03 (45) / 2024

CZASOPISMO RYNKU SECURITY

a&S POLSKA

RAPORT: CZY SMART JEST SAFE?

Inteligentne miasta inwestują w nowoczesne technologie. Priorytetem jest bezpieczeństwo i komfort życia mieszkańców.

KAMERY NASOBNE – MOŻLIWOŚCI I OGRANICZENIA

Kamery nasobne są niezbędnym narzędziem dla służb. Pomagają w ustaleniu przebiegu zdarzenia, nagrywając materiał dowodowy.

TWIERDZA PIENIĄDZA W SERCU WARSZAWY

Nie każdy wie, że Polska Wytwórnia Papierów Wartościowych to miejsce o strategicznym znaczeniu dla bezpieczeństwa kraju.

www.aspolska.pl

20 zł
(w tym 8% VAT)

ISSN 2451-5175 05
9 772451 517703

WARSAW SECURITY SUMMIT

Największa
Konferencja
Branży
Zabezpieczeń
Nowa
Formuła

06/06/2024

Po co nam inteligentne miasta?

Odpowiedź na tytułowe pytanie jest proste: by żyło się w nim dostatniej. Wygodniej, bardziej komfortowo. I co najważniejsze – bezpiecznie.

Bieżący numer „a&s Polska" jest poświęcony zagadnieniom smart city. Jednak to kwestie szeroko pojmowanego bezpieczeństwa są obecnie znacznie bardziej palące. W raporcie pod znamiennym tytułem *Czy smart jest safe?* (str. 12) skupiamy się na zagadnieniach bezpieczeństwa polskich miast i przedstawiamy przykłady dobrych praktyk z kraju i ze świata. Bezpieczeństwo miast i infrastruktury krytycznej jest też tematem przewodnim tegorocznego wydarzenia organizowanego przez „a&s Polska", czyli Warsaw Security Summit.

Inteligentne miasta to nie tylko nowoczesne technologie i cyfryzacja usług miejskich. To także wyzwania związane z zapewnieniem bezpieczeństwa mieszkańców i infrastruktury. W dobie rosnącego zagrożenia aktami przemocy, prób sabotażu (takich jak choćby seria tajemniczych pożarów) czy katastrof naturalnych (z jednej strony susze, z drugiej – gwałtowne ulewy) kwestia ta nabiera kluczowego znaczenia. Co na jej temat sądzą eksperci z branży? (*Głos branży,* str. 32). Zgodni są co do jednego: miasta muszą być bezpieczne, przy czym samo to pojęcie ma bardzo szeroki zakres, ale priorytetem jest ochrona ludzi i infrastruktury krytycznej.

Jednym z kluczowych elementów zwiększających poziom bezpieczeństwa są zaawansowane systemy monitoringu wizyjnego do wykrywania zagrożeń. Dzięki sieci kamer, czujników i systemów analityki danych władze miast są w stanie skutecznie nadzorować sytuację i szybko reagować na potencjalne niebezpieczeństwa. Wyposażone w nie służby dostają do ręki silne narzędzie, także o znaczeniu dowodowym. Jak go nie nadużyć? Odpowiedź znajdziecie na str. 44 w artykule *Kamery nasobne – możliwości i ograniczenia stosowania*.

W przypadku wystąpienia sytuacji kryzysowej kluczowe znaczenie ma skuteczne zarządzanie i koordynacja działań ratunkowych. Inteligentne systemy zarządzania budynkami nie tylko zwiększają ich efektywność energetyczną, ale także dbają o bezpieczeństwo przeciwpożarowe i kontrolę dostępu. O tym, że bywa z tym różnie, mieliśmy okazję się przekonać podczas ostatniej serii pożarów, z których najgłośniejszym chyba był ten w Warszawie, przy ul. Marywilskiej 44. Z tematem zmierzyliśmy się w artykule na str. 54.

Najsprytniejsze systemy i najlepsze projekty nie wystarczą, jeśli najsłabszym ogniwem w łańcuchu bezpieczeństwa będzie człowiek. Skuteczne zapewnienie bezpieczeństwa mieszkańców nie jest możliwe bez ich zaangażowania. Niestety widać, że ten aspekt jest niedoceniany. Firmy szkolą ludzi, ale nie robią tego władze miast. Obrona cywilna w zasadzie nie istnieje. Oddolne ruchy, jakie zawsze pojawiają się w czasie różnego rodzaju kryzysów, nie są na dłuższą metę rozwiązaniem – warto sobie przypomnieć wielką powódź, a z tych nowszych: pomoc Ukraińcom po wybuchu wojny oraz uchodźcom na granicy z Białorusią. Władze powinny prowadzić kampanie informacyjne, uświadamiające o potencjalnych zagrożeniach oraz zasadach postępowania w sytuacjach kryzysowych. Na razie mamy alerty RCB. Czy to wystarczy?

Można by rzec: „pożyjemy, zobaczymy". Rzecz w tym, że już teraz widać, że to nie wystarcza. Na barkach ekspertów ds. bezpieczeństwa, czyli Waszych – szanowni Czytelnicy – spoczywa wielka odpowiedzialność.

Redakcja

CZASOPISMO RYNKU SECURITY

a&S POLSKA

03 (45) / 2023

SPIS TREŚCI

RAPORT: SMART CITY

PRODUKT NUMERU

SMART CITY

REDAKCJA

ADRES REDAKCJI
a&s Polska
ul. M. Rodziewiczówny 1 lok. 801
04-187 Warszawa

info@aspolska.pl
www.aspolska.pl

PREZES ZARZĄDU
Mariusz Kucharski

REDAKTOR NACZELNA
Marta Dynakowska

Z-CA RED. NACZELNEGO
Jan T. Grusznic

REDAKCJA
Monika Żuber-Mamakis
Adela Prochyra

DZIAŁ REKLAMY
Iwona Krawiec

DZIAŁ PROJEKTÓW SPECJALNYCH
Jolanta A. Kucharska
Aleksandra Czapska

CENTRUM KOMPETENCJI
Jacek Grzechowiak

KOREKTA
Jolanta Kucharska

PROJEKT GRAFICZNY I SKŁAD
Bogusław Kalwala

WYDAWCA
SENS Group Sp. z o.o.
ul. Rondo ONZ 1
00-124 Warszawa

www.sensgroup.pl

BCS FLEX

NDAA COMPLIANT

BCS-F-NVR7004-U2

- Autorskie oprogramowanie tworzone przez markę BCS
- System operacyjny Linux
- Procesory intel i5 / i7
- Obsługa 70 kanałów
- Bbrak ograniczenia dla rozdzielczości kamer
- Bitrate ograniczony interfejsem sieciowym
- Możliwość instalacji do 8 dysków o pojemności 20TB każdy
- Funkcje: eMapa, POS, analizy obrazu z kamer
- Synchroniczne szybkie odtwarzanie (4× 128)
- Odtwarzanie w podglądzie

POLSKA MARKA BCS

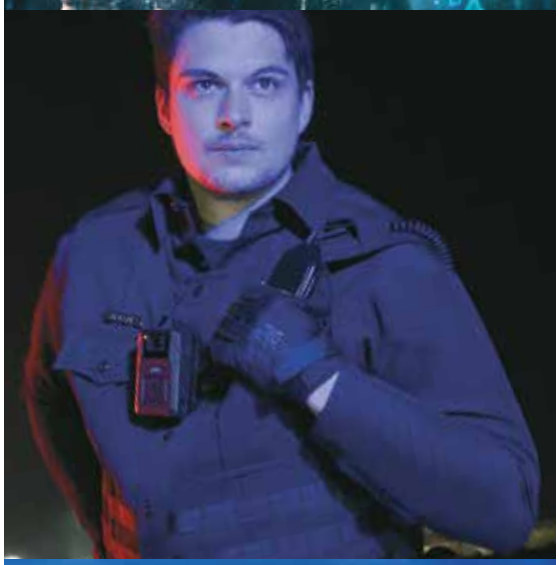
www.bcs.pl
www.facebook.com/bcspl

CZASOPISMO RYNKU SECURITY

a&S POLSKA

03 (45) / 2023

SPIS TREŚCI



ICT

ProtegeGX®

Nieograniczone możliwości rozbudowy

Zintegrowany system do kontroli dostępu, sygnalizacji włamania i napadu i automatyki budynkowej.

Nieskomplikowany w obsłudze

Prosty w integracji

Łatwy do rozbudowy

MIWI URMET Sp. z o.o.
ul. Pojezierska 90 A | 91-341 Łódź
42 616 21 00 | miwi@miwiurmet.pl

www.miwiurmet.pl

MIWI urmet

HIKVISION POLSKA

DS-2SF8C442MXG-EL – nowy model kamery PanoVu

Kamera PanoVu DS-2SF8C442MXG-EL/26(F0) jest jednym z nowych, flagowych i zaawansowanych urządzeń z oferty Hikvision.

Jest to kolejna generacja kamer łącząca moduł wieloprzetwornikowy z głowicą szybkoobrotową z 42-krotnym zoomem optycznym. Rozwiązanie tego typu doskonale sprawdza się w obiektach, które muszą być monitorowane całą dobę i potrzebują bardzo szczegółowego obrazu.

W kamerze DS-2SF8C442MXG-EL/26(F0) połączono szerokokątny obraz pochodzący z modułu panoramicznego o łącznej rozdzielczości 6 Mpix z technologią ColorVu (obraz w kolorze przed 24 godz.) z modułem szybkoobrotowym z oświetleniem IR. Istotną cechą nowej kamery jest zastosowanie bardzo wydajnego procesora dedykowanego do wspierania algorytmów głębokiego uczenia. Efektem tego jest duża uniwersalność zastosowania, za którą przemawia klasyfikacja obiektów w scenie (w zastosowaniach ochrony obwodowej) i strukturyzacja celu w module PTZ (np. robienie zdjęć osobom znajdującym się w scenie).

Kamera ma wbudowany system aktywnego odstraszania (migające światło oraz komunikaty głosowe), co zwiększa skuteczność urządzenia jako uniwersalnego środka ochrony technicznej. Kolejną istotną funkcją nowych kamer jest automatyczne śledzenie obiektów. Połączenie modułu panoramicznego, którego kąt widzenia jest bliski 180 stopni, z modułem PTZ daje doskonałe efekty podczas rozpoznawania i śledzenia obiektu w czasie rzeczywistym. Wykrycie celu następuje w module stałopozycyjnym, który następnie przekazuje sygnał alarmowy do modułu PTZ odpowiedzialnego za śledzenie obiektu.

Więcej na: www.hikvision.com/pl

LINC POLSKA

Magos | systemy radarowe – ochrona obiektów strategicznych

Radary są coraz częściej stosowane w systemach zabezpieczeń z uwagi na ich specjalne możliwości. Oferują bardzo duże zasięgi i precyzyjne wykrywanie intruza.

Radary mogą działać w trudnych warunkach niezależnie od pogody czy oświetlenia. Potrafią wykrywać człowieka, pojazd/statek na lądzie, w wodzie czy w powietrzu z odległości kilkuset metrów.

Integracja radarów z kamerami umożliwia nie tylko wykrywanie intruzów, ale także ich wideoweryfikację i śledzenie. Najnowocześniejsza technologia MASS+AI pozwala na automatyczną klasyfikację obiektów, w tym rozróżnianie ludzi i pojazdów od zwierząt. Pozwala to na generowanie tylko tych alarmów, które są istotne.

Radary idealnie sprawdzają się w zabezpieczeniu rozległych terenów, takich jak lotniska, parkingi, zaplecza techniczne, zakłady karne, zbiorniki wodne i ich ujęcia, boiska i inne otwarte obiekty sportowe, elektrownie, składy materiałów i odpadów, kopalnie odkrywkowe, centra logistyczne itp.

Doskonałym uzupełnieniem oferty Magos jest nowy model AR-300, radar 3D, który potrafi wykrywać miniaturowe drony z odległości ponad 300 m. Zastosowanie tego rozwiązania uzupełnia ochronę naziemną o zabezpieczanie przestrzeni powietrznej chronionego obiektu. Drony w niepowołanych rękach mogą wyrządzić wiele szkód. Dlatego tak ważne jest, aby mieć informację, że taki obiekt narusza chronioną przestrzeń i móc na to zdarzenie skutecznie zareagować.

Więcej na: www.linc.pl

TP-LINK

Most bezprzewodowy TP-Link Omada EAP211-Bridge

TP-Link EAP211-Bridge KIT to zestaw dwóch urządzeń mostu bezprzewodowego pozwalający na przesyłanie sygnału Wi-Fi na duże odległości. To idealne rozwiązanie np. do rozległych posiadłości z wieloma budynkami czy do obsługi systemów monitoringu na dużym obszarze.

Urządzenia EAP211-Bridge pracują w paśmie 5 GHz w standardzie 802.11ac i pozwalają na przesyłanie danych z prędkością do 867 Mb/s na odległość nawet 1 km. Każda z jednostek zestawu jest również wyposażona w 3-gigabitowe porty Ethernet umożliwiające stworzenie wydajnej sieci komputerowej, np. do obsługi kamer monitoringu.

Kierunkowe anteny o wysokim zysku 7dBi pozwalają na bezproblemową transmisję Wi-Fi nawet w najbardziej wymagających warunkach środowiskowych. Ponadto możliwość zasilania poprzez pasywne PoE (adapter znajduje się w zestawie z urządzeniem) umożliwia montaż urządzenia w miejscach, gdzie nie ma dostępu do gniazdka elektrycznego. Niezawodną pracę urządzenia w nawet najtrudniejszych warunkach środowiskowych gwarantuje odporna na warunki atmosferyczne obudowa z certyfikatem IP65 oraz ochroną odgromową 6 kV.

Wsparcie zaawansowanych funkcji, takich jak Omada Mesh, MU-MIMO, Beamforming oraz Airtime Fairness, zapewnia nie tylko doskonałą wydajność, ale także optymalizację działania sieci. Dzięki scentralizowanemu zarządzaniu w chmurze poprzez platformę Omada SDN oraz automatycznemu parowaniu instalacja i zarządzanie mostem EAP211-Bridge są niezwykle proste i efektywne, co pozwala na skoncentrowanie się na kluczowych aspektach prowadzonej działalności biznesowej.

Więcej na: www.tp-link.com/pl

camect

INTELIGENTNY REJESTRATOR
efektywna i skuteczna detekcja zagrożenia

SZTUCZNA INTELIGENCJA
wbudowana, zaawansowana sztuczna inteligencja

ROZRÓŻNIA PONAD 30 TYPÓW OBIEKTÓW
ludzi, pojazdy, zwierzęta

WSPÓŁDZIAŁANIE
z różnymi kamerami IP

KOMPATYBILNOŚĆ
z SAFESTAR

OFICJALNY DYSTRYBUTOR:

Linc Polska Sp. z o.o.
ul. Czarnkowska 22, 60-415 Poznań
tel.: +48 61 839 19 00
e-mail: info@linc.pl

www.linc.pl

WIĘCEJ O NAS:

Linc Polska Sp. z o.o.

AXIS COMMUNICATIONS

AXIS Q1806-LE – doskonały obraz z każdej odległości

AXIS Q1806-LE jest wydajną kamerą typu bullet, która oferuje jakość obrazu w rozdzielczości 4 Mpix z 32-krotnym zoomem optycznym. Pozwala to na uzyskanie doskonałych szczegółów obrazu rejestrowanych z dowolnej odległości.

Moduł przetwarzania z funkcjami opartymi na technologii głębokiego uczenia zapewnia wyjątkowe możliwości analityczne.

32-krotny zoom optyczny sprawia, że kamerę AXIS Q1806-LE można zamontować znacznie dalej od sceny, zachowując przy tym wyjątkową jakość obrazu. Kamera jest wyposażona w technologię OptimizedIR, która gwarantuje ostre i wyraźne nagrania w całkowitej ciemności na odległość do 100 m bez konieczności stosowania dodatkowego oświetlenia.

Dzięki Axis Lightfinder 2.0 kamera rejestruje obrazy o bardziej realistycznych i nasyconych kolorach oraz ostrzejsze obrazy poruszających się obiektów. AXIS Forensic WDR umożliwia rejestrację obrazów wysokiej jakości, nawet jeśli scena zawiera zarówno ciemne, jak i jasne obszary. Co więcej, optyczna stabilizacja obrazu (OIS) zapewnia stabilne obrazy nawet w warunkach słabego oświetlenia.

Zaawansowane narzędzia analityczne i inne funkcje sprawią, że sieciowa kamera AXIS Q1806-LE będzie bardziej inteligentna. W zestawie dostępne są: AXIS Live Privacy Shield, AXIS Video Motion Detection, AXIS Object Analysis. Ponadto kamera obsługuje: AXIS License Plate Verifier, AXIS Speed Monitor, AXIS Perimeter Defender. Wydajną ochronę urządzenia zapewnia oprogramowanie AXIS Edge Vault.

Więcej na: www.axis.com/pl-pl

BCS

Kamera BCS-U-SIP6436SR40-Ai2 z inteligentną analizą obrazu

Kamera BCS-U-SIP6436SR40-Ai2 jest produktem z nowej linii produktowej marki BCS zgodnej z amerykańską dyrektywą NDAA. Urządzenie zostało docenione za innowacyjność podczas targów Securex 2024, zdobywając dwa Złote Medale, jeden przyznany przez niezależnych ekspertów oraz drugi w kategorii Wybór Konsumentów.

Kamera ma 4-Mpix przetwornik, 36-krotny zoom optyczny, oświetlacz IR do 400 m i jest wyposażona w inteligentną analizę obrazu. Ponadto ma wiele funkcjonalności mających poprawić bezpieczeństwo nagrań i komunikacji z rejestratorem. Protokół komunikacyjny DirectIP 2.0 zapewnia uwierzytelnianie na podstawie certyfikatów, co znacząco zwiększa bezpieczeństwo, a także niweluje problem zastosowania zbyt prostego hasła do urządzenia.

W przypadku wystąpienia opóźnienia w transmisji danych spowodowanego chwilowym obciążeniem rejestratora lub sieci BCS-U-SIP6436SR40-Ai2 ma możliwość zapisywania danych w wewnętrznym buforze do 60 MB. W momencie powrotu sprawności zapisane dane są przesyłane do rejestratora.

Aby materiał zarejestrowany na nośniku danych był odpowiednio zabezpieczony, zastosowano funkcje zabezpieczające dane, takie jak iBank. Jest to specjalnie stworzony bazodanowy system plików, dzięki któremu pojedyncze błędy na nośniku danych nie wpływają na całe nagrania, a jedynie na ich niewielką część. Dodatkowo zaimplementowany wzorzec odcisku palca zabezpiecza nagrania przed próbami manipulacji, wysyłając ostrzeżenia do użytkownika w przypadku wykrycia braku zgodności danych. Dzięki tej funkcji nagrania uzyskują status niepodważalnych dowodów podczas spraw sądowych.

Więcej na: www.bcs.pl

&

GDE POLSKA

INVR-32P208H4 – rejestrator MAZi z detekcją ruchu 2.0 z rozpoznawaniem ludzi i pojazdów

Jedną z podstawowych funkcji rejestratorów jest detekcja ruchu. Dotychczasowe rozwiązania wykrywały każdy ruch, niezależnie od tego czy wywołał go człowiek, czy poruszające się gałęzie. Duża liczba fałszywych alarmów utrudniała przeszukiwanie nagrań.

Rozwiązanie przynoszą nowe rejestratory MAZi, np. INVR-32P208H4, które są wyposażone w zaawansowaną detekcję ruchu bazującą na uczeniu maszynowym z rozpoznawaniem ludzi i pojazdów na wszystkich kanałach. Opcjonalnie na dwóch kanałach dostępna jest detekcja przekroczenia linii oraz wtargnięcia w obszar, na jednym kanale rozpoznawanie twarzy, a na czterech porównywanie twarzy.

Dzięki rozpoznawaniu ludzi i pojazdów przeszukiwanie nagrań jest dużo łatwiejsze i szybsze, a także liczba fałszywych alarmów radykalnie mniejsza. Rozpoznawanie jest realizowane przez rejestrator, dlatego redukując koszty, można zastosować tańsze kamery bez wbudowanej analityki obrazu. INVR-32P208H4 współpracuje z kompatybilnymi kamerami o maks. rozdzielczości 8 Mpix.

Do rejestratora można podłączyć do 32 kamer 12 Mpix. Wyposażono go w dwa porty gigabitowe RJ-45, 4 porty SATA maks. 10 TB, 16 wejść i 4 wyjścia alarmowe, niezależne wyjścia HDMI 4K oraz VGA FullHD. Dodatkowym atutem jest duży strumień wejściowy 256 Mb/s. Dostępna jest także wersja 16-kanałowa o nazwie INVR-16L608H2. Wyłącznym dystrybutorem firmy MAZi jest GDE Polska.

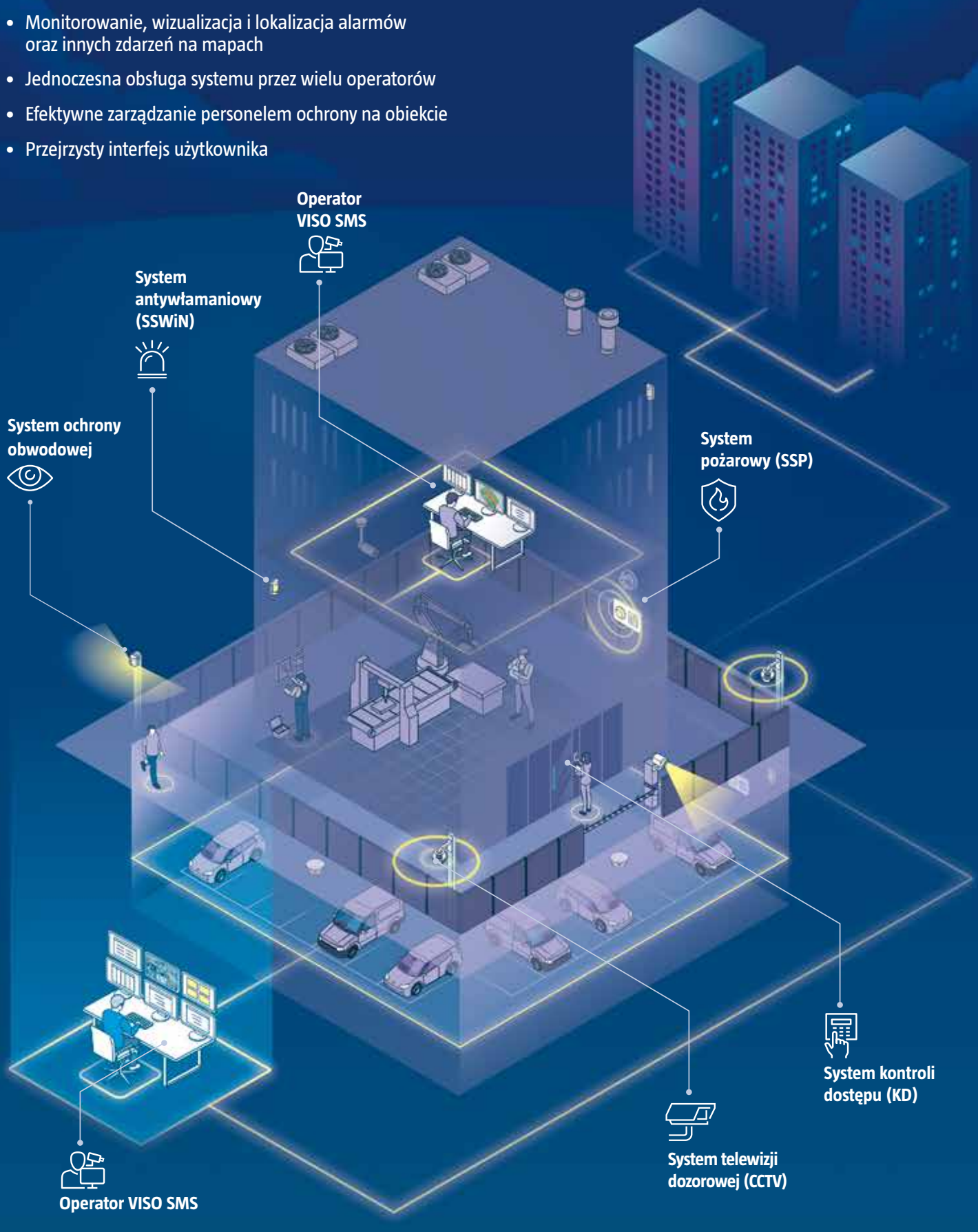
Więcej na www.gde.pl

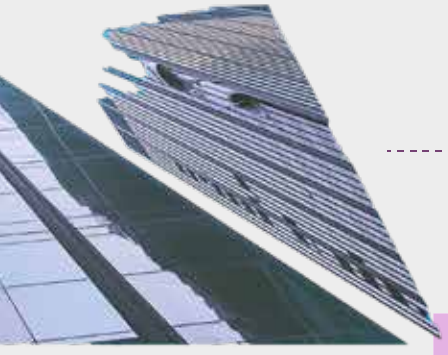
VISO SMS

Monitorowanie i wizualizacja systemów bezpieczeństwa

roger
Intelligence for Building

- Integracja z systemami Bosch, Dahua, Hikvision, Honeywell, Milestone, SATEL, Siemens i innymi w ramach jednej platformy
- Monitorowanie, wizualizacja i lokalizacja alarmów oraz innych zdarzeń na mapach
- Jednoczesna obsługa systemu przez wielu operatorów
- Efektywne zarządzanie personelem ochrony na obiekcie
- Przejrzysty interfejs użytkownika





Raport: Czy smart jest safe?

Miasto safe to miasto smart? Bieżący numer „a&s Polska” jest poświęcony zagadnieniom smart city, jednak to kwestie szeroko pojmowanego bezpieczeństwa są obecnie znacznie bardziej palące. Tym razem skupimy się na zagadnieniach bezpieczeństwa polskich miast i przedstawimy przykłady dobrych praktyk z kraju i ze świata.

Adela Prochyra

Bezpieczeństwo może być pojmowane co najmniej dwojako. W kategoriach takich jak poziom przestępczości, poziom korupcji, wiarygodność służb publicznych, infrastruktura, poziom zanieczyszczenia powietrza itd. tworzone są liczne rankingi, z których najsłynniejszym jest „Safe Cities Index"[1] promowany przez „The Economist". W jego ostatniej edycji z 2021 r. zwyciężyła Kopenhaga, a miejsca drugie i trzecie zajęły Toronto i Singapur. Wszystkie powyższe parametry, a także inne, pokrewne im, na podstawie których mierzone jest bezpieczeństwo miast, np. z perspektywy turysty, są bardzo istotne w warunkach stabilizacji. W warunkach coraz silniejszych globalnych zawirowań bezpieczeństwo miast zaczyna być rozumiane niekoniecznie jako powszechny i łatwy dostęp do służby zdrowia, ale do odpowiednio przygotowanego schronu; nie tyle jako skuteczność służb miejskich, ale skuteczność i szybkość reakcji służb na niespodziewane wydarzenia takie jak *blackout*, istotna przerwa w dostawie wody itp.

Smart w służbie bezpieczeństwa

Nawet przy tak pojmowanym bezpieczeństwie nie jesteśmy w stanie całkiem odżegnać się od materii inteligentnych rozwiązań w miastach, coraz częściej bowiem wskaźniki bezpieczeństwa mierzone są właśnie z zastosowaniem rozwiązań smart. Inteligentne rozwiązania są już dość powszechnie stosowane na świecie, jeśli chodzi o koordynowanie oświetlenia ulicznego, rozwiązania dotyczące parkowania, odbioru odpadów, monitorowania jakości powietrza i monitoringu miast inteligentnych. Zwłaszcza ten ostatni to bardzo intensywnie rozwijający się rynek – do 2028 r. ma być wart ok. 27,3 mld euro. W użyciu wciąż dominuje stacjonarna infrastruktura do monitoringu sieciowego, pomocna w wykrywaniu poszukiwanych osób lub podejrzanych o działanie na szkodę państwa, ale pojawiają się już rozwiązania takie jak kamery noszone na ciele i czujniki wykrywania strzałów jako ważne uzupełnienie działań związanych z monitoringiem miejskim.

Monitoring to także ogromna baza danych. Algorytmy stosowane w miejskich systemach monitorowania są coraz bardziej zaawansowane i są w stanie dostarczyć nieraz bardzo szczegółowe informacje. Mogą one posłużyć do przewidzenia pewnych zjawisk i podjęcia szybkich działań zaradczych w razie awarii lub kryzysu. O jakich danych mowa? Rozmieszczone bezpośrednio w miastach detektory i czujniki dostarczają – w czasie rzeczywistym lub jako podstawę do przygotowania raportów i analiz – dane dotyczące m.in.:

- natężenia ruchu samochodowego, pieszego, rowerowego,
- poziomu hałasu,
- jakości powietrza,
- pogody,
- stanu infrastruktury miejskiej,
- zużycia mediów,
- popełnianych przestępstw i wykroczeń.

Wszelkiego rodzaju mierzalne dane i sprawdzone informacje coraz częściej są wykorzystywane przez urzędników i zarządzających do podejmowania decyzji dotyczących miasta i jego mieszkańców w oparciu o fakty, a nie przekonania lub przypuszczenia. Pozwala to z dużym wyprzedzeniem planować działania na wielką skalę „na wypadek" np. braku prądu, awarii wodociągów, konieczności użycia schronów dla dużej liczby ludności.

Blackout

Jednym z bardziej realnych zagrożeń dla miast w Polsce jest *blackout,* czyli nieprzewidziana nagła przerwa w dostawie prądu na dużą skalę, której czas trwania jest trudny do przewidzenia, ponieważ czas przywracania sieci elektroenergetycznej do funkcjonowania zależy m.in. od rozmiaru awarii. Ostatni blackout w Polsce miał miejsce 8 kwietnia 2008 r. w Szczecinie. Obfite opady mokrego śniegu uszkodziły wówczas kilka linii wysokiego napięcia, w związku z czym w tysiącach domów nie było zasilania, wody i ogrzewania. Z ruchu zostały wyłączone tramwaje. Skutki dla miasta to także zamknięte sklepy i odwołane zajęcia w szkołach, zagrożenie życia i zdrowia pacjentów w szpitalach itd.

Choć przedstawiciele spółki Polskie Sieci Elektroenergetyczne zapewniają, że nie grozi nam *blackout*, należy wziąć pod uwagę to, że z roku na rok ryzyko jest większe. Czynniki, które je zwiększają to m.in.:

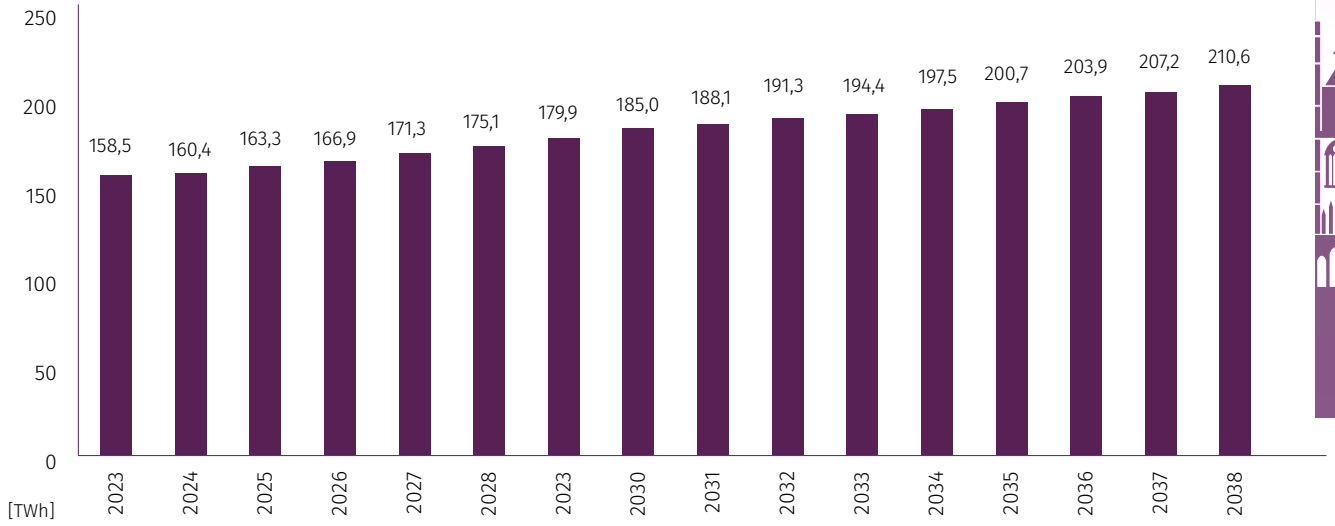
- **niedobór węgla** – ten surowiec to główne źródło energii w Polsce – odpowiada aż za 76% produkcji (dane z grudnia 2023 r.); krajowe zasoby są ograniczone, w dodatku problemy z dostępnością gazu po wybuchu wojny w Ukrainie w znacznym stopniu uszczupliły rodzime zasoby węgla;
- **wiek polskich elektrowni** – średni to 47 lat, podczas gdy średnia europejska to 35 lat;
- **nawracająca susza** – woda potrzebna jest do chłodzenia elektrowni, jednak utrzymujące się niskie poziomy rzek znacznie to utrudniają;
- **coraz większe zapotrzebowanie na energię elektryczną** – stale zwiększa się liczba urządzeń zasilanych prądem, używanych w gospodarstwach domowych oraz w miejscach użyteczności publicznej;
- **brak elektrowni jądrowej**.

„Zgodnie z Polityką Energetyczną Polski do 2040 r. budowa i uruchomienie pierwszego bloku jądrowego ma nastąpić do 2033 r." – podano w dokumencie *SPRAWOZDANIE Z WYNIKÓW MONITOROWANIA BEZPIECZEŃSTWA DOSTAW ENERGII ELEKTRYCZNEJ za okres od 1 stycznia 2021 r. do 31 grudnia 2022 r.* przygotowanym przez Ministra Klimatu i Środowiska. Polska jako pierwsza w regionie ma szansę zbudować reaktor najnowszej generacji AP1000. Program Polskiej Energetyki Jądrowej (PPEJ)

1 Indeks Bezpiecznych Miast to globalne narzędzie do porównywania polityk opracowane w celu pomiaru bezpieczeństwa w miastach. Nasz wynik indeksu opiera się na 76 różnych czynnikach w pięciu szerokich filarach: bezpieczeństwo osobiste, infrastruktura, zdrowie, bezpieczeństwo cyfrowe i środowiskowe. W ramach każdego filaru odpowiednie wskaźniki pogrupowano wg wkładów związanych z bezpieczeństwem – takich jak polityka lub personel zajmujący się pewnymi aspektami bezpieczeństwa – oraz wyników – od poziomu zanieczyszczenia powietrza po wskaźniki przestępczości. Źródło: https://impact.economist.com/projects/safe-cities/# (dostęp: 2.05.2024), tłumaczenie: Adela Prochyra.

» Inteligentne rozwiązania są już dość powszechnie stosowane na świecie, jeśli chodzi o koordynowanie oświetlenia ulicznego, rozwiązania dotyczące parkowania, odbioru odpadów, monitorowania jakości powietrza i monitoringu miast inteligentnych. Zwłaszcza ten ostatni to bardzo intensywnie rozwijający się rynek – do 2028 r. ma być wart ok. 27,3 mld euro. «

Rys. 1. Sumaryczna projekcja zapotrzebowania na energię elektryczną netto w latach 2023–38



Źródło: Minister Klimatu i Środowiska „SPRAWOZDANIE Z WYNIKÓW MONITOROWANIA BEZPIECZEŃSTWA DOSTAW ENERGII ELEKTRYCZNEJ" za okres od dnia 1 stycznia 2021 r. do dnia 31 grudnia 2022 r.

z 2020 r. zakłada budowę dwóch elektrowni jądrowych o łącznej mocy 6–9 gigawatów. Pierwsza z nich ma powstać w Choczewie na Pomorzu, a jej budowa ma ruszyć w 2026 r. W kwietniu br. rozpoczęto prace terenowe, a badania geologiczne – jeden z ważniejszych kamieni milowych – zaczną się w maju.

Blackouty dość powszechnie zdarzają się w Stanach Zjednoczonych, w Nowym Jorku są wręcz kultowym doświadczeniem społecznym. Państwa wolą im jednak zapobiegać ze względu na to, jak poważne mogą być ich skutki. Finlandia i Francja w tym celu apelują do obywateli o ograniczenie zużycia prądu, zwłaszcza w okresach zwiększonego zapotrzebowania (zwyczajowo są to okres grzewczy i upały). Francja i Wielka Brytania w sytuacji awaryjnej najpierw odcinają zasilanie w dużych firmach, a dopiero później w gospodarstwach domowych. W stosunkowo najlepszej sytuacji jest Bułgaria, której źródła pozyskiwania prądu są zdywersyfikowane – ma elektrownie atomowe, wodne oraz działające na węgiel brunatny, którego zasoby są wciąż duże. Ryzyko nagłego odcięcia prądu jest więc niewielkie. W Polsce taka sytuacja jest możliwa, gdy będziemy wygaszać energetykę opartą na węglu, a elektrownie atomowe nie będą jeszcze gotowe. Prognozy na lata 2025–30 nie są alarmujące – energii elektrycznej może brakować przez kilkanaście godzin rocznie, ale od 2030 r. może to być już nawet kilkaset godzin rocznie, gdyż zapotrzebowanie na energię elektryczną wówczas znacznie wzrośnie. Według projekcji Ministerstwa Klimatu i Środowiska zapotrzebowanie na energię elektryczną w ciągu najbliższych 15 lat wzrośnie o ponad 50 TWh – w 2024 r. wyniesie 160,4 TWh, a w 2038 r. – 210,6 TWh.

Z kolei zapotrzebowanie na moc elektryczną w tym samym okresie wzrośnie z 24,9 GW do 35,1 GW w szczycie rocznym, czyli o 40%!

Powyższe obliczenia powstały na bazie metody lat klimatycznych ENTSO-E *(European Network of Transmission System Operators*, europejskiej sieci zrzeszającej 40 operatorów sieci przesyłowych), która pozwala na odwzorowanie w przyszłości zmiennych warunków pogodowych obserwowanych w ubiegłych latach.

Krajowy System Energetyczny (KSE) staje się coraz bardziej wrażliwy na wahania pogody. Precyzyjne prognozowanie potencjalnych zdarzeń mających wpływ na bilans energetyczny wymaga uwzględnienia szerokiego spektrum możliwych kombinacji warunków klimatycznych, obejmujących zarówno normalne, jak i skrajne scenariusze.

Schrony

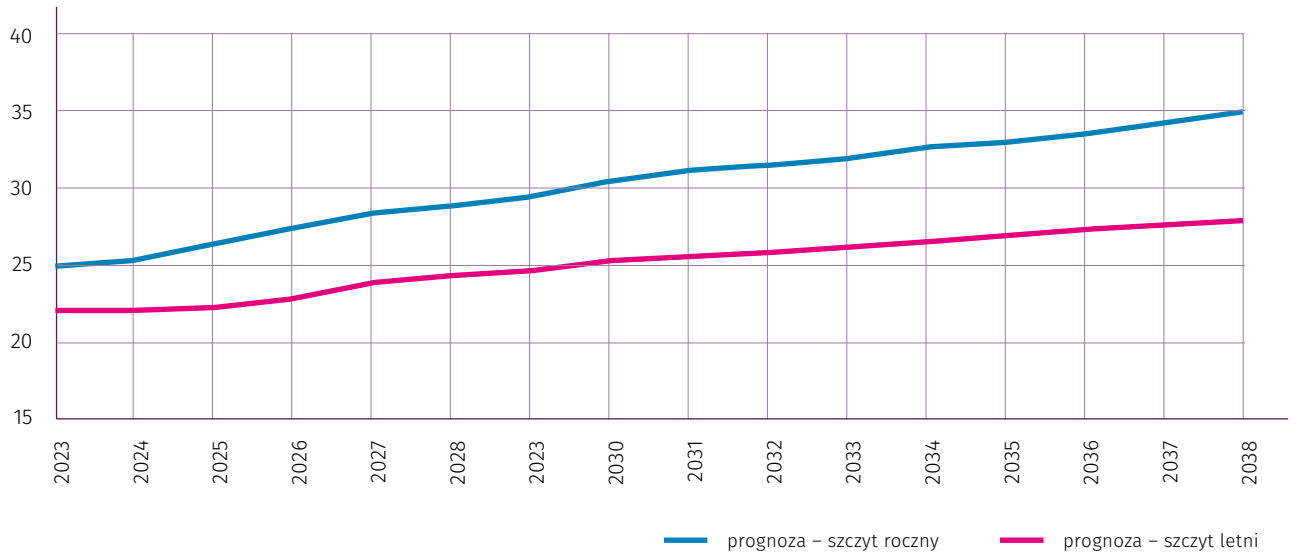
Bezpieczeństwo fizyczne ludności zależy także od niezawodnego systemu schronienia, który trzeba było w ostatnim czasie gruntownie przejrzeć i policzyć (ten temat został opisany w poprzednim numerze „a&s Polska"). Z inwentaryzacji 234 735 obiektów budowlanych na terenie kraju przeprowadzonej na początku br. przez Państwową Straż Pożarną wynika, że jako budowle ochronne, czyli schrony i ukrycia oraz miejsca doraźnego schronienia (MDS), pomieszczą one ok. 49 mln ludzi, a więc więcej niż wynosi populacja Polski. Miejsca doraźnego schronienia jednak nie spełniają podstawowych założeń schronu, czyli ochrony ludności cywilnej przed działaniem broni masowego rażenia, broni klasycznej, a także broni chemicznej, w tym m.in. broni atomowej, pocisków rakietowych, bomb lotniczych, pożarów i gruzów walących się budynków. Nic w tym dziwnego, gdyż miejsca doraźnego schronienia to piwnice, garaże podziemne, szkoły czy kościoły, czyli budowle, których konstrukcja jest na tyle odpowiednia, aby schronić się w nich np. w razie złych warunków atmosferycznych. Miejsca ukrycia z kolei to schrony niehermetyczne.

Jak można dowiedzieć się ze stron rządowych, na terenie całego kraju zewidencjonowano:

- 224 113 miejsc doraźnego schronienia (MDS);
- 10 622 budowle ochronne, w tym:
  - 903 – schrony,
  - 8719 – ukrycia.

Najwięcej obiektów zinwentaryzowano w województwach mazowieckim, niemal 30 tys., i śląskim – niemal 26 tys. Na potrzeby procesu

Rys. 2. Wyniki projekcji będące średnią arytmetyczną maksymalnych wartości zapotrzebowania na moc elektryczną w szczycie rocznym (zimowym) i letnim w latach klimatycznych 1982–2019 w okresie 2023–38



Źródło: Minister Klimatu i Środowiska „SPRAWOZDANIE Z WYNIKÓW MONITOROWANIA BEZPIECZEŃSTWA DOSTAW ENERGII ELEKTRYCZNEJ" za okres od dnia 1 stycznia 2021 r. do dnia 31 grudnia 2022 r.

» Powszechnie wykorzystywane w miastach nowoczesne rozwiązania z zakresu smart city ułatwiają codzienne życie mieszkańcom, a przy okazji dostarczają wielu istotnych informacji instytucjom państwowym i miejskim. «

inwentaryzacji została opracowana specjalna aplikacja na urządzenia mobilne (wraz z systemem opartym o serwer www) pod nazwą „Schrony". To w niej strażacy uzupełniali informacje o zinwentaryzowanych obiektach. Następnie na tej podstawie powstała aplikacja do użytku publicznego – dostępna powszechnie z przeglądarki internetowej pod adresem http://schrony.straz.gov.pl. Wskazuje ona co prawda najbliższe schrony i miejsca doraźnego schronienia, nie określa jednak, czy są one puste, czy przepełnione.

Komendant główny Państwowej Straży Pożarnej gen. brygadier Andrzej Bartkowiak podczas konferencji prasowej 6 kwietnia br. oszacował liczbę profesjonalnych, hermetycznych schronów na ok. 2 tysiące, a pojemność jako wystarczającą na schronienie dla ponad 300 tysięcy osób. – *To w pełni sprawne, hermetyczne miejsca, w których można się ukryć przed poważniejszymi zagrożeniami* – mówił. Podkreślił także znaczenie miejsc doraźnego schronienia dla bezpieczeństwa ludności. – *Zagrożeniem jest obecnie nie tylko ryzyko agresji zbrojnej na nasz kraj, ale także coraz gwałtowniejsze warunki atmosferyczne, przed którymi potrzeba schronienia* – dodał. Wiele z tych miejsc „jest w naprawdę bardzo dobrym stanie".

Jak radzą sobie z tym zagadnieniem inne kraje? Oto wybrane przykłady dobrych praktyk.

Flagowym przykładem jest Finlandia, która stale liczy się z ryzykiem rosyjskiej agresji na swoje terytorium. Ten kraj dysponuje 50 tys. schronów dla 5 mln ludzi. Cała populacja tego kraju liczy 5,5 mln. Ponadto schrony są wyposażone jak małe miasta – znajdują się w nich m.in. sale lekcyjne, siłownie, a nawet większe obiekty sportowe, np. lodowiska. Wiedza o ich rozmieszczeniu jest powszechna. Obecnie fińskie schrony stały się modelowym przykładem dla innych państw europejskich.

Ochrona cywilna w Norwegii budowana jest od 1936 r., w związku z czym jej struktura jest rozbudowana – to m.in. profesjonalny personel, siła robocza, ale też plany działania i schrony. Jej Siły Ochrony Cywilnej to służby mundurowe oparte na poborze otwartym zarówno dla mężczyzn, jak i dla kobiet w wieku od 18 do 55 lat. W czasie zimnej wojny powstał wymóg budowy schronów prywatnych – w budynkach mieszkalnych dla ich rezydentów – i publicznych – dla osób, które będą poszukiwać schronienia w przestrzeni publicznej. Odpowiadały za to władze lokalne. Od roku 1998 zaprzestano budowy nowych schronów. Obecnie ok. 25% z nich wymaga modernizacji, a w związku ze zwiększeniem się populacji kraju pokrycie zapotrzebowania wynosi obecnie 46–47%[2]. Od 2016 do 2020 r. Norwegia wdrożyła też Program Obrony Totalnej na wypadek pełnoskalowej wojny.

W roku 2012 Bartosz T. Wieliński pisał w wyborczej.pl: *Ćwierć wieku po zakończeniu zimnej wojny w Szwajcarii dalej nie wolno budować bloków mieszkalnych bez schronu atomowego w piwnicy. 300 tys. schronów rozsianych po kraju może pomieścić prawie 9 mln osób – o 1,5 mln więcej niż wynosi liczba ludności. Ich utrzymanie kosztuje fortunę*.

Od tamtego czasu sytuacja się nie zmieniła. Schrony są obowiązkowym elementem wyposażenia domów i bloków, a ich budowa jest dotowana przez rząd. Łącznie mogą pomieścić ponad 9 mln osób (dane z 2024 r.), podczas gdy populacja Szwajcarii wynosi 8,5 mln. Największym z nich jest znany na całym świecie tunel autostradowy Sonnenberg, w którym zmieści się 20 tys. ludzi.

Chyba największe wrażenie, jeśli chodzi o skalę przygotowań „na wypadek…", robi podejście Chin. Siły powietrzne Chińskiej Republiki Ludowej dysponują rozległą siecią 40 tajnych baz lotniczych ukrytych pod ziemią. Te imponujące obiekty, wykute w zboczach gór lub głęboko pod powierzchnią ziemi, skrywają nie tylko arsenał broni, ale również zapasy żywności, leków i innych niezbędnych do przetrwania środków. W magazynach tych stacjonuje także 1500 samolotów bojowych, gotowych do użycia dopiero po opadzie radioaktywnego pyłu po detonacji głowicy nuklearnej.

Podziemne bazy lotnicze stanowią jedynie fragment potężnej sieci schronów, którymi dysponuje Chińska Armia Ludowo-Wyzwoleńcza. Równie imponujący jest rozmach chińskich zabezpieczeń miejskich. Prawdziwe rozmiary podziemnej sieci bunkrów zbudowanych pod Pekinem za czasów Mao Tse-tunga pozostają tajemnicą. Eksperci szacują, że ich łączna długość sięga 4 tys. km, a całe podziemne miasto dorównuje niemal powierzchni naziemnej stolicy Chin. To imponująca skala, 32 razy większa od Warszawy!

Podziemny Pekin to prawdopodobnie największy schron atomowy na świecie, zdolny pomieścić ponad milion ludzi. Dostęp do niego zapewnia 70 tys. dróg dojazdowych prowadzących z niemal każdej uliczki miasta. Ale podziemny Pekin to nie tylko schron w dosłownym tego słowa znaczeniu. To prawdziwa aglomeracja z całą infrastrukturą niezbędną do przetrwania, obejmującą szkoły, szpitale, magazyny żywności, studnie głębinowe, linie kolejowe, magazyny samochodowe, pomieszczenia mieszkalne i administracyjne, centrum kryzysowe, a nawet centrum sztabu generalnego sił zbrojnych. Chińczycy z dumą nazywają swoją drugą stolicę Podziemnym Wielkim Murem. Ten imponujący kompleks nie jest jednak zamkniętą pułapką. Liczne tunele ewakuacyjne prowadzą na prowincję, a jeden z nich, o długości 100 km, łączy podziemny Pekin z pobliskim dużym miastem – Tiencin.

Smart and safe

Na ile bezpieczne są polskie miasta? W ramach podsumowania odpowiemy tak: powszechnie wykorzystywane w nich nowoczesne rozwiązania z zakresu smart city ułatwiają codzienne życie ich mieszkańcom, a przy okazji dostarczają wielu istotnych informacji instytucjom państwowym i miejskim. Świadomość stanu przygotowania (lub nieprzygotowania) miast na katastrofy naturalne, klęski żywiołowe czy ataki zbrojne jest dość zaawansowana – wiemy, ile energii będziemy zużywać w następnych latach i kiedy możemy spodziewać się *blackoutów*. Dramatycznie przedstawia się, zwłaszcza jak na kraj frontowy NATO, liczba schronów oraz ich stan. Gorzej od nas wypada chyba tylko Francja, jeden z najlepiej wyposażonych w reaktory jądrowe krajów, który przy okazji jest też jednym z najsłabiej wyposażonych w schrony przeciwatomowe. Jak twierdzi Artémis Protection, producent takiego sprzętu, w całym kraju jest ich nie więcej niż 1000, w tym zaledwie 600 wojskowych. Reszta to budowle prywatne.

Jak wiadomo, informacja to wiedza i władza. Pozostaje mieć nadzieję, że jedno i drugie zostanie wykorzystane w celu szybkiego nadrobienia braków. ●

2 Dane na podstawie wypowiedzi Øisteina Knudsena, szefa norweskiej Obrony Cywilnej, w programie „Skaner" InfoSecurity24.pl (dostęp: 9.05.2024).

Odporność miejska w czasach SuperVUCA

Obecnie pojęcie bezpieczeństwa miejskiego zostało zastąpione pojęciem miejskiej odporności. Jest bowiem znacznie pojemniejsze, lepiej opisujące rzeczywistą złożoność życia codziennego miast, szczególnie metropolii.

Jacek Tyburek

Zarządzanie odpornością miejską *(city resilience)* we współczesnych metropoliach to proces, który ma na celu przygotowanie miast na różne zagrożenia i wyzwania, np. zmiany klimatyczne, katastrofy naturalne, terroryzm, pandemie czy kryzysy ekonomiczne. Odporność miejska odnosi się do zdolności miasta do przeciwdziałania, absorbowania, adaptowania się i szybkiego powrotu do normalności po wystąpieniu takich zagrożeń.

Fundacja Rockefellera i 100 Resilient Cities

W roku 2013 Rockefellera powołała organizację 100 Resilient Cities, której głównym zadaniem miała być pomoc większej liczbie miast w budowaniu odporności na wyzwania fizyczne, społeczne i gospodarcze, które w XXI w. stały się częstsze, niż miało to miejsce wcześniej. Miasta należące do sieci 100RC otrzymały zasoby niezbędne do opracowania planu działania na rzecz odporności na cztery główne ścieżki:

- wytyczne finansowe i logistyczne dotyczące stanowiska Chief Resilience Officer, który powinien kierować działaniami miasta w zakresie odporności;
- wsparcie eksperckie w opracowaniu solidnej strategii odporności;
- dostęp do rozwiązań, usługodawców i partnerów z sektora prywatnego, publicznego i pozarządowego, którzy mogą pomóc w opracowaniu i wdrożeniu strategii odporności;
- członkostwo w globalnej sieci miast członkowskich, by mogły się uczyć od siebie nawzajem, ale i służyć wzajemną pomocą.

Fundacja wybrała 100 miast, w których wdrożono projekt wspólnej strategii budowania odporności. Na potrzeby niniejszego artykułu wybraliśmy kilka. Kluczem było reprezentowanie różnych kontynentów, a co za tym idzie też wielu kultur i punktów widzenia. Niestety nie ma na tej liście żadnego polskiego miasta, więc tym razem nie będziemy mogli dokonać porównania z innymi miastami. Ograniczamy się tylko do wycinka strategii, a mianowicie do zdefiniowanych kluczowych zjawisk dotyczących odporności opisanych w metodologii stworzonej przez 100RC.
Przyjrzyjmy się zatem strategiom trzech różnych pod wieloma względami miast: Rzymu, Los Angeles i Addis Abeby.

Rzym

Wszystkie drogi prowadzą do Rzymu, więc też zgodnie z logiką przysłowia prowadzą w świat. Zacznijmy więc od głównych wyzwań zdefiniowanych w strategii odporności w momencie jej publikowania w 2019 r. Zaliczono do nich:

- Wpływ recesji gospodarczej na Wieczne Miasto. Skuteczne zarządzanie wpływem, jaki globalna recesja gospodarcza miała na zatrudnienie, sieci społeczne oraz na zwiększone tendencje migracyjne.
- Wspieranie wydajnego i skutecznego zarządzania poprzez zachęcanie do lepszej komunikacji i precyzyjniejszych informacji poprzez korzystanie z mediów cyfrowych i przezwyciężenie ograniczeń spowodowanych biurokracją.
- Zapewnienie oczekiwanej jakości życia. Wspieranie dobrego samopoczucia i jakości życia, począwszy od dostępu do mieszkań, skończywszy na wydajniejszym transporcie publicznym; od projektów kulturalnych po poprawę zróżnicowania i recykling materiałów pokonsumpcyjnych.
- Zmiany klimatu. Monitorowanie i planowanie sytuacji klimatycznej oraz geologicznej wynikającej z położenia oraz przewidywanie i łagodzenie skutków zmian klimatu (wyspy ciepła, susze, powodzie, osunięcia ziemi itp.).
- Ochrona spuścizny historycznej. Ochrona, zachowanie i waloryzacja dziedzictwa kulturowego i krajobrazowego miasta poprzez zachęcanie do wprowadzania zasad zrównoważonej turystyki, rewitalizację tkanki miejskiej, zapobieganie procesom gentryfikacji.

Wymienione wyzwania postanowiono skonfrontować z 4 filarami działań, których zadaniem miało być zniwelowanie negatywnych skutków materializacji wyzwań. Zupełnie jak w klasycznej analizie ryzyka przeprowadzanej zgodnie z ISO.

Pierwszy filar „Skuteczne miasto w służbie obywatelom". W jego ramach postanowiono rozwijać takie zadania, jak utworzenie centrum operacyjnego i centrum zarządzania oraz ustanowienie biura ds. odporności miejskiej.

Drugi filar „Dynamiczne, silne i wyjątkowe miasto". Zadania szczegółowe dotyczące tego filaru zdefiniowano w następujący sposób: powołanie Specjalnego Biura ds. Tybru w celu przywrócenia rzece stanu, który umożliwiłby zarówno mieszkańcom, jak i turystom korzystanie z niej. Drugi program to ocena potencjału odpornościowego rewitalizacji dzielnic Ostiense. Kolejnym programem była zmiana postrzegania, wykorzystania i promocja archeologicznego i kulturowego dziedzictwa w Rzymie na rzecz życia mieszkańców.

Trzeci filar „Tworzenie otwartego, inkluzyjnego i wspierającego miasta". Programy mające realizować ten postulat to programy prozdrowotne, szczególnie sportowe, a także uruchomienie programu integracji społecznej dla osób ubiegających się o azyl i innych osób objętych ochroną międzynarodową.

Czwarty filar „Miasto, które chroni swoje zasoby naturalne". W jego ramach zostały uruchomione projekty służące wprowadzeniu ekologicznego transportu publicznego, a także poprawie selektywnej zbiórki odpadów.

Zaskakuje fakt, że w takim mieście jak Rzym, w głównych filarach odporności nie wskazano celów dotyczących tradycyjnie pojmowanego bezpieczeństwa. Natomiast patrząc z punktu widzenia branży security i branż pokrewnych, wdrożenie każdego z programów oznacza konieczność dopasowania technicznych i organizacyjnych rozwiązań wywodzących się z branży bezpieczeństwa. Sztandarowym przykładem jest lepsza ochrona zabytków, która ma uwzględniać to, że powinny służyć mieszkańcom.

Los Angeles

Skok za ocean do Los Angeles to wizyta w mieście doświadczanym kryzysami mającymi źródło w czynnikach naturalnych i niepokojach społecznych. Los Angeles to zupełnie inne warunki niż Rzym, stąd inne cele strategii opracowanej w marcu 2018 r. Strategia tego amerykańskiego miasta jest bardzo rozbudowana. Dokument ją opisujący został podzielony na 4 rozdziały zawierające 15 celów oraz 96 związanych z nimi aktywności.

Bezpieczni i prosperujący mieszkańcy Los Angeles to rozdział pierwszy służący podkreśleniu roli, jaką obywatele miasta, ich rodziny, firmy i właściciele nieruchomości mogą odegrać zarówno w zapobieganiu przyszłym problemom, jak i przygotowaniu się do nich. Cele ujęte w tym rozdziale dotyczą zadań edukacyjnych miasta, służących wykształceniu w mieszkańcach Los Angeles takich umiejętności, które spowodują, że będą samowystarczalni przez co najmniej od 7 do 14 dni po wystąpieniu poważnego wstrząsu. Kolejnymi celami były: rozwinięcie dodatkowych ścieżek zatrudnienia oraz dostarczenie narzędzi finansowych w celu wsparcia tych mieszkańców miasta, którzy w razie jakiegokolwiek kryzysu będą najboleśniej odczuwać jego skutki, oraz kształtowanie liderów, opieki nad środowiskiem i równości wśród młodych mieszkańców Los Angeles.

Silne i połączone dzielnice, czyli rozdział drugi, oznacza dążenie do wzmocnienia więzi społecznościowych oraz zwiększanie gotowości poprzez współpracę społeczności. Ma być więcej m.in. programów i partnerstw, które sprzyjają tworzeniu przyjaznych dzielnic. Tu znajdziemy także cel klimatyczny, czyli ochrona osób najbardziej narażonych na wzrost temperatur. Miasto będzie dążyć także do redukcji nierówności w zakresie zdrowia i dobrostanu między mieszkańcami różnych dzielnic.

Przygotowane i reagujące miasto to strategie opisane w rozdziale trzecim. Władze Miasta Aniołów wraz z miastami partnerskimi dążą do wprowadzenia zasad odporności do działań władz miasta w celu priorytetowego traktowania najbardziej narażonych osób, miejsc i systemów. W Los Angeles sukcesywnie są udostępniane rozwiązania techniczne, które mają ułatwić procesy, takie jak konieczność odbudowy po klęskach naturalnych charakterystycznych dla tamtego regionu. Jednym z priorytetów jest też zapewnienie bezpiecznego i przystępnego cenowo mieszkalnictwa wszystkim mieszkańcom Los Angeles.

Pionierski i współpracujący partner ma wspomóc miasto we wprowadzaniu innowacji, które utrzymają rozwój Los Angeles jako lidera wśród naszych globalnych partnerów. Czwarty rozdział zawiera też wytyczne co do wykorzystania najnowszych zdobyczy nauki o klimacie w celu opracowania strategii adaptacyjnych zgodnych z Porozumieniem klimatycznym w Paryżu i częściowe odzyskanie rzeki na potrzeby mieszkańców.

Strategie odporności miejskiej świata zachodniego są do siebie dość zbliżone w sensie kompleksowości wytycznych, liczby filarów, celów i zadań. Dla odmiany warto również sprawdzić strategie bezpieczeństwa kraju afrykańskiego mającego niezwykle bogatą historię, ugruntowaną tożsamość i państwowość oraz przeżywającego obecnie intensywny rozwój gospodarczy.

Addis Abeba

Addis Abeba jest największym ośrodkiem miejskim Etiopii i jednym z najszybciej rozwijających się miast na świecie. Rozwój stolicy jest odzwierciedleniem tego, jak rośnie gospodarka Etiopii. Ludność tego miasta stanowi tylko 3,6% całkowitej populacji kraju, a mimo to przyczynia się do wypracowania 30% produktu krajowego brutto (PKB). Postęp gospodarczy kraju jest szybki i stosunkowo równomierny, co nie zmienia faktu, że Addis Abeba co chwilę musi się zmagać z różnego rodzaju wydarzeniami niekorzystnie wpływającymi na życie miasta. Do katastrof należą powodzie spowodowane gwałtownymi ulewami, pożary i rozprzestrzeniające się choroby zakaźne, szybka i niekontrolowana urbanizacja, niedobór wody i wysokie bezrobocie.

Władze Addis Abeby postanowiły oprzeć strategię odporności miejskiej na trzech filarach.

1. **Inteligentne i prosperujące miasto.** Uzyskaniu tego celu ma służyć zdywersyfikowana gospodarka i skuteczne nią zarządzanie w sposób sprzyjający rozwojowi przedsiębiorstw. Oznacza to, że władze będą wspierać innowacje z uwzględnieniem nowych miejsc pracy. Będą dążyć do wykorzystania istniejących zasobów środowiskowych, kulturowych i ludzkich w celu wsparcia zrównoważonego wzrostu gospodarczego.
2. **Tworzenie inkluzywnych i bezpiecznych społeczności.** Przyjmowanie bardziej uczestniczącego i skoncentrowanego na człowieku podejścia do planowania miasta dzisiaj i jutro. W ramach tego filaru zostały opracowane takie cele, jak poprawa dostępu do tanich mieszkań dobrej jakości, promowanie zorientowanej na człowieka, wydajnej i zintegrowanej mobilności, rozwijanie zdolności do zarządzania ryzykiem, promowanie kultury odporności, ochrona młodzieży, kobiet i słabszych grup społecznych. W działaniach szczegółowych miasta planowane są takie inwestycje, jak stworzenie Centrum Zarządzania Kryzysowego oraz współpraca z NGOs.
3. **„Zdrowe i nadające się do życia miejsca".** Tworzenie miasta przyjaznego do życia, które promuje zdrowie i dobre samopoczucie jego mieszkańców. Zawiera on następujące cele: inwestycje w sieć wodno-kanalizacyjną, wprowadzenie zasad umożliwiających zrównoważone wykorzystywanie zasobów naturalnych, działania na rzecz jakości środowiska naturalnego, wprowadzenie dobrych praktyk urbanistycznych.

Choć potrzeby miast i mieszkańców są podobne, ponieważ wszyscy chcemy żyć w miejscach bezpiecznych, czystych i… przygotowanych na kryzys każdego rodzaju, to różne są sposoby mające zapewnić realizację tych potrzeb. Gdzie indziej kładziony jest nacisk.

To zrozumiałe. Wynika z poziomu rozwoju miast, ich wielkości czy skomplikowania procesów w nich zachodzących, ale też poziomu świadomości mieszkańców i władz miast. Nie bez znaczenia są pieniądze. I te potrzebne na to, by strategiczną odporność uzyskać, i te, które można stracić, gdyby plan się nie powiódł.

Charakterystyczne dla wszystkich opracowanych strategii jest to, że security właściwie nie występuje w tych opracowaniach. Tak jakby fizyczne bezpieczeństwo mieszkańców, turystów i przedsiębiorców nie było wystawione na żadne ryzyko, co jest nieprawdą.

Być może dlatego strategie 100 Resilent City nie wspominają o security sensu stricto, gdyż tradycyjne bezpieczeństwo wraz z jego narzędziami (kamery, aplikacje, systemy zarządzania kryzysowego itp.) zostały wchłonięte przez inne systemy miejskie obficie korzystające z rozwiązań bezpieczeństwa zarówno technologicznych, jak i metodologicznych.

Świat się zmienia

Refleksja nad przyszłością musi się opierać na analizie przeszłości i teraźniejszości. Do najważniejszych wniosków należą konieczność intensyfikacji działań wzmacniających miejską odporność oraz precyzyjne określanie wymagań dotyczących wzmacniania środowisk miejskich dzięki adaptacji nowych idei: cyfryzacji, gospodarki o obiegu zamkniętym, zielonej infrastruktury.
Z pewnością opisane strategie odporności miejskich muszą zostać zaktualizowane. Sam aspekt cyberbezpieczeństwa, nieznanego rozwoju AI i jego konsekwencji oraz realne w wielu obszarach świata (Europa, Azja Południowo-Wschodnia, Bliski Wschód) ryzyko hybrydowego i kinetycznego konfliktu zbrojnego czy wreszcie nieznana skala masowych migracji z Południa do miast Północy powodują, że strategie odporności miejskiej należy zmienić.
A nad zmianami trzeba zacząć już dziś pracować. ●

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.

Honeywell

35 NOWA SERIA KAMER
ZWIĘKSZ ŚWIADOMOŚĆ - NIE KOSZTY

Seria 35 korzysta z algorytmu sztucznej inteligencji – rozróżnia pojazdy i ludzi.

- Doskonała jakość obrazu do 8MP
- Elastyczny nadzór
- Wbudowana pamięć wideo
- Inteligentna detekcja ruchu i analityka
- Łatwa w instalacji i obsłudze

5 YEAR WARRANTY | SECURE BY DEFAULT | ONVIF | SGT | NDAA COMPLIANT | NIS2 DIRECTIVE COMPLIANT

OFICJALNY DYSTRYBUTOR:

Linc Polska Sp. z o.o.
ul. Czarnkowska 22, 60-415 Poznań
tel.: +48 61 839 19 00,
e-mail: info@linc.pl

www.linc.pl

WIĘCEJ O NAS:

Linc Polska Sp. z o.o.

Miasta inteligentne
Bezpieczeństwo i wygoda nie tylko dla mieszkańców

Wraz z ewolucją krajobrazu miejskiego zapewnienie bezpieczeństwa i ochrony wszystkim mieszkańcom terenów zurbanizowanych staje się coraz ważniejsze. Na południu Polski jest realizowana pionierska inicjatywa Smart Tourist City, w której ramach są wykorzystywane nowoczesne technologie i innowacyjne praktyki. Miasto wygodne i bezpieczne szybciej przyciągnie zwiedzających.

To oczywiste, że większość zwiedzających, o ile tylko świadomie nie wybiera tzw. *slummingu* (turystyki biedy), oczekuje, że odwiedzane miejsce będzie nie tylko ciekawe, ale także bezpieczne. Zapewnienie turystom wygody i bezpieczeństwa to najważniejsze założenie idei Smart Tourist City. Aby stworzyć przyjazne środowisko otwarte dla odwiedzających, integrowane są najlepsze praktyki w zakresie dozoru wizyjnego, zarządzania kryzysowego i kontroli dostępu.

Zwiększenie bezpieczeństwa turystów dzięki zaawansowanemu monitoringowi wizyjnemu

Dzięki strategicznemu rozmieszczeniu kamer o wysokiej rozdzielczości wyposażonych w inteligentną analizę obrazu władze mogą w czasie rzeczywistym monitorować kluczowe atrakcje turystyczne i przestrzenie publiczne, zapewniając proaktywną identyfikację zagrożeń i szybką reakcję na nie. Przestrzegając surowych przepisów dotyczących prywatności i wdrażając przejrzyste praktyki zarządzania danymi, miasto priorytetowo traktuje ochronę praw turystów przy jednoczesnym utrzymaniu wysokiego poziomu bezpieczeństwa. Z tego powodu w projekcie zostały zastosowane najnowsze serie kamer PTZ TandemVu z serii DS-2SF8C442M oraz kamery panoramiczne 360 stopni wieloobiektywowe z serii DS-2DP8A845IXG. Zaangażowanie w odpowiedzialne praktyki nadzoru wyznacza nowy standard rozwoju bezpieczeństwa miejskiego w miejscowościach turystycznych.

Modelowe zarządzanie kryzysowe w celu zwiększenia odporności

Równie ważna jak nadzór wizyjny jest strategia zarządzania kryzysowego zaprojektowana tak, by zminimalizować ryzyko wystąpienia sytuacji kryzysowych i ograniczyć ich ewentualny skutek. Poprzez kompleksowe planowanie, koordynację ze służbami ratunkowymi i wdrażanie zintegrowanych systemów komunikacji miasto zwiększa swoją odporność na różne zagrożenia, począwszy od klęsk żywiołowych, skończywszy na incydentach związanych z terroryzmem. Modelowe ramy zarządzania kryzysowego służą jako wzór dla miast na całym świecie, pokazując znaczenie proaktywnej gotowości i wspólnych strategii reagowania. Wykorzystując technologię i zaangażowanie społeczności, miasto zapewnia szybkie i skuteczne działania w czasach kryzysu, chroniąc zdrowie

i życie mieszkańców oraz infrastrukturę. Realizację takiej strategii ułatwia odpowiednie wyposażenie techniczne, np. w najnowsze rejestratory z funkcjami inteligentnej analizy obrazu, takie jak urządzenia z serii iDS-96xx wraz z nowoczesnym i wysoko zaawansowanym oprogramowaniem HikCentral Professional.

Turyści i mieszkańcy mogą więc spokojnie poruszać się po mieście, gdyż wiedzą, że są chronieni przez wyspecjalizowane zespoły szybkiego reagowania.

Inteligentne rozwiązania czynią miasto bezpiecznym i wygodnym

Turyści przybywający do miasta cenią atrakcje i wygodę. Równie ważne jest też bezpieczeństwo. Dlatego Smart Tourist City wykorzystuje usprawnione rozwiązania kontroli dostępu dostosowane do ich potrzeb. Dzięki cyfrowym systemom biletowym oraz mobilnym poświadczeniom zwiedzający mogą swobodnie poruszać się po mieście, nie czekając np. w kolejkach i nie martwiąc się opłatą za bilety komunikacji miejskiej.

Koncepcja Smart Tourist City oznacza wdrażanie takich rozwiązań, jak interaktywne mapy i wirtualne przewodniki oraz dostęp do wielu informacji i zasobów, które osobom przybywającym do miasta mają pomóc w poznawaniu jego uroków. Takie udogodnienia oferują rozwiązania Hikvision, w tym kamery z serii TandemVu oraz nowoczesne systemy zapisu czy oprogramowanie, które są wyposażone w najnowsze technologie wykorzystujące AI. Jednocześnie spełniają najwyższe wymagania i standardy bezpieczeństwa wynikające z dyrektywy NIS2.

Wykorzystując bezpieczną technologię i innowacje, miasto tworzy dynamiczne i angażujące doświadczenie turystyczne, jednocześnie stawiając na pierwszym miejscu bezpieczeństwo i ochronę. Turyści mogą zanurzyć się w kulturze i pięknie miasta, wiedząc, że ich bezpieczeństwo jest najwyższym priorytetem.

Zintegrowanie systemów kontroli dostępu z usługami i udogodnieniami turystycznymi powoduje, że miasto jest środowiskiem, w którym bezpieczeństwo i wygoda idą w parze.

O polskiej inicjatywie Smart Tourist City

Inicjatywa Smart Tourist City ma na celu wykorzystanie najnowszych technologii na rzecz zwiększenia bezpieczeństwa, wygody i ogólnego doświadczenia turystów. Poprzez strategiczne partnerstwa i zaangażowanie społeczności miasta zaangażowane w tę inicjatywę mają szansę stać się ulubionym celem podróżnych z całego świata wiedzących, że wygodzie zwiedzania towarzyszy absolutne bezpieczeństwo. ●

W przypadku pytań prosimy o kontakt:

Hikvision Poland
ul. Żwirki i Wigury 16B, 02-092 Warszawa
Michal.Swoboda@hikvision.com
https://www.hikvision.com/europe/

Twierdza pieniądza w sercu Warszawy

Co łączy paliwo i dane? Pozornie niewiele, ale faktycznie jedno i drugie stanowi napęd rozwoju gospodarczego i technologicznego kraju. Ich wykorzystanie może mieć ogromny wpływ na bezpieczeństwo. Z wartości danych jako współczesnego paliwa doskonale zdają sobie sprawę przestępcy, stąd powszechne zjawisko cyberataków, fałszerstw i kradzieży tożsamości. Mało kto zdaje sobie sprawę z tego, jakim narodowym skarbem jest Polska Wytwórnia Papierów Wartościowych. To miejsce o strategicznym znaczeniu dla bezpieczeństwa kraju. Mieliśmy rzadką okazję, by je zobaczyć od środka.

Jan T. Grusznic, a&s Polska

Na całym świecie działa tylko kilkadziesiąt zakładów zajmujących się security printingiem, w Unii Europejskiej – zaledwie kilkanaście. Wysoki koszt wejścia powoduje, że na rynku bardzo rzadko pojawiają się nowi gracze. Proces produkcji w zależności od przyjętego rozwiązania, poziomu oraz stopnia skomplikowania zabezpieczeń jest długotrwały i obejmuje nawet kilkanaście etapów. PWPW dysponuje zaawansowanym parkiem maszynowym oraz, jako jeden z niewielu podmiotów na świecie, jest w stanie przeprowadzić cały proces produkcyjny w jednym miejscu – od zaproponowania zabezpieczeń oraz przygotowania projektu graficznego, przez produkcję (począwszy od wytworzenia podłoża po zadruk poligraficzny oraz personalizację), po zaprojektowanie, wdrożenie i utrzymanie systemów IT. Dzięki temu Wytwórnia jest elastyczna, jeśli chodzi o dobór technologii produkcji dostosowanych do wymagań klientów. A tych ma naprawdę wielu. Produkty PWPW trafiają do instytucji w ponad 70 krajach na świecie. Z usług polskiego zakładu korzystają firmy i obywatele wielu państw – od Europy, przez kraje Ameryki i Azji, po Afrykę.

Głównym obszarem działalności spółki jest produkcja banknotów, paszportów, dowodów osobistych, dokumentów komunikacyjnych i innych wysoko zabezpieczonych druków. PWPW jako jedyna umożliwia weryfikację tożsamości przy użyciu e-dowodu dzięki opracowanej przez wewnętrzny zespół aplikacji eDO App, zapewniającej pełne zdalne wykorzystanie warstwy elektronicznej dowodu osobistego.

W Wytwórni ponadprzeciętnie rozwinięty jest dział kontroli jakościowej i ilościowej, który sprawuje nieprzerwany dozór nad bezpieczeństwem procesu i jego dokumentowaniem. W niektórych wypadkach konieczne jest ręczne liczenie półproduktów, w innych dopuszczalne jest wsparcie za pomocą liczenia maszynowego. Co ciekawe, wysoka jakość w produkcji liczy się również podczas utylizacji. Niszczenie banknotów jest znacznie bardziej skomplikowane niż typowe niszczenie dokumentów. Kluczowe jest tu bezpieczeństwo, które nie pozwala na nieautoryzowany dostęp, a rozmiar rozdrobnienia na tyle wysoki, by odtworzenie banknotów było niemożliwie (co spełnia też wymagania stawiane przez bank centralny).

Największym atutem spółki są jej pracownicy – wykwalifikowani specjaliści w swoich dziedzinach. PWPW zatrudnia ponad 2 tysiące osób, z których wiele może pochwalić się długim stażem, wynoszącym średnio 15 lat. Często są to osoby z rodzin o wielopokoleniowej tradycji, gdzie zarówno dziadkowie, jak i rodzice byli lub nadal są związani z Wytwórnią.

→

W PWPW tradycja łączy się z nowoczesnością – dobra szkoła rytowników, którzy pierwsze ryty tworzą w mydle lub gipsie, łączy się z technologią komputerową. Innowacyjność i kreatywność pracowników opiera się na badaniach naukowych oraz doświadczeniach. Stale analizują i wdrażają nowe pomysły, by wyprzedzać zmiany zachodzące w otoczeniu, dzięki temu w wielu aspektach Wytwórnia jest prekursorem na skalę światową. Przykładem może być walor testowy Coral z unikalnym zabezpieczeniem TOE *(Transmission Optical Element)* – elementem wydrukowanym w okienku, który zawiera ukryty obraz aktywowany światłem laserowym.

Odpowiednie procedury bezpieczeństwa, których gros dotyczy kontroli jakości w poszczególnych fazach wytwarzania, oraz wieloletnie doświadczenie w zabezpieczaniu druków gwarantują najwyższej jakości produkcję. PWPW posiada liczne certyfikaty, a dzięki temu spełnia wyśrubowane normy bezpieczeństwa, w tym certyfikat INTERGRAF (ISO 14298[1]) – dokument kluczowy dla producentów druków zabezpieczonych.

Ponadto posiada certyfikat CWA 15374[2] dla obszaru produkcji papieru zabezpieczonego. Przyczyniły się do tego zrównoważona i odpowiednio prowadzona polityka bezpieczeństwa dotycząca zarówno procesów wytwórczych, jak i bezpieczeństwa fizycznego. Audyt INTERGRAF stanowi duże wyzwanie organizacyjne i logistyczne. Audytorzy z uwagą przyglądają się procesom produkcyjnym, analizują dokumentację i weryfikują zapisy w elektronicznych systemach zabezpieczeń.

Dbałość o pracownika jest bardzo ważnym elementem całego procesu bezpieczeństwa. Każda z zatrudnionych osób przechodzi rygorystyczny screening powtarzany cyklicznie. PWPW ma własnych pracowników ochrony oraz utrzymania czystości. Firmy zewnętrzne i pracujące w nich osoby przechodzą drobiazgowy, wieloetapowy proces weryfikacji. Na terenie PWPW utrzymywany jest bezwzględny zakaz posiadania urządzeń umożliwiających rejestrację obrazu i dźwięku. Pracownicy przed wejściem do stref produkcyjnych zostawiają swoje telefony, zegarki i inne urządzenia w specjalnie przeznaczonych do tego skrytkach. Dostęp do stref produkcyjnych i wyjście z nich są chronione za pomocą systemów śluz wyposażonych w systemy biometryczne oraz weryfikacji liczby osób. Śluzy są połączone w specjalnie do tego celu zaprojektowany układ twardego *Anti-Pass-Back* (APB), który uniemożliwia ponowne wejście do strefy lub wyjście z niej. APB dotyczy zarówno pracowników, jak i gości. W przypadku gości identyfikatory są specjalnie zaprogramowane, by wejście do strefy było możliwe tylko przez osobę uprawnioną wg zasady 4 oczu. Stworzenie stref APB i wdrożenie w tak skomplikowanym układzie budynków zajęło zespołowi ponad rok (z uwzględnieniem zmian procedur, czasu na zmianę przyzwyczajeń pracowników i modyfikację systemu wymagającą uwzględnienia wyjątków). Na kompromisy nie było miejsca.

Identyfikatory SKD zostały wyprodukowane przez PWPW. Mają one podobne zabezpieczenia do tych, które wdrożono w polskich dowodach osobistych. Klucze niezbędne do szyfrowanej komunikacji w ramach systemów zabezpieczeń technicznych zostały opracowane i wprowadzone przez dział bezpieczeństwa Wytwórni, co pozwoliło na zmniejszenie poziomu ryzyka związanego ze skompromitowaniem posiadanych zabezpieczeń. Obok SKD w ramach systemu dozoru wizyjnego każdy etap procesu monitoruje przeszło 1700 kamer w odseparowanej sieci informatycznej.

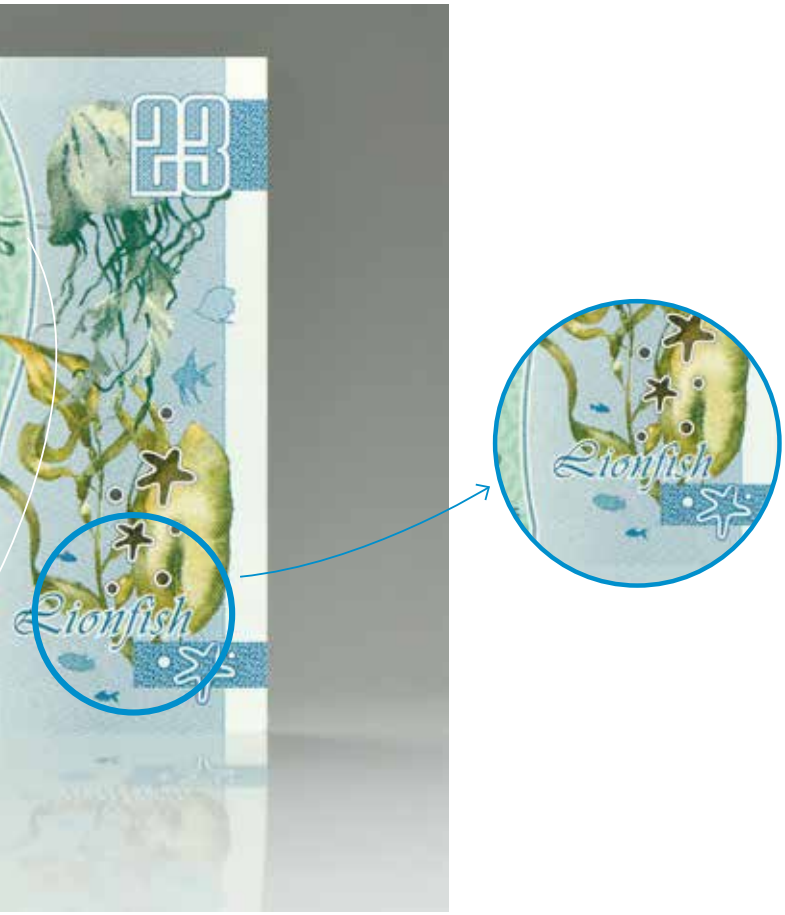


Foto: Rafał Jaworski / PWPW

Wyzwaniem utrzymania bezpieczeństwa na zunifikowanym poziomie jest rozproszona lokalizacja. Cała instytucja PWPW to kilka lokalizacji na terenie Warszawy: różne typy budynków, inne otoczenie, odmienne procesy są wyzwaniem dla standaryzacji. Ponadto historyczna lokalizacja przy ul. Sanguszki również stanowi pewne utrudnienie. To de facto kompleks budynków, które nie posiadają jednorodnego planu połączeń komunikacyjnych, co w efekcie wymusza wielokrotne przemieszczanie się klatkami schodowymi i zmiany kondygnacji. Te w budynkach są oznaczane względem poziomu „zero Wisły", stosowanego w wielu opracowaniach geodezyjnych, architektonicznych, geotechnicznych i geologiczno-inżynierskich w Warszawie i okolicach, a to nieco dezorientuje gości. Budynek wzniesiony w latach 1927–29 był najbardziej na północ wysuniętą powstańczą redutą na Starym Mieście, a jej załoga przez cztery tygodnie toczyła zacięte boje o utrzymanie kompleksu. Objęcie opieką konserwatora zabytków znacząco utrudnia utrzymanie właściwego poziomu zabezpieczenia technicznego, ale jak widać nie uniemożliwia.

Wszelkie zmiany, zwłaszcza na zewnątrz kompleksu, wymagają skrupulatnych projektów i uzgodnień. Jest to również wyzwanie dla ciągle rozwijającej się PWPW. Nowe maszyny muszą być niekonwencjonalnie wprowadzane do budynku za pomocą specjalnie na tę okazję przygotowanych otworów w dachu lub elewacji, dlatego często bardziej opłacalnym i niekiedy szybszym procesem jest modernizacja posiadanych maszyn. W przypadku urządzeń do produkcji papieru, które mogą zajmować aż 4 kondygnacje, jest to jedyne rozwiązanie. Dzisiaj obok nowych maszyn przeznaczonych dla poligrafii, pracują urządzenia liczące sobie nawet 50 lat. Każde z nich jest przeznaczone do innego procesu. Dbałość o ciągły rozwój pomimo ograniczeń spowodował, że Polska Wytwórnia Papierów Wartościowych jest obecnie zaawansowanym technologicznie zakładem, który do produkcji banknotów i papierów wartościowych wykorzystuje profesjonalne i nowoczesne metody druku i zabezpieczeń. Świadczy o tym m.in. akredytacja przyznana PWPW, która potwierdza gotowość wytwórni do produkcji banknotów euro dla Unii Europejskiej.

W zeszłym roku PWPW SA podpisała z TZF Polfa SA umowę o wartości 143 mln zł na zakup ponad 17-hektarowej działki na warszawskim Tarchominie. Transakcja ta wg Ministerstwa Spraw Wewnętrznych i Administracji zapoczątkowała budowę nowej narodowej drukarni polskich banknotów i polskiej papierni, zakładu wytwarzającego papier zabezpieczony, która ma być odpowiedzią na rosnące koszty produkcji związane z obecną lokalizacją Wytwórni oraz poważne utrudnienia logistyczne.

Wybór rozwiązań systemów kontroli dostępu i telewizji dozorowej stanowił duże wyzwanie dla działu bezpieczeństwa Wytwórni. Z uwagi na niewielką liczbę obiektów, na których można było się wzorować, koncepcja zabezpieczenia była tworzona od podstaw. Impulsem do zmiany było przejęcie istniejącego SKD przez innego producenta i zakończenie wsparcia dla tej linii produktowej. Wymagania z zakresu ISO 14298 i CWA 15374 narzucały określone wymagania w zakresie dostawców systemów. Wytwórnia postawiła na rozwiązania produkowane na terenie Unii Europejskiej i w USA po wcześniejszym zapoznaniu się z procesem produkcyjnym, listy dostawców podzespołów, jak również w czasie rozmów z użytkownikami systemów podczas wizyt referencyjnych.

PWPW stoi w tej chwili przed wyborem unifikującym system sygnalizacji włamania i napadu, który obecnie posiada przeszło 10 000 elementów.

Od dekady PWPW doskonale radzi sobie na rynkach zagranicznych. Produkty zdobywają kolejne nagrody w obszarze security printing (w tym za kolekcjonerski banknot 20-złotowy poświęcony Mikołajowi Kopernikowi i wyemitowany z okazji 550. rocznicy jego urodzin i 480. rocznicy śmierci czy wyemitowany przez NBP banknot kolekcjonerski z wizerunkiem prezydenta Lecha Kaczyńskiego, który został uznany za najlepszy banknot kolekcjonerski roku 2021). Banknoty, które wyprodukowano w Warszawie, noszą w swoich portfelach mieszkańcy m.in. Gwatemali, Paragwaju, Hondurasu czy Gruzji. Obywatele Armenii od kilku lat posługują się paszportami biometrycznymi i elektronicznymi dowodami osobistymi dostarczonymi im przez PWPW. Od marca 2024 r. także do obywateli Islandii trafia nowy dowód osobisty wyprodukowany również w Polskiej Wytwórni Papierów Wartościowych, która już dostarcza do tego kraju paszporty. Większość państw nie drukuje bowiem banknotów u siebie. Ze względu na koszty i wysokie zabezpieczenia przed ich podrabianiem, zleca produkcję za granicę, m.in. do PWPW. ●

1 Certyfikat ISO 14298 jest przeznaczony dla producentów druków wartościowych chronionych przed fałszowaniem, takich jak banknoty, dowody osobiste, paszporty, prawa jazdy, znaczki pocztowe i skarbowe, dyplomy, i dotyczy zarządzania procesami produkcji tych wyjątkowych produktów.

2 Certyfikat CWA 15374 opisuje system zarządzania bezpieczeństwem dla dostawców producentów druków wartościowych, czyli m.in. producentów papieru zabezpieczonego, specjalistycznych farb, atramentu, płyt laminujących, gilotyn, folii zabezpieczających, oprogramowania do projektowania zabezpieczeń, substratów, pigmentów czy powłok.

Wydział Filologiczny Uniwersytetu Łódzkiego – Smart Building XXI wieku

Wydział Filologiczny Uniwersytetu Łódzkiego może się pochwalić nowoczesnym systemem kontroli dostępu. Władze wydziału w ciągu 4-5 lat planują rozbudowę tego systemu tak, by kubistyczny budynek akademicki stał się prawdziwym smart building. Za pomocą otwartej platformy Genetec zaimplementowano już kontrolę dostępu do części sal dydaktycznych oraz sal specjalnego przeznaczenia (sala radiowa, pracownia translatoryczna wyposażona w kabiny tłumaczy czy studio telewizyjne). W kolejnych krokach władze wydziału zamierzają zintegrować system alarmowy, sygnalizację pożarową, wentylację i dostęp do parkingów.

Na teren nowego budynku Wydziału Filologicznego Uniwersytetu Łódzkiego pierwsi studenci weszli w 2014 r. i mniej więcej od tego momentu władze wydziału starają się, by bryła powstała z kombinacji szkła i aluminium była nowoczesna również pod kątem zabezpieczeń technicznych. Pierwszym krokiem do osiągnięcia tego rozwiązania jest elektroniczny system kontroli dostępu zaprojektowany przy użyciu platformy Genetec.

– *System ma za zadanie ułatwić pracownikom i studentom dostęp do różnych pomieszczeń. W czytniki elektroniczne są wyposażone wszystkie sale dydaktyczne, aule, laboratoria językowe, logopedyczne oraz pomieszczenia szczególne o ograniczonym dostępie, takie jak studio telewizyjne, studio radiowe czy pracownia translatoryczna, w której znajdują się kabiny tłumaczy. W sumie w tej chwili daje to 100 przejść* – mówi Aneta Sadach, kierownik Działu ds. Obsługi Administracyjno-Informatycznej Wydziału Filologicznego w Łodzi.

ŁÓDŹ MIASTO AKADEMICKIE

19 uczelni wyższych
7 wyższych uczelni publicznych

UNIWERSYTET ŁÓDZKI

26 tysięcy studentów

WYDZIAŁ FILOLOGICZNY UŁ

3500 studentów
400 pracowników
40 kierunków studiów

Pomysł na takie rozwiązanie pojawił się kilka lat temu. Przygotowanie wdrożenia, od zakupu oprogramowania i instalacji pierwszych 5 klamek wyposażonych w czytnik, trwało około roku. Dla zespołu zajmującego się systemem kontroli dostępu był to okres testowania i szukania rozwiązań przeznaczonych do budynku będącego częścią jednej z większych uczelni w Polsce. Elektroniczny dostęp był pierwszym na liście punktem do zrealizowania. System jest zintegrowany z monitoringiem wizyjnym. Kamery wysokiej jakości włączone w system pomagają skutecznie ustalić przebieg różnego rodzaju incydentów i wykryć ich sprawców.

Uprawnienia zarówno pracownikom, jak i studentom nadaje zespół obsługi systemu Genetec. Każda karta jest spersonalizowana, dlatego na stronie internetowej wydziału dostępnych jest kilka rodzajów formularzy wniosków o dostęp do sal wydziału (w zależności od zapotrzebowania). Na podstawie wniosku uprawnienia nadawane są automatycznie. Dane pracowników etatowych są pobierane z wewnętrznego systemu UŁ, co pozwala na szybkie przygotowanie kart i przypisanie uprawnień dostępu skorelowanych z charakterem pracy. Pracownikom prowadzącym zajęcia z innych wydziałów UŁ uprawnienia są przypisane na podstawie legitymacji pracowniczej zgodnie z harmonogramem zajęć prowadzonych w danym semestrze.

Osoby wizytujące otrzymują kartę gościa z dostępem do konkretnej sali czy auli. Studenci ubiegający się o udostępnienie pomieszczenia do pracy indywidualnej, zgodnie z wcześniej przesłanym wnioskiem za pośrednictwem platformy dostępnej na stronie wydziału, otrzymują uprawnienia na podstawie legitymacji studenckiej. Podczas konferencji swobodny dostęp do auli zapewnia synchronizacja z harmonogramem drzwi. Dzięki niej możliwe jest utrzymanie trybu otwarcia drzwi w żądanym przedziale czasowym..

– Przykładem sytuacji kryzysowej są osoby przebywające w budynku po godzinie 21.00, głównie w strefach alarmowych. Wszystkie strefy budynku wyposażone w system alarmowy po 21.00 zostają zakodowane (uzbrojone) i do tego czasu wszyscy użytkownicy pomieszczeń i przestrzeni ogólnodostępnej są zobowiązani do opuszczenia budynku. System pomaga wykryć osoby przebywające na wydziale po godzinach jego funkcjonowania – podkreśla Grzegorz Zgondek, główny specjalista w dziale ds. obsługi administracyjno-informatycznej Wydziału Filologicznego Uniwersytetu Łódzkiego.

Osoba, która zgubi kartę dostępu stałego lub czasowego, powinna zgłosić ten fakt za pośrednictwem formularza dostępnego na stronie wydziału. Formularz wpływa mailem do zespołu obsługi Genetec Security Center, który blokuje kartę. Osoba zgłaszająca zagubienie karty otrzymuje na 2 tygodnie tzw. token rezerwowy. Jeśli karta zostanie odnaleziona, pracownik obsługi systemu dokonuje jej aktywacji, jeśli natomiast nie ma jej, wysyła prośbę o wydanie duplikatu karty.

Odmowa dostępu jest sygnalizowana za pomocą diody w kolorze czerwonym. W tym samym czasie pocztą elektroniczną do pracowników obsługi systemu trafia informacja o nieuprawnionej próbie wejścia do sali. Obecnie system ma dwa tryby otwierania drzwi: zwykły i biurowy. Tryb biurowy został dopasowany do potrzeb uczelni. Pozwala on na swobodny dostęp do sali dydaktycznej przez 15 minut od momentu sczytania karty pracownika jako osoby uprawnionej do wejścia. – *System pomaga utrzymać dyscyplinę wśród studentów, skończyły się czasy kwadransa akademickiego, który czasem trwał nawet godzinę* – komentuje dr Sebastian Zacharow, nauczyciel akademicki z Instytutu Romanistyki.

– Uniwersytety rozwijają się bardzo dynamicznie. W strukturze uczelni często jest wiele budynków. System musi być elastyczny i otwarty, by z jednej strony umożliwiać nadzór nad rozproszoną strukturą, z drugiej – dawać możliwość scentralizowania spojrzenia na to, co się dzieje w ramach uniwersytetu. Tym, co wyróżnia Genetec Security Center spośród innych systemów, jest nie tylko kontrola dostępu i zabezpieczenia techniczne budynku, ale także integracja z podsystemem ściśle związanym z automatyką budynkową. Dzięki zastosowaniu urządzeń IoT, oprócz standardowych funkcji systemu zabezpieczeń, użytkownik może korzystać z podsystemu i optymalizować koszty zużycia energii elektrycznej, wody czy energii cieplnej. Ten system to nie tylko zabezpieczenie budynku, ale także zwiększenie logiki jego funkcjonowania – mówi Jakub Kozak, Regional Sales Manager East Central Europe Genetec.

W planach wydziału jest integracja elektronicznej kontroli dostępu z pełnym monitoringiem wizyjnym, a także sterowanie automatyką budynku. System ma generować raporty o alarmach na terenie wydziału, zdarzeniach pożarowych (dzięki integracji centrali przeciwpożarowej), działaniu czujników wycieku wody, zużyciu energii elektrycznej oraz sterowaniu harmonogramem pracy urządzeń wentylacyjnych.

– Dla nas najważniejsze jest to, że pomysł nie miał być jednorazową wymianą standardowych kluczy na karty, a całym szeregiem działań, które uczynią wydział nowocześniejszym i optymalnie zautomatyzowanym. Ten projekt jest pionierski, jeśli chodzi o uczelnie w Polsce. Chcemy, by nasz wydział był pierwszym w pełni smart wydziałem w Polsce. To ogromna satysfakcja, szczególnie że finansowanie takiego projektu w przypadku każdego wydziału jest osobne. Może inne wydziały, nie tylko naszego uniwersytetu, ale i innych uczelni będą chciały mieć podobny system – dodaje Dorota Cieślak, dyrektor administracyjna Wydziału Filologicznego Uniwersytetu Łódzkiego. ●

głos branży

Technologie Smart City są kluczem do inteligentnego zarządzania infrastrukturą miejską. Z punktu widzenia branży security najważniejszym aspektem jest oczywiście bezpieczeństwo. Systemy zabezpieczeń technicznych pomagają w zapobieganiu przestępczości i szybkim reagowaniu na sytuacje kryzysowe. Co jeszcze może pomóc w zapewnieniu bezpieczeństwa i poprawie komfortu życia mieszkańców?

Rafal Batkowski
RBS

Bezpieczeństwo miejskie i podmioty krytyczne

Wydaje się, że przed nami czas pilnego wzmacniania odporności miast i lokalnych miejskich społeczności na zagrożenia hybrydowe oraz inne wyzwania dotyczące ekstremizmu, terroryzmu i przestępczości.

Wiele innych czynników, uwzględniając rosyjską agresję, wpływa na nasze krajowe środowisko bezpieczeństwa, poczynając od otoczenia prawnego, poprzez procesy polityczne i gospodarcze, w tym inwestycyjne. Silne osadzenie w strukturach UE i relacje transatlantyckie mają istotne znaczenie dla bezpieczeństwa nas wszystkich. Dodatkowo konieczna implementacja Dyrektyw NIS2 i powiązanej CER oraz procedowany projekt ustawy o ochronie ludności (…), zmiany organizacyjne w administracji publicznej, zmiany w samorządach i spodziewane nowe akty prawne zmienią podejście w wielu kluczowych obszarach zarządzania bezpieczeństwem. Doniosłe znaczenie mają także wymogi – nie do końca spójne – związane z bezpieczeństwem obiektów podlegających obowiązkowej ochronie, obiektów szczególnie ważnych dla bezpieczeństwa lub obronności, operatorów usług kluczowych czy też obiektów infrastruktury krytycznej (IK) i innych. Sytuacja wymaga, w rozumieniu autora, pilnego uspójnienia i wdrożenia procesu edukowania lokalnych społeczności oraz pracowników/operatorów takich obiektów w kontekście rozumienia regulacji i zadań wynikających z wdrożonych planów. To wielkie czekające na realizację wyzwanie.

W tym kontekście obszary zurbanizowane wymagają wielkiej troski służb porządku publicznego i zaangażowania innych interesariuszy aktywnych w sferze bezpieczeństwa. Koncentracja ludności, *soft targets*, siedziby organów administracji państwowej i samorządowej, transport publiczny, ośrodki nauki i kultury, siedziby mediów, przemysł oraz infrastruktura krytyczna, istotna dla

całego państwa i ta o ważnym znaczeniu miejskim, charakteryzują nasze największe miasta. Kluczowe w tej perspektywie pozostanie optymalizowanie ochrony IK nie tylko tej najważniejszej (ujętej w stosownym, niejawnym wykazie), ale również takiej, która może być identyfikowana na poziomie miejskim, m.in. w rozumieniu *soft targets*, np. szpitale, obiekty urzędu miasta, uczelnie, hale sportowe i widowiskowe, media, wielkie galerie handlowe, porty morskie, lotnicze, kolejowe etc. wytwórcy/użytkownicy substancji chemicznych mogących stanowić zagrożenie dla ludności...

Podsumowując, należy podkreślić konieczność wdrożenia minimalnych wymogów – standardów bezpieczeństwa w zagrożonych miejscach publicznych oraz potrzebę identyfikacji kluczowych obiektów i systemów, poza obowiązkami ustawowymi dotyczącymi infrastruktury krytycznej państwa, w celu skorzystania z najlepszych praktyk budowania odporności miast na zagrożenia (w tym NIS2 i CER). Ponadto profesjonalne wdrożenie procedur zgodnych z normami ISO 270001 oraz ISO 22301 powinno być pilnym zaleceniem w miejskim wymiarze. Poza powyższym, dążąc do wzmacniania lokalnego miejskiego poziomu bezpieczeństwa, warto korzystać z gotowych bezpłatnych rozwiązań i szkoleń.

Konrad Badowski
AXIS COMMUNICATIONS

Ocena i modernizacja systemów

W najbliższych latach miasta będą musiały się zmierzyć z modernizacją systemów i urządzeń IT. Będzie to wynikać m.in. z nowej ustawy o Krajowym Systemie Cyberbezpieczeństwa. Nowelizacja ta w obecnym kształcie wprowadza postanowienia przyjętych w ostatnim czasie dyrektyw UE, NIS2 i CER.

O NIS2 pojawiło się już wiele publikacji. Wiadomo, że miasta będą podlegać jej wymaganiom. Tak jak NIS2 kładzie główny nacisk na zarządzanie ryzykiem dla bezpieczeństwa sieci i systemów informatycznych, tak CER skupia się na bezpieczeństwie sprzętu i systemów. Ponadto ustawa o KSC wprowadzi pojęcie Dostawcy Wysokiego Ryzyka. Te wszystkie czynniki będą wymuszać na miastach dokładną ocenę bezpieczeństwa swoich systemów oraz ich prawdopodobną modernizację. Nie wszystkie wymagania pojawią się w tym samym czasie. Sprzęt i oprogramowanie, dla którego producent nie oferuje już wsparcia, czyli nie bada podatności oraz nie publikuje poprawek, będzie musiał być wymieniony w pierwszej kolejności, natomiast na wymianę sprzętu i oprogramowania pochodzącego od dostawcy umieszczonego na liście Dostawców Wysokiego Ryzyka miasta będą miały ok. 7 lat. Dodatkowym wyzwaniem będzie koniec wsparcia dla systemu Windows 10, który Microsoft zapowiedział na 14 października 2025 r.

W związku z tym może się okazać, że równie ważny jak okres gwarancji będzie czas wsparcia sprzętu w zakresie poprawek oprogramowania. Dla przykładu dla urządzeń CCTV standardem już jest 5 lat gwarancji, jednak wsparcie oprogramowania powinno być dłuższe, przynajmniej na cały „czas życia" określany przez użytkownika. Najczęściej oczekuje się, aby kamery działały przez 7–10 lat. Dlatego przy wyborze rozwiązania warto sprawdzić deklarowany przez producenta okres wsparcia, aby nie trzeba było dokonywać przedwczesnej wymiany sprzętu.

MARCIN WALCZUK
BCS

Inteligentne miasta to miasta bezpieczne

Współczesne miasta stają przed wyzwaniami związanymi z szybkim wzrostem populacji, zanieczyszczeniem środowiska i koniecznością efektywnego zarządzania zasobami. W odpowiedzi na nie pojawiła się koncepcja Smart City – inteligentnego miasta, które wykorzystuje nowoczesne technologie do poprawy jakości życia mieszkańców i zrównoważonego rozwoju.

Technologie Smart City są kluczem do inteligentnego zarządzania infrastrukturą miejską. Systemy te obejmują szeroki zakres aplikacji, od inteligentnego oświetlenia ulic, przez zaawansowane systemy zarządzania ruchem, po innowacyjne metody gospodarowania odpadami. Zastosowanie sensorów ruchu i oświetlenia LED może znacząco obniżyć zużycie energii, a także poprawić bezpieczeństwo na drogach.

Zarządzanie ruchem w inteligentnych miastach to nie tylko kwestia sygnalizacji świetlnej i znaków drogowych. To także systemy GPS i analiza danych w czasie rzeczywistym, które pozwalają na płynne przepływy komunikacyjne i redukcję zatorów. Dzięki temu mieszkańcy mogą szybciej i wygodniej dotrzeć do celu, co przekłada się na zmniejszenie emisji spalin i poprawę jakości powietrza.

Przestawienie się z tradycyjnych źródeł energii na odnawialne, takie jak panele słoneczne i turbiny wiatrowe, które są integrowane z miejską infrastrukturą, zajmie jeszcze trochę czasu, ale jest kierunkiem, w którym nowoczesne miasta przyszłości powinny podążać. Wykorzystanie przy tym inteligentnych sieci energetycznych pozwoli na optymalizację zużycia energii i lepsze zarządzanie popytem.

Z punktu widzenia branży security najważniejszym aspektem w Smart City jest oczywiście bezpieczeństwo. Systemy monitoringu wizyjnego i analizy danych pomagają w zapobieganiu przestępczości i szybkim reagowaniu na sytuacje kryzysowe. Dla tak wielkiego organizmu, jakim jest miasto, najistotniejsza jest integracja wszystkich systemów, aby mogły szybko działać i się wspierać. Dzięki temu mieszkańcy będą mogli czuć się bezpieczniej w swoim otoczeniu.

Podsumowując, Smart City to przyszłościowy model miasta, który wykorzystuje innowacje technologiczne do tworzenia zrównoważonego i przyjaznego środowiska dla mieszkańców. To odpowiedź na potrzeby współczesnych społeczeństw, które dążą do poprawy jakości życia przy jednoczesnym zmniejszeniu negatywnego wpływu na środowisko naturalne. Wyzwaniem pozostaje jednak integracja nowych technologii z istniejącą infrastrukturą i zapewnienie prywatności oraz bezpieczeństwa danych w cyfrowym świecie. Z pomocą przychodzą rozwiązania oferowane przez BCS.

Michał Swoboda
HIKVISION POLAND

Rozwój bezpieczeństwa miejskiego

W czasach, kiedy bezpieczeństwo jest najważniejsze, miasta na całym świecie sięgają po zaawansowane technologie i innowacyjne strategie w celu zwiększenia środków bezpieczeństwa. Od kompleksowych systemów dozoru wizyjnego, przez modelowe ramy zarządzania kryzysowego kładziony jest nacisk na tworzenie bezpiecznych środowisk zarówno dla mieszkańców, firm, jak i odwiedzających.

U podstaw miejskich inicjatyw w zakresie bezpieczeństwa leży wdrożenie solidnych systemów dozoru wizyjnego. Systemy te nie tylko służą jako środek odstraszający przed przestępczością, ale także umożliwiają władzom skuteczne monitorowanie przestrzeni publicznych. Wykorzystując kamery wysokiej rozdzielczości i inteligentną analitykę, miasta mogą wykrywać podejrzane działania w czasie rzeczywistym i szybko reagować na potencjalne zagrożenia. Dobre praktyki w miejskim monitoringu stawiają na pierwszym miejscu ochronę prywatności i przestrzeganie standardów regulacyjnych. Anonimizacja danych i ograniczenie dostępu do upoważnionego personelu zapewniają, że technologie nadzoru są wykorzystywane w sposób odpowiedzialny i etyczny.

Oprócz dozoru wizyjnego miasta inwestują w modelowe ramy zarządzania kryzysowego, aby zwiększyć swoją odporność w czasach kryzysu. Od klęsk żywiołowych po incydenty związane z bezpieczeństwem kładziony jest nacisk na proaktywne planowanie, skuteczną komunikację i skoordynowane wysiłki w zakresie reagowania. Przeprowadzając regularne ćwiczenia i symulacje, zespoły zarządzania kryzysowego mogą zidentyfikować potencjalne słabe punkty i odpowiednio dostosować swoje strategie. Co więcej, integracja technologii, takich jak systemy alarmowe i mapowanie geoprzestrzenne, zwiększa wydajność i skuteczność reagowania, minimalizując wpływ sytuacji kryzysowych na społeczności miejskie.

W sektorze korporacyjnym zapewnienie bezpieczeństwa obiektów biurowych ma ogromne znaczenie. Wraz ze wzrostem wyrafinowanych zagrożeń firmy przyjmują zaawansowane rozwiązania kontroli dostępu w celu ochrony swoich obiektów i aktywów. Od uwierzytelniania biometrycznego po systemy oparte na RFID bezpieczne obiekty biurowe wykorzystują szereg środków kontroli dostępu w celu regulowania wejścia i monitorowania działań w pomieszczeniach. Wdrażając wielowarstwowe protokoły bezpieczeństwa, firmy mogą ograniczać ryzyko i utrzymywać bezpieczne środowisko pracy zarówno dla pracowników, jak i gości.

Kontrola dostępu w obiektach biurowych wykracza poza tradycyjne systemy oparte na kluczach, obejmując technologie innowacyjne, które oferują zarówno bezpieczeństwo, jak i wygodę. Wykorzystując platformy oparte na chmurze i mobilne dane uwierzytelniające, firmy mogą usprawnić procesy zarządzania dostępem przy jednoczesnym zachowaniu solidnych standardów bezpieczeństwa. Co więcej, integracja systemów kontroli dostępu z automatyką budynkową i inteligentnymi urządzeniami zwiększa wydajność operacyjną i komfort użytkowania. Pracownicy mogą płynnie poruszać się po bezpiecznych punktach wejścia, podczas gdy administratorzy zachowują pełną kontrolę nad uprawnieniami dostępu i ścieżkami audytu.

W sektorze mieszkaniowym technologie inteligentnego domu rewolucjonizują sposób, w jaki właściciele domów chronią swoje nieruchomości i bliskich. Od inteligentnych zamków po podłączone kamery monitorujące urządzenia te oferują możliwości zdalnego monitorowania i sterowania, zapewniając mieszkańcom spokój ducha. Integrując inteligentne systemy domowe z szerszymi ramami bezpieczeństwa miejskiego, miasta mogą wspierać wspólne podejście do bezpieczeństwa społeczności. Programy straży sąsiedzkiej i wspólne platformy danych umożliwiają mieszkańcom aktywne przyczynianie się do bezpieczeństwa ich otoczenia, tworząc bardziej odporne i wzajemnie połączone środowisko miejskie.

Podsumowując, rozwój bezpieczeństwa w miastach opiera się na wieloaspektowym podejściu, które obejmuje nadzór wideo, zarządzanie kryzysowe, kontrolę dostępu i integrację inteligentnych domów. Przyjmując najlepsze praktyki i wykorzystując technologie innowacyjne, miasta mogą tworzyć bezpieczniejsze i bardziej odporne środowiska dla wszystkich.

Konrad Fijołek
PREZYDENT MIASTA RZESZOWA

Kompleksowe podejście do cyberbezpieczeństwa

W ostatnich latach za sprawą pandemii oraz sytuacji geopolitycznej cyberbezpieczeństwo stało się jednym z podstawowych zagadnień, którymi muszą się zająć samorządy. W Rzeszowie jest to szczególnie ważne ze względu na nasze położenie, rolę, jaką pełnimy, i zainteresowanie świata, jakie budzimy od czasu, kiedy przyjęliśmy pod swoje dachy 100 tys. uchodźców z Ukrainy i od kiedy

jesteśmy hubem pomocowym. Inwestycja w SOC (Centrum Operacji Cyberbezpieczeństwa), w którego ramach pracujący specjaliści IT, wyposażeni w nowoczesne technologie i systemy, odpierają ataki cybernetyczne na infrastrukturę cyfrową miasta jest inwestycją w sprawne funkcjonowanie miasta i bezpieczeństwo mieszkańców.

Uzupełnieniem działań zapewniających cyberbezpieczeństwo są również odpowiednie działania edukacyjne podnoszące świadomość urzędników i mieszkańców w tym zakresie. To szkolenia i warsztaty uświadamiające, jakie zagrożenia mogą się pojawić i jak się przed nimi chronić.

Sławomir Świder

BIURO OBSŁUGI INFORMATYCZNEJ
I TELEKOMUNIKACYJNEJ W RZESZOWIE

Cyberbezpieczny Rzeszów

W Rzeszowie uruchomiliśmy SOC, pierwszą tego typu w kraju scentralizowaną jednostkę świadczącą usługi monitorowania, reagowania i zapobiegania cyberincydentom na rzecz podlegających miastu podmiotów. W ramach pojedynczej jednostki organizacyjnej SOC skupia nowoczesne technologie informatyczne, wyspecjalizowany personel oraz procedury i scenariusze zarządzania incydentami. Dzięki temu możliwe jest całodobowe monitorowanie sieci i szybka reakcja na potencjalne zagrożenia we wszystkich chronionych podmiotach.

W aspekcie technologicznym korzystamy z takich technologii, jak SIEAM/SOAR; XDR; NDR, dzięki czemu monitorujemy zarówno logi systemowe na urządzeniach sieciowych, serwerach i stacjach roboczych, jak i ruch sieciowy. Zaawansowane mechanizmy AI pozwalają wyłapywać automatycznie zagrożenia i anomalie oraz wspomagają w analizie i reagowaniu na wykryte incydenty.

Zespół Centrum Operacji Cyberbezpieczeństwa odpowiada również za poprawę strategii bezpieczeństwa miasta dzięki wyciąganiu wniosków z prowadzonego monitoringu bezpieczeństwa IT, np. poprzez propozycje zmian konfiguracji systemów czy też aktualizację procedur.

Centrum Operacji Cybrbezpieczeństwa w Rzeszowie spełnia również funkcję centrum kompetencyjnego na rzecz całego miasta. Umożliwia optymalizację kosztów związanych z cyberbezpieczeństwem, gdyż eliminuje potrzebę tworzenia analogicznych, mniejszych placówek lokalnych w każdej jednostce samorządu terytorialnego. •

Bezpieczne miasto, czyli jakie? Czy mieszkańcy polskich miast czują się bezpieczni?

Wojciech Kawa

EKSPERT DS. BEZPIECZEŃSTWA

„Bezpieczne miasto" to określenie, którego znaczenie w dużej mierze zależy po pierwsze od kontekstu, po drugie od tego, kto je stosuje. Władze samorządowe mówią głównie o ograniczeniu liczby wypadków oraz walce z przestępczością, teoretycy o rozwoju modelu smart city, a praktycy i aktywiści o planowaniu miast bezpiecznych dla pieszych, rowerzystów i osób w różnym wieku.

Natomiast mieszkańcy zwracają uwagę również na jakość powietrza i wody, zagrożenia naturalne (m.in. powódź, susza, burza, gradobicie, trąby powietrzne), zagrożenia chemiczne i biologiczne wód, gleby i powietrza, natężenie hałasu czy liczbę pożarów. Ważnymi dla nich kwestiami są potencjalne niebezpieczeństwa dnia codziennego, np. nieszczęśliwe wypadki i zdarzenia – na ulicy i w podróży (wypadki komunikacyjne, zamieszki, puszczone samopas psy). Ponadto zwracają uwagę na bezpieczeństwo w pracy, szkole, a także na relacje sąsiedzkie, zadbaną okolicę, komunikację, koszty życia, infrastrukturę i dostępność służby zdrowia. To wpływa na poczucie bezpieczeństwa.

Jeśli mówimy zatem o bezpiecznym mieście, to musimy pamiętać, że wiele zależy do tego, kto o nim mówi, jaki jest kontekst wypowiedzi i do czego porównuje swoje doświadczenia. Inaczej bowiem na bezpieczeństwo będzie patrzeć „mieszczuch", inaczej osoba mieszkająca na wsi. Co o ich doświadczeniach i przekonaniach mówią statystyki?

→

Statystyka vs rzeczywistość

Ponad 860 tys. – tyle przestępstw w 2022 r. odnotowała w całym kraju policja. Największa ich liczba (ponad 55 tys.) dotyczyła Warszawy. Ze względu na gęstość zaludnienia w policyjnych statystykach zwykle najgorzej wypadają miasta wojewódzkie, ale nie zawsze. Dla przykładu w śląskich Mysłowicach odnotowano blisko o 7 tys. przestępstw więcej niż w stolicy aglomeracji, czyli w Katowicach, gdzie było niemal 26 tys. naruszeń prawa. Na trzecim miejscu usytuował się Wrocław z liczbą 23,5 tys. stwierdzonych przestępstw.

W Polsce są 954 miasta – w tym 66 na prawach powiatu – i 302 gminy miejskie. Według danych GUS mieszka w nich 23 mln ludzi, co stanowi 60 proc. całej populacji. Postępująca urbanizacja sprawia, że przed polskimi miastami stoi coraz więcej wyzwań związanych m.in. z zapewnieniem bezpieczeństwa ich mieszańcom. Krajowa Mapa Zagrożeń Bezpieczeństwa publikowana przez Komendę Główną Policji oraz dane dotyczące przestępczości dowodzą, że to właśnie w ośrodkach miejskich notuje się największą liczbę incydentów, takich jak akty wandalizmu czy przekraczanie dozwolonej prędkości, oraz poważniejszych przestępstw typu pobicia czy kradzieże z włamaniem, kradzieże, oszustwa, uszkodzenia mienia, rozboje.

Z danych Komendy Głównej Policji i GUS-u wynika, że wciąż najwięcej różnego rodzaju wykroczeń i przestępstw rejestruje się na Śląsku, Dolnym Śląsku i w Małopolsce, gdzie występują jedne z większych skupisk ludzkich.

Życie w mieście oznacza, że mieszkańcy terenów zurbanizowanych są ponad 5-krotnie bardziej narażeni na kontakt z przestępczością niż mieszkańcy terenów wiejskich. Przynajmniej w Polsce, bo w Unii różnica jest „tylko" trzykrotna. Informacje te opublikował Eurostat w raporcie dotyczącym badania poziomu przestępczości w krajach Europy. Zgodnie z nim Polska to kraj wyjątkowo spokojny, bezpieczny.

Statystyki mają to do siebie, że w wersji surowej, niepoddane analizie mogą zaciemniać realny obraz. Konieczne są odpowiednia interpretacja danych i umiejscowienie ich w stosownym kontekście. Najlepszym przykładem takich informacji może być ta, że w czołówce miast najbardziej zagrożonych przestępczością (w przeliczeniu na 1000 mieszkańców) jest… Sopot. Rzecz w tym, że to nie mieszkańcy Sopotu mają problem z praworządnością. Za statystykami stoi ogromna liczba turystów przybywających każdego roku do tego kurortu. To na nich popełnianych jest wiele drobnych przestępstw. Statystyka bierze jednak pod uwagę liczbę stałych mieszkańców miasta, stąd takie wskaźniki.

Bezpieczeństwo jest zobiektywizowanym stanem braku zagrożenia, integralnie związanym z subiektywnym, emocjonalnym, psychologicznym odbieraniem przestrzeni jako bezpiecznej, inaczej poczuciem bezpieczeństwa. Prawdopodobieństwo, że ktoś stanie się ofiarą przestępstwa, wzrasta wraz z gęstością zaludnienia danego miejsca. W ostatnich pięciu latach ofiarą kradzieży padł co trzeci mieszkaniec miasta (34%), ale tylko co ósmy mieszkaniec wsi (13%). Prawie co piąty badany mieszkający w mieście (18%) doświadczył w tym okresie włamania do mieszkania lub domu. Respondentom mieszkającym na wsi przydarzało się to znacznie rzadziej (6%). Lęk o swoje bezpieczeństwo częściej wyrażają mieszkańcy większych miast (powyżej 100 tys. ludności) niż mieszkający w mniejszych miejscowościach.

Te dane potwierdzają, że przestępczość o charakterze ogólnym w poszczególnych regionach koncentruje się w miastach (metropoliach, aglomeracjach), a następnie z różnym natężeniem rozlewa się na obszar regionu. Po części można wskazać pewną prawidłowość, że w miarę procesu poszerzania się miast, szczególnie tych o charakterze metropolitalnym, następuje także rozprzestrzenianie się przestępczości (patrz: aglomeracja śląska).

Im większe miasto, tym lepiej nie wchodzić w zaułki

Przestępczość miejską charakteryzują pewne wzorce. Niektóre miejsca są bardziej kryminogenne niż inne. Centra miast, obszary o zróżnicowanym zagospodarowaniu, węzły transportowe itp. przyciągają przestępców bardziej niż dzielnice typowo mieszkaniowe. Pewne rodzaje użytkowania terenu „sprzyjają" popełnianiu wszelkiego rodzaju czynów zabronionych. Należą do nich sklepy, restauracje, lombardy, miejsca rozrywki, ale też stacje paliw, parkingi, dworce kolejowe, parkingi niestrzeżone. Z kolei są takie miejsca, których charakter i funkcja nie sprzyjają przestępczości (kościoły, cmentarze).

Miejscami ułatwiającymi dokonywanie przestępstw są te obiekty, które z powodu niedostatecznego i słabej jakości nadzoru mogą ułatwiać popełnienie przestępstwa. Najliczniejsze z nich to nieuporządkowane tereny otwarte, o niejasnym przeznaczeniu, niezagospodarowane i bez wiadomego właściciela, nieużytki, pustostany, zdegradowane tereny poprzemysłowe.

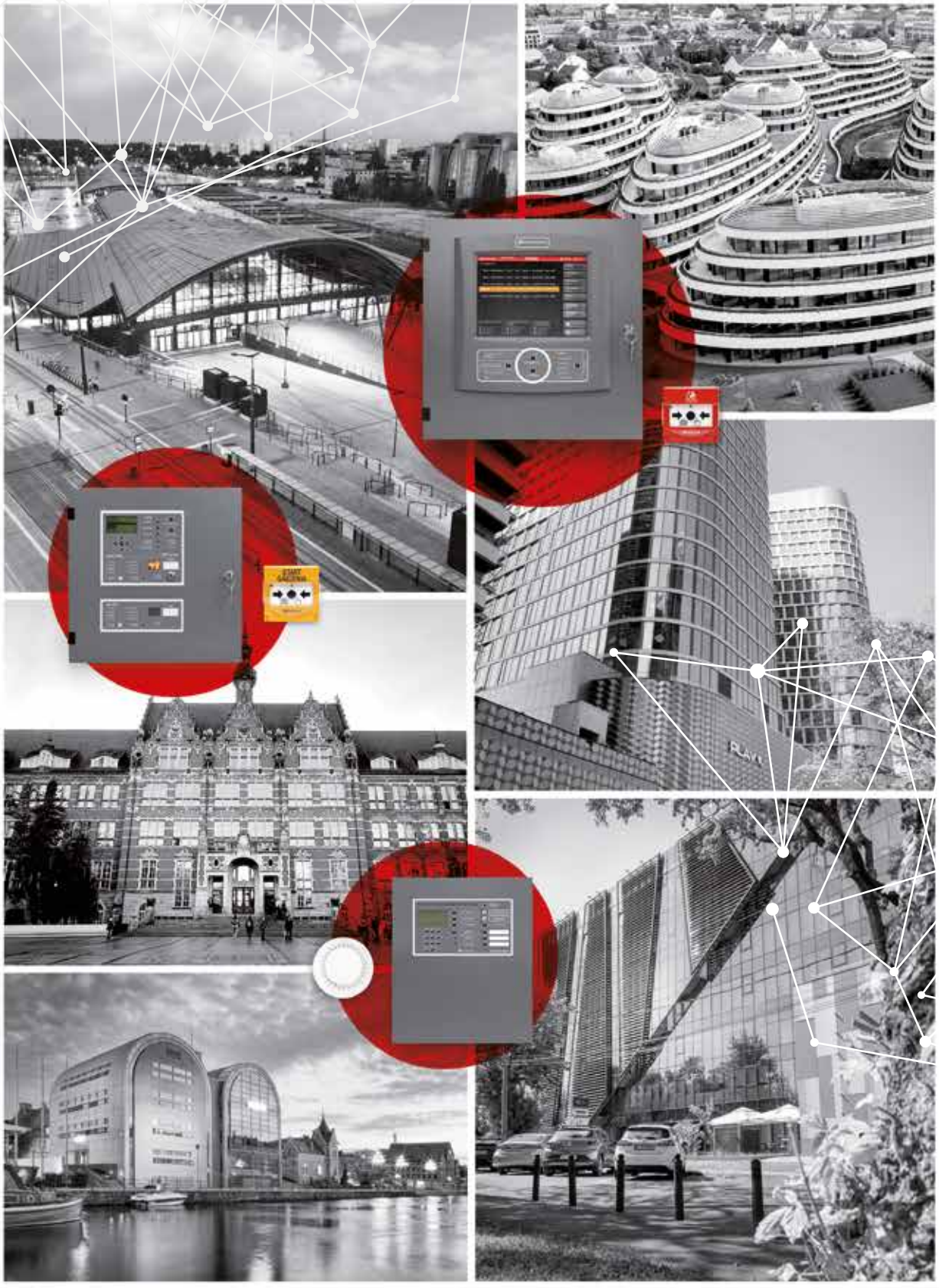
Z ostatnich badań CBOS-u wynika, że Polacy wyżej oceniają bezpieczeństwo w okolicy miejsca swojego zamieszkania niż ogólnie całego kraju. Niemal wszyscy ankietowani (96%) twierdzą, że mieszkają w miejscu bezpiecznym i spokojnym, a 88% uważa Polskę za bezpieczny kraj.

Większe poczucie bezpieczeństwa deklarują mieszkańcy wsi, mniejsze – mieszkańcy dużych i bardzo dużych miast. Na te deklaracje z pewnością wpływa sytuacja materialna ankietowanych. Im bardziej jesteśmy zamożniejsi, tym lepiej czujemy się chronieni.

W obecnym zarządzaniu bezpieczeństwem miejskim coraz częściej wspomagają nas nowoczesne technologie, bazujące na algorytmach sztucznej inteligencji i analizie ogromnych zbiorów danych dokonywanej w czasie rzeczywistym. Wykrywalność zagrożeń w przypadku tradycyjnego monitoringu wizyjnego ocenia się na 60%. Tymczasem system, w którym zastosowano technologie analityczne, oferuje skuteczność na poziomie 95%. Nie bez znaczenia jest fakt, że w przestrzeni miejskiej coraz częściej do ochrony są stosowane drony mogące docierać do trudno dostępnych miejsc. Warto także zwrócić uwagę na powszechne wykorzystywanie czujników i detektorów, dzięki którym służby są w stanie szybko zareagować w momencie wykrycia zagrożenia. W przestrzeni miejskiej powszechne są m.in. czujniki poziomu wód oraz detektory jakości powietrza służące do monitorowania zanieczyszczeń, czujniki poziomu hałasu, ruchu samochodowego, rowerowego i pieszego czy stanu infrastruktury miejskiej. Te nowoczesne urządzenia umożliwiają podjęcie natychmiastowej interwencji, również w zakresie prewencyjnym. Tak buduje się poczucie bezpieczeństwa. ●

Źródła: Statystyka Przestępczości Policji – dane za 2022 r. Dane Eurostatu dot. wskaźnika przestępczości w EU – dane z 2021 r. Dane GUS – ranking miast z najwyższym wskaźnikiem przestępstw stwierdzonych na 1000 mieszkańców – dane za 2022 r. Dane CBOS-u z 2023r dot. poczucia bezpieczeństwa Polaków.

POLON-ALFA



tradycyjnie KOMPLEKSOWA OCHRONA

tysięcy obiektów w kraju i za granicą

POLON-ALFA S.A. | 85-861 Bydgoszcz, ul. Glinki 155 | www.polon-alfa.pl

Czy Paryż wart jest igrzysk, a igrzyska Paryża?

Po co organizuje się Igrzyska Olimpijskie? Założenia są szczytne: promowanie sportu i zdrowego stylu życia, propagowanie pokoju i jedności, wzmacnianie wartości olimpijskich, takich jak przyjaźń, szacunek i fair play.

Monika Żuber-Mamakis

Jest jeszcze jeden cel – chyba najważniejszy – rozwój gospodarczy i promocja turystyki. A precyzyjnie rzecz biorąc, zysk. Zagrożenie bezpieczeństwa publicznego jest w tym przypadku wliczone w cenę. Co robi Francja, by cena ta była jak najniższa?

Szacuje się, że podczas Igrzysk Olimpijskich i Paraolimpijskich w Paryżu w 2024 r. stolicę Francji odwiedzi łącznie 15,3 mln gości. Jest to imponująca liczba, biorąc pod uwagę, że populacja regionu Île-de-France wynosi zaledwie 12,4 mln. Ile z tych osób będzie mieć niecne zamiary? Dla porównania podczas Letnich Igrzysk Olimpijskich w 2016 r. w Rio de Janeiro miasto odwiedziło 6,1 mln turystów, a podczas Igrzysk Olimpijskich w 2012 r. w Londynie 8,8 mln.

Czy gra jest warta świeczki?

Wzrost liczby turystów podczas igrzysk w Paryżu może mieć znaczący wpływ na miasto pod względem oferowanej bazy noclegowej, transportu i innych usług. Władze miasta, biorąc pod uwagę doświadczenia wcześniejszych olimpiad, przygotowują się na zalew turystów, inwestując w infrastrukturę i zwiększając liczbę dostępnych miejsc noclegowych. Wszystko to z nadzieją na zysk. Czy słusznie? Światło na tę sprawę rzuca praca Mateusza Kućmierczyka *Wpływ letnich igrzysk olimpijskich na gospodarki miast, regionów i krajów na przykładzie XXXI Olimpiady w Rio de Janeiro* (2018, „Przedsiębiorczość Międzynarodowa", 4[2], 119-135). Jak pisze autor: „Biorąc pod uwagę przedwojenne edycje igrzysk, pozytywny wydźwięk ekonomiczny, a więc zysk, pozostawiły po sobie przede wszystkim: londyńskie z 1908 r., sztokholmskie z 1912 r., a także te zorganizowane przez Los Angeles 20 lat później. Nieudane pod tym względem okazały się igrzyska w Paryżu w 1924 r. Po II wojnie światowej zysk przyniosły igrzyska w Londynie w 1948 r., natomiast stratę zanotowano po igrzyskach w Helsinkach w 1952 r. i w Melbourne w 1956 r.". Wspomniane na początku igrzyska w Londynie w 2012 r. „wniosły do brytyjskiej gospodarki ok. 16,5 mld GBP, a niemal 2 mld więcej, biorąc pod uwagę długoterminowe efekty związane z turystyką. W 2012 r. do Wielkiej Brytanii przybyło o 9% turystów więcej. Ich wydatki turystyczne w tym okresie wzrosły niemal dwukrotnie. Wydarzenie przyczyniło się także do utworzenia miejsc pracy, których to powstało 354 tys.".

Jak zatem widać, igrzyska mogą przynieść profity, ale nie muszą. Pewne jest tylko jedno: jak każda impreza masowa wymagają olbrzymich inwestycji w bezpieczeństwo. Im mniej stabilna sytuacja geopolityczna, tym większe muszą być starania organizatorów związane z zapewnieniem bezpieczeństwa. Obecną sytuację geopolityczną trudno uznać za stabilną. A imprezy masowe, takie jak igrzyska olimpijskie, są idealnym celem dla różnej maści ekstremistów. Historycznych przykładów zamachów dokonywanych podczas takich wydarzeń nie brakuje.

Podczas Letnich Igrzysk Olimpijskich w Monachium w 1972 r. członkowie palestyńskiej organizacji terrorystycznej Czarny Wrzesień zaatakowali izraelską drużynę olimpijską, zabijając 11 osób: sportowców i trenerów. W roku 1996, w czasie Letnich Igrzysk Olimpijskich w Atlancie, eksplodowała bomba w Parku Olimpijskim, zabijając 2 osoby i raniąc ponad 100. W 2013 roku podczas maratonu w Bostonie dwie bomby wybuchły w pobliżu linii mety. Zginęły wówczas 3 osoby, ponad 260 było rannych. Przykłady mniej znane to atak z użyciem broni palnej w marcu 2009 r. w Lahore na drużynę krykieta ze Sri Lanki, zamach samobójczy podczas meczu siatkówki w Laki Marwat, w północno-zachodnim Pakistanie w 2010 r. oraz atak z użyciem broni palnej w Cabindzie w Angoli wymierzony w reprezentację Togo w piłce nożnej. Najnowszy, głęboko poruszający przykład to atak terrorystyczny w Crocus City Hall w Krasnogorsku pod Moskwą. Zamaskowani napastnicy otworzyli wówczas ogień w hali koncertowej. Doszło także do eksplozji i pożaru. Rosyjski komitet śledczy poinformował o 133 ofiarach śmiertelnych.

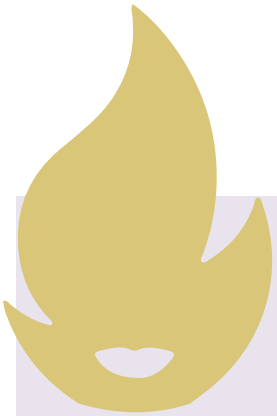
Imprezy masowe, takie jak igrzyska olimpijskie, stanowią dla terrorystów łatwy cel. Nie można jednak zapominać o innym aspekcie związanym z ich bezpieczeństwem: nieszczęśliwym wypadku będącym efektem błędu ludzi, zaniechania czy zwykłej głupoty.

29 maja 1985 r., przed finałowym meczem Pucharu Europy pomiędzy Juventusem a Liverpoolem, na stadionie Heysel w Brukseli doszło do starć między angielskimi i włoskimi kibicami. Około godziny 19.00 fani Liverpoolu bez problemu przedarli się przez niskie ogrodzenie i zaatakowali kibiców Juventusu. Włoscy kibice rzucili się do ucieczki, tratując się nawzajem. Część osób została przygnieciona trzymetrową ścianą, która zawaliła się pod naporem tłumu. W wyniku tych wydarzeń śmierć poniosło 39 osób, a około 600 zostało rannych. 4 listopada 1994 r. wybuchł pożar w hali Stoczni Gdańskiej, życie straciło wówczas 7 osób, ponad 300 osób uległo poparzeniu. Podczas studenckiej zabawy inaugurującej rok akademicki na Uniwersytecie Technologiczno-Przyrodniczym w Bydgoszczy w nocy z 14 na 15 października 2015 r., w wąskim korytarzu łączącym dwa budynki doszło do paniki, w wyniku czego zginęły 3 osoby, a kilkanaście osób zostało poszkodowanych. We wszystkich tych przypadkach zdecydowanie coś poszło nie tak.

Ważne, żeby w gazetach pisali

Jak zauważa Paulina Piasecka, była główna specjalistka Wydziału ds. Przeciwdziałania Zagrożeniom Terrorystycznym Departamentu Bezpieczeństwa Publicznego MSWiA, sekretarz Centrum Badań nad Terroryzmem Collegium Civitas w Warszawie: „Najważniejszym czynnikiem decydującym o wyborze celu ataku są jego konsekwencje medialne i propagandowe. Zamach terrorystyczny musi zyskać odpowiedni rozgłos, być wystarczająco spektakularny, aby jak najdłużej przyciągał uwagę zglobalizowanych mediów, a za ich pośrednictwem – światowej opinii publicznej. Ofiary w ludziach i szkody materialne są niezbędne do wywołania odpowiedniego natężenia strachu, a nawet paniki, która pochodzi z przekonania, że nikt nie jest bezpieczny, bo nie wiadomo, co będzie następnym

→



> *Igrzyska olimpijskie mogą przynieść profity, ale nie muszą. Pewne jest tylko jedno: jak każda impreza masowa wymagają olbrzymich inwestycji w bezpieczeństwo.*

celem ataku" *(Imprezy masowe, jako cel zamachów terrorystycznych,* konferencja „Badania Operacyjne i Systemowe – BOS 2008").

Letnie Igrzyska Olimpijskie w Paryżu w 2024 r. wymagają zatem od organizatorów podjęcia kompleksowych działań w celu zapewnienia bezpieczeństwa uczestnikom i kibicom. Władze Francji podejmują szereg środków, aby zminimalizować ryzyko zagrożeń terrorystycznych podczas tego wydarzenia. Międzynarodowy Komitet Olimpijski w tym przypadku nadzieję pokłada w organizatorach. Tuż po zamachu w podmoskiewskiej sali koncertowej, do którego doszło 22 marca tego roku, opublikował oświadczenie: „Jak zawsze odpowiedzialność za bezpieczeństwo spoczywa na władzach lokalnych. Poinformowały one MKOl, że od kilku lat pracowano przy założeniu, że wymagane będą najwyższe możliwe środki bezpieczeństwa. Jak zwykle istnieje również bardzo ścisła współpraca międzynarodowa. Na podstawie tego oraz regularnych raportów, które MKOl otrzymuje od nich, mamy pełne zaufanie do władz francuskich i ich ścisłej współpracy z partnerami międzynarodowymi".

Na czym polega wspomniana współpraca? Francja powołała międzynarodową koalicję, do której dołączyły m.in. Siły Zbrojne RP. Polska skieruje do Paryża grupę zadaniową żołnierzy, w tym przewodników z psami, których zadaniem będzie wykrywanie ładunków wybuchowych i przeciwdziałanie aktywności terrorystycznej. Poinformował o tym Władysław Kosiniak-Kamysz, minister obrony narodowej, który na platformie X (dawniej Twitter) napisał: „Siły Zbrojne RP dołączą do międzynarodowej koalicji powołanej przez Francję w celu wsparcia przygotowań i zabezpieczenia Letnich Igrzysk Olimpijskich w 2024 r. Do Paryża zostanie skierowana grupa zadaniowa naszych żołnierzy, w tym przewodników z psami. Jej głównym celem będzie podejmowanie działań związanych z wykrywaniem ładunków wybuchowych i przeciwdziałanie zjawiskom terrorystycznym". Minister spraw wewnętrznych Francji zapewnił, że wszystkie służby, w tym wywiad, będą w pełnej gotowości, aby zapewnić bezpieczeństwo igrzysk. Wspomniany wcześniej zamach w Krasnogorsku pod Moskwą spowodował, że władze Francji od razu podniosły stopień zagrożenia terrorystycznego do najwyższego poziomu.

Pod dachami Paryża – ograniczenia w ruchu

Po raz pierwszy w historii ceremonia otwarcia igrzysk nie odbędzie się na głównym stadionie, ale na barkach na Sekwanie, co również wymaga specjalnych środków bezpieczeństwa, m.in. wstrzymania żeglugi na rzece. Władze Francji już jednak ustąpiły – zaprotestowali m.in. rolnicy, którzy barkami przewożą zboże. Sekwana ma być dla nich niedostępna przez 6 dni, z 12 planowanych. W pozostałe dni igrzysk będzie spławna, co nie zmienia faktu, że ciągle jest brudna. Pod znakiem zapytania stoi więc np. rywalizacja triathlonistów oraz walka o olimpijskie złoto na otwartym akwenie na dystansie 10 km. Z jednej strony dla organizatorów kłopot, z drugiej – przynajmniej tym odcinkiem bezpieczeństwa nie trzeba się martwić. A martwić jest się czym, już bowiem miał miejsce incydent związany z bezpieczeństwem. Pracownik urzędu miasta Paryża zgłosił kradzież laptopa, na którym znajdował się plan zabezpieczenia igrzysk. Władze zapewniają jednak, że podjęły odpowiednie środki, aby zapobiec podobnym incydentom.

Jakie to środki? Po pierwsze, od 22 marca na terenie Francji obowiązuje najwyższy stopień zagrożenia terrorystycznego definiowanego przez francuski system powiadamiania o bezpieczeństwie narodowym Vigipirate (akronim z fr. *Vigilance et Protection des Installations contre les risques d'attentats terrorystes à l'explosif,* czyli nadzór i ochrona obiektów przed ryzykiem terrorystycznych ataków bombowych), oznaczający wysokie ryzyko zamachów. Władze przewidują wzmożone środki bezpieczeństwa w związku z tym zagrożeniem. Po drugie, Francja jako pierwszy kraj UE będzie wydawać wizy online dla 70 tysięcy sportowców, dziennikarzy i innych osób przyjeżdżających na igrzyska spoza strefy Schengen. System elektronicznego aplikowania o wizę Schengen ma usprawnić cały proces, a jednocześnie zwiększyć bezpieczeństwo dzięki lepszej kontroli nad przybywającymi. Po trzecie, wspomniane już ograniczenie żeglugi na Sekwanie. Po czwarte, policja, żandarmeria i francuski wywiad będą w pełnej gotowości, aby zapewnić bezpieczeństwo igrzysk. Niektórzy parlamentarzyści uznali jednak, że zapowiedziane przez prefekta policji Laurenta Nuñeza działania nie są w żaden sposób nadzwyczajne, a typowe dla… stanu wyjątkowego, a nie takiego, który w Planie Vigipirate jest określony jako czwarty, czyli najwyższy możliwy i jaki został wprowadzony. Środki, o których Nuñez mówił, m.in. w wywiadzie dla dziennika „Le Parisien", to plan, który przewiduje, że w trakcie igrzysk na ulicach miasta będzie obecnych codziennie od 15 tys. do 45 tys. funkcjonariuszy i zostanie ograniczona swoboda przemieszczania się.

W tym celu zostaną zainstalowane specjalne bariery, a pierwszeństwo w dostępie do obiektów będą mieli sportowcy i osoby akredytowane. Aby ułatwić poruszanie się w centrum miasta, zostanie wyznaczony specjalny obwód komunikacyjny, obejmujący takie miejsca jak Trocadero, Pole Marsowe, wieżę Eiffla, okolice Grand Palais i placu Inwalidów. Ma to na celu ułatwienie organizacji ruchu w kluczowych dla metropolii rejonach podczas igrzysk. Prefekt francuskiej policji powiedział, że w planach jest także wprowadzenie rejestracji na platformie cyfrowej poprzez przedstawienie dowodu podróży z kodem QR wszystkich kibiców oraz prowadzenie wyrywkowych ich kontroli. Takie same procedury będą dotyczyć osób, które ceremonię otwarcia planują oglądać z okien pobliskich apartamentów.

Igrzyska Olimpijskie w Paryżu rozpoczną się 26 lipca i potrwają do 11 sierpnia. Jednym z najważniejszych zadań, jeśli nie najważniejszym, jest zapewnienie bezpieczeństwa, w tym cyberbezpieczeństwa. Organizatorzy spodziewają się bezprecedensowej fali cyberzagrożeń spotęgowanych przez rozwój technologii takich jak sztuczna inteligencja. Analitycy przewidują, że w związku z igrzyskami wydatki na usługi cyberbezpieczeństwa w Europie wzrosną o 150 mln USD.

WSPÓŁPRACA MIĘDZYNARODOWA

- Francja powołała koalicję międzynarodową, do której dołączyły m.in. Siły Zbrojne RP. Polska skieruje do Paryża grupę zadaniową żołnierzy, w tym przewodników z psami, których zadaniem będzie wykrywanie ładunków wybuchowych i przeciwdziałanie aktywności terrorystycznej.

WZMOCNIENIE SIŁ BEZPIECZEŃSTWA

- Policja, żandarmeria i francuski wywiad będą w pełnej gotowości, aby zapewnić bezpieczeństwo igrzysk.
- Rząd Francji podniósł stopień zagrożenia terrorystycznego do najwyższego poziomu po zamachu w Krasnogorsku pod Moskwą.

OCHRONA INFRASTRUKTURY

- Zainstalowanie barier uniemożliwiających swobodne poruszanie się, pierwszeństwo będą mieli sportowcy i osoby akredytowane.
- Wyznaczenie dużego obwodu komunikacyjnego z dwoma poziomami w centrum miasta, aby ułatwić poruszanie się.
- Wprowadzenie ograniczenia ruchu, mieszkańcy będą mogli się przemieszczać na podstawie specjalnego zezwolenia.

Jednocześnie prawie 15 tys. żołnierzy ma strzec bezpieczeństwa podczas igrzysk, z czego 10 tys. będzie stacjonować w rejonie Île-de-France, a ok. 5 tys. żołnierzy będzie zakwaterowanych w namiotach na terenie La Pelouse de Reuilly, blisko centrum Paryża. W sumie prawie 30 tys. policjantów i żandarmów oraz 17 tys. agentów ochrony będzie każdego dnia czuwać nad bezpieczeństwem igrzysk olimpijskich i późniejszej paraolimpiady. Władze robią wszystko, aby zminimalizować ryzyko zagrożeń terrorystycznych. Pozostaje otwarta kwestia cyberzagrożeń.

Czy ma ktoś długopis?

Globalne imprezy sportowe, takie jak igrzyska olimpijskie i mistrzostwa Europy w piłce nożnej, stale zmagają się z rosnącą liczbą ataków cybernetycznych. Podczas Mistrzostw Świata w 2022 r. odnotowano oszustwa związane z zakładami sportowymi i sprzedażą biletów. Dostawca usług streamingowych FuboTV został zaatakowany, co zakłóciło transmisje meczów. Badania pokazują, że 70% organizacji sportowych pada ofiarą co najmniej jednego ataku cybernetycznego rocznie. Zagrożenia obejmują nie tylko kradzież danych, ale także oszustwa finansowe i manipulację wynikami. Popularność sportu i wynikające z niej duże przychody czynią wszystkie wydarzenia sportowe kuszącym celem dla cyberprzestępców. Jak poinformowała firma NTT odpowiedzialna za bezpieczeństwo IT podczas igrzysk w Tokio w 2021 r. odnotowano 450 mln cyberataków. To dwukrotnie więcej niż w Londynie w 2012 r. Co znaczy, że teraz może być ich jeszcze więcej, choćby ze względu na to, że hakerzy także ułatwiają sobie życie za pomocą sztucznej inteligencji.

Francuska Krajowa Agencja ds. Bezpieczeństwa Systemów Informatycznych (ANSSI) stara się trzymać rękę na pulsie i ostrzega przed zbliżającymi się zagrożeniami cyberbezpieczeństwa związanymi z tym długo oczekiwanym wydarzeniem. Szef ANNSI Vincent Strubel nie ma złudzeń. W wywiadzie udzielonym AFP w marcu tego roku powiedział: „Bez wątpienia celem będą igrzyska olimpijskie. (…) Przygotowujemy się na wszelkiego rodzaju ataki. Takie same jak te, z którymi mamy do czynienia na co dzień, ale jeszcze częstsze". Dodał, że możliwe są „ataki ze strony państw, które chcą zakłócić igrzyska (…) i które mogłyby próbować zakłócić ceremonię otwarcia lub spowodować problemy z transportem publicznym". Strubel wspomniał też, że cyberataki wspierane przez jakieś państwo to jedno z trzech głównych zagrożeń, z którymi trzeba się liczyć. Pozostałe to cyberprzestępcy próbujący wyłudzić pieniądze oraz hakerzy chcący sprawić kłopoty dla zabawy lub rozgłosu. „Dla mnie najgorszy scenariusz jest taki, że zostaniemy zasypani atakami na nieistotne obiekty, więc umknie nam poważniejszy atak wymierzony w krytyczną infrastrukturę transportową lub energetyczną odgrywającą kluczową rolę podczas igrzysk" – powiedział w wywiadzie dla AFP. Z kolei cytowana przez AFP Betsy Cooper, ekspertka ds. cyberbezpieczeństwa amerykańskiego Aspen Institute, obawia się o rejestrację wyników. „Zakłócanie kamer na mecie, manipulowanie systemem sędziowskim Hawk-Eye, usuwanie czasów, manipulowanie tablicami wyników. Sposobów zakłócenia jest wiele" – wymieniła. Zaleca, aby sędziowie stosowali stary sprawdzony sposób, czyli zapisywali wyniki na papierze.

W stosowne notesy powinni się jednak zaopatrzyć wcześniej, gdyż już teraz władze Francji poprosiły bookinistów, by zeszli z bulwarów nad Sekwaną, gdzie handel używanymi książkami, kalendarzami, pocztówkami i notesami ma już ponad 450-letnią tradycję.

Otwarte pozostaje zatem pytanie, czy Paryż wart jest igrzysk, a igrzyska Paryża (bo że wart był mszy, to wiadomo). Jak powiedział prof. Władysław Bartoszewski: „Na pewno nie wszystko, co warto, to się opłaca, ale jeszcze pewniej (…) nie wszystko, co się opłaca, to jest w życiu coś warte". ●

Czym jest ransomware? Poznaj sposób jego ataków i dowiedz się, jak się przed nim bronić

Ransomware to rodzaj złośliwego oprogramowania, który ma na celu zainfekowanie komputera, zaszyfrowanie plików lub zablokowanie całego systemu. Następnie atakujący żądają okupu w zamian za dostarczenie klucza deszyfrującego lub narzędzia odblokowującego.

Typowe metody ataków *ransomware* obejmują złośliwe załączniki do wiadomości e-mail, fałszywe strony internetowe lub wykorzystywanie luk w zabezpieczeniach systemu w celu uzyskania dostępu do komputera ofiary. Po pomyślnym zainfekowaniu oprogramowanie zaczyna szyfrować pliki, czyniąc je niedostępnymi dla właściciela, a następnie wyświetla żądanie okupu. Zazwyczaj takie żądania mają określony termin, a niezapłacenie okupu w wyznaczonym czasie może skutkować groźbą usunięcia zaszyfrowanych danych lub publicznego ujawnienia informacji o ich zawartości.

Ransomware atakuje różne gałęzie przemysłu, w tym instytucje finansowe, agencje rządowe, szkoły, szpitale i wiele innych. Może infekować dyski lokalne i rozszerzać swój wpływ na wszystkie podłączone urządzenia, a nawet wymazywać całe sieci i kopie zapasowe danych za jednym razem. Chociaż odzyskanie danych bez płacenia okupu jest czasami możliwe, może być czasochłonne i kosztowne, jeśli ofiara jest nieprzygotowana lub stoi w obliczu ukierunkowanego ataku. Aby zapobiec działaniom *ransomware*, organizacje powinny starannie zarządzać bezpieczeństwem poczty e-mail, zabezpieczeniami sieci, regularnie aktualizować systemy i tworzyć kopie zapasowe krytycznych danych.

Ransomware to rosnące i trwałe zagrożenie

Pierwszy atak *ransomware* miał miejsce w 1989 r. W tamtym czasie 90 prób usunięcia programu przez użytkownika i ponowne uruchomienie komputera spowodowało zaszyfrowanie wszystkich folderów. Dane pozostałyby niedostępne, chyba że dokonano by płatności na określone konto podane przez oszusta w celu uzyskania klucza deszyfrującego. Współczesne ataki ransomware są bardziej wyrafinowane i kosztowne. Pomimo gwałtownego wzrostu liczby cyberataków przed pandemią incydenty nie ustąpiły wraz z jej złagodzeniem. W regionie Azji i Pacyfiku odnotowano 22-proc. wzrost średniej tygodniowej liczby ataków cybernetycznych na organizację. W skali globalnej roczna stopa wzrostu utrzymuje się na poziomie blisko 40%.

Co więcej, firmy po doświadczeniu ataku często potrzebują kilku tygodni lub miesięcy na odzyskanie danych. Alarmujące jest to, że aż 71% przedsiębiorstw nie jest w stanie przywrócić swoich danych po ataku. Nawet zapłacenie okupu nie gwarantuje odzyskania dostępu do plików. Według statystyk 50% organizacji nadal traci niektóre pliki, a 13% nawet wszystkie. Dlatego zrozumienie wzorców zachowań oprogramowania *ransomware* i wdrożenie środków zapobiegawczych ma kluczowe znaczenie. Dla firm jest to fundament zapewnienia bezpieczeństwa danych i utrzymania ciągłości prowadzonej działalności.

Zrozumienie zachowań oprogramowania ransomware i sposoby zapobiegania tym atakom

Ataki za pomocą *ransomware* stały się lukratywnym biznesem dla grup hakerskich specjalizujących się w ukierunkowanych atakach na organizacje. Pierwszym krokiem, by uniknąć zainfekowania firmowej infrastruktury IT, jest zrozumienie, jak działają hakerzy. Zazwyczaj wykonują oni następujące kroki:

- **Obserwacja** – zbieranie informacji o celach ataków.
- **Infiltracja** – nakłanianie do klikania w złośliwe linki (wykorzystywanie luk w systemie lub oprogramowaniu w celu infiltracji, a następnie łączenie się ze stacją przekaźnikową).

Lista kontrolna bezpieczeństwa cyfrowego

Liczba urządzeń podłączonych do sieci stale rośnie, dlatego polecamy sprawdzenie swojej infrastruktury IT za pomocą bezpłatnej listy kontrolnej Synology. Wystarczy zeskanować kod QR, aby bezpłatnie pobrać listę kontrolną bezpieczeństwa cyfrowego.

Już na pierwszy rzut oka widać, co już jest dobrze chronione, a gdzie jeszcze jest miejsce na ulepszenia. Przejdź krok po kroku przez wszystkie ważne punkty bezpieczeństwa. Każde zaznaczone pole wyboru odpowiada punktowi. Im więcej punktów, tym lepiej. W sumie można zdobyć 44 punkty.

Nie poddawaj się i chroń cenne dane!

Zeskanuj kod QR i pobierz bezpłatną listę kontrolną, aby sprawdzić, jak bezpieczna jest infrastruktura IT w twojej firmie.

- **Ukrywanie się** – przygotowanie do ataku, które może trwać dłuższy czas, ciągłe zbieranie informacji organizacyjnych i pozyskiwanie krytycznych danych.
- **Zniszczenie i atak** – szyfrowanie oryginalnych danych u źródła i usuwanie kopii zapasowych.
- **Negocjacje** – jeśli negocjacje zawiodą, hakerzy mogą ujawnić istotne dla firmy informacje lub bezpośrednio je usunąć.

Ochrona przed *ransomware* polega na aktualizowaniu systemów i oprogramowania, instalowaniu oprogramowania antywirusowego i białej listy, szkoleniu pracowników, aby nie pobierali nieznanych aplikacji i byli czujni na najnowsze zagrożenia *ransomware*. Kluczowe znaczenie ma regularne wykonywanie kopii zapasowych danych z funkcjami niezmienności. W przypadku ataku przyspieszenie procesu odzyskiwania danych zapewnia nieprzerwaną działalność biznesową.

Rozwiązania służące ochronie danych, takie jak dostarczane przez Synology, stają się kluczowe we wzmacnianiu organizacji przed atakami *ransomware*. Kompleksowa ochrona danych Synology zapewnia najwyższy poziom bezpieczeństwa, dostępności i przywracalności, ułatwiając skuteczną ochronę przed atakami *ransomware*.

Rozwiązanie do tworzenia kopii zapasowych i odzyskiwania danych po awarii dzięki Synology Data Protection Solution

W obliczu stale rosnącego zagrożenia ze strony oprogramowania *ransomware* znaczenie ochrony danych staje się coraz bardziej oczywiste. *Ransomware* powoduje milionowe straty każdego roku i pomimo środków zapobiegawczych problem ten nie ustępuje. Co więcej, hakerzy mogą próbować licznych ataków, podczas gdy organizacje mają tylko jedną szansę na obronę przed nimi. W takim środowisku rozwiązania do ochrony danych stają się kluczem do zabezpieczenia organizacji przed atakami *ransomware*.

Firma Synology zapewnia kompleksową ochronę, gwarantując najwyższy poziom bezpieczeństwa. W przypadku ataku można szybko uruchomić odzyskiwanie danych, zapewniając nieprzerwaną działalność biznesową. Rozwiązania Synology pomagają personelowi IT w pełnym wdrożeniu ochrony danych, gwarantując bezpieczeństwo, dostępność i możliwość odzyskania danych firmowych, skutecznie powstrzymując ataki typu *ransomware*. ●

Synology GmbH
Grafenberger Allee 295
40237 Düsseldorf
Germany

Kamery nasobne – możliwości i ograniczenia stosowania

Urządzenia mają to do siebie, że stosowane są głównie wtedy, kiedy są użyteczne. Obserwując wykorzystanie urządzeń w ochronie obiektów i obszarów, można wyciągnąć ciekawe wnioski. Jeżeli użytkownik ma trudności ze zrozumieniem zasad użycia lub obsługą, nie będzie korzystał z urządzeń lub będzie robił to źle. Czasami będzie to działanie nieświadome, ale czasami świadome, by ukryć łamanie procedur lub prawa.

Cezary Mecwaldowski

Gdziekolwiek się znajdujemy, w zasięgu wzroku widać jakąś kamerę. Jednak nie zawsze systemy monitoringu działają skutecznie. Gdy dochodzi do zdarzenia, okazuje się, że parametry kamer dozorowych były niewystarczające, optyka i ustawienie nie obejmowały miejsca wydarzenia albo kamera obrotowa „patrzyła" akurat w inne miejsce. Wtedy ujawniają się zalety kamer nasobnych, które przydają się szczególnie wtedy, gdy służba ochrony wchodzi w przestrzenie niepoddane monitoringowi wizyjnemu przez systemy VSS *(Video Surveillance System)* lub przemieszcza się np. w konwoju. Zaletą kamer nasobnych jest także to, że osoby nieupoważnione mają skrajnie utrudniony dostęp do materiału zapisanego na danym urządzeniu. Dopóki materiał nie zostanie zapisany w sieci, dopóty można uznać, że jest on niedostępny.

Paradoksalnie to nie parametry techniczne decydują o tym, czy dana technologia jest w użyciu, tylko procedury jej stosowania. Obecne oczekiwania dotyczące kamer nasobnych ograniczają się głównie do bezawaryjnej funkcjonalności, niewymagającej troski użytkownika. Mają działać. Służby ochrony są wyposażone w wiele urządzeń: środki ochrony, środki łączności, broń palną i środki przymusu bezpośredniego, a to nie sprzyja obsłudze jeszcze innych narzędzi. Wymaga szeregu ćwiczeń podczas szkoleń, które wyposażą użytkownika w nawyki niezbędne do skutecznej reakcji na dynamiczne, silnie stresujące zdarzenia.

Niektóre parametry techniczne takie jak czas pracy akumulatora, czas ładowania i kopiowania zapisu na serwery kolidują z procedurami. Wracają sytuacje i doświadczenia służb z wykorzystaniem kamer nasobnych, które pojawiały się w pierwszych latach ich wprowadzenia na rynek. Dochodziło wtedy do sytuacji, że kamera nasobna nie zarejestrowała jakiegoś incydentu, bo nie zostało włączone nagrywanie albo urządzenie było zamontowane niezgodnie z założeniami lub akumulator był rozładowany. Takie przykłady pokazują, jak istotne są procedury stosowania kamer nasobnych, określenie, czy zapis uruchamia się automatycznie, czy ręcznie przez użytkownika, to czy można w takiej kamerze podmienić akumulator i na tej podstawie twierdzić, że był rozładowany w czasie zdarzenia itp. Również miejsce mocowania kamery nie jest przypadkowe, powinno zależeć od optyki kamery i ma znaczenie taktyczne. Miejsce ma być tak dobrane, by użytkownik mógł np. bez trudu ją uruchomić podczas pościgu, udzielania pierwszej pomocy itp. Także wtedy, gdy niezbędne okaże się zdjęcie kamizelki lub hełmu (a tam akurat zamocowano kamerę).

Na potrzeby dowodowe znaczenie ma także zapis przed zdarzeniem i po nim (tzw. pre- i postzdarzeniowe czasy zapisu). Jeżeli zapis uruchamiany jest np. sensorem w kaburze broni palnej lub paralizatora czy otwarcia drzwi pojazdu, naciśnięcia przycisku napadowego itp., istotnym dla procesu dochodzeniowego może być zapis, co działo się chwilę przed incydentem.

Kiedy użytkowników i kamer nasobnych jest więcej, należy zadbać o to kto, kiedy i którą kamerę może pobrać. Ważne, aby było wiadomo, gdzie znajduje się zapis z konkretnego zdarzenia,

kto był jego uczestnikiem, kiedy zdarzenie miało miejsce oraz czy pobrana kamera była gotowa do użycia, czyli sprawna i przygotowana do zapisu tak, by nie doszło do nadpisania wcześniejszego materiału, który nie został jeszcze skopiowany do archiwum. Użyteczne są stacje ładująco-archiwizujące z czytnikami RFID, pozwalające użytkownikowi pobrać i aktywować do pracy konkretną kamerę. Inne rozwiązania to systemy integrujące zabezpieczenia elektroniczne (np. PSIM) wspomagające użytkowników kamer lub depozytory (również z wbudowanymi stacjami do ładowania i archiwizowania nagrań).

Przypadki niewłączenia nagrywania, włączenia bez dźwięku, włączenia kamery zbyt późno wcale nie są rzadkie. Istnieje kilka sposobów, by do takich sytuacji nie dochodziło. Każdy ma zalety i wady, które warto przeanalizować.

Ręczne uruchamianie nagrywania. Wadą tego rozwiązania jest to, iż nagrywanie może nie zostać uruchomione, wyłączone za wcześnie lub uruchomione za późno (nawet przy uwzględnieniu czasu pre- i postzdarzeniowego nagrywania). Zaletą może być mniejsza liczba nagrań prawidłowo wybranych zdarzeń. Mniej miejsca zajmą nagrania w archiwum, mniej czasu będzie potrzeba na ich przeglądanie.

Automatyczne uruchamianie nagrywania inicjowane pobraniem kamery, harmonogramem, sensorem (np. czujnikiem w kaburze broni palnej, paralizatora, otwarciem drzwi pojazdu, przyciskiem antynapadowym, sygnałem zdalnym itp.). Wadą takiego rozwiązania może być duża liczba nagrań, ale z niewielką liczbą zarejestrowanych zdarzeń oraz niepełne ich uchwycenie. Zaletą będzie znacznie mniejsze ryzyko nieuruchomienia zapisu, w odróżnieniu od uruchamiania ręcznego. Wariantem działania automatycznego będzie ciągłe nagrywanie uruchamiane choćby w momencie pobrania kamery nasobnej przez użytkownika.

Hybrydowe uruchamianie nagrywania. Włączenie i wyłączenie nagrywania może następować zarówno ręcznie, jak i automatycznie. Wadą tego sposobu może być duża liczba nagrań niekoniecznie związanych z wydarzeniami istotnymi. Zaletą mniejsze ryzyko niewłączenia nagrywania przez użytkownika w określonych przypadkach (zadziałanie sensora).

Innym ważnym aspektem stosowania kamer nasobnych jest kwestia nagrywania wizerunku osób i głosu, których przetwarzanie musi spełniać rygory RODO. Stosowanie kamer nasobnych komplikuje się, kiedy służby są zmuszone do zastosowania środków przymusu bezpośredniego, kontroli osobistej lub ratowania życia. Takie kwestie wydają się nie komplikować stosowania kamer nasobnych, jednak w sytuacji zagrożenia, silnego stresu najprostsze czynności stanowią trudność nie zawsze do pokonania bez odpowiedniego wyszkolenia.

Podczas przemieszczania się służb ochrony z kamerą nasobną poza obszarem, obiektem chronionym czy w trakcie konwoju może dojść do nagrywania danych osobowych szczególnie chronionych lub innych informacji prawnie chronionych. Należy przewidzieć odpowiednie procedury do takich sytuacji. – *Stosowanie monitoringu jest szczególnie inwazyjną formą przetwarzania danych osobowych. Jego wprowadzenie powinno podlegać zatem wyjątkowo wnikliwej ocenie również na etapie prac legislacyjnych. Dlatego zgodnie z RODO jednym z priorytetów (...) powinno być przeprowadzenie oceny skutków planowanych operacji przetwarzania dla ochrony danych (art. 35 ust. 1, 7 RODO)* – komunikuje UODO. Osoby nagrywane powinny mieć przynajmniej świadomość, kto jest administratorem ich danych oraz gdzie mogą uzyskać więcej informacji. Wymaga tego zasada przejrzystości sformułowana w art. 5 ust. 1 lit. RODO, która stanowi, że wszelkie informacje i wszelkie komunikaty związane z przetwarzaniem danych osobowych muszą być łatwo dostępne i zrozumiałe oraz sformułowane jasnym i prostym językiem. Obowiązujące ustawodawstwo nakłada również na osoby wykonujące zawody medyczne obowiązek zachowania tajemnic zawodowych.

Nie zawsze kamery nasobne stosowane są we własnym obiekcie, ale na przykład przez konwojentów lub patrole służb bezpieczeństwa, pojawiając się doraźnie w różnych obszarach, śluzach ochronnych. Pojawienie się osób z kamerami nasobnymi w miejscach, gdzie dochodzi do ujawniania tajemnic, jak chociażby tajemnica lekarska, ekrany monitorów wyświetlające tajemnice instytucji lub firm, leżące dokumenty na biurkach, rozmowy itp. wymaga dostosowanych do takich sytuacji procedur[1]. Nie posiadając uprawnień do przetwarzania określonych danych, należy dokonać ich anonimizacji lub trwałego usunięcia, co niejednokrotnie wymaga dedykowanych narzędzi (oprogramowania). Podobnie jak ze stosowaniem kamer nasobnych ma się rzecz z kamerami w pojazdach lub dronach, kiedy osoby lub służby nie posiadają uprawnień do nagrywania w obszarach i obiektach objętych zakazem fotografowania.

> *» Należy zadbać o to kto, kiedy i którą kamerę może pobrać. Ważne, aby było wiadomo, gdzie znajduje się zapis z konkretnego zdarzenia, kto był jego uczestnikiem, kiedy zdarzenie miało miejsce oraz czy pobrana kamera była gotowa do użycia. «*

Podsumowując, wysokie parametry techniczne kamer nasobnych nie gwarantują ich skutecznego wykorzystania. Znacznie ważniejsze są procedury i wyszkolenie użytkowników, a im więcej uwagi poświęci się na analizę możliwych zdarzeń oraz analizę ryzyka stosowania systemu, tym mniejsze będą konsekwencje ewentualnego nieudanego wdrożenia. ●

Cezary Mecwaldowski

Komendant Centralnego Ośrodka Szkolenia Służby Więziennej, wykładowca Ośrodka Szkolenia Polskiej Izby Systemów Alarmowych, ekspert think tanku ObserwatoriumBezpieczenstwa.pl

1 „Ministerstwo Zdrowia rezygnuje z dalszych prac nad stosowaniem kamer nasobnych przez ratowników medycznych", UODO, IB/Rynek Zdrowia [dostęp: https://www.rynekzdrowia.pl/Prawo/MZ-rezygnuje-z-dalszych-prac-nad-stosowaniem-kamer-nasobnych-przez-ratownikow-medycznych,192200,2.html]

PRODUCENT: AXIS COMMUNICATIONS

Kamera AXIS W110 Body Worn Camera

Stosowanie kamer nasobnych daje podgląd zdarzenia na żywo, można je też później prześledzić w zarejestrowanym materiale. Już sam widok kamery może działać prewencyjnie i powstrzymywać nieodpowiednie zachowania intruzów. AXIS W110 Body Worn Camera sprawdza się w takich sektorach, jak handel detaliczny, opieka zdrowotna, transport, ale nie tylko. Korzystanie z AXIS W110 ogranicza przemoc i fałszywe oskarżenia oraz przyczynia się do dobrostanu w miejscu pracy. Wskaźnik i komunikat głosowy po włączeniu informują, że trwa zapis. Kamera jest kompatybilna z rozwiązaniem Body Worn Live do przesyłania strumieniowego na żywo. Zapis z kamery może służyć jako materiał dowodowy podczas różnego rodzaju dochodzeń. Tym bardziej że obraz jest bardzo wyraźny, a dźwięk poddawany jest dodatkowemu wzmocnieniu. Ponadto kamery pracujące w pobliżu mogą być uruchamiane automatycznie po włączeniu jednego urządzenia. Dzięki obrazom z różnych kamer i wstępnym buforowaniu trwającym do 90 sekund można uchwycić wszystko, co naprawdę się wydarzyło, z różnych perspektyw.

Cecha	AXIS W110
Rozdzielczość i poklatkowość	1920 x1080 @ 30 fps
Kąt widzenia (szer. x wys.)	140° x 91°
Czas pracy na baterii [godz.]	–7 (@ 720p) –11,5 (tryb czuwania)
Wewnętrzna pamięć [GB]	128
Masa [g]	85
Łączność	Bluetooth, Wi-Fi
Stopień ochrony	IP54
Bufor zapisu (pre-recording) [s]	90 konfigurowalne do 120
Możliwość podłączenia zewnętrznego źródła zasilania	Nie

Więcej na www.axis.com/pl-pl

UNIFORCE TVPRZEMYSLOWA

Nowa kamera nasobna AXIS ze streamingiem na żywo 4G/LTE

Jako partner firmy Axis, Uniforce TVPrzemyslowa oferuje AXIS W120, najnowszą z linii kamer nasobnych (*body worn*) szwedzkiego producenta. W120 została zaprojektowana z myślą o służbach mundurowych i agencjach ochrony. Na tle podobnych rozwiązań konkurencji wyróżnia ją typowa dla Axis jakość i niezawodność, funkcja streamingu na żywo obrazu i dźwięku przez 4G/LTE i WiFi, skalowalność oraz możliwość integracji z dowolnym systemem VMS. Obraz z kamery jest buforowany – urządzenie przechowuje obraz ze 120 sekund poprzedzających włączenie nagrywania. Dzięki temu zarejestrowany zostanie nawet niewinny początek rozwijającej się sytuacji. Zaszyfrowany stream wideo, audio i metadanych (np. lokalizacji GPS) daje operatorowi pełną świadomość sytuacyjną i w razie konieczności możliwość wysłania wsparcia. Szerokokątna kamera rejestruje znakomitej jakości obraz Full HD przy oświetleniu nawet 0,1 lux (światło księżyca w pełni). Z kolei dzięki zaawansowanej redukcji szumów i wiatru operatorzy dysponują wyjątkowo czytelnym dźwiękiem, co zwiększa możliwości oceny sytuacji. Kamery mogą być łatwo dystrybuowane pomiędzy pracowników. Skanowanie tagu RFID automatycznie przypisuje urządzenie do danej osoby, co radykalnie ułatwia zarządzanie systemem.

Cecha	AXIS W120
Rozdzielczość i poklatkowość	1080p @30 fps
Kąt widzenia (szer. x wys.)	137° x 76°
Czas pracy na baterii [godz.]	15
Wewnętrzna pamięć [GB]	64
Masa [g]	200
Łączność	LTE, WiFi, BlueTooth, GPS, GLONASS, Galileo, BeiDou
Stopień ochrony	IP-67
Bufor zapisu (pre-recording) [s]	120
Możliwość podłączenia zewnętrznego źródła zasilania	Tak

Więcej na: www.tvprzemyslowa.pl

PRODUCENT: MOTOROLA SOLUTIONS

Kamera nasobna VB400

VB400 to następna generacja kamer noszonych na mundurze. Charakteryzuje się wytrzymałą konstrukcją, wysoką wydajnością i wieloma opcjami łączności. Zapewnia funkcje niezbędne do zachowania kontroli w każdej sytuacji.
Kamera VB400 powstała, aby chronić członków zespołu interwencyjnego i wspierać ich profesjonalizm. Pomagają w tym możliwość nagrywania na całej zmianie roboczej, nagrywanie wstępne oraz wiele opcji łączności.
Funkcja nagrywania wstępnego rejestruje dźwięk i obraz przed momentem rozpoczęcia nagrywania. Łącząc czujniki Bluetooth z technologią nagrywania uruchamianego przez współpracowników *(Peer-assisted Recording)*, kamera VB400 umożliwia uzyskanie szerszego obrazu sytuacji bez konieczności naciskania przycisku nagrywania.

Kamera VB400 nagrywa nawet przez 12 godzin po jednokrotnym ładowaniu. Nagrywanie przez całą zmianę oznacza lepszą ochronę pojedyńczych pracowników lub personelu pracującego w niebezpiecznym środowisku. Wzmocniona obudowa kamery VB400 jest odporna na deszcz, śnieg i pył. Została przetestowana zgodnie z normami wojskowymi.

Cecha	WB400
Rozdzielczość i poklatkowość	1920 × 1080p, 1280 × 720p i 640 × 360p; 25 kl./s
Kąt widzenia (szer. x wys.)	120° w poziomie, 65° w pionie, 140° po przekątnej
Czas pracy na baterii [godz.]	12
Wewnętrzna pamięć [GB]	64
Masa [g]	162
Łączność	Bluetooth® Wi-Fi®
Stopień ochrony	IP67
Bufor zapisu (pre-recording) [s]	60
Możliwość podłączenia zewnętrznego źródła zasilania	b.d.

Więcej na www.motorolasolutions.com/pl_pl/

PRODUCENT: MOTOROLA SOLUTIONS

Kamera VT100

Kamera VT100 to konfigurowalne i w pełni zintegrowane rozwiązanie przenośne do rejestrowania obrazu wideo w jakości HD 720p. Charakteryzuje się zdalną aktywacją alarmów, konstrukcją przyjazną dla użytkownika oraz bezproblemową integracją z istniejącym systemem telewizji dozorowej.
Dzięki zdalnej aktywacji alarmów kamera VT100 pozwala zespołom dyspozytorskim na szybką reakcję w przypadku incydentów.

Funkcja ostrzeżeń o transmisji strumieniowej *(Push-to-stream)* w kamerach VT100 dostarcza obraz wideo na żywo do dyspozytorni, gdy użytkownik naciśnie przycisk nagrywania.
Dzięki prostej obsłudze i długiej pracy na akumulatorze kamerę VT100 można z łatwością zintegrować z istniejącymi planami pracy zespołów interwencyjnych.
Obraz w kamerze VT100 jest zabezpieczony w celu ochrony integralności materiału filmowego i przestrzegania przepisów o ochronie danych.

Lekki model VT100 został zaprojektowany dla zespołów mających kontakt z klientami.
Na przedniej etykiecie kamery można umieścić własne logo i kolory marki, aby model VT100 stał się integralną częścią ubioru pracowników.

Cecha	WT100
Rozdzielczość i poklatkowość	1280 x 720 HD; 30 kl./s
Kąt widzenia (szer. x wys.)	130°
Czas pracy na baterii [godz.]	3 godz. nagrywania; 1,5 godz. transmisji na żywo i nagrywania
Wewnętrzna pamięć [GB]	16
Masa [g]	72
Łączność	Wi-Fi
Stopień ochrony	IP54
Bufor zapisu (pre-recording) [s]	60
Możliwość podłączenia zewnętrznego źródła zasilania	b.d.

Więcej na: www.motorolasolutions.com/pl_pl/

Kamery nasobne Axis odporne na manipulację

Kiedy w 2020 r. firma Axis wprowadziła na rynek swój pierwszy system kamer nasobnych, nie było zaskoczeniem, że sektorami, które od razu je zastosowały, były organy ścigania i prywatna ochrona.

Oparty na otwartej architekturze system kamer nasobnych Axis został zaprojektowany tak, aby być jak najbardziej elastycznym, w sposób ułatwiający dalsze udoskonalanie. Wraz z kolejnymi ulepszeniami i dodatkami, takimi jak opcja aktywacji transmisji na żywo, popularność kamer nasobnych znacznie wzrosła. Sektory, które wcześniej nie uważały kamer nasobnych za realne rozwiązanie, od handlu detalicznego po opiekę zdrowotną, teraz doświadczają wielu korzyści, jakie przynoszą one w zakresie bezpieczeństwa osobistego, wydajności operacyjnej i ochrony przed odpowiedzialnością.

Otwarta architektura i pełna elastyczność

Filozofia otwartości leży u podstaw Axis jako organizacji, a jej system kamer nasobnych jest tego kolejnym przykładem. Od AXIS W101 po bardziej dyskretne moduły optyczne nasobne – AXIS TW1201 mini cube i AXIS TW1200 mini bullet – Axis zaprojektował swoje kamery tak, aby były najbardziej elastyczną opcją na rynku. Elastyczność sprzętu to jedno, ale to otwarta architektura systemu otwiera nowe możliwości.

– *System kamer nasobnych Axis jest architekturą otwartą, by można było go bezproblemowo połączyć z już działającym w każdej firmie oprogramowaniem. Kamery nasobne Axis mogą być używane z dowolnym istniejącym systemem zarządzania wideo (VMS) lub systemem zarządzania dowodami (EMS) – lokalnie lub w chmurze – umożliwiając integrację z innymi danymi dozoru wizyjnego* – wyjaśnia Fredrik Johansson, Global Product Manager w Axis Communications. – *Widzimy, że klienci chętnie testują kamery nasobne. Na przykład supermarkety używają ich, aby upewnić się, że sprzątanie odbywa się na bieżąco, a organizacje opieki zdrowotnej wyposażyły w kamery kierowców karetek i ratowników medycznych.*

Skalowalność dostosowana do potrzeb każdej organizacji dziś i w przyszłości

Architektura rozwiązania pozwala również na niemal nieograniczoną skalowalność. Po pierwszych testach i wdrożeniach na małą skalę klienci szybko przechodzą do wprowadzenia kamer w całej organizacji.

Kamery nasobne pojawiły się w handlu detalicznym, instytucjach opieki zdrowotnej, transporcie i energetyce. W tych firmach zostali w nie wyposażeni przede wszystkim pracownicy ochrony. Widząc korzyści płynące z ich stosowania, firmy rozważają wyposażenie w kamery także pracowników hal produkcyjnych, personelu medycznego, kierowców i kontrolerów biletów lub w tych działach, które obsługują np. reklamacje, ponieważ odpowiedni materiał filmowy ułatwi obsługę skarg klientów lub roszczeń ubezpieczeniowych.

Obsługa intuicyjna

Łatwość obsługi ma kluczowe znaczenie. Korzystanie z kamery nasobnej nie może nastręczać trudności. Dlatego urządzenia Axis zostały zaprojektowane tak, aby ich obsługa była jak najprostsza.

Jak wyjaśnia Fredrik Johansson: – *Korzystanie z kamery nasobnej Axis jest bardzo proste. Wystarczy odpiąć kamerę ze stacji dokującej i kliknąć przycisk nagrywania, aby je uruchomić, a po zakończeniu pracy wyłączyć je i odłożyć kamerę do stacji. Osoby noszące kamerę nie mają dostępu do materiału ani nie mogą go udostępniać. Nie muszą też martwić się o przesyłanie nagrań – wszystko odbywa się automatycznie.*

Za pomocą jednego kliknięcia użytkownicy mogą aktywować kamerę, aby w czasie rzeczywistym rozpocząć przesyłanie obrazu do operatora. Jednocześnie użytkownik otrzymuje powiadomienie, że również operator na żywo śledzi przebieg wydarzeń.

Wbudowana integralność kamer nasobnych: procesy i nagrania odporne na manipulacje

Materiał filmowy rejestrowany przez kamery nasobne może być istotną częścią wszelkich późniejszych dochodzeń. Ze względu na to, że stanowić może on dowód w różnego rodzaju postępowaniach, musi być możliwość udowodnienia, że film nie został w żaden sposób zmanipulowany. Szczególnie, gdy nagranie ma być dowodem, np. w postępowaniu sądowym lub odszkodowawczym, bądź ma być pomocne przy realizacji reklamacji. Axis zadbał o to, by żadna klatka filmu nie mogła zostać zmanipulowana, i zminimalizował też ryzyko zakłóceń cyfrowych.

Gwarancji autentyczności nagrania służą:

Szyfrowanie. Wszystkie dane są szyfrowane za pomocą algorytmu szyfrowania symetrycznego *Advanced Encryption Standard* (AES) z kluczem 256-bitowym oraz *Transport Layer Security,* czyli kryptograficznego protokołu sieciowego zapewniającego bezpieczną komunikację przez szyfrowanie transmisji danych między klientem a serwerem. Dzięki temu tylko upoważniony operator może zobaczyć obraz z kamery transmitowany na żywo lub odtwarzany, ponieważ jest on automatycznie przechowywany przez 24 godziny.

Pełna automatyzacja. Proces przesyłania materiału wideo z kamery na serwer jest w pełni zautomatyzowany, co oznacza, że nie jest wymagana żadna ludzka interakcja i – co ważne – nie da się usunąć żadnego fragmentu wideo.

Ograniczone prawa dostępu. Aby zachować integralność wszystkich nagranych materiałów, systemy kamer nasobnych Axis są skonfigurowane tak, aby użytkownik urządzenia nie miał żadnego wpływu na pracę urządzenia (poza oczywiście jego włączeniem i wyłączeniem). Jedynym wyjątkiem jest możliwość aktywowania transmisji na żywo. Szyfrowanie zapewnia, że nikt poza operatorem nie ma dostępu do transmisji.

Bezpieczne przechowywanie i przesyłanie danych. Wszystkie kamery są zarejestrowane w jednym systemie i tylko do niego może być przesyłany materiał wideo. Każda kamera jest wpinana do stacji dokującej. Te zaś podpięte są do kontrolerów z funkcją redundancji. Awaria jednego kontrolera w żaden sposób nie wpływa na możliwość przesłania danych z kamer podłączonych do stacji dokujących korzystających z takiego kontrolera. Zadanie przesłania przejmują pozostałe urządzenia w systemie.

Wyjątkowa jakość potwierdzona testami

Kolejnym ważnym aspektem wszystkich rozwiązań Axis jest jakość, zarówno w odniesieniu do urządzeń, oprogramowania, jak i użyteczności. Dotyczy to zatem także kamer nasobnych.

Projektanci Axis wzięli pod uwagę potencjalnie trudne warunki pracy kamer: deszcz, wysoka lub niska temperatura, wstrząsy lub możliwość upadku. Podczas testów dbają o to, by wiernie oddać najtrudniejsze warunki, w jakich przyjdzie pracować urządzeniom tak, aby zapewnić ich odporność na nieprzerwane działanie. Testowane są więc odporność na warunki atmosferyczne, trwałość przycisków, odporność chemiczna i wiele innych czynników. Dzięki temu kamery nasobne Axis mogą być stosowane niemal wszędzie, od sklepów detalicznych po kopalnie jako część infrastruktury krytycznej. Testy wykraczają poza samą kamerę, a uchwyty i uprzęże są testowane pod kątem zapewnienia najlepszego połączenia wytrzymałości i komfortu.

Te dokładne testy są jednym z powodów, dla których Axis z całym przekonaniem udziela trzyletniej gwarancji na swoje kamery nasobne, co jest ponadprzeciętnym okresem w porównaniu z innymi rozwiązaniami.

Rosnąca popularność kamer nasobnych we wszystkich sektorach

Jeśli jakakolwiek firma dostrzega korzyści płynące z dozoru wizyjnego w szerszym zakresie, jest prawdopodobne, że znajdzie również przekonujące zastosowanie dla kamer nasobnych. Większość osób, która wchodzi w interakcje z ogółem społeczeństwa w ramach swojej roli zawodowej, może skorzystać z tych systemów, biorąc pod uwagę nieodłączny związek z powstrzymywaniem niepożądanych zachowań. Poza bezpieczeństwem nowe przypadki użycia, które mogą wspierać kamery nasobne – od lepszej obsługi klienta po ulepszone szkolenia i wydajność operacyjną – przynoszą wiele korzyści organizacjom w każdym sektorze.

Filozofia otwartej platformy wszystkich rozwiązań Axis sprawia, że kamery nasobne są bezproblemowym dodatkiem do każdego funkcjonującego już w danej firmie systemu dozoru, a zatem są optymalnym wyborem dla wszystkich organizacji, które chcą wykorzystać potencjał kamer nasobnych przez swoich pracowników. ●

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

Kompleksowa oferta do zabezpieczenia farm fotowoltaicznych

Elektryzującą solidność hurtowni Grodno widać w wielu obszarach działalności jej stu oddziałów zlokalizowanych w całej Polsce. Jedną z wielu dziedzin, w której ma do zaoferowania kompleksowy zestaw rozwiązań, jest zabezpieczenie farm fotowoltaicznych.

Przedsięwzięcia tak wielkie, zarówno pod względem powierzchni, jak i nakładów sprzętowych i finansowych, wymagają doboru rozwiązań o najwyższym współczynniku bezpieczeństwa. I takie można znaleźć w Grodnie, gdzie cały asortyment najlepszych dostawców, takich jak EMU, Pulsar czy ATS Forms, jest dostępny od ręki. Na każdym etapie inwestycji jest zapewnione wsparcie fachowców.

Firma tworzy naturalną platformę współpracy, porozumienia i korzyści dla inwestorów, instalatorów i dostawców. Już na etapie planowania i konsultacji specjaliści Grodna pomagają określić wymagania dotyczące zabezpieczeń farmy PV i dopasować ich jakość do konkretnych warunków i potrzeb projektu. Wybrane komponenty są szybko dostarczane na miejsce realizacji dzięki olbrzymiemu magazynowi pracującemu na trzy zmiany, który zaopatruje ponad 100 oddziałów. Specjaliści zapewniają pomoc na etapie uruchamiania i konfiguracji oraz w fazie eksploatacji i serwisowania. Wspierają klientów również na etapie pogwarancyjnym, doskonale orientują się też w kwestiach pozyskiwania dofinansowań.

Lekkie i żywotne akumulatory dostarcza Emu

Dostawcy Grodna to firmy sprawdzone w obsłudze największych instalacji PV.

Firma **ATS Forms** w ciągu ostatnich 4 lat dostarczyła systemy montażowe do kamer na farmach fotowoltaicznych o mocy ok. 2 GW nie tylko w Polsce, ale także za granicą. To godny zaufania producent gotowych rozwiązań o najwyższej jakości i w przystępnej cenie, obejmujący słupy, uchwyty, wieszaki, fundamenty, elementy skrętne i wszelkie niezbędne akcesoria.

Firma **EMU** z kolei dostarcza lekkie i żywotne akumulatory Europower, o dużej wytrzymałości prądowej i zakresie temperatury pracy, o niskim samorozładowaniu i rezystencji wewnętrznej, bezpieczne i elastyczne w użytkowaniu. Magazyny energii EMU to niezbędne narzędzie do pracy w systemach zabezpieczeń i przy współpracy z instalacjami PV.

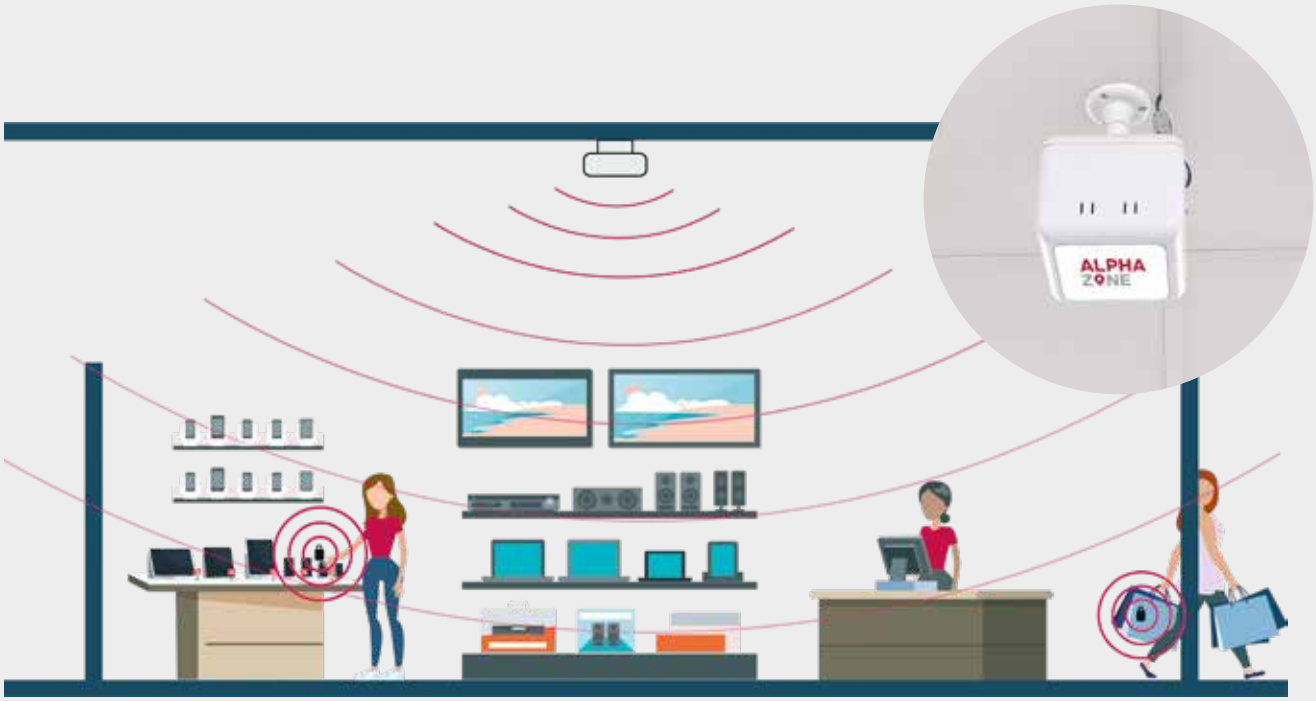
Natomiast **Pulsar** to producent doskonałych switchów przemysłowych i modułów SFP do połączeń z wykorzystaniem światłowodów. Przełączniki te mogą pracować w szerokim zakresie temperatury (od -30°C do 70°C). Oferują możliwość redundantnego zasilania, jak również porty w standardzie „BT", czyli umożliwiają zasilanie z portów PoE urządzeń, których zapotrzebowanie na moc może dochodzić nawet do 60 W. Wysoka jakość tych urządzeń jest potwierdzona 5-letnią gwarancją producenta. Pulsar dostarcza także zasilacze buforowe w obudowach hermetycznych, które mogą służyć do podtrzymania lokalnego punktu kilku kamer (SWBH-60) lub punktu dostępu, czyli mostu telekomunikacyjnego w przypadku rozległego systemu, gdzie instalacja światłowodowa z jakiegoś powodu nie została rozłożona (HPSG2H-12V5A-C).

Dzięki współpracy na linii inwestor – instalator – producent – hurtownia Grodno dostarcza kompleksowe i solidne zabezpieczenia farm PV oparte na wiedzy, doświadczeniu i nowoczesnych systemach monitoringu. Zastosowanie termowizji, inteligentnej analizy obrazu w czasie rzeczywistym i najwyższej jakości komponentów umożliwia osiągnięcie wysokiego poziomu zabezpieczenia farmy PV, minimalizując ryzyko strat, jednocześnie zwiększając efektywność energetyczną i stabilność sieci. ●

GRODNO S.A.
GRODNO S.A., ul. Kwiatowa 14
05-126 Michałów-Grabina
www.grodno.pl

Systemy montażowe do kamer dostarcza ATS Form

Switche przemysłowe i elementy światłowodowe dostarcza Pulsar



Sezonowe stoiska i wyspy handlowe? Opłacalne, jeśli dobrze chronione

Gdzie handel opłaca się najbardziej? Wszędzie, gdzie są klienci! Jednak tam, gdzie potencjalnych klientów jest najwięcej, stawki za wynajem lokalu są największe. Alternatywą jest zainwestowanie w wyspę handlową. Aby jednak ten rodzaj działalności się opłacił, musi być spełniony pewien warunek – skuteczna ochrona towaru.

Koszt wejścia w ten rodzaj biznesu jest relatywnie niski, stawki czynszu wyraźnie mniejsze, a umowę można dość łatwo rozwiązać. Nawet znane sieci spożywcze decydują się na wyspy handlowe w popularnych obiektach. Inwestycja w taki punkt sprzedaży to wydatek od 35 tys. do 80 tys. zł w zależności od branży i poziomu zatowarowania. To znacznie mniej niż w przypadku tradycyjnego sklepu.

Warto znać zagrożenia

Obok licznych zalet prowadzenia wysp handlowych, takich jak duży ruch, niższe koszty działalności, łatwość zmiany asortymentu czy możliwości działań sezonowych, nie można nie wspomnieć o zagrożeniach tego rodzaju prowadzenia sprzedaży. Jednym z największych są kradzieże i uszkodzenia towaru. Przy sporym natężeniu ruchu w galeriach handlowych czy w miejscowościach turystycznych pilnowanie towaru przez zazwyczaj jedną osobę jest praktycznie niemożliwe. To może się przyczynić do poważnych strat, a w konsekwencji sprawić, że biznes zamiast zysków odnotuje straty.

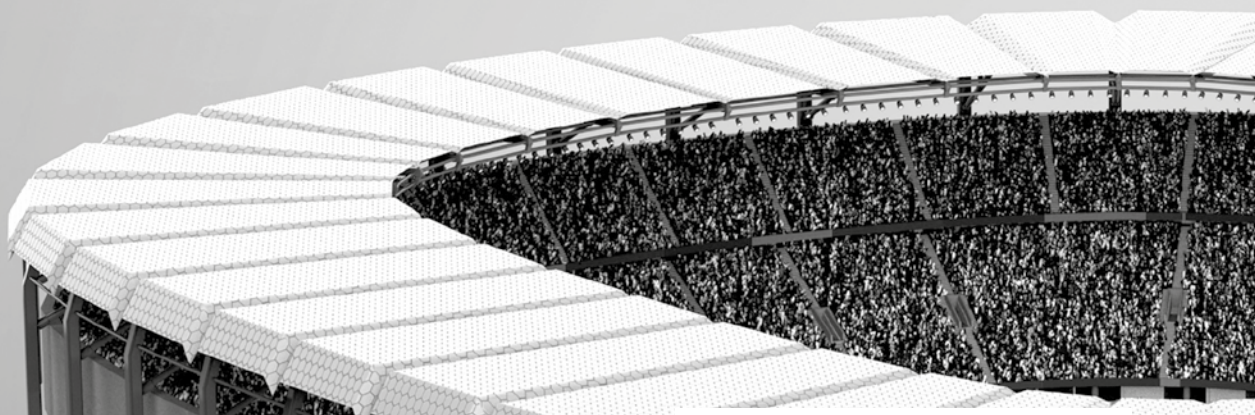
– *Zabezpieczenie towarów na wyspach handlowych i stoiskach sezonowych zawsze było problemem sprzedawców. Zamknięte pod kluczem gabloty skutecznie zniechęcają konsumentów. Nie sposób kupić okularów przeciwsłonecznych bez przymierzenia choćby kilku par. Jednocześnie otwarte stoiska to zachęta dla złodziei. Właśnie dlatego opracowaliśmy wysoce skuteczny system zabezpieczeń Alpha Zone. Pozwala on na nieskrępowany dostęp do produktów, a jednocześnie chroni je przed kradzieżą. Specjalne klipsy umieszczone na towarach – dopasowane do szerokiego asortymentu produktów, takich jak odzież, buty, okulary, butelki, alkohole czy kosmetyki – pozwalają na poruszanie się z produktem po stoisku w określonym obszarze. W chwili opuszczenia strefy wyznaczonej przez specjalne anteny uruchamiany jest alarm. To bardzo wygodne rozwiązanie, które nie wymaga wydzielania wejść lub montowania bramek ograniczających przestrzeń* – komentuje Robert Głażewski, Business Unit Director w Checkpoint Systems Polska. – *Uniwersalność tego rozwiązania powoduje, że staje się ono coraz popularniejsze. Wprowadziła je m.in. sieć sklepów Blain's Farm & Fleet, która w ten sposób zabezpieczyła stoiska z drogimi elektronarzędziami. Każdy klient może spokojnie zapoznać się z właściwościami sprzętu prezentowanego na stoisku, ale nie może go wynieść poza wyznaczoną strefę.*

Jest potencjał

O tym, że ten sposób sprzedaży może być lukratywny, świadczą dane z USA. Przychód z wysp handlowych i kiosków w 2023 r. to prawie 12 mld USD, a liczba pracowników w nich zatrudnionych wynosi 120 tys. (wg serwisu IbisWorld, *Mall Carts & Kiosks in the US industry analysis*). Dane z polskiego rynku również dowodzą, że handel ma i będzie miał się dobrze. Z raportu przygotowanego przez firmę JLL (*Rynek handlowy w Polsce* – IV kw. 2023, luty 2024) wynika, że nieruchomości przeznaczone pod działalność handlową w 2023 r. zwiększyły się o ponad 560 000 m², czyli o 14% w porównaniu z poprzednim rokiem i 8% od pięcioletniej średniej. Do tego *Retail Confidence Index* dla Polski znacznie się poprawia. Jest więc potencjał.

To świetna wiadomość dla każdego, kto chce rozpocząć swój biznes w branży, zaczynając od wyspy handlowej lub stoiska sezonowego, tym bardziej że centra handlowe są coraz bardziej elastyczne i niektóre z nich pozwalają na wynajem miejsca nawet na jeden dzień. ●

Checkpoint Systems Polska
ul. L. Idzikowskiego 16
00-710 Warszawa
biuro@checkpt.com



Mapa inwestycji

Budowa trzech zupełnie nowych obiektów sportowych oraz wykonanie robót wykończeniowych i instalacyjnych na istniejącym stadionie, modernizacja stacji elektroenergetycznej, prace budowlane na obiektach lotniskowych czy budowa hali magazynowo-produkcyjnej – między innymi te nowe inwestycje wybraliśmy dla Was w bieżącym numerze „a&s Polska". Jak zwykle, są to duże przedsięwzięcia, realizowane w całej Polsce, przez renomowane firmy. To zamierzenia budowlane, które dopiero zostały ogłoszone, a terminy ich zakończenia nie upływają przed końcem bieżącego roku.

Adela Prochyra, a&s Polska

BUDIMEX

Co: BUDOWA I PRZEBUDOWA PŁASZCZYZN LOTNISKOWYCH W PORCIE LOTNICZYM WE WROCŁAWIU (WYBÓR OFERTY)
Gdzie: Wrocław
Kiedy: 26 miesięcy od dnia podpisania umowy
1

DEKPOL

Co: ROBOTY BUDOWLANE HALI MAGAZYNOWO-PRODUKCYJNEJ W WOJEWÓDZTWIE POMORSKIM
Gdzie: Barniewice
Kiedy: III kwartał 2024 – I etap
2

ELEKTROTIM

Co: MODERNIZACJA STACJI 220/110 KV ADAMÓW
Gdzie: Adamów
Kiedy: 31.10.2024
3

Co: WYKONANIE SYSTEMU POMOCY NAWIGACYJNYCH NA LOTNISKU SZCZECIN-GOLENIÓW WRAZ Z INFRASTRUKTURĄ TOWARZYSZĄCĄ
Gdzie: Szczecin-Goleniów
Kiedy: 17 miesięcy od dnia podpisania umowy (21.02.2024)
4

MIRBUD

Co: BUDOWA SKIERNIEWICKIEGO CENTRUM SPORTU I REKREACJI
Gdzie: Skierniewice
Kiedy: 32 miesiące (umowa podpisana 07.05.2024)
5

Co: BUDOWA I UTRZYMANIE OŚRODKA SPORTOWO-REKREACYJNEGO W FORMULE PPP
Gdzie: Łódź
Kiedy: brak informacji
6

Co: PODKARPACKIE CENTRUM LEKKIEJ ATLETYKI
Gdzie: Rzeszów
Kiedy: 31.10.2026
7

MOSTOSTAL ZABRZE

Co: WYKONANIE ROBÓT WYKOŃCZENIOWYCH I INSTALACYJNYCH NA OBIEKCIE STADIONU IM. ERNESTA
Gdzie: Zabrze
Kiedy: I kwartał 2025
8

P.A. NOVA

Co: WYBUDOWANIE OBIEKTU HANDLOWO-USŁUGOWEGO
Gdzie: Opole
Kiedy: 06.01.2025
9


2
4
5
6
3
1
9
8
7

Czemu się zapaliło? Czemu się spaliło?

Ostatnio w Polsce miało miejsce wiele ogromnych pożarów. Spaliły się poddasze historycznego budynku uczelni w Gorzowie Wielkopolskim, centrum handlowe przy Marywilskiej w Warszawie, hala w Wólce Kosowskiej (to już kolejny taki incydent na przestrzeni niespełna roku w tej lokalizacji). Jak do nich doszło?

Michał Zalewski

Najczęstszą przyczyną pożaru jest ludzkie działanie albo zaniechanie. Brak ostrożności przy eksploatacji urządzeń elektrycznych lub zawierających łatwopalne środki. To pospolite przyczyny. Jednak jest jeszcze coś, na co należy zwrócić uwagę. Bardzo często powodem pożarów obiektów jest niewłaściwie wykonana lub eksploatowana instalacja elektryczna. Wadliwie wykonane połączenia instalacji, niechlujnie wykonane wpięcia przewodów do urządzeń, złącza kablowe niedostosowane do przekrojów przewodów. Na dodatek pozostawione bez należytych przeglądów technicznych.

Skutki takiego niechlujstwa albo bezmyślności są opłakane. Dochodzi do iskrzenia styków podnoszącego ich temperaturę, w konsekwencji następuje ich korozja, co pogłębia iskrzenie, aż w końcu może doprowadzić do pożaru. Nawet taki wydawałoby się drobiazg, jak wadliwie wykonana puszka umieszczona na suficie

podwieszanym, na którym przypadkiem znalazły się jakieś, nawet niewielkie elementy łatwopalne, oznacza ogromne ryzyko. Inna bardziej „wyrafinowana" przyczyna to błędy w bilansie prądowym lub oszczędności realizacyjne skutkujące zbyt małymi przekrojami przewodów, połączone dodatkowo z przeładowanymi trasami kablowymi. W efekcie dochodzi do wzrostu temperatury przewodów, co powoduje przyspieszenie degradacji izolacji, pojawienie się prądów upływnościowych, zwiększa to wielkość prądu przepływającego, dodatkowe podniesienie temperatury przewodów, w konsekwencji pożar.

Jak przeciwdziałać?

Nie zaniedbywać zasad eksploatacji urządzeń, dbać o ich należyty stan, okresowe przeglądy, to po stronie użytkownika. A na etapie budowy: dokładnie określone moce urządzeń (tzw. *Motor Lista*), odpowiedni poprawny projekt, jego weryfikacja zarówno przez wykonawcę, jak i nadzór. Podczas pierwszego uruchomienia należy dokonać pomiarów działania urządzeń i udokumentować to. Wręcz obowiązkowe wydaje się wyposażanie inspektorów oraz obsługi w coraz łatwiej dostępne kamery termowizyjne, które błyskawicznie pozwolą sprawdzić, że jakieś fragmenty instalacji są zbyt gorące. Ogromnie ważna jest rola inspektora nadzoru budowlanego. To od jego czujnego oka zależy, czy zwróci uwagę na fakt, że rozdzielnica elektryczna została wręcz „zasypana" pyłem budowlanym. Nawet po intensywnym odkurzaniu może nieprawidłowo działać i stwarzać zagrożenie pożarowe. Czujny inspektor wychwyci takie „kwiatki".

Czemu się spaliło?

Odpowiedzieć na to pytanie jest o wiele trudniejsza. Przecież nowoczesne budynki są tak projektowane i teoretycznie budowane, by ograniczać rozprzestrzenianie się ognia. Stosowane są strefy pożarowe, oddzielenia ścian i przejścia instalacyjne przez granice stref. W wielu miejscach umieszczane są odpowiednio oznakowane gaśnice i hydranty. A za wczesne wykrywanie pożaru odpowiada system detekcji, często z automatycznym powiadamianiem obsługi i automatycznie wysyłający zgłoszenie do straży pożarnej. Niektóre nowoczesne obiekty są też wyposażone w stałe urządzenia gaśnicze. Takie zabezpieczenia powodują, że pożar powinno się udać wykryć, a co za tym idzie opanować w jego wczesnej fazie i w ten sposób ograniczyć straty materiałowe. Czemu zatem się nie udaje?

Zaczynając od początku: jeżeli do pożaru dojdzie z powodu np. rozlania się i zapalenia ogromnej ilości cieczy łatwopalnej, jeżeli materiały łatwopalne są składowane niezgodnie z zasadami (częsty przypadek w centrach handlowych), to zagrożenie pożarowe wzrasta ponad przyjęte w projektach i taki pożar trudniej jest opanować. Po macoszemu traktowane są często strefy przeciwpożarowe.

> *» Szczególna jest rola doświadczonego pracownika nadzoru, którego zadaniem jest kontrolowanie, czy na każdym etapie prac wszystko prowadzone jest prawidłowo, począwszy od projektu, przez wykonawstwo, aż po testy uruchomieniowe i pomiary. «*

Co z tego, że zostały zaprojektowane prawidłowo, jeżeli ich ściany zostały podziurawione podczas innych prac lub nieodpowiednio wykonano styk ściany ze stropem, a klapy wentylacji nie zostały podłączone lub zacinają się, czego nikt nie sprawdził. W takich warunkach pożar rozprzestrzeni się inaczej i szybciej niż w założeniach projektowych.

Podobnie z systemem detekcji. Nawet najlepszy nie poradzi sobie z faktem, że są błędy w adresacji czujników i wizualizacja jest niewłaściwa, testy zostały przeprowadzone bardzo wybiórczo z uwagi na brak czasu. Czujniki zostały zablokowane lub zasłonięte na czas prac remontowych i nikt nie zadbał o ich odsłonięcie. Może się też zdarzyć, że obsługa nie potrafi obsługiwać tych urządzeń, ponieważ szkolenie było jedno, tuż po oddaniu obiektu do użytku, pracownicy się zmieniają, a nowych nikt nie przeszkolił. Każdy z tych elementów oznacza zwiększone zagrożenie pożarowe. Dlatego podobnie, jak przy zapobieganiu wybuchowi pożaru, zwracajmy uwagę na prawidłowe projektowanie i wykonanie instalacji elektrycznych zgodnie z projektem.

Szczególna jest rola doświadczonego pracownika nadzoru, którego zadaniem jest kontrolowanie, czy na każdym etapie prac wszystko prowadzone jest prawidłowo, począwszy od projektu, przez wykonawstwo, aż po testy uruchomieniowe i pomiary.

Pamiętajmy o tym, że nie każdy błąd od razu spowoduje pożar, ale suma większej liczby błędów może doprowadzić do prawdziwej tragedii. ●

Michał Zalewski

Absolwent Politechniki Gdańskiej i studiów podyplomowych Zarządzania Projektami Politechniki Warszawskiej. W branży od 25 lat, od 14 lat niezależny konsultant, inżynier uruchomieniowy.

Mazurski Security BootCamp

Piękne słońce, malownicze jeziora i wspaniała pogoda – tak przywitały nas Mazury w Rucianem-Nidzie, bo tu właśnie zorganizowaliśmy w maju kolejny Security BootCamp. Spotkaliśmy się w gronie security managerów, szefów bezpieczeństwa największych firm i instytucji z całego kraju.

Nasi goście zostali podzieleni na grupy i w tych grupach uczestniczyli w konkurencjach przygotowanych przez partnerów technologicznych: Axis Communications, Nedap Security Management, STid oraz Securitas. Na każdym stoisku czekały na nich inne zadania i różne niespodzianki.

Security BootCamp zakończyliśmy nowymi znajomościami, nowymi informacjami i wiedzą, którą wykorzystamy w pracy. Na kolejne wydarzenie zapraszamy już jesienią.

Piotr Karpiński
STid

W tym roku skupiliśmy się na rozwiązaniach NIS 2, nowej dyrektywie cyberbezpieczeństwa, która budzi większe zainteresowanie ze względu na wejście jej przepisów w życie już w październiku. I choć dotyczy głównie obszaru IT, to ważne jest, co zmienia w obszarze bezpieczeństwa fizycznego. Zwracałem uwagę na dobór właściwego czytnika i karty, co jest kluczowe, jeśli chodzi o zabezpieczenie obiektów. Często to karta jest najsłabszym ogniwem systemu, bo łatwość jej skopiowania umożliwia dostęp, np. do serwera i wykradzenia wrażliwych danych. Pokażemy również, jak łatwo jest ukraść np. samochód zabezpieczony „bezpieczną" kartą za pomocą *man in the middle attack*.
Uczestnicy zadawali wiele pytań o ustawę o KSC (NIS2) a także o to, jak rozpoznać, czy karty, czytniki są bezpieczne i jakie rozwiązania wybierać w przyszłości. Interesowali się też bezpieczeństwem kart płatniczych, które nie różnią się od kart kontroli dostępu. Tu dostawcy kart zabezpieczają je prawidłowo, czyli wymieniają je co trzy, cztery lata, by wprowadzać nowocześniejsze zabezpieczenia.
Niestety też są podatne na *man in the middle attack*, a wystarczyłoby wybrać czytnik z funkcją *proximity check*.

Konrad Badowski

Axis Communications

W tej edycji BootCampu prezentujemy nasze rozwiązania kamerowe połączone z analityką i dodatkowymi urządzeniami, takimi jak radary. Chcemy pokazać integrację kamer z techniką radarową, nakładanie informacji z radaru na obraz, w tym prędkości poruszających się obiektów. Przygotowaliśmy też pokaz wykrywania odzieży ochronnej, np. kasków, co można wykorzystać m.in. przy wejściu na plac budowy. Co roku staramy się pokazać nowości. Tym razem prezentujemy nasz nowy głośnik w obudowie wandaloodpornej, który świetnie sprawdzi się w zastosowaniach zewnętrznych w obiektach infrastruktury krytycznej. Komunikaty mogą być odtwarzane automatycznie w zależności od tego, co wykryją funkcje analityczne w kamerach. Uczestnicy sami będą mogli przetestować działanie analityki, spacerując po pomoście z kaskiem lub bez niego, i sprawdzić, czy analityka rzeczywiście zadziała.

Dla nas liczy się to, że odwiedzający nasze stoisko sami dochodzili do wniosku, że z kamer monitoringu można uzyskać znacznie więcej informacji niż tylko obrazy do celów dozorowych. Były ożywione dyskusje i ciekawe pytania, co oznacza duże zainteresowanie naszymi rozwiązaniami. Dla nas liczy się to, że odwiedzający nasze stoisko sami dochodzili do wniosku, że z kamer monitoringu można uzyskać dużo więcej informacji niż tylko obrazy do celów dozorowych. Były ożywione dyskusje i ciekawe pytania, co oznacza duże zainteresowanie naszymi rozwiązaniami.

Błażej Ożga

Nedap Security Management

Na BootCam przyjeżdżamy już kolejny raz, ponieważ to tutaj spotykamy się z security managerami z kluczowych obiektów naszego kraju. Specjalnie dla nich przygotwowaliśmy prezentację, w której pokażemy praktyczne wskazówki, w jaki sposób można sprawdzić funkcjonowanie poodbiorowe systemu kontroli dostępu. Skupiliśmy się na tym, w jaki sposób system powinien być zabezpieczony, ponieważ producent, np. Nedap, dostarcza pewnych narzędzi. To nie oznacza, że będą one odpowiednio wdrożone. Dlatego podpowiadamy security managerom, o co powinni zapytać przy odbiorze systemu, aby działał poprawnie. Przygotowaliśmy również konkursy. W tym roku jest to szafa z niespodzianką, ale żeby do niej się dostać, trzeba będzie rozwiązać zagadkę.

Marek Skowronek

Securitas

Uczestników tej edycji BootCampu zaprosiliśmy do serca naszej działalności, czyli do Securitas Operation Center. Chcieliśmy pokazać, jak naprawdę wygląda codzienna praca operatorów i jak trudno zidentyfikować zagrożenie bez wsparcia zaawansowanych technologii. Skupiliśmy się na praktycznym pokazaniu korzyści, jakie zaawansowane rozwiązania z inteligentną analizą danych przynoszą klientom. Goście mieli niepowtarzalną okazję samodzielnie użyć technologii, przejąć zadania operatorów i samemu przekonać się o zaletach wideoweryfikacji, analityki i perymetrii.

Zastanawiając się nad gotowością branży security na nowe technologie, zaprezentowaliśmy też, jako ciekawostkę, kroczącego robota-psa wyposażonego w kamerę i lidar. W przyszłości taki robot może mieć także kamerę termowizyjną, mikrofon oraz głośniki i całkowicie autonomicznie, bez ingerencji pracownika ochrony, wykonywać zautomatyzowane patrole oraz kontrolować miejsca, gdzie zdrowie i życie człowieka może być zagrożone.

Security BootCamp, rozmowy z klientami oraz wymiana doświadczeń z partnerami są dla nas zawsze inspiracją do poszukiwania nowych rozwiązań. To właśnie potrzeby rynku i naszych klientów prowadzą nas do innowacji, które zwiększają efektywność i bezpieczeństwo naszych usług.

Andrzej Pecio
Philip Morris Polska

Wysoko oceniam to, co pokazały firmy. Najbardziej podobała mi się prezentacja funkcji analitycznych w kamerach. Z różnych względów nie wszystko da się wprowadzić w firmie, a tu uświadomiłem sobie, że możemy jeszcze wykorzystać funkcje związane z BHP. Fascynuje mnie analityka, ponieważ kamery potrafią dziś robić wiele rzeczy, o których parę lat temu nam się jeszcze nie śniło.

Joanna Potrykus
CBRE

W takich szkoleniach zawsze najciekawsi są ludzie i wymiana doświadczeń. Z punktu widzenia facility managera zdecydowanie najbardziej podobała mi się prezentacja kontroli dostępu, której rozwiązania możemy u siebie wykorzystać, np. lockery. Bardzo wartościowa jest rozmowa z innymi uczestnikami i wiedza, jak to się robi w ich firmach i co moglibyśmy wykorzystać u siebie. Ciekawe jest to, że pomimo iż jesteśmy z różnych branż, różnych zakresów działalności, bo są tu przedstawiciele i zakładów produkcyjnych, i tak jak my, obiektów biurowych, to jednak te rozwiązania się przenikają. I możemy skorzystać z różnych doświadczeń.

Tomasz Grzelak
Nedap Security Management

Superprezentacje, świetni prelegenci, świetni partnerzy. Pokazano wiele nowych rzeczy z najnowszymi technologiami. Wartościowa jest możliwość testowania działania urządzeń na żywo, sprawdzenie skuteczności w realnym działaniu, nie tylko w prezentacji w PowerPoincie. Wiele rzeczy może nam się przydać. Rozmawiamy o nowościach, które pojawią w przyszłości, i już zastanawiamy się, jak i gdzie je wykorzystać. Takie BootCampy są potrzebne, każdy z uczestników wyciągnie coś dla siebie i z pewnością wykorzysta tę wiedzę w swojej pracy.

Tomasz Pawlikowski
Hydro Extrusion Poland

Najbardziej podobały mi się rozwiązania cyfrowe. Dla mnie to zupełna nowość. Możliwości, które wprowadza nowoczesna technologia, sztuczna inteligencja, analiza danych, pokazały mi, jakie korzyści możemy z tego czerpać. Spotkałem tu mnóstwo ciekawych osób, przeprowadziłem wiele interesujących dyskusji i zdobyłem wiedzę, którą na pewno wykorzystam w pracy.

Piotr Pasek
Empik

BootCamp jest dla mnie wyjątkowym eventem, bo za każdym razem odkrywamy coś nowego. Spotykamy się z różnymi osobami, z którymi możemy wymienić się doświadczeniami. W tym roku bardzo wartościowa dla mnie była prezentacja kontroli dostępu. Pokazano nam ryzyka, które przed nami stawia zastosowanie nowoczesnej technologii. I za to dziękuję.

Piotr Rusin
Autostrada Eksploatacja

Dzięki wiedzy, którą zdobyłem na BootCampach, bo jestem już kolejny raz, dzięki rozmowom z uczestnikami, podczas których wymieniamy się doświadczeniami, udało mi się przekonać nasz Zarząd do przeprowadzenia gruntownej restrukturyzacji. Przechodzimy od tradycyjnej ochrony fizycznej do zupełnie nowoczesnych technologii, którą sukcesywnie wdrażamy.

Jan T. Grusznic
a&s Polska

Tym razem na tapet wzięliśmy nowelizację *Ustawy o Krajowym Systemie Cyberbezpieczeństwa*. Mówiliśmy o tym, jaki ma wpływ na systemy bezpieczeństwa fizycznego i elektroniczne systemy zabezpieczeń. Co mamy zrobić, jak do tego podejść, no i jakie zmiany zaproponować. Było burzliwie, chwilami dramatycznie, ale udało się przejść przez 93 strony Uzasadnienia i 123 strony Nowelizacji. Dzięki temu jesteśmy gotowi do zabezpieczeń!

AXIS COMMUNICATIONS

Głośniki typu „wszystko w jednym" – eleganckie, elastyczne rozwiązanie i zadziwiający dźwięk

Axis Communications wprowadza nową serię inteligentnych głośników z przeznaczeniem do emisji komunikatów głosowych i tła muzycznego. Doskonale sprawdzą się w instalacjach wewnętrznych i zewnętrznych. Wyróżniają się eleganckim wzornictwem, są dostępne w dwóch wersjach kolorystycznych: czarnej i białej.

Nowe głośniki uzupełniają ofertę Axis i mogą być wykorzystywane w każdej instalacji. Większy model, AXIS C1110-E, zapewnia bogatszą reprodukcję niskich tonów niż mniejszy AXIS C1111-E, który znakomicie nadaje się do odtwarzania tła muzycznego. Oba głośniki zapewniają wyraźną emisję komunikatów głosowych na żywo i z nagrania, tak więc sprawdzą się w systemach zabezpieczeń, i nie tylko.

Uniwersalne systemy głośnikowe Axis są dostarczane z oprogramowaniem do zarządzania dźwiękiem umożliwiającym tworzenie harmonogramów emisji, podział na strefy i zarządzanie użytkownikami. Oprogramowanie jest oparte na otwartych standardach, co ułatwia integrację z telefonią VoIP, systemami zarządzania obrazem czy rozwiązaniami w zakresie analizy obrazu. Wbudowane obwody cyfrowego przetwarzania sygnału zapewniają znakomity dźwięk bez potrzeby dodatkowej konfiguracji fabrycznie nowego urządzenia. Połączenie ze standardową siecią IP umożliwia konstruowanie skalowalnych i ekonomicznych rozwiązań. Głośniki są wyposażone także w inteligentne funkcje. Porty we/wy umożliwiają integrację z takimi urządzeniami, jak przyciski i sygnalizatory optyczne, a wbudowany mikrofon pozwala na zdalne testowanie stanu i dwukierunkową komunikację z eliminacją echa.

Instalacja jest prosta i bezproblemowa. Po zamontowaniu znajdującego się w zestawie wspornika pozostaje jedynie zatrzasnąć mocowanie głośnika i dokręcić elementy mocujące. Można go instalować w poziomie lub w pionie na ścianach, sufitach bądź masztach – wszędzie tam, gdzie potrzebne jest wysokiej jakości nowoczesne nagłośnienie. ●

CHECKPOINT SYSTEMS

Nowy system Alpha Zone odpowiedzią na wyzwania wysp handlowych i sezonowych stoisk!

Checkpoint Systems opracował Alpha Zone, wysoko skuteczne rozwiązanie do zabezpieczeń produktów. Ten nowy system lokalizacji, należący do oferty Alpha High-Theft Solution, umożliwia sprzedawcom detalicznym ochronę produktów o wysokiej wartości w czasie rzeczywistym dzięki dokładnemu monitorowaniu ich położenia.

Alpha Zone pozwala na nieskrępowany dostęp klientom do produktów, a jednocześnie skutecznie chroni je przed kradzieżą. Specjalne znaczniki umieszczone na towarach są dopasowane do szerokiego asortymentu produktów, a w połączeniu z dedykowaną anteną pozwalają na poruszanie się z produktem po stoisku w określonym obszarze. W chwili opuszczenia „bezpiecznej strefy", czyli przy potencjalnej próbie kradzieży, uruchomiony zostaje alarm dźwiękowy. Jeśli zabezpieczony produkt zostanie przeniesiony z powrotem do „bezpiecznej strefy", alarm automatycznie się wyłączy.

Alpha Zone to wygodne rozwiązanie, nie wymaga wydzielania wejść czy montowania bramek antykradzieżowych ograniczających przestrzeń. System cechuje szybki i łatwy montaż, wdrożenie rozwiązania następuje już tego samego dnia. Co ważne, Alpha Zone jest kompatybilny z innymi rozwiązaniami Alpha High-Theft Solution, takimi jak pudełka zabezpieczające. System antykradzieżowy jest przeznaczony do stosowania m.in. na wyspach handlowych, sezonowych stoiskach, stoiskach typu *pop-up*, stoiskach targowych czy w kioskach. System Alpha Zone jest już dostępny w Polsce. ●

HANWHA VISION

Wysokowydajne kamery AI PTZ Plus od Hanwha Vision

Hanwha Vision, globalny dostawca rozwiązań wizyjnych, wprowadził na rynek dwie nowe wysokowydajne kamery AI PTZ Plus, XNP-C9310R i XNP-C7310R. Urządzenia te wykorzystują sztuczną inteligencję do szybkiego przybliżania i ustawiania ostrości, aby zapewnić większą świadomość sytuacyjną i krótszy czas reakcji.

Quick Zoom to szybki ruch przybliżania napędzany silnikiem AI, który umożliwia operatorom natychmiastowe dostrzeżenie szczegółów zachodzącego zdarzenia. Jest to szczególnie pomocne w obszarach o dużym natężeniu ruchu, np. na ulicach miast lub podczas dużych zgromadzeń publicznych. Quick Focus – szybkie ustawianie ostrości – uzupełnia tę funkcję, wykorzystując sztuczną inteligencję i wcześniej zapisane informacje w celu przyspieszenia automatycznego ustawiania ostrości klatki. Po wykryciu twarzy, osoby lub obiektu kamera automatycznie oblicza odległość między urządzeniem a obiektem, aby natychmiast dostosować ostrość i udostępnić wyraźne obrazy.

Analityka oparta na sztucznej inteligencji wykonywana w kamerze poprawia wydajność operacyjną i umożliwia szybkie wyszukiwanie pod kątem kryminalistycznym dzięki dokładnemu wykrywaniu i klasyfikacji obiektów (osób, twarzy, tablic rejestracyjnych i pojazdów).

Operatorzy mogą korzystać z kamer o wysokiej rozdzielczości do 4K, dostosowywanych oświetlaczy podczerwieni do 300 m i dużego sensora wizualnego 4K 1/1,8", który zapewnia jasny obraz nawet przy słabym oświetleniu. Operatorzy mogą z łatwością monitorować szczegóły oraz szerokie przestrzenie dzięki rozszerzonemu zakresowi pochylenia i precyzyjnemu sterowaniu PTZ.

Kamery doskonale sprawdzają się w trudnych warunkach pogodowych, w tym podczas burz i opadów śniegu, dzięki funkcjom Spin Dry i Heater, które potrafią usuwać wodę i roztapiać lód, aby zachować ostrość obrazu. Ponadto czujnik indukcyjny dokładnie wykrywa pozycję kamery bez żadnego błędu podczas długotrwałej pracy.

XNP-C9310R i XNP-C7310R mają najwyższy stopień bezpieczeństwa dzięki złotemu standardowi cyberbezpieczeństwa Hanwha Vision. Funkcje obejmują TPM 2.0 do szyfrowania i Secure Boot zapewniające użycie zaufanego oprogramowania. Hanwha Vision ma również wewnętrzny zespół ds. reakcji kryzysowej w zakresie bezpieczeństwa komputerowego (S-CERT), który koncentruje się na usuwaniu wszelkich potencjalnych luk w zabezpieczeniach swoich produktów.

Hanwha Vision od dawna angażuje się w cyberbezpieczeństwo, zachowując pełną zgodność z *Ustawą o autoryzacji obrony narodowej* (NDAA), a także dostosowując się do nadchodzących dyrektyw europejskich: *Dyrektywy w sprawie bezpieczeństwa sieci i informacji* 2. wydanie (NIS2) oraz *Ustawy o odporności cybernetycznej* (CRA), które mają na celu zwiększenie cyberbezpieczeństwa na obszarze całej Europy. ●

VCS

iTower® w rozmiarze XS Mniejszy rozmiar i duże możliwości!

iTower® Compact to najnowszy model wieży do monitoringu oferowany przez firmę VCS.

CHARAKTERYZUJĄ GO:

- atrakcyjna cena,
- kompaktowy rozmiar,
- niewielka waga,
- łatwość transportu,
- elastyczność zastosowań.

Wyposażenie wieży, tak jak we wszystkich rozwiązaniach marki VCS, jest dostosowywane do wymagań i oczekiwań klientów. Ponadto każda wieża może stanowić mobilną reklamę po oklejeniu jej stosowną grafiką. Niewątpliwymi zaletami tego rozwiązania są atrakcyjna cena i łatwość transportu.

W portfolio VCS znajduje się bogaty asortyment rozwiązań mobilnych, m.in. wieże do monitoringu, maszty oświetleniowe i wiele innych rozwiązań. Ich produkcja jest kontynuowana i ciągle rozwijana, czego przykładem jest najnowszy model iTower® w rozmiarze XS. ●

NASK

Dwa nowe certyfikaty bezpieczeństwa wydane przez NASK

Jednostka Certyfikująca NASK jest jedyną w Polsce, która ma uprawnienia do wydawania międzynarodowych certyfikatów Common Criteria (CC). Jest to międzynarodowy standard (dostępny jako norma PN-EN ISO/IEC 15408) służący ocenie właściwości bezpieczeństwa produktów i systemów IT. Także w dziedzinie urządzeń z branży security.

Standard określa wymogi bezpieczeństwa oraz metodologię dokumentowania zabezpieczeń. Dwa produkty, dla których ostatnio pozytywnie zakończył się proces certyfikacji, to: biocertiX (Asseco Data Systems, Xtension i Samsung) oraz SimplySign (Asseco Data Systems). NASK wręczył przedstawicielom ADS certyfikaty Common Criteria 21 maja w Warszawie.

BiocertiX, certyfikowany podpis biometryczny, pozwala podpisywać własnoręcznie (rysikiem, na ekranie tabletu) wszelkie dokumenty, umowy, protokoły czy oświadczenia w formacie pliku PDF. Tak podpisane e-dokumenty zachowują pełną moc prawną. BiocertiX wykorzystuje oprogramowanie Xtension i tablet Samsunga.

Z kolei SimplySign to kwalifikowany podpis elektroniczny w aplikacji mobilnej SimplySign. Narzędzie to umożliwia bezpieczne podpisywanie dokumentów elektronicznych w dowolnym miejscu i czasie, niezależnie od używanego sprzętu – telefonu, tabletu czy komputera. ●

ROGER

Integracja RACS 5 z systemem Zonifero

System kontroli dostępu RACS 5 wprowadzony do oferty w 2016 r. jest rozwiązaniem przeznaczonym do obiektów klasy biznes. Dzięki niezawodności i funkcjonalności znalazł zastosowanie w wielu biurowcach i kompleksach biurowych w największych polskich miastach.

Aplikacja mobilna Zonifero służy do zarządzania biurem, umożliwiając rezerwację sal konferencyjnych i innych przestrzeni oraz lokalizowanie pracowników i obszarów biurowych. To narzędzie, które skutecznie zwiększa efektywność zarządzania przestrzenią biurową w obiekcie.

Integracja obu systemów pomnaża korzyści płynące z ich jednoczesnego zastosowania. Daje możliwość kompleksowego gospodarowania udostępnionymi zasobami biurowymi, obejmując rezerwację spotkań w zintegrowanym kalendarzu, samochodów służbowych, miejsc parkingowych wraz z ich lokalizacją na interaktywnej mapie czy wyposażenia.

Umożliwia również organizację spotkań dla pracowników i gości zewnętrznych, a także zgłaszanie problemów i awarii. Ponadto dzięki zastosowaniu czytników QR goście odwiedzający budynek mogą w wygodny i szybki sposób przemieszczać się po nim, skanując kod otrzymany w zaproszeniu e-mail na spotkanie. Kod ten działa podobnie jak wirtualna karta i umożliwia dostęp do określonych przestrzeni bez konieczności instalowania aplikacji na telefon.

Współpraca Zonifero i firmy Roger gwarantuje wsparcie projektowe na każdym etapie: od doboru produktów, instalacji i konfiguracji aż po obsługę posprzedażową. Zintegrowane rozwiązanie wdrożono z powodzeniem w takich obiektach jak biurowiec Carbon Tower holdingu Cavatina SA czy kompleksie biurowym LAKESIDE firmy dewelopera ATENOR. ●

ALNET SYSTEMS

Polskie profesjonalne zintegrowane rozwiązania VMS
Ponad 200 000 instalacji na całym świecie
Jesteśmy z Wami od 2003 roku

www.alnetsystems.com

Nie zawsze to, co widzimy, jest tym, co nam się wydaje

Konferencyjna agenda wyglądała niezwykle kusząco. Młody historyk sztuki Tomasz Pszczółka, od niespełna trzech lat pracownik muzeum powiatowego w miasteczku, jakich tysiące we wschodniej Polsce, wiele sobie obiecywał po wyprawie do stolicy. Jeszcze tylko tydzień i wyrwie się choć na trzy dni.

Od czasu studiów miał do tego miasta sentyment, tym bardziej że nieco ostygł jego pracowniczy entuzjazm związany z niesieniem kaganka oświaty albo księgami trafiającymi pod strzechy. I nawet nie chodziło o to, czego świadkiem był właśnie w tej chwili, ale o ogólny marazm, stagnację i jakąś dziwną atmosferę, którą rozsiewał wokół dyrektor Paszczakowski, bezpośredni przełożony Pszczółki. Nigdy nic mu się nie chciało, nic się nie opłacało, wystawy czasowe były kłopotem, a przegląd magazynu, by odświeżyć wystawę stałą, nazywał „zawracaniem gitary". Nawet inwentaryzacje uważał za zbędne.

Dzień w muzeum

Niestety nie został i ma za swoje. Może teraz co najwyżej brylować przed bandą siódmoklasistów, dla których sztuka to co najwyżej „sztukamięs” albo „Oczy zielone” w wersji unplugged w wykonaniu dętej orkiestry miejskiej. Od użalania się nad własnym nędznym muzealnym losem (zjedzą mnie tu myszy) oderwała go awanturka, do jakiej doszło przed jednym z najważniejszych obrazów tutejszej kolekcji.

– Dla mnie się to nie podoba. – Rudy piegowaty nygus, na oko 13-latek, stał przed obrazem znanego malarza prymitywisty, przechylając się raz na lewą, raz na prawą stronę.

– Te, Tomasino, weź się tak nie gibaj jak gibon, bo się wywalisz. – Mały Karolek zaczął przedrzeźniać kolegę.

– Proszę pani, proszę pani, a Kajol wyzywa Tomaszka – jojczyła Zosia z krzywym zgryzem i wadą wymowy.

– Chłopacy! – Nauczycielka Rosół czuła, że jest bliska łez. Co też ją podkusiło, żeby zabrać klasę do muzeum.

Pszczółka uznał, że czas na interwencję. Odchrząknął znacząco, by wszyscy zwrócili na niego uwagę, i zaczął:

– Młodzieży – aż jęknął, kiedy usłyszał sam siebie (brzmię jak dziaders) – przed wami najważniejsze chyba dzieło w zbiorach naszego muzeum, które wróciło do nas po półrocznej przerwie konserwatorskiej. Ten krajobraz malarza prymitywisty przedstawia rynek naszego miasteczka…

Nie skończył, bo rudy nygus ryknął śmiechem:

– Sam bym lepiej namalował. Przecież tak to pięciolatek potrafi.

– Tomasz! – ryknęła nauczycielka.

Pszczółka aż się wzdrygnął, ale okazało się, że chodzi o rudego nygusa, który z kolei zupełnie się nie przejął.

– No psze pani, pani patrzy, wszystko tu krzywe i jakieś takie namazane. I te kolorki. Takie to ja mam w zestawie chińskich farbek, które dostałem na urodziny. Straszna tandeta.

Nauczycielka pomyślała, za co też od razu się skarciła, że w zasadzie ma chłopak rację. Sama miała dwie lewe ręce, ale tak to i ona by potrafiła.

Pszczółka przewrócił oczami.

– Ten obraz został wyceniony na co najmniej kilkaset tysięcy… – rzekł, a klasa jęknęła, słysząc tę kwotę.

– Fiu, fiu – rudy Tomek zagwizdał z podziwem – to może i ja zrobię karierę.

Młodzi ludzie postali jeszcze chwilę przed obrazem, a potem poszli szurać dalej muzealnymi kapciami, poganiani przez zbolałą nauczycielkę, która przysięgała sobie, że nigdy więcej.

A Pszczółka stał przy obrazie i uważnie mu się przyglądał. Coś mu w nim nie pasowało.

Tydzień później

Konferencja była świetna. Tomasz Pszczółka czuł się jak ryba w wodzie, brylując z jednej strony wśród muzealników, z drugiej – wśród speców od bezpieczeństwa. Przyjemność psuła mu tylko obecność dyrektora Paszczakowskiego, który uparł się, by również wziąć udział w wydarzeniu. Prelegent zaproszony na drugi dzień konferencji mówił ze swadą i barwnie. Pszczółka notował pilnie.

– Otóż, drodzy państwo – i tu został wyświetlony slajd – rzeczy mają się następująco. Kradzieże dzieł sztuki i zabytków przez pracowników muzeów to niestety częste zjawisko. Oto kilka przypadków. W 2000 roku w Muzeum Narodowym w Poznaniu doszło do kradzieży obrazu Moneta „Plaża w Pourville” przez pracownika obsługi. Obraz o wartości miliona dolarów został odzyskany dopiero po dziewięciu latach. W Muzeum Brytyjskim w Londynie wykryto ogromną kradzież prawie dwóch tysięcy antyków, dokonaną prawdopodobnie przez pracowników w ciągu kilkudziesięciu lat. Skradziono m.in. szkła, ceramikę i biżuterię. W Muzeum Narodowym w Warszawie w 2010 roku pracownik ochrony ukradł sześć cennych obrazów, m.in. Malczewskiego i Gierymskiego. Dzieła o wartości 16 mln zł zostały odzyskane. W Muzeum Narodowym w Krakowie w 2012 roku pracownik administracyjny ukradł 516 monet i medali z kolekcji numizmatycznej. Straty oszacowano na ponad milion złotych.

Mówca na chwilę przerwał. Poczekał, aż zgromadzeni przyswoją te informacje, i przeszedł do następnego slajdu prezentacji. A na nim, ni stąd, ni zowąd pojawiło się zdjęcie obrazu przedstawiającego wielką dłoń.

Pszczółka uniósł brew w zdumieniu. Skądś znał ten obraz. Gdzie go widział?

Już prawie sobie przypomniał, ale w tym momencie fachowiec od bezpieczeństwa wyjaśnił:

– Tak, nie mylicie się, to kadr z filmu „Poszukiwany, poszukiwana” Stanisława Barei. Kto zna? Ręka do góry?

Pszczółka rozejrzał się i ujrzał las rąk. Ktoś nawet głośno powiedział: *Ja Marysię kocham, ja się z Marysią ożenię.* W odpowiedzi rozległo się: *Sto procent cukru w cukrze!* Przez salę przeszedł głośny śmiech i nieliczne oklaski. Prelegent też się roześmiał.

– Widzę, że Bareja wiecznie żywy. Ale dlaczego o tym filmie wspominam i pokazuję ten obraz? No cóż, jak powiedziałem wcześniej, na zbiory muzealne nie zawsze czyha zamaskowany zbir. Jest jeszcze jedna kwestia i tej się pewnie już domyślacie. Nie zawsze to, co widzimy, jest tym, co nam się wydaje. I nie zawsze w muzealnych przestrzeniach podziwiamy orygina…

Pszczółka kątem oka dostrzegł, że siedzący obok dyrektor Paszczakowski zaczął się nerwowo kręcić.

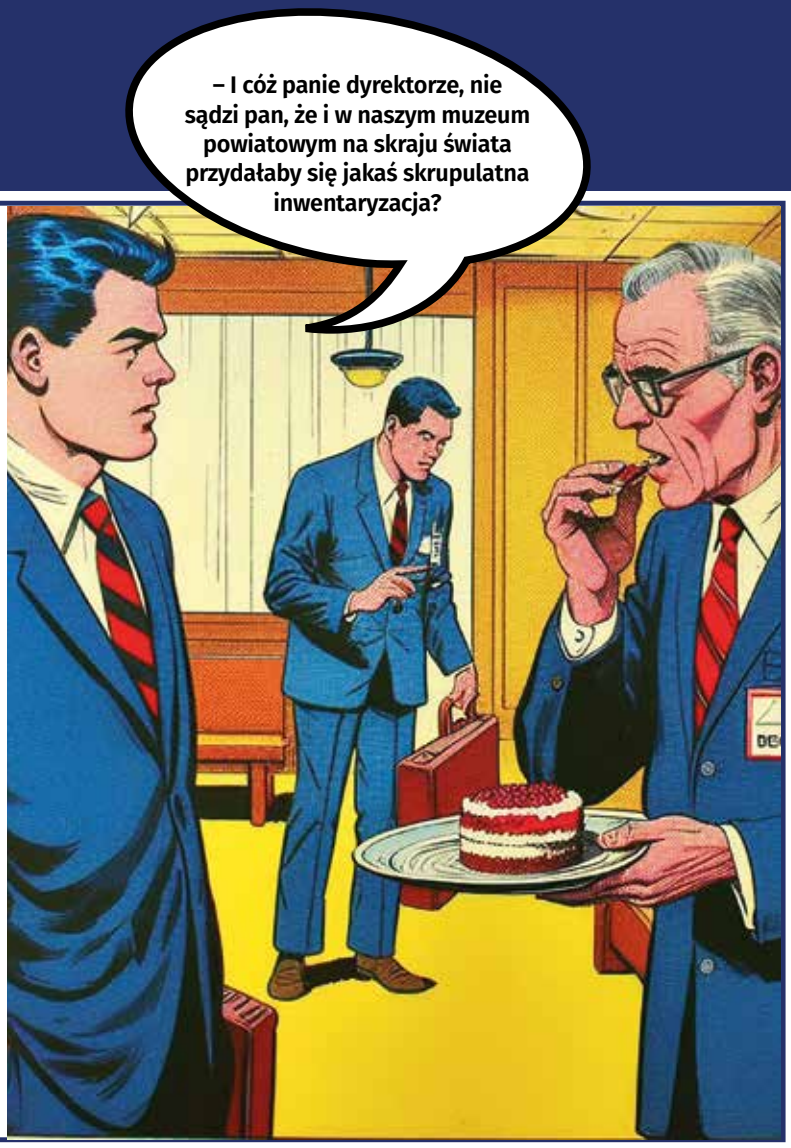
Niepokojące przeczucie

Tomasz nie należał do typów szczególnie przebiegłych, ale w głowie utkwiły mu słowa prelegenta: *Nie zawsze to, co widzimy, jest tym, co nam się wydaje.*

I tym razem coś go podkusiło. Podczas przerwy podszedł do Paszczakowskiego zajadającego tartinkę. Patrząc mu prosto w oczy, zapytał:

– I cóż panie dyrektorze, nie sądzi pan, że i w naszym muzeum powiatowym na skraju świata przydałaby się jakaś skrupulatna inwentaryzacja?

Życie dyrektora uratował chwyt Heimlicha.



- **Zapewne, jako eksperci z branży, domyślacie się, dlaczego dyrektor Paszczakowski zareagował tak nerwowo i co takiego zaczął podejrzewać Tomasz Pszczółka. Nasz ekspert Jacek Grzechowiak podpowiada, na co zwracać uwagę:**

Jacek Grzechowiak, ekspert do spraw security

Całkiem niedawno świat akademicki, ale i specjaliści od ochrony został zszokowany kradzieżą starodruków z Biblioteki Uniwersytetu Warszawskiego. Kradzież – jak wynika z doniesień medialnych – dokonana w jednej z najważniejszych bibliotek w naszym kraju została drobiazgowo przygotowana i dokładnie zrealizowana przez osoby trudniące się tym procederem można powiedzieć zawodowo. Na razie wiemy za mało, aby odpowiedzieć na kluczowe pytania, ale warto przeprowadzić burzę mózgów, bo to właśnie zapewne zrobili złodzieje, zanim przybyli na miejsce najwyraźniej bardzo dobrze przygotowani. Niekiedy jednak złodziejem jest osoba odpowiedzialna za zbiory. A i sam przedmiot kradzieży może być zupełnie inny, jak dowodzi historia złomowania fagotu, po którym pozostał tylko futerał, a sam zezłomowany instrument wkrótce odnalazł się na międzynarodowej stronie dla muzyków, gdzie można było go kupić za kilkadziesiąt tysięcy euro. W zabezpieczeniu mienia niezmiernie istotna jest „perspektywa złodzieja". Myślenie kategoriami złodzieja pomaga nie tylko lepiej wytypować mienie interesujące dla niego, ale także zrozumieć luki w naszym systemie bezpieczeństwa i co istotne, te luki nie zawsze będą w systemie ochrony.


check. create. manage.
Checly
Zakład produkcyjny
wszystkie lokalizacje
Zadania do wykonania
dla mnie
wszystkie
2 gru
Kontrola ochrony fizycznej
Krzysztof Pacel
3 gru
Inspekcja obiektu Południe
Zbigniew Kaczwara
4 gru
Kontrola bramy głównej
Łukasz Bleniek
5 gru
Sprawdzenie czujek na wejściu
Jarosław Reguła
6 gru
Kontrola pracownika w recepcji
Franciszek Gola
checly.app
Checly

BCS ULTRA

NDAA COMPLIANT
MADE IN KOREA

BCS-U-SIP6436SR40-AI2

W kamerze zastosowano wiele protokołów zwiększających jej atrakcyjność i bezpieczeństwo takich jak algorytmy inteligentnej analizy obrazu z funkcją auto trackingu, autorski bazodanowy system plików z nagraniami iBank, autorski protokół szyfrowanej komunikacji kamery z urządzeniami zdalnymi DirectIP 2.0, autorski protokół Fingerprint dla nagrań.

» Więcej przeczytasz na stronie 8

POLSKA MARKA BCS

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