biznesowej, poprawiającej wydajność i efektywność.

Obserwujemy zwiększony popyt w handlu detalicznym – sektorze, który szuka funkcjonalności wykraczających poza security. Standardowe systemy zabezpieczeń nie są tanie, ale jeśli uzupełnimy je o dodatkowe funkcje, możemy liczyć na większy zwrot z inwestycji. Przykładowo, dzięki mapom natężenia ruchu klientów sklep może zwiększyć sprzedaż, odpowiednio eksponując swoje towary – podkreśla Kenneth Hune Petersen z Milestone Systems.

Współczesny rynek charakteryzuje się tym, że inwestorzy coraz częściej poszukują nie produktów, lecz rozwiązań mogących sprostać wyzwaniom i zapewniających im rzeczywiste korzyści biznesowe. Biorąc jako przykład system dozoru wizyjnego w sieciach handlowych, nie wystarczy już, że kamery jedynie monitorują otoczenie. System dozorowy powinien również podnieść efektywność pracy i ograniczyć potencjalne ryzyka – twierdzi Fu Liquan z Dahua Technology.

W handlu możemy analizować zachowanie klientów i pracowników. Systemy wizyjne są w stanie kontrolować nie tylko przepływ ludzi, ale i gotówki oraz wszystko, co się dzieje w sklepie – mówi Thomas Lausten, prezes Mobotix.

Z pozytywnym nastawieniem na kolejny rok

Większość dostawców, zakładając kontynuację obecnego trendu wzrostu na całym świecie, z optymizmem patrzy na to, co przyniesie 2019 r. Światowy rynek security będzie się nadal rozwijał, a firmy skupią swoje działania na tworzeniu rozwiązań, które będą lepiej integrować systemy zabezpieczeń w wybranych przez klientów środowiskach pracy i życia.

– *Nasza prognoza na 2019 r. zakłada ostrożny optymizm i kontynuację pozytywnego trendu z roku 2018. Spodziewamy się rozwoju branży security na całym świecie, być może największego w krajach regionu APAC i Ameryce Północnej* – zapowiada Dror Sharon. *Oczywiście jest jeszcze na to za wcześnie, ale w 2019 r. przewidujemy wyniki lepsze od tegorocznych. Wzrost będzie się wiązał z większą aktywnością w przemyśle i handlu, wspartą kilkoma prowadzonymi megaprojektami z sektora naftowo-gazowego oraz ochroną obwodową.*

Spodziewamy się, że światowy rynek security będzie nadal rósł, a popyt na produkty konwergentne, które można powiązać z Internetem Rzeczy, a nie z pojedynczymi urządzeniami, się zwiększy – zauważa Paulo Byun. – *Przewiduje się, że wschodzące gospodarki wraz z rozwojem rynku pokonają konkurencję. Ważnym rynkiem jest Ameryka Północna.*

Spośród sektorów gospodarki wymienia się miejskie systemy monitoring wizyjnego oraz smart city jako segmenty o większym potencjale. Operatorzy miejscy bowiem sięgają po rozwiązania z obszaru sztucznej inteligencji i Internetu Rzeczy, by rozwiązać problemy, z którymi borykają się włodarze miast.

W obszarze bezpiecznego miasta można zrobić dużo więcej dzięki nowym technologiom, a także IoT i big data oraz wpomóc miasta, by stały się bardziej inteligentne – uważa Ray Mauritsson. *Jesteśmy zaangażowani w innowacje i postęp technologiczny, więc koncentrujemy się na rozwijaniu nowej generacji sztucznej inteligencji i rozwiązań zabezpieczeń technicznych przeznaczonych dla smart city i inteligentnych systemów ruchu* – deklaruje Fu Liquan z Dahua Technology.

Paulo Byun
COMMAX

Ray Mauritsson
Axis Communications

Keen Yao
Hikvision

Thomas Lausten
Mobotix

Trendy technologiczne na rok 2019

U progu 2019 r. wiele osób zastanawia się, które technologie w branży security będą zyskiwały na popularności. Przedstawiciele firm notowanych w zestawieniu TOP 50 Security podali swoje typy.

Cyberbezpieczeństwo

Gorącym tematem w 2019 r. nadal będzie cyberbezpieczeństwo. Przez amerykańską organizację SIA (*Security Industry Association*) zostało ono uznane za numer jeden w rankingu 10 megatrendów, które mają kształtować branżę security w przyszłym roku. W obliczu cyberzagrożeń skierowanych przeciwko urządzeniom security, coraz częściej działającym w sieci, ich dostawcy muszą zapewnić, że rozwiązania są odporne na ataki. – *W 2019 r. cyberbezpieczeństwo będzie nadal głównym ważnym tematem, a stopień odporności na ataki stanie się kluczowym aspektem rozwoju produktów* – uważa John Distelzweig z FLIR Systems.

AI/Analityka

Sztuczna inteligencja i zaawansowana analityka również zdominują obszar security. – *Sztuczna inteligencja, uczenie maszynowe oraz głębokie uczenie nadal będą wyznaczały kierunek rozwoju technologicznego, który przyniesie radykalną poprawę wydajności i zwiększy możliwości systemów zabezpieczeń* – przewiduje Dror Sharon z Magal Security Systems. – *W niektórych produktach zaimplementowaliśmy wyrafinowane procesy klasyfikacji, zwiększając ich wydajność i dostarczając użytkownikom dodatkowe informacje.*

Ochrona prywatności użytkowników i danych

Rozwój technologii sztucznej inteligencji wywołuje poważny problem związany z wykorzystywaniem i ochroną danych osobowych. – *W branży sporo dyskutuje się na temat sztucznej inteligencji i głębokiego uczenia. Przewidujemy, że presja na ochronę prywatności będzie coraz większa. Rozwiązanie tego problemu i wykorzystywania danych osobowych będą jednym z najważniejszych aspektów rozwoju biznesu* – uważa Ray Mauritsson z Axis Communications.

Edge Computing

Z technologiami sztucznej inteligencji i uczenia maszynowego ściśle wiąże się zarówno przetwarzanie danych w urządzeniach brzegowych sieci o coraz większej mocy obliczeniowej mogącej już obsłużyć złożone algorytmy, jak i przetwarzanie w chmurze w celu wykorzystania wszystkich gromadzonych danych. – *Edge Computing będzie rozwijany dzięki „inteligentniejszym" urządzeniom brzegowym. W całej branży będzie też większa akceptacja dla rozwiązań chmurowych, m.in. bardziej inteligentnego przetwarzania w chmurze do głębszej analizy zdarzeń* – zapowiada J. Distelzweig z FLIR Systems.

Uwierzytelnianie mobilne

W obszarze kontroli dostępu akceptację rynku będą zyskiwały systemy bezprzewodowe oraz poświadczenia mobilne. – *Uwierzytelnianie przy użyciu smartfonu zamiast plastikowej karty wydaje się atrakcyjniejsze. Przykładowo, nasze rozwiązanie SMARTair Openow zostało wdrożone w jednym z największych amerykańskich kampusów uniwersyteckich oraz w przestrzeniach współdzielonych w Hiszpanii. W Finlandii Abloy wprowadził bezprzewodowe zamki Pulse z własnym zasilaniem energią kinetyczną obrotu klucza. Oba rozwiązania są przełomowe, więc usłyszymy o nich więcej w 2019 r. i w kolejnych latach* – twierdzi Thomas Schulz, dyrektor ds. marketingu i komunikacji w Digital and Access Solutions w ASSA ABLOY.

Wciąż jest potencjał

W perspektywie krótkoterminowej obecna dynamika rozwoju globalnego rynku security nie powinna zwolnić. Coraz więcej użytkowników stosuje rozwiązania security w swojej działalności zarówno związanej z ochroną osób i mienia, jak i z nią niezwiązanej. Umacnia się wykorzystanie zaawansowanej analityki i sztucznej inteligencji, które zapewniają użytkownikom większą proaktywność i skuteczność. Wszystko to, w połączeniu z dobrymi wynikami ekonomicznymi w różnych regionach świata, powinno mieć w nadchodzących latach pozytywny wpływ na branżę zabezpieczeń technicznych.

W najbliższych latach branża security zwiększy przychody na wszystkich głównych rynkach: w Ameryce Północnej oraz regionach EMEA (kraje Europy, Bliskiego Wschodu i Afryki) i APAC (Azji i Pacyfiku). **Wiodący integratorzy systemów z całego świata opowiedzieli nam o swoich przewidywaniach co do najbardziej rozwijających się sektorów rynku.**

Integratorzy systemów wskazują sektory o największym wzroście

AMERYKA PÓŁNOCNA:

Największe środki na rozwiązania security przeznaczają sektory administracji publicznej i infrastruktury krytycznej

W Ameryce Płn. administracja rządowa i wojsko są wymieniane jako ten sektor, który w ostatnim roku dużo inwestował w zabezpieczenia osób i mienia. – *Instytucje rządowe przeznaczają fundusze przekazane przez administrację na poprawę bezpieczeństwa i minimalizowanie potencjalnych zagrożeń, np. takich jak drony* – mówi Sean Ahrens, Security Market Group Leaders, Affiliated Engineers.

Ze względu na powszechnie stosowane w tym sektorze systemy ochrony obwodowej, klienci poszukują rozwiązań zaawansowanych. – *Segment wojskowy jest szczególnie zainteresowany kamerami o dużym zasięgu, termowizyjnymi i wizyjnymi z oświetlaczami laserowymi* – podkreśla Dennis Gallen, wiceprezes Kintronics.

Kolejnym sektorem, który spore kwoty przeznaczył na rozwiązania security, jest infrastruktura krytyczna, w szczególności centra przetwarzania danych oraz dostawcy mediów publicznych. – *Naruszenie bezpieczeństwa obiektów infrastruktury użyteczności publicznej może mieć zasięg zarówno regionalny, jak i lokalny. Mogłoby spowodować zakłócenia w dostawie wody, gazu i elektryczności dla dużej liczby osób* – twierdzi S. Ahrens.

Coraz więcej firm zostaje poszkodowanych w wyniku kradzieży własności intelektualnej – tajemnicy handlowej lub dokumentacji związanej z badaniami i rozwojem, których przejęcie może nawet zniszczyć konkurencję. W wyniku kradzieży własności intelektualnej najbardziej ucierpiały firmy biotechnologiczne, opracowujące leki nowej generacji. – *W ostatnim czasie zanotowano kilka przypadków kradzieży własności intelektualnej, które miały duży wpływ na organizacje. Dotyczyły one utraty tajnych informacji handlowych lub innej poufnej dokumentacji. Klienci powoli zdają sobie sprawę z tego ukrytego zagrożenia i zaczynają inwestować w zabezpieczenia ograniczające dostęp do tego rodzaju informacji* – mówi S. Ahrens.

W obliczu wielu wyzwań odbiorcy końcowi sięgają po nowe technologie, które pozwalają rozwiązać ich problemy i zaspokoić potrzeby.

- A Administracja publiczna
- B Infrastruktura krytyczna
- C Biotechnologia

Administracja publiczna i ochrona zdrowia wykazują zainteresowanie większą integracją systemów, zapewniającą większą funkcjonalność, coraz bardziej inteligentnych. Rośnie zainteresowanie rozwiązaniami analitycznymi z algorytmami „jeśli, to", wykrywaniem przypadków użycia broni, kontrolą dostępu na podstawie cech biometrycznych, rozpoznawaniem twarzy oraz odczytem tablic rejestracyjnych (LPR) – podkreśla D. Gallen. – *Kontrola dostępu oparta na cechach biometrycznych lub technologii Bluetooth jest stosowana w połączeniu z algorytmami LPR, rozpoznawania twarzy i wykrywania broni m.in. w celu podjęcia konkretnych reakcji w odpowiedzi na określone zdarzenia. Przykładowo, wykryty wystrzał z pistoletu może inicjować automatyczną blokadę, z odtworzeniem wcześniej nagranego komunikatu zawierającego instrukcje.*

W prewencji włamań lub nieautoryzowanego dostępu zyskały na popularności również systemy zarządzania gośćmi. *Systemy zarządzania gośćmi obsługują informacje zwrotne, np. gdy odwiedzający obiekt próbuje ominąć system, korzystamy z funkcji anti-tailgate. Możemy wtedy przez telefon wysłać komunikat o próbie wtargnięcia* – wyjaśnia S. Ahrens. – *Możemy przeprowadzać zdalne uwierzytelnianie, śledzić gości kiedy wchodzą i wychodzą. Korzystając z takich rozwiązań, jak beacony Bluetooth, wiemy, dokąd kierują*

Sean Ahrens
Affiliated Engineers, USA

> *Naruszenie bezpieczeństwa infrastruktury użyteczności publicznej może mieć zasięg zarówno regionalny, jak i lokalny. Mogłoby spowodować zakłócenia w dostawie wody, gazu i elektryczności dla dużej liczby osób*

Dennis Gallen
Kintronics, USA

> *Nie sprzedajemy produktów masowych, a raczej złożone rozwiązania. Dzięki przejściu do bardziej skomplikowanych aplikacji, z zaawansowaną funkcjonalnością, obsługujemy projekty korporacyjne i ogólnie rzecz biorąc większe.*

się poszczególne osoby, mamy pewność, że nie docierają do obszarów o ograniczonym dostępie. Zainteresowanie systemami zarządzania gośćmi z roku na rok będzie się zwiększać.

Perspektywy wzrostu

Ameryka Północna pozostaje rynkiem o dużym wzroście, szczególnie ze względu na dobre wyniki ekonomiczne Stanów Zjednoczonych. Według prognoz Banku Światowego USA powinny w tym i następnym roku odnotować wzrost odpowiednio o 2,3 i 2,7 proc. *Pod rządami obecnej administracji obserwujemy wzrost PKB, co skutkuje m.in. spadkiem stopy bezrobocia i wpływa pozytywnie na rozwój gospodarki. Organizacje uzyskują większe przychody, a tym samym mają większe budżety na zaspokajanie swoich potrzeb, także w zakresie bezpieczeństwa* – twierdzi S. Ahrens.

Kintronics odnotował wzrost o 20–25 proc. w okresie od 2017 do 2018 r. – szacuje D. Gallen, dodając, że ma to związek głównie ze skoncentrowaniem się firmy na technologiach zaawansowanych. – *Nie sprzedajemy produktów masowych, a raczej złożone rozwiązania. Dzięki przejściu do bardziej skomplikowanych aplikacji, z zaawansowaną funkcjonalnością, obsługujemy projekty korporacyjne i ogólnie rzecz biorąc większe.*

Wzrostu sprzedaży można oczekiwać również w przyszłym roku, przy założeniu że obserwowany obecnie na rynku amerykańskim wzrost gospodarczy w najbliższym czasie nie wyhamuje. – *Spodziewam się wzrostu tak długo, jak długo będzie rządzić administracja o podobnych poglądach na ekonomię* – uważa S. Ahrens. Pytany o trendy technologiczne na rynku amerykańskim w nadchodzących latach, Sean Ahrens wymienia robotykę. Będzie ona bardziej inteligentna i stanie się realną alternatywą dla ludzi. – *Dałoby to ogromny zwrot z inwestycji. Pracownicy ochrony generują duże koszty. Zwykle są to pracownicy firm zewnętrznych, nie można więc mówić o lojalności. Możemy ograniczyć konieczność zatrudniania personelu patrolującego wnętrza budynku tylko do obszarów krytycznych. Robotyka byłaby powiązana z systemem, którym zarządzałby pracownik, natomiast wstępną obserwację zapewniałby robot* – twierdzi.

EUROPA I BLISKI WSCHÓD:

Na znaczeniu zyskują aplikacje niezwiązane z zabezpieczeniami

Rozwiązania oferowane przez branżę security to rosnący rynek również w Europie i na Bliskim Wschodzie. Najwięcej inwestującymi sektorami gospodarki są admi nistracja publiczna, handel detaliczny i bankowość. Jednak coraz więcej odbiorców końcowych korzysta także z rozwiązań security, ale w zastosowaniach niezwiązanych *stricte* z zabezpieczeniami.

W związku z wejściem w życie ogólnego rozporządzenia o ochronie danych osobowych (RODO/GDPR) klienci końcowi w Unii Europejskiej większą uwagę zwracają na zapewnienie poufności danych.

Bliski Wschód

Również na Bliskim Wschodzie sektor rządowy stanowi główne źródło dochodu dla branży security ze względu na wymogi zabezpieczenia biur i agencji przed różnego rodzaju zagrożeniami. – *Użytkownicy z tego sektora kupują zabezpieczenia, aby chronić dostęp do obiektów, kontrolować przyznawanie dostępu konkretnemu użytkownikowi w określonym czasie oraz monitorować związane z tym zdarzenia* – wyjaśnia Ahmed Matari, szef działu operacji i utrzymania w firmie Ideal Information z Kuwejtu.

Działamy w Libanie, gdzie znajduje się centrala, w Iraku i Nigerii. Rządowe zapotrzebowanie na produkty security w tych krajach jest związane przede wszystkim z zagrożeniem terroryzmem. W związku z tym dostarczamy rozwiązań spełniające najwyższe standardy i o wysokiej niezawodności, skuteczne w likwidowaniu wszelkich zagrożeń – mówi Ziad Monla, dyrektor generalny firmy Guardia Systems, która realizowała projekt monitoringu miejskiego w Bejrucie. – *Wdrożyliśmy pod klucz system monitoringu miejskiego w rekordowym czasie jednego roku. Obejmował on 2 tys. kamer zainstalowanych w 350 lokalizacjach, 200 kamer rozpoznających tablice rejestracyjne, całą infrastrukturę światłowodową, dwa centra danych, w tym jedno modułowe i mobilne, a także dwie stacje monitorujące dla 50 operatorów, wyposażone w najnowsze technologie.*

Ważnym rynkiem dla branży security jest też handel detaliczny. – *Detaliści potrzebują zabezpieczeń, które wyzwalając alarmy w momencie zaistenienia zagrożenia, umożliwiają zapobieganie stratom i przestępstwom* – podkreśla A. Matari. – *Dostarczamy sieciowe systemy dozoru wizyjnego, systemy kontroli dostępu i antywłamaniowe, które pozwalają ograniczyć wspomniane problemy.*

Ważnym sektorem jest również bankowość, w której inwestorzy coraz częściej poszukują zintegrowanych rozwiązań centrum dowodzenia. – *Banki muszą w centralnej lokalizacji monitorować wszystkie swoje rozproszone oddziały. Muszą mieć możliwość podglądu obrazu z kamer na żywo i zarejestrowanego, sterowania dostępem fizycznym, a także monitorowania sygnałów alarmowych i pożarowych z jednego miejsca*– wyjaśnia Ziad Monla, którego firma realizuje projekt z Al Rafidain Bank w Iraku. – *Wdrażamy obecnie rozwiązanie Oracle Core Banking, które umożliwi bankowi wejście w nową erę bankowości cyfrowej.*

Zdaniem integratorów systemów na rynkach Bliskiego Wschodu można oczekiwać dalszego wzrostu sprzedaży ze względu na bieżące potrzeby klientów w zakresie security. – *W 2018 r. spodziewamy się takich samych przychodów jak w 2017 r., natomiast wzrost nastąpi w 2019 r., gdy wprowadzimy nowe usługi i rozwiązania* – przewiduje Z. Monla.

Europa

W Europie – po takich incydentach, jak atak zamachowca, który ciężarówką taranował ludzi w Nicei w 2016 r., czy atak na moście London Bridge z 2017 r.

Ziad Monla
Guardia Systems, Liban

Klienci muszą w centralnej lokalizacji monitorować wszystkie swoje rozproszone oddziały. Muszą mieć możliwość podglądu obrazu z kamer na żywo i zarejestrowanego, sterowania kontrolą dostępu, a także monitorowania sygnałów alarmowych i pożarowych z jednego miejsca.

Kevin Bowyer
NW Security Group, Wlk. Brytania

Popyt wzrasta w reakcji na incydenty i tragiczne wydarzenia. Gdy coś się wydarzy, rozwiązaniem są systemy CCTV. To nie zawsze jest dobry moment na zakup produktów security lub usług ochrony, ale od tego rozmowę zaczynają nasi klienci.

– bezpieczeństwo pozostaje najwyższym priorytetem. W rezultacie jest duże zapotrzebowanie na rozwiązania z zakresu security. – *Popyt wzrasta w reakcji na zdarzenie. Gdy coś się wydarzy, rozwiązaniem są systemy CCTV. To nie zawsze jest dobry moment na zakup CCTV lub usług ochrony, ale od tego zaczynają rozmowę organizacje kontaktujące się z nami* – mówi Kevin Bowyer, dyrektor techniczny brytyjskiej firmy NW Security Group. – *Coraz więcej użytkowników końcowych korzysta z rozwiązań security w aplikacjach niezwiązanych z ochroną – np. aby ulepszyć analitykę biznesową, poprawić wydajność czy zwiększyć zadowolenie klientów.*

Jako przykłady wymienia następujące branże: logistykę i transport, rekreację i turystykę oraz przemysł. *Zazwyczaj nasza praca w tych sektorach polega na zmianie bieżących operacji i ekspansji w ramach organizacji, z którymi współpracujemy. Inwestycja w wysokiej klasy system nie tylko szybko się zwraca, ale także tworzy ścieżkę do poprawy skuteczności i wydajności, którą nasi klienci chętnie akceptują i wdrażają* – wyjaśnia. – *Dostarczamy rozwiązania, które znacząco wpływają na ich bezpieczeństwo, a także prowadzoną działalność.*

W sytuacji, gdy produkty security stają się coraz bardziej masowe, zastosowanie rozwiązań pozwalających użytkownikowi rozwijać analitykę biznesową będą kluczowym czynnikiem wzrostu. – *W 2019 roku oczekujemy wzrostu wynikającego z postępu technologicznego. Dzięki niemu w coraz większym stopniu klienci odnoszą realne korzyści zarówno w obszarze security, jak i analityki biznesowej. Pod względem komercyjnym ceny tych technologii stają się coraz bardziej przystępne* – uważa K. Bowyer.

W Europie obowiązują już regulacje RODO/GDPR, które zmuszają do bardziej rygorystycznej ochrony danych osobowych. Będą one miały wpływ na sposób wdrażania rozwiązań security przez użytkowników końcowych. Ważna jest dobra współpraca integratorów z klientami, by ich systemy były zgodne z nowymi przepisami. – *W efekcie wprowadzenie GDPR w maju tego roku przyczyni się do stosowania wyższych standardów w branży, co zdecydowanie popieramy* – mówi K. Bowyer. – *Nasza firma zapewnia zgodność z GDPR całego systemu dostarczanego w perspektywie długoterminowej.*

Ahmad Al Matari
Ideal Information, Kuwejt

Użytkownicy kupują zabezpieczenia, aby chronić dostęp do obiektów, kontrolować przyznawanie dostępu konkretnym użytkownikom w określonym czasie oraz monitorować związane z tym zdarzenia.

AZJA:

Przepisy prawne i rozwój turystyki stymulują rynek security

Region Azji i Pacyfiku jest rynkiem rosnącym. Według prognoz Banku Światowego gospodarki tego regionu mogą osiągnąć w tym roku wzrost PKB na poziomie 4,1–6,9 proc. Tym samym użytkownicy końcowi będą mieli więcej pieniędzy na wydatki związane z ochroną, zgodnie z ich potrzebami wynikającymi ze stanu zagrożeń w regionie.

W porównaniu z 2017 r. w tym roku wzrost będzie wyższy, ponieważ rośnie popyt. Mam nadzieję, że również w roku 2019 sprzedaż będzie się zwiększać, zapewnienie bezpieczeństwa bowiem stało się elementem niezbędnym – mówi Vincent San Diego, wiceprezes HYE Enterprises, filipińskiego integratora systemów.

Inwestycje w ochronę są również stymulowane przez regulacje rządowe. Przykładowo, stosowana na Filipinach zasada „bez CCTV nie ma pozwolenia" zmusza do instalowania systemu dozoru wizyjnego jako warunku wstępnego dla wniosku o wydanie zezwolenia na rozpoczęcie działalności lub jej odnowienie. W wielu krajach z regionu Azji i Pacyfiku w nowych budynkach wymagane jest zainstalowanie systemów sygnalizacji pożarowej spełniających określone standardy. *Zapewnienie zgodności z przepisami to zdecydowanie kluczowa potrzeba, skłaniającą użytkowników do inwestowania w security* – twierdzi Sovan Hok, dyrektor techniczny w firmie NKTech, która jest integratorem systemów w Tajlandii.

Branża hotelarsko-gastronomiczna jest uważana przez integratorów w regionie APAC za główny generator przychodów. Co nie dziwi, ze względu na tamtejsze wysiłki na rzecz rozwoju turystyki. Według Światowej Rady Podróży i Turystyki (World Travel and Tourism Council) inwestycje w turystykę w Azji Południowo-Wschodniej wyniosły w 2017 r. 48,8 mld USD, co stanowi 6,4 proc. wszystkich nakładów. Oczekuje się, że do 2028 r. wzrosną do 86,8 mld USD. W efekcie buduje się coraz więcej hoteli i kasyn, a to przekłada się na sprzedaż rozwiązań security.

Według Sovana Hoka hotele i kasyna to podstawowa branża inwestująca w rozwiązania security. – *Potrzeby użytkowników końcowych w tym sektorze obejmują monitorowanie zachowania ludzi, rejestrację materiału dowodowego naruszeń prawa i ochronę. Oferujemy systemy dozoru wizyjnego i kontroli dostępu, automatykę oświetlenia i systemy parkingowe dostosowane do potrzeb klientów* – wylicza.

Kolejnym ważnym sektorem są obiekty komercyjne. Budowlany boom w regionie APAC potęguje sprzedaż. – *Ze względu na szybki rozwój budownictwa z udziałem zagranicznych inwestorów spodziewamy się, że w tym roku przychody będą wyższe niż w 2017 r.* – mówi S. Hok.

Popyt wciąż rośnie

Rozwiązania oferowane przez branżę security są ważnym elementem dla klientów końcowych, i to niezależnie od regionu geograficznego czy sektora gospodarki. Chociaż niektóre organizacje zaczynają korzystać z rozwiązań security ze względu na analitykę biznesową i inne aplikacje niezwiązane z zastosowaniami stricte security, to większość nadal wdraża systemy zabezpieczeń w celu ochrony ludzi i mienia. Mając to na względzie, można spodziewać się rozwoju branży security w nadchodzących latach.

Sovan Hok
NKTech, Tajlandia

Potrzeby użytkowników końcowych w tym sektorze obejmują monitorowanie zachowania ludzi, rejestrację materiału dowodowego naruszeń prawa i ochronę. Oferujemy systemy dozoru wizyjnego i kontroli dostępu, automatykę oświetlenia i systemy parkingowe dostosowane do potrzeb klientów

Vincent San Diego
HYE Enterprises, Filipiny

W porównaniu z 2017 r. w tym roku wzrost będzie wyższy, ponieważ rośnie popyt. Mam nadzieję, że również w roku 2019 sprzedaż będzie się zwiększać, zapewnienie bezpieczeństwa bowiem stało się elementem niezbędnym

Rok 2018 przyniósł wzrost

i stworzył dobre perspektywy na przyszłość

Według raportu Memoori poświęconego branży security całkowita wartość światowej sprzedaży produktów zabezpieczeń technicznych, liczona według cen producentów, wyniosła w tym roku 31,55 mld USD. Oznacza to wzrost o 7,5 proc. w stosunku do 2017 r.

Tegoroczna wartość światowej sprzedaży produktów security jest o prawie 1 punkt proc. większa od średniej rocznej stopy wzrostu (CAGR), wynoszącej 6,87 proc. w ciągu ostatnich czterech lat. W ostatniej dekadzie rynek rósł średnio o 5,92 proc. rocznie, jednak stopy wzrostu różnią się w każdym z trzech jego segmentów. Prognozujemy, że w 2023 r. rynek będzie wart 44,25 mld USD, a w ciągu najbliższych pięciu lat średnia stopa wzrostu wyniesie 7 proc.

W aspekcie rozkładu sprzedaży w 2018 r. produkty systemów telewizji dozorowej osiągnęły wartość 17,7 mld USD, co przekłada się na 55,6 proc. udziału w rynku, kontroli dostępu – odpowiednio: 7,45 mld USD i 23,6 proc., sygnalizacji włamania i napadu – 6,72 mld USD, z 21 proc .udziałem w rynku.

Segment dozoru wizyjnego zanotował najwyższą stopę wzrostu na poziomie 9,9 proc., co oznacza wzrost o 4,4 proc. w stosunku do 2017 r.

Rok 2018 nie był szczególnie dobry dla producentów spoza Chin, głównie z powodu agresywnej rywalizacji cenowej. Tegoroczny wynik oznacza powrót do średniej stopy wzrostu z poprzednich pięciu lat. W kolejnych pięciu latach, do 2023 r., rynek będzie rósł w tempie 13,2 proc. rocznie. Będzie to w znacznej mierze spowodowane szybko rosnącą sprzedażą rozwiązań analityki wideo opartej na technologii sztucznej inteligencji, która w 2023 r. może osiągnąć 2,3 mld USD – pod warunkiem że rozwój technologii będzie się odbywał zgodnie z założeniami. Stopa wzrostu z wyłączeniem analityki wideo wyniesie ok. 8,5 proc. Taki wynik będzie jednak wymagać wzrostu wolumenu sprzedaży, który przełoży się na CAGR o wartości znacznie przekraczającej 10 proc. w sytuacji obniżenia cen komponentów i mniej agresywnej polityki cenowej chińskich producentów.

Wzrost sprzedaży w obszarze kontroli dostępu miał przekraczać nieco 8 proc. – wobec postępującego przenikania technologii do sieci IP, rozwoju biometrii, zarządzania uprawnieniami, systemów zamków bezprzewodowych oraz usług ACaaS. Dla systemów KD miał to być trzeci rok z rzędu o najwyższej stopie wzrostu w trzech segmentach. Jednak presja cenowa spowodowała mniejszy prognozowany wzrost mierzony wartością sprzedaży. Wydaje się też, że producenci niechętnie wspierają otwarte standardy, chroniąc swoje tajemnice technologiczne. W perspektywie długoterminowej może się to odbić na rozwoju, umożliwiając chińskim producentom przejęcie inicjatywy i mocne wejście w biznes, na którym działają od niedawna.

Segment systemów sygnalizacji włamania i napadu już dawno osiągnął dojrzałość. Jednak coraz większe zastosowanie radarów oraz kamer termowizyjnych i wieloprzetwornikowych przyczyniło się do 4,5 proc. wzrostu w 2018 r. Miał na to wpływ także rozwój czujników i technologii bezprzewodowych oraz integracja z systemami dozoru wizyjnego i kontroli dostępu oraz oświetleniem zewnętrznym.

Strategie biznesowe wymagają fundamentalnych zmian

Istnieje wiele czynników, które mają wpływ na branżę security. Pięć wymienionych poniżej będzie wymagać zasadniczych zmian w strategiach biznesowych.

1 Dystans między głównymi dostawcami a setkami mniejszych z roku na rok rośnie, a w związku z tym podnosi się próg ekonomiczny osiągania zysków w tej branży. Wkroczyliśmy w taką fazę, w której firma zajmująca się dozorem wizyjnym wymaga strategii koncentrującej się na wolumenie sprzedaży do rynku SMB lub na silnej marce na rynku *enterprise*. Do roku 2023 nie więcej niż pięciu dostawców będzie się rozwijać, działając jednocześnie w obu segmentach rynku.
W dziedzinie dozoru wizyjnego dwóch chińskich producentów zbudowało swój wolumen sprzedaży, zaczynając od działań na rynku małych i średnich przedsiębiorstw. Ich obecna przewaga nad zachodnimi firmami jest tak duża, że nie wydaje się prawdopodobne, aby można było ten trend odwrócić. A już z całą pewnością nie w wyniku konkurowania wyłącznie ceną. Dwie chińskie firmy przyjęły strategię rewolucji w branży, podcinając marże swoim konkurentom, a jednocześnie poszerzając rynki i zwiększając w nich udziały. Ma to kluczowe znaczenie dla branży w momencie, gdy czynnikiem krytycznym staje się wielkość sprzedaży i następuje upowszechnienie kamer wideo.

Allan McHale
Memoori Research

Dwie chińskie firmy przyjęły strategię rewolucji w branży, podcinając marże swoim konkurentom, poszerzając jednocześnie rynki i zwiększając w nich udziały. Ma to kluczowe znaczenie w momencie, gdy czynnikiem krytycznym staje się wielkość sprzedaży i następuje upowszechnienie kamer dozorowych.

Niektórzy wiodący producenci zachodni, którzy musieli obniżyć marże, w tym roku poprawili swoje wyniki finansowe. Stało się to możliwe dzięki kontynuowaniu inwestycji w dostarczanie produktów o lepszych parametrach i bardziej odpornych na cyberataki. Wzmacnianie marki okazało się ważne w tej grze, ale w obecnej sytuacji nie wystarczy, by zagrozić dominacji dwóch chińskich producentów.

Możliwym działaniem zmierzającym do zwiększania potencjału są fuzje i przejęcia między czołowymi zachodnimi producentami, ale w najlepszym wypadku mogą one spowolnić dalsze poszerzanie się luki. Kolejną opcją zagwarantowania sobie zysków w przyszłości dla silnych marek oferujących kompleksowe rozwiązania jest skoncentrowanie się na wielu sektorach gospodarki i zawieranie mocnych sojuszy z firmami specjalizującymi się w innych usługach z obszaru automatyki budynkowej (BMS).

2 Regionem o największym wzroście i największym udziale w rynku zabezpieczeń technicznych są Chiny i Azja. Charakteryzuje się najniższą penetracją urządzeń systemów zabezpieczeń, mierzoną w sprzedaży na mieszkańca, a mimo to odpowiada za ponad 28 proc. całego rynku światowego i ponad 40 proc. segmentu dozoru wizyjnego. Dlatego powinien on otwierać przed zachodnimi producentami największe możliwości przyszłego wzrostu. Aby znaleźć się w pierwszej dwudziestce światowych dostawców w 2023 r., trzeba będzie wykazać się znaczącym udziałem w tym rynku.

3 Jak na ironię, to branży security, dostarczającej rozwiązania z zakresu ochrony ludzi i mienia w budynkach i miejscach publicznych, przypisuje się najwyższy poziom ryzyka związanego z cyberprzestępczością. To największe zagrożenie dla branży, w szczególności dla systemu dozoru wizyjnego IP, który często okazuje się najsłabszym ogniwem. Ci dostawcy, którzy mogą wykazać się wysokim poziomem zabezpieczeń przed cyberatakami, spełniają obecnie najważniejsze kryteria dotyczące wyboru rozwiązań na rynku enterprise. Ci zaś, którzy sprzedają produkty podatne na zagrożenia, w najlepszym wypadku odnotują spadek udziału w rynku albo – co bardziej możliwe – poniosą poważne straty finansowe, które mogą zrujnować ich działalność. Branża zabezpieczeń technicznych będzie zatem jedną z najwięcej inwestujących w systemy cyberbezpieczeństwa, szczególnie w obszarze inteligentnych budynków.

4 Usługi oparte na oprogramowaniu, we wszystkich swoich postaciach, osiągnęły najwyższe wskaźniki wzrostu wśród wszystkich komponentów w branży zabezpieczeń technicznych. W ciągu ostatnich pięciu lat odnotowały one prawie dwukrotnie większy wzrost sprzedaży w porównaniu ze sprzętem, choć nadal stanowią nie więcej niż 12 proc. rynku. Oprogramowanie będzie jednak szybko zwiększać swój udział, wykazując wyższe stopy wzrostu w następnych latach. Duży w tym udział będzie miało przetwarzanie ogromnych ilości danych generowanych z różnych czujników, zwłaszcza kamer wideo.
Firma badawcza Memoori opublikowała raport o analityce wideo opartej na AI, który dowodzi, że potencjał rynku dla zastosowań tej technologii w istniejących instalacjach może wynosić ok. 65 mld USD i może nie wyczerpać się nawet przez 30 lat. Aby oddać całkowity potencjał rynkowy, do tej sumy zostały dodane koszty implementacji algorytmów analityki wideo opartej na AI w nowych instalacjach.

W 2017 r. światowy rynek produktów dozoru wizyjnego osiągnął wartość 15,87 mld USD, a szacunkowe przychody ze sprzedaży narzędzi analizy wideo opartej na AI wyniosły 115 mln USD. Oznaczałoby to, że nowa technologia stanowiła tylko niewielki odsetek całego rynku dozoru wizyjnego w ubiegłym roku. Do 2022 r. będzie ona odpowiadać za ok 13 proc. sprzedaży, pod warunkiem że wszystkie kanały rynkowe zostaną w pełni rozwinięte, a popyt nie będzie ograniczony słabą wydajnością oprogramowania opartego na AI.

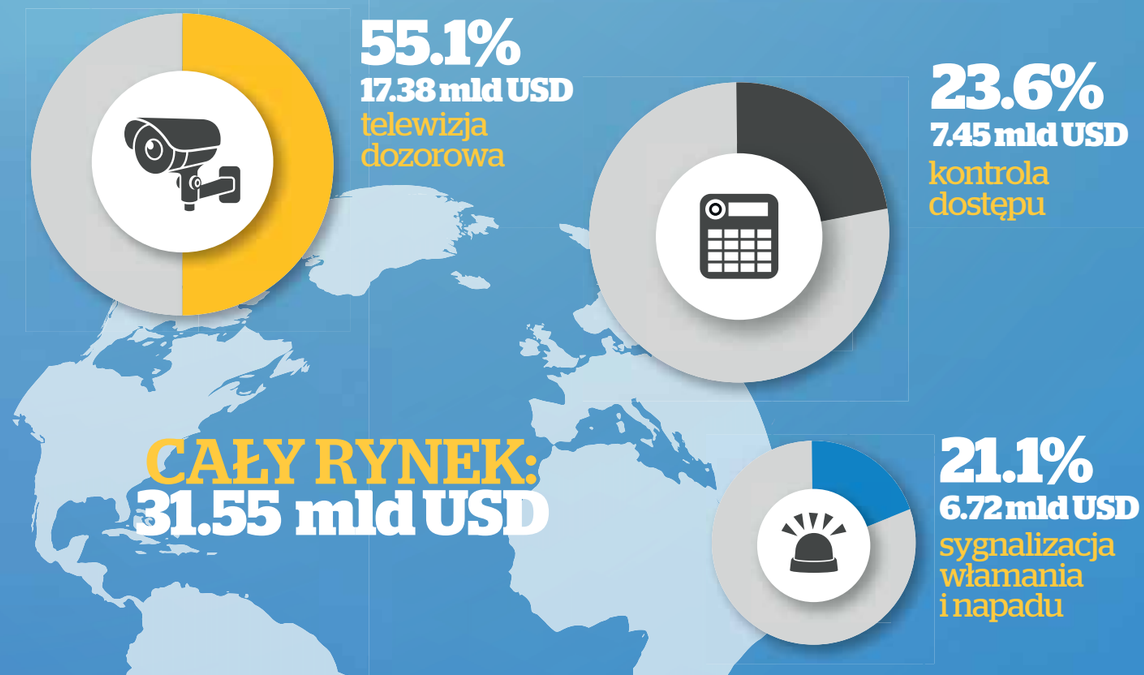
Jak na ironię, to branży security przypisuje się najwyższy poziom ryzyka związanego z cyberprzestępczością. To największe zagrożenie szczególnie dla systemu dozoru wizyjnego IP, który często okazuje się najsłabszym ogniwem.

5 Integracja i konwergencja z IT od prawie dekady mają wpływ na wszystkie trzy segmenty branży security, w szczególności dozór wizyjny. Jednak dopiero w ostatnich latach – dzięki sieciom IP i standardowi ONVIF – integracja we wszystkich segmentach jest w stanie zapewnić bardziej wyrafinowane i efektywne kosztowo rozwiązania. Co więcej, integracja rozwija się obecnie w kierunku tworzenia Internetu Rzeczy (IoT) i budynkowego Internetu Rzeczy (BIoT), łącząc wszystkie usługi automatyki budynkowej w sieć dwukierunkową. Powstałe w ten sposób otwarte, kompleksowe i holistyczne rozwiązania będą działać na autopilocie, nie wymagając do kontroli interwencji ludzi. Obecne zaawansowane zintegrowane systemy zabezpieczeń potrafią zapewnić dostęp do wszystkich istotnych punktów danych. Dzięki temu pracownicy ochrony mogą szybko monitorować i lepiej rozumieć zawiłe i skomplikowane informacje dostarczane przez „inteligentne" rozwiązania budynkowe. Jak już wspomniano, firmy eksperymentują obecnie z wykorzystaniem *big data*, by udoskonalać i przyspieszać procesy.

Wszystkie te działania będą wymagały zawiązywania strategicznych sojuszy pomiędzy firmami specjalizującymi się w różnych usługach BMS, co będzie miało duży wpływ na możliwości zaistnienia na rynku. Nadszedł już czas, by się zaangażować.

Informacje pochodzą z 10. edycji raportu Memoori The Physical Security Business 2018–2023.

Światowa sprzedaż produktów security w roku 2018



Analityka wideo oparta na AI

O krok od przełomu

Analityka wideo *(Video Analytics – VA)* nie odnotowała specjalnych sukcesów w ciągu ostatnich 15 lat, ale z pomocą sztucznej inteligencji (AI) jest teraz na dobrej drodze do dokonania przełomu w branży monitoringu wizyjnego.

Wyzwań przed branżą jest jeszcze wiele. Trzeba przekonać klientów, że nowe rozwiązania są solidne i efektywne kosztowo, gdyż ci inaczej nie będą w nie inwestować. Niestety, część opartych na AI produktów do rozpoznawania twarzy została wprowadzona na rynek jeszcze przed zakończeniem testów beta (na prototypach), nie zrobiły więc dobrego wrażenia na klientach i źle przysłużyły się sprawie. Niemniej jednak, gdy nowe układy scalone i oprogramowanie do inteligentnej analizy obrazu będą pracować na olbrzymiej ilości danych, efektem będzie poprawa bezpieczeństwa i ochrony, większa wydajność pracowników, budynków i przedsiębiorstw. Niewielkie wpadki mogą opóźnić osiąganie celu, jakim jest ożywienie ekosystemu dozoru wizyjnego, ale go nie powstrzymają.

Raport *Memoori The Global Market for AI Video Analytics 2018 to 2023* identyfikuje wiele czynników mogących świadczyć o tym, że od przełomu dzieli nas krok. Po pierwsze ogromny rozwój w układach scalonych, zwłaszcza mikroprocesorów, doprowadził do znacznego zwiększenia ich mocy obliczeniowych. Tym samym umożliwił obsługę algorytmów *deep learning* i *machine learning* oraz wielokrotnie szybsze, niż było to do tej pory możliwe, przetwarzanie i analizowanie danych.

To właśnie rozwiązania analityki wideo „napędzane" przez AI wykorzystującą wspomniane algorytmy są oparte na procesorach GPU. Producenci układów komputerowych odkryli, że procesory graficzne mogą ze znacznie większą wydajnością obsługiwać układy scalone obsługujące technologię AI. Innowacje pochodzą od stosunkowo niedużych producentów układów scalonych, którzy obecnie opracowują specjalizowane struktury półprzewodnikowe (tzw. *chipy*) dla sztucznej inteligencji i produkty oparte na oprogramowaniu analitycznym.

Tego rodzaju dostawców zasilają dzisiaj miliardami dolarów fundusze *venture capital*. Raport wskazuje na 128 firm działających obecnie na całym świecie, które w jakiś sposób biorą udział w dostarczaniu opartych na AI rozwiązań analityki wideo (sprzęt i oprogramowanie).

Jednak rozwój i doskonalenie tej technologii wymaga dużych inwestycji w nowe procesy biznesowe, ludzi i innowacje. Jak wynika z raportu, wydano już miliardy dolarów, pojawia się też nowy kapitał, więc nie ma sygnałów, by ten strumień pieniędzy miał się wkrótce wyczerpać.

Nadal pozostaje wiele do zrobienia w zakresie doskonalenia nowej technologii i dotarcia do rynku. Nowe narzędzia i procesy już otworzyły możliwości wprowadzania produktów wykorzystujących sztuczną inteligencję na rynek oprogramowania VA, potencjalnie rewolucjonizując jego wydajność i możliwości.

W 2018 r. panuje silne przekonanie, że VA daleko wykracza poza to, co można osiągnąć za pomocą konwencjonalnych systemów opartych na standardach. Nowe platformy sztucznej inteligencji, wsparte algorytmami *deep learning* i *machine learning,* są w stanie dostarczać inteligentne rozwiązania dozoru wizyjnego. W rezultacie jeszcze bardziej zwiększy się zapotrzebowanie na opartą na AI analitykę wideo nie tylko w przypadku nowych projektów – ogromny potencjał tkwi bowiem w modernizacji milionów istniejących instalacji dozoru wizyjnego.

Wprowadzanie rozwiązań AI na rynek nie będzie łatwe, ponieważ wymaga czegoś więcej niż tylko drobnych modyfikacji w ustalonych sposobach dystrybucji i instalacji.

Systemy dozoru wizyjnego generują mnóstwo danych, które, niestety, nie są obecnie wykorzystywane. Szacuje się, że działające dzisiaj miliony kamer dostarczają 60 proc. danych wejściowych – więcej niż jakiekolwiek inne czujniki w budynkach, kampusach czy miastach. Istnieje więc ogromny potencjał, aby zmaksymalizować wartość tych danych, przekształcając je w użyteczne informacje. Materiał jest już dostępny i czeka na eksplorację.

Rynek przedsiębiorstw, obejmujący wiele najważniejszych sektorów gospodarki, dokonuje obecnie znaczących inwestycji w oparte na AI rozwiązania analityki wideo. Punkt zwrotny na krzywej wzrostu mógłby zostać osiągnięty w ciągu najbliższych 18 miesięcy, lecz wymagałoby to dużego wysiłku.

Światowy rynek analityki wideo wspieranej przez AI

Rynek VA opartej na AI jest we wczesnej fazie rozwoju. Nie ma wielu jeszcze statystyk mogących dostarczyć wskazówek na temat jego obecnej wielkości. Według naszych szacunków globalna sprzedaż wspieranych przez AI rozwiązań VA, w tym produktów na etapie testów beta, osiągnęła w 2017 r. ok. 115 mln USD. Większość wdrożeń przeprowadzono w Chinach.

Szacujemy też, że obecny rynek konwencjonalnych systemów opartych na standardach osiągnął w 2017 r. ponad dwukrotnie większą wartość – około 250 mln USD. Wraz z pojawieniem się systemów sztucznej inteligencji jego rozmiar zmniejszy się w ciągu następnych trzech lat – w miarę jak oparta na AI analityka wideo będzie przejmować jego udział w biznesie analitycznym. Oceniając wartość sprzedaży oprogramowania VMS w 2017 r. na 1,4 mld USD i przewidując, że do końca 2022 r. osiągnie ona 3,1 mld USD, prognozujemy zrównanie się do tego czasu rynków VA opartej na AI oraz VMS. W następnym okresie analityka wideo z technologią AI stanie się liderem, kontynuując szybki wzrost przez co najmniej dwie kolejne dekady.

Na *rysunku* przedstawiono prognozę popytu na opartą na AI analitykę wideo do 2022 r. Od roku 2017, w którym przychody szacujemy na 115 mln USD, średnia roczna stopa wzrostu w ciągu następnych pięciu lat wyniesie 90 proc., co przełoży się na sprzedaż o wartości 3,1 mld USD w 2022 r. To prognoza ambitna, ale możliwa do zrealizowania. Zakładamy jednak, że oparta na AI analityka wideo będzie odnotowywać stały rozwój, w pełni odpowiadając na zakupowe potrzeby użytkowników końcowych w ciągu najbliższych 18 miesięcy.

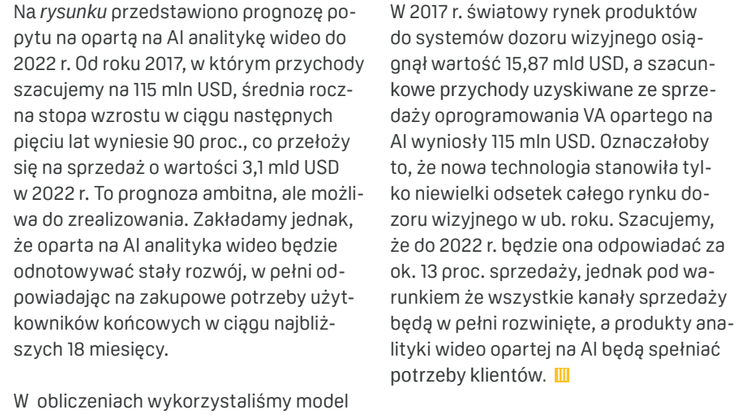
W obliczeniach wykorzystaliśmy model oparty na liczbie 600 mln kamer zainstalowanych w 2017 r. na całym świecie (bez rynku mieszkaniowego). Model uwzględnia przychody ze sprzedaży w przypadku modernizacji istniejącego systemu dozorowego, jak i nowych instalacji.

Szacujemy, że wartość rynku dotycząca zastosowania VA wspieranej przez AI w istniejących instalacjach może wynosić około 65 mld USD. Zakładamy, że jego nasycenie może zająć nawet 30 lat. Aby przedstawić całkowity potencjał rynku, dodaliśmy do tej kwoty koszty wdrożenia analityki wideo z AI w nowych instalacjach.

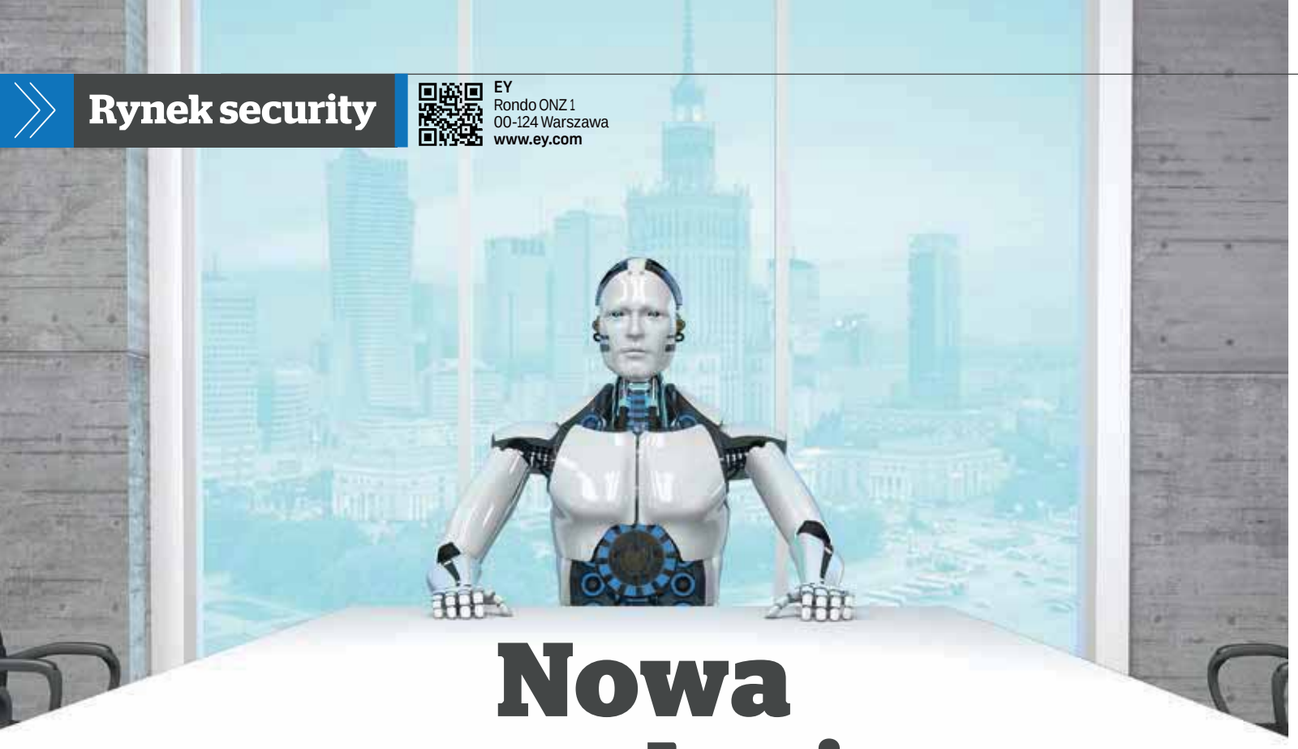
Te liczby są jedynie przybliżonymi szacunkami. Tworzą jednak skalę, na podstawie której można ocenić potencjalną wielkość rynku VA opartej na AI.
W 2017 r. światowy rynek produktów do systemów dozoru wizyjnego osiągnął wartość 15,87 mld USD, a szacunkowe przychody uzyskiwane ze sprzedaży oprogramowania VA opartego na AI wyniosły 115 mln USD. Oznaczałoby to, że nowa technologia stanowiła tylko niewielki odsetek całego rynku dozoru wizyjnego w ub. roku. Szacujemy, że do 2022 r. będzie ona odpowiadać za ok. 13 proc. sprzedaży, jednak pod warunkiem że wszystkie kanały sprzedaży będą w pełni rozwinięte, a produkty analityki wideo opartej na AI będą spełniać potrzeby klientów.

Dane pochodzą z raportu *Memoori The Global Market for Intelligent Video Analytics 2018 to 2023*.

Światowy rynek inteligentnej analityki wideo
prognoza na lata 2017–2022



EY
Rondo ONZ 1
00-124 Warszawa
www.ey.com



Nowa rewolucja technologiczna wielką szansą polskiej gospodarki

Polska systematycznie awansuje w międzynarodowych rankingach odnoszących się do poziomu innowacyjności, ale wciąż plasujemy się daleko za czołówką najbardziej rozwiniętych gospodarek. **Ogłoszona w 2016 r. „Strategia na rzecz odpowiedzialnego rozwoju" (tzw. Plan Morawieckiego) wskazuje rozwój innowacyjnych firm jako jeden z filarów rozwoju gospodarczego Polski.**

Technologie, które mogą wesprzeć i przyspieszyć zmiany, to Internet Rzeczy oraz Sztuczna Inteligencja. W raporcie *Internet of Things (IoT) i Artificial Intelligence (AI) w Polsce. Jak wykorzystać rewolucję technologiczną Internetu Rzeczy i Sztucznej Inteligencji w rozwoju Polski* eksperci wskazali drogi tworzenia wartości dodanej w 15 różnych obszarach gospodarki, korzystając z tych technologii, oraz polskie przedsiębiorstwa oferujące już rozwiązania IoT i AI. Partnerami raportu są Cisco, EY i Phoenix Systems.

Olbrzymie ilości danych oraz możliwości przetwarzania współczesnych komputerów zmieniają paradygmat rozwoju. Dotychczas, gdy pojawiał się problem, naukowcy, politycy i przedsiębiorcy stosowli różne procesy lub sposoby działania, które miały się przyczynić do znalezienia rozwiązania. Mówiąc językiem matematyki, celem całego działania było poszukiwanie właściwych algorytmów, które przetworzą problem w rozwiązanie. Można to działanie zapisać poniższym wzorem:

Obecnie, dzięki olbrzymim możliwościom obliczeniowym i ilości danych wzór ten przybiera inną postać. Przedstawiamy maszynom opis oczekiwanego rozwiązania, a one podają algorytm. Dziś wzór ten wygląda następująco:

Nie wiemy jeszcze, jak dokładnie zmiana paradygmatu rozwoju wpłynie na nasze życie, ale jedno jest pewne – będzie olbrzymia. Jeżeli Polska włączy się w proces kreowania tej zmiany, zamiast dalej podążać drogami wyznaczonymi przez innych, to zdefiniuje na nowo swoje miejsce w gospodarce świata na następne dwa, trzy pokolenia.

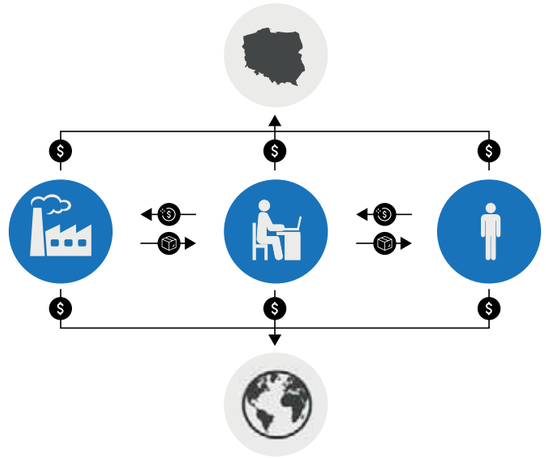
Pierwszy raz, w czasach dokonującej się na świecie kolejnej rewolucji technologicznej, to od nas zależy, jaką rolę w niej odegrają polskie firmy i polscy przedsiębiorc. – podkreśla Bartłomiej Michałowski, autor raportu.

Z kolei dr Aleksander Poniewierski, partner i Global IoT Leader w EY uważa, że *Internet Rzeczy i sztuczna inteligencja to technologie, które stwarzają możliwość krajom, które nie robiły historycznie potężnych inwestycji, ale są zdeterminowane, by osiągnąć postęp, na zrobienie tzw. żabiego skoku. Oczywiście pewne fundusze są jak zawsze potrzebne, natomiast szanse wszystkich gospodarek są bardzo wyrównane. Dlatego państwa takie jak Niemcy, Włochy czy Francja ogłaszają rządowe programy wsparcia właśnie po to, by zapewnić stymulację tym technologiom. Takich przykładów, kiedy nowoczesna technologia pozwala na żabi skok, jest na świecie dużo, np. bankowość mobilna w Afryce. Dzieje się tak, ponieważ ludzie łączą konwencjonalne metody z nowoczesnymi technologiami i to zmienia modele biznesowe oraz modele operacyjne. Druga kwestia jest taka, że Internet sprawił, że nowe trendy nie mają granic. Biznes i technologia zostały odmiejscowione. Tutaj też środki finansowe na rozwój są niezbędne, ale ta bariera nie jest tak duża, jak w przypadku trzeciej rewolucji przemysłowej. Jedyne ograniczenia w przypadku korzystania z IoT czy AI to opór ludzi przed adaptowaniem i uznaniem zmian oraz brak wiedzy w tym zakresie. To, co będzie decydowało o przewadze konkurencyjnej gospodarek, to właśnie wiedza, świadomość i podatność na zmiany, a nie technologie, która są już powszechne i względnie tanie.*

Raport zawiera rekomendacje i propozycje dla polskich polityków i decydentów

> Jeśli nie uda się zapewnić odpowiedniego poziomu bezpieczeństwa urządzeń IoT, ich wykorzystanie w gospodarce będzie bardzo ograniczone. Nie będzie poparcia społecznego dla wdrażania systemów, których użytkowanie może wiązać się z zagrożeniem bezpieczeństwa, życia lub zdrowia

ŁAŃCUCH TWORZENIA WARTOŚCI B-B-C



gospodarczych, abyśmy ekonomicznie skorzystali na nowej rewolucji technologicznej.

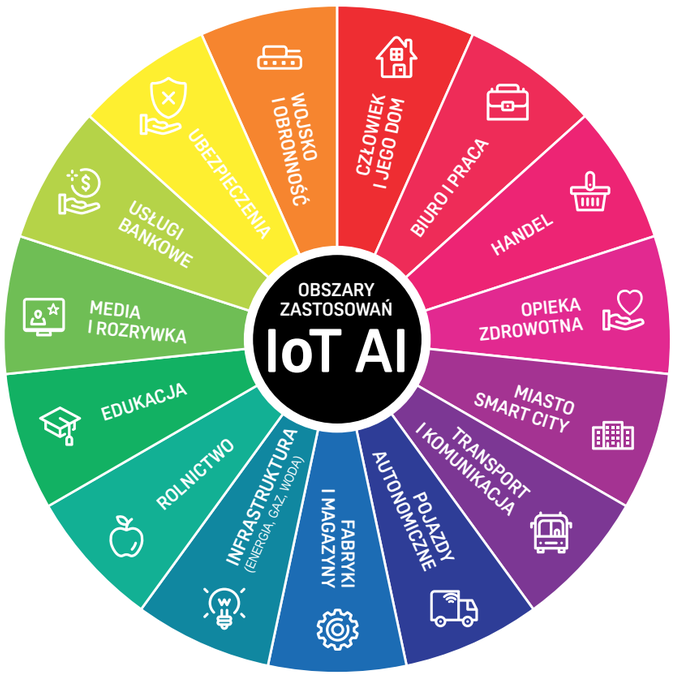
15 obszarów gospodarki, w których polskie firmy IoT i AI mogą zarabiać

Raport Instytutu Sobieskiego *Internet of Things (IoT) i Artificial Intelligence (AI) w Polsce* odpowiada na pytanie, jak wykorzystać rewolucję technologiczną Internetu Rzeczy i Sztucznej Inteligencji w rozwoju Polski. Autorzy podają listę rekomendacji działań dla rządu i polskich decydentów gospodarczych oraz wymieniają polskie firmy, które na rynku IoT i AI już działają.

Eksperci zalecają przeprowadzenie analiz całego łańcucha tworzenia wartości B-B-C dla IoT i AI w każdym z 15 obszarów polskiej gospodarki pod kątem zysków i korzyści dla niej. Strategia działania i uwzględnienie polskich przewag konkurencyjnych jest konieczne, aby wykorzystać nową rewolucję technologiczną. Najważniejszą rekomendacją dla rządu, ale również samorządów i spółek Skarbu Państwa jest kreowanie popytu na rozwiązania IoT i AI poprzez zamówienia publiczne oraz zachęty fiskalne dla inwestycji w rozwiązania, które zgodnie z wynikiem analizy całego łańcucha B-B-C generują wartości dodane dla polskiej gospodarki.

W raporcie przedstawiono konkretne pomysły działań i rekomendacji dla

OBSZARY ZASTOSOWAŃ IOT I AI



każdego obszaru zastosowań IoT i AI. Przykładowo, w obszarze Biuro i Praca rekomenduje się wprowadzenie współdzielenia powierzchni biurowych przez różne ministerstwa i przeniesienie części tej powierzchni poza Warszawę. W obszarze Opieka Zdrowotna wskazywane działania to wprowadzenie dodatkowych refundacji dla zakładów opieki zdrowotnej, których lekarze określoną liczbę badań i konsultacji będą wykonywać zdalnie, bez konieczności wezwania chorego lub rehabilitowanego do placówki medycznej.

Bardzo ciekawe i przynoszące największą wartość dodaną dla polskiej gospodarki są rekomendacje w obszarach Infrastruktura oraz Usługi Bankowe. W tym pierwszym autorzy zalecają utworzenie podlegającego bezpośrednio premierowi zespołu składającego się z ekspertów pracujących na zlecenie wielu ministerstw. Celem tego zespołu byłoby zdefiniowanie nowego modelu biznesowego opłat za energię elektryczną z wykorzystaniem nowych możliwości IoT i AI. W drugim obszarze sugerują, aby polski bank, zgodnie z prawem i regulacją NBP i KNF dotyczącą emisji pieniądza elektronicznego, wyemitował określoną liczbę e-złotych w technologii *blockchain*, a Ministerstwo Nauki i Szkolnictwa Wyższego wypłaciło w nich stypendia. W raporcie jest również pomysł ustanowienia miliona dolarów międzynarodowej nagrody dla twórców gry z „polskim DNA", czyli takiej, która promuje polską kulturę lub historię.

Wszystkie rekomendacje mają wspólny cel – sprawić, aby polskie firmy z obszaru IoT i AI miały szansę rozwoju i tworzenia rozwiązania, również jako światowi liderzy. – *Integracja rozwiązań Internetu Rzeczy i Sztucznej Inteligencji daje zupełnie nowe otwarcie w wielu obszarach gospodarki. Jeśli w Polsce zrobimy „coś" jako pierwsi i najlepiej, to stworzymy szansę na definiowanie standardów i eksport know-how polskiej firmy, która to „coś" zrobi* – mówi Bartłomiej Michałowski.

Aspekt społeczny

Poza aspektem rozwojowym i finansowym autorzy zwrócili również uwagę na aspekt społeczny związany z nową rewolucją technologiczną. Twierdzą, że całe społeczeństwo musi mieć dostęp do infrastruktury, która umożliwia konsumowanie produktów i usług IoT i AI, mieć możliwość korzystania z rządowych programów dających szansę na przekwalifikowanie zawodowe w momencie utraty pracy z powodu wprowadzania robotyzacji oraz dbać o zatrzymywanie talentów w Polsce. Jeśli najzdolniejsi Polacy będą rozwijać talenty oraz firmy IoT i AI poza Polską, stracimy szansę na rozwój.

Autorzy proponują mierzyć sukces lub porażkę programów rozwojowych rządu w zależności od wzrostu lub spadku Polski w trzech międzynarodowych rankingach: *Better Life Index* publikowanego przez OECD, *Networked Readiness Index* prowadzonego przez World Economic Forum oraz *Corruption Perceptions Index* opracowanego przez Transparency International.

Cyberbezpieczeństwo

We wszystkich 15 omawianych obszarach zastosowania i rozwoju IoT i AI największe ryzyko jest związane z dwoma zagadnieniami:

– ochroną infrastruktury umożliwiającej korzystanie z Internetu i technologii cyfrowych,
– ochroną integralności i poprawności danych oraz zabezpieczeniem własności intelektualnej i tajemnicy przedsiębiorstwa.

W rewolucji IoT i AI cyberbezpieczeństwo jest sprawą kluczową, tymczasem na liście 500 największych firm z obszaru cyberbezpieczeństwa nie ma żadnej polskiej firmy. Równocześnie w polskiej kodyfikacji kont kosztowych samorządów nie istnieje kod wydatków na ochronę w cyberprzestrzeni. Dużo mówi się o powołaniu nowej formacji obrony terytorialnej, nie wspominając o zapewnieniu budżetu na specjalistów od bezpieczeństwa w sieci informatycznej.

Autorzy raportu rekomendują utworzenie celowego budżetu na wynagrodzenia dla najlepszych specjalistów z obszaru informatyki, cybernetyki i robotyki w wysokości co najmniej 500 000 zł na etat rocznie. Państwo powinno mieć zespół ok. 100 najlepszych specjalistów od technologii cyfrowych i cyberbezpieczeństwa, którym będzie zapewniać konkurencyjne w skali świata wynagrodzenia.

W coraz bardziej połączonym świecie, w którym technologie się przenikają, kluczowe jest bezpieczeństwo łańcucha biznesowego na każdym jego etapie. Nie wystarczy już, że organizacje skupiają się wyłącznie na ochronie wewnętrznych modeli biznesowych, ofert i infrastruktury. Dlatego przede wszystkim konieczne jest identyfikowanie wszystkich kluczowych graczy w 15 obszarach gospodarki i rozumienie ich wpływu na bezpieczeństwo całego łańcucha B-B-C. Opracowanie elastycznej architektury bezpieczeństwa, którą można udostępniać i wdrażać u wszystkich uczestników łańcucha biznesowego, wymusza wyższy poziom współpracy niż dotychczas.

Łukasz Bromirski, przedstawiciel Cisco – partnera raportu i lidera w obszarze rozwiązań cyberbezpieczeństwa, mówi: *Zapewnienie cyberbezpieczeństwa całego łańcucha B-B-C jest warunkiem koniecznym, aby korzystać z technologii i rozwiązań Internetu Rzeczy i sztucznej inteligencji w sposób odpowiedzialny. Konieczny jest wręcz nowy paradygmat w myśleniu o cyberbezpieczeństwie, traktujący to zagadnienie w sposób holistyczny, jako spójną, wielowarstwową architekturę technologiczną, wbudowaną w tkankę sieci, a nie jako dodatek w postaci jednego czy drugiego urządzenia punktowego. Sieć łączy ze sobą miliardy urządzeń IoT na całym świecie, dlatego zapewnienie widoczności ruchu w sieci pozwala wykrywać zagrożenia przez nią przepływające. Co ciekawe, z pomocą przychodzą mechanizmy uczenia maszynowego i sztuczna inteligencja, które analizują terabajty danych ruchu sieciowego w poszukiwaniu anomalii, charakterystycznych dla złośliwego kodu. Pamiętajmy, że jeśli nie uda się zapewnić odpowiedniego poziomu bezpieczeństwa urządzeń IoT, ich wykorzystanie w gospodarce będzie bardzo ograniczone. Nie będzie poparcia społecznego dla wdrażania systemów, których użytkowanie może wiązać się z zagrożeniem bezpieczeństwa, życia lub zdrowia.*

System operacyjny Phoenix-RTOS może stać się standardem w świecie IoT. Nowoczesna energetyka *(smart grid)* to pierwszy obszar zastosowań, w których ten system potwierdza swoje przewagi technologiczne. Wkrótce powinien być także stosowany jako podstawa roju dronów i innych urządzeń wykorzystujących sztuczną inteligencję

Jacek Madajczyk, wiceprezes Phoenix Systems, dostawcy rozwiązań IoT i AI dla energetyki, zwraca uwagę, że *rewolucja technologiczna, jaka w tej chwili dokonuje się w świecie mikrokontrolerów i bazujących na nich urządzeniach Internetu Rzeczy, może być porównywana jedynie z rewolucją związaną z pojawieniem się i upowszechnieniem komputerów PC w końcu ubiegłego wieku. Polskie firmy mają szansę odegrać główną rolę w tej rewolucji, a system operacyjny Phoenix-RTOS może stać się standardem w świecie Internetu Rzeczy. Nowoczesna energetyka (smart grid) to pierwszy obszar zastosowań, w których Phoenix-RTOS potwierdza swoje przewagi technologiczne. Wierzymy, że wkrótce będzie także stosowany jako podstawa roju dronów i innych urządzeń wykorzystujących sztuczną inteligencję (AI)* – wyjaśnia dr Madajczyk.

FRAGMENT RAPORTU

Obszar 13 – usługi bankowe i finansowe

Firmy technologiczne rozwijające się w obszarze są określane firmami *FinTech*. Technologie IoT i AI mają w nim kluczowe znaczenie. Po obszarze mediów i handlu (*e-commerce, marketplace* i szeroko rozumiane platformy wymiany handlowej), które już poddały się masowej cyfryzacji, usługi bankowe i finanse są w tej chwili największym na świecie obszarem generowania wartości dodanej.

Szczególnym nowym polem jest stosowanie technologii *blockchain* [1]. Dziś ta technologia, dająca nowe możliwości zabezpieczania danych i informacji o transakcjach w sieci, jest znana głównie dzięki pierwszej walucie wirtualnej *bitcoin* [2]. *Blockchain* może stanowić przełom w obszarze technologii cyfrowych, o czym świadczy popularność tego tematu na ostatnim forum w Davos i omawianie tej technologii na najważniejszych uniwersytetach świata [3].

W Polsce technologię tworzenia cyfrowej wersji waluty narodowej w oparciu o *blockchain* rozwija firma Bilion. Dostała ona w 2017 r. nagrodę prezydenta Rzeczypospolitej Andrzeja Dudy.

Rząd mógłby wyemitować określoną ilość złotego w postaci waluty cyfrowej, w pełni regulowanej jak złoty „papierowy". Waluty cyfrowej nie należy mylić z walutą *bitcoin*, która nie podlega żadnej regulacji i nie ma żadnego banku emitenta. Cyfrowy złoty byłby emitowany przez polski bank w ramach jego standardowej działalności. Rząd mógłby np. wypłacać wszystkie stypendia naukowe wyłącznie w cyfrowym złotym. Warunkiem jest przygotowanie odpowiedniej infrastruktury umożliwiającej zakupy za pomocą e-złotego. Dzięki temu Polska miałaby szansę budować światowe standardy. Dziś Polska Wytwórnia Papierów Wartościowych drukuje pieniądze dla kilku państw na świecie, przyczyniając się do zwiększania polskiego eksportu. W przyszłości moglibyśmy eksportować cyfrowe waluty.

[1] *Blockchain* – zdecentralizowana i rozproszona baza danych o architekturze *peer-to-peer* bez centralnych komputerów i niemająca scentralizowanego miejsca przechowywania danych, zakodowana za pomocą algorytmów kryptograficznych.
[2] *Bitcoin* – waluta niekontrolowana przez żaden bank, a jedynie przez inteligentny algorytm. Korzysta z technologii *blockchain*. Jej twórcą jest Satoshi Nakamoto, który wprowadził ją przed ponad 10 laty.
[3] https://www.extension.harvard.edu/academics/courses/breakthroughinnovation-blockchaintechnology/25067

Cztery typy uczenia maszynowego

Początki uczenia maszynowego sięgają przełomu lat 50. i 60. Kluczowym momentem w rozwoju tej technologii było powstanie systemu eksperckiego Dendral na Uniwersytecie Stanforda. Podstawowym zadaniem systemu było ustalenie struktury molekularnej nieznanych chemicznych związków organicznych.

Katarzyna Kwiecień
SAS Institute

Obecnie *machine learning* jest wykorzystywane w biznesie na szeroką skalę, m.in. do personalizacji ofert sprzedażowych czy identyfikacji nowych form kontaktu z klientami. Potwierdzają to dane SAS, z których wynika, że 68% firm postrzega uczenie maszynowe jako istotny trend technologiczny. Maszyny uczą się dzięki algorytmom, czyli ciągom zdefiniowanych czynności niezbędnych do pozyskania danej wiedzy. Za każdym razem, gdy system zasilają nowe dane, prezentowane przez niego wyniki są coraz dokładniejsze. Uczenie maszynowe polega głównie na 4 działaniach:

- kategoryzacji / katalogowaniu informacji,
- przewidywaniu określonych zdarzeń na podstawie zidentyfikowanych wzorców,
- identyfikacji nieznanych do tej pory wzorców i zależności między danymi,
- wykrywaniu anomalii oraz nieprzewidywalnych zdarzeń.

Różne rodzaje uczenia maszynowego

Uczenie maszynowe nie jest jednolitą technologią. Sposób jej działania zależy w dużej mierze od tego, z jakich algorytmów korzysta i jakimi danymi zostanie zasilona. Eksperci SAS wskazują 4 podstawowe techniki uczenia maszynowego:

- **Uczenie nadzorowane** *(Supervised Learning)* – maszyny uczą się na podstawie przykładów. To tak jakby uczniowie otrzymali klucz do testu i zostali poproszeni o jego rozwiązanie. Dane wejściowe są wykorzystywane do wyszukiwania zależności, które służą do rozwiązania określonego problemu. Gdy uda się ustalić pewien wzorzec, jest on wykorzystywany w podobnych przypadkach.

Przykłady zastosowania uczenia nadzorowanego: zarządzanie ryzykiem, wykrywanie nadużyć, personalizacja interakcji, rozpoznawanie mowy, tekstu i obrazu oraz segmentacji klientów.

- **Uczenie częściowo nadzorowane** *(Semi - Supervised Learning)* – w tym przypadku maszyna otrzymuje dane wejściowe zarówno oznaczone (zawierające odpowiadające im dane wyjściowe, konkretne przykłady), jak i nieoznaczone (wymagające przyporządkowania do danych wyjściowych, znalezienia odpowiedzi). Ten rodzaj uczenia maszynowego wykorzystuje się w sytuacjach, gdy organizacja dysponuje zbyt dużą ilością danych lub gdy informacje są na tyle zróżnicowane, że nie sposób przyporządkować odpowiedzi do każdej z nich. System sam proponuje odpowiedzi i jest w stanie stworzyć ogólne wzorce.

Przykłady zastosowania uczenia częściowo nadzorowanego: rozpoznawanie mowy i obrazu, klasyfikacja stron internetowych.

- **Uczenie nienadzorowane** *(Unsupervised Learning)* – maszyna nie posiada „klucza odpowiedzi" i musi sama analizować dane, szukać wzorców i odnajdywać relacje. Ten rodzaj *machine learning* najbardziej przypomina sposób działania ludzkiego mózgu, który wyciąga wnioski na podstawie spontanicznej obserwacji i intuicji. Wraz ze wzrostem zbiorów danych prezentowane wnioski są coraz bardziej precyzyjne.

Przykłady zastosowania uczenia nienadzorowanego: analiza koszyka zakupowego, wykrywanie anomalii, rozpoznawanie podobnych obiektów.

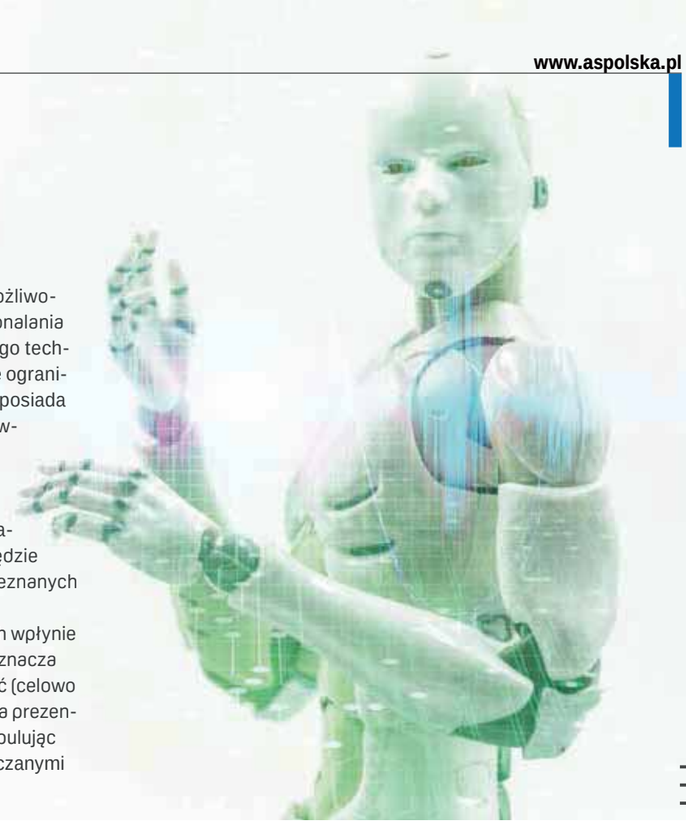
- **Uczenie wzmocnione** *(Reinforcement Learning)* – maszyna otrzymuje gotowy zestaw dozwolonych działań, reguł i stwierdzeń. Działając w ich ramach, dokonuje analizy i obserwuje ich skutki. Wykorzystuje reguły w taki sposób, aby osiągnąć pożądany efekt. Można to porównać do nauki gry w koszykówkę. Zasady określające, kiedy są kroki, faul czy aut pozostają niezmienne. Natomiast to, w jaki sposób drużyna zdobędzie punkt (zawodnik rzuci z dystansu, wbiegnie pod kosz lub poda) zależy od decyzji graczy, którzy podejmują ją na bieżąco.

Przykłady zastosowania uczenia wzmocnionego: nawigacja (wybór trasy na podstawie informacji o natężeniu ruchu i warunkach na drodze), gaming (dostosowywanie scenariuszy rozgrywki do działań gracza), robotyka (dostosowanie pracy robotów do obłożenia i rodzaju wytwarzanego produktu).

Czego maszyna się nie nauczy?

Mimo ogromnych możliwości i ciągłego udoskonalania uczenia maszynowego technologia ta ma pewne ograniczenia. Maszyna nie posiada umiejętności kreatywnego myślenia i nie przedstawi spontanicznie hipotezy bez odpowiednich danych. Ponadto nie będzie odbierać nowych, nieznanych bodźców.

Każda zmiana danych wpłynie na pracę maszyny. Oznacza to, że można wpłynąć (celowo lub przez pomyłkę) na prezentowane wyniki, manipulując informacjami dostarczanymi do systemu.



Ela-compil
ul. Szczepanowskiego 8, 60-541 Poznań
tel. 61 869 38 50
office@ela.pl

Integracja systemów bezpieczeństwa przyszłością branży security

Z **Jakubem Bartkowiakiem**, **dyrektorem Działu Oprogramowania w Ela-compil**, rozmawia Jan T. Grusznic, zastępca redaktora naczelnego „a&s Polska”

Od lat obserwujemy pozytywny trend związany ze zintegrowanymi systemami zabezpieczeń. Łącząc sygnały z wielu podsystemów, znacząco ograniczają one ryzyko wystąpienia zdarzeń niepożądanych, takich jak pożar lub włamanie. Ponadto ułatwiają zarządzanie obiektem i wpływają na jego funkcjonalność. GEMOS jest jednym z takich systemów. Co go wyróżnia na tle konkurencji?
Jest kilka elementów. Przede wszystkim liczba różnych podsystemów, które jest w stanie połączyć. Architektura systemu wymusza, żeby każda integracja była samodzielnym modułem, dzięki czemu jej rozwój jest niezależny od rozwoju rdzenia systemu, a raz stworzona może być ponownie użyta. W ten sposób system doczekał się ponad 750 różnych takich modułów. Drugim ważnym atutem jest jego uniwersalność i elastyczność. Nie ma takich samych instalacji systemu GEMOS, a jest ich ponad tysiąc. Należy podkreślić różnicę pomiędzy systemami, które są tworzone pod kątem klienta, a systemami takimi jak GEMOS, które są konfigurowane pod jego kątem. W pierwszym przypadku producent tworzy wariację swojego produktu, która ma własny cykl życia i nadaje się do użytku tylko w docelowym projekcie. System GEMOS natomiast zawsze jest ten sam, a jego rozbudowane możliwości konfiguracji zapewniają uzyskanie pożądanego poziomu integracji. Dzięki takiemu podejściu klienci mogą szybciej aktualizować system, a producent może planować dalszy rozwój oprogramowania.
Ostatni argument jest dyskusyjny, ale postaram się go obronić. Chodzi o fakt, że GEMOS działa w przeglądarce internetowej. Jako główną zaletę takiej architektury najczęściej podaje się brak konieczności instalowania dodatkowego oprogramowania na stacji klienckiej, ponieważ przeglądarka praktycznie zawsze w komputerze jest zainstalowana. Ułatwia nam to życie i ma jeszcze jedną zaletę. Zadajmy sobie pytanie, z jakich aplikacji na co dzień korzystamy i ile spośród nich obsługujemy lub moglibyśmy obsługiwać przez przeglądarkę. Dzisiaj Internet zdominował nasze życie, a rozbudowane aplikacje przeglądarkowe zadomowiły się i zaczęły wypierać klasyczne. Przeglądarki dają dziś ogromne możliwości. Są nawet dostępne komputery, takie jak Google Chromebook, w których pełnią one funkcję systemu operacyjnego. Rynek aplikacji dostępnych przez przeglądarkę rozwija się dynamicznie. Ten trend sugeruje, że wkrótce nasi użytkownicy będą korzystać wyłącznie z aplikacji dostępnych przez przeglądarkę lub ze smartfonu i powoli zapomną, jak wyglądają klasyczne aplikacje desktopowe lub jak się je instaluje. GEMOS może na tym tylko skorzystać.

Tyle że typowy interfejs użytkownika platformy PSIM prezentuje się dość siermiężnie w porównaniu do obecnie dostępnych aplikacji przeglądarkowych. Choć na tegorocznych targach w Essen pokazaliście, że można wprowadzić nową jakość w sposobie prezentacji planów i danych. Na czym polega GEMOS MOSAIC i skąd pomysł na jego stworzenie?
W naszej branży takie rzeczy, jak wygląd czy intuicyjność obsługi interfejsu użytkownika aplikacji, często niestety schodzą na dalszy plan. Liczy się przede wszystkim wywiązanie z zapisów zawartych w SIWZ. Poza tym trudno byłoby je opisać, ponieważ to kwestia percepcji i subiektywnej opinii. Każdego interfejsu użytkownika można się przecież nauczyć, a systemów PSIM nie wdraża się bez serii szkoleń. Warto jednak zatrzymać się na chwilę i przyjrzeć systemom typu *smart home*, które są de facto rodzajem PSIM w skali mikro. Co prawda oferują ubogą funkcjonalność w porównaniu do PSIM, ale zwykle ich interfejs użytkownika stoi na wysokim poziomie. Może to wynikać stąd, że klientem końcowym jest zwykle tzw. pokolenie *plug-and-play,* które kupuje oczami i oczekuje, że bez szkolenia czy instrukcji obsługi będą mogli korzystać z aplikacji.
Ta obserwacja była zalążkiem pomysłu stworzenia nowego modułu wizualizacji planów w GEMOS, który wyglądem i intuicyjnością obsługi nie odstawałby od nowoczesnych aplikacji internetowych. Chcieliśmy zaprzeczyć tezie, że sposób działania nie jest tak ważny, i udowodnić, że nasza branża doceni te same aspekty, które wymuszają klienci indywidualni. Tak powstał moduł MOSAIC, który wnosi nową jakość do wizualizacji planów w GEMOS. Wspiera różne formaty map w sposób zunifikowany, oferując płynność obsługi, znacznie większy zakres przybliżania, animacje, poruszające się punkty, dynamiczne rysowanie stref, wykrywanie kolizji, obsługę ekranów dotykowych i wiele innych funkcji, zachowując przy tym wsteczną kompatybilność z dotychczasowymi rozwiązaniami. To na początek, bo dopiero się rozkręcamy.

Ale, ale… Przecież to samo można osiągnąć, stosując grafikę wektorową?
Z grafiki wektorowej korzystaliśmy od dawna. W 2005 r. na konferencji SVG Open prezentowano korzyści z zastosowania wektorowego formatu SVG w przeglądarkach internetowych właśnie na przykładzie systemu GEMOS. Należy dodać, że natywne wsparcie dla tego formatu pojawiło się w pierwszych przeglądarkach dopiero trzy lata później. Dzisiaj format SVG nie wymaga instalowania jakichkolwiek dodatków, jednak użycie go do wizualizacji planów w przeglądarce internetowej nadal stanowi wyzwanie. Trzeba zmierzyć się z problemami wydajności, kontrolą tego, co jest wyświetlane, detekcją interakcji z użytkownikiem i wieloma innymi. Pracując nad modułem MOSAIC, zdecydowaliśmy, że wspierane dotychczas wektorowe formaty SVG oraz DWG będą nadal używane, ale jedynie jako punkt wyjścia do konwersji na format docelowy. Umożliwia to aktualizację i użycie tego modułu przez obecnych klientów, jak również nie wprowadza nowych nieznanych standardów.

A propos standardów. Coraz częściej w urządzeniach zabezpieczeń technicznych dostępne są otwarte standardy komunikacji. Przykładem może być ONVIF, który w tym roku skończył 10 lat. Czy popularyzacja otwartych standardów wymiany informacji pomaga w integracji?
Zdecydowanie pomaga, pod warunkiem że standardy te nie są ściśle powiązane z konkretnym językiem programowania lub platformą, a producenci systemów prawidłowo z nich korzystają. Za pozytywny przykład

niech posłuży wspomniany standard ONVIF spopularyzowany w CCTV. Nie jestem zwolennikiem formatu XML i protokołu SOAP, ale muszę przyznać, że od czasu, gdy zaczął być powszechnie stosowany, wysterowanie pozycji predefiniowanej w kamerze czy uzyskanie adresu strumienia wideo nie stanowi już problemu. Nie trzeba się w tym celu kontaktować z producentem lub stosować specjalnie stworzonych do tego celu rozwiązań. Negatywnym przykładem jest, moim zdaniem, standard OPC DA, bardzo popularny w automatyce budynkowej, stosowany również na rynku security. Już na starcie integrator jest zmuszony do korzystania wyłącznie z systemu Windows, ponieważ na nim standard został oparty. Potem nie jest łatwiej. Konfigurowanie zdalnego połączenia z serwerem OPC przypomina czasami drogę przez mękę. Problemów można by uniknąć, instalując różne programy firm trzecich, które wszystko za nas zrobią i podadzą informacje w bardziej przyjazny sposób – ale nie po to stosuje się standardy, żeby ich potem unikać.

Każdy standard jest inny, więc nie można jednoznacznie powiedzieć, że ich użycie zawsze ułatwi wszystkim życie. Jeżeli integrator nie ma wsparcia programistycznego, wtedy na pewno będzie preferował standardy otwarte. Jeżeli natomiast dysponuje działem programistów, skomplikowany otwarty standard może okazać się czasem bardziej pracochłonny niż zaimplementowanie i użycie optymalnego natywnego protokołu komunikacyjnego producenta.

Czyli jednak protokół natywny góruje nad otwartym?

Na pewno protokoły natywne, czyli stworzone przez producentów systemów, są optymalnie dopasowane i często „lżejsze" niż otwarte uniwersalne protokoły ze swoimi „ciężkimi" warstwami abstrakcji. Przykładowo, przesłanie prostej wartości do systemu integrującego przy użyciu protokołu BACnet wymaga implementacji całego stosu komunikacyjnego i wsparcie tego standardu przynajmniej w minimalnym zakresie. W przypadku protokołu natywnego, jeżeli system jest prosty, producent może wysłać wartość opakowaną w bajty kontrolne i na tym koniec. Integracja byłaby na pewno szybsza w drugim przypadku i wymagałaby minimalnego wysiłku programisty. Ale uwaga: nawet najprostszy protokół natywny może okazać się bezużyteczny, gdy integrator dysponuje tylko gotową platformą, w którą nie może ingerować. Są też wady protokołów natywnych, które uwidoczniają się przede wszystkim w dwóch przypadkach. Po pierwsze, gdy protokół jest bardzo rozbudowany i skomplikowany. Jeżeli producent dostarcza pakiet SDK, większego problemu nie ma. Jeśli natomiast na integratora spada konieczność implementacji protokołu zgodnie z jego 200-stronicową specyfikacją, którą uzyskał po podpisaniu NDA (umowy poufności – przyp. redakcji), to koszty integracji znacząco rosną, ponieważ próżno szukać w Internecie przykładów wdrożeń. Drugim przypadkiem, często spędzającym sen z powiek, jest sytuacja, kiedy protokół na pierwszy rzut oka wydaje się prosty i czytelny. Ale gdy nie zastosowano w nim logicznych reguł lub jest pełen wyjątków, gdy brakuje powtarzających się schematów, wtedy implementacja staje się problematyczna i podatna na błędy.

Raporty, które publikujemy na łamach a&s alarmują o rosnącym niebezpieczeństwie cyberataków na urządzenia przemysłowe oraz elementy platformy PSIM jako najbardziej podatne. Jako szef działu programistów jak oceniasz to zagrożenie? Na co zwracać uwagę, administrując takim systemem, by ryzyko skutecznego ataku było mniejsze?

Zagrożenie jest jak najbardziej realne, zwłaszcza gdy wydaje się nam, że skoro system nie jest podłączony do Internetu, to jest bezpieczny. Często spotykam się ze stanowczym sprzeciwem podłączania jakichkolwiek komponentów systemów do Internetu ze względu na przepisy bezpieczeństwa. Moim zdaniem to wylewanie dziecka z kąpielą, a takie przepisy są drogą na skróty. Korzystanie w obiekcie z sieci Wi-Fi, portów USB, komputerów przenośnych, brak polityki aktualizacji systemów operacyjnych czy też obecność sieci VPN łączącej rozproszone lokalizacje już stanowi punkty ataku i zagrożenie. Prawda jest taka, że samo ukrywanie się nie spowoduje, że będziemy bezpieczniejsi. Spójrzmy natomiast, co w efekcie takiej polityki tracimy. Dzisiaj moc obliczeniowa, jaką udostępniają nam operatorzy chmur, daje nowe możliwości, których nie bylibyśmy w stanie uzyskać, korzystając wyłącznie z zasobów lokalnych. Przykładem jest Microsoft, który intensywnie rozwija własną chmurę i planuje wykorzystanie dobrodziejstw sztucznej inteligencji i uczenia maszynowego do wspomagania procesów np. w fabrykach. Zamiast na ślepo blokować jakikolwiek ruch z i do Internetu, zdecydowanie lepszym rozwiązaniem jest zatrudnienie specjalistów ds. bezpieczeństwa IT i okresowe zamawianie testów. Nie należy myśleć, że „nikt mnie nie zaatakuje", a raczej, że „kiedy mnie zaatakują, wiem, jak mam się bronić".

Wracając do rozwoju oprogramowania: słyszałem, że po sukcesie MOSAIC Ela-compil otrzymała większą swobodę w tworzeniu kolejnych innowacji dla systemu GEMOS. Możesz zdradzić, nad czym obecnie pracujesz?

Przygoda z MOSAIC zaczynała się niepozornie, był to projekt wymyślony na przerwie kawowej i realizowany początkowo w wolnym czasie jako prosty *proof-of-concept*. Szybko zyskał jednak zainteresowanie i fakt prezentowania niedawno efektów naszej ciężkiej pracy na najważniejszej imprezie w branży, czyli targach Security w Essen, był zwieńczeniem naszego sukcesu. Z uwagi na potencjał, jaki oferuje MOSAIC, zaczęliśmy być zasypywani pomysłami nowych funkcjonalności, a w przyszłym roku, gdy moduł trafi do obecnych i nowych klientów, pomysłów będzie na pewno jeszcze więcej. Przygotowujemy się na dalszy jego rozwój, ale na horyzoncie mamy już kolejny, znacznie większy projekt. MOSAIC miał wprowadzić nową jakość do interfejsu użytkownika platformy GEMOS i to się udało, ale stanowi on sam w sobie tylko jedną z części całego systemu. Pora zrobić kolejny krok i zabrać się kompleksowo za pozostałe. Zdradzić mogę, że nie tylko ja podzielam ten pogląd i przyszły rok zapowiada się bardzo pracowicie!

Dziękuję za rozmowę.

Obserwacja z chmury

Niepodzielne rządy rozwiązań dozoru wizyjnego opartych na lokalnych systemach sieciowych powoli zaczynają ustępować coraz bardziej popularnym rozwiązaniom chmurowym.

Michał Marciniak

Rynek reaguje na te zmiany dynamicznie. Nasycenie już jest widoczne w sektorze konsumenckim, należy spodziewać się powolnego przełamywania stereotypów związanych z dostępnością i bezpieczeństwem również dla rozwiązań firmowych. Co zatem stanowi o sile tego rozwiązania i czy faktycznie jest to trend, który nie straci na popularności w najbliższych latach?

Rynek konsumencki

Na rynku konsumenckim wybór jest ogromny i, co ciekawe, wiele rozwiązań można spotkać nie tylko w zaciszu domowym, ale również w niedużych projektach komercyjnych. Większość producentów stosuje zbliżony model działania – kamerę bądź rejestrator łączy się z dedykowaną usługą w chmurze po zeskanowaniu przez aplikację producenta spersonalizowanego kodu QR znajdującego się na produkcie. Korzystając z trzech metod: dedykowanej (wybrany port producenta), szyfrowanej (port 443) lub nieszyfrowanej (port 80), urządzenie rozpoczyna wysyłanie strumienia audio-wideo, nawet gdy znajduje się za firewallem lub NAT-em *(Network Address Translation)*[1]. Te dwa ostatnie czynniki spopularyzowały tę formę transmisji, gdyż obecnie – ze względu na malejącą liczbę publicznych adresów IPv4 [1] i problemy z uzyskaniem odpowiedniej adresacji od operatora (część dostawców usług internetowych dostarcza je wyłącznie w puli adresów prywatnych IP) – jest to jedyna możliwa forma pobrania strumienia wideo przez aplikację podłączoną do Internetu. Dodatkowym atutem tego rozwiązania jest brak potrzeby przekierowywania portów i jakichkolwiek zmian na routerze (co niekiedy, ze względu na urządzenie dostarczone przez dostawcę telekomunikacyjnego, byłoby niewykonalne).

Kolejną cechą, która przyciąga uwagę kupujących, jest możliwość rejestracji zdarzeń zarówno lokalnie (karta SD), jak i w chmurze. Zaletą jest dostęp praktycznie z każdego miejsca lub urządzenia poprzez przeglądarkę internetową oraz pewność, że dane nie zostaną utracone, gdyż rozwiązania *cloud* bazują najczęściej na serwerach Amazon Web Services (AWS). Dostępność oraz odporność na utratę danych są na nich bardzo wysokie, wynoszą odpowiednio 99,99% oraz 99,999999999% [2]. Opcje standardowe, takie jak zarządzanie kamerą, sterowanie pan/tilt/zoom (PTZ), przegląd nagrań i inne są dostępne również z poziomu przeglądarki lub aplikacji na smartfon.

[1] Większość systemów korzystających z NAT ma na celu umożliwienie dostępu wielu hostom w sieci prywatnej do Internetu przy wykorzystaniu pojedynczego publicznego adresu IP.

Dziś już niemal wszyscy producenci rozwiązań telewizji dozorowej mają w swoim portfolio propozycję związaną z technologią *cloud*, np. Axis – Companion, Dahua – Imou, Hikvision – Hik-Connect, itd. Prostota konfiguracji i metoda pracy *plug & play* zwiększyły zapotrzebowanie na tego typu usługi w tym sektorze rynku. Dotychczas konfiguracja kamer i rejestratorów sprawiała wielu niedoświadczonym użytkownikom duży problem i zniechęcała do zakupu tego typu urządzeń.

Rozwiązania dla MŚP

Łącze internetowe, aspekt praktycznie pomijany w rozwiązaniach konsumenckich, w przypadku małych i średnich przedsiębiorstw musi zostać dokładnie rozważony i zbadany przed podjęciem decyzji o przeniesieniu usług do chmury. Najczęściej spotykanym rozwiązaniem na naszym rynku jest dostęp asynchroniczny. Cechuje go wysoka prędkość pobierania przy niskiej prędkości wysyłania danych. Zakup łącza synchronicznego (prędkość wysyłania i pobierania jest na tym samym poziomie) wiąże się z reguły z większym comiesięcznym kosztem za usługę telekomunikacyjną. Ponadto nie każda lokalizacja, szczególnie poza granicami większych miast, umożliwia zestawienie szybkiego i stabilnego łącza opartego na infrastrukturze światłowodowej. Można, a w systemach krytycznych wręcz należałoby zapewnić redundantne łącze od niezależnego operatora, ponieważ przypadki wielogodzinnych awarii dotykają praktycznie wszystkich dostawców. Poziom SLA *(Service Level Agreement)* stanowi kolejny czynnik, który świadczy o stabilności łącza i czasie ewentualnych przestojów lub napraw. Stąd ważne jest to, aby – oprócz decyzji o rezygnacji z części niezbędnej do przechowywania i zarządzania nagraniami (NVR, systemy VMS) – pamiętać o kosztach, które znajdą odzwierciedlenie w przypadku podejścia opartego na TCO *(Total Cost Ownership)*.

Kiedy zadbamy już o aspekt sieciowy, pozostaje decyzja o wyborze rozwiązania. W przypadku firmy kluczowe są jego skalowalność, bezpieczeństwo oraz modułowość. Czynniki te wymuszają stosowanie zdecydowanie bardziej agresywnego i odpowiedniego podejścia niż w rozwiązaniach konsumenckich. Oznacza to, że możemy skorzystać z dwóch głównych modeli:

1. Gotowe rozwiązanie dostarczone przez producenta, które umożliwiają implementację systemów wizyjnych w dużej skali przy zachowaniu wysokiego poziomu bezpieczeństwa i dowolnej konfiguracji, np. Stratocast lub Federation firmy Genetec (rozwiązanie SaaS – *Software as a Service)*.
2. Wdrożyć własne środowisko wirtualne w chmurze, oparte na dowolnym oprogramowaniu VMS (IaaS – *Infrastructure as a Service)*. To doskonałe rozwiązanie dla firmy, która posiada już część infrastruktury przeniesioną do chmury. W tym przypadku będzie to dodanie kolejnej usługi, która rozwinie już posiadaną farmę serwerów. W tym rozwiązaniu kwestia łącza internetowego jest często powiązana nie tylko z dużymi prędkościami, ale także z redundancją na poziomie operatorów niezależnych.

Innym, częściowym rozwiązaniem może być traktowanie chmury tylko jako miejsca przechowywania nagrań czy zdjęć (*cloud storage*). W tym przypadku należy liczyć się z potrzebą długiej retencji zdarzeń, które muszą być zachowane w celach dowodowych. Nic nie stoi na przeszkodzie, aby używać tego modelu jako głównej macierzy dyskowej, jednak wydajność – przy większej liczbie kamer i środowisku rozproszonym – może być istotnym problemem, który należy uwzględnić już na etapie projektowania.

Pomostem łączącym rynki konsumencki i biznesowy są rozwiązania VaaS/VPaaS *(Video as a Service/Video Platform as a Service)* – gotowe produkty, które możemy wdrożyć za pośrednictwem kilku kliknięć w panelu dostawcy. Co zatem można zyskać, stosując takie podejście? Przede wszystkim wiele rozwiązań w jednym miejscu: strumieniowe przesyłanie materiału z kamery IP na stronę internetową w trybie „na żywo", przechowywanie nagrań w chmurze, statystyki, analiza itp. Często dodatkowym atutem jest zapewnienie szyfrowania całej transmisji oraz dostęp do API lub rozwiązań mobilnych. Ze względu na prostotę rozwiązania, skalowalność i różne warianty cenowe dostosowane do liczby kamer (strumieni wideo) oferta ta może znaleźć zastosowanie w każdym segmencie rynku.

Skalowalność, bezpieczeństwo i modułowość to kluczowe aspekty doboru usług w chmurze.

Bezpieczeństwo i przyszłość

Obawa o bezpieczeństwo to jeden z fundamentalnych czynników branych pod uwagę w trakcie podejmowania decyzji o „wyprowadzce" z własnej sieci lokalnej. Obawy te mają uzasadnienie, gdyż – jak wiadomo – nie istnieje system podłączony do Internetu, którego nie można złamać. Ale co zrobić, gdy lokalne urządzenia nie nadążają za zmieniającymi się wymogami bezpieczeństwa? Przykładem może być router brzegowy kupiony kilka lat temu, wycofany z produkcji, do którego producent nie dostarcza już bieżących uaktualnień systemowych. Środowiska chmurowe zmieniają się z dnia na dzień – każdy z dostawców wprowadza nowe usługi, udogodnienia oraz – co najważniejsze – dba o bezpieczeństwo i redundancję (dane, łącza, zasilanie, temperatura, lokalizacje). Jak w każdym systemie zarządzanym przez człowieka, mogą zdarzyć się wpadki [3], ale i tak środowiska te są znacznie bezpieczniejsze i mniej podatne na ataki niż lokalne serwerownie w firmach.

Obserwując trend coraz większych prędkości Internetu oraz zbliżający się powoli dostęp bezprzewodowy 5G, warto rozważyć i skalkulować, który z modeli będzie korzystniejszy, a w szczególności bardziej elastyczny i bezpieczny w planowanych systemach.

Literatura

[1] https://ipv4.potaroo.net/

[2] https://docs.aws.amazon.com/AmazonS3/latest/dev/DataDurability.html

[3] https://www.techrepublic.com/article/aws-outage-how-netflix-weathered-the-storm-bypreparing-for-the-worst/

BIO

Michał Marciniak
Architekt rozwiązań CCTV; od 20 lat w branży IT i security – promotor, wdrożeniowiec i pasjonat nowych technologii z pogranicza monitoringu wizyjnego oraz IT.

Honeywell
ul. Domaniewska 39,
02-672 Warszawa
www.security.honeywell.com/ee/

Honeywell Security Solutions: MAXPRO® Cloud

Chmura to rozwiązanie sieciowe, które z dnia na dzień zdobywa coraz większą popularność wśród użytkowników komputerów, smartfonów, aplikacji biurowych itp. Coraz śmielej wkracza do systemów zabezpieczeń.

Arkadiusz Gmitrzak, Michał Mielczarek
Zespół Honeywell PL || Security Solutions

Każdy producent z branży zabezpieczeń oferuje rozwiązanie wykorzystujące usługi w chmurze. Najczęściej mówi się o chmurze w systemach telewizji dozorowej, rzadziej o systemach sygnalizacji włamania i napadu czy systemach kontroli dostępu. Czym zatem wyróżnia się MAXPRO Cloud? Po pierwsze, z analizy rynku wynika, że jest to prawdopodobnie jedyny produkt, który oferuje komplet rozwiązań w chmurze: telewizję dozorową, system sygnalizacji włamania i napadu oraz kontrolę dostępu. Dzięki temu integracja pomiędzy urządzeniami odbywa się na zewnętrznych serwerach utrzymywanych przez firmę Honeywell. Co za tym idzie użytkownik ma gwarancję, iż jego dane nie są przetrzymywane w nieznanym „dzierżawionym" miejscu. Serwery Honeywella są zlokalizowane na terenie Unii Europejskiej.

Kiedy system bezpieczeństwa łączy się z twoimi interesami

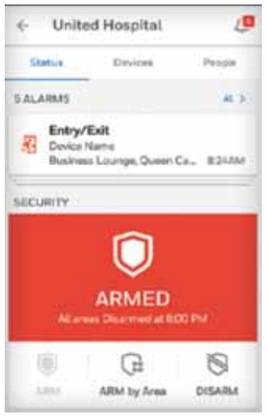
MAXPRO Cloud to coś więcej niż tylko system bezpieczeństwa. To także dynamiczne narzędzie biznesowe pozwalające na monitorowanie procesów w każdej lokalizacji użytkownika, niezależnie od tego, czy łączy się lokalnie, czy zdalnie z dowolnego miejsca na świecie. Usługa dostarcza przydatne informacje, które może wykorzystać do poprawy usług w swojej działalności. MAXPRO Cloud nie wymaga posiadania serwera lub płatnego oprogramowania. Umożliwia także sterowanie firmą z jednego interfejsu aplikacji mobilnej lub/i przeglądarki internetowej: sterowanie drzwiami, uzbrajanie systemów alarmowych, przeglądanie klipów wideo, analizę zdarzeń oraz alarmów na obiekcie. Dzięki temu użytkownik może podejmować decyzje szybciej!

Najważniejsze mieć dobre podstawy

MAXPRO Cloud to już druga odsłona chmury oferowanej przez Honeywell. W tym wydaniu silnik jest oparty na najlepszym oferowanym obecnie rozwiązaniu na rynku: Microsoft Azure. Ten popularny, znany i dobrze oceniany produkt sprawia, iż usługa już na tym etapie dostarcza wielu unikatowych rozwiązań.
Patrząc z kolei w przyszłość, można stwierdzić, iż partnerstwo w tym zakresie firm Honeywell i Microsoft będzie przynosiło coraz więcej przydatnych funkcji. Już teraz słyszy się o planach wprowadzenia różnego rodzaju analiz i mechanizmów, które jeszcze lepiej będą filtrowały dane w zależności od preferencji użytkownika.

Integrator

MAXPRO Cloud to przydatne narzędzie dla integratora, w późniejszym etapie także dla serwisanta urządzeń bezpieczeństwa. Scentralizowany system (w chmurze) umożliwia nadzorowanie zachowań poszczególnych urządzeń z jednego miejsca. Dzięki elastycznemu podejściu do uprawnień to także klient końcowy decyduje, co i w jakim zakresie będzie widoczne dla serwisanta. Serwisant może np. widzieć urządzenia na liście, natomiast nie będzie w stanie przeglądać zdarzeń i oglądać obrazów z kamery na żywo. Dzięki temu pracownicy serwisu są informowani tylko w sytuacjach, które tego wymagają.
Podłączenie urządzeń do usługi jest bardzo łatwe. Po wstępnym skonfigurowaniu rejestratora, centrali alarmowej czy kontrolera drzwi dodajemy je do chmury poprzez wpisanie adresu MAC. Jeżeli wszystkie parametry komunikacji i bezpieczeństwa połączenia są spełnione, systemy są od razu widoczne na koncie integratora. Teraz integrator może przypisać im dodatkowe globalne atrybuty i dodać je do konta użytkownika końcowego.
Posiadając tak skonfigurowany system, instalator może przystąpić do budowania scenariuszy i powiązań pomiędzy urządzeniami, tworzyć harmonogramy pracy urządzeń czy generować cykliczne raporty.



Fot. 1. System CCTV, SSWiN, SKD w zasięgu ręki – wspólny interfejs

Fot. 2. Dostęp przez aplikację mobilną

Fot. 3. Interfejs sieciowy www MAXPRO Cloud – przykłady paneli użytkownika

Klient, użytkownik końcowy

Właściciel obiektu, ochrona czy też inne osoby mające dostęp do interfejsu chmury mogą otrzymywać informacje spersonalizowane. Dla właściciela sieci restauracji czy też stacji paliw istotną informacją będzie liczba osób odwiedzających lokal. Dla właściciela kafejki internetowej – liczba osób korzystających z danego stanowiska komputerowego. Te dane mogą być w prosty i przejrzysty sposób prezentowane na pierwszej stronie po zalogowaniu w formie np. wykresu lub tabeli z danymi. Ponadto właściciel może otrzymywać raporty z różną częstotliwością na swoją skrzynkę poczty elektronicznej.
Dla ochrony, opiekuna technicznego obiektu istotne będą inne kwestie, przede wszystkim związane z bezpieczeństwem obiektu i znajdujących się w nim osób. Dzięki scentralizowanej architekturze, również w formie grafów, operator otrzyma informację o stanie systemu lub alarmach na obiektach, stanie przejść czy też kamer. Analizując przedstawione w prosty sposób dane, będzie wiedział, czy może bezpiecznie uzbroić system, czy też należy sprawdzić obiekt, udając się na miejsce osobiście lub wysyłając ekipę interwencyjną.
Opcja powiadomień wysyłanych na aplikację mobilną zapewnia też, iż każdy wybrany użytkownik zostanie powiadomiony o zdarzeniu niezależnie od tego, czy jest, czy też nie jest zalogowany do chmury.

Dostęp z każdego miejsca

Mimo że mówimy o chmurze, to ważnym aspektem jest scentralizowanie wszystkich systemów pod jednym interfejsem. Chmurę możemy porównać do popularnych systemów czy programów integrujących i wizualizujących. Ze względu na ich ograniczenia, potrzebę posiadania serwerów, odpowiednich modułów komunikacyjnych, licencji itd. nie są one jednak w stanie być tak mobilne, jak narzędzie sieciowe – chmura. MAXPRO Cloud może być przekonfigurowana w dowolnym momencie i w dowolny sposób. Jednego dnia możemy przeglądać zdarzenia np. z drzwi wejściowych (kontrola dostępu) ze wszystkich lokalizacji użytkownika, innego – najważniejszym dla nas parametrem będzie stan systemów alarmowych.

Dla kogo MAXPRO Cloud?

Idealnym odbiorcą MAXPRO Cloud są sieci sklepów, restauracji, stacji benzynowych czy też oddziałów jednej firmy. Interfejs aplikacji umożliwia budowanie wielopoziomowej struktury ułatwiającej orientację w obiektach, a brak ograniczeń sprawia, iż sieć można rozbudowywać bez końca.
MAXPRO Cloud – dzięki takiemu podejściu – staje się idealnym rozwiązaniem dla małych i średnich obiektów o rozproszonej architekturze.

Dahua Technology Poland
ul. Salsy 2
02-823 Warszawa
www.dahuasecurity.com/pl

Inteligentne roboty w security

Robot patrolujący
https://pbs.twimg.com/media/C040GsdVIAETMhO.jpg

Idea tworzenia sztucznych istot istnieje w ludzkiej kulturze od czasów starożytnych, kiedy Archytas z Tarentu konstruował mechaniczne przedmioty, **jednak dopiero schyłek XX wieku przyniósł prawdziwy przełom w tej dziedzinie.**

Robert Sienkiewicz
Dahua Technology Poland

Pierwsze roboty (rok 1961, robot Unimate) były stosowane wyłącznie w produkcji – jako stacjonarne ramię robota wykonywały z góry określone czynności. Dopiero od 1999 r. wkroczyły do wielu dziedzin naszego życia, takich jak rozrywka (zabawka Aibo), medycyna (robot da Vinci) czy odkrywanie kosmosu (łazik Curiosity).

Od 19 lat jesteśmy świadkami niebywałej rewolucji zwanej drugą erą maszyn. Dzięki dynamicznemu rozwojowi sztucznej inteligencji roboty pojawiły się również w branży security. Powierzamy im coraz bardziej odpowiedzialne i skomplikowane zadania: całodobową nieprzerwaną ochronę ludzi i mienia.

W branży security są stosowane dwa podstawowe typy robotów: inteligentny robot gaśniczy oraz autonomiczny robot patrolujący.

Walka z ogniem i ratowanie ludzkiego życia to zadanie odpowiedzialne i ryzykowne. *Strażacy częściej niż inne grupy zawodowe są narażeni na ryzyko wypadku przy pracy. Zgodnie z danymi PSP w okresie 5 lat miało miejsce 8518 wypadków przy pracy, w których rannych zostało 8635 strażaków* [1].

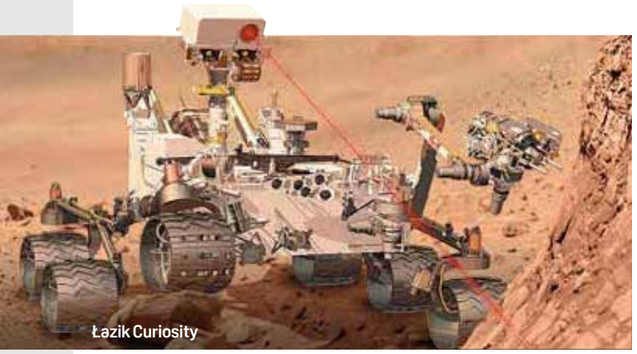
W takich przypadkach nieodzownym wsparciem człowieka jest robot gaśniczy wyposażony w zaawansowane systemy prewencji i eliminowania zagrożenia. Jest na tyle inteligentny, że potrafi zlokalizować źródło ognia, ma czujniki niebezpiecznych związków chemicznych, a przy tym nie jest bezpośrednio narażony na wysoką temperaturę, ponieważ dysponuje zasięgiem strumienia wody do 85 m. Zalety te znacząco poprawiają komfort pracy strażaków, zwiększając jednocześnie ich bezpieczeństwo.

Z kolei pojawienie się robotów patrolujących stanowiło kamień milowy w ewolucji systemów zabezpieczeń. *47 robotów, 24 godz./dobę, w 10 stanach USA pełni swoją służbę* [2], patrolując centra handlowe, parkingi i kampusy korporacyjne. Roboty używają różnych środków: laserów, kamer, czujników termicznych i GPS do wykrywania działalności przestępczej i ostrzegania władz. W przeciwieństwie do ludzi nie potrzebują czasu na odpoczynek, pracują w każdych warunkach atmosferycznych. Ponadto ich zmysły wzroku i słuchu są dokładniejsze niż człowieka, a zarejestrowany materiał z pracy robota może stanowić dowód w sprawie. Stawka godzinowa pracy robota w USA jest mniejsza niż ochroniarza, co w przyszłości będzie miało wpływ na branżę ochroniarską.

Czy sztuczna inteligencja w robotach na tym etapie rozwoju poradzi sobie z otaczającą nas rzeczywistością, pełną nieoczekiwanych scenariuszy?

Nawet człowiek ma problem z właściwym podjęciem decyzji, a co dopiero maszyna. Liczne przykłady wskazują, że autonomiczne roboty, mimo ułomności, są akceptowane przez ludzi.

Cofnijmy się do roku 1938, kiedy to Isaac Asimov sformułował trzy prawa robotyki mówiące, że robot nie może skrzywdzić człowieka, musi być posłuszny jego rozkazom, musi też chronić sam siebie, pod warunkiem że nie koliduje to z dwoma poprzednimi prawami. Jeśli będą one rygorystycznie przestrzegane, kolejne generacje robotów mają szansę nam służyć w utrzymywaniu ładu i porządku na świecie.


Łazik Curiosity

Źródło: https://cdn.galleries.smcloud.net/t/galleries/gf-b799-3Xsf-yaL2_lazik-curiosity-jest-na-marsie-1920x1080-nocrop.jpg

[1] http://medpr.imp.lodz.pl/The-analysis-outlining-the-occurrence-nand-consequences-of-accidents-in-the-work-environment-nof-the-firefighters-employed-by-the-State-Fire-Service-nin-Poland-in-2008-2013,58298,0,1.html

[2] http://www.govtech.com/public-safety/Can-Robots-Replace-Human-Security-Guards.html

Oszuści hotelowi
Problem i szansa na rozwój branży

Michał Czuma

Lista oszustw, na jakie narażeni są właściciele hoteli i ich klienci, a pośrednio także banki obsługujące transakcje hotelowe, jest długa. Zmieniły się metody działania oszustów, pojawiły się też zupełnie nowe zagrożenia.

Banki jakiś czas temu borykały się z ogromnym problemem oszustw. Jeszcze 15 lat temu uważano, że obecność strażnika w banku działa odstraszająco. Dzisiaj strażnicy zaczęli być sukcesywnie zastępowani przez technikę. Obecnie klient banku nawet nie wie, ile ukrytych systemów dyskretnie czuwa nad bezpieczeństwem jego pieniędzy – czy jest w oddziale banku, czy sięga po telefon, by dokonać przelewu za pomocą aplikacji bankowej. To właśnie oszuści spowodowali, że banki zaczęły w końcu inwestować w systemy zmniejszające ryzyko oszustw, dokonując skoku technologicznego. Dzięki temu mogą oferować usługi, o jakich jeszcze kilka lat temu nawet nie myślano.

Oszuści spędzają sen z powiek nie tylko bankom. Branża turystyczna, w tym usługi hotelarskie, to obok sektora finansowo-bankowego, handlu i telekomunikacji ich główny cel. Hotelarze mogą podać liczne przykłady nieuczciwych zachowań w hotelach. W mediach opisano historię bezdomnego Davida Price'a, który przez dwa lata mieszkał na ulicy Orlando. Wpadł on jednak na oryginalny pomysł. Stwierdził, że mógłby mieszkać w... hotelach. Opracował sposób na podglądanie listy gości hotelowych i pilnował dat, kiedy ci opuszczają hotel. Obserwował, kiedy dana osoba się wyprowadza, by zająć jej miejsce. Jeśli udało mu się wejść do zwolnionego pokoju, dzwonił z hotelowego telefonu na recepcję i w imieniu poprzedniego gościa dokonywał przedłużenia pobytu. Wybierał prestiżowe hotele, toteż do niektórych jego ofiar po pewnym czasie zaczęły przychodzić rachunki na wiele tysięcy dolarów.

Price stosował proste zabiegi socjotechniczne, dzięki którym mógł mieszkać na koszt wymeldowanych i korzystać z zasobów na ich kartach. Goście hoteli, otrzymując informacje o zadłużeniu swoich kart, reklamowali zwiększone wydatki związane z ich fikcyjnym pobytem. Po ujawnieniu przestępstwa banki zwróciły pobrane niesłusznie środki. David Price przez wiele miesięcy skutecznie oszukiwał hotele, wybierając na cel ekskluzywne sieci, takie jak Ritz czy Hard Rock. Prawdopodobnie korzystał z faktu, że obsługa nie może być zbyt natarczywa i wścibska wobec bogatych gości. Jego proceder został przerwany – schwytano go i znalazł schronienie w więzieniu.

Zmorą hoteli są też osoby, które nie płacą za pobyt, stosując znane obsłudze środki i metody. Dla wielu mieszkanie na koszt hotelu stało się sposobem na życie. Narażeni na oszustwa są też klienci hotelu, np. kuszeni atrakcyjnymi ofertami oferowanymi w sieci w celu wyłudzenia przedpłat. Wiosną tego roku głośno było o nowym hotelu w Toruniu. Na Booking.com, popularnym serwisie do internetowej rezerwacji noclegów, konto założył Riess Palace, reklamujący się jako pierwszy pięciogwiazdkowy obiekt w mieście. Pod wskazanym adresem mieści się dawny pałac królewskiego poczmistrza Jakuba Teodora Riessa, który później służył jako placówka PZU. Ubezpieczyciel sprzedał go, a nowy właściciel rozpoczął remont. Zdjęcia na Booking.com prezentowały budynek z zewnątrz, a także wyposażenie pokoi: meble w starym stylu, gustowne tapety, porcelana dekorująca ściany. Właściciele hotelu zachwalali, że obsługa włada czterema językami. Pierwszych gości miał przyjąć 20 kwietnia. Najtańszy pokój dwuosobowy kosztował 549 zł, trzyosobowy – 722 zł. Szybko sprzedano rezerwację, pozostały tylko droższe apartamenty, od 1850 zł do 2200 zł za dobę. W kolejny piątek, 27 kwietnia, ceny spadły – za pokój życzono sobie od 400 zł.

Oferta ta okazała się oszustwem. Nowy właściciel nieruchomości budował w nim apartamenty, a nie hotel. Zdjęcia wnętrz pochodziły z oferty hotelu w Paryżu. Uważna analiza oferty mogła budzić zastrzeżenia. Telefon wskazany do kontaktu nie należał do bazy hotelu (dzwoniący dowiadywał się, że to pomyłka), w odróżnienia od innych hoteli trzeba było z góry zapłacić za cały pobyt.

Tu dotykamy kolejnego tematu, jakim są zabezpieczenia portali pośredniczących w oferowaniu rezerwacji w hotelach. Booking.com posiada profesjonalny zespół antyfraudowy. *Jako wiodąca firma e-commerce na Booking.com stale optymalizujemy silne środki bezpieczeństwa, które mają chronić klientów i partnerów* – podało biuro prasowe. – *Zgodnie z najwyższymi standardami technicznymi nasze zespoły ds. bezpieczeństwa i oszustw monitorują działalność 24 godziny na dobę przez siedem dni w tygodniu, wykorzystując indywidualne, najnowocześniejsze narzędzia do szybkiego wykrywania i rozwiązywania wszelkich potencjalnie podejrzanych aktywności. W tym rzadkim i szczególnym przypadku nieruchomość została usunięta z Booking.com, a wszyscy klienci, których dotyczy problem, przeniesieni do alternatywnej lokalizacji przez nasz zespół obsługi klienta.* Innymi słowy, nawet sprawny system nie zadziałał prewencyjnie wystarczająco wcześnie – kilku klientów zostało oszukanych. Nie wiadomo, czy organy ścigania złapały oszustów.

> Branża turystyczna, w tym usługi hotelarskie, to obok sektora finansowo-bankowego, handlu i telekomunikacji ich główny cel

Latem tego roku pojawił się nowy rodzaj oszustw. Tym razem to znane tureckie hotele w Bodrum, Fethiye i w regionie Antalyi padły ofiarą oszustów internetowych, którzy uruchomili strony internetowe do złudzenia przypominające oryginalne. Przestępcy stworzyli kopie serwisów wybranych, drogich obiektów i przyjmowali od turystów rezerwacje. Sprawa wyszła na jaw, kiedy jeden z klientów zadzwonił do hotelu Sianji w Bodrum, chcąc zamówić przejazd z lotniska. Wtedy okazało się, że nie ma on rezerwacji. Menedżer ds. marketingu hotelu zadzwonił pod numer telefonu podany na fałszywej stronie internetowej, który – jak się okazało – był zarejestrowany za granicą. Rozmówca zażądał 100 tys. bitcoinów za dezaktywację 50 stron opartych na nazwie obiektu.

Bezpieczny hotel

Kolejne oszustwa dotyczą konkursów organizowanych na portalach społecznościowych, oferujących w nagrodę pobyt w ekskluzywnych hotelach. W ostatnim czasie pojawiły się nowe formy naciągania. Jedna z nich polega na wysyłaniu e-maila z następującą informacją: *Dzięki swojej ostatniej aktywności na portalach podróżniczych zostałeś wytypowany do wzięcia udziału w Badaniu Preferencji Turystycznych. W zamian za poświęcony czas mamy dla Ciebie voucher na 3 noclegi dla 2 osób w wybranym przez Ciebie hotelu spośród naszej bazy niemal 1000 obiektów. Badanie Preferencji Turystycznych to kilkuminutowa anonimowa ankieta, której wyniki pozwolą polepszyć funkcjonowanie rynku turystyki indywidualnej i dostosować oferty do oczekiwań turystów. Możesz bezpośrednio przyczynić się do poprawy jakości usług turystycznych w Europie, w zamian za poświęcony czas oferujemy Ci voucher na darmowe noclegi.*

Ankieta jest tylko jednym z elementów mających uwiarygodnić pomysł wyłudzenia. W następnych etapach odbiorca takiej wiadomości albo zostaje zachęcony do wykupienia członkostwa w klubie, dzięki któremu może skorzystać z tysięcy atrakcyjnych lokalizacji w atrakcyjnej cenie, albo w innej wersji zachęca do wybrania hotelu, w którym może zamieszkać w dogodnym czasie pod warunkiem wykupienia voucherów obiadowych lub śniadaniowych (droższych niż doba w danym hotelu). Najmniejszy problem, jeśli będzie się to wiązać tylko z przepłaceniem za ofertę. Gorzej, jeśli na miejscu klient dowiaduje się, że o jego pobycie w danym hotelu nikt nic nie wie.

Lista oszustw, na które narażeni są i właściciele hoteli, i ich klienci, a pośrednio także banki obsługujące transakcje hotelowe, jest długa. Do niej można dopisać nieuczciwe firmy obsługujące hotele, fikcyjne lub nieuczciwe biura podróży czy pośredników kierujących do hoteli grupy, za które później nie płacą.

Jak się przed tym bronić?

Portale społecznościowe oraz świadczące usługi turystyczne czy pośredniczące w rezerwacji hoteli i sprzedaży usług hotelowych powinny stosować zaawansowane systemy antyfraudowe i działać prewencyjnie, weryfikując dane i oferty hoteli, zanim dopuszczą je do sprzedaży – bez tego mogą nie tylko ponieść stratę, ale także utracić reputację. Takie rozwiązania nie są tanie, ale minimalizują ryzyko oszukania ich klientów. Korzystając z Internetu do poszukiwania atrakcyjnych ofert, hoteli czy innych usług turystycznych, warto weryfikować informacje przed uregulowaniem należności. Dostawcy usług powinni współpracować z hotelami i wymieniać się informacjami o różnego rodzaju *modus operandi* stosowanymi przez oszustów. Niestety większość właścicieli sieci hotelowych i hoteli dotknęły konsekwencje wprowadzenia regulacji w zakresie ochrony danych osobowych. Jedynie sektor finansowy otrzymał zgodę na wymianę informacji o oszustach (art. 6 ust. 1 lit. *f* Ogólnego Rozporządzenia o Ochronie Danych Osobowych) i w swoich regulaminach przedstawianych do akceptacji przez klientów umieszcza klauzulę, że może przetwarzać dane gromadzone do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub stronę trzecią na podstawie wskazanego artykułu tego Rozporządzenia, za które administrator uznaje m.in. marketing bezpośredni, dochodzenie i obronę przed roszczeniami, zapobieganie oszustwom, prowadzenie statystyk i analiz, zapewnienie bezpieczeństwa środowiska teleinformatycznego, stosowanie systemów kontroli wewnętrznej. Mimo że nieformalnie hotele i sieci wymieniają między sobą ostrzeżenia o oszustach, to jednak brak regulacji w tym zakresie sprawia, że oszuści stają się coraz bardziej bezczelni, a koszty ponoszone przez hotele rosną.

Czy można legalnie, bez lęku bronić się przed oszustwami?

Jest to możliwe, ale wymaga sięgnięcia po pewne rozwiązania systemowe, których koszt szybko się zwraca. Słabym punktem oszusta jest to, że nie potrafi on zmienić swoich zachowań i przyzwyczajeń, a najbardziej zuchwały schemat oszustwa można rozpoznać. Weźmy np. proste oszustwo, jakich setki opisów można znaleźć w sieci. Oszust dokonuje rezerwacji w sieci, ale mając do wyboru wniesienie opłaty poprzez dokonanie preautoryzacji, przelewem z konta bankowego, usługi płatnicze lub transakcję kartą debetową lub kredytową, wybiera opcję przelewu z konta. Hotel, wiedząc, że oszust ma różne możliwości dokonania oszustwa (od przedstawienia sfałszowanego dowodu przelewu poprzez wskazanie, iż przelew wpłynie na konto hotelu w trakcie pobytu w hotelu), może założyć, że tylko potwierdzony przez bank dowód przelewu albo wpływ na konto jest podstawą do realizacji usługi. Oszuści, stosując metody socjotechniczne, manipulują obsługą w celu uzyskania tego, na czym im zależy. Mając tego świadomość, hotele powinny tworzyć profile predykcyjne takich zachowań i rozpoznawać te, które stwarzają ryzyko, że mają do czynienia nie ze zmęczonym klientem, ale z oszustem.

Hotel stosujący system rezerwacji korzysta z narzędzi udostępnionych przez operatorów pośredniczących w bukowaniu miejsc hotelowych, a ponadto monitoruje zachowania nie tylko pracowników, ale także gości np. w celu podniesienia jakości oferowanych usług. Każdy taki system monitorujący, każda informacja o tym, co klient robi, jakie usługi kupuje, co zamawia, pozwala również rozpoznać tych, którzy przygotowują się do oszustwa. Dzisiaj hotele stają się budynkami inteligentnymi, z dyskretnymi systemami zarządzania jakością usług i systemami generującymi leady pozwalające systemom rozpoznającym oszustwa na podjęcie działań uniemożliwiających skuteczne wyłudzenia. Taka inwestycja szybko się zwraca.

Z chwilą, gdy klient wkracza do hotelu, jego bezpieczeństwo jest chronione, monitorowane są również działania oszustów. Dzięki zastosowanym technologiom może uzyskać dostęp do wielu usług i możliwości, takich jak otwieranie pokoju własnym smartfonem, zamawianie usług z hotelowego tabletu, taksówki, dań z innych źródeł niż hotelowa restauracja, biletów do muzeów czy kin albo pomocy konsjerża, a nawet skorzystanie z pomocy recepcji także poza hotelem.

Dzisiaj klucz hotelowy to jednocześnie elektroniczna portmonetka, identyfikator umożliwiający dostęp do usług i miejsc dostępnych tylko dla klientów hotelu. We wszystkich drzwiach i przejściach stosowane są pętle indukcyjne pozwalające zlokalizować gościa i każdego pracownika hotelu. Dzięki tym i wielu innym rozwiązaniom ryzyko, iż hotel lub jego gość zostaną oszukani, a usługi i pieniądze wyłudzone, spada. Nie można też rezygnować ze szkoleń dla personelu, które są jedną z metod rozpoznawania oszustw i sposobów reagowania na nie.

Inwestowanie w bezpieczeństwo banków sprawia, że oszukanie instytucji finansowych, które stosują nowoczesne systemy zabezpieczeń, jest mało prawdopodobne. Jeśli jednak udaje się oszukać bank, wykorzystuje się do tego słabe punkty każdego systemu, jakim są ludzie. To człowiek – nieprzeszkolony, wprowadzony w błąd przez oszusta lub przez niego szantażowany – może sprawić, że oszustwo się powiedzie. Najlepsze systemy antyfraudowe są jednak na to przygotowane, jeśli jedną z metod rozpoznawania oszustwa są dobrze sprofilowane modele predykcyjne oparte na analizie behawioralnej. Stosując nawet w mniejszej skali proste systemy zabezpieczeń oraz znając *modus operandi* oszustów, średniej wielkości hotele, a także większe mogą z sukcesem chronić się przed oszustwami. Trudno byłoby uwierzyć, że są dzisiaj hotele, które nie broniłyby się przed oszustami – chociażby ukrytym na portierni skanerem sprawdzającym autentyczność banknotów i dokumentów tożsamości. To wydatek kilkuset złotych. Oszczędzanie na bezpieczeństwie jest proszeniem się o kłopoty i wystawianiem na poważne ryzyko.

W roku 2012 r. straty wynikające z oszustw dokonywanych w sektorze hotelarskim w Wielkiej Brytanii oszacowano na 2 mld funtów brytyjskich. W raporcie *The Resilience to Fraud of the UK Hotel Sector* przygotowanym przez firmę doradczą PKF i uniwersytet w Portsmouth m.in. wskazano, że kwota strat odpowiada 5,7 proc. łącznych przychodów branży, które wynoszą ok. 40 mld funtów brytyjskich rocznie. Według autorów raportu sektor hotelarski należy do najmniej odpornych na oszustwa. – *Oszustwa są poważnym problemem dla hoteli i mają wpływ nie tylko na kondycję branży, ale także na jakość i ceny usług, z których korzystają klienci. Zmniejszenie strat wynikających z oszustw jest jedną z najmniej bolesnych metod zminimalizowania wydatków firm w obecnej sytuacji gospodarczej, tym bardziej że koszty nadużyć finansowych – w odróżnieniu od wydatków związanych z personelem, towarami i wyposażeniem oraz obsługą nieruchomości – są niepotrzebne i bezproduktywne* – uważa Stuart Collins, National Hotel Partner w firmie PKF.

Można zakładać, że na naszym kształtującym się dopiero rynku, gdy większość obiektów nie ma jeszcze doświadczenia i odpowiednich procedur, odsetek strat spowodowanych oszustwami jest większy niż w Wielkiej Brytanii. Może to być 150–200 mln zł, gdyż hotele nie ujawniają wartości strat. Wydaje się, że nie jest to nawet kwota szacunkowa, ale raczej pokazująca rząd wielkości. Inwestycje w bezpieczeństwo i działania antyfraudowe, które zmniejszają straty nawet o 50–60%, są warte zainwestowania środków.

> Korzystając z Internetu do poszukiwania atrakcyjnych ofert, hoteli czy innych usług turystycznych, warto weryfikować informacje przed uregulowaniem należności

BIO

Michał Czuma
Niezależny ekspert, wcześniej wiceprezes i współwłaściciel G+C Kancelaria Doradców Biznesowych. Stworzył i zarządzał pierwszymi w kraju Biurami Antyfraudowymi w spółkach grupy PKO BP. Były wieloletni z-ca dyrektora Departamentu Bezpieczeństwa PKO BP.

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

Komfortowy i bezpieczny hotel

Dostęp do pokoju hotelowego za pomocą karty nie jest żadną nowością – wręcz przeciwnie, funkcjonuje to w praktycznie każdym hotelu. A zatem, czy oprócz tego, że elektroniczny klucz ma kompaktowe wymiary, możliwe są inne udogodnienia i funkcjonalności, wynikające z użytkowania takich kart?

Hotele, chcąc ze sobą konkurować, sięgają po coraz ciekawsze i nowocześniejsze rozwiązania. Jednym z nich jest zaawansowany system kontroli dostępu, dzięki któremu administratorzy zyskują jeszcze lepszą kontrolę nad tym, na jakich zasadach, kiedy i do jakich pomieszczeń udzielany jest dostęp konkretnym osobom – nie tylko gościom, ale także personelowi. Wszystko po to, aby goście czuli się w ich progach jak najlepiej, a personel pracował sprawniej i efektywniej. Zobaczmy, jak to działa w praktyce.

- Podczas meldunku recepcjonista nadaje gościom dostęp do pokoju oraz np. parkingu hotelowego. Każdemu z gości tego samego pokoju może wydać spersonalizowaną kartę. W efekcie np. wstęp do sali konferencyjnej może mieć tylko ta osoba, która jest uczestnikiem odbywającego się tam sympozjum.
- Po wejściu do windy z użyciem karty jej użytkownik będzie mógł wybrać jedynie przypisane do niej piętra. Oznacza to także koniec z „zabawami windą" urządzanymi przez najmłodszych gości.
- Otwarcie kartą drzwi do pokoju automatycznie uruchamia zasilanie. Po zmroku może także włączyć światło – nie trzeba szukać uchwytu na kartę.
- Wraz z zakończeniem pobytu karty gości „tracą ważność" i nie będą mogli oni wejść ponownie np. na basen.
- Przejścia ewakuacyjne, strefy techniczne czy pomieszczenia obsługi są chronione przed dostępem nieuprawnionych osób.
- Uprawnienia personelu mogą być nadawane/zmieniane w każdej chwili. Sprawdzi się to np. podczas codziennego przydzielania pokojówkom rejonu do sprzątania.

Wszystkie wymienione możliwości oferuje system ACCO NET firmy SATEL. Jego unikalną cechą jest możliwość integracji z systemami alarmowymi INTEGRA i INTEGRA Plus. Dzięki temu wybrani pracownicy mogą za pomocą jednej karty nie tylko uzyskiwać dostęp, ale także sterować czuwaniem SSWiN w zintegrowanej strefie. I tak np. kierownik może zamknąć biuro i jednocześnie włączyć system alarmowy. Funkcjonalność ta może być udostępniana także gościom, aby podczas ich nieobecności pokoje były dodatkowo strzeżone.

Atutem ACCO NET jest skalowalność, tj. możliwość obsługi nieograniczonej liczby central KD. Dzięki temu system może pracować w bardzo dużym obiekcie hotelowym, a nawet nadzorować całą ich sieć. Także w przypadku rozbudowy istniejącej struktury, np. o nowe skrzydło, można je szybko objąć nadzorem systemu kontroli dostępu.
Wygodną obsługę systemu ACCO NET zapewnia aplikacja internetowa ACCO Web, do której dostęp można uzyskać z dowolnego miejsca na świecie. Kilku operatorów jednocześnie może mieć szybki i wygodny wgląd w stan obiektów oraz przełączać się między nimi, jak również pomiędzy pojedynczymi strefami systemu.
Każdy z budynków może mieć przypisaną mapę, z której poziomu dostępna jest zdalna obsługa pojedynczych przejść i podgląd obrazu z kamer IP. ACCO Web umożliwia nie tylko dodawanie użytkowników oraz nadawanie i zmienianie ich uprawnień, dopasowując do potrzeb organizacji. Aplikacja udostępnia także tworzenie raportów dotyczących obecności, m.in. ze zliczaniem czasu pobytu gości lub pracy obsługi, monitorowaniem lokalizacji użytkowników i weryfikacji ścieżek, którymi się przemieszczali – dzięki temu można szybko sprawdzić np. kto, kiedy i jak długo sprzątał dany pokój.

Bezpieczny hotel

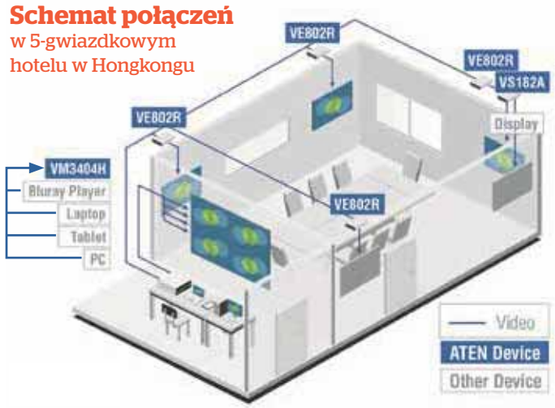
ATEN Poland Sp. z o.o.
ul. Gottlieba Daimlera 2
02-460 Warszawa
www.aten.com/pl/pl

Idealna wielofunkcyjna sala konferencyjna hotelu

Hotele, oprócz funkcji noclegowej, oferują również powierzchnię udostępnianą na spotkania, prezentacje i różnego rodzaju imprezy. **Ważnym elementem przestrzeni hotelowych są sale konferencyjne. Podstawę ich nowoczesnego wyposażenia stanowi niezawodny sprzęt audio-wideo.**

Firma ATEN podjęła się wyzwania, by w 5-gwiazdkowym hotelu w Hongkongu zaaranżować wielofunkcyjną przestrzeń konferencyjną przeznaczoną do użytku przez gości z całego świata. Wyposażenie sali miało się wpisywać w elegancki wizerunek hotelu, dlatego instalacja audio-wideo musiała być minimalistyczna, a zarazem wyrafinowana. Pomieszczenie o wymiarach 22 x 12 m wyposażono w pięć monitorów HDMI, które służą zarówno do wyświetlania treści promocyjnych hotelu w jakości 4K, jak i materiałów z urządzeń klientów, np. komputerów osobistych, laptopów, czy tabletów z systemem Android oraz iPadów. W małym pomieszczeniu obok sali konferencyjnej ulokowano stację roboczą wyposażoną w cztery monitory HDMI, skąd również można sterować treściami wyświetlanymi w sali konferencyjnej.

Schemat połączeń
w 5-gwiazdkowym hotelu w Hongkongu



Wyzwaniem tego projektu było zapewnienie szybkiego, a zarazem stabilnego przełączania między dwoma (maks. czterema) źródłami sygnałów HDMI w rozdzielczości 4K. Kolejne wymaganie dotyczyło możliwości przesyłania sygnałów audio-wideo i sterowania pilotem podczerwieni maks. 9 monitorami HDMI jednocześnie, na odległość 40 m. Wszystko musiało być dostosowane do eleganckiego wystroju sali, zatem należało zastosować minimalną liczbę zasilaczy i dodatkowego okablowania oraz maksymalnie wyeliminować wszelkie zakłócenia.
Firma ATEN opracowała idealne rozwiązanie w postaci matrycy (krosownicy wizyjnej) VM3404H HDMI HDBaseT, odbiornika z zasilaniem POH VE802R HDMI HDBaseT oraz splittera (dzielnika sygnału) VS182A z dwoma portami HDMI 4K.
Urządzenia VM3404H i VE802R firmy ATEN zapewniły idealną transmisję obrazu w formacie UHD 4K poprzez HDBaseT. Krosownica VM3404H, dzięki funkcji sterowania na podczerwień, ma również możliwość zdalnego przełączania z dowolnego miejsca. Zarówno VM3404H, jak i VE802R pozwalają zminimalizować niezbędne okablowanie oraz wyeliminować konieczność stosowania dodatkowych połączeń. Obraz o rozdzielczości 4K może być przesyłany bez żadnych zakłóceń na odległość 40 m od VM3404H za pomocą pojedynczego kabla Cat 6a.
Sala konferencyjna w hotelu w Hongkongu – stylowa i elegancka – cieszy się opinią niezawodnie funkcjonującego miejsca spotkań klientów i pracowników hotelu.

RAJ International Sp. z o.o.
ul. Wał Miedzeszyński 552 B,
03-994 Warszawa, tel. 22 679 92 11
raj-biuro@raj-international.net

CASE STUDY

Stylowy i bezpieczny hotel na Stalowej

ARTHOTEL STALOWA 52 to wyjątkowy, butikowy hotel, który mieści się w zrewitalizowanej kamienicy na warszawskiej Pradze. Oryginalny charakter miejsca podkreślają wyeksponowana czerwona cegła i industrialna zabudowa patio. Hotel działa od 2012 r. i może pochwalić się standardem trzech gwiazdek.

W kamienicy znajduje się 19 przestronnych i oryginalnie wyposażonych pokoi. Część z nich ma nowoczesny, loftowy charakter, część została zaprojektowana w klasycznym stylu. Hotel dysponuje również salami konferencyjnymi na 80 osób, do dyspozycji gości jest też restauracja.

Zadbano o odpowiednie zabezpieczenie obiektu. W budynku działa system telewizji dozorowej, który monitoruje teren zewnętrzny, parking hotelowy i części wspólne kamienicy. System alarmowy jest podłączony do stacji monitorowania alarmów, agencja ochrony sprawuje nadzór nad obiektem przez całą dobę. Do zabezpieczenia ppoż. wybrano system sygnalizacji pożarowej Schrack Seconet, złożony z centrali Integral IP BXF, czujek CUBUS MTD533X (ponad 80 szt.) oraz ręcznych ostrzegawczy pożarowych MCP 545X (17 szt.). Do systemu podłączono sygnalizatory akustyczne SAK-5N firmy W2, zasilane i sterowane z wyjść przekaźnikowych centrali. Systemem oddymiania grawitacyjnego z kompensacją powietrza poprzez wentylator mechaniczny steruje centrala Mercor 9705. Ręczne przyciski oddymiania zainstalowano na klatce schodowej, natomiast klapa oddymiająca została ulokowana na dachu budynku.

Wszystkie algorytmy sterowania systemem oddymiania są realizowane przez centralę Integral IP BXF.

Instalację systemów ppoż. i oddymiania w hotelu wykonała firma Raj International. – *Spółka zarządzająca obiektem zdecydowała się na współpracę z Raj International ze względu na doświadczenie w pracach prowadzonych w obiektach zabytkowych, w których z dużą dbałością należy podejść do robót instalacyjnych. Właścicielom hotelu zależało na tym, aby wszystkie systemy i instalacje urządzeń wpisały się w industrialny klimat kamienicy budynku* – mówi Magdalena Walenczak-Allain, współwłaścicielka hotelu.

Aby zaprojektować odpowiednio dopasowany system sygnalizacji pożarowej, musieliśmy zacząć od zapoznania się ze specyfiką aranżacji wnętrz. Największym wyzwaniem okazało się wkomponowanie okablowania oraz elementów pętlowych, np. czujek dymu, ręcznych ostrzegaczy pożarowych i sygnalizatorów akustycznych, w wystrój poszczególnych pokoi, aby nie zakłócić wizji architekta – wyjaśnia Rafał Rusiecki, wiceprezes Zarządu, dyrektor generalny Raj International. – *Nie było to zadanie łatwe, ponieważ każdy pokój zaprojektowano w innym stylu, należało więc za każdym razem dopasowywać usytuowanie poszczególnych urządzeń do charakteru pomieszczenia.*

Ze względu na stropy, które zostały zabezpieczone płytami ognioodpornymi, nie było możliwości wykonania instalacji techniką podtynkową, trzeba było zastosować technikę natynkową. Przewody do elementów pętlowych ułożono w czarnych rurkach, przewody ognioodporne natomiast bezpośrednio na atestowanych uchwytach na stropie i ścianach. Dzięki temu idealnie pasują do charakteru kamienicy.

– *Goście Arthotelu Stalowa 52 doceniają klimat i oryginalną aranżację wnętrz, a instalacje świetnie pasują do industrialnej zabudowy. Często słyszymy opinie, że tak ułożone przewody dodają pomieszczeniom charakteru* – zauważa Magdalena Walenczak-Allain.

Firma Raj International wykonała w obiekcie również instalację hydrantową oraz kompensacji powietrza dla systemu oddymiania grawitacyjnego.

Głos branży

Hotel jest obiektem specyficznym i skomplikowanym. Zarządzający nim muszą zadbać o bezpieczeństwo zarówno gości, jak i pracowników, nie bagatelizując przy tym ochrony mienia. **Jak do kwestii zabezpieczeń hoteli podchodzą przedstawiciele branży security?**

Wojciech Pawlica
Product Manager,
Dahua Technology Poland

Rozwiązania wspierające bezpieczeństwo w hotelu

Od wielu lat systematycznie rośnie liczba osób korzystających z usług hotelowych. Aby przyciągnąć gości, właściciele muszą zadbać o wysoki poziom bezpieczeństwa w obiekcie. Jednym z podstawowych wymogów jest wyposażenie obiektu w systemy ochrony przeciwpożarowej i kontroli dostępu do pokoi.

Uzupełnieniem są systemy telewizji dozorowej IP coraz powszechniej stosowane w przestrzeni ogólnodostępnej. Bardzo często kamery są instalowane w sposób dyskretny (np. w czujkach dymu, włamania), by nie zakłócać komfortu gości.
Możliwość rejestracji obrazu z kamer, jak również wykorzystanie zaawansowanych metod analizy obrazu (np. rozpoznawania twarzy czy numerów tablic rejestracyjnych), zdecydowanie poprawia jakość usług hotelowych, a tym samym komfort gości.

Kolejnym proponowanym przez Dahua Technology rozwiązaniem zwiększającym bezpieczeństwo hotelu jest system kontroli dostępu. Zastosowany w newralgicznych pomieszczeniach hotelu, takich jak serwerownia, recepcja czy sejf, nie tylko chroni dobro gości, ale również poprawia komfort bezpieczeństwa osób tam pracujących.
W ofercie mamy kompletne rozwiązanie do kontroli dostępu – od różnego rodzaju czytników (klawiatura, karty RFID, czytniki biometryczne), poprzez kontrolery 2- i 4-drzwiowe w różnych wersjach (montowane w samodzielnych skrzynkach lub np. w rozdzielniach na szynie DIN), aż po elektroniczne zamki i zwory elektromagnetyczne.
Zapewnienie odpowiedniego poziomu bezpieczeństwa obiektów hotelowych należy rozpatrywać na wielu płaszczyznach. To nie tylko kontrola dostępu do pokoi, ochrona przed włamaniem, pożarem czy zalaniem. To również dbanie o wysoki poziom dyskrecji, zwłaszcza teraz, kiedy obowiązują przepisy RODO.

Własne „oko” w pokoju hotelowym

Jak dużo kamer zainstalowano w hotelu i jak precyzyjnie nas śledzą, przekonał się osobiście w 2007 r. ówczesny szef MSWiA Janusz Kaczmarek. Każdy jego ruch można było prześledzić właśnie dzięki zainstalowanym w hotelu kamerom. Jako że sprawa była w tamtym czasie bardzo medialna, każdy mógł zobaczyć, jak takie zapisy z kamer wyglądają w praktyce.
Kamery w hotelach są teoretycznie po to, aby zapewnić gościom bezpieczeństwo. Jednak nigdy nie możemy mieć pewności, że działają właściwie. Niestety zdarza się również, że liczba kamer jest niewystarczająca lub po prostu ich nie ma.

Czy w hotelach często dochodzi do przywłaszczenia mienia? Z pewnością tak. Również mnie się to przytrafiło. Padłem ofiarą kradzieży, której sprawcą byli prawdopodobnie pracownicy hotelu. Z sali konferencyjnej, do której dostęp miał jedynie personel, przez noc zniknęły przedmioty przeznaczone dla uczestników jednego z moich szkoleń.
Oczywiście w takim przypadku pracownicy hotelu w żaden sposób nie starali się pomóc w ustaleniu, kto był sprawcą… Do podobnego zdarzenia może dojść w pokoju hotelowym. Choć zazwyczaj do dyspozycji gości jest sejf, to nie jest on pewnym zabezpieczeniem, choćby dlatego, że na czarnym rynku można zdobyć klucze uniwersalne do takich sejfów. Poza tym rozmiar sejfu często nie pozwala na schowanie elektroniki, aparatury fotograficznej i innych urządzeń, które niejednokrotnie mają większą wartość niż gotówka, jaką zabieramy w podróż.
O swoje bezpieczeństwo najlepiej zadbać samemu, tym bardziej że jest to możliwe. Jak to zrobić?
W pokoju hotelowym można zostawić kamerę wyposażoną w kartę SIM i zasilaną power bankiem. Dzięki temu zyskujemy niezależność od hotelowego Internetu i zasilania, które często jest odcinane po wyjściu z pokoju. Obraz z takiej kamery w czasie rzeczywistym powinien być zarejestrowany w chmurze. Wówczas, nawet gdy ktoś wyniesie kamerę, nagrań już nie uda się ukraść. Obraz zarówno na żywo, jak i zarejestrowany jest dostępny w każdej chwili, np. na ekranie telefonu.
W podróży nie można tracić głowy, a dla własnego bezpieczeństwa zawsze warto zostawić „oko” w pokoju hotelowym.

Jakub Sobek
certyfikowany trener techniczny, Linc Polska

Komfort i bezpieczeństwo

Andrzej Krasowski
Hikvision

Któż z nas chociaż raz prywatnie lub służbowo nie musiał zatrzymać się w hotelu? Dla większości na wybór spośród olbrzymiej liczby ofert wpływa nie tylko dogodna lokalizacja hotelu i komfort, ale także w coraz większym stopniu bezpieczeństwo. Nie jest to wyłącznie oczekiwanie jednej strony, gdyż hotele same dokładają starań, aby zapewnić gościom maksimum komfortu i bezpieczeństwa, jednocześnie dbając o zachowanie prywatności.

Ich właściciele starają się chronić zarówno obiekt, jak i znajdujące się na jego terenie mienie przed aktami wandalizmu czy zamierzonego i celowego przywłaszczenia, czyli kradzieżami. Przede wszystkim jednak dbają o bezpośrednie bezpieczeństwo przebywających w obiekcie osób.

Wyposażenie hotelu w odpowiedni system telewizji dozorowej pozwala zrealizować wiele tego rodzaju potrzeb. Ponieważ większość hoteli pracuje w trybie 24/7, system powinien być przystosowany do pracy ciągłej. Dobór urządzeń (kamery, rejestratory) i funkcjonalność systemu powinny być zaprojektowane na podstawie analizy zagrożeń, aby optymalnie dozorować istotne części obiektu.

Zaawansowana analiza obrazu (VCA) dostępna w kamerach wspomaga pracę ochrony, działając w sposób automatyczny i zaprogramowany na ustawione zdarzenia, alarmując personel w momencie ich zajścia. Mając do dyspozycji takie narzędzia, obsługa hotelu jest w stanie szybko i z zaangażowaniem reagować w sytuacjach wymagających szybkiej interwencji.

Kamery zapewniają nie tylko bezpieczeństwo, ale także poprawiają komfort pobytu gości. Zastosowanie kamer z funkcjami rozpoznawania numerów tablic rejestracyjnych (LPR) umożliwi wjazd auta na parking bez konieczności pojawienia się przed recepcją i zgłoszenia potrzeby rezerwacji miejsca parkingowego. Wystarczy w momencie rezerwacji hotelu podać numer tablicy rejestracyjnej swojego pojazdu. Taka funkcjonalność ułatwia gościom korzystanie z parkingu w trakcie całego pobytu.

Ważny jest również czas i komfort obsługi. Z pomocą przychodzą kamery z funkcjami liczenia osób i czasu ich przebywania w wyznaczonych strefach. Wspomogą w dyskretny sposób pracę recepcji lub restauracji w sytuacji, gdy liczba osób oczekujących, a tym samym czas obsługi ulegają wydłużeniu. System CCTV automatycznie powiadamia personel o konieczności pojawienia się dodatkowego pracownika do obsługi gości.

Firma HIKVISION już dzisiaj dysponuje tego rodzaju rozwiązaniami, oferując szeroką gamę kamer i urządzeń końcowych, a także pomoc w ich doborze i podczas użytkowania. Bez zbędnego zwiększania nakładów inwestycyjnych hotele mogą korzystać ze współczesnych rozwiązań podnoszących komfort i bezpieczeństwo w swoich obiektach, jednocześnie ułatwiając i uatrakcyjniając gościom pobyt.

Bezpieczny i dyskretny hotel

Michał Kozak
dyrektor generalny hotelu Arłamów

Czterogwiazdkowy hotel Arłamów to obiekt wyjątkowy. Rzadko zdarza się bowiem, aby w jednym miejscu skupić tak wiele różnych możliwości, w tym centrum sportowe oferujące aż 33 dyscypliny sportowe (z pełnowymiarowym stadionem piłkarskim z naturalną murawą), bazę konferencyjno-eventową z zapleczem gastronomicznym, spa, miejsca noclegowe, własne lądowisko i heliport, stoki narciarskie. Całość wymaga zastosowania najnowocześniejszych rozwiązań techniki ochronnej, przy zachowaniu najwyższego poziomu bezpieczeństwa dla gości i pracowników hotelu.

Zróżnicowanie potrzeb, mnogość atrakcji i przepisy stanowiły ogromne wyzwania. Jednocześnie należało zachować dyskrecję, aby goście czuli się nie tylko bezpiecznie, ale także swobodnie. Nie bez znaczenia jest również lokalizacja hotelu, główny atut, który jednak zobowiązuje.

W tym celu od początku funkcjonowania obiektu został utworzony odrębny dział, który zajmuje się *stricte* ochroną i bezpieczeństwem. Własny system ratownictwa medycznego okazał się strzałem w dziesiątkę! Codziennie prowadzimy wnikliwe analizy każdej imprezy – zarówno dla gości konferencyjnych, jak i indywidualnych. Pełny przegląd sytuacyjny umożliwia nowoczesny system monitoringu wizyjnego, który niejednokrotnie już spełnił swoją funkcję. System sygnalizacji pożarowej, systemy oddymiania i detekcji tlenku węgla, rozbudowany system kontroli dostępu oraz system sygnalizacji włamania i napadu to rozwiązania techniczne, z jakich korzystamy na co dzień.

Jednak nawet przy najbardziej zaawansowanej technice nie wolno zapominać, że najważniejszym ogniwem jest czynnik ludzki. Pamiętamy, że ostateczne decyzje podejmuje człowiek, dlatego stale zwiększamy kompetencje personelu w radzeniu sobie w sytuacjach kryzysowych.

Obiekty hotelarskie wymagają specjalnych rozwiązań. Krajobraz bezpieczeństwa stale ulega zmianom, dlatego jednym z najistotniejszych zadań jest świadome zarządzanie i precyzyjne integrowanie systemów zabezpieczeń, aby w trudnych sytuacjach gwarantowały najwyższy poziom bezpieczeństwa.

Należy jednak pamiętać, że to wszystko musi się dziać przy równoczesnym zachowaniu pełnej wygody i swobody gości. Dyskretnie...

Informowanie o pożarze – rozwiązania specjalne

Krzysztof Kunecki
dyrektor ds. technicznych, Schrack Seconet Polska

Wczesne wykrycie pożaru i szybkie powiadomienie o nim personelu służb ochrony hotelu (tak jak każdego innego obiektu budowlanego) to kluczowe funkcje systemu sygnalizacji pożarowej. Obsługa poinformowana o alarmie może go szybko zweryfikować i potwierdzić poprzez wciśnięcie najbliższego ręcznego alarmu pożarowego, co skutkuje natychmiastowym uruchomieniem urządzeń odpowiedzialnych za powiadomienie straży pożarnej i zaalarmowanie osób przebywających w obiekcie.

Podstawowym urządzeniem przeznaczonym do sygnalizacji i obsługi alarmu pożarowego jest centrala sygnalizacji pożarowej (CSP). Ponadto stosuje się wyniesione panele obsługi instalowane w pomieszczeniu ochrony lub w miejscu przebywania personelu obiektu, czyli np. w recepcji hotelu.

W szczególnych przypadkach personel służb ochrony może przebywać poza pomieszczeniem ochrony lub nie mieć dostępu do panelu wyniesionego. Wówczas w celu poinformowania o alarmie pożarowym, uszkodzeniu lub innym stanie zagrożenia mogą zostać wykorzystane specjalne rozwiązania do informowania bezprzewodowego.

Funkcję tę może zrealizować znajdująca się w ofercie firmy Schrack Seconet specjalna aplikacja Integral Mobile, instalowana na urządzeniach mobilnych, takich jak smartfon lub tablet. Aplikacja ma spójny z panelem obsługi centrali interfejs użytkownika i pozwala na szybkie przedstawienie informacji o zagrożeniu.

W momencie wystąpienia alarmu pożarowego lub uszkodzenia w instalacji sygnalizacji pożarowej wiadomość zawierająca adres logiczny i informację o lokalizacji elementu trafia na telefon komórkowy personelu ochrony za pośrednictwem sieci telefonii komórkowej lub sieci Wi-Fi.

Dzięki zastosowanej funkcji powiadamiania (*push notification*) aplikacja przekazuje informację o zdarzeniu w postaci tekstu i odpowiedniego sygnału dźwiękowego, co zapewnia natychmiastową reakcję użytkownika urządzenia.

Pełna funkcjonalność aplikacji jest dostępna po dodatkowej autoryzacji za pomocą hasła lub po weryfikacji odcisku palca i pozwala na sprawdzenie dokładnego stanu pracy systemu (prezentowane informacje pokrywają się z informacjami na panelu obsługi CSP).

Ponadto aplikacja umożliwia odczytanie historii zdarzeń i dokładne przeanalizowanie całego przebiegu zdarzenia. Dodatkowo bezpieczny dostęp do aplikacji zapewniają również zdefiniowane koordynaty GPS, które pozwalają na jej użytkowanie tylko w przypadku obecności operatora w konkretnej lokalizacji (w tym przypadku hotelu). Z tego narzędzia mogą z powodzeniem korzystać osoby zarządzające hotelem w celu szybkiego informowania o zagrożeniach lub zdalnej kontroli stanu instalacji sygnalizacji pożarowej – zapewnione są większe bezpieczeństwo oraz komfort użytkownika instalacji sygnalizacji pożarowej.

Należy jednocześnie pamiętać, że opisane rozwiązanie służy do informowania i stosowane jest jako uzupełnienie podstawowych urządzeń, takich jak np. panel obsługi centrali sygnalizacji pożarowej.

Poczucie bezpieczeństwa i zadowolenie gości

Bogumił Szymanek
Axis Communications

Prowadząc hotel lub restaurację, odpowiadasz za bezpieczeństwo swoich gości i pracowników. Ponadto zależy ci na tym, aby goście czuli się swobodnie w dobrej atmosferze panującej w obiekcie, bo jest szansa, że polubią miejsce, będą powracać i zachęcać innych. Oprócz klasycznego zabezpieczenia za pomocą niezawodnego systemu telewizji dozorowej jedną z ważniejszych cech oferowanych rozwiązań jest możliwość prowadzenia dyskretnego dozoru, a zarazem zapewnienia prywatności gościom. Kluczowe są również kwestie cyberbezpieczeństwa, którym należy nadać najwyższy priorytet.
Z kolei otwartość integracyjna różnych urządzeń sprawia, że możliwe jest wykorzystanie danych z analizy wizyjnej i innych systemów do optymalizacji funkcjonowania obiektu i przygotowania lepszej oferty dla klientów.
Urządzenia instalowane w hotelu lub restauracji, dzięki estetycznym obudowom czy nawet możliwości ich malowania, można również dobrać do wystroju wnętrza. Na tym jednak nie kończą się możliwości zwiększenia satysfakcji gości. Liczy się również miła atmosfera. W jaki sposób zapewnić odpowiedni nastrój w hotelu, stosując nowoczesne technologie? Odpowiedź Axis jest prosta – sieciowe systemy audio nadają się idealnie do tego celu. Łatwe w instalacji urządzenia audio pozwalają na elastyczne planowanie emisji muzyki w tle. Dzięki możliwości tworzenia playlist, harmonogramów odtwarzania i różnych stref z łatwością dopasujemy muzykę do klimatu lobby, restauracji, spa, siłowni czy nawet pory dnia.
Systemy audio wspierają również strumieniowanie materiału z serwisów muzycznych online, co uatrakcyjnia ofertę i zwiększa poziom zadowolenia gości. Co więcej, systemy audio stają się pomocne w optymalizacji pracy, np. w razie potrzeby automatycznie przywołując pracownika obsługi.

Bezpieczeństwo klientów i danych w bankowości

Marcin Morzyk
BCS

Banki starają się przenosić większość swoich usług do świata cyfrowego. Wiąże się to m.in. z koniecznością jak najlepszego zabezpieczenia danych oraz połączeń pomiędzy użytkownikiem a serwerami. Na bezpieczeństwo danych wydaje się nieporównywalnie większe kwoty niż na inne systemy związane z bezpiecznym funkcjonowaniem każdej placówki banku. To praktyka jak najbardziej uzasadniona, jednak warto pamiętać o fizycznym (technicznym) zabezpieczeniu obiektów bankowych, w których jeszcze cały czas jest gotówka.
Stosując systemy telewizji dozorowej z inteligentnymi funkcjami analizy obrazu zawartymi w kamerach lub oprogramowaniu, zabezpieczymy newralgiczne miejsca placówki. Obecne w wybranych modelach kamer funkcje zliczające osoby lub analizujące liczbę osób w strefie idealnie sprawdzą się, gdy zostaną zainstalowane nad wejściem. Odpowiednia konfiguracja parametrów poinformuje obsługę banku o liczbie osób oczekujących w kolejce, jak również zaalarmuje ochronę o podejrzanym zachowaniu lub gromadzeniu się ludzi w strefie, gdzie nie powinna przebywać więcej niż jedna osoba. Również kamery montowane na zewnątrz mogą sygnalizować o zbyt długim przebywaniu lub pojawieniu się w strefie pojazdu, przekroczeniu wirtualnej bariery w wyznaczonym kierunku itp. zachowaniach.
Obecnie systemy monitoringu oferują również algorytmy do rozpoznawania twarzy i porównywania jej z zapisem w bazie danych. Tego typu funkcjonalność idealnie sprawdza się w kontroli dostępu do miejsc szczególnie chronionych, gdy do strefy może wejść osoba dopiero po podwójnej weryfikacji, np. standardową kartą i poprawną weryfikacją twarzy. Takie algorytmy można również łatwo zastosować do zapisywania metadanych twarzy i w późniejszym czasie do wyszukania konkretnej osoby na obrazie. Pojawia się tu jednak aspekt prawny związany z ochroną zebranych danych w świetle ustawy RODO.
Warto również zadbać o to, aby wszystkie informacje zostały przekazane z odpowiednim priorytetem, wówczas reakcja na alarm będzie szybka i adekwatna do zaistniałej sytuacji.

Prawdziwy koszt bezpieczeństwa

Współpracując z odbiorcami systemów zabezpieczeń, zwłaszcza w sektorze B2B, **spotykamy się coraz częściej z koniecznością ograniczania kosztów ponoszonych na bezpieczeństwo.**

Hubert Żak
Consulting for AccorHotels

Czy taki sposób kształtowania polityki kosztowej firm w zakresie safety i security jest zasadny? Koncentrowanie działań na ograniczaniu kosztów zakupu i utrzymania przekłada się wprost na niską jakość i małą efektywność zainstalowanych systemów. Jako jedni z największych na świecie dostawców usług hotelowych testujemy i implementujemy większość dostępnych na rynku rozwiązań z obszaru zabezpieczeń technicznych (elektronicznych i mechanicznych), jak również analizy operacyjnej (np. dane pozyskane za pomocą *beacon*). Istotą zrównoważenia jest wdrożenie rozwiązań o optymalnej efektywności i atrakcyjnych ekonomicznie, jednocześnie obniżających koszty i maksymalizujących zyski. Systemy monitoringu wizyjnego to w znakomitej części czynnik ludzki skupiający uwagę na zdarzeniach zagrażających bezpieczeństwu. W przedmiotowym obszarze pomocna staje się analityka zdarzeń i obrazu umożliwiająca pozyskiwanie danych w spektrum detekcji, np. zliczanie osób, analizę większych skupisk osób w obszarach ogólnodostępnych. Wykorzystanie zebranych informacji wpływa na poprawę jakości usług. Analogicznie w sposób operacyjny można przekierować pracowników w czasie ich nieaktywności do wykonywania innych czynności w obszarach o charakterystyce dynamicznej.

Z kolei zastosowanie systemów rejestracji czasu pracy, czasu aktywności, mapowania obiektów pozwoli unikać niezgodności w ewidencji oraz zakresie czasu pracy. Połączenie technologii *beacon*, RFID itp. z systemami monitoringu wizyjnego i kontroli dostępu pozwala na zmaksymalizowanie zarządzania pracownikami firm *outsourcingowych* i podwykonawczych, umożliwiając w efekcie amortyzację części systemów poprzez odpowiednie wykorzystanie zasobów.

Przykładem właściwego zastosowania rozwiązań wielopoziomowych jest np. kontrola zakresu pracy serwisów i dostawców usług. Odpowiednio zbudowane systemy (nie cena, a efektywność powinna być ich kluczowym elementem) przyniosą w trakcie długotrwałej eksploatacji wymierne korzyści:

- ograniczenie liczby roszczeń wynikające z zarządzania ryzykiem,
- profity w zakresie ubezpieczeń,
- optymalizacja pracy personelu i firm zewnętrznych,
- zmniejszenie kosztów eksploatacji, pracy urządzeń z obszaru BMS,PMS itd. (ogrzewanie, klimatyzacja, oświetlenie), i urządzeń elektrycznych, kurtyn powietrznych, dźwigów,
- poprawa wizerunkowa firmy: reklama, lokowanie produktu i usług poprzez efektywne wykorzystanie systemów,
- efektywniejsza sprzedaż miejsc parkingowych,
- zmiana dynamiki pracy na podstawie cyklicznej analizy okresów miesięcznych, rocznych (np. martwy sezon),
- analiza w zakresie użytkowania i dostępności, np. automatów sprzedażowych (*vending machine*), kiosków multimedialnych itd.,
- sprzedaż powierzchni itp.

Pytania powstające w procesie budowy spektrum użyteczności systemów sprowadzające się do twierdzenia *due for money* (jakość a cena) przy odpowiednim profilowaniu znajdują odpowiedzi we właściwym i umiejętnym ich zastosowaniu.

Korzyści płynące z analizy danych z różnych systemów zabezpieczeń elektronicznych przekładają się na wymierne zyski. Zapewnienie bezpieczeństwa staje się nieodzowne i ekonomicznie uzasadnione. Należy zmienić podejście do kwestii stosowania techniki w obszarze bezpieczeństwa. Powinna ona stanowić stały, niezbędny koszt zapewnienia bezpieczeństwa firmy.

BIO

Hubert Żak
Ekspert ds. bezpieczeństwa i techniki zabezpieczeń, menedżer projektów. Wieloletni pracownik służb, od kilkunastu lat związany z bezpieczeństwem biznesu. Zrealizował wiele innowacyjnych projektów ochrony fizycznej i zabezpieczeń technicznych. Szczególnie interesuje go zarządzanie kryzysowe, prewencja, zapobieganie zagrożeniom i bezpieczeństwo publiczne. Obecnie związany z AccorHotels, gdzie odpowiada za nowe rozwiązania w systemach bezpieczeństwa w obiektach hotelowych oraz specjalistyczne szkolenia.

Rola systemów sygnalizacji pożarowej w świecie obiektów hotelowych

Zapewnienie wczesnego wykrycia pożaru, przeprowadzenie bezpiecznej ewakuacji i zminimalizowanie liczby fałszywych alarmów w hotelach to podstawowe wyzwania, jakie stoją przed projektantami systemu sygnalizacji pożarowej. Właściwie wykonana integracja systemu z systemami zewnętrznymi odgrywa istotną rolę w prawidłowym funkcjonowaniu obiektu. Przed podjęciem decyzji o wyborze rozwiązania warto zweryfikować elementy mające wpływ na jego działanie, cenę i koszty eksploatacji.

Monika Kołodziejczyk

Pojęcie obiektów hotelowych jest szerokie – zalicza się do nich m.in. hotele, motele i pensjonaty. Ich główną rolą jest świadczenie usług noclegowych i wielu innych związanych z pobytem turystów. Goście, wybierając obiekt hotelowy po raz pierwszy, kierują się jego wyglądem, standardem wyposażenia i zakresem świadczonych usług. Obsługa hotelu dba zarówno o ich jakość, jak i komfort oraz bezpieczeństwo gości. Chodzi o zapobieganie kradzieżom, dyskrecję powiązaną z ochroną danych osobowych, bezpieczeństwo działania urządzeń technicznych, w tym systemów ochrony przeciwpożarowej. Gdy pobyt zostanie zakłócony niepożądanymi zdarzeniami, klient będzie oceniał hotel przez pryzmat właśnie tych zdarzeń. Ważne jest zatem, aby obiekt hotelowy był nie tylko przyjazny i funkcjonalny, ale też spełniał wszystkie wymogi prawne dotyczące m.in. bezpieczeństwa pożarowego. Bez względu na to, czy powstał na bazie obiektu zabytkowego, czy jest przykładem nowoczesnej architektury, wymaga zastosowania odpowiednich systemów, które będą nie tylko efektywnie informować o pożarze, ale także wyglądem nie zaburzą architektury i wnętrza budynku. Najważniejszym aspektem jest jednak skuteczność sygnalizowania o pożarze.

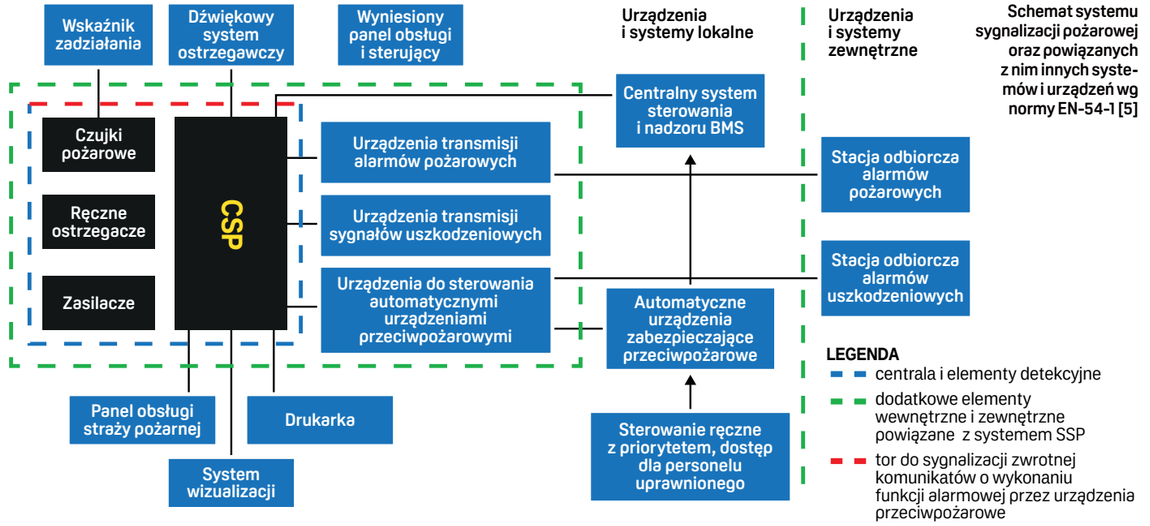
Czym się kierować przy wyborze systemu sygnalizacji pożarowej w hotelu? Jakie elementy powinny się w nim znaleźć?

Sercem systemu jest centrala sygnalizacji pożarowej (CSP) , która zbiera informacje z elementów detekcyjnych o stanie nadzorowanego obiektu, a także sygnalizuje zagrożenia pożarem i wystąpienia awarii (*rys.*). W zależności od scenariusza pożarowego przekazuje informacje do wielu powiązanych systemów, takich jak dźwiękowe systemy ostrzegawcze (DSO), systemy wentylacji, oddymiania, sterowania klapami, systemy gaszenia.

Dobrze wykonana integracja SSP z innymi zewnętrznymi systemami odgrywa istotną rolę w prawidłowym funkcjonowaniu obiektu. Przed podjęciem decyzji o wyborze centrali sygnalizacji pożarowej (systemu) warto znać odpowiedzi na kilka pytań:

- Czy wybrany system ma wymagane certyfikaty na centralę, elementy pętlowe, konwencjonalne?
- Czy system spełnia wymagania pod względem funkcjonalnym?
- Czy dane rozwiązanie pozwoli zrealizować przewidziany scenariusz pożarowy?
- Czy obsługa centrali jest przyjazna dla użytkownika?
- Czy w systemie można zastosować rozwiązania pozwalające na weryfikację fałszywych alarmów (np. koincydencję)?
- Czy system pozwala na późniejszą jego rozbudowę?
- Jakie są graniczne wartości parametrów systemu?
- Ile elementów można podłączyć do pętli lub pojedynczej centrali?
- Jak długie pętle można stworzyć?
- Czy system może być zintegrowany z systemem wizualizacji lub innymi systemami w obiekcie?
- Jakie będą koszty serwisowania i eksploatacji systemu?
- Kto będzie odpowiedzialny za przeszkolenie personelu, czy przewidziano na to odpowiednie fundusze?
- Jaki jest okres gwarancyjny i kto zapewni wsparcie techniczne?

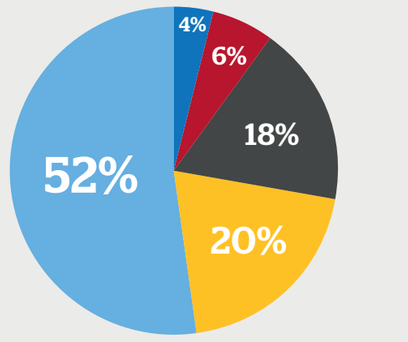
Wszystkie te czynniki mają wpływ na działanie systemu, jego cenę i późniejsze koszty eksploatacji. Rolą projektanta SSP jest przede wszystkim dobór czujek i innych elementów systemu w zależności od przeznaczenia pomieszczeń hotelowych, w których mają być zainstalowane, aby system zapewniał wczesną detekcję pożaru, minimalną liczbę fałszywych alarmów oraz przeprowadzenie bezpiecznej ewakuacji. Niewłaściwie dobrany system może wręcz sparaliżować pracę hotelu, zmuszając niepotrzebnie gości do opuszczenia pokoi. w najmniej odpowiednim momencie (często w nocy). Wadliwie działający system sygnalizacji pożarowej negatywnie wpływa na odczucia gości hotelowych.



Schemat systemu sygnalizacji pożarowej oraz powiązanych z nim innych systemów i urządzeń wg normy EN-54-1 [5]

PRZYCZYNY POŻARÓW W OBIEKTACH MIESZKALNYCH, W TYM HOTELOWYCH, W 2017 R. [3]

Według raportu GUS[1] liczba turystycznych obiektów hotelowych rośnie, w 2017 r. w Polsce było ich 10 681 [2]. W tym samym roku według KG PSP odnotowano ok. 600 pożarów w obiektach hotelowych [3]. Jako ich główną przyczynę podaje się nieostrożność osób dorosłych i nieletnich, wady urządzeń i instalacji elektrycznych, grzewczych, mechanicznych oraz sposób ich eksploatacji. Zdarza się, że przyczyna pożaru jest nieustalona. Rozmiar pożarów i zagrożenie utraty życia czy mienia jest również zróżnicowane.



[1] *Wykorzystanie turystycznych obiektów noclegowych w 2017 roku*, Główny Urząd Statystyczny, 6.04.2018 r.

Większość certyfikowanych systemów dostępnych na rynku ma zbliżone funkcjonalności, wymuszone przepisami. Różnią się jakością, ceną oraz kosztami eksploatacji i serwisu

Zabezpieczając przeciwpożarowo hotele, projektanci muszą zmierzyć się z licznymi wyzwaniami, ponieważ każdy obiekt jest inny. We współczesnych obiektach mamy nie tylko pokoje hotelowe, ale również lobby, korytarze, sale konferencyjne, restauracje, serwerownie, garaże podziemne, kuchnie, palarnie, sklepy, strefy wellness, windy. W większości pomieszczeń instaluje się czujki punktowe, dobierając ich rodzaj w zależności od przewidywanego rozwoju pożaru. Czujki oferowne na rynku są badane na wykrywanie pożarów testowych TF (*Test Fire – tab.),* więc można je właściwie dobrać do przewidywanego zagrożenia w konkretnym pomieszczeniu.

Producenci systemów SSP dążą do skonstruowania czujki o wysokiej czułości, a jednocześnie odpornej na fałszywe alarmy. Dostępne na rynku rozwiązania obejmują rozmaite czujki: od termicznych, przez optyczne z dwoma sensorami, skończywszy na czujkach wielosensorowych i z częścią chemiczną. Dostępne są także

Charakterystyka pożarów testowych opracowana na podstawie normy EN-54-7 (zakres TF2-TF5) i dodatkowo (TF1, TF6, TF7,TF8,TF9 na podstawie ISO/TS 7240-9:2006 [6]

Rodzaj pożaru (paliwo)	Płomieniowe spalanie celulozy	Szybki rozkład termiczny piroliza (drewna)	Pożar tlący (bawełna)	Płomieniowe spalanie tworzywa (poliuretan)	Spalanie cieczy wydzielającej dym (n-heptan)	Spalanie cieczy nie-wydzielającej dymu (alkohol etylowy)	Powolne tlenie się drewna	Spalanie cieczy wydzielającej dym bez ciepła (dekalina)	Tlenie się bawełny złożonej
Wzrost temperatury	silny	do pominięcia	do pominięcia	silny	silny	silny	do pominięcia	do pominięcia	do pominięcia
Prędkość wznoszenia	duża	mała	bardzo mała	duża	duża	duża	mała	mała	mała
Dym	jest	jest	jest	jest	jest	nie ma	jest	jest	jest
Widmo dymu	przeważnie niewidoczne	przeważnie widoczne	przeważnie niewidoczne	częściowo niewidoczne	przeważnie niewidoczne	nie ma	przeważnie widoczne	przeważnie widoczne	przeważnie widoczne
Część widzialna dymu	ciemna	jasna, silnie rozpraszająca	jasna, silnie rozpraszająca	bardzo ciemna	bardzo ciemna	nie ma	jasna, silnie rozpraszająca	ciemna	ciemna
Występowanie CO	nie ma	znaczne	duże	słabe	słabe	nie ma	znaczne	bardzo słabe	duże

detektory bardziej odporne na czynniki zewnętrzne (istotne w obiektach hotelowych), takie jak dym papierosowy, zapylenie, wilgoć, a nawet zakłócenia elektromagnetyczne. Nie w każdych pomieszczeniach hotelowych czujki punktowe znajdą zastosowanie. Często nie tylko przeznaczenie czy wyposażenie pomieszczeń decyduje o wyborze elementu detekcyjnego, ale także architektura budynku. Atria i wysokie hole recepcyjne wymagają użycia czujek liniowych; szyby windowe, mroźnie czy sauny – dedykowanego rozwiązania, jakim są systemy zasysające.

W nowoczesnych hotelach dużą rolę odgrywa estetyka pomieszczeń, dlatego producenci oferują czujki w różnych kolorach i kształtach, które nie zaburzają wystroju wnętrz, wtapiając się w otoczenie.

Powiadamianie o pożarze i szybka ewakuacja

Podstawowym źródłem alarmowania o pożarze w przypadku hoteli do 200 miejsc noclegowych są przede wszystkim sygnalizatory akustyczne, uzupełniane o sygnalizatory optyczne w obszarach, w których mogą przebywać osoby niesłyszące, lub w pomieszczeniach, w których ze względu na panujące warunki sygnalizatory akustyczne byłyby nieskuteczne. Ciekawym rozwiązaniem są sygnalizatory adresowalne, które pojawiają się w coraz większej liczbie projektów SSP dla hoteli. To rozwiązanie, które w przypadku wykrycia pożaru pozwala na wysterowanie sygnalizatora w konkretnym pokoju hotelowym lub innym pomieszczeniu. Jest to bardzo wygodne rozwiązanie, ponieważ nie alarmujemy wszystkich osób w strefie pożarowej, a tylko osoby w zagrożonym pomieszczeniu. Dopiero po weryfikacji i potwierdzeniu pożaru alarm jest uruchamiany w całej strefie. Projektanci chętnie sięgają po sygnalizatory adresowalne akustyczno-głosowe. W hotelach, w których nie ma DSO, znacznie przyspieszają ewakuację, tym bardziej że dostępne na rynku sygnalizatory mogą mieć wgrywane komunikaty w różnych językach, a sekwencje sygnałów akustycznych i głosowych są programowalne, podobnie jak poziom natężenia dźwięku czy synchronizacja.

Rola obsługi hotelowej

Nawet najbardziej doskonały system sygnalizacji pożarowej może nie spełnić swojej funkcji, jeżeli personel hotelu nie zostanie odpowiednio przeszkolony do jego obsługi. Alarmy i procedury pożarowe są priorytetowe dla recepcjonisty i ochrony hotelu. W razie ewentualnego zagrożenia to właśnie obsługa obiektu do czasu przyjazdu straży pożarnej prowadzi ewakuację i dba o bezpieczeństwo gości. Dlatego niezwykle ważna jest wiedza, opanowanie i cykliczne szkolenia personelu. Każdy alarm pożarowy to sytuacja stresująca zarówno dla pracownika, jak i dla gościa przebywającego w hotelu. Nigdy nie wiadomo, czy dane zdarzenie jest fałszywe, czy prawdziwe. Goście hotelowi nie znają obiektu i nie wiedzą, jak się zachować podczas alarmu. Personel musi umieć radzić sobie z klientami – często zdenerwowanymi lub niechętnie stosującymi się do procedur. Od ich prawidłowego zachowania może zależeć życie ludzkie.

BIO

Monika Kołodziejczyk

Z branżą zabezpieczeń związana od 2000 r. Obecnie prezes firmy C-AIM. Ma bogate doświadczenie w zakresie projektowania i wdrażania rozwiązań z zakresu systemów sygnalizacji pożarowej.

Literatura

[1] Rozporządzenia MSWiA z 7 czerwca 2010 r. w sprawie ochrony ppoż. budynków, innych obiektów budowlanych i terenów (Dz.U.2010, nr 109, poz. 719).

[2] Raport Głównego Urzędu Statystycznego „Wykorzystanie turystycznych obiektów noclegowych w 2017 roku".

[3] Raport KG PSP w Warszawie „3_2017 pożary według kategorii obiektów".

[4] Raport „Colliers_Raport-Market-Insights-2018".

[5] Norma PN-EN-54-1 Systemy Sygnalizacji Pożarowej. Część Wprowadzenie.

[6] Norma PN-EN-54-7 Systemy sygnalizacji pożarowej – Część 7: Czujki dymu – Czujki punktowe działające z wykorzystaniem światła rozproszonego, światła przechodzącego lub jonizacji i ISO/TS 7240-9:2006 ISO/TS 7240-9: 2006 Fire detection and alarm systems – Part 9: Test fires for fire detectors.

[7] Norma PN-EN-54-3 i PN Systemy sygnalizacji pożarowej – Część 3: Pożarowe urządzenia alarmowe – Sygnalizatory akustyczne.

[8], [9] Norma PN-EN-54-2 Systemy sygnalizacji pożarowej – Część 2: Centrale sygnalizacji pożarowej.

DEKK FIRE SOLUTIONS
ul. Zielona 52, 05-500 Piaseczno
tel. 22 244 22 00, faks 22 24422 01
e-mail: info@dekk.pl

Jeśli gaszenie gazem, to tylko INERGEN!

Zabezpieczenie przeciwpożarowe strategicznych pomieszczeń np. serwerowni, pomieszczeń ruchu elektrycznego czy muzeów, to oprócz wyboru odpowiedniego systemu detekcji pożaru także wybór właściwego systemu gaśniczego. **Niektóre związki chemiczne, kiedyś rozpowszechniane i chwalone, dziś przechodzą do lamusa (zgodnie z ustawą z 15.05.2015 poz. 881).**

Beata Kazimierska
Fire Eater Polska sp. z o.o.

Technologia gazów obojętnych, w tym najbezpieczniejszego wśród nich inergenu, rozwija się od lat. Pionierzy, którzy wprowadzili INERGEN® do obrotu, z satysfakcją obserwują trend ekspansji gazów obojętnych, jednorodnych oraz ich mieszanin. INERGEN jest jednym z najnowocześniejszych systemów gaśniczych. Bezpieczny dla sprzętu, środowiska i ludzi, jest jednym z najczęściej używanych, skutecznych środków gaszących. Jego działanie gaśnicze polega na redukowaniu tlenu w pomieszczeniu z 21% do 14% objętości i mniejszej. Pożar jest gaszony, a ludzie mogą oddychać.

Dlaczego INERGEN?

Do podstawowych jego zalet należy duża skuteczność systemu przy równoczesnej elastyczności po kątem projektowania. Gaz ten jest bezpieczny dla ludzi przy projektowanych stężeniach i bezpieczny dla środowiska, czego nie można powiedzieć o środkach chemicznych. INERGEN – Fire Eater nie wywołuje mikrokorozji, nie wytwarza szkodliwych substancji w połączeniu z dymem czy pożarem, co istotnie wpływa na bezpieczeństwo chronionych materiałów i urządzeń. Nie powoduje zamglenia w pomieszczeniu w trakcie wyzwalania, ma relatywnie niską cenę środka gaśniczego, nie pozostawia pozostałości po gaszeniu (aerozole). Dopuszczony wg ISO 14520 i inne dłuższy czas wyzwolenia INERGENU nawet do 120 s świadczy o jego elastyczności i zarazem możliwości płynnego, spokojnego wypływu. Przy dużej swobodzie projektowania instalacji z użyciem tłumików fali akustycznej system zapewnia najbardziej bezpieczny proces wypływu.

System wielostrefowy, który może znacząco obniżyć koszty instalacji przy zabezpieczaniu większej liczby pomieszczeń, ma prostą budowę, co dowodzi, że jest on niezawodny, a ryzyko popełnienia błędów podczas montażu minimalne. INERGEN był testowany na ludziach – solidna dokumentacja techniczna potwierdza, że dla człowieka jest bezpieczny.

Ochrona ludzi, sprzętu i pomieszczeń

Instalacje gaśnicze INERGEN są montowane głównie w pomieszczeniach komputerowych, biurowcach, archiwach, rozdzielniach elektrycznych, hotelach, szpitalach, obiektach muzealnych. Archiwa i muzea korzystają z długich czasów utrzymania stężeń gaśniczych, gdyż w ten sposób skutecznie unika się pożarów połączonych z żarzeniem materiału.

Jak działa system?

Szybkość skutecznej akcji gaszenia jest ściśle związana z właściwym doborem systemu detekcji pożaru i czasem przygotowania pomieszczenia do gaszenia. Gdy detektory automatycznie wykryją rozprzestrzeniający się pożar, centrala sterująca włącza sygnalizatory akustyczne i optyczne sygnały ostrzegawcze. Po krótkim czasie zwłoki na przygotowanie do wyzwolenia sygnał z centrali uruchamia zawór elektromagnetyczny, wyzwalając zestaw gaśniczy do chronionego pomieszczenia. Każdorazowo układ hydrauliczny z rurociągami i dyszami jest kalkulowany nie na podstawie założeń, a za pomocą profesjonalnych programów obliczeniowych, których poprawność była sprawdzona podczas wielu testów wyzwalania i pomiarów stężeń.

System gaśniczy INERGEN ma wiele zalet. Zapewnia bezpieczeństwo ludziom i obszarom chronionym. Jego prosta budowa przekłada się na sprawność układu. To coraz bardziej popularny i coraz częściej wybierany środek gaśniczy, skuteczny i niepowodujący skutków ubocznych. Producent systemu Fire Eater przeprowadza testy rzeczywistego wyzwalania gazu, które potwierdzają jego dużą skuteczność.

WSPÓŁODPOWIEDZIALNOŚĆ ZA CYBERBEZPIECZEŃSTWO W SEKTORZE FINANSOWYM

Szybko dokonujące się zmiany cywilizacyjne i rozwój nowoczesnych technologii spowodowały, że niemal wszystkie sfery życia ogarnęło cyfrowe tsunami. Otwarty Internet usunął bariery między państwami, społecznościami i obywatelami, pozwalając na wymianę informacji w niewyobrażalnej dotychczas skali. Cyberprzestrzeń stała się forum wymiany doświadczeń, promuje nowe idee, ale uzależnienie człowieka i otaczających go procesów gospodarczych od wszechobecnej innowacyjności niesie również wiele niebezpieczeństw.

Krzysztof Gawkowski

Jednym z sektorów, który w sposób wyjątkowy korzysta ze zdobyczy nowych technologii do poprawy swoich procesów i usług, jest bankowość. Postęp technologiczny zapewne nie sprawi, że oddziały banków znikną, ale bez wątpienia instytucje finansowe będą coraz szybciej zmierzać w kierunku bankowości mobilnej.
Zmiany towarzyszące rozwojowi technologii informacyjno-komunikacyjnych są widoczne w każdym obszarze funkcjonowania świata finansów. Bankowość elektroniczna spowodowała, że nie ma już kolejek do kasy w banku, a klienci otrzymali zdalny dostęp do swojego rachunku za pomocą komputera, tabletu czy smartfonu. E-bankowość zwiększa szybkość transakcji, zapewnia wygodne korzystanie z konta, wzmacnia dostępność usług i pozwala na ograniczenie kosztów. Stała się ważną i nierozłączną częścią całego sektora finansów.

PROGNOZY NA NAJBLIŻSZE LATA

Z tegorocznego badania Polskiego Instytutu Cyberbezpieczeństwa „#PolskiBarometrCyberbezpieczeństwaSpołecznego2018 (#PBCS18)" wynika, że polskie banki i instytucje finansowe cieszą się największą wiarygodnością i zaufaniem klientów spośród wszystkich branż, które intensywnie wdrażają nowoczesne technologie. Wysoki poziom zaufania wynika zapewne z presji klientów oraz wdrażania systemów bezpieczeństwa opartych na sztucznej inteligencji, analityce dużych zbiorów danych czy uczeniu maszynowym. Globalna firma badawcza IDC prognozuje, że w 2019 r. wydatki na sztuczną inteligencję i systemy kognitywne na całym świecie przekroczą 30 mld dol., z czego najwięcej przeznaczy na nią właśnie bankowość. Z prognozy Digital Banking wynika, że w 2019 r. co najmniej jedno rozwiązanie z zakresu *machine learning* wdroży blisko połowa organizacji finansowych, natomiast wg wspominanego wcześniej raportu #PBCS18 w ciągu najbliższych 10 lat nawet 50 proc. zadań w sektorze finansowym przejmą roboty.

Integracja cyfrowa w sektorze bankowym na całym świecie stała się zjawiskiem tak powszechnym, że większość z nas nawet nie zdaje sobie sprawy, jak bardzo jesteśmy uzależnieni od cyfrowych zer i jedynek. Dostępność i rozwój nowych technologii implikują stopniowe przedefiniowanie roli banku w życiu człowieka. Z danych Związku Banków Polskich wynika, że liczba aktywnych użytkowników bankowości mobilnej przekroczyła już 7 mln, internetowej – 16 mln, kart płatniczych w Polsce – ponad 35 mln. Liczby te w ślad za rozwojem technologii będą coraz większe, a w związku z tym zagrożenie również będzie rosło. Nawet jeśli dotychczas nie było dużych kradzieży pieniędzy czy wycieków danych klientów banków, trzeba się przygotować na to, że taki atak jest kwestią czasu.

Cyberataki i próby kradzieży danych, informacji czy wirtualnego pieniądza są na całym świecie zjawiskiem coraz bardziej powszechnym. Tylko w tym roku przestępcy obrali za cel kilka kluczowych instytucji finansowych w państwach zarówno poniżej średniej światowej PKB, jak i przodujących w globalnej gospodarce. Ze skoordynowanym atakiem musiał zmierzyć się m.in. meksykański bank Banco Nacional de Comercio Exterior, z którego hakerzy próbowali wykraść ponad 110 mln dol. Atak był nieudany, ale kilka miesięcy później meksykańskie instytucje finansowe ujawniły inną informację o cyberataku, w którego wyniku skradziono ponad 300 mln pesos (ponad 15 mln dol.). Podobne zdarzenie miało miejsce w Indiach, gdzie hakerzy w ciągu dwóch godzin dokonali blisko 15 tys. transakcji opiewających na łączną kwotę 805 mln rupii (prawie 11 mln dol.). Indyjski Cosmos Bank stracił ok. 139 mln rupii (tj. blisko 3 mln dol.), ponieważ przestępcy przekazali środki finansowe na rachunek podstawionej firmy z siedzibą w Hongkongu, dokonując kilku nieautoryzowanych transakcji w globalnej sieci płatności SWIFT.

> Korzystając z bankowości internetowej, zatrważająco źle wypadamy w kontekście stosowanych zasad bezpieczeństwa

Przestępcy nie próżnują również w Europie. Podczas tegorocznych wakacji doszło do cyberataku na infrastrukturę rosyjskiego PIR Banku, w którego wyniku skradziono 1 mln dol. Całe zdarzenie rozpoczęło się dość niewinnie od incydentu związanego z routerem używanym przez jeden z oddziałów banku. Za jego pomocą hakerzy uzyskali bezpośredni dostęp do sieci lokalnej i dzięki automatycznej stacji roboczej Rosyjskiego Banku Centralnego wygenerowali zlecenia płatnicze.
W 2018 r. serię ataków DDoS przypuszczono także na holenderski bank ABN AMRO. Mimo że w wydanym oświadczeniu bank twierdził, że ataki zostały powstrzymane, a zasoby finansowe i bazy danych są w pełni bezpieczne, to pracownicy banku uważają, że z kont zniknęło prawie 3 mln euro, a akcja dezinformacyjna ma na celu ochronę dobrego imienia instytucji finansowej.

Polskie banki również nie są wolne od ataków hakerskich. W 2017 r. dziennik „New York Times" poinformował, że atak na instytucje bankowe w Polsce rozpoczął się, gdy północnokoreańscy hakerzy zainfekowali złośliwym oprogramowaniem strony Komisji Nadzoru Finansowego, licząc, że banki nieświadomie pobiorą zakładkę. Działania dotyczyły ponad 20 banków w Polsce i do dziś nie ustalono, jakie dokładnie straty w związku z tym poniesiono.
W maju 2018 r. analitycy firmy ESET odkryli nowe zagrożenie, dotyczące tym razem klientów pięciu czołowych banków polskich. Atak próbowano przypuścić za pośrednictwem wiadomości e-mail zawierających zainfekowany załącznik, który wyglądał jak faktura. Wyjątkowo

złośliwe oprogramowanie BackSwap modyfikowało numery rachunków w przelewach internetowych – kiedy klient banku wykonywał przelew na kwotę większą niż 10 tys. zł, skrypt niezauważalnie podmieniał numer konta i pieniądze trafiały do przestępcy.

Mimo zdarzających się incydentów trzeba podkreślić, że polski sektor bankowy należy do najbardziej zaawansowanych technologicznie na świecie i przeznacza olbrzymie środki zarówno na wdrożenie innowacji rynkowych, jak i modelowanie cyberbezpieczeństwa. Bardzo dobrym przykładem korzystania z technologii cyfrowych w sektorze e-bankowości są płatności zbliżeniowe.

Okazuje się, że Polska należy do grupy dziesięciu państw na świecie przodujących w tej technologii. Dane z raportu „Sektor finansowy coraz bardziej #fintech", przygotowanego przez firmę doradczą PwC wskazują również, że oprócz dbałości o cyberbezpieczeństwo oraz wdrażania najnowszych zabezpieczeń banki i instytucje finansowe muszą także podnosić świadomość swoich klientów i pracowników, ponieważ zwykle to człowiek jest najsłabszym ogniwem w łańcuchu bezpieczeństwa.

Z badania Komisji Europejskiej wynika, że chociaż w ciągu ostatnich siedmiu lat zastosowanie bankowości internetowej w Polsce wzrosło prawie dwukrotnie, to w porównaniu do pozostałych państw UE plasujmy się w środku europejskiej stawki. 58 proc. ankietowanych Polaków odpowiedziało, że korzysta z bankowości internetowej. Zdecydowanie bardziej popularne jest użytkowanie nowoczesnych form bankowości w krajach skandynawskich, np. w Dani i Finlandii – ok. 93 proc. Najmniej użytkowników rozwiązań mobilnych w sektorze finansów mają Rumunia i Bułgaria (zaledwie kilkanaście procent).

Znacznie gorzej wypadają polscy użytkownicy w kontekście stosowanych zasad bezpieczeństwa – ponad 70 proc. korzystających z bankowości internetowej nie zmieniło hasła dostępowego w ciągu ostatniego roku! Są to dane zatrważające, pokazują, jak bardzo bagatelizujemy zagrożenia czyhające w cyberświecie.

Polski sektor bankowy, przeznaczający olbrzymie środki finansowe na wdrożenie innowacji i modelowanie cyberbezpieczeństwa, należy do najbardziej zaawansowanych technologicznie na świecie

Polska należy do grupy 10 państw świata przodujących w płatnościach zbliżeniowych

Ustawa o krajowym systemie cyberbezpieczeństwa

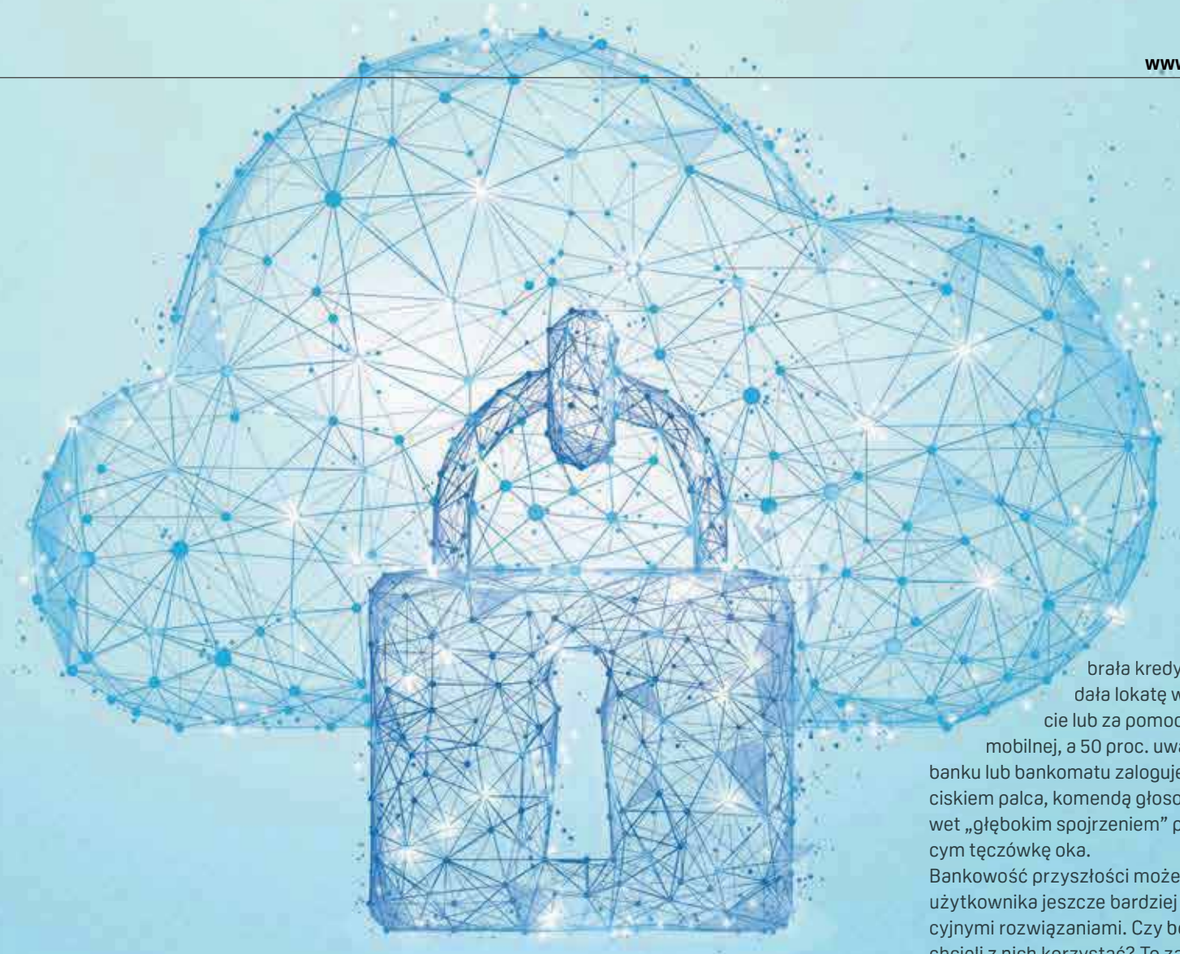
Naprzeciw niskiej świadomości społecznej dotyczącej zagrożeń, jakie niesie cyberprzestrzeń, wychodzi ustawa o krajowym systemie cyberbezpieczeństwa, która implementuje do polskiego prawodawstwa europejską dyrektywę NIS – *Network and Information Systems Directive.* Mimo że weszła w życie w sierpniu 2016 r., jej wdrożenie do polskiego systemu prawnego trwało blisko dwa lata. Dokument jest pierwszym ogólnounijnym aktem prawnym w dziedzinie cyberbezpieczeństwa gwarantującym równy poziom zabezpieczeń sieci i systemów w całej Wspólnocie. Przygotowane regulacje dotyczą bezpieczeństwa sieci i informacji, a na ich podstawie m.in. banki i instytucje finansowe zostały wpisane do rejestru operatorów usług kluczowych, na których ciążą obowiązki związane z zapewnieniem cyberbezpieczeństwa.

Zgodnie z ustawą i rozporządzeniami wykonawczymi banki najpóźniej na początku 2019 r. muszą m.in. powołać wewnętrzne struktury do zarządzania cyberbezpieczeństwem lub skorzystać z firm zewnętrznych. Ponadto każdy operator usług kluczowych musi wdrożyć program systematycznej analizy i zarządzania ryzykiem, a także uruchomić sprawnie funkcjonujący proces zarządzania incydentami bezpieczeństwa, który pozwala m.in. na zgłaszanie poważnych incydentów do krajowego zespołu CSIRT (sieci Zespołów Reagowania na Incydenty Bezpieczeństwa Komputerowego) w czasie nieprzekraczającym 24 godzin od ich wykrycia.

Ustawa o krajowym systemie cyberbezpieczeństwa wskazuje również na inne konkretne działania, jakie banki i instytucje finansowe muszą podjąć. Z początkiem 2019 r. operatorzy usług kluczowych będą mieli obowiązek wdrożenia zabezpieczeń proporcjonalnych do oszacowanego ryzyka. Odpowiednie przygotowanie systemów zabezpieczających w obszarze cyberprzestrzeni powinno zatem obejmować także wprowadzenie planów ciągłości działania, objęcie systemów informatycznych monitorowaniem w trybie ciągłym, uruchomienie sprawnych procesów zarządzania podatnością na cyberzagrożenia i gromadzenia wiedzy na ich temat.

Ważnym obowiązkiem jest także konieczność opracowania i zapewnienia aktualnej dokumentacji dotyczącej cyberbezpieczeństwa systemów informatycznych wykorzystywanych do świadczenia usługi kluczowej. Po spełnieniu wszystkich obowiązków oraz ich uporządkowaniu banki będą zobowiązane do przeprowadzenia w terminie roku zewnętrznego audytu bezpieczeństwa. Później audyty będą odbywać się co dwa lata. Za niewykonanie tego obowiązku grozi grzywna w wysokości 200 tys. zł.

Nawet najlepsze prawodawstwo nie uchroni banków ani klientów indywidualnych przed cyberatakami, jeśli sami nie będziemy dbali o jakość usług cyfrowych. Głównymi zaleceniami służącymi budowaniu współodpowiedzialności za cyberbezpieczeństwo w sektorze finansowym jest regularne podnoszenie świadomości o problemach mogących stanowić źródło cyberataku. Podstawą jest tworzenie silnych haseł, które powinny składać się z wielkich i małych liter, cyfr oraz znaków specjalnych. Nawykiem powinno być zmienianie haseł dostępu do mobilnych usług finansowych raz w miesiącu oraz nieużywanie tego samego hasła do wielu serwisów, np. bankowości internetowej, poczty elektronicznej czy serwisów społecznościowych. Trzeba również pamiętać, aby nie udostępniać swojego komputera innym osobom, wyłączyć automatyczne zapamiętywanie haseł oraz nie podłączać urządzeń do publicznych sieci Wi-Fi, gdy planujemy logowanie do bankowości elektronicznej. To oczywiście tylko podstawy, ale ważne, zważywszy że wg badania #PBCS18 wykonanego przez Polski Instytut Cyberbezpieczeństwa 29 proc. ankietowanych skłonnych byłoby pozytywnie odpowiedzieć na autoryzację banku, o którą zwróciłby się on za pomocą poczty elektronicznej.



Obecnie trudno sobie nawet wyobrazić codzienne życie bez bankowości elektronicznej. Kluczowym wyzwaniem w świecie wirtualnego pieniądza jest jednak ciągłe wzmacnianie reputacji instytucji odpowiedzialnych za obrót środkami płatniczymi i ich bezpieczeństwo. Skłonność do zaufania bankom może się szybko skończyć, jeśli zarówno instytucje sektorowe, jak i klienci indywidualni nie zastosują wszelkich sił i środków do poprawy standardów cyberbezpieczeństwa. Z badania #finanseprzyszlosci przeprowadzonego przez ośrodek IBRiS na zlecenie banku Millennium wynika, że Polacy wyrażają coraz większe zainteresowanie wdrażaniem innowacji umożliwiających kontakt z bankiem. Zdaniem 90 proc. ankietowanych w ciągu 10 lat własnoręczny podpis zostanie zastąpiony elektronicznym, obsługa w większości oddziałów bankowych będzie automatyczna, a prawie wszystkie sprawy będzie można załatwić za pomocą rzeczywistości wirtualnej. Co więcej, blisko 80 proc. pytanych twierdzi, że w 2028 r. będzie brała kredyt czy zakładała lokatę w bankomacie lub za pomocą aplikacji mobilnej, a 50 proc. uważa, że do banku lub bankomatu zalogujemy się odciskiem palca, komendą głosową czy nawet „głębokim spojrzeniem" prezentującym tęczówkę oka.

Bankowość przyszłości może zaskoczyć użytkownika jeszcze bardziej rewolucyjnymi rozwiązaniami. Czy będziemy chcieli z nich korzystać? To zależy przede wszystkim od tego, czy człowiek w tej sieciowej pajęczynie poczuje się komfortowo i bezpiecznie. Pozytywnym elementem rozwoju usług mobilnych w sektorze finansowym jest to, że świadomość konieczności inwestycji w ten obszar rośnie z roku na rok. Banki, decydując się na udział w audytach, badaniach czy testach potwierdzających przygotowanie do ochrony przed atakiem w cyberprzestrzeni, wykazują chęć przeciwdziałania zagrożeniom. Coraz więcej informacji szkoleniowych trafia również do klienta, a synergia na linii bank – konsument daje nadzieję, że przed bankowością elektroniczną jeszcze lepszy czas. ■

BIO

Krzysztof Gawkowski

Społecznik i wykładowca akademicki. Doktor nauk humanistycznych specjalizujący się w zakresie bezpieczeństwa państwa. Dyrektor Polskiego Instytutu Cyberbezpieczeństwa oraz kierownik Katedry Bezpieczeństwa Wewnętrznego Uczelni Techniczno-Handlowej im. Heleny Chodkowskiej w Warszawie. Członek Komitetu Technicznego PKN oraz przewodniczący Rady Programowej Instytutu Bezpieczeństwa Inteligentnych Miast. Autor książek: *Obudzić państwo* oraz *Administracja samorządowa w teorii i praktyce*, a także powieści kryminalnych *Piętno prawdy* oraz *Cień przeszłości*.

Jeśli potrafisz w prosty sposób opisać swoją pracę, prawdopodobnie w najbliższym czasie zostanie ona zautomatyzowana.

BANKING SECURITY

BACK to the FUTURE

Kilkakrotnie podejmowałem temat przeszłości rynku safety i security oraz zmian, jakie na nim zachodzą. **Czas zastanowić się, dokąd zmierzamy, gdy wszystko wokół nas zaczyna przybierać wymiar 4.0.**

Rafał Łupkowski

W obszarze zarządzania bezpieczeństwem również dokonują się zmiany, można powiedzieć, że przenosi się ono z metalowej szafy do sieci. Trwa dynamiczny rozwój strefy cybersecurity. Chodzi o zasady globalnej komunikacji, a przede wszystkim o postępującą automatyzację procesów. Wiadomo że bezpieczeństwo to proces wpływający na podstawową działalność operacyjną organizacji, zatem także i ono może być automatyzowane w niemal dowolny sposób – byle mądrze.

Kiedy ostatnio badałem różne obszary i organizacje pod kątem oceny ich stanu bezpieczeństwa, dostrzegłem tendencję do automatyzacji podstawowych procesów w zakresie bezpieczeństwa fizycznego, w szczególności procesu nadawania praw dostępu i zarządzania uprawnieniami (chodziło głównie o prozaiczne z punktu widzenia użytkownika czynności, takie jak obsługa recepcji).

W większości przypadków, z jakimi miałem styczność, odpowiedzialni zarządzający zamierzali ten proces w pełni automatyzować, by ograniczyć do niezbędnego minimum koszty pracownicze – przy zachowaniu podstawowych funkcji, mało kto bowiem chce dziś realizować podstawowe aspekty bezpieczeństwa w wersji *concierge*. Przypadek? Raczej pragmatyczne podejście do kosztów i zadań.

W zasadzie można by to skwitować krótko – w tym zakresie od lat niewiele się zmienia. Bezpieczeństwo wciąż kojarzy się z wydatkami. Współczesne założenia różnią się od tych sprzed lat przede wszystkim dostępnością niedrogiej i skutecznej technologii pozwalającej w relatywnie prosty sposób te potrzeby realizować, a jednocześnie osiągać skutecznie swoje cele biznesowe.

Spróbujmy jednak na przykładzie banków odnieść proces automatyzacji np. do obsługi gotówki. Czy relacja transakcji gotówkowych do bezgotówkowych znacznie się zmieniła i czy wpłynęło to na procesy bezpieczeństwa i ich traktowanie przez instytucje finansowe? Odpowiedź wydaje się oczywista. Inny przykład – obszar telewizji dozorowej i możliwości jego rozwoju w ślad za rozwojem sieci i aplikacji. Czy operatora docelowo zastąpi analityka obrazu? Jak długo można tłumaczyć efektywność człowieka patrzącego na ekrany monitorów, na których wyświetlają się obrazy z blisko 80 kamer? To duże uproszczenie. Gdy jednak połączymy to z inteligentną analizą obrazu, dość szybko uznamy termin wirtualny obchód za trafny i znajomy.

Coraz częściej w swojej codziennej pracy przekonuję się, że dyskusję o roli człowieka w zapewnieniu podstawowych usług w zakresie bezpieczeństwa (mam na myśli proste i często nieskuteczne usługi ochrony) można spuentować następująco: „Branża ochrony poszukuje nowej formuły". Zgadzam się w 100%, gdyż skala optymalizacji wynikająca z potrzeb rynku, a także coraz większa świadomość kupujących wszelkiego rodzaju usługi rośnie w postępie geometrycznym. Tendencja ta powoduje określone postrzeganie struktur zarządzania bezpieczeństwem. W dobie recesji sektorowej i ciągłej konsolidacji rynku obszar bezpieczeństwa niebędący sferą wspomnianego *cyber* jest cyklicznie ograniczany i sprowadzany do prostych serwisów administracyjnych. Co gorsza, w naszych realiach świat się nie zawala z tego powodu, a instytucje zaufania publicznego, np. banki, rzadko tracą wizerunek, co potęguje przekonanie o słuszności takich działań.

Jakiś czas temu nie zgadzałem się z takim stanem – dziś z zupełnie innej perspektywy widzę to jako nieuniknioną konsekwencję wymienionych czynników, a tym samym ogromny potencjał do wykorzystania. Skuteczne zarządzanie bezpieczeństwem, szczególnie fizycznym, nigdy nie przestanie być ważne, niemniej musi zostać sprowadzone do roli świetnie naoliwionego mechanizmu, gdzie mechanika (człowiek) i elektronika (technologia) będą współgrały ze sobą jak dobrze funkcjonujący multisejf czy dyspenser, które odesłały do lamusa tradycyjne szafy pancerne, a z pewnością znacznie zmniejszyły ich udział w procesie.

Działania rynku związane bezpośrednio z bezpieczeństwem, szczególnie fizycznym, przypominają trochę sytuację ze zbliżającym się okresem zimowym i sektorem motoryzacyjnym. Z jednej strony uświadamia się ryzyko braku odpowiednich opon zimowych, gdy temperatura spada poniżej 7°Celsjusza, jednak większość kierowców z podjęciem decyzji czeka na opady śniegu. Sytuację komplikują też producenci, stawiając na produkcję znacznie tańszych opon całorocznych. Wielu kierowców, zwłaszcza w dużych miastach, nie zmienia opon na zimowe, uważając, że ryzyko jest niewielkie. Do czasu „zimy stulecia" można skutecznie ograniczać koszty, zwłaszcza przy użyciu nowej, tańszej technologii.

Czy warto z tym walczyć, czy może lepiej się dopasować? Dziś wiele systemów bezpieczeństwa jest przeinwestowanych, nieskutecznych, a także oderwanych od realnych potrzeb i specyfiki danej organizacji. Pokutują lata przekonań o słuszności pewnych założeń w organizacji bezpieczeństwa, które zamieniają się w wygodę lub strefę komfortu niewymagającą zmiany przez właściciela danego systemu. Taki stan rzeczy powoduje brak rozwoju i świadomości zmieniającego się rynku, a także pewne ułomności w organizacji bezpieczeństwa, także w bankach. Trwanie w przekonaniu, że „nadzorowanie" ochrony i systemów zabezpieczeń bez wyraźnego wpływu na generowanie wartości dodanej dla organizacji jest błędem, który w rezultacie może doprowadzić do daleko idącej optymalizacji nakładów i zatrudnienia.

Z ciekawością obserwuję, w jakim kierunku zmierza rynek, szczególnie europejski. Zauważam tendencję napływania do nas najlepszych praktyk z pewnym, nawet kilkuletnim opóźnieniem – monitoring wizyjny z powodzeniem działał od lat w Skandynawii i innych krajach. To samo dotyczy rezygnacji z prostych usług ochrony na rzecz np. patroli – tzw. ochrona *on demand*. Fakt, że nasz rynek otwiera się coraz bardziej na usługi doradcze, w tym outsourcing, nie pozostaje bez znaczenia. Na domiar złego koszty pracy stale rosną, a technologii maleją – kolejny przypadek?

Bezpieczeństwo to proces wpływający na podstawową działalność operacyjną organizacji

Czy w rezultacie technologia ma całkowicie zastąpić człowieka? Patrząc na dynamiczny rozwój pojazdów autonomicznych, mam wątpliwości co do celów podobnych „misji".

Przenosząc to na własne profesjonalne podwórko, uważam, że zawsze za bezpieczeństwem będzie stał człowiek – jednak będzie to człowiek w pełni świadomy tego, co robi i jaką wartość dodaną wytwarza. Ponadto żyjący w pełnej symbiozie z nowoczesną technologią dopasowaną do potrzeb, czego z pewnością nie da się porównać do pracownika „uzbrojonego" w kamerę, ponieważ będzie to miało znacznie szerszy wymiar.

PS. Tradycyjne „Książki meldunków" z pewnością przejdą do lamusa.

BIO

Rafał Łupkowski
Niezależny doradca w obszarze bezpieczeństwa biznesu, właściciel firmy SecurityBroker.
Pasjonat i wieloletni praktyk zarządzania bezpieczeństwem biznesu w korporacjach międzynarodowych, współtwórca Kongresu Security.

Rośnie skala nadużyć
dotykających instytucje finansowe

Nasila się zjawisko nadużyć na rynku finansowym. Każdy z respondentów tegorocznego badania „Nadużycia w sektorze finansowym”, przeprowadzonego przez EY i Konferencję Przedsiębiorstw Finansowych (KPF), został w minionych 12 miesiącach dotknięty większą liczbą nadużyć, w wyniku których poniósł większe straty finansowe.

Oeskalacji problemu świadczy fakt, że odsetek podmiotów, które straciły z powodu nadużyć więcej niż 10 mln zł, wzrósł prawie dwukrotnie (z 5 do 10 proc.) w porównaniu z 2017 r. Odnotowano także wzrost udziału spółek, które osiągnęły straty na poziomie między 1 a 10 mln zł – w tym przedziale mieściła się już co trzecia ankietowana instytucja finansowa.

Mimo że każda badana instytucja jest inna i boryka się z nieco innymi problemami w obszarze przeciwdziałania nadużyciom, wyniki badania potwierdzają, że główne wyzwania i trendy są takie same i nie ulegają istotnym zmianom na przestrzeni czasu. Nadużycia, zidentyfikowane w instytucjach finansowych w ostatnim roku najczęściej dotyczyły podstawowej działalności tych instytucji. Wszystkie banki były narażone na wyłudzenia z wykorzystaniem kart płatniczych, wszystkie firmy leasingowe na przywłaszczenia przedmiotu leasingu, a firmy pożyczkowe – na wyłudzenia pożyczek.

Banki

Zjawisko nadużyć w bankach było większe niż przed rokiem. Każde z wskazywanych przez banki rodzajów wyłudzeń występowało częściej niż w 2017 r. W poprzednim badaniu najczęściej wskazywanym przez respondentów nadużyciem były wyłudzenia kredytów, natomiast w tym roku są to właśnie wyłudzenia z użyciem kart płatniczych. Z tym rodzajem nadużycia miały do czynienia wszystkie ankietowane banki! Aż 86 proc. uczestniczących w badaniu spotkało się z wyłudzeniami kredytów i nieautoryzowanymi transakcjami. Podobnie jak przed rokiem najrzadziej spotykanymi w bankach były nadużycia wewnętrzne, choć i tak zaobserwowano ich wzrost o 11 punktów procentowych.

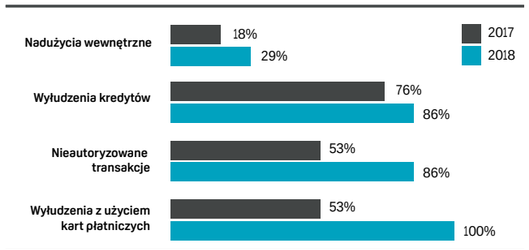
Wspólny problem – cyberprzestępczość

Niemal co drugi respondent był przynajmniej raz narażony na straty wynikające z cyberprzestępczości. I chociaż odsetek ankietowanych, którzy spotkali się w ostatnim roku z cyberprzestępczością spadł (do 44 proc. w 2018 r. vs. 50 proc. w 2017 r.), nadal jest to bardzo poważne zagrożenie w sektorze finansowym. Spośród badanych organizacji największy problem mają banki. W branży leasingowej cyberprzestępczość prawie nie występuje.

Zjawisko cyberprzestępczości, choć już lepiej rozpoznane, nadal wzbudza obawy. W tym roku kolejny raz obserwujemy wzrost liczby respondentów wskazujących, że ryzyko związane z cyberprzestępczością będzie rosnąć – w 2016 r. takich odpowiedzi udzieliło 31 proc. ankietowych, w tym roku jest to już 42 proc.

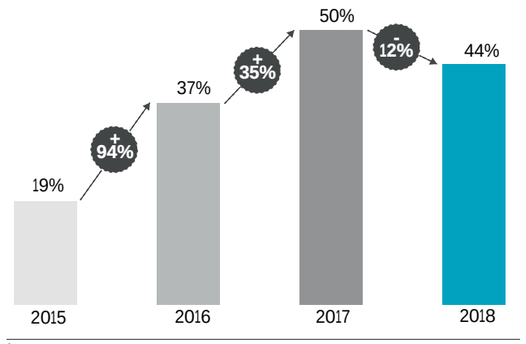
– Cyberbezpieczeństwo i socjotechnika wyłudzeń pozostają w centrum uwagi instytucji finansowych. Zdaniem szefa Bank of England, Marka Carneya, możliwą przyczyną przyszłego kryzysu finansowego będzie cyberatak, którego cel i skalę do tej pory wykluczano z rozważań. I trudno się z nim nie zgodzić – wystarczy wyobrazić sobie sytuację, gdy nie mamy dostępu do swoich pieniędzy nie w skali kraju, ale systemu. A przecież, w naszej opinii, mamy bezpieczne metody, które dają natychmiastowy dostęp do naszych pieniędzy na rachunkach bankowych. Chwalimy system bankowy za strategie cyberliderów i cyfrowych buntowników, ale jednocześnie zapominamy, że stwarzamy szanse dla cyberprzestępców na niespotykaną do tej pory skalę – podkreśla dr Mirosław A. Bieszki, doradca ds. ekonomicznych Konferencji Przedsiębiorstw Finansowych.

Odsetek banków, które spotkały się z danym typem nadużycia w ciągu ostatnich 12 miesięcy



Źródło: Nadużycia w sektorze finansowym. Raport EY i KPF.

Udział respondentów, którzy spotkali się z nadużyciem popełnionym przez cyberprzestępców w kolejnych edycjach badania (2015-2018)



Źródło: Nadużycia w sektorze finansowym. Raport EY i KPF.

DŻUNGLA MIASTA cz.2

URBAN RESILIENCE, CZYLI SWOISTY „RAPORT MNIEJSZOŚCI" ZARZĄDZANIA BEZPIECZEŃSTWEM...

To drugi z serii artykułów o bezpieczeństwie. Inspiracji do powstania cyklu dostarczył poradnik Jacka Pałkiewicza „Dżungla miasta. Klucz do bezpieczeństwa". Na łamach „a&s Polska" partneruje mu wieloletni praktyk zarządzania bezpieczeństwiem Jacek Tyburek. Wspólnie przedstawią swój punkt widzenia na bezpieczeństwo w jego różnych aspektach.

Jacek Tyburek & Jacek Pałkiewicz

W obszarze bezpieczeństwa miast pojawia się metodologia pomagająca dogłębnie analizować rzeczywistość i doświadczenia, pozwalająca skutecznie przewidywać wystąpienie zagrożeń. Tym procesem jest model tworzenia strategii *urban resilience*, czyli odporności miasta.

Przekształca się również problematyka bezpieczeństwa, stanowiąca kluczową wartość w funkcjonowaniu miast. Obserwujemy zmiany w podejściu do sposobów definiowania bezpieczeństwa i metod zapewnienia jego satysfakcjonującego poziomu. Pojęcie bezpieczeństwa i jego postrzeganie ewoluuje od klasycznego zapewnienia stanu możliwie wolnego od przestępstw do tzw. *urban (city) resilience.* Termin resilience w bezpośrednim tłumaczeniu oznacza odporność, sprężystość, elastyczność, prężność, żywotność. W kontekście miast jest używany do określenia ich zdolności do odbudowy, szybkiego przywrócenia stanu sprzed kryzysu lub innych problemów przejściowych.

Koncepcja *urban (city) resilience*

Nośność tej interdyscyplinarnej idei jest na tyle duża, że doczekała się już kilku źródeł opracowania. Prace nad stworzeniem i rozwojem koncepcji odporności miasta podjęto niedawno. Niekwestionowanym liderem jest Fundacja Rockefellera i Projekt 100 Resilient Cities (100RC) oraz współpracująca z nią firma Arup. Nie są to jedyne organizacje zajmujące się tym zagadnieniem.

Wśród innych podmiotów należy wymienić:

- ICLEI (*Local Governments for Sustainability*) – inicjatywa skupiająca 1500 miast i regionów na całym świecie, skoncentrowana na idei zrównoważonego rozwoju (http://resilient-cities.iclei.org/);
- UNISDR (*United Nations International Strategy for Disaster Reduction*) – realizuje program *Making Cities Resilient* (https://www.unisdr.org/we/campaign/cities);
- Grosvenor – jedna z największych na świecie firm branży zajmująca się obrotem nieruchomościami; w 2014 r. przygotowała raport na temat miejskiej odporności;
- BuroHappold Engineering – międzynarodowa firma inżynieryjna dostarczająca rozwiązania m.in. dla miast; w 2016 r. opublikowała raport nt. aglomeracji miejskich;
- British Standard Institution pracujący nad rozwinięciem standardu *City Resilience* (https://www.bsigroup.com/en-GB/our-services/events/2016/City-Resilience-Workshops-/).

Definicje opracowane przez organizację Projekt 100 Resilient Cities (100RC) we współpracy z firmą Arup określają odporność miasta jako *zdolność jednostek, społeczności, instytucji, przedsiębiorstw oraz systemów funkcjonujących w mieście do przetrwania (...) sytuacji trudnych, stresowych lub kryzysowych bez względu na stopień ich dolegliwości.* Takie ujęcie tematu wywołuje skojarzenia z systemem zarządzania kryzysowego znanego z procedur zarówno państwowych, miejskich, jak i obowiązujących w większych organizacjach biznesowych. Jest jednak znacznie bardziej kompleksowe, a zgodnie z intencjami jego autorów ma okazać się także skuteczniejsze niż obecne systemy zarządzania kryzysowego. *Urban resilience* nie jest zatem prostym rozwinięciem znanego zarządzania kryzysowego w miastach. To zupełnie nowa metoda, z wysoko rozwiniętą funkcją prewencyjną, opartą na dostępnej wiedzy i danych, poszerzanych w coraz większym stopniu. *Urban resilience* opiera się również na uczeniu się za pomocą dostępnych narzędzi, doświadczeniu oraz budowaniu skutecznych rozwiązań służących obronie przed możliwymi, szeroko rozumianymi zagrożeniami, a także szybkiemu powrotowi do codziennej działalności.

Wdrażanie koncepcji *resilience*

Koncepcja urban *resilience* znajduje się w fazie dynamicznego, lecz wciąż wczesnego rozwoju. To niewątpliwie nowatorskie rozwiązanie, w którego ramach kluczowi miejscy interesariusze podejmują wspólny wysiłek zmierzający do budowania zdolności miasta do funkcjonowania pomimo zakłóceń krótko- i średnioterminowych. Zasadniczą korzyścią wyłaniającą się z myślenia i zarządzania w kategoriach zapewnienia miejskiej odporności jest stworzenie platformy integrującej różne aspekty strukturalnego zapewnienia bezpieczeństwa miasta odpowiedzialne za to służby i podmioty. Bezpieczeństwo jest jednak tylko jednym z elementów składających się na ten model. Wdrażanie koncepcji *resilience* przejawia się bowiem w uwzględnianiu – we wszystkich kluczowych aspektach życia miasta – konieczności zapewniania jego odporności na różnorodne ryzyka i zagrożenia. W tradycyjnym ujęciu poszczególne dziedziny funkcjonowania miast stanowią zwykle zamknięte enklawy, których przedstawiciele ograniczają się często do planowania własnych działań na możliwie najwyższym poziomie, nie uwzględniając przy tym wiedzy na temat dokonań dziedzin pokrewnych. Model *resilience* pozwala zmienić to podejście, tworząc ramy dla wieloaspektowej współpracy międzysektorowej. Zarządzanie miastem oparte na koncepcji *resilience* wzmacnia również elastyczność w dostosowywaniu się do zmieniających się okoliczności i podejmowaniu nowych wyzwań. Inicjowanie działań w ramach modelu elastycznego reagowania, a jednocześnie w systemie „naczyń połączonych" pozwala również lepiej alokować środki oraz bardziej efektywnie i adekwatnie reagować na konkretne zdarzenia.

Punktami odniesienia dla podmiotów zarządzających miastem, odpowiedzialnych za wdrażanie i integrację działań zmierzających do budowania odporności miasta, są następujące założenia:

- odporność zapewnia ciągłość funkcjonowania pomimo występowania „wstrząsów i stresów" z dostosowaniem do długoterminowych zmian, pojawiających się zagrożeń i możliwości;

- odporność jest środkiem do rozwiązywania problemów – należy znaleźć odpowiedzi na pytania, dlaczego jest ona istotna, i jakie działania należy podjąć, aby uzyskać zakładany cel;
- odporność wymaga spójności działań;
- odporność jest specyficzna dla kontekstu „co?" należy zrobić, „dlaczego?" i „jak?" będzie się różnić w zależności od miejsca i czasu. Ma wymiar „twardy" (np. aspekty fizyczne i infrastrukturalne) oraz „miękki" (np. zaangażowanie społeczności lokalnej). Żaden z nich nie jest dominujący, są one równie ważne;
- odporność stanowi odpowiedź na potrzeby pojawiające się zarówno „odgórnie", jak i „oddolnie". Ze względu na to, że miejska odporność leży w interesie wszystkich mieszkańców, kluczowe znaczenie ma osiąganie oczekiwanych wyników na różnych szczeblach oraz zaangażowanie różnorodnych podmiotów;
- w pierwszej kolejności należy rozwiązywać problemy społeczne i gospodarcze, co ma sprzyjać zrównoważonemu rozwojowi;
- podczas wdrażania modelu odporności istotne są struktury i procesy, ale to zaangażowanie uczestników ma kluczowe znaczenie;
- mimo że pomiar postępów w budowaniu odporności jest trudny, to jednak niezbędny do utrzymania odpowiedniego tempa tego procesu.

Podsumowując rozważania na temat przydatności budowania odporności miast, należy podkreślić, iż *urban resilience* nie jest *de facto* nowym systemem – odgrywa raczej rolę „systemu systemów" integrującego działania podejmowane w ramach różnych dziedzin w celu uzyskania synergicznych efektów. To stanowi też realną siłę tego podejścia. Nie mamy bowiem do czynienia z kolejną próbą redefinicji podejścia – takie rewolucyjne tendencje zazwyczaj są bardzo kosztowne i jeszcze bardziej nieefektywne. Najbardziej korzystają na nich konsultanci, którzy miesiącami je wdrażają, później szacują wyniki i na końcu audytują.

Kryteria oceny odporności

W opisach koncepcji *urban resilience* zazwyczaj znajdują się określenia wskazujące na to, że korzysta ona z wielu źródeł danych oraz odnosi się do szerokiej palety pojęć i zjawisk (np. „kompleksowy", „różnego rodzaju stresy", „kryzysy bez względu na ich charakter"). Ponownie odnieśmy się do pracy wykonanej przez firmę Arup. Efektem doprecyzowania pojęcia *urban resilience* było wydanie w 2016 r. poradnika zatytułowanego *City Resilience Index. Understanding and measuring city resilience*, proponującego kryteria oceny czy pomiaru wskaźnika odporności miasta. Podstawowym celem tego dokumentu było opracowanie narzędzia umożliwiającego aglomeracjom, a właściwie osobom nimi zarządzającym, kompleksową ocenę stopnia ich odporności i funkcjonowania, a także ewentualne zidentyfikowanie tych obszarów, które wymagają poprawy.

City Resilience Index jest narzędziem dość skomplikowanym, które mimo że służy do samooceny, to wykorzystuje rozwiązania opracowane na potrzeby audytu bezpieczeństwa, z elementami oceny ryzyka.

W ramach *City Resilience Index* wyróżniono 4 obszary, 12 celów oraz 56 wskaźników służących do oszacowania miejskiej odporności. Dokument ten obejmuje łącznie 156 pytań i wskaźników. Warto się z nimi zapoznać – samorządowcy powinny zacząć od odbycia warsztatów, podczas których uczestnicy „przejdą" przez listę pytań, na które udzielą szczerych odpowiedzi. Następnie z dużym prawdopodobieństwem poproszą fachowców o wsparcie.

Odpowiedzi na poszczególne pytania pozwolą na dokonanie zarówno ilościowej oceny adekwatności stosowanych w mieście mechanizmów i procesów pozwalających osiągnąć zamierzone efekty, jak i jakościowej oceny stopnia spełnienia założeń, które do tych efektów mają prowadzić.

Zastosowania strategii *city resilience*

Pojawia się pytanie, czy jakieś miasta wdrożyły już strategię *city resilience*, choćby na poziomie deklaracji czy spisanego dokumentu. Dziedzina zarządzania jest młoda, nawet bardzo młoda, więc pytanie jest zasadne. Odpowiedź brzmi: nawet sporo i co ważne, są to różne miasta, na różnym „podkładzie" kulturowym i cywilizacyjnym, m.in. Amman, Ateny, Bangkok, Boston, Buenos Aires, Dakar, Dallas, Los Angeles, Medellín, Melbourne, Mexico City, Montreal, Nowy Jork, Oakland, Panama, Paryż, Rio de Janeiro, Rzym, Rotterdam, San Francisco, Sydney. W sumie dotychczas 49 miast – jak na kiełkującą ideę to niezły wynik. Kiedy na tej liście pojawią się polskie miasta… lub choćby z Europy Środkowo-Wschodniej?

Co w praktyce oznacza wdrożenie strategii *city resilient*? Oto, jak to wygląda w przypadku Rotterdamu i Rio de Janeiro. Mieszkańcy Rotterdamu twierdzą, że dbanie o bezpieczeństwo i odporność swojego miasta mają prawie w genach – i tak właśnie brzmi oficjalne hasło ich strategii: *Resilience is in our DNA*. Podczas jej tworzenia zdecydowano się skorzystać z metodologii opracowanej w ramach 100RC. Pozwoliło to na wskazanie sześciu obszarów, dla których zdefiniowano reguły zapewnienia odporności. Są to:

- edukacja i spójność społeczna,
- przesył energii,
- dostosowanie do zmian klimatycznych,
- bezpieczeństwo cybernetyczne,
- infrastruktura krytyczna,
- zarządzanie zmianą w mieście.

Po wyszczególnieniu obszarów działania zespoły powołane do opracowania strategii odporności przystąpiły do kreślenia wizji przyszłości miasta.

Rio de Janeiro liczy niemal 7 mln mieszkańców i jest drugim co do wielkości miastem Brazylii. Podobnie jak Rotterdam, władze Rio de Janeiro postanowiły przystąpić do Projektu 100RC oraz skorzystać z zaproponowanej w nim metodologii. Do obszarów funkcjonowania miasta, które stanowią źródło największych wyzwań i powinny stać się przedmiotem rozważań oraz planowania odporności, zaliczono:

- gospodarkę wodną,
- infrastrukturę,
- spójność społeczną (budowanie poczucia wspólnoty lokalnej).

Gospodarowanie zasobami wodnymi w Rio de Janeiro wiąże się z koniecznością ciągłego mierzenia się z warunkami pogodowymi. Są one z jednej strony związane z okresowymi intensywnymi opadami deszczu, w których wyniku wzbierają płynące przez miasto rzeki odprowadzające wodę do jeziora i oceanu, z drugiej natomiast z długotrwałymi okresami suszy oraz niedoboru wody pitnej. W związku z tym projekty mające na celu tzw. zarządzanie wodą (*water management*) stanowią podstawę strategii odporności miasta.

Jeśli chodzi o drugi obszar wyzwań – infrastrukturę – należy zauważyć, że wprawdzie Rio de Janeiro w ponad 450-letniej historii przechodziło okresy burzliwego rozwoju gospodarczego, to w XX wieku nie należało już do najbardziej

Koncepcja *urban resilience* nie jest prostym rozwinięciem znanego miejskiego zarządzania kryzysowego

rozwiniętych miejsc świata i borykało się z licznymi nieprawidłowościami w funkcjonowaniu infrastruktury miejskiej. Nieskoordynowany rozwój spowodował elementarne braki w infrastrukturze sanitarnej, wodociągowej, energetycznej, a także w sferach związanych z wypoczynkiem mieszkańców. Miasto produkuje niewiele energii pozyskiwanej z paneli słonecznych, odnotowuje się w nim również znaczące marnotrawstwo wody.

Z kolei potrzeba podejmowania działań na rzecz wzmacniania wspólnoty lokalnej wynika z istniejących w Rio de Janeiro nierówności społecznych. W mieście rozwijają się strefy biedy i przestępczości, których emanacją są fawele. Ich istnienie sprawia, że kwestia społecznej spójności należy do kluczowych wyzwań.

W strategii budowania odporności miasta zostały wymienione czynniki „stresu", rozumianego jako cyklicznie występujące zjawiska niepożądane. Znalazły się wśród nich: intensywne opady deszczu; silny wiatr; fale upałów oraz miejska wyspa ciepła; podnoszenie się poziomu oceanu; epidemie; susze; problemy w ruchu drogowym (korki); katastrofy i wypadki spowodowane niewłaściwym funkcjonowaniem infrastruktury miejskiej; zachowania antyspołeczne w czasie dużych imprez; przestępstwa popełniane w przestrzeni publicznej; niedostateczny dostęp do infrastruktury sanitarnej.

Konkluzje

Model *urban resilience* łączy działania analityczne i prewencyjne z klasycznym zarządzaniem kryzysowym. Czerpie on z osiągnięć w takich dziedzinach, jak *big data* czy *smart city*, ponieważ jego funkcjonowanie jest oparte na ciągłym dostępie do informacji (danych), które we współczesnym mieście stanową olbrzymi oraz coraz trudniejszy do zarządzania i wykorzystania zasób.

Metody wdrażania strategii odporności, korzystając z doświadczeń zarządzania miastem w sytuacjach kryzysowych, zostają uzupełnione i wzmocnione poprzez systemy techniczne i zarządzania oraz wiedzę wypracowaną przez sektor prywatny.

Model odporności miast stwarza możliwość wzmocnienia ich dobrostanu poprzez lepsze zadbanie o bezpieczeństwo mieszkańców, ich majątku i miejsc pracy. Zwiększa atrakcyjność miast, które nieustannie konkurują ze sobą w wyścigu o inwestycje, kapitał, technologie i ludzkie talenty, które mogą być w sposób pełniejszy realizowane w metropoliach odpornych na wstrząsy i zagrożenia.

Czy uprawnione jest stwierdzenie, że na naszych oczach wykluwa się nowa metoda zarządzania kryzysem, a także bezpieczeństwem – technika rodem z „Raportu mniejszości"? Z pewnością nie jest to proces „zamiast", tylko „bardziej". Jak zwykle w takiej sytuacji kluczową rolę odgrywają ludzie.

Czy „kupią" nowe podejście, czy wystarczy umiejętności, wiedzy i dobrej woli, żeby podobny proces wdrożyć jako standard? Jesteśmy przekonani, że tak.

Wiek XXI i kolejne będą wiekami miast o ciężarze gatunkowym często większym od niejednego średniej wielkości państwa. Zarządzanie bezpieczeństwem takich organizmów w epoce informacji wymaga stosowania adekwatnych procedur i narzędzi.

BIO

Jacek Pałkiewicz
Reporter, jeden z najbardziej aktywnych podróżników i eksploratorów naszych czasów. Trener i twórca pierwszej szkoły survivalu w Europie. Członek rzeczywisty Królewskiego Towarzystwa Geograficznego w Londynie.
Na swoim koncie ma wiele osiągnięć i wyróżnień, m.in. odkrycie źródła Amazonki, szkolenia kosmonautów i jednostek antyterrorystycznych.
Autor ponad 40 książek i wielu publikacji w prasie międzynarodowej.

BIO

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

ONVIF Profil T

W październiku organizacja ONVIF z dumą ogłosiła, że wprowadza na rynek najnowszą specyfikację profilu T służącego do zaawansowanego przesyłania strumieniowego wideo. Nowy profil jest rozszerzeniem znanego i powszechnie używanego profilu S używanego przez rynek od 2011 r. Najistotniejszymi zmianami są wparcie kodowania H.265 – coraz częściej stosowanego formatu kompresji w branży, obsługa komunikacji dwukierunkowej audio, strumieniowanie po protokole HTTPS, konfiguracja PTZ i stref detekcji ruchu oraz zarządzanie wejściami i wyjściami alarmowymi.

Część branży w Polsce sceptycznie postrzega ONVIF. Jednym z powodów jest trwająca pamięć o problemie z kompatybilnością między wersjami ONVIF 1.01 i 1.02, który rozwiązano 7 lat temu, m.in. wprowadzając koncepcję profili. Ta pierwsza niedogodność rodzącego się standardu nieprzerwanie ogranicza wiarę w jego możliwości. Do dzisiaj zjednał sobie blisko 100 członków dostarczających na rynek ok. 10 tys. produktów zgodnych ze standardem ONVIF. Z dobrodziejstw standardu korzystają systemy rejestracji producentów kamer, których rynek zmusił do choćby częściowej otwartości na innych producentów. ONVIF-em stoi nasz rodzimy Alnet – system VMS do zarządzania strumieniami wizyjnymi.

Forum[1] zostało założone w 2008 r. przez trzech liderów rynku CCTV w celu *ułatwienia integracji różnych marek sieciowego sprzętu wideo oraz pomocy producentom, programistom i niezależnym dostawcom oprogramowania w zapewnieniu interoperacyjności produktów*[2]. Wydaje się, że po 10 latach „panowania" standardu cel można uznać za osiągnięty. ONVIF nie spoczywa jednak na laurach. Efektywne wykorzystanie zasobów dyskowych i redukcja zajętości łącza przez sieciowe systemy wizyjne zdominowały sposób postrzegania skutecznego systemu dozoru wideo. Bogate portfolio kamer o rozdzielczościach 4K i wyższych wymusiło korzystanie z nowych osiągnięć w zakresie kodowania obrazu wizyjnego, w tym H.265. Również coraz skuteczniejsza analiza obrazu dostępna w urządzeniach wymaga właściwego określenia formatu metadanych, powstałych w wyniku rozkładu obrazu wideo, i sposobu ich przesyłania. Zagrożenia cybernetyczne zmusiły producentów do aktywnego stosowania protokołu HTTPS w celu zabezpieczenia wymiany informacji między urządzeniami oraz do strumieniowania danych wizyjnych. ONVIF, rozumiejąc nowe potrzeby rynku, opracował profil T, który standaryzuje powyższe kwestie.

Profil T jest przeznaczony do systemów wizyjnych opartych na IP. Obsługuje funkcje przesyłania strumieni wizji kodowanych zgodnie z H.264 i H.265, ustawień parametrów obrazu i zdarzeń alarmowych, takich jak wykrywanie ruchu i sabotażu. Obowiązkowe funkcje urządzeń obejmują także sposób wyświetlania informacji na obrazie (ekranie) i strumieniowanie metadanych, a funkcje obowiązkowe dla klientów obejmują również sterowanie PTZ. Profil T obejmuje również wytyczne dla strumieniowania HTTPS, konfiguracji PTZ, konfiguracji regionu ruchu, wejść cyfrowych i wyjść przekaźnikowych oraz dwukierunkowego dźwięku dla zgodnych z nim urządzeń i klientów obsługujących takie funkcje.

Jak wskazuje Per Björkdahl, przewodniczący komitetu sterującego ONVIF: *Wraz z rozwojem profilu T użytkownicy mają więcej możliwości wspólnego wykorzystania profili i stworzenia najlepszego, najbardziej przyszłościowego systemu nadzoru*. Jednocześnie zastrzega, że profil T nie ma na celu zastąpienia profilu S, a jest jego naturalnym rozwinięciem. I dodaje, że koncepcja profili zakłada, iż urządzenia mogą wspierać kilka profili jednocześnie bez uszczerbku na wydajności. *JTG*

ONVIF REKOMENDUJE:

Profil S – przesyłanie strumieni wideo,
Profil G – rejestracja i przechowywanie danych wizyjnych,
Profil C – fizyczna kontrola dostępu,
Profil Q – szybsze wyszukanie urządzeń w sieci i ich konfiguracja,
Profil A – szersza konfiguracja systemów kontroli dostępu,
Profil T – zaawansowane przesyłanie strumieni wideo.

1) Określenie „Forum" jest powszechnie używane wewnątrz organizacji. Nazwa ONVIF jest akronimem pochodzącym od *Open Network Video Interface Forum* – Forum na rzecz otwartego interfejsu sieciowego wideo.

2) Informacja prasowa z 12 maja 2008 r. o powołaniu kooperacji Axis, Bosch i Sony w celu ustalenia standardu dla sieciowych produktów wideo w branży zabezpieczeń.

Powstał sojusz Open Security & Safety Alliance

Bosch Building Technologies, Hanwha Techwin, Milestone Systems, Pelco oraz Vivotek założyły Open Security & Safety Alliance – sojusz przemysłowy w odpowiedzi na rosnące znaczenie Internetu Rzeczy w branży zabezpieczeń.

fot. Bosch

Celem inicjatywy jest rozwój standardów i specyfikacji dotyczących Internetu Rzeczy (IoT), w tym także systemu operacyjnego dostosowanego do potrzeb branży, koniecznej infrastruktury IoT oraz wytycznych w zakresie bezpieczeństwa i ochrony danych.
Należący do Bosch start-up Security and Safety Things GmbH pracuje nad innowacyjną platformą IoT, z której wspólnie będą korzystać członkowie Open Security & Safety Alliance. Koalicja jest organizacją non profit.
Ta inicjatywa stanowi kamień węgielny pod budowę bezpiecznego i niezawodnego ekosystemu dla branży security. Zgromadziła producentów sprzętu, deweloperów oprogramowania, integratorów systemów, projektantów, doradców, użytkowników i inne zainteresowane strony – wyjaśnia Tanja Rückert, prezes Bosch Building Technologies. Dzięki bliższej współpracy oraz zdefiniowaniu wspólnych standardów i specyfikacji podmioty należące do koalicji mogą skoncentrować się na swojej głównej działalności. Równocześnie wspólna platforma umożliwia rozwijanie nowych aplikacji w obszarze IoT. W planach jest opracowanie definicji standardów i specyfikacji dla systemu operacyjnego dostosowanego do potrzeb branży, koniecznej infrastruktury IoT oraz wspólnych wytycznych w zakresie bezpieczeństwa i ochrony danych.
Zawiązanie współpracy podmiotów z naszej branży, świadomych konieczności standaryzacji i innowacji w naszym obszarze działania, pojawiło się we właściwym momencie. Ten kierunek musimy obrać w imieniu naszych użytkowników końcowych, którzy są ostatecznym beneficjentem oferowanych przez nas rozwiązań w dziedzinie zabezpieczeń – podkreśla Bernhard Schuster, wiceprezes Bosch Building Technologies odpowiedzialny za dystrybucję, marketing i działalność handlową firmy na świecie.

Integracja z Internetem i rozwiązania cyfrowe wymagają bliższej współpracy

Bosch Building Technologies widzi konieczność obrania nowego strategicznego kierunku dla branży zabezpieczeń, uwzględniającego rozwiązania oparte na centralizacji danych. Brak wiążących standardów branżowych uniemożliwia na razie pełną realizację nowego kierunku. Ze względu na obecność na rynku różnych systemów autorskich korzystanie z danych jest obecnie utrudnione.
Standaryzacja, integracja z Internetem i płynna współpraca umożliwią oferowanie naszym klientom innowacyjnych rozwiązań opartych na IoT, sztucznej inteligencji i wykorzystaniu danych. Nowy kierunek rozwoju wymaga standaryzacji w zakresie bezpieczeństwa i ochrony danych, powinien być konsekwentnie realizowany przez wszystkie podmioty. Inicjatywa Open Security & Safety Alliance oferuje idealne warunki ramowe umożliwiające zdefiniowanie wspólnych standardów – mówi T. Rückert.

Włączenie do inicjatywy licznych podmiotów z branży zabezpieczeń

Powołanie Open Security & Safety Alliance przez pięciu członków założycieli, którzy tworzą równocześnie radę nadzorczą koalicji, poprzedziły intensywne dyskusje pomiędzy wieloma podmiotami z branży, reprezentującymi takie segmenty jak dozór wizyjny, kontrola dostępu, ochrona antywłamaniowa czy automatyzacja budynków. Oprócz producentów sprzętu w rozmowach brali udział także dostawcy części, deweloperzy oprogramowania, integratorzy oraz dystrybutorzy i użytkownicy rozwiązań. Zainteresowanie przystąpieniem do inicjatywy *Open Security & Safety Alliance* wyraziło aż 30 firm, m.in. Ambarella, Anixter, AndroVideo, Kings Security oraz NetApp. Open Security & Safety Alliance jest otwarta na przyjęcie wszystkich podmiotów z branży zabezpieczeń i branż pokrewnych.

Ścisła współpraca z sojuszem

Z koalicją Open Security & Safety Alliance będzie ściśle współpracowała spółka Security and Safety Things GmbH (SAST), powstały niedawno start-up z siedzibą w Monachium, udostępniając jego członkom innowacyjną i kompatybilną platformę IoT. SAST pracuje obecnie nad systemem operacyjnym i cyfrową platformą handlową.

Współpraca OPTEX z głównymi dostawcami oprogramowania do nadzoru wizyjnego

OPTEX – największy na świecie producent czujek zewnętrznych – wychodzi naprzeciw potrzebom swoich klientów i nawiązuje współpracę z czołowymi dostawcami CCTV i systemów VMS oraz PSIM.

Koncepcja systemu

Przygotowane we współpracy z partnerami technologicznymi gotowe sposoby integracji ułatwią zastosowanie czujek IP OPTEX w systemach dozoru wizyjnego. Komunikacja *Power-over-Ethernet* wykorzystuje wewnętrzny protokół OPTEX – *Redwall Event Code* lub protokół HTTP. Sygnał alarmowy generowany przez czujki OPTEX może zostać użyty do sterowania kamerą IP automatycznie śledzącą ruch intruza lub do zarządzania sygnałami alarmowymi w systemie dozoru wizyjnego.

Korzyści

Użycie czujek firmy OPTEX jako uzupełnienie działania systemów dozoru wizyjnego zapewnia wiele korzyści. Czujki pozwalają na wizyjną weryfikację zdarzeń oraz kontrolę granicy chronionego obszaru niezależnie od warunków. Wpływa to na poprawę efektywności dozoru, redukując liczbę fałszywych alarmów

(wywoływanych np. przez opady atmosferyczne, słabe oświetlenie czy owady fruwające przed obiektywem kamery lub pełzające po nim) nawet o 70–80%. Ma to znaczenie szczególnie w rozbudowanych systemach, w których operator musi reagować na sygnały z wielu źródeł.

OPTEX podjął współpracę z producentami systemów telewizji dozorowej takimi jak Axis, Bosch, Exacq, Gemos, Genetec, Hikvision, Milestone, OnSSI. Informacje na temat integracji z rozwiązaniami innych producentów są dostępne na stronie www.optex-vms.com.

Security Forum by Dahua

Pierwsza edycja Security Forum by Dahua za nami. Siedmiu partnerów technologicznych i sześciu ze strony mediów oraz blisko 300 osób decyzyjnych spotkało się 29 listopada w warszawskim hotelu Airport Renaissance, aby wspólnie porozmawiać na temat bezpieczeństwa infrastruktury krytycznej.

W czasie dziewięciu prelekcji poruszono wiele tematów, które razem stanowią o poziomie bezpieczeństwa całego systemu. Nowa formuła wydarzenia opierała się przede wszystkim na zaproszeniu przez Dahua Technology do współpracy największych liderów branży. Wśród nich znaleźli się Seagate, Intel, AxxonSoft, QNAP i BFT.

Na konferencji nie mogło zabraknąć *case study*, słuchacze mieli więc okazję zobaczyć prezentację systemu ochrony granicy węgierskiej, opartego na rozwiązaniach Dahua Technology. Kristof Kralovanszky, gość specjalny z Węgier, przedstawił wymagania oraz zaimplementowane rozwiązania.

Patronat honorowy nad konferencją objęły PISA oraz IPMA Polska. Redakcja „a&s Polska" była głównym patronem medialnym wydarzenia.

Konferencja przerosła nasze oczekiwania. Bardzo wysoka jakość zarówno merytoryczna, jak i organizacyjna sprzyjały nawiązywaniu wartościowych relacji i zainteresowaniu gości produktami AxxonSoft. Bardzo ciekawa formuła. Gratuluję inicjatywy!

Paweł Trojak
Prezes Zarządu
AxxonSoft Polska

Organizując pierwsze tego typu Forum w Europie, nie spodziewałam się tak wielkiego zainteresowania ze strony Partnerów i tak ogromnej frekwencji ze strony klientów. Podjęliśmy się stworzenia nowej formuły, polegającej na zebraniu liderów branży oraz osób decyzyjnych w kwestii bezpieczeństwa różnych sektorów, takich jak hotele, placówki publiczne, służby bezpieczeństwa kraju itp.

Joanna Skarbek
Event & Training Manager
CEE& Nordic
Dahua Technology Poland

Case study to jedna z głównych wartości stanowiących o innowacyjności Security Forum by Dahua. Dlatego w trakcie prezentacji, bazując na wdrożonych już rozwiązaniach, starałem się pokazać, że technologie przyszłości, takie jak algorytmy sztucznej inteligencji, dostępne są już dzisiaj i z powodzeniem mogą być implementowane zarówno w nowych, jak i istniejących już systemach zabezpieczeń.

Maciej Pietrzak
Technical Team Leader
Dahua Technology Poland

Security Forum by Dahua to doskonała okazja do wymiany doświadczeń między liderami w branży security. Na konferencji przedstawiono gotowe rozwiązania, na podstawie stworzonych projektów.

Colin Wang
Managing Director
Dahua CEE & Nordic
Dahua Technology

Security Forum by Dahua to miejsce wymiany doświadczeń oraz prezentacji najnowszych rozwiązań, sprzętu i oprogramowania w zakresie bezpieczeństwa. Integracja systemów wymaga myślenia projektowego. Miałam ogromną przyjemność wystąpić przed liczną grupą uczestników konferencji z prezentacją na temat zarządzania projektami. Wskazałam na rolę, jaką pełnią w firmach projekty oraz jak ważna jest osoba project managera i posiadane przez nią kompetencje do zarządzania zespołem i projektem. Wiele ciekawych rozmów na ten temat odbyło się w kuluarach z osobami, których celem jest doskonalenie kultury projektowej w swojej organizacji. Świetna organizacja i interesująca warstwa merytoryczna konferencji stanowią argument do zorganizowania kolejnej edycji wydarzenia.

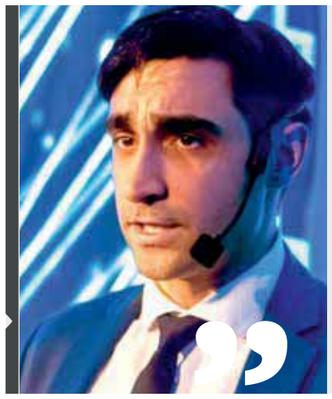
Wioletta Kastrau
dyrektor ds. rozwoju
produktów i usług
IPMA Polska

Wśród wielu jesiennych konferencji branżowych Security Forum cechowało się różnorodnością tematyki, a jednocześnie kompleksowym przedstawieniem zagadnień bezpieczeństwa. Przekaz poszczególnych prezentacji odnosił się do praktycznych zastosowań nowoczesnych technologii, co moim zdaniem znacząco podniosło wartość uczestnictwa w tym wydarzeniu. Cieszę się,że tak wiele osoób mogło się o tym przekonać osobiście.

Karol Narojczyk
Marketing Manager of CEE & Nordic
Dahua Technology Poland

Bartłomiej Stępień
Business Development Representative
Qnap

Dzięki konferencji Security Forum by Dahua mieliśmy okazję poznać wielu partnerów z Polski i Europy. Konferencja była dobrze przemyślana, na bardzo wysokim poziomie. Mieliśmy możliwość zaprezentować rozwiązania storage na naszym stanowisku oraz podczas prelekcji, która cieszyła się dużym zainteresowaniem słuchaczy.



Security Forum by Dahua 2018 to inspirujące miejsce, by dzielić się wiedzą i doświadczeniem z bezpośrednio zainteresowanymi stronami branży security. To doskonała okazja do omówienia przyszłości systemów wizyjnych i sztucznej inteligencji w segmencie transportu oraz tego, w jaki sposób Intel pomaga partnerom w osiągnięciu wyjątkowej wydajności systemu i skróceniu czasu wprowadzania na rynek.

Syamak Nazary
Global Sales Director Transportation
Intel

Security Forum by Dahua to nowa formuła, dużo spotkań i miejsce wymiany doświadczeń. Prezentowałem zapory antyterrorystyczne pozwalające sterować ruchem samochodowym, ale przede wszystkim skutecznie zabezpieczyć przed wjazdem niepożądanych pojazdów. Nowe zapory posiadają niezbędne certyfikaty przyznane przez niezależny instytut badawczy. W przerwach była okazja do nawiązania ciekawych kontaktów. Brawo za pomysł i organizację. Mam nadzieję, że Forum będzie organizowane cyklicznie.

Waldemar Stehbach
BFT Polska

Security Forum by Dahua to nowa forma produktu branżowego nie tylko promująca najnowocześniejsze rozwiązania technologiczne partnerów Dahua, to przeprowadzone z niespotykanym rozmachem organizacyjnym przedsięwzięcie edukacyjne skupiające nieskrywaną uwagę wielkiej grupy odbiorców. Zawartość merytoryczna niektórych prezentacji okazała się na tyle nowatorska, że wywołała żywe zainteresowanie nawet seniorów naszej branży. Trudno o lepszą rekomendację.
Jest jednak jeszcze coś ważnego. Bogata treść wymaga równie wysokiej jakości „opakowania", stworzenia jej szczególnych warunków i form przekazu. W tym dziele organizatorzy okazali się profesjonalni. Po doświadczeniach wyniesionych z tej konferencji ujawnił się nowy problem: co można zrobić, żeby dotrzymać kroku, żeby każde następne ważne dla branży wydarzenie nie było oceniane przez pryzmat tego, z czym spotkaliśmy się 29 listopada tego roku.

Henryk Dąbrowski
dyrektor
Polska Izba Systemów Alarmowych

Jermaine Campbell
Head of Surveillance Sales - Europe
Seagate Technology UK

Podczas konferencji zorganizowanej przez Dahua miałem możliwość podzielenia się z uczestnikami wiedzą o możliwościach, jakie udostępnia firma Seagate. Jak poprzez dobór odpowiednich dysków można bezpiecznie przechowywać i odzyskiwać dane. Security Forum by Dahua to niesamowita konferencja, gdzie mogłem w jednym miejscu poznać i porozmawiać z ważnymi graczami branży security z ponad 10 krajów i wymienić z nimi doświadczenia.

Dahua Forum pokazuje nam, że na rynku jest miejsce na nowe innowacyjne pomysły. Po stronnie klientów jest bardzo duże zapotrzebowanie na wiedzę popartą konkretnymi doświadczeniami lub pochodzącą z wdrożeń. Dla nas to jasny sygnał, że taka formuła się sprawdziła i warto pokusić się o kolejną edycję.

Andrzej Jarzyna
Sales and Operations Director CEE&Nordic
Dahua Technology Poland

Gratuluję organizatorom konferencji. Jest to niewątpliwie nowa inicjatywa, zorganizowana bądź co bądź przez producenta rozwiązań technicznych. Bardzo dobrze oceniam prezentacje, moją uwagę przykuła prelekcja Seagate dotycząca dysków ze względu na ewidentną potrzebę użycia i rozumienia systemów zapisu. A ponieważ dane są coraz istotniejsze, stąd i storage będzie coraz ważniejszy.

Jan T. Grusznic
z-ca redaktora naczelnego
a&s Polska

Kristof Kralovánszky

Wydarzenie było wspaniałą okazją dla naszych aktualnych i przyszłych klientów do zdobycia ogromnej wiedzy specjalistycznej, jaką Dahua posiada w bardzo szczególnych dziedzinach, takich jak ochrona granic państwowych i deep learning w połączeniu ze sztuczną inteligencją w pełni zintegrowanych rozwiązaniach inteligentnego miasta. Opinie naszych gości dowiodły, że dzielenie się doświadczeniem i pokazywanie naszych prawdziwych możliwości za pomocą technologii i wiedzy jest najlepszym sposobem na dalszą współpracę.

Schrack Seconet Polska
ul. A. Branickiego 15
02-972 Warszawa
http://schrack-seconet.pl

Schrack Seconet i Partnerzy

Ogólnopolskie Dni Zintegrowanych Systemów Bezpieczeństwa Pożarowego – VII edycja

W dniach 25-26 października w hotelu Windsor w Jachrance odbyła się VII edycja Ogólnopolskich Dni Zintegrowanych Systemów Bezpieczeństwa Pożarowego – Schrack Seconet i Partnerzy. W dwudniowym szkoleniu wzięła udział rekordowa liczba uczestników: ponad 580 osób! Organizatorzy zapewnili możliwość udziału w wydarzeniu również tym, którzy nie mogli osobiście pojawić się na miejscu – przez dwa dni była prowadzona transmisja LIVE w Internecie. Zgodnie z wcześniejszymi zapowiedziami przygotowano także wiele nowości i udoskonaleń w formule spotkania.

Dwa dni merytorycznych spotkań były doskonałą okazją do zapoznania się z najnowszymi rozwiązaniami technologicznymi w zakresie systemów i urządzeń stosowanych w obiektach budowlanych oraz aktualnymi wytycznymi w zakresie ich projektowania, instalacji i eksploatacji. W przyjętej formule analizy konkretnych studiów przypadku zwracano szczególną uwagę na współdziałanie urządzeń i systemów podczas normalnej eksploatacji oraz wystąpienia zdarzenia niebezpiecznego, takiego jak alarm pożarowy czy atak terrorystyczny. Analizując poszczególne przypadki, eksperci koncentrowali się na kluczowych kwestiach ważnych zarówno dla inwestora, jak i projektanta oraz instalatora na całym etapie „życia" projektu.

Wszystkie wystąpienia stanowiły uzupełnienie i komentarz do pokazu zadziałania zintegrowanych ze sobą urządzeń, a podsumowanie każdego studium przypadku kończyła dyskusja ekspercka. Zespoły specjalistów i ekspertów dokonały analizy przypadków zastosowania urządzeń służących ochronie zdrowia, życia i mienia (w tym procesów technologicznych) w obiektach różnego przeznaczenia, m.in. w obiekcie wielofunkcyjnym (hotel, biura, galeria handlowa, parking), szpitalu oraz obiekcie przemysłowym. W drugiej połowie każdego dnia szkolenia uczestnicy mieli okazję brać udział w sesjach warsztatowych, w trakcie których bardziej szczegółowo omawiano rozwiązania poszczególnych Partnerów, wcześniej zaprezentowane podczas studium przypadku. Zajęcia odbywały się w dwunastu salach równolegle!

Podczas dwóch dni spotkań z najlepszymi ekspertami w branży słuchacze zapoznali się z najnowszymi wytycznymi dotyczącymi projektowania, instalacji oraz użytkowania m.in. takich systemów, jak SSP, DSO, SUG, BMS, SMS, CCTV (VSS), SKD, systemów interkomowych oraz interkomowo-radiokomunikacyjnych, systemu integrującego urządzenia przeciwpożarowe (SIUP), dynamicznego oświetlenia ewakuacyjnego (DOE), systemów przyzywowych i komunikacji, systemów kontroli rozprzestrzeniania się dymu i ciepła, systemów i urządzeń sterujących oddzieleniami pożarowymi i innymi instalacjami technicznymi obiektu.

Udział w dwudniowych warsztatach zostanie potwierdzony wspólnym certyfikatem wystawionym przez Schrack Seconet Polska oraz Partnerów spotkania. Otrzymanie dokumentu z kompletem podpisów producentów jest uzależnione od udziału uczestnika w poszczególnych sesjach szkolenia.

Schrack Seconet Polska w imieniu swoim oraz tegorocznych Partnerów projektu składa serdeczne podziękowania wszystkim prelegentom, uczestnikom, przedstawicielom instytucji oraz uczelni technicznych, patronom merytorycznym i medialnym. Organizatorzy dziękują Partnerom projektu za wspólną, wielotygodniową pracę nad całokształtem szkolenia.

Firma Schrack Seconet Polska już dziś zaprasza do udziału w kolejnej edycji Ogólnopolskich Dni Zintegrowanych Systemów Bezpieczeństwa Pożarowego 2019. Termin zostanie podany na początku przyszłego roku.

PARTNERZY TECHNOLOGICZNI:
Belimo, Cobs, Dekk, Gazex, Hikvision, Hybryd, Nedap, Novatel, Smay, VTT

WSPARCIE MERYTORYCZNE:
ARDOR, Instytut Bezpieczeństwa Pożarowego NODEX, Instytut Bezpieczeństwa RESCON

Hanwha Techwin Roadshow

Firma Hanwha Techwin Europe (dawniej Samsung Techwin Europe) zorganizowała w październiku kolejną podróż z nowościami po Polsce. Podczas jesiennego cyklu spotkań pod nazwą „Wisenet Roadshow 2018" przedstawiciele polskiego oddziału odwiedzili Warszawę (16.10), Gdańsk (18.10), Kraków (23.10) i Poznań (25.10).

Na spotkaniach prezentowano działanie urządzeń znanych z najwyższej koreańskiej jakości. Piotr Rogalewski z polskiego oddziału Hanwha Techwin omawiał m.in. nowe funkcje oprogramowania Wisenet Wave do zarządzania systemami dozoru wizyjnego i kontroli dostępu, które działa na systemach Windows, MAC i Linux. Przedstawił rozwiązania Hanwha Techwin dla handlu i transportu, w których zastosowano technologię sztucznej inteligencji. Zaprezentował najnowsze kamery wieloprzetwornikowe oraz kamery termowizyjne z wbudowaną analityką obrazu. Omówił także funkcję *Extra-LUX*, umożliwiającą odwzorowanie kolorów nawet przy bardzo słabym oświetleniu sceny, np. w nocy.
Całość uzupełniały pokazy sprzętu na żywo, wystąpienia gości specjalnych i praktyczne informacje z zakresu stosowania nowych regulacji RODO w systemach telewizji dozorowej.

Ogólnopolska Konferencja i Szkolenie Projektowe Honeywell

Firma Honeywell Fire and PA/VA Solutions na początku listopada zorganizowała ogólnopolskie szkolenie projektowe systemów sygnalizacji pożarowej ESSER by Honeywell oraz konferencję z prelekcjami ekspertów, które odbyły się w Wyższej Szkole Menedżerskiej w Warszawie.
Prelekcje prowadzili m.in. Marcin Cichy, Jarosław Kraszewski, Maciej Żawrocki, Piotr Gronek, Andrzej Obłój oraz przedstawiciele CNBOP i VdS. Wywiązała się ciekawa dyskusja na temat nowych norm w systemach sygnalizacji pożarowej (PN-EN 54-22: *Liniowe czujki ciepła*, PN-EN 54-23: *Sygnalizatory optyczne*, PN-EN 54-27: *Kanałowe czujki dymu oraz* TS 54-32: *Dźwiękowe systemy ostrzegawcze*). Rozmawiano też o zasadach opracowywania rozwiązań zamiennych w ochronie ppoż.
Podczas trzech dni dostępna była też część wystawowa partnerów, którzy prezentowali nowości produktowe z zakresu systemów zabezpieczeń i automatyki budynkowej. Na stoiskach można było obejrzeć rozwiązania z działów automatyki budynkowej, bezpieczeństwa i sygnalizacji pożarowej Honeywella, a także firm Belimo, CenterLine, Merawex, Partner, TAP, Technokabel oraz Xtralis.

RetailShow – targi i konferencja dla handlu

Targi RetailShow są największą imprezą dla sektora handlu detalicznego w Polsce. Tegoroczna, dziewiąta już edycja, odbyła się w połowie listopada 2018 r. w Warszawskim Centrum EXPO XXI.
Podczas 2 dni targowych ponad 200 firm z Polski i ze świata zaprezentowało ofertę z zakresu m.in. projektowania sklepów, mebli i wyposażenia, kas fiskalnych i wag, systemów informatycznych do zarządzania sieciami handlowymi i systemów zabezpieczeń.
Na targach po raz kolejny, co jest już ich wyróżnikiem, zbudowano modelowy sklep – The Perfect Store, w którym można było poznać trendy projektowe, porównać najnowsze urządzenia i wyposażenie dla handlu. Rozwiązania branży security dla tego sektora prezentowały m.in. firmy Bosch Securty Systems, American Security Polska, Checkpoint, Gunnebo, Koncept-L, Nova, SkyNet i Unicard.
W zaaranżowanym na targach Modelowym Sklepie panował ciągły ruch. Wyposażony w innowacyjne produkty nowoczesny market spożywczy stanowił świetną platformę do rozmów biznesowych. Był przeglądem najciekawszych nowości z oferty wystawców.
Targom towarzyszyła konferencja Retail Congress oraz warsztaty i prezentacje w Retail Innovations Theatre, a także konkursy: Innowacje Handlu oraz Best Shop Concept – oficjalne wręczenie nagród odbyło się podczas RetailShow Afterparty.
Zwycięzcą konkursu za produkt *Inteligentna półka* w kategorii Projekty i wyposażenie wnętrz sklepowych została firma: Modern-Expo.

Konferencja KRONOS POLSKA

Firma Kronos Polska, oferująca rozwiązania dla agencji ochrony, już po raz szósty zorganizowała doroczną konferencję poświęconą najnowszym rozwiązaniom dla tego sektora. Tegoroczna edycja odbyła się w połowie listopada w hotelu Arche w Częstochowie. Jej współorganizatorami były firmy: CBC Polska, Fibar Group, ICS Polska, Linc Polska, NSS i Toyota Carolina Bielsko.
W trakcie wykładów prowadzonych przez ekspertów branży ochrony, m.in. Daniela Kamińskiego z ALERTCONTROL i Marcina Kamieniorza z ING Banku Śląskiego, omówiono trendy na rynku ochrony oraz nowe aplikacje biznesowe. Wystąpienia wzbogaciły prezentacje firmowe współorganizatorów konferencji.
Bartłomiej Dryja przybliżył gościom tegoroczne nowości wprowadzone w systemie Kronos. Rozwiązania z zakresu teleopieki przedstawiła Ewa Zagrabska, a możliwości współpracy systemu Kronos z urządzeniami inteligentnego domu Fibaro zaprezentował Sławomir Piela.
Odbyły się również pierwsze „Mistrzostwa Polski w wykorzystywaniu możliwości systemu KronosNET", w których główną nagrodą był przelot szybowcem nad Tatrami z Sebastianem Kawą, mistrzem świata w szybownictwie. Do rywalizacji stanęli przedstawiciele trzech firm: Electronics Box, Rossmann i Era. Zaszczytny tytuł Mistrza zdobył Tomasz Wypych z firmy Rossmann – gratulujemy!
Konferencję uświetnił wieczór z Marcinem Podlińskim, Sushi Masterem topowej restauracji Sakana. Dodatkową atrakcją były jazdy testowe nowym modelem Lexusa RX 300.

Nowy *bullet* z górnej półki

Odkąd monitoring wizyjny stał się niemal niezbędnym źródłem danych w ramach czynności dochodzeniowo-śledczych, firmy prześcigają się w tworzeniu nowych systemów obserwacji i analiz wideo, skrojonych na miarę potrzeb służb. Rynek w Europie i w Polsce stał się polem ostrej konkurencji z producentami z Chin. Lepiej jednak, aby w tak krytycznej dla bezpieczeństwa publicznego sferze wygrywały jakość i gwarancja skutecznego serwisu, a nie cena.

Tym właśnie przekonuje do siebie nowa kamera Axis w obudowie typu *bullet*. Spośród wielu wchodzących na rynek urządzeń przeznaczonych do monitoringu wizyjnego miast, dróg, infrastruktury krytycznej czy granic, a zarazem spełniających kryteria funkcjonalności w pracach służb mundurowych na uwagę zasługują modele AXIS Q1785-LE oraz AXIS Q1786-LE. To kamery sieciowe najnowszej generacji z 32-krotnym zoomem optycznym i funkcją OptimizedIR, dzięki której całe pole widzenia pozostaje zawsze równomiernie oświetlone. Stosowane wewnętrznie i zewnętrznie umożliwiają identyfikację zdarzeń oraz scen statycznych i dynamicznych, pomagają w detekcji twarzy, identyfikacji tablic rejestracyjnych i innych szczegółowych oznaczeń, a w konsekwencji ułatwiają prawidłową analizę zdarzeń oraz rozpoznanie ich uczestników.

Zaletą tej serii jest możliwość instalacji kamery w znacznej odległości od obszaru docelowego bez straty jakości obrazowania. Monitorując np. rondo lub drogę, gdy bezpośredni montaż jest niemożliwy, kamera może być umieszczona w odległości większej niż 260 m i nadal wyraźnie pokazywać szczegóły. Drugą istotną cechą nowych kamer serii Q17 jest wytrzymałość mechaniczna – zamknięte w aluminiowej obudowie odpornej na uderzenia (IK 10) mogą pracować w szerokim zakresie temperatury (-40…60°C).

Technologia *Corridor Format* umożliwia efektywne monitorowanie z niezmienioną rozdzielczością scen pionowych, np. długich ulic, ciągów komunikacyjnych, ogrodzeń i obrzeży obiektów niż w przypadku obrazowania panoramicznego.

Dane techniczne

- Wysoka jakość przechwytywania z rozdzielczością 4 Mpix/Quad HD 1440p przy 50/60 kl./s (AXIS Q1786-LE) oraz 2 Mpix/HDTV 1080p przy 50/60 kl./s (AXIS Q1785-LE)
- Optymalizacja zasięgu do 80 m
- Klasa ochrony obudowy: IP66, IP67 i NEMA 4X oraz IK10
- Funkcje *Forensic WDR, Lightfinder* i *Zipstream*, elektroniczna stabilizacja obrazu, wykrywanie wstrząsów, *profile scen,* funkcja *defog*
- Fabrycznie zainstalowany system *AXIS Motion Guard, AXIS Fence Guard* i *AXIS Loitering Guard*
- Temperatura pracy -40…60°C

DH-HAC-ME2241C-W: kamera, czujka i odbiornik w jednym

Systemy monitoringu wizyjnego to od wielu już lat nie tylko kamery i rejestratory. Integracja różnych rozwiązań nie jest dziś zaskoczeniem, a łączenie ze sobą systemów dozoru wizyjnego, kontroli dostępu, przeciwpożarowych czy alarmowych to chleb powszedni firm integracyjnych.

Współpraca pomiędzy różnymi systemami to jedno podejście do tematu, nieco inny model stanowią urządzenia będące hybrydą kilku. Przykładem jest „kamero-czujka" Dahua DH-HAC-ME2241C-W. Model ten wyposażono w wysokoczuły przetwornik obrazu o rozdzielczości full HD i stałogniskowy obiektyw 2,8 mm (kąt widzenia 110°). Maksymalny zasięg detekcji modułu czujnika PIR wynosi 15 m przy kącie pokrycia również 110°.

Po wykryciu włamania przez PIR i XVR kamera aktywnie ostrzega o nim, sygnalizując wizualnie (intensywnym białym światłem) lub dźwiękowo (syreny). Te dwie funkcje sugerują jednoznacznie, że oprócz funkcji detekcyjnej i obserwacyjnej urządzenie zapewnia również ochronę czynną, gdyż w razie naruszenia może natychmiast nadawać stosowny komunikat, odstraszając potencjalnego intruza.

DH-HAC-ME2241C-W jest również odbiornikiem dla innych czujników Dahua komunikujących się za pomocą protokołu Airfly. Jest w stanie obsłużyć do 32 takich detektorów, transmisja sygnałów zaś korzysta z protokołu HDCVI. Biorąc pod uwagę to, że w jednej obudowie znajdują się wysokiej jakości kamera, czujka PIR oraz odbiornik sygnałów, otrzymujemy wszechstronne rozwiązanie będące ciekawą propozycją do wykorzystania tam, gdzie potrzeba kombinacji kilku systemów.

CYBERKOLONIALIZM
– o wpływie technologii na życie ludzi

Nawet XIX-wieczna rewolucja przemysłowa nie przyczyniła się w tak dużym stopniu do zmiany codziennego życia, ewolucji struktur społecznych czy uwarunkowań psychologicznych, jak współczesny postęp cybernetyczno-internetowy. Nowoczesna technologia już dawno przekroczyła granicę wieku użytkownika, teraz mierzy się z granicą czasu. Na pytanie, dokąd zmierza ludzkość pod batutą technologii w książce „Cyberkolonializm" próbuje odpowiedzieć Krzysztof Gawkowski.

Zaledwie 2 proc. ludzi na świecie, którzy mają dostęp do komputera, smartfonu czy Internetu, deklaruje, że mogłoby bez nich żyć. Dobrodziejstwa technologiczne oplotły życie człowieka jak pajęczyna, z której już dziś wydostać się jest niezwykle trudno, a za kilka lat może to być niemożliwe. Autor stawia kilka fundamentalnych pytań, m.in. czy stoimy przed kolejną fazą rewolucji przemysłowej, czy raczej jesteśmy u progu nowego etapu darwinowskiej ewolucji, czy Ziemia jest kolonizowana przez obcych, których sami stworzyliśmy. Człowiek czy maszyna – kto w tym tandemie jest kolonizatorem, a kto kolonizowanym. Jaka czeka nas przyszłość i gdzie jest nasze miejsce w cyberprzestrzeni.

Rozwój nowoczesnych technologii niesie ze sobą wiele korzyści i jeszcze więcej zagrożeń. Większość społeczeństwa na co dzień nie zastanawia się, jaki wpływ na ich na życie mają nowoczesne technologie. Myśl o bezpieczeństwie ustąpiła miejsca użyteczności, a konsekwencje rozpychających się nowoczesnych technologii stanowią realne zagrożenie.

W dobie rewolucji IT dzięki systemom zarządzania ruchem korki w mieście można zniwelować o 70 proc., a inteligentny miejski monitoring wizyjny pozwala w czasie rzeczywistym wykrywać akty wandalizmu czy kradzieży. Wyobraźmy sobie, że intruz włamuje się do systemu zarządzania sygnalizacją świetlną – oznacza to nie tylko zakorkowane miasto i olbrzymie zagrożenie życia człowieka, ale też ogromne straty finansowe w sektorach publicznym i prywatnym. W jednej chwili przyjazne miasto może przekształcić się w miasto strachu.

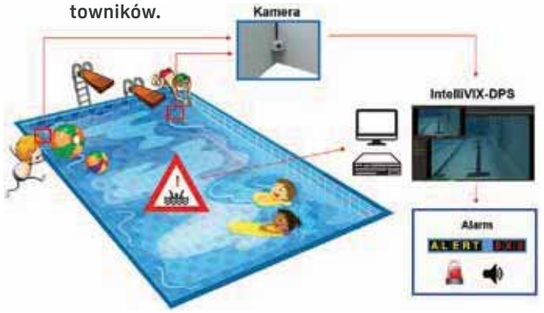
Krzysztof Gawkowski podkreśla, że szacunkowy przyrost danych w Internecie wynosi ponad 50 GB/s. W ciągu sekundy internauci pobierają ponad tysiąc aplikacji, przeprowadzają dwa tysiące rozmów na Skypie, wrzucają 5 tys. zdjęć na Instagram czy dokonują 15 tys. wpisów na Twitterze. Portale społecznościowe i informacyjne zbierają o nas wszelkie dane, później za pomocą odpowiednich algorytmów przetwarzają je tak, by w odpowiednim czasie proponować nam pralki, suszarki czy żelazka. Odbywa się handel tymi informacjami, a najbardziej zaawansowane firmy potrafią wykorzystać je np. do wpływania na decyzje wyborców. Olbrzymie zbiory danych oznaczają dziś wielkie pieniądze dla sektorów publicznego i prywatnego. Dzięki tym danym służby specjalne mogą inwigilować w zasadzie każdego obywatela, a prywatne firmy – sprzedać mu niemal wszystko.

Rozwój i dostępność technologii spowodowały, że smartfony, komputery, inteligentne domy czy samochody posiadające dostęp do sieci internetowej ułatwiają życie i niewiele osób chciałoby z tych dobrodziejstw zrezygnować. Człowiek tworzy nowe urządzenia i uważa, że to on jest władcą. Liczy się przede wszystkim użyteczność, a sprawy bezpieczeństwa są pomijane. Autor stawia tezę, że to jednak maszyna coraz bardziej zniewala człowieka. Żyjemy w świecie, którego większość z nas nie rozumie i nie wie o skomplikowanych algorytmach wpływających na nasze decyzje w prawie każdej sprawie. Człowiek zgadza się na to praktycznie bezwolnie, jednocześnie ciesząc się, jak ułatwia mu to życie.

Warto poświęcić czas na lekturę książki, która przystępnym językiem opowiada nie o przyszłości, ale otaczającej nas teraźniejszości. „Cyberkolonializm" wskazuje, gdzie czyhają niebezpieczeństwa i jak się przed nimi chronić. To książka, która nie spowoduje, że zrezygnujemy z nowoczesnych technologii, ale na pewno pozwoli zrozumieć, co może się stać, jeśli równolegle z postępem technologicznym nie będziemy myśleli o bezpieczeństwie.

Moduł analizy obrazu IntelliVIX-DPS

Firma IntelliVIX opracowała moduł analizy obrazu, wchodzący w skład pakietu IntelliVIX-DPS, który ma na celu poprawę bezpieczeństwa osób pływających w basenach.
Przypadki tonięcia i śmierci w wodzie zdarzają się niestety bardzo często, również w obiektach strzeżonych przez wysoko wykwalifikowanych ratowników.



IntelliVIX-DPS to wyjątkowe rozwiązanie inteligentnej analizy obrazu w czasie rzeczywistym. Pakiet IntelliVIX-DPS, oprócz modułu analizy obrazu, składa się z wodoodpornych kamer, tablicy elektronicznej oraz lampy ostrzegawczej z wbudowanym głośnikiem alarmowym.

Moduł IntelliVIX-DPS w czasie rzeczywistym wykrywa tonięcie obiektu i w ciągu kilku sekund powiadamia ratownika o potencjalnym zagrożeniu.

Dzięki integracji z lampą oraz dźwiękowym systemem ostrzegawczym pracownicy basenu oraz pozostałe osoby przebywające tam zauważą ostrzeżenie.

Instalacja systemu IntelliVIX-DPS znacząco zwiększa szansę na szybkie zlokalizowanie osoby tonącej oraz skuteczne udzielenie jej pomocy. Rozwiązanie to znakomicie ułatwia pracę ratownikom oraz poprawia bezpieczeństwo w tego typu obiektach sportowych.

Więcej o IntelliVIX-DPS oraz pozostałych produktach IntelliVIX:
www.intellivixeu.com
intellivixeu@intellivix.com

Ś.P. Jacek Drogosz 1945-2018 *Wspomnienie*

Z wielkim smutkiem pożegnaliśmy Jacka Drogosza, wieloletniego redaktora naczelnego czasopisma „Systemy Alarmowe", który zmarł po długiej chorobie w wieku 73 lat. Przez kilkanaście ostatnich lat nie udzielał się już publicznie – młodsze branżowe pokolenia nie miały więc szansy Go poznać.

Jacek był absolwentem i pracownikiem dydaktycznym Wydziału Elektroniki Politechniki Warszawskiej, a następnie kierownikiem pracowni w Przemysłowym Instytucie Elektroniki. Zajmował się tam czujkami zbicia szyby. Był niezwykle utalentowanym inżynierem-praktykiem, projektantem i konstruktorem zafascynowanym elektroniką, jej rozwojem i światowymi nowościami.

Całe swoje życie zawodowe poświęcił branży security. Był jednym z pierwszych producentów elektronicznych urządzeń do systemów sygnalizacji zagrożeń. Jego firma UEL-TRONIC (wcześniej znana jako PZ Converta) uzyskała w 1987 r. wpis do rejestru jednostek innowacyjno-wdrożeniowych. Bazował na własnych, oryginalnych opracowaniach, wdrożył do produkcji kilkanaście typów urządzeń: czujki, urządzenia szyfrujące, centrale alarmowe (w tym pierwsze centrale mikroprocesorowe na zamówienie MSZ dla polskich ambasad; oryginalność tych rozwiązań była istotnym czynnikiem podnoszącym poziom bezpieczeństwa), sygnalizatory, zasilacze.

Jacka poznałam w połowie lat 80., kiedy to podjął współpracę z miesięcznikiem „Elektronizacja" wydawnictwa SIGMA-NOT. W 1991 r. zarejestrowaliśmy własny tytuł „Systemy Alarmowe", rozpoczynając pionierską działalność wydawniczą związaną z branżą security. Byliśmy wtedy jednym z pierwszych niezależnych wydawców prasy technicznej w Polsce! Jackowi udało się zgromadzić w kolegium redakcyjnym grono znakomitych ekspertów i autorów, autorytety w swoich specjalnościach, którzy później, przez lata, wspierali także mnie w redagowaniu i wydawaniu „Systemów".

Poważnie traktował liczne problemy w jej rozwoju, z odwagą podejmował na łamach najtrudniejsze tematy i nowe wyzwania. Po dramatycznych, bolesnych przeżyciach osobistych w 2002 r. próbował się podnieść, jeszcze wyjechał na jesienne targi Expoprotection 2002 do Paryża i była to jego ostatnia aktywność zawodowa. Ostatecznie zamilkł, a funkcję redaktora naczelnego pełnił tylko honorowo. Czuję się niejako zobowiązana przypomnieć, jakimi problemami dzielił się z Czytelnikami „SA".

Był zafascynowany Internetem, kiedy ten dopiero raczkował, jego możliwościami i wpływem na rozwój branży. Miał w planach organizowanie branżowych targów internetowych – ten pomysł wymagał jednak dobrego wsparcia informatycznego i nigdy nie został zrealizowany. Jego pomysłem była „Wystawa internetowa" na łamach „SA" – edytorska forma marketingowa dla firm działających na rynku security. Pisał: - *Każdy sklep posiada nie tylko szyld z nazwą (logo) i zaplecze, ale również wystawę z towarami, która przyciąga uwagę i zachęca klienta do wejścia.* Zdjęcia dwóch wybranych produktów zwracały uwagę na e-wystawie tego e-sklepu.

W tzw. Dialog Box w 1994 r. tak „dialogował" z Czytelnikami: S*taramy się dostarczać Czytelnikom nie tylko wiedzę merytoryczną z zakresu szeroko rozumianych systemów sygnalizacji zagrożeń losowych i wymuszonych, ale również maksimum informacji branżowych z kraju i ze świata. Polska w przemianach w Europie miała szczególną rolę, dlatego też branża systemów alarmowych w naszym kraju rozwijała się odmiennie. Dotychczasowa, praktycznie dobrowolnie organizowana działalność stopniowo dostosowuje się do standardów europejskich. Powstało już 14 arkuszy Polskich Norm. Prezes Polskiego Komitetu Normalizacji i Miar (dzisiejszy PKN – przyp. red.) przyjął oficjalnie propozycję naszej redakcji (z 1992 r.) na opracowanie PN na systemy alarmowe zgodnych ze standardami IEC.*

Składając w 1999 r. życzenia noworoczne, dodał: *Możemy z pełnym przekonaniem stwierdzić, że nasza wspólna pionierska działalność wydawnicza ma sens. Nie tylko ukształtowała branżę i rynek security w kraju, ale kreuje ich rozwój zgodnie z tendencjami światowymi. (…) Chcemy zwrócić Państwa uwagę na nowy dział FORUM, w którym wszyscy zainteresowani mogą się wypowiadać na temat ważnych rozwiązań systemowych dla dalszego prawidłowego rozwoju branży i rynku security w Polsce. Staramy się – nadążając za dynamicznie rozwijającymi się technikami poligraficznymi – zmieniać również szatę graficzną „Systemów".*

O roli prasy technicznej pisał tak: – *Problem technicznych wydawnictw branżowych nie tkwi w ilości wydawanych tytułów. Jest o wiele poważniejszy. W artykułach merytorycznych, traktowanych przez wielu Czytelników jako materiał edukacyjny, musi być zawarta zweryfikowana wiedza branżowa. Wiele szkody może wyrządzić obszerna publikacja „o niczym", wydawca nie może polegać tylko na wiedzy autora, musi być przygotowany do jej zweryfikowania. Rzetelność i obiektywizm muszą obowiązywać każdego wydawcę.*

Ogromną wagę przywiązywał do poprawności terminologicznej: *– Poruszając obecnie problem poprawności terminologii, muszę zauważyć, że zostałem do tego niejako sprowokowany. Mając na uwadze fakt, że nad poprawnością nazewnictwa technicznego w branży pracowało od lat wiele osób, nie można się zgodzić z dziwną czasami terminologią spotykaną głównie w materiałach promocyjnych i ofertowych. W mojej ocenie pojawia się ona w wyniku nieudolnego tłumaczenia tekstów technicznych z języków obcych. (…) W tym wydaniu „SA" znajdziecie Państwo omówienie terminologii i definicji z projektu normy na systemy dozorowe CCTV.*

Jacek był jednym z animatorów rozwoju branży security w Polsce. W 1999 r. zaproponował np. zmianę algorytmu działania w usługach security (realizacji systemu zabezpieczenia technicznego): *Projektanci i instalatorzy przyzwyczajeni są do następującego algorytmu:*

- *inwestor zwraca się z problemem zabezpieczenia obiektu (przeważnie) do firmy instalatorskiej,*
- *projektant/instalator zapoznaje się z obiektem, jego planem budowlanym i wykonuje tzw. ZTE (założenia techniczno-ekonomiczne),*
- *wykonywany jest projekt wstępny i kosztorys wstępny,*
- *po uzgodnieniach strony podpisują umowę (…).*

Przedstawił optymalne wg siebie rozwiązanie: *Inwestor precyzuje (ew. z pomocą ekspertów) i przedstawia swoje Wymagania Funkcjonalne (WF) na zabezpieczenie obiektu, a projektant/instalator (wykonawca) – na podstawie tych wymagań i własnej wiedzy i doświadczenia zawodowego – opracowuje Założenia Techniczne (ZT) na system. (…) Jeżeli inwestor nie potrafi przedstawić swoich WF, pomocy powinien oczekiwać od wykonawcy. Analiza zagrożeń powinna być wykonana albo w ramach opracowania WF, albo na styku WF-ZT.*

Żegnaj, Przyjacielu…

Marta Dynakowska, redaktor naczelna „a&s Polska"
wraz z zespołem redakcyjnym

Tak powstawał czarny rynek

W dzieciństwie, w resztkach gruzów u podnóża warszawskiej Starówki, znalazłem mosiężną wojskową pieczęć pocztową do lakowania przesyłek. Ktoś z wklęsłych znaków cyrylicą odczytał słowo: „Suworow”. Ten marszałek to narodowy bohater sąsiada. Jego wojska, tłumiąc insurekcję kościuszkowską w 1794 r., wyrżnęły w pień ludność cywilną warszawskiej Pragi, jakieś 20 tys. ludzi. Namówiłem mamę, byśmy oddali archeologiczny zabytek do muzeum Warszawy. Chciałem być patriotą. Niestety muzealnego pokwitowania tego aktu w pamiątkach rodzinnych nie znalazłem.

Kto ryje w ziemi? Dzisiejsza Polska stoi wykopkami. Tak żartobliwie można określić początkowe etapy powstawania autostrad i dróg oraz inwestycji budowlanych. Pod zdejmowaną glebą zabłyszczą czasem skarby historyczne i majątkowe.

Nie jest tajemnicą, że ochronie zabytków – z punktu widzenia rozwiązań prawnych, proceduralnych i stosowania zabezpieczeń technicznych – daleko do ideału. Potwierdziły to tegoroczne wyniki kontroli NIK dot. ochrony zabytków architektury drewnianej. Teraz Izba przyjrzała się ochronie zabytków archeologicznych. Zbadano działania m.in. w 12 muzeach oraz 8 wojewódzkich urzędach ochrony zabytków. Nie ma się z czego cieszyć. Z danych konserwatorów można ocenić skalę grzebania w ziemi. Jest duża. Tylko ci kontrolowani w latach 2013-2017 wydali 26 tys. pozwoleń na prowadzenie badań archeologicznych na budowach.

A jaka jest skala znajdowania czegoś? NIK proponuje wprowadzenie spójnego systemu informatycznego do monitorowania losów takich zabytków. Po odkryciu nie są odpowiednio chronione, a nawet prawidłowo ewidencjonowane i inwentaryzowane. Blisko 1/3 skontrolowanych muzeów nie wiedziała, ile ma tych obiektów, ponieważ ich nie ewidencjonowała – niektóre, zamiast liczby obiektów przyjętych w depozyt, zapisywały liczbę decyzji konserwatora. W efekcie – w 88% sprawozdania ocenionych muzeów pokazywały nieprawdziwe dane.

I silny akcent z branży security – we wszystkich skontrolowanych muzeach znaleziono nieprawidłowości. Dotyczyły takich zagadnień, jak wdrożenie „Instrukcji przygotowania zbiorów do ewakuacji”, analizy stanu zabezpieczenia muzeum przed pożarem, kradzieżą i innymi ryzykami – brakowało planów ochrony i ich aktualizacji.

Inny temat – dawno temu w czasie mojej dwuletniej zasadniczej służby wojskowej żołnierze chronili swoje jednostki. Teraz wojsko jest tylko zawodowe i ochrona obiektów wojskowych to spory fragment rynku security. Gdzie indziej nie jest to nawet dziwne i np. amerykańskie bazy są chronione przez sektor usług security. Podobno, gdyby te obiekty chroniła sama armia, kosztowałoby to nawet 2 mld zł. W Polsce ochroną wojskowego majątku zajmują się SUFO - firm tego rodzaju jest w kraju blisko siedemset. W 2017 r. MON zapłaciło za pilnowanie 537 mln zł. Jeszcze 4 lata temu kosztowało to resort ok. połowy tej kwoty, ale wzrosły liche wynagrodzenia ochroniarzy i trochę ucywilizowano warunki pracownicze wykonywanych zamówień publicznych.

I cóż? Już polityczna mysz próbuje urodzić górę i knuje, czy nie warto powołać państwowej agencji ochroniarskiej. Te pół miliarda i fotele w zarządzającej strukturze to łakomy kąsek. W „Dzienniku Gazecie Prawnej” – opisującym tę sytuację – znalazłem wypowiedź eks-wiceministra MON od „udanej” modernizacji armii pod miłościwym parasolem ministra Antoniego – że niedpuszczalne jest, aby tak duża kwota szła do prywatnych firm ochroniarskich.

Przed gwiazdką tematów branżowych przybywa, ale czasopismo nie jest z gumy. Wybrałem ochronę informacji w samorządach. Kolejna kontrola NIK– ta była na Podlasiu – ujawniła, że elektroniczne dane o obywatelach, w tym wrażliwe, nie są bezpieczne. Mogą być w każdej chwili przejrzane, przejęte lub zniszczone. Samorządy nawet nie wiedzą, kto ma do nich dostęp, bo nie monitorują tej kwestii. Większość skontrolowanych 31 urzędów miast i gmin, starostw powiatowych i ośrodków pomocy społecznej nawet nie podejmuje działań zmniejszających ryzyko wycieku informacji. W prawie wszystkich poziom bezpieczeństwa systemów informatycznych i usług sieciowych był kiepski. Jedynie w Suwałkach autoryzację dostępu do sieci wykonano profesjonalnie, zasoby informacyjne były chronione przed nieuprawnionym dostępem, kradzieżą lub utratą, a praca sieci znajdowała się pod pełną kontrolą administratora. Dobrze że na bezrybiu chociaż pływa karp złoty. Ale ten widok pobudza apetyt.

BIO

Andrzej Popielski
Dziennikarz, fotograf. Autor felietonów o bezpieczeństwie w „Systemach Alarmowych” (w latach 2005–2015).

organizator

a&S POLSKA

Security BootCamp

Warsztaty Strategiczno-Terenowe

13-14 czerwca 2019

sprawdzimy

działanie

systemów security
w praktyce
w zespole
w terenie

W gronie najlepszych w kraju

security managerów
szefów bezpieczeństwa

odbędziemy warsztaty strategiczne
z wykorzystaniem rozwiązań security

- gra strategiczna
- scenariusze kryzysowe
- testy systemów security

szczegóły wkrótce...

informacje:
www.SecurityBootCamp.pl

30.05.2019 r.

3. MIĘDZYNARODOWA KONFERENCJA

Warsaw Security Summit

3rd INTERNATIONAL CONFERENCE

ZAPRASZA

a&S POLSKA

Więcej informacji:
www.WarsawSecuritySummit.eu

Uchwyć każdy szczegół, który ma znaczenie

Dahua prezentuje linię kamer - Machine Vision

- 20 letnie doświadczenie w pozyskiwaniu, przetwarzaniu i rozpoznawaniu obrazów
- Darmowe i łatwe w użyciu SDK z zestawem instrukcji bibliotek API dostępnych dla różnych języków programowania
- Wysoka niezawodność produktu potwierdzona testami jakości
- Nasze działy techniczne na całym świecie zapewniają dostosowanie zastosowań kamer do indywidualnych potrzeb Klienta, oraz pełne wparcie serwisowe
- Bogata oferta produktów zapewniająca skanowanie obszaru / skanowanie linii (GigE lub USB3.0) z szerokim spektrum obiektywów przy niskich zniekształceniach

CE FC ISO 9001:2000

Dahua Technology Poland Sp. z o.o.
ul. Salsy 2, 02-823 Warszawa
tel. +48 22 395 74 00, fax +48 22 395 74 10
e-mail: biuro.pl@dahuatech.com
www.dahuasecurity.com/pl