CZASOPISMO RYNKU SECURITY

№ 02
2020 (20)
marzec / kwiecień

a&S POLSKA

www.aspolska.pl

infrastruktura krytyczna

15 zł
(w tym 8% VAT)

ISSN 2451-5175
05
9 772451 517703

HIKVISION

POMIAR TEMPERATURY
ROZWIĄZANIA TERMOGRAFICZNE

SAFER. FASTER. SMARTER

HIKVISION

Wysoka wydajność
Tylko 1 SEKUNDA, by dokonać pomiaru temperatury

Bezpieczeństwo
Brak kontaktu - pomiar temperatury z odległości - bez kontaktu fizycznego

Dokładność
Dokładność pomiarowa: ±0.3C z ciałem czarnym & ±0.5C bez ciała czarnego

Brak kontaktu

Pomiar wielu osób

Tylko 1 sekunda

Algorytm AI

Hikvision Poland
Hikvision Poland
ul. Żwirki i Wigury 168
02-092 Warszawa
T +48 22 4600150
info.pl@hikvision.com

REKOMENDOWANE PRODUKTY

- Zakres pomiarowy: 30-45°C
- Temperatura pracy: 10-35°C

DS-2TD2636B/P

- 384*288 rozdzielczość modułu termowizyjnego
- 15 mm ogniskowa obiektywu modułu termowizyjnego (Rekomendowana odległość pomiaru temperatury: 4.5-9 m)
- 6 mm ogniskowa modułu optycznego

DS-2TD2617B/PA

- 160*120 rozdzielczość modułu termowizyjnego
- 3/6 mm ogniskowa obiektywu modułu termowizyjnego (Rekomendowana odległość pomiaru temperatury: 0.8-1.5 m / 1.5-3.0 m)
- 4 / 6 mm ogniskowa modułu optycznego

DS-2TD1217B/PA

- 160*120 rozdzielczość modułu termowizyjnego
- 3/6 mm ogniskowa obiektywu modułu termowizyjnego (Rekomendowana odległość pomiaru temperatury: 0.8-1.5 m / 1.5-3.0 m)
- 4 / 6 mm ogniskowa modułu optycznego

DS-2TP21B-6AVF/W/P

- 160*120 rozdzielczość modułu termowizyjnego
- Max 8 MP rozdzielczość obrazu
- 6 mm ogniskowa obiektywu modułu termowizyjnego (Rekomendowana odległość pomiaru temperatury: 1.5-3.0 m)

EDYTORIAL

Drodzy Czytelnicy

Świat się zatrzymał, nasze życie sparaliżowała pandemia koronawirusa. To ogromne wyzwanie przede wszystkim dla służby zdrowia. Szczególna odpowiedzialność spoczywa także na osobach zapewniających bezpieczeństwo, prewencję i ciągłość świadczonych usług – przede wszystkim w obiektach infrastruktury krytycznej.

Zapewnienie ciągłości pracy wymaga wdrożenia planów zarządzania kryzysowego. Z pewnością przydatne będą też porady, które zminimalizują skutki COVID-19 (s. 14). Trwają gorączkowe poszukiwania technologii pomocnych w walce z epidemią. Bardzo istotne w szybkim diagnozowaniu zdrowia pracowników są na pewno specjalizowane kamery termowizyjne do mierzenia temperatury ciała – bogatą ofertę rynkową tych urządzeń przedstawiamy w produktach numeru i artykułach firmowych.
Aktywne działania w zakresie zarządzania bezpieczeństwem IK prowadzi się obecnie na całym świecie, włączając w nie specjalistów z wielu dziedzin (s. 24). W tak trudnych warunkach jeszcze bardziej istotne niż dotychczas jest profesjonalne podejście do zarządzania bezpieczeństwem (s. 32).

Zakłady zwiększonego ryzyka i zakłady dużego ryzyka (tzw. obiekty sevesowskie) często mylnie kwalifikuje się do kategorii infrastruktury krytycznej. Warto poznać różnice w podejściu do zabezpieczeń obiektów podlegających obowiązkowej ochronie (s. 28).

Dla prawidłowego funkcjonowania firm, nie tylko z sektora infrastruktury krytycznej, ważne jest dbanie o higienę bezpieczeństwa przedsiębiorstwa. O tym, jak uniknąć najczęstszych oszustw, napisał Michał Czuma. Z wielkim smutkiem przyjęliśmy wiadomość o Jego nagłej śmierci. W tym wydaniu publikujemy ostatni artykuł Michała. Będzie nam brakowało Jego cennych spostrzeżeń i wskazówek...

Trudna walka z epidemią uniemożliwiła nam organizowanie zaplanowanych dużo wcześniej spotkań i konferencji. W trosce o bezpieczeństwo uczestników postanowiliśmy zmienić termin naszego największego wydarzenia. Konferencja Warsaw Security Summit 2020, która miała się odbyć 4 czerwca, została przeniesiona na 24 września 2020 r. Mamy nadzieję, że do tego czasu sytuacja wróci do normy.

Tymczasem zwiększamy naszą aktywność w sieci. Na portalu **aspolska.pl** oraz naszych profilach na portalach Facebook i LinkedIn będziemy na bieżąco publikowali informacje dotyczące naszych nowych form aktywności i kontaktu z Czytelnikami.

Życzymy zdrowia i bezpiecznego powrotu do normalności.

Marta Dynakowska
REDAKTOR NACZELNA

Jan T. Grusznic
Z-CA REDAKTORA NACZELNEGO

Mariusz Kucharski
DYREKTOR ZARZĄDZAJĄCY

a&S POLSKA

www.aspolska.pl

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

Dyrektor zarządzający
Mariusz Kucharski

Redaktor naczelna
Marta Dynakowska

Z-ca redaktora naczelnego
Jan T. Grusznic

Stały felietonista
Andrzej Popielski

Dział marketingu i reklamy
Iwona Krawiec

Dział eventów i konferencji
Jolanta A. Kucharska
Aleksandra Czapska

Projekt graficzny i skład
Bogusław Kalwala

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

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

Korekta
Jolanta Kucharska

Prenumerata
www.aspolska.pl/prenumerata

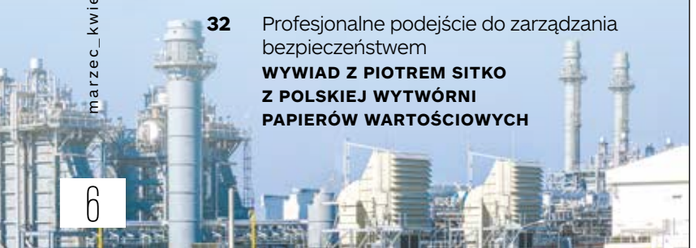
SPIS TREŚCI

№ 02

2020 (20)
marzec/kwiecień

a&S POLSKA

BEZPIECZEŃSTWO INFRASTRUKTURY KRYTYCZNEJ



RYNEK SECURITY

BEZPIECZEŃSTWO POŻAROWE

OCHRONA DANYCH

BEZPIECZNE MIASTO

SERWIS INFORMACYJNY

AXIS COMMUNICATIONS www.axis.com/pl

AXIS D2110-VE Security Radar

Axis Communications wprowadza do oferty nowy detektor radarowy AXIS D2110-VE Security Radar – inteligentne, sieciowe urządzenie wyposażone w technologię radarową do skutecznej detekcji intruza na znacznym obszarze. Radar dostarcza informacji o dokładnym położeniu i prędkości przemieszczania się obiektu. Idealnie sprawdzi się w instalacjach na zewnątrz budynków, takich jak obszary przemysłowe, parkingi czy stacje przeładunkowe.

Dzięki wbudowanej analityce wizyjnej wykorzystującej głębokie uczenie radar wykrywa (z dużym prawdopodobieństwem), klasyfikuje obiekty oraz śledzi ludzi i pojazdy, nie generując fałszywych alarmów. Wykorzystując wyjścia PoE, można łatwo podłączyć i zasilić zewnętrzne urządzenia, np. kamerę służącą do weryfikacji wizyjnej lub sieciowy megafon nadający zdalne komunikaty w celu przeciwdziałania niepożądanym zachowaniom.

Najważniejsze parametry:
→ **180-stopniowe** pole detekcji (w poziomie),
→ wbudowana analityka,
→ niezawodna **detekcja 24/7,** z niskim poziomem fałszywych alarmów,
→ inteligentna współpraca z innymi urządzeniami,
→ **wyjście PoE** do zasilania dodatkowych urządzeń.

Dzięki nowemu procesorowi firmy Axis to przystępne cenowo urządzeniet oferuje podpisany *firmware* i bezpieczny start. Inteligentna współpraca z innymi urządzeniami umożliwia instalację wielu radarów na niewielkiej przestrzeni. Przykładowo dwa współpracujące ze sobą radary zainstalowane tyłem do siebie gwarantują pole detekcji 360°.

BCS www.bcscctv.pl

BCS-BIP8201IDT

Kamera kompaktowa BIP-8201IDT to nowość w ofercie marki BCS. Funkcją, która wyróżnia ten model spośród pozostałych tego typu rozwiązań, jest rozpoznawanie i identyfikacja twarzy. Dzięki zaimplementowanemu algorytmowi sztucznej inteligencji, który oprócz standardowego wykrywania twarzy (funkcja już dość powszechna nawet w najprostszych rejestratorach) może również dostarczyć dodatkowych informacji, np. przybliżony wiek, płeć, nastrój osoby uchwyconej przez kamerę, czy ma zarost, nosi okulary bądź czapkę.
Do kamery można wgrać bazę danych twarzy, na podstawie której będzie prowadzone porównanie. Jeśli określone kryteria zostaną spełnione, wyzwalane jest zdarzenie w postaci uruchomienia wyjścia alarmowego, co w połączeniu z systemem kontroli dostępu uruchomi automatyczne otwarcie drzwi, zezwalając danej osobie na wejście.
W zarejestrowanym w rejestratorach **BCS Line** materiale, uzupełnionym o dane dotyczące wykrytej twarzy, można dużo łatwiej wyszukać nagranie, gdyż zawężamy krąg przeszukiwanych w bazie osób. Jednocześnie zmniejsza się ilość nagrań, które operator systemu musi przejrzeć, aby wychwycić interesujące go zdarzenia.
Obudowa umożliwia wyposażenie kamery w dowolny obiektyw, aby jak najlepiej uchwycić kadr detekcji. Kamera wspiera również inne funkcje zaawansowanej analizy obrazu (przekroczenie linii, wkroczenie w strefę, pojawienie się/zniknięcie obiektu) oraz standardowe funkcje, w tym obsługę **kart micro SD**, wejścia/wyjścia audio czy wspomniane wcześniej wejścia/wyjścia alarmowe.

CC PARTNERS www.ccpartners.pl

Integracja Audio-CCTV za pomocą ONVIF Profil S

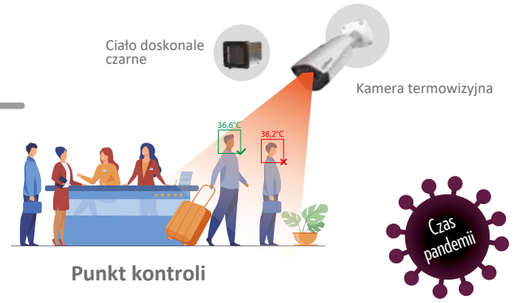
Obsługa systemów rozgłoszeniowych audio PA staje się kluczowym elementem wspierającym pracę systemów CCTV/VMS. Głośniki IP, interkomy, a nawet wzmacniacze **100 V** firmy **Commend Int.** mogą być zarządzane bezpośrednio za pomocą interfejsu **ONVIF Profile S Audio** i **protokołu SIP** w systemach **VMS/CCTV.**
Nadawanie na żywo komunikatów głosowych z poziomu stacji operatorskiej **VMS/CCTV** do urządzenia Commend czy strumieniowanie sygnału audio z mikrofonu wbudowanego do **VMS/CCTV** to funkcje obecnie dostępne za pomocą interfejsu **ONVIF**.

Głośniki tubowe wymagają do samodzielnego działania wyłącznie **switcha PoE**. Urządzenie **AFLS10HHG** ma obudowę wandaloodporną IK10 o klasie szczelności **IP66**. Zawiera wbudowany wzmacniacz o mocy **10 W**, maks. poziom ciśnienia akustycznego wynosi **SPL 118 dB**. Przez wbudowane wejścia można podłączyć np. przyciski wywołania i alarmowy czy sygnał z systemu ochrony obwodowej, za pomocą wbudowanych wyjść przekaźnikowych można wysterować np. sygnalizator optyczny, bramkę czy szlaban. Wbudowany mikrofon umożliwia prowadzenie dwukierunkowej rozmowy w trybie Open Duplex. Głośnik tubowy ma wiele funkcji programowanych: automatyczna regulacja głośności, monitoring poprawnego działania mikrofonu i głośnika, monitoring audio (wyzwolenie zdarzenia, np. komunikat audio zapisany na podstawie poziomu hałasu otoczenia).
Urządzenie jest zgodne z aktualnymi standardami bezpieczeństwa IT, może pracować w sieci TCP/IP wspierając wiele protokołów, np. **SRTP, SIPS, TLS/SSL, Certyfikat X.509.**

DAHUA TECHNOLOGY POLAND

www.dahuasecurity.com/pl

Pomiar temperatury człowieka przy użyciu termowizji



Dahua Technology zaprezentowała rozwiązanie pozwalające na bezkontaktowy pomiar temperatury ludzkiego ciała przy wykorzystaniu kamery termowizyjnej. Zapotrzebowanie na tego typu rozwiązania gwałtownie wzrosło po wybuchu światowej pandemii **koronawirusa SARS-CoV-2**. Kamera termowizyjna mierzy temperaturę każdej osoby znajdującej się w kadrze.

Do oceny stanu zdrowia człowieka poprzez zmierzenie jego temperatury wykorzystano kamerę **DH-TPC-BF3221-T.** To kamera hybrydowa, wyposażona w dwa moduły – termowizyjny bazujący na niechłodzonym przetworniku bolometrycznym (rozdzielczość 256 x 192) oraz moduł optyczny z przetwornikiem **Sony CMOS 1/2,8"** (rozdzielczość 2 Mpix). Bazowanie wyłącznie na kamerze termowizyjnej nie pozwala osiągnąć wysokiej dokładności pomiaru (błąd wynosi ±1°C), dlatego proponowane rozwiązanie, oprócz kamery, wykorzystuje istotny element, jakim jest ciało czarne. Umożliwia ono ciągłą kalibrację kamery, dzięki czemu dokładność pomiaru wynosi aż ±0,3°C.

Kolejnym istotnym elementem jest serwer **IVSS7008-1I** z funkcją detekcji twarzy. Dzięki temu mierzona jest temperatura wyłącznie osób w kadrze, z pominięciem innych elementów sceny. W przypadku wykrycia podwyższonej temperatury system automatycznie informuje obsługę o potrzebie podjęcia interwencji.

System pozwala na szybki pomiar temperatury ciała nawet kilku osób jednocześnie, nie narażając służb bezpieczeństwa na bezpośredni kontakt z osobami potencjalnie zainfekowanymi wirusem.

HIKVISION

www.hikvision.com/pl

Rozwiązania termowizyjne do mierzenia temperatury ciała

Firma Hikvision przedstawia wyróżniające się dokładnością kamery mierzące temperaturę ciała. Dostępne są modele bispektralne (przetwornik obrazu tradycyjny + termowizja) w wersji stacjonarnej, w obudowach typu bullet lub turret oraz ręczne modele przenośne. Na uwagę zasługuje bardzo wysoka dokładność pomiaru ⁺₋0,5°C (przy zastosowaniu kamer bez zewnętrznego źródła referencyjnego, tzw. *blackbody*) lub nawet ⁺₋0,3°C (we współpracy z *blackbody*).

Zastosowanie algorytmów sztucznej inteligencji w wybranych modelach pozwala na automatyczne wykrywanie twarzy i jednoczesny, błyskawiczny pomiar temperatury wielu osób (do 30) w polu widzenia kamery. Możliwe jest wyeliminowanie niechcianych pomiarów, np. temperatury kubka z gorącym napojem, który osoba trzyma. Dzięki programowalnym progom temperatury oraz alarmowaniu dźwiękowemu i optycznemu obsługa jest natychmiast powiadamiana o osobach, u których wykryto podwyższoną temperaturę ciała. Dodatkowy obiektyw dla pasma widzialnego gwarantuje identyfikację kontrolowanych osób oraz możliwość dokumentowania pomiarów w postaci nagrań, np. na rejestratorze lub bezpośrednio w kamerze na karcie Micro SD. Wyposażenie modeli przenośnych w łączność Wi-Fi pozwala na swobodne przemieszczanie się obsługi, bez konieczności instalacji stanowiska pomiarowego. Całość uzupełnia bezpłatne oprogramowanie iVMS-4200, pozwalające na zarządzanie systemem, odbiór alarmów, konfigurowanie kamer, obsługę kopii zapasowych nagrań itd.

LINC POLSKA

www.linc.pl

FLIR = sprawdzony sposób pomiaru temperatury

Szybki i bezkontaktowy pomiar temperatury jest szczególnie istotną metodą zapobiegania szerzeniu się epidemii, z jaką przyszło się nam obecnie mierzyć. To właśnie przesiewowy pomiar temperatury pozwala na szybką identyfikację osób chorych i ich wczesną izolację. Takie rozwiązania sprawdzają się nie tylko na lotniskach, ale też przy wejściach do biurowców, zakładów pracy czy hal produkcyjnych.

Kamera **FLIR A320** to sprawdzone na całym świecie rozwiązanie do bezkontaktowego pomiaru temperatury. Jej skuteczność została już potwierdzona przy wcześniejszej epidemii ebola w 2014 r. Doświadczenia z tamtego czasu pozwoliły na dalsze doskonalenie rozwiązań tego producenta.

FLIR A320 ma funkcję **ATC** *(Ambient Temperature Compensator* - kompensacja temperatury otoczenia) optymalizującą odczyty temperatury - uwzględniającą temperaturę otoczenia i minimalizującą wpływ zmiennej temperatury środowiska na dokładność odczytów. Kamera charakteryzuje się prostą konfiguracją i kalibracją przez wbudowany **WebServer.** Osoba bez specjalistycznej wiedzy technicznej może ją uruchomić i rozpocząć pracę. Obraz jest przekazywany przez wyjście analogowe lub jako strumień **RTSP,** co ułatwia integrację kamery w istniejących systemach monitoringu wizyjnego. Można zdefiniować obszary, gdzie przekroczenie temperatury będzie interpretowane jako zdarzenie alarmowe. W ten sposób operator systemu od razu zostaje poinformowany o potencjalnym zagrożeniu.

LINC POLSKA www.linc.pl

Eagle Eye – system monitoringu wizyjnego w chmurze

Eagle Eye Cloud VMS to uniwersalny system zabezpieczeń umożliwiający pełne zarządzanie w chmurze, zdalny dostęp do systemu z poziomu urządzeń mobilnych i przeglądarek internetowych, a także pełny zapis w chmurze. W dowolnym momencie można kliknięciem dodać kamerę analogową lub IP oraz zmienić czas przechowywania nagrań.
System Eagle Eye oparto na nowoczesnej redundantnej architekturze w chmurze, która zapewnia interfejs webowy i wszechstronne aplikacje na smartfony i tablety z system **Android lub iOS**. Używając **Eagle Eye Cloud VMS**, nie ma potrzeby kupowania, instalowania i konfigurowania dodatkowego oprogramowania, kluczy licencyjnych ani systemu operacyjnego.
Wielowymiarowe podejście Centrów Danych w **Chmurze Eagle Eye** do bezpieczeństwa sieciowego obejmuje zapory, systemy zapobiegania włamaniom do sieci, translację adresu sieciowego (**NAT**) i segmentację sieciową. Dzięki temu serwery i bazy danych nie są widoczne publicznie. Lokalne urządzenia Eagle Eye są zarządzane z poziomu chmury i automatycznie aktualizowane za pomocą bezpiecznej funkcji aktualizacji.

Dzięki **Eagle Eye Cloud VMS** można bezpiecznie rozbudowywać system o kolejne lokalizacje. Oprogramowanie wraz ze specjalnie zaprojektowanym sprzętem tego producenta o przeznaczeniu lokalnym jest oferowane w formie usługi. To praktyczny i ekonomiczny sposób, aby osiągnąć najwyższy poziom ochrony i elastyczności w atrakcyjnej cenie.

SCHRACK SECONET POLSKA www.schrack-seconet.pl

SIS-FIRE – system integrujący urządzenia ppoż.

System integrujący urządzenia przeciwpożarowe SIS-FIRE stosowany jest do wizualizacji, sterowania i zarządzania urządzeniami przeciwpożarowymi, a także do integracji innych systemów, mających wpływ na bezpieczeństwo pożarowe (kryzysowe) obiektu, aby zapewnić jego maksymalny poziom ochrony.
SIS-FIRE powstał na bazie wieloletnich doświadczeń firmy Schrack Seconet w zakresie produkcji systemów bezpieczeństwa pożarowego. W skład systemu wchodzą następujące elementy:

- platforma informatyczna do zarządzania bezpieczeństwem pożarowym **SIS-FIRE/SIS-FIRE Lite**,
- centrala sygnalizacji pożarowej i sterowania urządzeniami ppoż. **Integral IP MX, Integral IP CX, Integral IP BX** wraz z modułami wejścia/wyjścia techniki X-LINE,
- sterowniki urządzeń technicznych i przeciwpożarowych **SF-CONTROL** (w różnych wersjach).

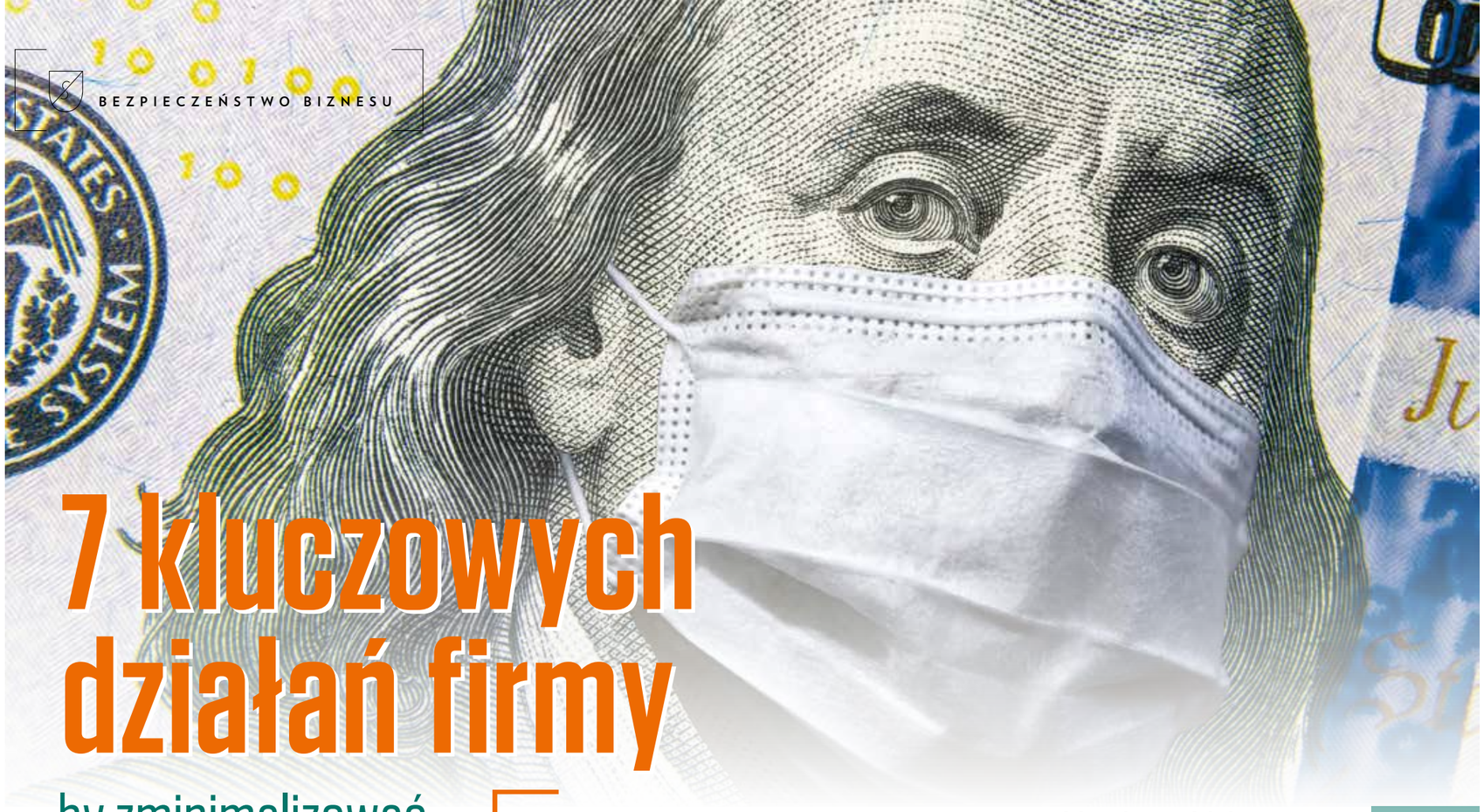
Podstawową zaletą systemu jest jego elastyczność, która umożliwia optymalny – z perspektywy konkretnego typu obiektu przemysłowego – dobór elementów oraz funkcji, z zapewnieniem ścisłej współpracy i podziału kompetencji pomiędzy komponentami systemu. Redundancja komponentów bazujących na systemie **Integral IP MX** oraz (opcjonalnie) platformy informatycznej SIS-FIRE – zapewnia ciągłość działania systemu również w przypadku wystąpienia awarii pojedynczych elementów całego układu.
Istotną cechą systemu integrującego (w przeciwieństwie do standardowego systemu sygnalizacji pożarowej) jest możliwość spełnienia nieograniczonej liczby zadań i funkcji logicznych związanych z obsługą, sterowaniem i nadzorowaniem zintegrowanych systemów w obiekcie.

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

TL-SL1226P – przełącznik PoE+ do monitoringu wizyjnego

Przełącznik został zaprojektowany specjalnie z myślą o monitoringu IP. Dzięki zgodności ze standardem 802.3af/at PoE+ instalacja systemu jest łatwa, bezpieczna i mniej kosztowna. Zastosowanie trybu Extend zwiększa zasięg transmisji **PoE** nawet do 250 m, dzięki czemu **TL-SL1226P** to doskonałe rozwiązanie w przypadku pracy kamer IP na dużym obszarze.
TL-SL1226P oferuje do 30 W mocy na każdym porcie PoE. 250 W łącznej mocy przełącznika wyposażonego w **24 porty PoE+** to rozwiązanie idealne dla systemów monitoringu wizyjnego małych i średnich firm.
Użytkownik ma też do dyspozycji **2 gigabitowe porty RJ45** oraz 2 gigabitowe sloty **Combo SFP.** Gdy całkowity pobór mocy przekracza **250 W,** funkcja inteligentnego zarządzania zużyciem energii wyłącza zasilanie portu o najniższym priorytecie, co pozwala zapewnić zasilanie portów o wyższych priorytetach i chronić urządzenie przed przeciążeniami.

Możliwość nadania wyższych priorytetów portom 1–8 za pomocą trybu Priority uruchamianego jednym kliknięciem gwarantuje wysoką jakość aplikacji wrażliwych na opóźnienia, np. nagrań wideo. Z kolei tryb Isolation rozdziela ruch na portach 1–24, aby eliminować problem podsłuchu i kopiowania danych. Przełącznik może w ten sposób odizolować od sieci burze broadcastowe, poprawiając bezpieczeństwo sieci lokalnej i transmisji danych.
Przełącznik **TL-SL1226P** nie wymaga konfiguracji i instalacji. Wystarczy wpiąć go do zasilania i podłączyć do niego urządzenia końcowe – i jest gotowy do pracy.



7 kluczowych działań firmy

by zminimalizować skutki COVID-19

W OBLICZU GLOBALNEGO ZAGROŻENIA KORONAWIRUSEM SARS-COV-2 TYLKO DOBRZE PRZYGOTOWANE FIRMY BĘDĄ W STANIE ZAPEWNIĆ ZARÓWNO OCHRONĘ SWOIM PRACOWNIKOM, JAK I CIĄGŁOŚĆ DZIAŁALNOŚCI.

Eksperci prowadzonego przez PwC Global Crisis Centre na co dzień zajmują się kryzysami różnego typu. Napięta sytuacja spowodowana przez koronawirus SARS-CoV-2, który wywołuje groźną chorobę COVID-19, wpłynęła na znaczne zwiększenie liczby pytań kierowanych do specjalistów tego Centrum. Kadra kierownicza firm jest głęboko zaniepokojona zdrowiem swoich pracowników i funkcjonowaniem organizacji.

Żadne zagrożenie nie jest odosobnionym, pojedynczym incydentem, ale koronawirus SARS-CoV-2 jest wyjątkowy pod każdym względem. Kryzys wywołany nim w krótkim czasie rozlał się na wiele regionów świata, a fakt, że nadal niewiele wiadomo o koronawirusie i jego rozprzestrzenianiu, zwiększa niepewność. Ta sytuacja wykracza poza doświadczenie większości liderów biznesu – kadencja dyrektora generalnego trwa średnio pięć lat, a ostatnią epidemią, o podobnej skali i zagrożeniu, był kryzys wywołany przez SARS w 2003 r. Na SARS zachorowało wówczas ponad 8000 osób, a epidemia trwała dziewięć miesięcy. W znacznie krótszym czasie COVID-19 dotknął ponad dziesięć razy więcej ludzi, jednocześnie błyskawicznie się rozprzestrzeniając.

Jaki wpływ na globalną gospodarkę będzie miał COVID-19?

Na tym etapie bardzo trudno precyzyjnie oszacować jego skutki. Uważa się, że epidemia SARS pochłonęła około 40 mld dolarów. Ekonomista, który dokonał tych obliczeń, twierdzi, że na walkę z koronawirusem SARS-CoV-2 i tym, co po sobie zostawi, trzeba będzie wydać trzy lub cztery razy więcej. Międzynarodowy Fundusz Walutowy obniżył swoje szacunki dotyczące globalnego wzrostu, a Organizacja Współpracy Gospodarczej i Rozwoju przewiduje, że może on zostać zmniejszony o połowę. Już obecnie występują zakłócenia w łańcuchach dostaw, zamykane są granice państw, szkoły, galerie handlowe, niektóre miejsca pracy. Liderzy biznesu postrzegają zarządzanie kryzysem jako podstawową część swoich zadań. Według najnowszego badania PwC Global Crisis Survey prawie siedmiu na 10 prezesów przedsiębiorstw (69%) doświadczyło co najmniej jednego kryzysu w ciągu ostatnich pięciu lat, a szacuje się średnio trzy kryzysy w tych firmach.

Jak zminimalizować skutki koronawirusa w firmie?

Kluczem do zarządzania każdym kryzysem jest odpowiednie przygotowanie. Oto lista siedmiu działań, które powinny zostać podjęte przez kadrę kierowniczą, aby zminimalizować negatywne skutki kryzysu wywołanego przez koronawirus SARS-CoV-2.

1. Zidentyfikuj miejsce pobytu pracowników, ustal zasady podróży

Najważniejsze jest ustalenie, gdzie dokładnie pracuje zespół i ilu pracowników przebywa na obszarach dotkniętych zagrożeniem lub potencjalnie zagrożonych. Trzeba zastanowić się, czy konieczne jest przeniesienie pracowników lub zlecenie pracy zdalnej. Zaplanowane podróże muszą zostać poddane ocenie i być przełożone bądź anulowane.

W firmie powinny istnieć jasne zasady postępowania w przypadku nieobecności z powodu choroby lub opieki nad członkami rodzin, procedury zgłaszania choroby i ograniczeń podróży. Należy także ustalić zasady na wypadek zamknięcia szkół, co jest bardzo ważne dla pracujących rodziców.

Istotną kwestią są też podatki. Jeśli pracownicy są zmuszeni przebywać za granicą dłużej, niż planowano, a ich płace podlegają opodatkowaniu, trzeba wiedzieć, jakie zasady wówczas obowiązują. Należy też przygotować się na aktualizowanie tych zasad wraz z rozwojem sytuacji.

Ustawa o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19 wprowadza konkretne uprawnienia oraz obowiązki dla pracodawcy i pracownika. Co muszą wiedzieć pracodawcy.

2. Zrewiduj plany kryzysowe i zapewnienia ciągłości działania

Każda dobrze zarządzana firma ma plan kryzysowy. Wiadomo jednak, że rzeczywistość nie zawsze odpowiada teorii. Przykładowo, w planie na wypadek wystąpienia epidemii jednej z azjatyckich organizacji wyznaczono jedno z europejskich miast jako miejsce ewakuacji pracowników i ich rodzin, ale loty z Chin do tego miasta zostały zawieszone wkrótce po wybuchu epidemii.

Plany kryzysowe muszą być dostosowane do konkretnych wyzwań związanych z epidemią. Jeśli np. duża liczba pracowników musi pracować zdalnie, trzeba sprawdzić, czy została zapewniona wystarczająca przepustowość technologii, aby sobie z tym poradzić. Ponadto trzeba wiedzieć, w jakim stopniu praca zdalna dużej liczby pracowników wpłynie na funkcjonowanie firmy. Należy też opracować procedury aktualizacji zasad podróży i spotkań oraz sposób komunikowania się z pracownikami.

Podczas każdego kryzysu największym zmartwieniem kadry zarządzającej jest szybkie gromadzenie dokładnych informacji. Jaki będzie przepływ informacji podczas obecnego kryzysu?

W takiej sytuacji kluczowe staje się zapewnienie ciągłości działania firmy. Dowiedz się, jak reagować i sprawnie zarządzać sytuacją kryzysową wywołaną przez koronawirusa.

3. Oceń łańcuch dostaw

Dokładna znajomość łańcucha dostaw pomoże ujawnić wszelkie potencjalne luki w zabezpieczeniach. Należy rozpocząć od najbardziej krytycznych produktów i wyjść daleko poza dostawców pierwszego i drugiego rzędu, aż po surowce, jeśli to możliwe. Jeśli w wytwarzaniu produktów niezbędny jest komponent z kraju, który jest odizolowany, to trzeba sprawdzić, czy w firmie są niezbędne jego zapasy. Plany kryzysowe mogą szybko napotkać trudności w sytuacji rozprzestrzeniania się pandemii.

Realizacja umów handlowych może zostać utrudniona wskutek zakłócenia łańcucha dostaw. Sprawdź, jak temu przeciwdziałać.

4. Zidentyfikuj słabe punkty

Kim są zespoły i osoby, od których zależą krytyczne procesy lub usługi? Czy wyznaczono pracowników o odpowiednich umiejętnościach, którzy w razie potrzeby mogliby zająć kluczowe stanowiska? Centra obsługi klientów i centra usług wspólnych są potencjalnie narażone, jeśli wirus będzie się rozprzestrzeniał. Należy sprawdzić, czy można podjąć działania w celu zmniejszenia liczby kontaktów międzyludzkich podczas np. pracy zmianowej.

5. Zapewnij odpowiednią komunikację

Pracodawcy zazwyczaj znają najlepsze sposoby komunikacji ze swoimi pracownikami, ale w przypadku pandemii dezinformacja i chaos informacyjny są dużym wyzwaniem. Pracownicy i pozostali interesariusze chcą wiedzieć, że została im zapewniona ochrona i firma jest przygotowana na podołanie kryzysowi. Przywództwo należy postrzegać jako źródło prawdy. Zgodnie z *Barometrem zaufania Edelman 2020* zaufanie do biznesu jest większe niż do rządów czy mediów. Kluczem jest spójność i dokładność przekazywania wiadomości, podobnie jak wiarygodność zarządzających. Pracownicy muszą być pewni tego, że ich bezpieczeństwo jest priorytetem kadry zarządzającej.

6. Przeanalizuj scenariusze

Z powodu dużej niepewności rozwoju sytuacji spowodowanej przez COVID-19, która może potrwać nawet kilka miesięcy, planowanie scenariuszy jest kluczowym narzędziem do testowania gotowości. Trzeba się przygotować na najlepsze i najgorsze scenariusze, a także ocenić, czy firma jest w stanie sobie poradzić. Jaki może być wpływ w dłuższej perspektywie, np. na kapitał obrotowy lub umowy bankowe, a nawet czynsze, gdy miejsca publiczne są zamknięte. O tego typu kwestiach należy rozmawiać z zespołem ds. finansów.

Firmy w niektórych sektorach mogą zaobserwować wzrost popytu, jeśli znaczna część populacji spędza więcej czasu w domu niż w pracy. Czy przedsiębiorstwa są na to przygotowane, wiedząc, że supermarkety ograniczają różnorodność produktów, gromadzą zapasy artykułów spożywczych i opracowują plany kryzysowe.

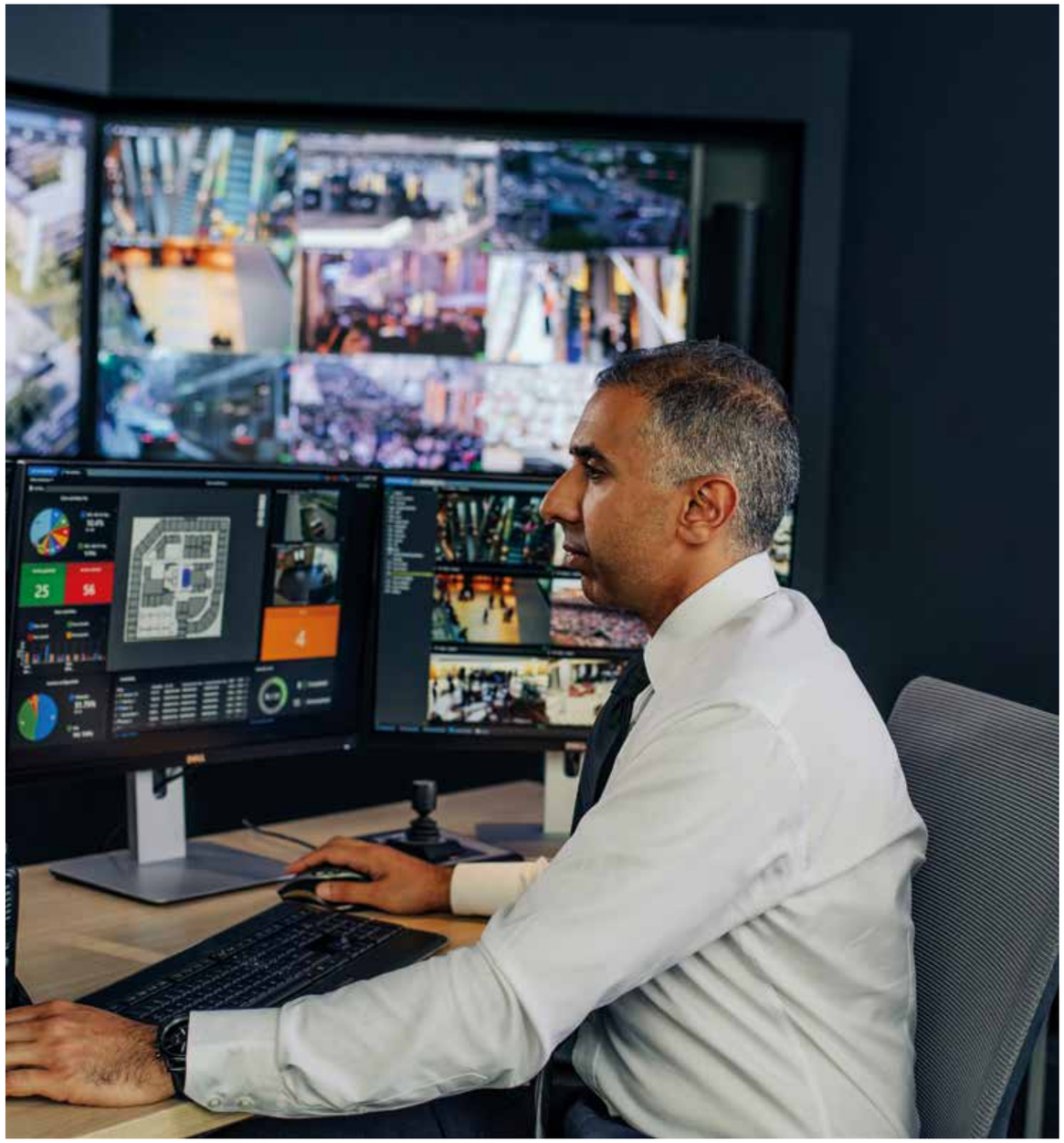
7. Pamiętaj o innych zagrożeniach

COVID-19 nie jest jedynym zagrożeniem, jakie czyha na firmy, a organizacje są najbardziej narażone na kryzys właśnie wtedy, gdy coś odwraca ich uwagę. Inne rodzaje ryzyka nadal zagrażają ich działalności. Należy dbać o cyberbezpieczeństwo – ono zawsze powinno mieć najwyższy priorytet. Nie wiemy, co mogą przynieść następne tygodnie i miesiące. Światowa Organizacja Zdrowia zmieniła status epidemii COVID-19 na pandemię, a w związku z tym należy podjąć zdecydowane kroki, by zapewnić ochronę pracownikom i firmie, aby utrzymać działalność przedsiębiorstw. □

Materiał opracowano na podstawie informacji prasowej PwC.

PwC

ul. Polna 11, 00-633 Warszawa
https://www.pwc.pl/



24 MARCA ZMARŁ NAGLE **MICHAŁ CZUMA, NASZ PRZYJACIEL, AUTOR PUBLIKACJI** W „A&S POLSKA”, PRELEGENT WARSAW SECURITY SUMMIT I AKTYWNY UCZESTNIK „ŚNIADAŃ EKSPERTÓW”.

Z WIELKIM ŻALEM PRZYJĘLIŚMY INFORMACJĘ O JEGO ŚMIERCI. RODZINIE I NAJBLIŻSZYM MICHAŁA SKŁADAMY NAJSZCZERSZE KONDOLENCJE.

Michał Czuma był niezależnym ekspertem, ostatnio prowadzącym własną działalność doradczą. Wcześniej stworzył i zarządzał pierwszymi w kraju Biurami Antyfraudowymi w spółkach grupy PKO Banku Polskiego. Przez wiele lat był z-cą dyrektora Departamentu Bezpieczeństwa PKO Banku Polskiego.

Będzie nam Go brakowało... W tym numerze publikujemy Jego ostatni artukuł.

Jak zadbać o swoją higienę bezpieczeństwa?

NIEWIELE OSÓB ZDAJE SOBIE SPRAWĘ, JAKĄ WIEDZĄ DYSPONUJĄ OSZUŚCI. DLATEGO NALEŻY ZWRACAĆ UWAGĘ NA SPRAWY NIEZBĘDNE, BY CHRONIĆ NIE TYLKO SWOJĄ FIRMĘ, ALE TAKŻE SIEBIE, SWOICH BLISKICH I ZNAJOMYCH PRZED DZIAŁANIAMI PROWADZONYMI PRZEZ WYŁUDZACZY I HAKERÓW.

TEKST
Michał Czuma

Śledczy z zespołu ds. cyberprzestępczości policji w Toronto 21 listopada 2019 r. dyskretnie dotarli do rodzinnej rezydencji podejrzanego, położonej w spokojnej dzielnicy mieszkaniowej w północno-wschodniej części Montrealu, z nakazem przeszukania i aresztowania. Nie zastano tam głównego celu operacji – 18-letniego Samy’ego Bensaciego, jednak wkrótce został on aresztowany w Victorii, w Kolumbii Brytyjskiej. Śledczy z Toronto, wspierani przez funkcjonariuszy SQ (Sûreté du Québec – policja prowincji Quebec) przejęli jednak kilka telefonów, kart SIM i sprzęt komputerowy z domu podejrzanego. I zapewne dopiero wtedy rodzice Samy’ego dowiedzieli się, że ich syn został zatrzymany jako podejrzany o przynależność do kręgu hakerów, którzy ukradli ponad 50 mln USD, wykorzystując do tego dostęp do telefonów komórkowych posiadaczy kryptowalut. Jak donosi kanadyjski dziennik „La Presse”, Samy Bensaci przebywa w areszcie domowym w oczekiwaniu na proces w Toronto. Może on opuścić rezydencję tylko w obecności jednego z trzech członków rodziny, którzy wpłacili kaucję 200 000 USD. Zabroniono mu dostępu do „każdego komputera, tabletu, telefonu komórkowego, konsoli do gier, w tym PS3, PS4, Xbox, Nintendo Switch lub innego urządzenia zdolnego do uzyskania dostępu do Internetu”. Sąd zakazał mu również posiadania lub wymiany jakiejkolwiek formy kryptowaluty.

Podejrzany z Montrealu jest oskarżony o oszustwo, nieautoryzowane użycie komputera, oszustwo związane z danymi komputerowymi i kradzież tożsamości. Musiał oddać swój paszport, by nie móc opuścić terytorium Kanady. Bensaci został opisany przez źródła policyjne jako jeden z „głównych podejrzanych” w amerykańskim dochodzeniu w sprawie aktywnego kręgu hakerów, którzy obrabowali dziesiątki osób w Stanach Zjednoczonych i Kanadzie począwszy od wiosny 2018 r. Wiele ofiar tej fali rabunków ma cechę wspólną: większość uczestniczyła w corocznych targach kryptowalut o nazwie Consensus, które odbywały się w Nowym Jorku. – *Podejrzewa się, że hakerzy namierzali cele na takich imprezach* – mówi Rob Ross, Amerykanin, który w dwóch atakach został okradziony z kryptowalut o wartości 1 mln USD. Prowadzi teraz stronę internetową StopSIMCrime.org.

Gdy w kwietniu 2019 r. US Secret Service, odpowiedzialne za zwalczanie oszustw w Stanach Zjednoczonych, poinformowało władze kanadyjskie, że wobec obywatela Kanady jest prowadzone dochodzenie przez wyspecjalizowany oddział kalifornijski o nazwie REACT (*Regional Enforcement Allied Computer Team*), dwaj kanadyjscy operatorzy telefonii komórkowej od miesięcy męczyli się jeszcze, by złapać hakera, który opracował podstępną metodę wyłudzania kopii kart SIM, omijając czujność pracowników technicznych operatora.

SIM swap

Do kradzieży kryptowalut doszło przy wykorzystaniu oszustwa nazwanego *SIM swap*. To skuteczny atak komputerowy, który pozwala sprawcy przejąć pełną kontrolę nad usługą telefonii komórkowej ofiary, w tym linii telefonicznej i SMS-ów. Aby atak się powiódł, haker musi posiadać dane osobowe ofiary, które zazwyczaj uzyskuje poprzez infiltrację jej e-maili lub kont w serwisach społecznościowych. Następnie dzwoni do dostawcy usług telekomunikacyjnych, przedstawiając się np. jako pracownik kiosku z telefonami komórkowymi lub punktu obsługi danego telekomu, który pomaga klientowi zmienić kartę SIM (*Subscriber Identity Module*) w jego urządzeniu. W ten sposób otrzymuje duplikat karty i przejmuje kontrolę nad połączeniami telefonicznymi, dzięki czemu może skutecznie podszywać się pod swoją ofiarę, która nie ma już dostępu do usług telefonicznych. Zanim osoba zaatakowana zda sobie z tego sprawę i zaalarmuje swojego operatora telefonii komórkowej czy bank, często jest już za późno: haker zdoła zmienić wszystkie jej hasła. Osoba, która nie ma dostępu do swoich

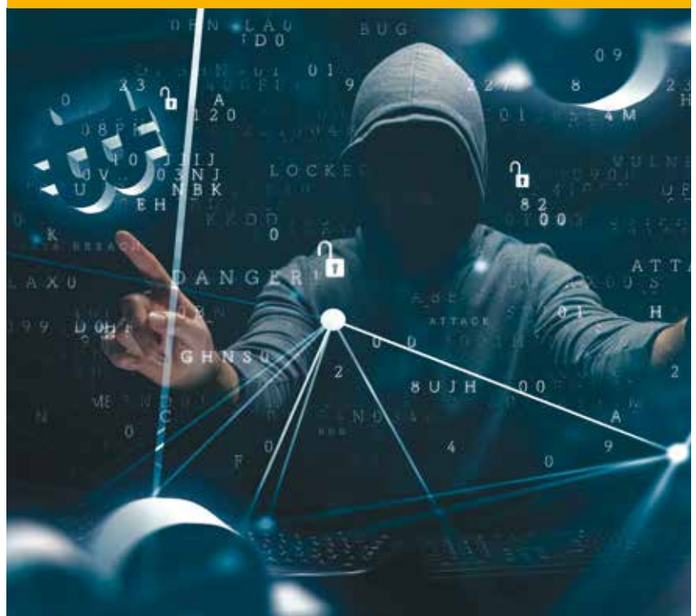
kont, zostaje chwilowo pozbawiona cyfrowej tożsamości. Im później zareaguje, tym straty są większe.

Ten złośliwy schemat ataku jest szczególnie skuteczny w zwalczaniu systemów weryfikacji dwuskładnikowej, które są wykorzystywane do sprawdzania tożsamości użytkowników poprzez wysłanie na ich telefon komórkowy wiadomości SMS zawierającej tymczasowy kod numeryczny do odblokowania konta czy dokonania transakcji. Dzięki wprowadzeniu kolejnych dyrektyw większość banków wprowadziła SMS jako potwierdzenie dyspozycji w bankowości internetowej i mobilnej. Dlatego zdolny haker po zdobyciu niezbędnych danych będzie mógł uzyskać dostęp do konta i wykorzystując chociażby znane ze stron bankowych procedury reklamacyjne, zdobyć dane do logowania (zmienić dotychczasowe) do konta i tym sposobem bez trudu wypłacić wszystkie pieniądze, założyć na te dane konta w innych bankach, wyłudzić pożyczki w firmach pożyczkowych, które kierując się chęcią przyciągnięcia klientów, przyśpieszają procedury weryfikacji.
I tak w ciągu kilku minut oszust będzie mógł wykonać każdą operację na koncie swojej ofiary. A wszystko dlatego, że SMS-y generowane przez system, a mające na celu weryfikację klienta, trafiają na zdublowany przez wyłudzoną kartę SIM na telefon oszusta. Takie historie są impulsem do tego, by zadbać o bezpieczeństwo swoich finansów.

Jak dbać o bezpieczeństwo naszych systemów informatycznych?

Trudno ustrzec się przed tym, by numer telefonu nie dotarł do oszustów. Niewiele osób ma wpływ na to, gdzie trafia ich numer telefonu. Metodą prób i błędów lub posługując się socjotechniką, nadal łatwo wyłudzać za pomocą SIM Swap numery telefonów w większości telekomów. Kiedy jednak otrzymujesz dziwnie brzmiące SMS-y albo telefon staje się głuchy, trzeba działać błyskawicznie. Nie tylko poinformować swojego operatora, ale przede wszystkim od razu zadzwonić do banku i zablokować swoje konto.

Najpierw głuchnie twój telefon, a potem dowiadujesz się, że na twoim koncie w banku nie ma ani grosza



Jakiś czas temu dowiedziałem się przypadkiem, że w jednej z firm finansowych doszło do kradzieży książki adresowej pracowników. Później odwiedzając koleżankę, która jest szefem jednostki antyfraudowej tej firmy, zapytałem ją, czy nie mają z tego tytułu kłopotów. Koleżanka zaskoczona nie zapytała mnie, skąd o tym wiem, ale od razu przyznała, że faktycznie ktoś wykradł książkę adresową pracowników ich firmy, ale nic złego się nie stało, bo złodziej uzyskał dane imienia i nazwiska pracowników, ich e-maile oraz numery telefonów służbowych i właściwie niewiele z tym może zrobić. Wyjaśniłem jej, że rzeczywiście pracownicy nie są zagrożeni, ale sprytny oszust, mając te dane, może się teraz pod dowolnego pracownika podszywać, a skutki tego mogą być opłakane nie tylko dla banku, ale także dla klientów. Bo jak zareaguje klient np. banku, gdy otrzyma e-mail od opiekuna klienta, który faktycznie tam pracuje? Czy jego uwaga nie zostanie uśpiona?

Pamiętaj, że twoje dane są wbrew pozorom łatwo dostępne

Często na szkoleniach i podczas dyskusji powtarzam, że dzisiaj wszyscy powinniśmy żyć ze świadomością, iż wszelkie nasze dane są znane osobom nieupoważnionym. Gdy mamy tego świadomość, chcemy się na taką okoliczność zabezpieczyć. Żyjąc ze złudnym przeświadczeniem, że nasze dane osobowe są bezpieczne, nie reagujemy na sygnały, które temu przekonaniu przeczą. Najlepsze systemy zabezpieczeń są mało skuteczne, jeśli ludzie będący elementem tych systemów nie dbają o bezpieczeństwo powierzonych im danych i o swoje bezpieczeństwo. Typowym przykładem jest telefon z banku, i to nie jest nic niestandardowego. Trzeba jednak się zastanowić, czy ktoś nie podszywa się pod pracownika banku, zakładając, że większość ludzi np. po długim weekendzie świątecznym może mieć opóźnienia w płatnością. Może zdobył bazę telefonów klientów banku i chce wyłudzić twoje dane. Jeśli już zna imię i nazwisko oraz numer telefonu, może potrzebować tylko twojej daty urodzenia i imienia ojca, by uzyskać zdalny dostęp do twojego konta. Jeśli masz wątpliwości co do wiarygodności takiego kontaktu, możesz podać błędną datę urodzin. Operator infolinii nie zniechęci się, tylko poinformuje, że dane są błędne, i zada drugie pytanie kontrolne. Na przykład zapyta, ile kart debetowych zostało wydanych do twojego konta. Podaj wówczas nieprawdziwą liczbę. Pracownik banku w tym momencie powinien przerwać rozmowę i poinformować cię, że dane są błędne, dlatego poprosi o wizytę w oddziale banku. A jeśli faktycznie jest pracownikiem banku, musi poinformować służby bezpieczeństwa banku, że coś jest nie tak, i klient nie zna daty urodzenia, imienia ojca i liczby produktów i możliwe, że doszło do duplikacji kart. W tym momencie system banku powinien natychmiast zablokować wszelkie transakcje na kontach, a infolinia zadzwonić do klienta, że istnieje podejrzenie, że został zhakowany. Sprawdź więc przy najbliższej okazji, czy tak działa bank, w którym masz konto. Jeśli tak funkcjonuje, to znaczy, że masz konto w bezpiecznym, troszczącym się o swojego klienta banku. Jeśli nie, oznacza, że twoje konto jest podatne na atak. W tej sytuacji zalecam zmianę banku.

Na szczęście, używam telefonu i rozumu zgodnie z przeznaczeniem, dlatego gdy wyświetla się nieznany numer, używam aplikacji Truecaller, która nawet w okrojonej wersji darmowej pomaga wskazać osobę dzwoniącą. Można też po prostu zapytać dzwoniącego, kim jest i skąd dzwoni, a następnie skontaktować się z infolinią banku i sprawdzić, czy rzeczywiście ktoś z banku próbował się z tobą skontaktować. Trzeba bowiem pamiętać, że podszywanie się pod infolinię banku to jedna z metod pozyskiwania danych, jeśli ktoś chce cię okraść. Oszuści wykorzystują socjotechnikę, by wyłudzać nie tylko dane, ale także instrumenty logowania.

I tu pojawia się pytanie, co z odpowiedzialnością tych, którzy dysponują tymi danymi i nie dość dokładnie ich strzegą. Okazuje się, że to także problem instytucji finansowych, gdyż oszuści dokonują i na nie ataków, by wykraść dane klientów banku. Większość, znając konsekwencje niedostatecznej ochrony i mając wdrożone wymogi RODO, pilnuje danych osobowych klientów jako oka w głowie. Dlatego oszuści próbują dotrzeć do potencjalnych ofiar bezpośrednio. W opisywanym wyżej przypadku gros okradzionych to byli uczestnicy corocznych targów poświęconych kryptowalutom o nazwie Consensus, które odbyły się w Nowym Jorku. Consensus to spotkanie świata technologii poświęcone kryptowalutom i sieci *blockchain*. Od 2015 roku impreza przyciąga każdą dużą firmę, dewelopera, założyciela i inwestora w świecie kryptowalut i łańcuchów blokowych do udziału w corocznej dyskusji na temat przyszłości branży. Niestety, przyjeżdżają też oszuści. Prawdopodobnie to tam zdobyli oni wszystkie potrzebne dane uczestników, być może uruchomili swoje stanowisko, by w trakcie imprezy dotrzeć do innych danych, w tym do ich portfeli kryptowalutowych. Mając dane ich portfeli, wykorzystując *SIM Swap*, wykradzenie zawartości tych portfeli było dziecinnie łatwe.

Co może zrobić oszust, by nas okraść?

Wszystko co teraz opiszę, celowo zostało zniekształcone, by nie było instrukcją dla oszustów, ale nadal będzie zawierać fakty. Ku przestrodze. Zdobycie numeru PESEL nie stanowi dzisiaj większego problemu. W większości są one jawne i łatwo dostępne. Dzięki uruchomionej usłudze e-recepta otrzymujemy na swój numer telefonu kod, który podaje się w aptece wraz z numerem PESEL. Wystarczy, stojąc w kolejce za potencjalną ofiarą, podsłuchać podawany PESEL.
Ponadto jest on ogólnie dostępny w Krajowym Rejestrze Sądowym, jeśli więc masz firmę lub jesteś członkiem władz firmy, każdy ma dostęp do tych danych. Jeśli jesteś właścicielem nieruchomości, wystarczy znać adres zamieszkania, by dowiedzieć się, jaki jest numer księgi wieczystej, w której widnieją dane osobowe wraz z numerem PESEL oraz imieniem rodziców. Numery PESEL łatwo też wyłudzić. Tak więc oszust, który chce ukraść pieniądze, nie musi nawet badać, kogo ma okraść. Wystarczy, że jadąc samochodem, skieruje się za kimś, kto mu wpadnie w oko. Namierzy, gdzie mieszka. Zapisze adres, pod którym mieszka. Może także pojechać za potencjalną ofiarą i sprawdzić, gdzie pracuje. Stworzenie wygodnej legendy pozwala mu telefonicznie zdobyć wszystkie dane. Jeśli jesteś w mediach społecznościowych, tam może dane zweryfi-

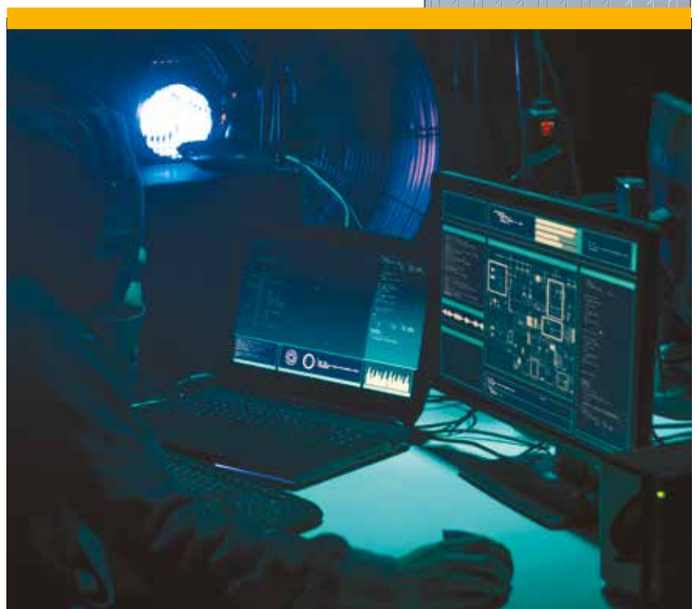
kować, a jeśli zna się na socjotechnice, to może też tam wszystko zdobyć, m.in. numer konta lub informację, w jakim banku masz konto. Brakujący numer dowodu osobistego i wszystkie dane można łatwo zdobyć, doprowadzając np. do stłuczki (spisując protokół, podaje się przecież dane dowodu osobistego). Czasami sprawca zaproponuje przelanie pieniędzy, by nie zgłaszać szkody, i poprosi o podanie numeru konta. Potem wystarczy tylko zdobyć numer telefonu i oszust, mając niezbędne dane, zgłosi się do twojego operatora telekomunikacyjnego. Najpierw ogłuchnie telefon, a potem dowiesz się, że na twoim koncie nie ma ani grosza.

Jak widać, nie potrzeba do tego hakera, który włamuje się do komputera. Dzisiaj nawet nie trzeba komputera, wystarczy kartka i telefon, do tego socjotechnika i niezadbanie o higienę swojego bezpieczeństwa.

Czy nasze firmy nas dostatecznie chronią?

Nie prowadziłem statystyk, jak są chronione firmy i jak bezpiecznie mogą się czuć właściciele, kadra zarządzająca i pracownicy. Jestem w stanie przyjąć, że większość firm dostatecznie chroni swoje zasoby informatyczne. Kupują drogie systemy zabezpieczające przed typowymi atakami. Sporo firm jednak rezygnuje z cyklicznych szkoleń, które wzmacniają najsłabsze ogniwo bezpieczeństwa w firmach – ludzi. Niektóre organizują szkolenia e-learningowe. Najczęściej są obowiązkowe, więc trzeba przerwać pracę. Zazwyczaj pracownik niechętnie loguje się do korporacyjnego modułu e-learningowego, czyta opracowanie wstępne, a następnie na gorąco odpowiada na pytania z ankiety, patrząc, czy je zaliczył. Większość osób, które kończą tego rodzaju szkolenia obowiązkowe, po kilku tygodniach zapomina o temacie. Dlatego trzeba przeprowadzać takie szkolenia nie tylko online, ale także stacjonarnie, organizować warsztaty, by wbudować do świadomości ludzi swego rodzaju firewall chroniący i firmę, i jego przed oszustami. Pamiętam szkolenie, które prowadziłem dla służb sprzedaży pewnej firmy, pokazując, ile danych ludzie sami ujawniają w sieci (zaczynając od dokładnej daty urodzin podanej na Facebooku...). Widziałem niedowierzanie w oczach moich słuchaczy, ile informacji można wyciągnąć o człowieku ze zwykłegoo czata czy podszywając się pod znajomego.

> Pośpiech, nieostrożność, działania instynktowne, nieświadomość i brak podstawowej wiedzy to nasza słabość



Niestety pośpiech, nieostrożność, działania instynktowne, nieświadomość i brak podstawowej wiedzy to nasza słabość. Aby wyłudzić pieniądze z firm, oszuści dzwonią do prezesów, księgowych, asystentek, podszywając się pod kontrahentów. Udają pracowników banków, wysyłając pisma, w których proszą o przekazanie niewinnych z pozoru informacji. Dostajesz e-maile od ludzi, którzy potrafią się podszyć pod pracowników, szefów albo osoby z help desku. Przez trzydzieści lat pracy z oszustami poznałem chyba wszystkie skuteczne metody pozwalające na to, by ukraść nie tylko pieniądze, ale także zrujnować firmy, a życie ludzi zamienić w piekło.

Jak dbać o swoje bezpieczeństwo?

Szefowie firmy i osoby zarządzające bezpieczeństwem i zasobami ludzkimi muszą cały czas szkolić pracowników z procedur obowiązujących w firmie, a także tego, jak rozpoznać symptomy i anomalie, które wskazują na potencjalne próby rozpoznawania zabezpieczeń, penetracji i planowanie ataków. Czujność ludzi wzmacnia bezpieczeństwo firmy, pracowników, ich rodzin, domów i życia.

Znalazłeś pendrive'a w łazience. Czy wiesz, co masz wtedy zrobić? Czy sprawdzasz, dlaczego śmieci koło kosza pod twoim domem są rozrzucone? Czy pisma z banku palisz w piecu lub niszczysz w zniszczarce, czy tylko rwiesz i wyrzucasz do kosza? Odbierasz dziwne telefony od kolegi z działu, który wypytywał cię o rzeczy, o jakich każdy powinien wiedzieć. Nie spowodowało to twojej właściwej reakcji? Czy wiedziałeś, co masz wtedy zrobić? Czy uważałeś, gdy ktoś podesłał ci na e-mail dziwne linki? Czy wiesz, co robić, gdy przyjedzie kurier z niezamówioną paczką? Czy podałeś swoje dane, gdy ktoś dzwonił z firmy prowadzącej badania rynkowe? Pamiętasz, kiedy to było? Czy odrzucasz w mediach społecznościowych zaproszenia od osób, których nie znasz? Ile poznałeś potem realnie? Czy jesteś pewien, że wiesz, jak rozpoznać konto fejkowe od prawdziwego? Czy wiesz, kto zna twój numer telefonu? Czy wiesz, dlaczego nie wolno kopiować dowodu osobistego? Dlaczego lepiej wezwać policję, niż podawać sprawcy zdarzenia na drodze swoje dane i dlaczego musisz wezwać policję? Czy potrafisz sprawdzić, kto do ciebie dzwoni? Na co musisz zwracać uwagę, podając komuś swoje dane? Czy potrafisz przeczytać i zapamiętać numer rejestracyjny samochodu, który cię śledzi?

Na te pytania każdy musi umieć odpowiedzieć. Musi wiedzieć, co się za nimi kryje, i potrafić na nie zareagować. Są to elementy osobistego systemu bezpieczeństwa, o którego higienę musisz dbać tak samo, jak dbasz o zdrowie, dobro bliskich i bezpieczeństwo pieniędzy. Jeśli na większość powyższych pytań potrafisz odpowiedzieć, to dobry wynik. Ale jeśli większość odpowiedzi była negatywna, jesteś zagrożony. Warto czytać w sieci ostrzeżenia o nowych formach ataków. Zaglądać na strony ekspertów od bezpieczeństwa, oglądać w telewizji programy poświęcone zagadnieniom bezpieczeństwa. Dzisiaj wszyscy pilnujemy kluczy do naszych mieszkań i domów. Większość wie, gdzie położyła kluczyki do samochodu. W pracy dbamy o wyposażenie. Ale to tylko chroni drobny promil sfery bezpieczeństwa każdej osoby. Położone na stole klucze ktoś postronny może skopiować, odciskając je w plastelinie. Samochód można ukraść w ciągu kilku sekund bez użycia kluczyków. Zawartość portfela zainteresuje kieszonkowca. Ryzyko włamania do zabezpieczonego przez firmę ochroniarską mieszkania jest niewielkie. Ale już to, co masz na koncie w banku, możesz stracić błyskawicznie, jeśli nie będziesz pamiętać, że ktoś chce stać się posiadaczem tych danych i mając je, pozbawić cię wszystkiego. W ten sposób można wykraść pieniądze firmy albo kosztowne jej tajemnice. I w tym celu czujnie obserwuje to, co piszesz w sieci, poznaje twoich przyjaciół, członków rodziny i próbuje się pod nich podszyć. Notuje skrzętnie dane, jakie pozostawiasz w sieci, by później przejąć twoją tożsamość. Wiedzieć, jak wygląda twój plan dnia, rozkład tygodnia, z kim pracujesz, kogo nie lubisz, czego ci brak i jakie masz potrzeby, a to wszystko będzie służyć oszustwu lub wyłudzeniu. **Jeśli po przeczytaniu tego artykułu będziesz teraz bacznie uważał, zaprosisz do firmy ekspertów, by przeszkolili pracowników, wezwiesz szefa bezpieczeństwa i wypytasz go, jak jesteś chroniony, a jeśli nie masz takiego, to zatrudnisz kogoś, kto tym profesjonalnie się zajmie, możesz czuć się bezpiecznie. Uważaj na siebie, przyjacielu. Uważaj...**

IK²

czyli o krytycznej infrastrukturze infrastruktury krytycznej

Infrastruktura krytyczna jest miejscem, w którym ogniskuje się wiele zagrożeń, a większość z nich ma najwyższy poziom wpływu na organizację i społeczeństwo. Stąd obiekty IK podlegają tak dużemu zainteresowaniu, są wnikliwie obserwowane przez odpowiednie instytucje oraz podlegają większym, niż inne obiekty, obostrzeniom w zakresie ochrony.

TEKST
Jacek Grzechowiak

Wiele krajów prowadzi aktywne działania w zakresie zarządzania bezpieczeństwem infrastruktury krytycznej, włączając w nie specjalistów z wielu dziedzin, reprezentujących różnych uczestników procesu zarządzania bezpieczeństwem. Ciekawym przykładem są w tym obszarze Niemcy. Zorganizowany tam system zapewnia podstawy do efektywnej współpracy między wszystkimi stronami zaangażowanymi w proces zarządzania bezpieczeństwem, postrzeganej jako część procesu zarządzania ryzykiem w dziedzinie ochrony ludności. System skupia zarówno rząd federalny, kraje związkowe, gminy, operatorów IK, jak i organizacje obywatelskie, np. straż pożarną[1]. Model ten jest swego rodzaju platformą, na której funkcjonują instytucje zarówno publiczne, jak i prywatne, dostawcy i odbiorcy usług ochrony, a także interesariusze, czyli przede wszystkim przedstawiciele społeczeństwa. Rozwiązania formalne i praktyczne tworzone w ramach prac tego gremium bazują zarówno na analizach, jak i danych scenariuszowych. Dzięki temu można głębiej analizować przyczyny i skutki incydentów w bezpieczeństwie infrastruktury krytycznej, przy większym zaangażowaniu społeczeństwa, zwłaszcza skupionego wokół struktur lokalnych. Rozwiązanie ma jeszcze jedną ważną zaletę, mianowicie tak szerokie gremium, głównie praktyków, daje dużo większą szansę na identyfikację słabych punktów systemu ochrony, zwłaszcza jeśli – przynajmniej pozornie – nie są one zlokalizowane w samym procesie bezpieczeństwa.

1) Services for modern civil protection, Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), Bonn 2017, za: https://www.bbk.bund.de/EN/Publications/publications_node.html

Jak wiadomo, łańcuch jest tak mocny, jak jego najsłabsze ogniwo. W związku z tym panuje powszechne przekonanie, że głównym celem działów, pionów bezpieczeństwa jest tworzenie jednakowo silnych ogniw tego łańcucha. Jednak dużo ważniejszym zadaniem jest zdefiniowanie wszystkich elementów systemu, także tych, a może nawet przede wszystkim tych, które są zlokalizowane poza strukturami i procesami bezpieczeństwa, a mają na nie choćby najmniejszy wpływ. To właśnie w tych miejscach z reguły łańcuch okazuje się bardzo słaby albo wręcz przerwany, dlatego szeroka reprezentacja różnych środowisk w procesach zarządzania bezpieczeństwem jest tak ważna i tak efektywna.

Model niemiecki od lat inspiruje mnie do szukania przysłowiowej dziury w całym i prowadzi wciąż do zaskakujących wniosków. Popatrzmy więc na te elementy, które mogą być krytycznymi elementami bezpieczeństwa infrastruktury krytycznej. Najpierw chciałbym poświęcić kilka słów źródłom incydentów i ich „nietypowemu" postrzeganiu. Artykuł musi być materiałem niewielkim, więc przedstawię tylko próbkę zagrożeń, jakie pojawiają się w tym obszarze, aby jedynie zainspirować innych do rozważań w tym zakresie.

Jak powszechnie wiadomo, źródła incydentów dzielimy na trzy kategorie:

- zagrożenia naturalne,
- błąd człowieka, awaria techniczna,
- zagrożenia kryminalne, terroryzm.

Bardzo często mamy jednak jeszcze czwartą przyczynę incydentów – miks, mieszankę wszystkich trzech przyczyn, w różnych proporcjach rzecz jasna. Taka mieszanka zawsze będzie groźniejsza od jej elementów składowych nie tylko dlatego, że będzie je łączyła, ale również z powodu konieczności tworzenia rozwiązań niekonwencjonalnych, zapewniających odpowiedź na kumulację jakże różnych czynników. A przy tym nawet jedno zagrożenie może mieć w praktyce różne oblicza.

Zagrożenia naturalne są najczęściej postrzeganie przez pryzmat stworzenia zagrożenia dla obiektu lub mienia przez siły natury, np. powódź i jej niszczący wymiar. To oczywisty, ale czy jedyny aspekt? Czy zagrożenia naturalne zawsze powinny być główną perspektywą? Spójrzmy szerzej – anomalie atmosferyczne zawsze powodowały problemy, jednak coraz częściej przybierają one charakter nadzwyczajny. Dokładnie tak, jak w roku 1997, kiedy na terenie południowo-zachodniej Polski odnotowano opady przekraczające w ciągu kilku dni nawet 10-krotnie miesięczną sumę, a gwałtownie wzbierająca fala opadów powodowała paraliż procesów, także proce-

Wiele krajów prowadzi aktywne działania w zakresie zarządzania bezpieczeństwem IK, włączając w nie specjalistów z wielu dziedzin. Mnie inspiruje model niemiecki

sów bezpieczeństwa. Spójrzmy zatem na tę przykładową powódź przez pryzmat trwałości systemu ochrony. Inspiracją do rozważania tej kwestii od lat są dla mnie wydarzenia, które miałem możliwość obserwować w różnych miejscach południowo-zachodniej Polski podczas powodzi tysiąclecia. W sytuacji gdy cała okolica ewakuuje się przed powodzią, trudno oczekiwać, że ochrona pozostanie na posterunkach. Faktycznie, trudno oczekiwać. Stan siły wyższej szybko przychodzi na myśl i jest komunikowany równie szybko, mimo że niekiedy jeszcze daleko do faktycznej siły wyższej. Działania zostają uruchomione, ale mienie pozostaje na terenie i niestety zaczyna być niechronione.
W takich sytuacjach powstają ponadprzeciętne zagrożenia, ponieważ w myśl maksymy „okazja czyni złodzieja" zawsze znajdą się tacy, którzy zechcą wykorzystać okazję. Powódź dla jednych jest tragedią, dla innych – jakkolwiek by to zabrzmiało – okazją. Pojawienie się złodziei, i to w dużej liczbie, ze specjalistycznym wyposażeniem nie jest niczym nadzwyczajnym. Ich kreatywność jest niesamowita. Jeśli złodziej nie ma narzędzi, znajdzie je, zrobi albo po prostu ukradnie. Jest przecież złodziejem, to dla niego norma. Musimy się z tym pogodzić. Takie są reguły tej walki, że złodzieje nie uznają żadnych reguł. Tak dzieje się u nas i w krajach sąsiednich. To samo zdarzało się i zdarza wciąż podczas huraganów w Stanach Zjednoczonych. Doświadczenia z Florydy i Kalifornii są bardzo ciekawym materiałem analitycznym. Na tyle poważnym, że przedstawiane przez rządowe agencje materiały nt. planów ewentualnościowych zawierają stosowne rekomendacje w tym zakresie[2]. Trzeba to mieć na względzie.

I tu właśnie jest ten drugi aspekt powodzi. Musi być ona rozpatrywana także w kontekście wstrzymania ochrony obiektu. A skoro tak, wstrzymanie ochrony powinno być jak najmniej dotkliwe. Przede wszystkim najkrótsze, ale także z zachowaniem możliwie największej liczby funkcji ochronnych. To właśnie tutaj pojawiają się kwestie zasilania awaryjnego, ale nie tylko sensu stricto, ale także jego odporności nawet na taki kryzys. A więc nie tylko liczba godzin podtrzymania napięcia systemów (z transmisją na zewnątrz – ta kwestia znacznie wykracza poza zakres tego artykułu), ale też lokalizacja elementów zasilania awaryjnego, odporność agregatów oraz linii napięciowych i sygnałowych na zalanie itd. Te sprawy powinny pojawić się już na etapie projektowania obiektu, wtedy będzie możliwe optymalne zbudowanie systemu. Później będzie znacznie drożej.
Kwestia zasilania systemów alarmowych jest bardzo ważna i – jak dowodzą choćby najświeższe incydenty – newralgiczna. Należy ją rozpatrywać szeroko, detalicznie, naprawdę szukając dziury w całym. Przykładem może być niedawne włamanie do Galerii „Zielone Sklepienie" w Dreźnie, gdzie sprawcy najpierw zneutralizowali zasilanie, które – jak wynika z doniesień medialnych – znajdowało się w strefie niechronionej[3]. Kwestia ta co do zasady dotyczy także innych elementów, przede wszystkim newralgicznych elementów zasilania w energię elektryczną, ale nie tylko, bo przecież głównym medium może być paliwo, gaz czy nawet woda. Urządzenie odcinające strategiczne medium bardzo często jest zlokalizowane na zewnątrz obiektu. I niestety zazwyczaj jest chronione słabiej, a nawet dużo słabiej, niż reszta obiektu. Plany ochrony bardzo często nie wspominają nic na ten temat (sic!). Nawet trwające obecnie prace nad nowelizacją ustawy o ochronie osób i mienia jakby nie dostrzegają tego problemu. A to jeden z najpoważniejszych błędów, jakie są dziś popełniane, na poziomie zarówno branży ochrony, zarządców obiektów, jak i administracji państwowej.
Najdalszy taki punkt odcięcia, jaki udało mi się znaleźć, był zlokalizowany trzy kilometry od obiektu, pod śmietnikiem na terenie obiektu zarządzanego przez zupełnie inną firmę. Dowiedziałem się o tym przypadkiem, od pewnego emeryta, który jako jedyny w okolicy pamiętał czasy budowy obiektu. Pewnie nie jestem rekordzistą w tym zakresie. Krytyczny element nie był znany. Po tej konkluzji z ust prezesa zarządu padło bardzo budujące pytanie: Czy to jedyny element, o którym nie wiemy? Dalej poszły działania. I o to chodzi w planach ewentualnościowych, w ćwiczeniach scenariuszowych, w audytach i w zarządzaniu bezpieczeństwem.

Kwestia zabezpieczenia newralgicznych dla bezpieczeństwa miejsc ma także znaczenie z punktu widzenia zagrożeń kryminalnych. Należy bowiem pamiętać, że zagrożenia kryminalne, w tym terrorystyczne, ale także zagrożenia wynikające z awarii wywołanych błędem człowieka lub awarii technicznej nie muszą mieć źródła w obiekcie, aby na niego oddziaływać. Mogą pojawić się w obiektach sąsiednich i być równie niebezpieczne, np. z powodu rozprzestrzeniającego się pożaru, spadających szczątków po eksplozji ładunku wybuchowego czy też utraty zasilania w wyniku uszkodzenia linii energetycznych poza terenem obiektu. Innym scenariuszem jest wystąpienie kilku zdarzeń w krótkim odstępie czasu, mogących powodować wykładniczy wzrost intensywności zagrożenia z powodu uniemożliwienia lub utrudnienia działań ratowniczych lub koncentracji zasobów ratowniczych w miejscu pierwszego – niekiedy pozornego – ataku[4].

2) Więcej: https://www.ready.gov/business/implementation/emergency
3) https://www.theguardian.com/world/2019/nov/25/thieves-steal-priceless-treasures-dresden-green-vault-museum
4) Protection of Critical Infrastructures – Baseline Protection Concept Recommendation for Companies, Das Bundesministerium des Innern, für Bau und Heimat, Berlin, za: https://www.bmi.bund.de/SharedDocs/downloads/EN/publikationen/Basisschutzkonzept_kritische_Infrastrukturen_en.pdf?__blob=publicationFile&v=1

Dlatego zabezpieczenie najważniejszych miejsc czy zasobów nie może przesłaniać nam perspektywy całego obiektu, gdyż początek incydentu może być zupełnie gdzie indziej. Bardzo ważną funkcję pełnią ćwiczenia scenariuszowe. I, o pewnie nie będzie dla większości czytelników zaskakujące, im bardziej niekonwencjonalny (nieraz wręcz absurdalny) scenariusz, tym bardziej zaskakujące, niekiedy przykre wnioski z jego realizacji. Przypominam sobie jeden z projektów, w którym założyliśmy wejście „na plecach uprawnionych" do strefy newralgicznej. Klient stwierdził, że szkoda na to czasu, bo „ludzie są przeszkoleni", bo „tam wchodzą tylko nieliczni" albo „właściwie to tylko kilka osób wie, gdzie to jest". Umówiliśmy się więc, że zrealizujemy to jako wartość dodaną do projektu, w ramach doskonalenia własnych umiejętności. Wystarczyły trzy dni jazdy jednym autobusem z pracownikami obiektu, aby nasz audytor został uznany za „swojego" i wszedł do serwerowni bez przepustki. Bez żadnej przepustki. Wszedł więc na teren obiektu, następnie do budynku, wreszcie do samej serwerowni. Pokonał więc trzy poziomy zabezpieczeń. A test był wykonywany metodą „black box" – nasz zespół nie znał obiektu, nie znał lokalizacji serwerowni, nie znał zasad wydawania przepustek. Przypadek? Być może. Pozostała tylko dość uciążliwa świadomość, że przecież ten scenariusz miał być absurdalny...

Krytycznych elementów w obszarze bezpieczeństwa obiektów będących infrastrukturą krytyczną jest wiele. Działy bezpieczeństwa z reguły poświęcają sporo czasu na ich zdefiniowanie i opracowanie procesów zarządzania nimi. Jednak często brakuje wśród nich kilku elementów, wydawałoby się „poza wszelkimi podejrzeniami". Chciałbym zwrócić uwagę na trzy najczęściej spotykane i jednocześnie najczęściej niedoceniane.
Jednym z najczęściej lekceważonych elementów jest umundurowanie i oznakowanie pracowników ochrony. Mundur jest krytycznym elementem z tego względu, iż osoby spoza zespołu ochronnego traktują osobę w mundurze ochrony jako uprawnioną do wejścia do wielu stref, do których oni sami nie mają uprawnień dostępowych. Ponadto obecność osób w mundurach ochrony w takich miejscach nie wzbudza podejrzeń. Teoretycznie sprawa jest oczywista, bo nawet uregulowana prawnie. Czy jednak na pewno jest ona oczywista? Przyjrzałem się kilku obiektom – dość często pracownicy ochrony noszą po prostu ubiór z napisem „Ochrona". Zdarzają się rozbieżności pomiędzy oznakowaniem firmy ochrony na umundurowaniu a danymi na legitymacji (na mundurze jest inna firma niż w legitymacji). Ale nikt się tym nie przejmuje, a weryfikacja tego w praktyce jest sporadyczna (jeśli w ogóle ktoś na to zwróci uwagę). Co więcej, zarządzanie mundurami także funkcjonuje sporadycznie, a na serwisach aukcyjnych można je kupić bez problemu. Przypadki użycia munduru do dokonania przestępstwa są odnotowywane, więc każdy zarządzający obiektem (nie tylko IK) powinien podchodzić do sprawy poważnie. Jeśli jednak „standardem" jest, że dane na mundurze i w Legitymacji Pracownika Ochrony lub Legitymacji Kwalifikowanego Pracownika Ochrony nie są spójne, to potencjalny intruz nie musi się specjalnie wysilać, aby stworzyć fałszywą legitymację. W efekcie problem z infiltracją obiektu, a nawet dokonaniem sabotażu staje się dużo poważniejszy.
Druga sprawa to zakres obowiązków pracownika ochrony, który coraz częściej staje się krytycznym elementem systemu bezpieczeństwa. Przykładem mogą być prośby zarządców nieruchomości o wykonywanie przez pracowników ochrony również innych czynności, takich jak dystrybucja korespondencji, sprzątanie, odśnieżanie, a nawet tankowanie pojazdów. Jest rzeczą oczywistą, że podejmowanie czynności niezwiązanych z ochroną powoduje, iż pracownik ochrony nie wykonuje zadań ochronnych. Równie oczywiste jest, że angażowanie do tych czynności pracownika ochrony całkowicie zmienia strukturę ochrony. Oczywiście *in minus*. Ponadto pracownik ochrony chodzący bez celu przez dłuższy czas w strefach, gdzie nie powinno go być, nie zwraca niczyjej uwagi. Znane informacje o incydentach wskazują na ważną rolę takich praktyk w ułatwianiu przeprowadzania incydentów.
Trzecim krytycznym elementem, na który chciałbym zwrócić uwagę, są klucze. Są tym elementem, który może zarówno umożliwić dostęp osobie nieuprawnionej, jak i uniemożliwić dostęp osobie upoważnionej. W obu przypadkach konsekwencje mogą być bardzo poważne. Pierwszy przypadek dotyczy gospodarowania kluczami, zwłaszcza w sytuacjach ich kopiowania, zwrotu przez osoby kończące pracę w organizacji czy ich utraty w wyniku zagubienia lub kradzieży. Obie sytuacje często mają nadawany niski priorytet, co w praktyce prowadzi do utraty kontroli nad kluczami, a tym samym nad prawami dostępu do budynków i pomieszczeń. Drugi przypadek jest najczęściej efektem niekontrolowanej wymiany zamków, której konsekwencją jest posiadanie przez zespół ochronny niewłaściwych kluczy. Problem pojawia się podczas awarii technicznych, alarmu systemu wykrywania i sygnalizacji pożarowej czy podczas samego pożaru, kiedy to brak dostępu do pomieszczeń uniemożliwia lub utrudnia usunięcie awarii, weryfikację alarmu pożarowego czy szybkie podjęcie akcji gaśniczej.
Ostatnie trzy elementy mogą być przykładem erozji systemu ochrony, a występując równolegle, bardzo często powodują nawet jego destrukcję. □

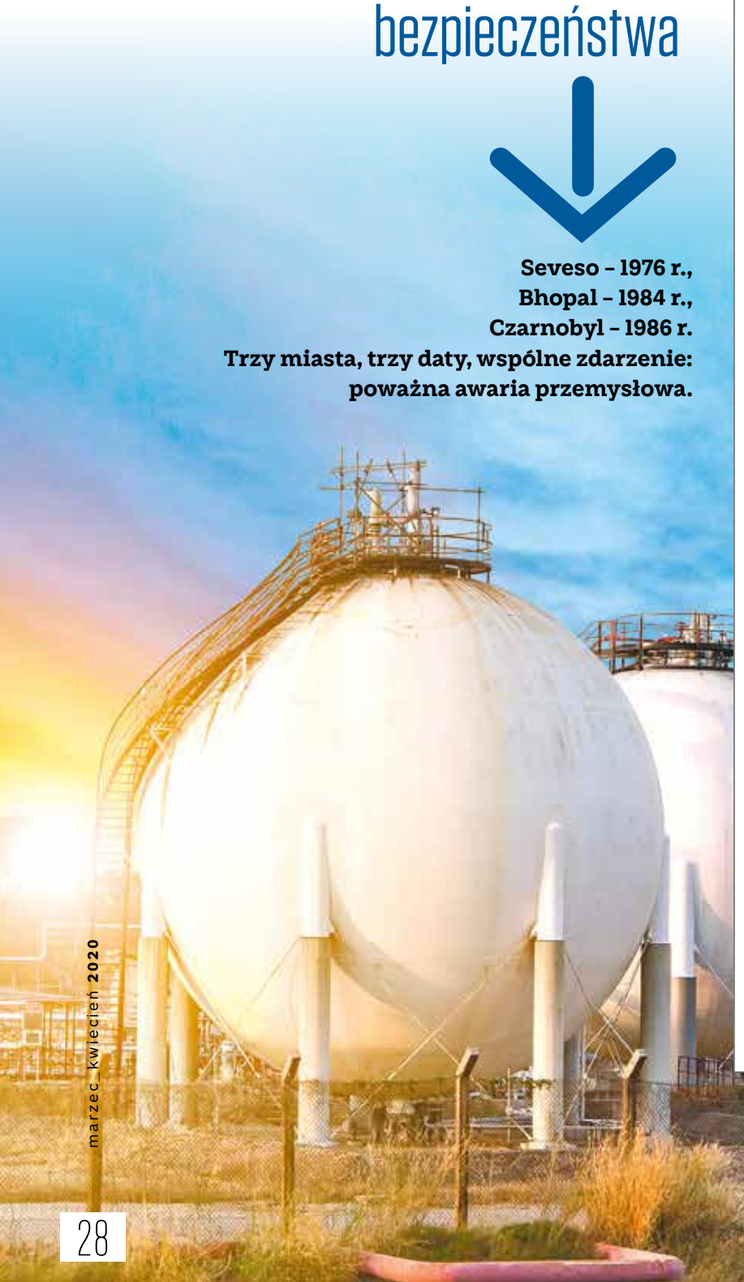
BIO

Jacek Grzechowiak

Menedżer ryzyka i bezpieczeństwa. Związany z grupą Securitas w Polsce, gdzie zarządza ryzykiem. W przeszłości zarządzał bezpieczeństwem polskich operacji Avon i Celsa. Absolwent WAT, studiów podyplomowych w SGH i Akademii L. Koźmińskiego. Gościnnie wykłada na uczelniach wyższych.

Zakłady Seveso – wyższy poziom bezpieczeństwa

**Seveso – 1976 r.,
Bhopal – 1984 r.,
Czarnobyl – 1986 r.
Trzy miasta, trzy daty, wspólne zdarzenie:
poważna awaria przemysłowa.**



TEKST
Łukasz Stępień

Najbardziej znaną awarią przemysłową jest wypadek, który miał miejsce w Czarnobylu 26 kwietnia 1986 r. W wyniku błędów technologicznych i działania człowieka doszło do przegrzania się rdzenia reaktora jądrowego, dwóch wybuchów i uwolnienia materiałów radioaktywnych do środowiska. W efekcie 146 tys. km² uległo skażeniu radioaktywnemu, 350 tys. osób zostało przesiedlonych. Z kolei najbardziej tragiczna w historii awaria przemysłowa miała miejsce 3 grudnia 1984 r. w indyjskiej miejscowości Bhopal. W wyniku serii zaniedbań w fabryce należącej do amerykańskiej korporacji Union Carbide doszło do rozszczelnienia się zbiornika zawierającego izocyjanian metylu. Ponad 40 ton trującego, cięższego od powietrza gazu spłynęło do gęsto zaludnionej doliny, 4 tys. osób poniosło zgon natychmiast, 25 tys. zmarło w wyniku powikłań, a około 50 tys. zostało trwale niezdolnych do pracy.
Jednak największy wpływ na problematykę bezpieczeństwa przemysłowego w Europie miało zdarzenie w niewielkiej miejscowości Seveso oddalonej o 50 km od Mediolanu. W wyniku błędów proceduralnych doszło tam do uwolnienia do atmosfery 2 ton niebezpiecznych substancji, w tym 3 kg skrajnie toksycznego TCDD, środka znanego w Polsce pod nazwą dioksyny (była wykorzystana do otrucia byłego prezydenta Ukrainy Wiktora Juszczenki). Z powodu katastrofy 400 osób wymagało interwencji medycznej. Zarządzono ubój 33 tys. zwierząt domowych, a całkowite koszty usunięcia skażenia środowiska szacuje się na 147 mln dolarów. Awaria i jej konsekwencje były szokiem dla państw zrzeszonych w Europejskiej Wspólnocie Gospodarczej (EWG – jeden z filarów przyszłej Unii Europejskiej).

Dyrektywa Seveso dot. przeciwdziałania awariom przemysłowym

Aby w przyszłości zapobiec takim zdarzeniom, przystąpiono do prac, których efektem była opublikowana w 1982 r. dyrektywa znana współcześnie jako Seveso I. Była to pierwsza dyrektywa zawierająca wymogi w zakresie przeciwdziałania występowaniu awarii przemysłowych i redukowaniu strat związanych z tego typu katastrofami. Obecnie funkcjonuje już trzecia wersja tej dyrektywy, zaimplementowana do polskiego systemu prawnego w ramach ustawy – Prawo ochrony środowiska z 27 kwietnia 2001 r. Cały jej rozdział IV dotyczy problematyki awarii przemysłowych. W ustawie znajduje się również definicja poważnej awarii, za którą uważa się zdarzenie, w szczególności emisje, pożar lub eksplozje, powstałe w trakcie procesu przemysłowego, magazynowania lub transportu, w których występuje jedna lub więcej niebezpiecznych substancji, prowadzące do natychmiastowego powstania zagrożenia życia lub zdrowia ludzi, lub środowiska, lub powstania takiego zagrożenia z opóźnieniem. Poważne awarie przemysłowe są związane nie tylko z zagrożeniami życia i zdrowia człowieka, ale także negatywnym oddziaływaniem na środowisko.

W ustawie – Prawo ochrony środowiska wprowadzono również pojęcie zakładów zwiększonego ryzyka awarią przemysłową (ZZR) oraz zakłady dużego ryzyka awarią przemysłową (ZDR). Są to obiekty, w których składuje się lub przetwarza określone substancje niebezpieczne w ilościach przekraczających limity określone w rozporządzeniu Ministra Rozwoju z 29 stycznia 2016 r. w sprawie rodzajów i ilości znajdujących się w zakładzie substancji niebezpiecznych, decydujących o jego zaliczeniu do zakładu o zwiększonym lub dużym ryzyku wystąpienia poważnej awarii przemysłowej. Kwalifikacja opiera się tylko na ilości substancji niebezpiecznych, bez oceny poziomu bezpieczeństwa w zakładzie ani oceny ryzyka związanego z prowadzonymi procesami. W języku potocznym obiekty tego typu są również nazywane zakładami sevesowskimi.

Często spotykanym błędem jest mylenie zakładów zwiększonego ryzyka (ZZR) i zakładów dużego ryzyka (ZDR) z obiektami podlegającymi obowiązkowej ochronie. To dwie niezależne kategorie obiektów, bazujące nie tylko na różnych podstawach prawnych (prawo ochrony środowiska – zakłady seveso; ustawa o ochronie osób i mienia – obiekty podlegające obowiązkowej ochronie), ale także odmiennych przesłankach. Wymogi nakładane na ZZR i ZDR mają za zadanie chronić życie i zdrowie ludzi oraz środowisko przed awariami przemysłowymi. Obiekty podlegające obowiązkowej ochronie mają natomiast kluczowe znaczenie dla funkcjonowania państwa. Niemniej jednak zdarzają się zakłady, które muszą jednocześnie spełniać wymogi dla zakładów sevesowskich oraz obiektów podlegających obowiązkowej ochronie. Przykładem mogą być terminale i bazy paliw.
Kwalifikacja do ZZR lub ZDR może przebiegać na podstawie kategorii zagrożeń stwarzanych przez substancje niebezpieczne albo ze względu na konkretną substancję. Na przykład składowanie 10 ton gazów łatwopalnych (niezależnie od ich składu chemicznego) jest kwalifikacją do listy zakładów zwiększonego ryzyka (ZZR), a zwiększenie tej ilości do 50 ton podwyższa kwalifikację do zakładu dużego ryzyka (ZDR). Natomiast obiekt, w którym może się znajdować 10 ton fluoru, podlega automatycznie wymogom dla ZZR, ale już zwiększenie ilości tej substancji do 20 ton podwyższa kategorię do ZDR. W ramach kwalifikacji bierze się pod uwagę potencjalną ilość substancji niebezpiecznych, która może się znajdować w obiekcie. Jeżeli ze względów produkcyjnych utrzymuje się 20 dm³ substancji w zbiorniku o pojemności 50 dm³, to zgodnie z wymogami prawnymi należy przyjąć podczas analizy wartość 50 dm³, nawet jeżeli zbiornik nigdy nie zostanie napełniony.

> Nie mylmy zakładów zwiększonego ryzyka i zakładów dużego ryzyka (obiektów sevesowskich) z obiektami podlegającymi obowiązkowej ochronie

> W każdym obiekcie zakwalifikowanym do ZZR lub ZDR musi być opracowany i wdrożony system zarządzania bezpieczeństwem

Trzy filary systemu przeciwdziałania awariom

System przeciwdziałania awariom przemysłowym opiera się na trzech filarach. Są to: działania podejmowane przez zakłady, przygotowanie instytucji państwowych na wypadek awarii oraz kontrola społeczna.
Wszystkie zakłady sevesowskie podlegają ścisłemu nadzorowi ze strony organów Państwowej Straży Pożarnej (ZZR – Komendanta Powiatowego, ZDR – Komendanta Wojewódzkiego) oraz Wojewódzkiego Inspektora Ochrony Środowiska (zarówno ZZR, jak i ZDR). Każdy zakład musi dostarczyć organom nadzorującym dokumentację, która stanowi potwierdzenie, że zakład aktywnie podejmuje działania mające na celu minimalizację ryzyka wystąpienia awarii przemysłowej. Dokumenty muszą być złożone przed uruchomieniem zakładu oraz przed każdą zmianą technologiczną lub surowcową, która może mieć wpływ na zagrożenia związane z poważnymi awariami.
Pierwszy dokument to zgłoszenie, które zawiera informacje o zakładzie: charakterystykę prowadzonej produkcji wraz z opisem instalacji, właściwości substancji niebezpiecznych obecnych w zakładzie oraz podstawę do zakwalifikowania jako ZZR lub ZDR. W ramach zgłoszenia należy uwzględnić charakterystykę otoczenia, ze szczególnym naciskiem na czynniki mogące przyczynić się do zwiększenia ryzyka wystąpienia awarii przemysłowej lub pogłębienia jej skutków, np. w wyniku efektu domina, kiedy awaria przemysłowa w jednym zakładzie może powodować wystąpienie awarii przemysłowej w sąsiednich zakładach.

W każdym zakładzie sevesowskim musi być opracowany i wdrożony system zarządzania bezpieczeństwem, gwarantujący adekwatny poziom ochrony ludzi i środowiska. Opis części systemu, która dotyczy zapobiegania awariom przemysłowym, musi zostać opisany w programie zapobiegania awariom. To drugi dokument wymagający złożenia do właściwej Komendy PSP oraz Wojewódzkiego Inspektora Ochrony Środowiska. Program musi zawierać informacje nt. analizy i oceny ryzyka wystąpienia awarii, podjętych sposobów jej zapobiegania oraz minimalizacji skutków. Zarządcy zakładów dużego ryzyka awarią przemysłową muszą przekazać jeszcze dwa dokumenty – raport o bezpieczeństwie oraz wewnętrzny plan operacyjno-ratowniczy. Celem raportu o bezpieczeństwie jest potwierdzenie, że są realizo-

wane zadania określone w programie zapobiegania awariom, np. wdrożenie systemu bezpieczeństwa, przeprowadzenie analizy ryzyka wystąpienia awarii przemysłowych. Raport o bezpieczeństwie zawiera również szczegółowy opis scenariuszy awaryjnych, jakie mogą wystąpić w instalacjach. Z kolei wewnętrzny plan operacyjno-ratowniczy zawiera informacje nt. postępowania w przypadku wystąpienia awarii przemysłowej oraz wymaganych sił i środków, aby ograniczyć jej skutki, wraz ze sposobami usunięcia skutków awarii oraz przywrócenia środowiska do stanu poprzedniego.
Teoretycznie wszystkie dokumenty muszą być złożone na 30 dni przed uruchomieniem zakładu. Teoretycznie, ponieważ zakład lub instalacja nie mogą zostać uruchomione bez uzyskania akceptacji przedstawionej dokumentacji przez jednostki PSP. W przypadku wewnętrznego planu operacyjno-ratowniczego Komenda Wojewódzka PSP ma 60 dni na wyrażenie sprzeciwu co do zawartości dokumentacji, przy czym czas ten może być przedłużony. Zgodność dokumentacji ze stanem faktycznym jest sprawdzana cykliczne podczas kontroli realizowanych przez PSP oraz Wojewódzki Inspektorat Ochrony Środowiska. W obiektach ZZR kontrole odbywają się raz na trzy lata, a w przypadku ZDR raz do roku.
Oprócz wymogów zawartych w ustawie – Prawo ochrony środowiska są realizowane również czynności kontrolno-rozpoznawcze odnoszące się do przepisów z zakresu bezpieczeństwa pożarowego. Niezależnie od kontroli planowych, po każdym zdarzeniu mającym znamiona awarii przemysłowej w obiekcie przeprowadza się kontrolę interwencyjną, z której jest sporządzany odpowiedni protokół.

Instytucje państwowe regularnie przeprowadzają ćwiczenia, przygotowując się do działania w przypadku wystąpienia awarii przemysłowych. Dla zakładów dużego ryzyka każda Komenda Wojewódzka PSP opracowuje zewnętrzny plan operacyjno-ratowniczy. Ten dokument stanowi podstawę do działań na wypadek wystąpienia takich awarii. Zewnętrzne plany operacyjno-ratownicze podlegają ćwiczeniom i analizie raz na trzy lata. Są w nie zaangażowane wszystkie instytucje uwzględnione w planie – policja, centra zarządzania kryzysowego na różnych szczeblach oraz przedstawiciele wojewódzkiego inspektora ochrony środowiska.
Społeczna kontrola jest realizowana poprzez zapewnienie dostępu do informacji nt. zagrożeń związanych z wystąpieniem awarii przemysłowych. Właściwe organy

PSP umieszczają na swoich stronach w Biuletynie Informacji Publicznej informacje o zakładach dużego i zwiększonego ryzyka znajdujących się na danym obszarze oraz o planowanych kontrolach. Ponadto każda osoba może wystąpić do właściwego dla danego zakładu Komendanta PSP o udostępnienie złożonej dokumentacji dotyczącej ZZR i ZDR. Jeżeli udostępnienie pełnej dokumentacji może mieć negatywny wpływ na zachowanie tajemnicy przedsiębiorstwa, to jego zarządca może wystąpić o ograniczenie zakresu udostępnianych informacji. W takiej sytuacji udostępnia się nie komplet dokumentacji, ale jej nietechniczne streszczenie, przy zachowaniu jawności informacji kluczowych dla bezpieczeństwa społeczności. Również na stronach internetowych ZDR muszą pojawić się informacje na temat zagrożeń, jakie mogą wystąpić w instalacjach, oraz sposobów postępowania dla ludności na wypadek wystąpienia awarii.
W przypadku niewywiązywania się przez prowadzącego zakład z obowiązków, jakie na nim spoczywają, przepisy przewidują karę grzywny, ograniczenia wolności lub aresztu. W przypadku naruszeń stwarzających zagrożenie życia i zdrowia organy prowadzące nadzór nad zakładem mogą podjąć decyzję o natychmiastowym wstrzymaniu użytkowania instalacji aż do usunięcia uchybień.

Zgodnie z informacjami podanymi przez Głównego Inspektora Ochrony Środowiska w 2018 r. funkcjonowały w Polsce 184 zakłady dużego ryzyka oraz 255 zakładów zwiększonego ryzyka. W tym samym roku doszło do 48 poważnych awarii przemysłowych, ale tylko 16 miało miejsce w miejscowościach, w których znajdowały się zakłady zwiększonego lub dużego ryzyka. Czy w takim razie w Polsce nie ma problemów z poważnymi awariami przemysłowymi? Wręcz przeciwnie. Polska jest obecnie krajem szczególnie dotkniętym przez poważne awarie przemysłowe. Tylko w zeszłym roku doszło do ponad 200 pożarów składowisk odpadów. Każdy taki pożar skutkuje uwolnieniem ogromnych ilości substancji toksycznych i niemożliwych do oszacowania, w perspektywie długofalowej, strat dla środowiska i zagrożeń dla ludzi.
Wszyscy żyjemy w cieniu ryzyka awarii przemysłowej, jednak wiele osób wciąż patrzy w niewłaściwą stronę. □

BIO

Łukasz Stępień

Specjalista z zakresu bezpieczeństwa pożarowego i zarządzania kryzysowego. Członek Krajowego Stowarzyszenia Ochrony Przeciwpożarowej w USA.

PWPW

Profesjonalne podejście do zarządzania bezpieczeństwem

O TYM, JAK BUDOWANO KONCEPCJĘ BEZPIECZEŃSTWA W POLSKIEJ WYTWÓRNI PAPIERÓW WARTOŚCIOWYCH, ROZMAWIAMY Z PIOTREM SITKO, ZASTĘPCĄ DYREKTORA BIURA OCHRONY I BEZPIECZEŃSTWA.

Piotr Sitko

Specyfika produkcji Polskiej Wytwórni Papierów Wartościowych wymaga skutecznego, efektywnego i zaawansowanego systemu bezpieczeństwa. Dotyczy to nie tylko ochrony obiektów, zabezpieczenia produkcji wartościowej i ochrony zasobów informacyjnych, ale także bezpieczeństwa zatrudnionych pracowników. Wdrożone procedury i instrukcje dotyczące zabezpieczenia produkcji wartościowej są wspomagane przez nowoczesne systemy elektroniczne, m.in. dozór wizyjny obiektów, monitoring ciągów produkcyjnych, kontrolę dostępu, sygnalizację włamania i napadu czy zaawansowane systemy sygnalizacji pożarowej.

JAKA JEST WASZA FILOZOFIA PODEJŚCIA DO KONCEPCJI BEZPIECZEŃSTWA W FIRMIE?

Na naszą fabrykę składa się zespół jedenastu gmachów budowanych w różnych czasach. Sam projekt pochodzi z okresu Polski międzywojennej, ale kompleks został całkowicie zniszczony w czasie II wojny światowej. Układ budynków jest skomplikowany ze względu na dużą liczbę przejść i klatek schodowych, które nie są ze sobą spójne. Dlatego, aby ułatwić komunikację pomiędzy pracownikami, wprowadziliśmy oznaczenia literowe i cyfrowe poszczególnych części zakładu. Oprócz głównej siedziby są jeszcze inne obiekty, ale ich struktura jest dużo mniej skomplikowana. Biorąc to wszystko pod uwagę, musieliśmy stworzyć zupełnie nową koncepcję w podejściu do zapewnienia bezpieczeństwa firmy. Nie mogliśmy czerpać z doświadczeń innych tego typu obiektów, do tego tematu trzeba było podejść całkiem nowatorsko, tzn. wymyśleć, w jaki sposób zabezpieczyć zakład, żeby móc spełnić normy obowiązujące drukarnie na światowym poziomie. Przede wszystkim zrezygnowaliśmy z autonomicznych śluz mechanicznych, ponieważ każdy nasz budynek jest inny, miejsce usytuowania tych śluz byłoby różne, więc tak naprawdę nie mielibyśmy jak ich użyć. Wymyśliliśmy formułę śluzy jako drzwi-drzwi, z biometrią 3D i czujką obecności. I to się sprawdza, takich śluz mamy kilkanaście. Zmieniliśmy całą kontrolę dostępu w tych śluzach i w nowych przejściach po to, aby zunifikować system. Również przy wyborze systemu dozoru wizyjnego kierowaliśmy się zasadą, że aby systemy uporządkować, nie należy ich mnożyć. Wiele firm ma ten problem, że w jednym obiekcie ma zainstalowanych kilkanaście systemów różnych producentów. My nasze systemy chcemy rozwijać i unifikować, by lepiej nimi zarządzać.

NO WŁAŚNIE, JAK RADZICIE SOBIE Z INTEGRACJĄ SYSTEMÓW?

Robimy to stopniowo. We wszystkich lokalizacjach zainstalowaliśmy system telewizji dozorowej jednego producenta. Jesteśmy z tego bardzo zadowoleni, ponieważ oprócz względów ekonomicznych, tzn. kosztów użytkowania czy obsługi – przeszkoleni pracownicy poradzą sobie z obsługą w każdym obiekcie – mamy również wsparcie techniczne partnera, który dostarczył nam te urządzenia. Podobnie działamy w przypadku kontroli dostępu. Wymieniamy ją sukcesywnie po to, aby zarządzać systemem z jednego centralnego serwera. To też wpłynie na ekonomię kosztów w tej części, którą zarządzam. Nie będę musiał mieć w obiekcie z kilkudziesięcioma pracownikami osoby nadającej im uprawnienia na miejscu, tylko będę mógł to robić z jednego miejsca. I dzisiaj już tak się dzieje, w tym kierunku zmierzamy. W przypadku systemu sygnalizacji i włamania jeszcze szukamy najlepszego rozwiązania, podobnie jest z wymianą systemu sygnalizacji pożarowej. Wybór będzie podyktowany tym, by na końcu wszystkie te systemy w niezbędnym dla nas zakresie zunifikować i zintegrować. Teraz już widzimy, jakie są tego korzyści, mając np. mapę wizualizacji tego, co dzieje się w naszych jedenastu obiektach. Jest to szczególnie ważne, ponieważ przy tak dużym skomplikowaniu przejść i klatek schodowych nawet osoby z długim stażem pracy nie zawsze w sytuacji stresowej potrafią szybko dotrzeć w określone miejsce.

ZARZĄDZACIE SYSTEMAMI NA MIEJSCU CZY KORZYSTACIE Z USŁUG FIRM TRZECICH??

Z racji specyfiki obiektu nasze systemy zabezpieczeń są odłączone od innych działających w fabryce i zarządzamy nimi z własnej centrali, przez własnych pracowników. Nie korzystamy z rozwiązań chmurowych, gdyż nie są one jeszcze w wymaganym przez nas stopniu bezpieczne. Oczywiście do innych zastosowań ich zabezpieczenia mogą być wystarczające, ale specyfika naszej działalności sprawia, że systemami zabezpieczeń zarządzamy sami i na miejscu.

JAKIMI KRYTERIAMI KIERUJECIE SIĘ PRZY WYBORZE SYSTEMU?

Nasze oczekiwania co do rozwiązań podzieliłbym na dwie kategorie. Po pierwsze ważne są aspekty techniczne, czyli związane z nowoczesnością produktu, by wykorzystywał najnowsze technologie i spełniał wszelkie normy bezpieczeństwa. Po drugie zwracamy uwagę na to, czy sys-

tem jest rozwojowy – tzn. czy w przypadku, gdy w przepisach pojawi się dodatkowy sposób zabezpieczenia, np. zliczania osób w danym pomieszczeniu, to tę funkcjonalność będzie można łatwo do systemu dołożyć.
Kolejną sprawą jest wybór systemu oparty na kryteriach stabilności producenta. Badamy, jak długo firma jest na rynku, czy nie stosuje wrogich przejęć, czy sama nie zamierza się sprzedać, jak wygląda jej portfolio biznesowe i historyczne. Bardzo istotne dla nas było sprawdzenie, czy system jest otwarty – oczywiście nie w rozumieniu, że każdy może się do niego dostać, ale czy będę mógł przeszkolić swoich pracowników lub firmę zewnętrzną, która jest naszym integratorem, w zakresie podstawowej konserwacji czy serwisowania. Chodzi o to, żeby nie być zmuszonym do korzystania z usług firmy trzeciej, która będzie narzucała określone ceny. To wiąże się z dużym problem, głównie finansowym. Na przykład kiedy kupię dobry system w dosyć konkurencyjnej rynkowej cenie, później może okazać się, że w ciągu kilku lat użytkowania koszty serwisu i konserwacji staną się głównym wydatkiem w budżecie.
Następna rzecz – przed wyborem określonego rozwiązania wykonywaliśmy wizyty referencyjne. Chcieliśmy zobaczyć, jak te wybrane systemy funkcjonują w dużych obiektach, które też wymagają zapewnienia wysokiego poziomu bezpieczeństwa. To nas upewniało, że podjęte decyzje będą dobre. Zapraszaliśmy również producentów na prezentacje do naszej firmy, odbyliśmy co najmniej kilkanaście takich spotkań.
Bardzo ważne dla nas było również śledzenie oferty rynku. Odwiedzaliśmy targi branżowe, nie tylko krajowe, ale i międzynarodowe, np. Ifsec w Londynie czy Intersec w Dubaju. Przyglądaliśmy się nie tylko pojawiającym się nowościom, ale także informacjom biznesowym. Nie ukrywam, że jest to rynek bardzo trudny i skomplikowany. Często zdarza się bowiem, że niedawno zakupiony system nie będzie dłużej wspierany z powodu przejęcia producenta przez inną firmę. A to może stanowić poważny problem z użytkowaniem urządzeń zabezpieczających naszą firmę.

CZY – JAKO EKSPERT – MOŻE PAN UDZIELIĆ KILKU PORAD, JAK UNIKNĄĆ NAJCZĘSTSZYCH BŁĘDÓW W PRZYGOTOWANIU KONCEPCJI BEZPIECZEŃSTWA W OBIEKTACH INFRASTRUKTURY KRYTYCZNEJ?

Pierwsza rzecz, jaką należy zrobić, to dokonać analizy własnych potrzeb. Sprawdzić, w jakim miejscu jest firma, a w jakim miejscu chcielibyśmy ją widzieć za rok lub dwa lata. I przekonać osoby zarządzające do tego, że inwestowanie w bezpieczeństwo jest dziś bardzo istotne. Widzimy to zwłaszcza w obecnej sytuacji kryzysowej, jak ważne jest szybkie i sprawne reagowanie oraz podejmowanie właściwych decyzji.
Po drugie należy dokładnie przyjrzeć się temu, co jest oferowane na rynku i sprawdzić potencjalnego partnera. Czy system, który chcemy wybrać, jest stabilny i niezawodny, jak wygląda jego otwartość. Czy producent oferuje szkolenia z obsługi i konserwacji, które nie będą obarczone dodatkową opłatą.
Trzecią bardzo ważną rzeczą jest wzajemna współpraca z integratorem i partnerstwo z dostawcą. Często jest tak, że nie mamy bezpośrednich umów z producentem konkretnego systemu, ale jego wsparcie techniczne, współodpowiedzialność za utrzymanie wysokiego poziomu bezpieczeństwa w zakładzie jest bardzo ważne. My jesteśmy bardzo zadowoleni ze współpracy z naszymi partnerami. Przy wymianie zarówno systemu kontroli dostępu, jak i systemu dozoru wizyjnego mieliśmy poczucie wsparcia i pewność, że w każdej chwili możemy liczyć na ich pomoc. Ważne jest więc szukanie takich rozwiązań i takich partnerów, którzy będą właśnie w ten sposób podchodzili do współpracy.
Moim zdaniem bardzo ważna jest też ciągła edukacja własna i pracowników firmy. Pomaga w tym uczestniczenie w targach i różnego rodzaju konferencjach branżowych. Możliwość rozmowy i wymiany doświadczeń jest bardzo pomocna. Osobiście polecam też systematyczną lekturę czasopisma „a&s Polska", z wieloma ciekawymi opracowaniami ekspertów z kraju i całego świata.

NIE SPOSÓB UNIKNĄĆ PYTANIA O SYTUACJĘ ZWIĄZANĄ Z EPIDEMIĄ KORONAWIRUSA. JAKIE DZIAŁANIA PODJĘLIŚCIE W PWPW?

Staraliśmy się reagować jak najszybciej. Jeszcze zanim oficjalnie ogłoszono stan pandemii, wdrożyliśmy opracowane wcześniej procedury gwarantujące ciągłość działania firmy i te związane z planem zarządzania kryzysowego. Rozpoczęliśmy mierzenie temperatury ciała pracownikom, jeszcze zanim wejdą na teren zakładu. Do minimum ograniczyliśmy serwis zewnętrzny, odwołaliśmy wyjazdy zagraniczne i udział w konferencjach. Sztab kryzysowy spotyka się codziennie, aby szybko reagować na zaistniałe sytuacje. Wdrożyliśmy procedury ograniczające kontakty osobowe, które pozwolą funkcjonować zakładowi nawet wtedy, gdy przypadek zarażenia koronawirusem zostanie wykryty u jednego z naszych pracowników. Jesteśmy zakładem, który ze względu na rodzaj działalności związanej z bezpieczeństwem funkcjonowania państwa nie może pozwolić sobie na zaprzestanie działalności.
Ograniczyliśmy liczbę pracowników – osoby, które mogą pracować zdalnie, pracują w trybie home office. Tam, gdzie nie możemy ograniczyć kontaktów, np. z klientami, minimalizujemy strefy możliwych zagrożeń, stosujemy maseczki, rękawiczki, odstępy między poszczególnymi osobami. Zaczynamy pracę o różnych godzinach po to, aby ograniczyć liczbę osób przebywających jednocześnie przy wejściu. Jak powiedział Maciej Biernat, prezes PWPW, to jest test na nasze człowieczeństwo. Wszystko zależy od tego, jak się ludzie zachowają, jaka będzie atmosfera, czy umiemy podporządkować się procedurom. Na razie ten test nasi pracownicy zdają celująco, za co jesteśmy im bardzo wdzięczni. To oni są naszym motorem działania – dla nich tu jesteśmy, podejmujemy działania, żeby oni i ich rodziny czuli się jak najbezpieczniej.

BYĆ MOŻE TERAZ, W OBECNEJ SYTUACJI, TO PYTANIE ZABRZMI DZIWNIE, ALE JAK PAN WIDZI PRZYSZŁOŚĆ RYNKU SECURITY?

Myślę, że w części technicznej rynek nadal będzie się intensywnie rozwijał. Systemy będą się coraz bardziej integrowały, udział człowieka zostanie ograniczony na rzecz wykorzystania sztucznej inteligencji. Ale dziś nie widzę takiej możliwości, żebyśmy mogli całkowicie wyeliminować pracę człowieka i zastąpić go maszyną. Do tego jeszcze daleko.
Mam nadzieję na stabilizację rynku w przyszłości, na to, że będziemy mieli liderów w każdym sektorze branży, czy to telewizji dozorowej, kontroli dostępu, czy w zabezpieczeniach przeciwpożarowych, z rozwiązaniami zbliżonymi cenowo. Wtedy zdrowa konkurencja będzie napędzała rozwój rynku. Bo nie chodzi o to, żeby wymuszać na kliencie wymianę urządzeń na nowe, ale proponować systemy rozwojowe, które umożliwią korzystanie z dobrodziejstw nowoczesnej technologii bez konieczności wyrzucania tego, co już mamy.

BARDZO DZIĘKUJEMY ZA ROZMOWĘ

DEEP LEARNING
w systemach zabezpieczeń IK

Obiekty infrastruktury krytycznej mają podstawowe znaczenie dla funkcjonowania społeczeństwa i gospodarki, dlatego wymagają specjalnego zabezpieczenia. Ważny jest dobór odpowiednich rozwiązań gwarantujących utrzymanie wysokiego poziomu bezpieczeństwa. Wychodząc naprzeciw tym potrzebom, firma Hikvision oferuje najnowsze urządzenia wykorzystujące zdobycze technologii głębokiego uczenia.

Technologia głębokiego uczenia (*deep learning*) **pozwala na klasyfikację obiektów, umożliwiając filtrowanie zdarzeń alarmowych pod kątem wykrycia ruchu człowieka lub pojazdu.** Nie analizuje się jednak grupy pikseli o odpowiedniej wielkości i poruszających się z odpowiednią prędkością – jak to ma miejsce w typowej analizie wizyjnej. W technologii *deep learning* szuka się wzorca, czyli takich obiektów, które system identyfikuje jako człowieka lub pojazd. Eliminuje to w dużym stopniu liczbę fałszywych alarmów, ułatwiając zarządzanie bezpieczeństwem obiektu.

– *Dzięki szerokiej ofercie mamy rozwiązania dla obiektów zarówno bezobsługowych (system jest obsługiwany z innego miejsca), jak i takich, które z racji specyfiki działania mają osoby zarządzające bezpieczeństwem na miejscu. Polecamy przede wszystkim najnowsze modele kamer z serii Deepinview i rejestratory serii Deepinmind. Najpopularniejsze są kamery typu bullet z linii siódmej: 2- i 4-megapikselowe (DS-2CD7A26G0-IZHS, DS-2CD7A46G0-IZHS) oraz analogiczne modele w wersji kopułowej z funkcją face capture, która wykrywa człowieka i obraz jego twarzy przesyła do systemu. Dzięki temu bardzo szybko można zweryfikować, czy osoba ma uprawnienia do przebywania w danej strefie. Kamery z funkcją face capture współpracują z rejestratorami Deepinmind z funkcją identyfikacji twarzy i dedykowanymi serwerami Hikvision oraz systemami innych producentów, zintegrowanymi z naszymi urządzeniami* – wyjaśnia Tomasz Goljaszewski, Key Account Manager w Hikvision Poland.

W obiektach bezobsługowych najważniejsze jest szybkie wykrycie naruszenia strefy, zlokalizowanie intruza i natychmiastowe przekazanie tej informacji grupie interwencyjnej. Do ochrony perymetrycznej takiego obiektu – oprócz kamer typu *bullet* – Hikvision poleca kamery termowizyjne, również z wbudowaną technologią *deep learning*. Oprócz funkcji zaawansowanej analizy obrazu wykorzystującej klasyczny wskaźnik liczby naruszonych pikseli, mają one detekcję opartą na wykrywaniu wzorca, realizowaną do ustalonej odległości.

– *Odległość tę ustala się jako 3-krotną wartość ogniskowej obiektywu, czyli np. dla kamer termowizyjnych z sensorami 384 x 288 i 640 x 512 pix i obiektywem 25 mm jest to odległość do 75 m. Kamery te znakomicie sprawdzają się w ochronie takich obiektów, jak stacje energetyczne, elektrownie i elektrociepłownie, porty lotnicze, miejsca składowania ropy i gazu* – dodaje T. Goljaszewski.

W roku 2019 Hikvision wprowadził do oferty radary o zasięgu 60 m i 120 m. Ich pracy nie ograniczają złe warunki atmosferyczne (np. obfite opady śniegu, deszczu czy mgła), jak to ma miejsce w przypadku kamer wizyjnych lub, w mniejszym stopniu, termowizyjnych. I choć sam radar nie zidentyfikuje człowieka, to dzięki możliwości integracji z głowicami szybkoobrotowymi Hikvision (maks. czterema) można taką weryfikację szybko przeprowadzić. W momencie wykrycia obiektu radar przekazuje sygnał do głowicy szybkoobrotowej, która natychmiast kieruje się na wyznaczony punkt i podąża za obiektem.

W ofercie Hikvision znajdują się też kamery termowizyjne stosowane do pomiaru temperatury ciała człowieka z dokładnością ±0,5°C. Obecnie są one szczególnie przydatne w walce z koronawirusem – mogą być stosowane na lotniskach, dużych węzłach komunikacyjnych czy przejściach granicznych, czyli wszędzie tam, gdzie konieczna jest szybka ocena stanu zdrowia ludzi. Pomiar jest bardzo szybki, trwa ok. 1 s, a temperatura może być mierzona jednocześnie kilkunastu osobom przebywającym w polu widzenia kamery. □

Hikvision Poland

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

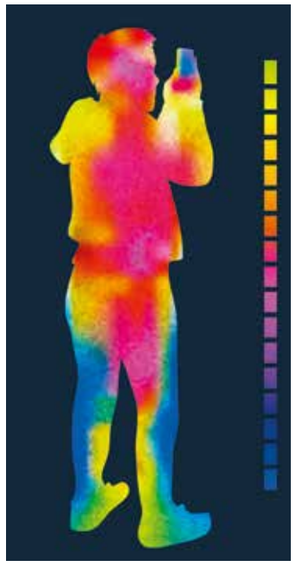
Termowizja, VMS, PSIM+

– niezbędne elementy ochrony zewnętrznej IK dostarczane przez C&C Partners

Pomimo zawrotnego rozwoju technologii, wprowadzania sieci neuronowych i sztucznej inteligencji wciąż sytuacją wysokiej wagi w zapewnieniu bezpieczeństwa fizycznego obiektów infrastruktury krytycznej jest wpływ środowiska zewnętrznego.

Opady śniegu lub deszczu, mgła czy cienie drzew powodują, iż analiza obrazu z kamer generuje bardzo dużą liczbę fałszywych alarmów. Tę sytuację częściowo poprawia serwerowa analiza obrazu wykonywana przez zaawansowane systemy zarządzania wizją VMS, certyfikowane przez niezależne ośrodki potwierdzające jakość analizy obrazu w restrykcyjnych testach poligonowych, np. i-LIDS@.

Tam, gdzie liczy się czas reakcji, pewność rozwiązania, zarządzanie wieloma obiektami o strategicznym znaczeniu dla bezpieczeństwa energetycznego, militarnego czy zdrowotnego w kraju, nie ma miejsca na pomyłki. Rozwiązaniem zapewniającym najwyższy poziom bezpieczeństwa obiektów, o minimalnym wskaźniku fałszywych alarmów, wysokim poziomie pewności, minimalnym czasie reakcji oraz znikomych wymaganiach dotyczących transmisji danych są kamery termowizyjne Opgal. Ich izraelski producent specjalizuje się w zaawansowanych systemach termowizyjnych, o zastosowaniu zarówno w obszarach cywilnych, jak i tajnych technologiach wojskowych.
Idealnym rozwiązaniem dla ochrony perymetrycznej rozległych terytorialnie systemów jest seria kamer wieloprzetwornikowych ACCURACII, zawierających dwa moduły kamerowe – z przetwornikiem optycznym i termowizyjnym, bolometrem chłodzonym (model XR) lub niechłodzonym (model XRU) – umieszczone na głowicy obrotowej PTZ. Jednostka kamerowa nadzoruje obszar o średnicy do 40 tys. m. Automatyczne wysterowanie modułów (obrót, pochylenie i zoom optyczny) umożliwia system radarowy. Radar wykryje każdy ruch obiektów, ale nie jest w stanie zidentyfikować, czym jest namierzony cel. Z kolei kamery termowizyjne Opgal oceniają, czy namierzony cel stanowi zagrożenie. Dane na temat położenia obiektu są precyzyjnie wskazywane na koordynatach GPS bazujących na mapach GIS systemu PSIM Winguard, obraz wideo natomiast jest wyświetlany na ścianie wizyjnej kontrolowanej przez system VMS VDG Sense. Układ kamerowy ACCURACII XRU zapewnia detekcję najnowszego dużego zagrożenia, jakim są ataki dokonywane z wykorzystaniem dronów.



W ochronie mniejszych obszarowo obiektów, np. stacji energetycznych czy systemów uzdatniania wody, dobrze sprawdza się seria kamer stacjonarnych Sii OP. Oprócz modułu termowizyjnego taka kamera w jednej obudowie zawiera również moduł wizyjny (podwójna weryfikacja zdarzeń). Zapewnia detekcję intruza na odległość 200–800 m. Kamery z serii Sii mogą być również wyposażone w funkcje analizy obrazu, gwarantując zarówno ochronę przed wtargnięciem intruza, jak i ochronę mienia przed pożarem czy przegrzewaniem się elementów infrastruktury, z automatycznym alarmowaniem w systemie VMS VDG Sense oraz PSIM Winguard.

Ochrona infrastruktury krytycznej, tak istotna dla bezpieczeństwa państwa i jego obywateli, jest najważniejszym zadaniem stawianym przed szefami administracji rządowej i samorządowej. Powinni oni zwracać szczególną uwagę na dobór odpowiednich technologii, niezawodnych, o wysokim poziomie zaawansowania technicznego, co decyduje o skuteczności przeciwdziałania aktom wandalizmu czy atakom terrorystycznym. ▫

ABLOY – zaufany doradca w kluczowych dla bezpieczeństwa sprawach

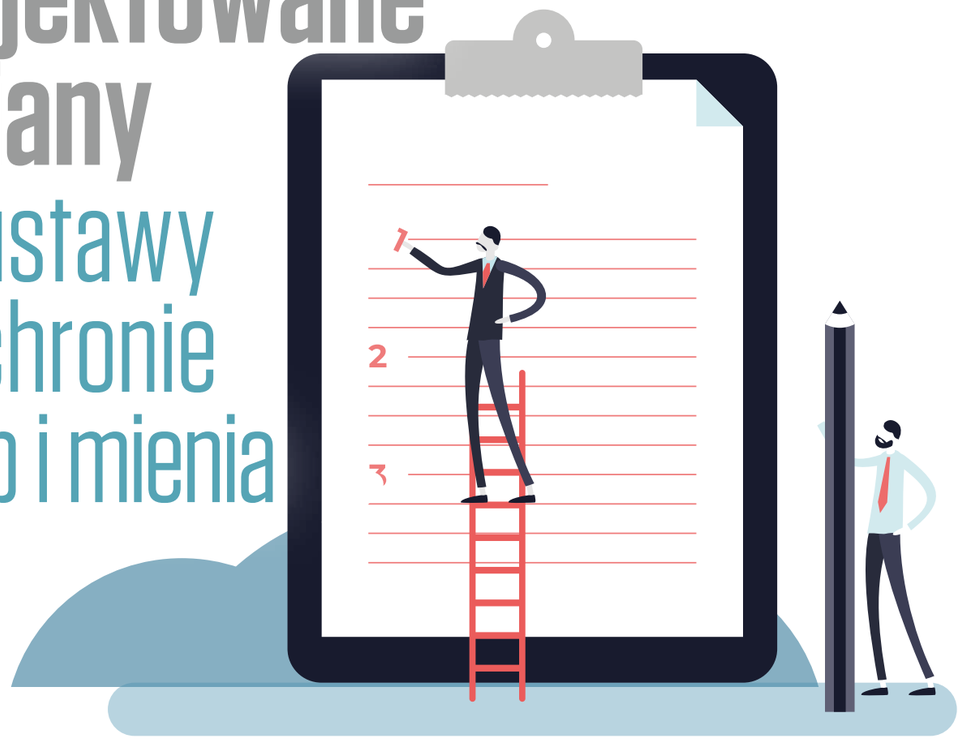
Zakwalifikowanie obiektów do kategorii infrastruktury krytycznej bądź szczególnie ważnych dla bezpieczeństwa i obronności państwa czy podlegających obowiązkowej ochronie niesie za sobą obostrzenia i obciążenia dla zarządców. Najważniejszym wymaganiem jest zapewnienie odpowiedniego stopnia zabezpieczenia i poziomu bezpieczeństwa. To ogromne wyzwanie dla osób odpowiedzialnych za opracowanie koncepcji ochrony. Szczególną trudnością jest jej wdrożenie w obiektach już istniejących oraz w infrastrukturze rozproszonej.

Konrad Szadkowski
Key Account Manager PEU

Największym sprzymierzeńcem infrastruktury rozproszonej są zabezpieczenia mechaniczne, które jako jedyne stawiają rzeczywisty opór potencjalnym atakom. Z tego powodu obiekty wyposaża się w ogrodzenia, kraty, drzwi i okna o odpowiedniej klasie odporności na włamanie. Istotne jest, aby wszystkie przyjęte rozwiązania stanowiły przeszkodę dla intruzów, ale jednocześnie nie utrudniały dostępu osobom uprawnionym.
W osiągnięciu kompromisu pomoże zastosowanie wkładek do zamków, kłódek czy zamków przemysłowych wykonanych w technologii dyskowej ABLOY PROTEC2. Są to rozwiązania odporne na manipulacyjne metody otwierania – do obiektu dostaniemy się jedynie, używając właściwego klucza albo niszcząc zamknięcie (przy stosowaniu klasycznych zamknięć zastawkowych powszechne są tzw. włamania bez śladu).
Zamknięcia PROTEC2 mają także wysoką odporność na środowisko korozyjne i niekorzystne warunki atmosferyczne. Wytrzymałość środowiskowa i udarowa wynika z zastosowania wysokiej jakości materiałów oraz wyeliminowania sprężyn. Unikatową zaletą ABLOY PROTEC2 jest brak możliwości kopiowania klucza (ścisły nadzór fabryki nad surówkami kluczy).
Ponadto w kluczu znajduje się ruchoma kulka współpracująca z zamknięciem (ochrona patentowa do 2031 r.). Zadaniem kulki jest uniemożliwienie wykonania kopii klucza na drukarce 3D. Tak zabezpieczony klucz można bez obaw powierzyć pracownikom i podwykonawcom, wiedząc, że po jego zwrocie nie dostaną się oni do obiektów bez naszej wiedzy.

Korzystna z punktu widzenia bezpieczeństwa jest rejestracja wejścia do obiektu. Wdrożenie kontroli dostępu w klasycznym ujęciu w infrastrukturze rozproszonej nastręcza mnóstwa problemów: wymaga instalacji specjalnych urządzeń, prowadzenia okablowania, zapewnienia zasilania, utrzymania łączności z centrum nadzoru. Wychodząc naprzeciw potrzebom zarządców obiektów, ABLOY zaproponował innowacyjne rozwiązanie łączące zabezpieczenia mechaniczne (PROTEC2) z elektroniką mającą wszystkie zalety kontroli dostępu – ABLOY PROTEC2 CLIQ. Wkładki, kłódki i zamki przemysłowe w systemie CLIQ, oprócz obracających się dysków, zawierają elektronikę. Co ciekawe, zamknięcia nie wymagają żadnego zasilania! Klucze w tym rozwiązaniu mają, oprócz klasycznego brzeszczotu, elektronikę z wymienną baterią – wprowadzony klucz jest dla zamknięcia źródłem zasilania.
W kluczu są zapisane prawa dostępu – do określonych obiektów i pomieszczeń, w określonych dniach i godzinach. Każde zamknięcie i każdy klucz CLIQ ma rejestr zdarzeń, dzięki czemu wiadomo kto, kiedy i jak długo przebywał w danej lokalizacji. Prawa dostępu dla użytkownika klucza można nadawać zdalnie, a w przypadku zgubienia klucza łatwo go dezaktywować. Decydując się na ABLOY PROTEC2 CLIQ, można elastycznie korzystać z zamknięć elektronicznych (w obiektach wrażliwych) i mechanicznych (w mniej istotnych). Zamknięcia można przenosić między lokalizacjami, aby dopasować się do dynamicznie zmieniającego się przedsiębiorstwa. ▫

Projektowane zmiany do ustawy o ochronie osób i mienia



Dla administratorów obiektów kluczowych dla bezpieczeństwa państwa obecnie istotna jest następująca informacja: resort spraw wewnętrznych i administracji przygotował projekt ustawy o zmianie ustawy o ochronie osób i mienia oraz niektórych innych ustaw. Obecnie projekt znajduje się na etapie uzgodnień międzyresortowych. Projektowane zmiany do ustawy o ochronie osób i mienia mają służyć przeciwdziałaniu zagrożeniom o charakterze terrorystycznym wobec obiektów ważnych dla funkcjonowania państwa, które – w kontekście wzrostu zagrożenia terroryzmem w Europie – stanowią potencjalny cel ataku.

TEKST
Jarosław Stelmach

Projekt zakłada m.in. wprowadzenie obligatoryjnego stosowania zarówno specjalistycznych uzbrojonych formacji ochronnych (SUFO), jak i zabezpieczenia technicznego w celu zapewnienia ochrony obszarów podlegających obowiązkowej ochronie. W dotychczasowej ustawie pomiędzy kluczowymi dla branży określeniami ochrona fizyczna i zabezpieczenie techniczne było słowo LUB, teraz będzie łącznik I (choć w praktyce i tak nie było szans na uzgodnienie planu ochrony jedną formą jej realizacji). Zaplanowane jest wprowadzenie wymogu obligatoryjnej ochrony na zasadach określonych w ustawie o ochronie osób i mienia, zakładów produkujących, remontujących oraz magazynujących broń i amunicję do użytku cywilnego – obowiązywało do tej pory tylko w stosunku do sektora wojskowego.
Podobnie planowane jest objęcie wymogiem zapewnienia obowiązkowej ochrony centrów dystrybucji gotówki przetwarzających wartości pieniężne w znacznych ilościach (nie było ich do tej pory). Planuje się wprowadzenie obowiązku przedkładania planu ochrony obszarów, obiektów lub urządzeń podlegających obowiązkowej ochronie w terminie najpóźniej sześciu miesięcy od dnia otrzymania informacji o umieszczeniu obszaru, obiektu lub urządzenia w ewidencji (dotychczas nie było takiego terminu i stąd wiele obiektów do dzisiaj nie posiada planów ochrony).

W mojej ocenie ważne jest to, że w ramach projektowanych rozwiązań zapewnia się ujednolicenie zakresu planów ochrony opracowywanych na podstawie dwóch odrębnych reżimów prawnych, tj. ustawy o zarządzaniu kryzysowym oraz ustawy o ochronie osób i mienia. W tym zakresie proponowane jest określenie (na podstawie upoważnienia ustawowego przewidzianego w projekcie) struktury planu ochrony w taki sposób, by spełniał on jednocześnie wymogi określone w ustawie z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym. Powyższe rozwiązanie pozwoli zmniejszyć liczbę obowiązków administratorów obiektów infrastruktury krytycznej przy jednoczesnym zapewnieniu kompletności informacji zawartej w wymaganej dokumentacji. Choć w mojej opinii będzie to w praktyce trudne do wykonania. Nie sądzę, by instytucje zatwierdzające powyższe dokumenty zgodziły się na przedkładanie jednego planu mającego przecież inną strukturę i formę zapewne.

Przewiduje się przy tym wprowadzenie upoważnienia ustawowego w celu dookreślenia przez Radę Ministrów (w drodze rozporządzenia) trybu tworzenia, uzgadniania i aktualizacji, a także szczegółowego zakresu danych i struktury planu ochrony obiektów podlegających obowiązkowej ochronie (do tej pory mieliśmy metodykę KGP, bez żadnej wzmianki ustawowej na ten temat). Proponuje się także wprowadzenie okresu ważności tychże planów ochrony (przedłożenie do uzgodnienia planów ochrony będzie się odbywać nie rzadziej niż raz na pięć lat).
Jest też element egzekucji. W celu zapewnienia skutecznego egzekwowania niektórych obowiązków określonych w ustawie o ochronie osób i mienia projektowane jest wprowadzenie zmian w przepisach karnych tej ustawy. W tym zakresie przewiduje się wprowadzenie grzywny za nieprzedłożenie planu ochrony do uzgodnienia wbrew obowiązkowi określonemu w projektowanym art. 7 ust. 3 i ust. 7. Za niezapewnienie, wbrew obowiązkowi, fizycznej i technicznej ochrony obszaru, obiektu, urządzenia lub transportu przewidywana jest z kolei grzywna, ograniczenie wolności albo pozbawienie wolności do lat 2.

Zmiany są koniecznością i odpowiedzialnym krokiem ustawodawczym, by nadążyć za rosnącymi zagrożeniami ze strony różnych sprawców, w tym o charakterze terrorystycznym

Dla infrastruktury krytycznej ważne jest to, że w ustawie z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2019 r. poz. 1398 oraz z 2020 r. poz. 148) wprowadza się przepis w art. 6: Rada Ministrów określi, w drodze rozporządzenia, minimalne wymagania wobec właścicieli, posiadaczy samoistnych i zależnych obiektów, instalacji, urządzeń i usług infrastruktury krytycznej w zakresie zapewnienia bezpieczeństwa osobowego, fizycznego i teleinformatycznego, mając na uwadze dobór odpowiednich środków związanych z przeciwdziałaniem zagrożeniom dla infrastruktury krytycznej. (Miałem zaszczyt pracować w latach 2017–2018 nad tymi standardami, personalnie bardzo cieszę się, że udaje się to powoli wprowadzać w życie).
Informacją istotną dla kierowników obiektów jest ustawowy obowiązek prowadzenia Książki Elektronicznego Systemu Zabezpieczeń, dokumentującej zdarzenia utrwalone przez urządzenia i systemy alarmowe. To kierownik będzie również ustawowo odpowiadał za sprawność tych systemów.

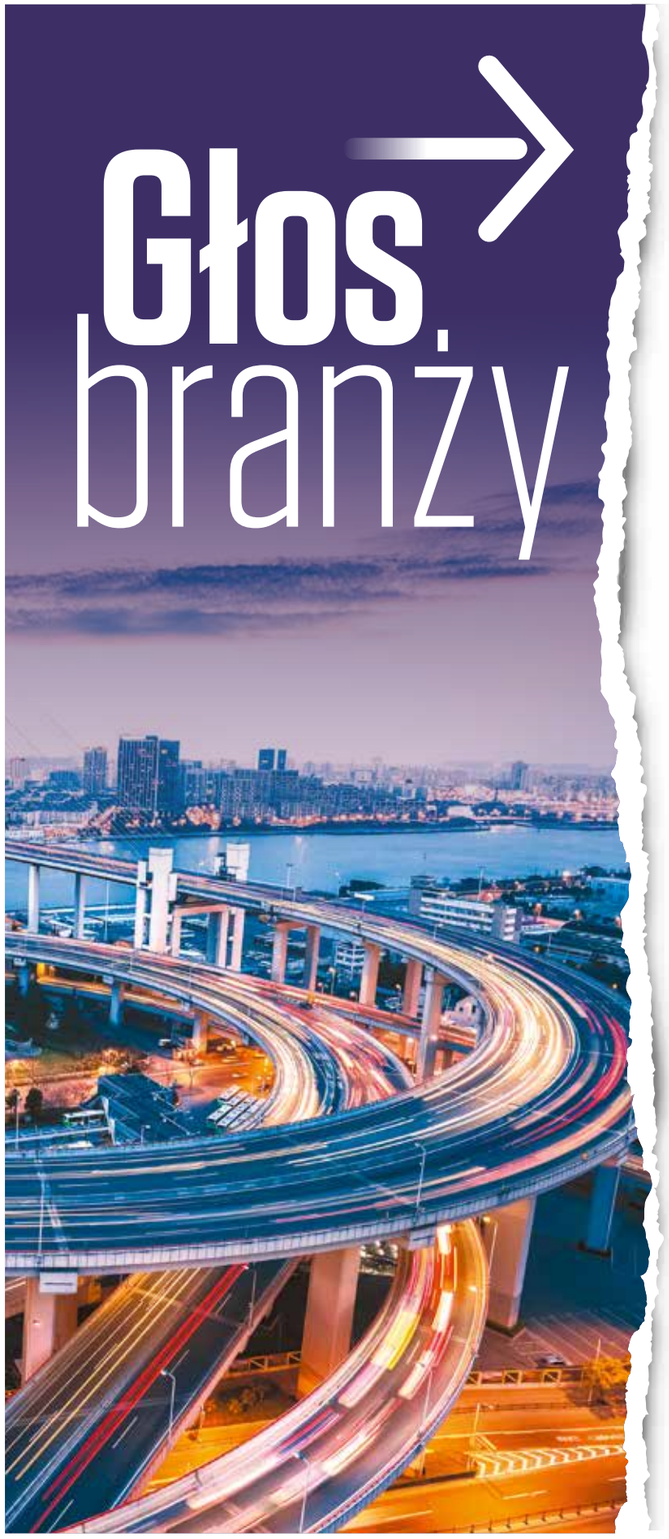
Te i wiele innych zmian jest proponowanych w ustawie o ochronie osób i mienia – zapraszam do zapoznania się z projektem zmian w ustawie oraz do poczytania uzasadnienia. Zainteresowanym prześlemy wersje PDF tych dokumentów z linkami do śledzenia zmian ustawowych. Prosimy o kontakt pod adresem: kontakt@safetyproject.pl. W mojej ocenie powyższe zmiany są koniecznością i odpowiedzialnym krokiem ustawodawczym, by nadążyć za rosnącymi zagrożeniami ze strony różnych sprawców, w tym o charakterze terrorystycznym. Pozostaje tylko jedna i zarazem podstawowa wątpliwość – czy i kiedy administratorzy obiektów kluczowych zagospodarują środki, by te uchwalane zmiany i standardy wprowadzić.

BIO

mjr rez. dr inż. Jarosław Stelmach

Ekspert w obszarze antyterroryzmu oraz bezpieczeństwa obiektów użyteczności publicznej. Właściciel firmy doradczo-szkoleniowej Safety Project oraz pomysłodawca i organizator międzynarodowego kongresu bezpieczeństwa antyterrorystycznego SAFE PLACE. Posiada aktualne wpisy na listy kwalifikowanych pracowników ochrony oraz zabezpieczenia technicznego. Ekspert zewnętrzny w grupie zadaniowej MSWiA w zakresie bezpieczeństwa AT IK w latach 2017–2018.

Głos branży



CO RADZĄ EKSPERCI NA TEMAT BEZPIECZEŃSTWA OBIEKTÓW INFRASTRUKTURY KRYTYCZNEJ SZCZEGÓLNIE W ZAKRESIE ZAPEWNIENIA CIĄGŁOŚCI DZIAŁANIA W CZASACH EPIDEMII KORONAWIRUSA

Adam Brzezicki

AXIS Communications

Rozwiązania Axis dla obiektów IK

Placówki infrastruktury krytycznej to obiekty bardzo wymagające pod względem stosowanych zabezpieczeń i monitoringu wizyjnego. Jakość produktów jest traktowana niezwykle poważnie i nie ma tu miejsca na kompromisy.

Bardzo istotnym aspektem jest ograniczenie dostępu osobom niepowołanym. Oprogramowanie Axis Perimeter Defender działające bezpośrednio w kamerach Axis gwarantuje skuteczną detekcję intruzów, np. podczas próby sforsowania ogrodzenia. Oprogramowanie Axis License Plate Verifier pozwoli zarządzać pojazdami wjeżdżającymi na teren obiektu lub wyjeżdżającymi z niego. Z kolei systemy kontroli dostępu zintegrowane z systemami wizyjnymi pozwolą w łatwy i skuteczny sposób kontrolować dostęp do obiektu.

Kamerom i urządzeniom stosowanym w ochronie infrastruktury krytycznej często stawia się specjalne wymagania, gwarantujące wymagany poziom bezpieczeństwa oraz długi czas działania. Na przykład kamery pracujące w strefach zagrożenia wybuchem bezwzględnie muszą spełniać normy ATEX, a w przypadku instalacji nadmorskiej wymagana jest obudowa ze stali nierdzewnej.

Systemy zabezpieczeń muszą być bezpieczne i niezawodne również od strony oprogramowania. Urządzenia powinny wspierać poziom zabezpieczeń obowiązujący w danej organizacji. Dlatego urządzenia marki Axis mają zarówno podstawowe zabezpieczenia, np. filtrację adresów IP, jak i bardziej zaawansowane funkcje, takie jak szyfrowana komunikacja, wsparcie SNMP czy Secure Boot i Signed Firmware. „Wisienką na torcie" jest dostępność oprogramowania z rodziny LTS – *Long Term Support* – zapewniającego stabilność działania, bezpieczeństwo oraz bezproblemowe aktualizacje systemów zabezpieczeń.

Marcin Walczuk

BCS

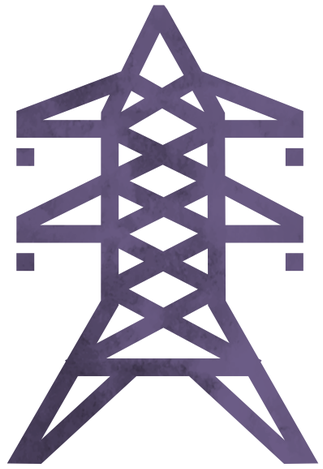
By uniknąć paniki

W sytuacji szalejącej na świecie pandemii koronawirusa szczególnie istotne jest unikanie paniki wśród ludności cywilnej. Ludzie są już wystarczająco wystraszeni tym, co dzieje się wokół. Każde dodatkowe zakłócenie normalnego funkcjonowania może powodować niepotrzebne sytuacje zagrażające zdrowiu i życiu. Dlatego niezwykle istotne jest odpowiednie zabezpieczenie nieprzerwanego dostępu do tak podstawowych usług, jak dostawy energii elektrycznej, bieżącej wody, gazu i równie ważnych środków zapewniających łączność: telefonii komórkowej czy Internetu. Wszystkie te usługi są świadczone przez przedsiębiorstwa infrastruktury krytycznej. Zachowanie ciągłości pracy i dostaw jest krytyczne i niezbędne do prawidłowego i niezachwianego funkcjonowania państwa.

Znaczna część przedsiębiorstw infrastruktury zaliczanej do krytycznej znajduje się w rękach prywatnych i wtedy to na nich spoczywa konieczność zapewnienia bezpieczeństwa swojego sektora. W takiej sytuacji nie mogą szczędzić wydatków na zabezpieczenia. Czy to będzie system telewizji dozorowej, włamania i napadu, kontroli dostępu, czy sygnalizacji pożarowej – nie powinno być tutaj mowy o półśrodkach i oszczędnościach.

Nie wolno również zapominać o ludziach, którzy cały ten sprzęt mają obsługiwać. Muszą być odpowiednio przeszkoleni, aby móc w pełni wykorzystać oferowane możliwości zabezpieczeń elektronicznych, i we właściwy sposób zachować się w sytuacjach kryzysowych. Konieczne jest stosowanie się do już istniejących procedur bezpieczeństwa, a w razie potrzeby tworzenie nowych, które przygotują na nieuwzględnione do tej pory źródła zagrożenia.

BCS proponuje rozwiązania dla każdego sektora wchodzącego w skład infrastruktury krytycznej, czy będzie to związane z zabezpieczeniem dużych zakładów produkcyjnych, rozległych linii przesyłowych, gazociągów, czy mniejszych placówek, takich jak banki lub urzędy. Korzystając z naszych produktów IP, można tworzyć rozproszone systemu CCTV obsługiwane z centralnej stacji monitoringu za pomocą stale rozwijanej aplikacji BCS Manager. Kamery termowizyjne, kamery klasyczne i rejestratory korzystające z zaawansowanej analizy wideo pomogą wykryć każde zagrożenie lub reagować tylko na sytuacje, które takiej reakcji wymagają.



Nie tylko dostarczamy rozwiązania techniczne najwyższej jakości, dbamy również o rozwój osób, które będą z nich korzystać, dlatego prowadzimy cykle szkoleń, na których przybliżamy wszystkie oferowane przez nas produkty.

Tomasz Goljaszewski

Hikvision Polska

Nowe wyzwania dla zapewnienia bezpieczeństwa

Największe wyzwania dla menedżerów bezpieczeństwa infrastruktury krytycznej będą w tym roku związane najprawdopodobniej z rozpoczynającą się przemianą energetyczną kraju, poprawieniem bezpieczeństwa dla procesu produkcji czystej wody oraz z... niestety niedoborami kadrowymi.

Przemiana energetyczna kraju to przede wszystkim nowe inwestycje związane z magazynowaniem, transportowaniem i produkcją energii z gazu oraz z produkcją energii ze źródeł odnawialnych (farmy wiatrowe i fotowoltaiczne). Istotne też będzie poprawienie sprawności istniejących stacji energetycznych i budowa nowych. Wszystkie inwestycje gazowe wymagają dużo bardziej wyrafinowanego podejścia do bezpieczeństwa, dlatego jestem przekonany, że rynek w coraz większym stopniu będzie potrzebował kamer wizyjnych i termowizyjnych z zaawansowaną analizą wizyjną, wspartą technologia *deep learning*. Rozległość tego typu instalacji będzie wymagała łączenie różnych technik, np. techniki radarowej. To samo dotyczy farm fotowoltaicznych ze względu na ich rozległość, duży

koszt i wrażliwość na ewentualną ingerencję osób nieuprawnionych.
Produkcja czystej wody dla dużych miast do niedawna nie była traktowana jako duże wyzwanie dla bezpieczeństwa, bo co mogłaby ukraść lub zniszczyć potencjalnie niebezpieczna osoba w takim obiekcie. Spojrzenie na rodzaje zagrożeń tego typu obiektów na szczęście się zmieniło. To znacząco wpłynie na dobór środków technicznych do ich zabezpieczenia, spodziewamy się z tego powodu sporych inwestycji.
Niedobory kadrowe będą wynikały z dwóch ważnych powodów. Pierwszy – związany ze wzrostem wynagrodzenia minimalnego. Firmy ochrony fizycznej będą musiały w większym stopniu wykorzystać narzędzia techniczne, starając się efektywniej zarządzać kadrą, a może nawet ją redukować.
Drugi powód to wirus SARS-CoV-2, który z całą pewnością będzie miał wpływ na dyspozycyjność osób, które dla zapewnienia bezpieczeństwa infrastruktury krytycznej będą niezbędni. Jednym słowem mniejszą grupą ludzi będzie trzeba zabezpieczyć więcej i lepiej. Więcej operacji będzie wykonywanych zdalnie i w większym stopniu będziemy musieli zaufać inteligencji systemów ochrony technicznej. A to będzie stanowiło również wyzwanie dla takich producentów, jak Hikvision.
I już tak zupełnie na koniec. Najprawdopodobniej w tym roku kamery do wykrywania podwyższonej temperatury ciała staną się powszechne i wielu menedżerów bezpieczeństwa będzie musiało uwzględnić je w swoich procedurach.

Piotr Kiliszek

Niezależny audytor

Operator systemu bezpieczeństwa – potrzebna specjalizacja

Obecnie mamy na rynku bardzo dużą różnorodność kamer, czujników i systemów zabezpieczeń, jednak dostęp do wdrożenia segmentów dedykowanych konkretnym potrzebom jest utrudniony. Menedżerowie bezpieczeństwa chcą rozwiązań w różnych przedziałach cenowych, tak aby ich wdrożenie nie stanowiło obciążenia dla budżetu firmy, co w wielu przypadkach jest czynnikiem blokującym poprawę bezpieczeństwa. Istotne są modularność oraz otwartość proponowanych rozwiązań na pojawiające się zagrożenia.
Drugim elementem jest działanie firm świadczących usługi ochrony. Przez wiele lat traktowania jako zło konieczne branża ochrony została zdeprofesjonalizowana, pozbawiona profesjonalistów. Wpływ na to miało głównie podłoże finansowe, gdyż kierowano się minimalizacją kosztów, przekonaniem zamawiających usługi, że ochrona to zbędny wydatek. Ale to przekonanie okazało się błędne. Współpraca z dobrze działającą firmą ochrony pozwala ograniczyć straty, zachować zdolność do realizacji procesów biznesowych i obniżyć wypadkowość. W przypadku infrastruktury krytycznej konieczne jest wyznaczenie standardów i wymagań minimalnych. W wymogach tych powinno się znaleźć miejsce dla audytu zewnętrznego, który przydzielany byłby losowo. Wykluczyłoby to możliwość wpływania na wynik audytu, a co za tym idzie wskazany poziom bezpieczeństwa musiałby być zrealizowany.

Należy zacząć poważnie podchodzić do „krytyczności" ochranianej infrastruktury. Świetne rozwiązania systemowe powinny być wspierane przez wyspecjalizowane grupy zawodowe, które powinny mieć wskazaną ścieżkę zawodową, możliwości rozwoju, godnych zarobków oraz stabilności zatrudnienia. Jeśli takie podejście do kształcenia kadr znajdzie uznanie w oczach kuratorów oświaty, należy spodziewać się pojawienia klas dających zawód operatora systemów bezpieczeństwa. Byłby to duży krok w kierunku podniesienia poziomu bezpieczeństwa w chronionych obiektach. A wtedy będzie możliwość wykorzystania całego potencjału technologicznego, sztucznej inteligencji, systemów antyfraudowych i szeregu innych rozwiązań.

Wincenty Ignatowski

Niezależny audytor

Zarządzanie kryzysowe

Każda szanująca się organizacja (nie tylko infrastruktura krytyczna), powinna posiadać Plan Zarządzania Kryzysowego i konsekwentnie wprowadzać go za pośrednictwem sztabu kryzysowego. W naszej firmie funkcjonuje Zespół Szybkiego Reagowania *(Rapid Responce Team)*. W jego skład wchodzą osoby z zarządu firmy, dyrektor BHP, menedżer ds. analizy ryzyka, menedżer ds. komunikacji i oczywiście menedżer ds. bezpieczeństwa.
Ponieważ sytuacja i okoliczności związane z pandemią koronawirusa SARS-CoV-2 rozwijają się dynamicznie, Zespół Szybkiego Reagowania (ZSR) musi nie tylko konsekwentnie realizować zapisy Planu Zarządzania Kryzysowego, ale również odpowiednio je modelować w zależności od zmieniających się warunków. Dostosowanie każdego, nawet najlepszego planu jest kluczem do sukcesu, jakim jest dla nas przeprowadzenie naszych współpracowników przez najtrudniejszy okres w czasie trwania groźnej choroby zagrażającej ich zdrowiu i życiu. Gdy firma prowadzi działalność gospodarczą w środowisku międzynarodowym, ten fakt często determinuje realizowanie spójnych działań. Jednym z najważniejszych elementów jest szybkość podejmowania decyzji i wprowadzania ich w życie. W firmie o zasięgu globalnym wypracowane sposoby reagowania na dynamicznie rozwijające się okoliczności związane z epidemią muszą być natychmiast korygowane w zależności od wprowadzanych uregulowań przez rząd Polski lub instytucje związane z ochroną zdrowia. Lokalne prawo ma nadrzędną rolę w procesie zarządzania kryzysowego i musimy je wprowadzać, w pierwszej kolejności informując na bieżąco współpracowników o sposobie działania.
Kluczowym elementem zarządzania kryzysowego jest właściwa i spójna komunikacja, dlatego ważną funkcję pełni tutaj lider ZSR, który m.in.:

- organizuje spotkanie zespołu, podczas którego analizowana jest sytuacja i podejmowane są decyzje,
- prowadzi telekonferencję z osobami zarządzającymi rozproszoną infrastrukturą naszych zakładów produkcyjnych,
- przygotowuje komunikaty do współpracowników,
- przygotowuje i dystrybuuje ulotki nt. radzenia sobie z groźną chorobą.

Jaką rolę pełni w tym procesie menedżer ds. bezpieczeństwa? Przede wszystkim w sytuacji kryzysowej wspólnie z menedżerem ds. analizy ryzyka pełnią funkcję koordynatora i w każdym przypadku odpowiadają za bezpieczeństwo spotkań i całego zespołu, za łączność i utrwalanie za pomocą środków technicznych decyzji podejmowanych przez zespół. Jest też doradcą Działu Komunikacji i dba o właściwą komunikację i wizerunek firmy oraz wspiera aktywności Działu Zarządzania Zasobami Ludzkimi. Ponadto menedżer ds. bezpieczeństwa wspiera zespół i wprowadza zasady i procedury związane z epidemią, mające na celu ograniczenie rozprzestrzeniania się choroby w miejscu pracy. Zapewniamy pracownikom:

- maseczki,
- rękawiczki jednorazowe,
- mydło w płynie,
- ręczniki i chusteczki jednorazowe,
- bezdotykowe urządzenia do dezynfekcji rąk przy wejściu do budynku,
- w miarę możliwości dostarczamy urządzenia do sali konferencyjnej,
- odpowiedni poziom zapasów.

Przygotowujemy materiały dotyczące kampanii komunikacji lokalnej (e-maile, materiały drukowane). Powiadamiamy na bieżąco współpracowników, umieszczając ogłoszenia / plakaty we wszystkich punktach wejścia. Odradzamy pracownikom i gościom, aby nie wchodzili, jeśli mają objawy choroby. Podejmujemy decyzję o pozostawaniu współpracowników w domu w razie niepokojących objawów choroby, dla tych, którzy mają możliwość wykonywania pracy w domu, organizujemy pracę zdalną. Personel recepcji i pracownicy ochrony zostali przeszkoleni i poinstruowani, jak rozpoznawać objawy choroby związane z pandemią.
Oceniamy dostęp i dostępność usług medycznych dla naszych pracowników i wzmacniamy je w razie potrzeby. ZSR musi być przygotowany również na wypadek podejrzenia wejścia osoby z objawami choroby na teren firmy. Wprowadzane są wtedy zasady postępowania polegające m.in. na poinformowaniu miejscowego lekarza, Działu Zarządzania Zasobami Ludzkimi i Zespołu Bezpieczeństwa.
Pracownicy lub kontrahenci o temperaturze ciała powyżej 37,5°C nie będą mogli wejść do obiektu i zostaną poproszeni o pomoc lekarską. Wobec pracownika, u którego stwierdzono objawy choroby w miejscu pracy, należy podjąć ww. działania, jego stanowisko pracy oraz wszelkie miejsca publiczne, w których przebywał, powinny zostać wyczyszczone i zdezynfekowane, a wszelkie z nim kontakty w firmie powinny być ujawniane.
Podsumowując, każda firma musi docenić w kryzysie rolę czynnika ludzkiego, emocjonalnego, kulturowego i organizacyjnego. Zaangażowana musi być cała organizacja (firma) i być skłonna do dzielenia się wiedzą i doświadczeniem z innymi, w tym również z konkurencją.

Mirosław Lukowski

Niezależny audytor

Prewencja misją naszej branży

Jako niezależny ekspert ds. bezpieczeństwa z bagażem doświadczeń w branży RETAIL, z niepokojem obserwuję sytuację, jaka rozwija się dziś w kraju. Security managerowie zawsze walczyli o uznanie przez zarządy swoich firm PREWENCJI jako środka działania koniecznego, ale niewymiernego (niemieszczącego się w plikach Excel).
Analizując działania rządu, nie sposób nie uznać zamknięcia szkół, przedszkoli i uczelni oraz ograniczenia imprez kulturalnych i sportowych za działania słuszne. Można polemizować, czy nie były spóźnione, ale niepodważalne jest, że są słuszne. Wpisują się w szeroko rozumianą prewencję i przeciwdziałania, co jest misją branży security.
Sytuacja jest dynamiczna i naturalną siłą rzeczy powoduje niepokój wśród obywateli, niekiedy graniczący z paniką, co było widać w sklepach. Takie uwarunkowanie rodzi spekulacje, ale jest też motorem napędowym gromadzenia zapasów.
Zbierając wszystkie fakty, mieliśmy obraz IMPREZY MASOWEJ na terenie placówki handlowej, czyli sytuację, której powinniśmy unikać. Działaniami optymalnie skutecznymi są:

1. Ograniczenie liczby klientów na terenie sklepu.
2. Zwiększenie liczby obsadzonych kas, co poprawi płynność.
3. Ze względu na wzmożony ruch w sklepach zaopatrzenie każdego kasjera

w rękawiczki i maseczkę (przy zachowani wymogu stworzenia procedury korzystania i utylizacji zużytych akcesoriów).
4. Ze względu na wzmożony ruch, który przekłada się na zwiększoną liczbę interwencji przeprowadzanych przez pracowników, wyposażenie tej grupy w maseczki i rękawiczki oraz wdrożyć stosowne procedury.
5. Zminimalizowanie obrotu gotówki poprzez przeniesienie płatności na bezgotówkowe (pieniądze stanowią nośnik wszelkiego rodzaju bakterii).
6. Wyposażenie pokoi kontroli w środki dezynfekcyjne, rękawiczki i maseczki.
7. Przeprowadzanie obowiązkowych pomiarów temperatury pracowników przed podjęciem pracy.

Dzięki takim działaniom zapobiegawczym, być może przez niektórych uznanych za zbyt drastyczne, słowo „prewencja" uzyska wymiar ważny, pozwoli ograniczyć rozprzestrzenianie się wirusa i poprawi komfort pracy osób mających każdego dnia kontakt z setkami osób, które w przypływie niepokoju ruszyły szturmować sklepy. Zapominając o bezpieczeństwie swoim i innych.

Jakub Sobek

Linc Polska

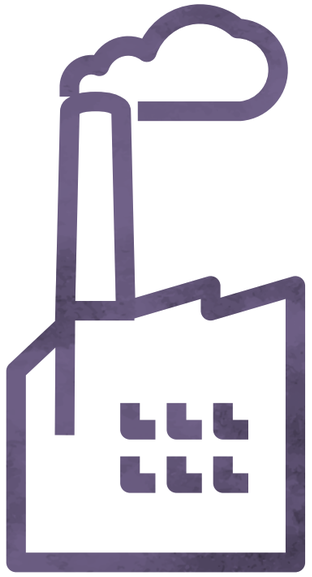
Otwartość warunkiem bezpieczeństwa

Istotą ochrony infrastruktury krytycznej jest zachowanie ciągłości jej funkcjonowania, tak aby żadna próba wtargnięcia lub ataku na obiekt nie zachwiała trwałością świadczonych usług. Uzależnienie obywateli, administracji państwowej i przedsiębiorców od infrastruktury krytycznej rośnie każdego roku. Zatem problemy z jej funkcjonowaniem bardzo szybko wywołałyby straty w wielu różnych sektorach spowodowane np. przestojami w dostawie mediów lub wstrzymaniem produkcji. Dlatego tak istotna jest wiedza i kompetencje nt. potencjalnych zagrożeń oraz prowadzenie stałej oceny ryzyka, pozwalające na zaplanowanie wszystkich możliwych scenariuszy reagowania.

Należy pamiętać, że ochrona obiektów IK to ciągły proces doskonalenia systemu. Wymaga on zaangażowania wielu specjalistów i doradców. Współczesny skuteczny system ochrony musi bowiem składać się z wielu technologicznie zróżnicowanych rozwiązań. Powinna powstać spójna koncepcja ochrony, zależna od szacowanego ryzyka, zakładająca hierarchizację działań i nadanie im odpowiednich priorytetów. Wszelkie podejmowane kroki powinny być jednak proporcjonalne do ewentualnych zagrożeń, ponieważ zawsze trzeba uwzględniać siły i środki, jakie muszą zostać zainwestowane.

Planując system zabezpieczenia technicznego przy tak szybko zmieniających się zagrożeniach, należy szukać rozwiązań otwartych, dających łatwo integrować się z pozostałymi elementami systemu. Decydowanie się na rozwiązania tylko jednego producenta, inwestowanie w zamknięte systemy i autorskie platformy powoduje uzależnienie się od jednego dostawcy. Późniejsze odejście od takiego systemu jest zazwyczaj bardzo kosztowne, a dodanie elementu od innego dostawcy jest często niemożliwe lub wymaga dużych nakładów finansowych.

Wiele osób nadal z pewną rezerwą podchodzi do systemów w chmurze, a okazuje się, że przy ochronie infrastruktury krytycznej mogą być one nieocenionym wsparciem. To właśnie analiza ogromu danych *(big data)* pozwoli już wkrótce z wyprzedzeniem informować osoby odpowiedzialne za ochronę IK o nadchodzących zagrożeniach. Dzięki temu będzie można zareagować w odpowiednim czasie, unikając potencjalnych prób ataków i destabilizacji.



Agnieszka Pitrus

Satel

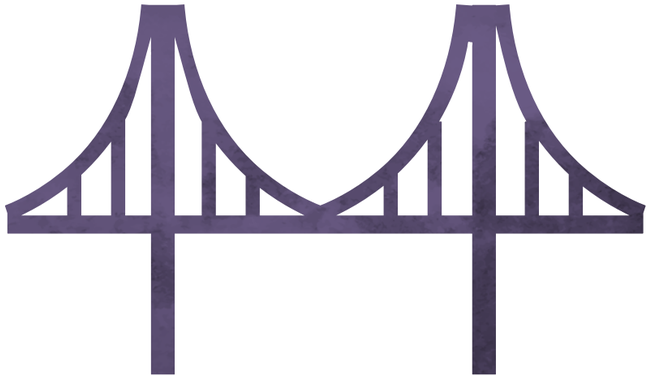
Systemy alarmowe GRADE 3

Do głównych zadań zabezpieczeń technicznych pracujących w budynkach infrastruktury krytycznej – obiektach o wysokim i średnim ryzyku włamania – należy zapewnienie ciągłości ochrony oraz natychmiastowej reakcji na niebezpieczne zdarzenia. Stosowane tam systemy sygnalizacji włamania i napadu powinny skutecznie zapobiegać wtargnięciu intruzów, jednocześnie ograniczając do minimum ryzyko wyrządzenia przez nich potencjalnych szkód. Instalacje te powinny zapewniać wysoki stopień ochrony – spełniać rygorystyczne wymagania stopnia 3 (Grade 3) normy EN 50131. Oznacza to, że do ich neutralizacji lub obejścia potrzebna jest głęboka wiedza na temat budowy i działania zarówno pojedynczych urządzeń, jak i całych tego typu systemów, trzeba także posiadać specjalistyczne narzędzia i umiejętność korzystania z nich.

System alarmowy spełniający wymogi Grade 3 musi posiadać właściwości i funkcje wskazane przepisami. Są to m.in. szyfrowanie danych oraz mechaniczna odporność na czynniki środowiskowe, wandalizm czy sabotaż. Ten ostatni może polegać na próbach demontażu lub unieszkodliwienia poszczególnych elementów systemu (np. zasłonięciu, zaklejeniu taśmą lub zamalowaniu czujek ruchu).

Ponieważ o poziomie zabezpieczenia instalacji stanowi „najsłabsze ogniwo", w jej skład powinny wchodzić wyłącznie urządzenia spełniające wymogi stopnia 3 lub wyższego – począwszy od central alarmowych, przez urządzenia sterujące, moduły rozszerzeń, detektory, sygnalizatory, aż po zasilacze i obudowy. Zgodność z wymogami poświadczają stosowne certyfikaty wydawane przez akredytowane jednostki badawcze.

Z kolei w przypadku, gdy jest wymagana możliwość centralnego zarządzania rozproszonymi instalacjami pracującymi w sieci obiektów, strategicznym rozwiązaniem może okazać się wdrożenie specjalistycznego oprogramowania integrującego. Tego typu rozwiązania informatyczne wspomagają procesy administrowania wieloma systemami SWiN i ich użytkownikami, pozwalając zaoszczędzić czas oraz zoptymalizować związane z tym nakłady finansowe.



Krzysztof Kunecki

Schrack Seconet

Reorganizacja zarządzania bezpieczeństwem pożarowym w dobie koronawirusa

Obiekty zakwalifikowane do infrastruktury krytycznej są kluczowe dla bezpieczeństwa państwa i jego obywateli, dlatego też na etapie tworzenia koncepcji i projektowania wymagają szczegółowego przeanalizowania i zidentyfikowania przede wszystkim krytycznych źródeł zagrożeń, ryzyka ich występowania oraz wpływu na bezpieczeństwo ludzi, mienia i ciągłość działania procesów związanych z funkcjonowaniem organizacji.

W obliczu obecnej sytuacji na świecie związanej z koronawirusem należy szczegółowo przeanalizować organizację zarządzania systemami zabezpieczeń technicznych, aby zapewnić ich ciągłość działania w sytuacji ograniczonego dostępu do obiektu i jego instalacji, czy też ze względu na odizolowanie specjalistów od możliwości lokalnego nadzoru i obsługi urządzeń. Koncentrując się na obszarze zarządzania bezpieczeństwem pożarowym, należy w większym zakresie projektować urządzenia pozwalające na bezpieczny zdalny dostęp do obiektu i jego instalacji.

Należy tu podkreślić rolę systemów integrujących urządzenia przeciwpożarowe (SIUP), ponieważ w stosunku do prostych systemów wizualizacji realizują one zaawansowane funkcje nadzoru, sterowania i zarządzania urządzeniami przeciwpożarowymi i innymi zintegrowanymi z nim urządzeniami czy systemami mającymi wpływ na bezpieczeństwo pożarowe obiektu. SIUP umożliwia zastosowanie oprócz lokalnych stacji operatorskich także stanowiska do zdalnego zarządzania, co powoduje, że istnieje możliwość łatwiejszego przekierowania kompetencji nadzoru i zarządzania poza obiekt do zewnętrznych centrów zarządzania na potrzeby bieżącej eksploatacji, czy też w przypadku ograniczeń związanych z dostępem do obiektu.

Pamiętajmy że system integrujący jako jedyny jest umocowany prawnie do zarządzania ewakuacją ludzi, co jest istotne nie tylko w przypadku wystąpienia pożaru, ale również innych zdarzeń kryzysowych, takich jak np. wyciek toksycznego gazu. Tym, co wyróżnia SIUP, jest możliwość dynamicznego ręcznego przesterowania systemu (zmiana automatycznego scenariusza działania) w odpowiedzi na niekontrolowany rozwój pożaru. W sytuacji zagrożenia system aktywnie wspiera operatora dzięki specjalnym instrukcjom i procedurom postępowania przygotowanym na podstawie instrukcji bezpieczeństwa pożarowego i innych procedur bezpieczeństwa obiektu.

Zastosowanie rozwiązań pozwalających na zdalny nadzór i zarządzanie wymaga zapewniania odpowiednich środków bezpieczeństwa w zakresie ciągłości działania infrastruktury informatycznej (np. redundancja krytycznych tras komunikacyjnych i/lub urządzeń), zastosowania odpowiedniej wielostopniowej autoryzacji dostępu oraz ochrony w zakresie szeroko rozumianego cyberbezpieczeństwa.

Andrzej Sobolewski

Polska Agencja Przemysłowo-Obronna

Uwarunkowania techniczne i organizacyjne bezpieczeństwa infrastruktury państwa

Bezpieczeństwo wewnętrzne państwa uwarunkowane jest przede wszystkim jakością funkcjonowania systemów infrastruktury krytycznej rozumianą jako zapewnienie usług koniecznych dla codziennego życia obywateli, takich jak: zdrowie i ratownictwo, żywność i woda, energia i paliwa, łączność i telekomunikacja, komunikacja i transport, administracja i bankowość. Nie bez znaczenia jest także zapewnienie ciągłości produk-

cji i usług mających wpływ na rozwój kraju i dobrobyt obywateli.
Zapewnienie tych usług wymaga poprawnego działania systemów tej potężnej struktury, na którą składają się obiekty, w tym obiekty kubaturowe i liniowe wraz z urządzeniami i skomplikowanymi instalacjami, za których poprawne funkcjonowanie odpowiada rząd i poszczególni ministrowie. Tak jest w skali makro i taka zasada przenosi się na niższe szczeble zarządzania, aż do podstawowego pracownika obsługi i eksploatacji.
Najsłabszym, a zarazem najważniejszym ogniwem zarzadzania infrastrukturą krytyczną jest człowiek. Każdy człowiek, członek tej struktury ma swoją mentalność, poziom wykształcenia i doświadczenia zawodowego oraz różne nawyki, które nabył w swoim środowisku, jest bardziej lub mniej kreatywny i skłonny do stosowania innowacji. Wszystko to wpływa na jego świadomość, a w konsekwencji na umiejętność przestrzegania warunków technicznych zawartych w uregulowaniach prawnych. Znajduje to odzwierciedlenie w podejściu do przedmiotu i efektów pracy, a tym samym odpowiedzialności za wykonywaną pracę.
Rozwiązaniem tego paradoksu jest tworzenie coraz to doskonalszych organizacyjnych i elektronicznych systemów zabezpieczeń technicznych dla sprawnego funkcjonowania obiektów infrastruktury krytycznej. I tu powstaje pewien istotny problem, a mianowicie budowanie tych systemów wiąże się z działalnością gospodarczą. Powstaje relacja koszt – efekt. Podstawą funkcjonowania każdego obiektu, działania gospodarczego jest jego efektywność ekonomiczna co w praktyce może oznaczać, że efektywniej jest ubezpieczyć np. środki łączności od kradzieży niż tworzyć do tego celu system zabezpieczenia technicznego. Z punktu widzenia zapewnienia bezpieczeństwa obiektom infrastruktury krytycznej jest to najgorsze z możliwych rozwiązań.
W systemach infrastruktury krytycznej podstawę stanowi szybkość przepływu informacji istotnych dla sprawnego jej funkcjonowania. Jednak jest to pewne uproszczenie. Za informacją stoi jej prawdziwość, poprawność i zgodność z intencją nadawcy. Jej ważność, decyzyjność i poprawne zrozumienie przez odbiorcę. Na to nakłada się dodatkowo możliwość jej zakłócenia, zniekształcania, ingerowania w jej treść lub braku możliwości jej nadania czy odbioru. Bardzo ważną sprawą jest ustalenie priorytetów i terminów przekazywanych informacji. Szczególnie jeżeli zjawiska decyzyjne dotyczą wielu różnorodnych obiektów infrastruktury krytycznej, np. komunikacji i łączności czy też transportu i paliw. Mogą tu wystąpić zjawiska interferencji i negatywnego wpływu na inne obiekty całej infrastruktury krytycznej.
Obiekty infrastruktury krytycznej wymagają stałego przepływu informacji o ich stanie – do decydenta, a w konsekwencji, zwrotnie, decyzji dotyczącej ich funkcjonowania. Stan obiektów może być oceniany w różny sposób od badania, oglądu audytorów, poprzez opinie specjalistów do informatycznego systemu włącznie, bazującego na różnorodnych sensorach, informacjach statystycznych, wywiadowniach, informacjach krajowych i zagranicznych, a przede wszystkim sztucznej inteligencji i Internecie.
Bezpieczeństwo obiektów infrastruktury krytycznej wymaga zatem stosowania systemów zabezpieczeń opartych o nowoczesne, wysokiej jakości, wielofunkcjonalne sensory, powielane systemy informatyczne, bezpieczne, szyfrowane i redundantne środki telekomunikacji i łączności, a przede wszystkim ścisłej współpracy wszystkich poziomów zarządzania. Nie mniej istotnym elementem jest pełne i adekwatne do potrzeb zabezpieczenie energetyczne stanowiące podstawę funkcjonowania wszystkich systemów zabezpieczeń technicznych.

Andrzej Żochowski

TNT

Integracja systemów poprawi bezpieczeństwo

Security managerowie w pierwszej kolejności są zobligowani do dokonania oceny potencjalnego ryzyka zakażenia koronawirusem w poszczególnych lokalizacjach firmy, przy jednoczesnym uwzględnieniu specyfiki prowadzonej działalności w różnych obszarach i działach organizacji. Należy przy tym pamiętać, że w sytuacji epidemii jest niezbędna współpraca z przedstawicielami BHP w firmie, tak aby poszczególne działania były spójne i skoordynowane.
W kolejnym etapie należy rozpocząć opracowanie i wdrożenie dodatkowych procedur, np. na poziomie ochrony fizycznej – wewnątrz chronionych obiektów firmy (recepcje, punkty odbioru przesyłek) oraz bram wjazdowych (np. do centrów logistycznych, dystrybucyjnych). Mam na myśli wyposażenie pracowników ochrony w takie środki, jak rękawiczki ochronne, maski skutecznie chroniące drogi oddechowe, środki dezynfekujące dłonie i pomieszczenia.
Należy rozważyć zastosowanie pomiaru temperatury, w szczególności u kierowców, którzy przyjeżdżają z innych krajów Europy i wchodzą na teren naszych obiektów. Jednocześnie organizacja powinna posiadać, a jeżeli nie posiada, to niezwłocznie opracować i wdrożyć tzw. Plany Ciągłości Działania. Pozwolą one na zachowanie ciągłości działania w sytuacji stwierdzenia pierwszych przypadków zainfekowania osób wewnątrz organizacji czy na jej styku w kontakcie z osobami z zewnątrz.
Niezwykle ważne jest także regularne, systemowe podnoszenie świadomości personelu wobec tego zagrożenia oraz metod profilaktycznych dotyczących zapobiegania zakażeniu lub zminimalizowania takiego ryzyka. Jednym z ostatnich elementów będzie utrzymanie wśród pracowników „konsekwentnej dyscypliny" w stosowaniu wdrożonych środków zapobiegawczych. ▫

O Białej Księdze Unii Europejskiej w sprawie sztucznej inteligencji

Do wielu pracowników ochrony fizycznej i pracowników zabezpieczenia technicznego dotarła już zapewne informacja o tym, że 19 lutego 2020 r. Komisja Europejska udostępniła państwom członkowskim – do konsultacji – Białą Księgę dot. sztucznej inteligencji. Konsultacje mają trwać trzy miesiące, do 19 maja br. Potem rozpoczną się prace nad dyrektywą europejską, która określi podstawy i ramy prawne rozwoju technologii sztucznej inteligencji (AI, *Artificial Intelligence*) w krajach członkowskich Unii Europejskiej. Należy oczekiwać, że będą się one toczyć w trybie pilnym (urgent), gdyż drażliwy moralnie dla wielu europejskich pięknoduchów problem bezpiecznego dla ludzi wdrażania i stosowania AI w technice z pewnością nie ominie Europy.

TEKST
Marek Ryszkowski

Zanim przystąpię do przybliżenia myśli zawartych w Białej Księdze Unii Europejskiej w sprawie AI (dalej „BKUEws.AI"), chciałbym przywołać definicję AI, a właściwie kilka spośród wielu definicji, które zostały sformułowane w różnych szkołach informatycznych, od lat zajmujących się tym skomplikowanym zagadnieniem. Pierwsza z przywołanych poniżej pochodzi z Wielkiej Encyklopedii PWN, z jej tomu 26, wydanego w 2005 r. Zatem definicja ta odzwierciedla stan wiedzy o „sztucznej inteligencji", jaki badacze problemu ówcześnie, przed piętnastu laty, posiadali. Oto fragmenty obszernego hasła „sztuczna inteligencja", znajdującego się na stronach 478-479 podanego tomu encyklopedii.

Sztuczna inteligencja (SI), ang. Artificial Intelligence (AI), dziedzina nauki zajmująca się badaniem mechanizmów ludzkiej inteligencji oraz modelowaniem i konstruowaniem systemów, które są w stanie wspomagać lub zastępować inteligentne działanie człowieka. Nazwa dziedziny została zaproponowana w 1956 r. przez J. McCarthy'ego (USA). W nurcie teoretycznym SI łączy zagadnienia z: informatyki, psychologii, antropologii, matematyki, neurofizjologii, elektroniki [i] filozofii; w nurcie doświadczalnym (SI stosowana) jest traktowana jako gałąź informatyki; [...] W ujęciu hist. można wyodrębnić 4 niekoniecznie rozdzielne etapy rozwoju SI: dojrzewania koncepcji (1943 56), wczesnego entuzjazmu (1952-69), dozy realizmu i systemów opartych na wiedzy (1966-79) oraz etap zastosowań SI w przemyśle [...] (od 1980). [...] Od połowy lat 80. XX w. [...] [w] wielu dziedzinach, takich jak gry, wnioskowanie log. i dowodzenie, planowanie oraz diagnozy med., [...] systemy [SI] działają równie dobrze, a nawet lepiej niż człowiek ekspert. Do chwili obecnej [rok 2005] [...] większość sformułowanych definicji SI można podzielić na 4 kategorie, w których system komputerowy może: 1) myśleć jak człowiek, 2) działać jak człowiek, 3) myśleć racjonalnie (wg schematów logiki klas.) oraz 4) działać racjonalnie (co wymaga, chociaż nie we wszystkich sytuacjach, ustalenia celów i wnioskowania log. prowadzącego do ich osiągnięcia) [...].

Tekst zacytowanego hasła opracował Andrzej Wiśniewski. Różne wstawki ujęte w nawiasy kwadratowe są dziełem autora niniejszego artykułu.

Dla ilustracji różnic w sposobie definiowania terminu „sztuczna inteligencja" przytoczę kilka wersji definicji tego terminu, które znajdują się w tekście polskojęzycznym BKUEws.AI. Mam nadzieję, że jest to tłumaczenie profesjonalne, wiernie oddające literę i ducha tekstu angielskiego cytowanej definicji. Oto definicja, która znajduje się na str. 2 Białej Księgi, dokumentu Komisji Europejskiej oznaczonego symbolem unijnym **COM(2020) 65 final.** Wszystkie cytaty z tego dokumentu, który liczy łącznie 30 stron znormalizowanego wydruku komputerowego formatu A4, zapisanych czcionką Calibri 11, opatrzono cudzysłowem.

„Sztuczna inteligencja to zbiór technologii łączących dane, algorytmy i moc obliczeniową. [...]. Ekosystem sztucznej inteligencji może zapewnić korzyści płynące z tej technologii dla całego społeczeństwa i gospodarki:

- ***dla obywateli** – np. lepsza opieka zdrowotna, rzadziej psujący się sprzęt AGD, bezpieczniejsze i czystsze systemy transportu, lepsze usługi publiczne;*
- ***dla rozwoju przedsiębiorstw** – np. nowa generacja produktów i usług w obszarach, w których Europa jest szczególnie silna (sektor maszyn, transportu, cyberbezpieczeństwa [podkr. M.R.], rolnictwa, zielona gospodarka o obiegu zamkniętym, sektor opieki zdrowotnej i sektory o wysokiej wartości dodanej, takie jak moda i turystyka); oraz*
- ***dla usług interesu publicznego** – np. zmniejszenie kosztów świadczenia usług (transport, edukacja, energia i gospodarowanie odpadami), poprawa zrównoważonego charakteru produktów oraz wyposażenie organów egzekwowania prawa w adekwatne narzędzia zapewniające bezpieczeństwo obywateli [podkr. M.R.], przy zachowaniu odpowiednich zabezpieczeń w odniesieniu do ich praw i swobód".*

Inne brzmienie definicji AI ze str. 19 Białej Księgi:

„Termin sztuczna inteligencja odnosi się do systemów, które wykazują inteligentne zachowanie dzięki analizie otoczenia i podejmowaniu działań – do pewnego stopnia autonomicznie – w celu osiągnięcia konkretnych celów. Systemy AI mogą być oparte na oprogramowaniu, działając w świecie wirtualnym (np. asystenci głosowi, oprogramowanie do analizy obrazu, wyszukiwarki, systemy rozpoznawania mowy i twarzy [podkr. M.R.]), lub mogą być wbudowane w urządzenia (np. zaawansowa-

ne roboty, samochody autonomiczne, drony lub aplikacje Internetu Rzeczy)”.

Na 19 stronie BKUEws.AI znajduje się także poniższy tekst uzupełniający przytoczoną wyżej definicję terminu AI: „*Systemy sztucznej inteligencji (AI) to oprogramowanie (i ewentualnie również sprzęt komputerowy – ang. hardware) zaprojektowane przez człowieka, które – aby osiągnąć złożony cel – działają w wymiarze fizycznym lub cyfrowym, postrzegając swoje środowisko poprzez pozyskiwanie danych, interpretując zgromadzone dane (ustrukturyzowane lub nie), wyciągając wnioski na podstawie tych danych lub przetwarzając informacje, których źródłem są te dane, oraz podejmując decyzje w sprawie najlepszych działań, jakie należy podjąć, aby zrealizować dany cel. Systemy sztucznej inteligencji mogą wykorzystywać zasady symboliczne albo uczyć się na podstawie modelu numerycznego i mogą również dostosować swoje zachowanie poprzez analizę wpływu ich wcześniejszych działań na środowisko”.* Uważny czytelnik zauważy niewątpliwie w tekście ww. Białej Księgi jeszcze inne definicje terminu AI i teksty je uzupełniające.

W BKUEws.AI zaproponowano warianty strategiczne, umożliwiające bezpieczny rozwój godnej zaufania sztucznej inteligencji w Europie, przy pełnym poszanowaniu wartości i praw obywateli państw zrzeszonych w UE. Głównymi elementami Białej Księgi są:

- „Ramy polityczne określające środki służące połączeniu wysiłków na szczeblu europejskim, krajowym i regionalnym. Dzięki partnerstwu sektora publicznego i prywatnego ramy te powinny zmobilizować zasoby w celu osiągnięcia ekosystemu doskonałości wzdłuż całego łańcucha wartości, począwszy od badań naukowych i innowacji, a także stworzyć odpowiednie zachęty do przyspieszenia przyjmowania rozwiązań opartych na sztucznej inteligencji, w tym przez małe i średnie przedsiębiorstwa (MŚP).

- Kluczowe elementy przyszłych ram regulacyjnych dotyczących sztucznej inteligencji w Europie, które stworzą wyjątkowy ekosystem zaufania. W tym celu muszą one zapewniać poszanowanie przepisów UE, w tym przepisów służących ochronie praw podstawowych i praw konsumentów, w szczególności w odniesieniu do wykorzystywanych w UE systemów AI, charakteryzujących się wysokim ryzykiem. Budowanie ekosystemu zaufania jest celem politycznym samym w sobie i powinno zachęcać obywateli do stosowania sztucznej inteligencji oraz oferować przedsiębiorstwom i organizacjom publicznym pewność prawa umożliwiającą innowacyjność z wykorzystaniem AI. Komisja zdecydowanie popiera podejście, w którego centrum jest człowiek i które będzie opierać się na komunikacie w sprawie budowania zaufania do sztucznej inteligencji ukierunkowanej na człowieka. Komisja uwzględni również wkład uzyskany w fazie pilotażowej prac nad wytycznymi dotyczącymi etyki, przygotowanymi przez grupę ekspertów wysokiego szczebla ds. sztucznej inteligencji”.

Europejska strategia w zakresie danych proponowana w Białej Księdze ma na celu umożliwić Europie szybkie osiągnięcie statusu najbardziej atrakcyjnej, bezpiecznej i dynamicznej gospodarki, która sprawnie wykorzystuje dane, wyposażając Europę w wiedzę umożliwiającą podejmowanie lepszych decyzji, co niewątpliwie poprawi życie obywateli państw członkowskich UE. W strategii tej określono szereg środków z zakresu polityki, m.in. mobilizację inwestycji prywatnych i publicznych niezbędnych do osiągnięcia tego celu. Wpływ sztucznej inteligencji, Internetu Rzeczy i innych technologii cyfrowych na przepisy dotyczące bezpieczeństwa i odpowiedzialności został przeanalizowany w Sprawozdaniu Komisji towarzyszącym Białej Księdze *(ramka na s. 18 księgi)*.

Pracowników branży bezpieczeństwa i ochrony (ang. *safety & security*) zainteresuje niewątpliwie to, co w BKUEws.AI napisano w sprawie stosowania biometrycznych urządzeń i systemów identyfikowania osób, szeroko wykorzystywanych już od lat przez przedsiębiorstwa tej branży. Oto niektóre z tych zapisów:

- „Dane biometryczne definiuje się jako dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczne uwierzytelnienie lub identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne.

- W odniesieniu do rozpoznawania twarzy identyfikacja oznacza, że wzór obrazu twarzy danej osoby jest porównywany z wieloma innymi wzorami przechowywanymi w bazie danych w celu stwierdzenia, czy obraz twarzy tej osoby jest przechowywany w tej bazie danych. Uwierzytelnienie (lub weryfikacja) natomiast często odnosi się do porównania „jeden do jednego”. Umożliwia ono porównanie dwóch wzorców biometrycznych, co do których zasadniczo zakłada się, że należą do tej samej osoby. Dwa wzorce biometryczne są porównywane w celu określenia, czy osoba wskazana na dwóch obrazach jest tą samą osobą. Taka procedura jest np. stosowana w bramkach zautomatyzowanej kontroli granicznej wykorzystywanych do odprawy granicznej w portach lotniczych.

- Na przykład w odniesieniu do godności ludzkiej, jeśli chodzi o korzystanie z technologii rozpoznawania twarzy, prawo do poszanowania życia prywatnego i ochrony danych osobowych jest ważnym elementem kwestii związanych z prawami podstawowymi. Występuje również potencjalny wpływ związany z brakiem dyskryminacji i prawami grup specjalnych, takich jak dzieci, osoby starsze i osoby z niepełnosprawnościami. Ponadto stosowanie tej technologii nie może ograniczać wolności słowa, zrzeszania się i zgromadzeń”. [Zob.: *Facial recognition technology: fundamental rights considerations in the context of law enforcement* (Technologia rozpoznawania twarzy: kwestie związane z prawami podstawowymi w kontekście egzekwowania prawa, https://fra.europa.eu/en/publication/2019/facial-recognition)]

Regulacje europejskie w sprawie ochrony danych biometrycznych znajdują się także w art. 9 RODO, art. 10 dyrektywy w sprawie egzekwowania prawa, a także w art. 10 rozporządzenia (UE) 2018/1725 (mającego zastosowanie do instytucji i organów UE), które znajdują się także w Polsce.
W BKUEws.AI zaznaczono obawy związane głównie z gwałtownym i niekontrolowanym prawnie rozpowszechnianiem się AI w krajach unijnych. (cyt.): *„Sztuczna inteligencja może przynieść wiele korzyści, w tym poprzez zwiększenie bezpieczeństwa produktów i procesów, może ona również wyrządzić szkody. Szkody te mogą być zarówno materialne (dla bezpieczeństwa i zdrowia osób, w tym utrata życia, szkody rzeczowe), jak i niematerialne (utrata prywatności, ograniczenie prawa do wolności słowa, naruszenie godności ludzkiej, dyskryminacja związana np. z dostępem do zatrudnienia) i mogą wiązać się z wieloma różnymi rodzajami ryzyka. Ramy regulacyjne powinny koncentrować się na tym, jak zminimalizować różne rodzaje ryzyka związane z potencjalnymi szkodami, zwłaszcza najpoważniejszymi. Główne zagrożenia związane z AI dotyczą stosowania przepisów mających na celu ochronę praw podstawowych (w tym przepisów dotyczących ochrony danych osobowych i prywatności oraz niedyskryminacji), a także kwestii związanych z bezpieczeństwem i odpowiedzialnością. [...] Zagrożenia te mogą być wynikiem wadliwego opracowania systemów sztucznej inteligencji (w tym w odniesieniu do nadzoru przez człowieka) lub wykorzystywania danych bez korygowania możliwych uprzedzeń (np. system jest szkolony z wykorzystaniem wyłącznie lub*

głównie danych pochodzących od mężczyzn, co może prowadzić do nieoptymalnych wyników w odniesieniu do kobiet)".

Temat zagrożeń jest kontynuowany w BKUEws.AI następująco:

„Sztuczna inteligencja może pełnić wiele funkcji, które wcześniej mogły być wykonywane wyłącznie przez człowieka [podkr. M.R.]. W związku z tym obywatele i osoby prawne będą w coraz większym stopniu podlegać działaniom i decyzjom podejmowanym przez systemy sztucznej inteligencji lub z ich pomocą, które czasami mogą być trudne do zrozumienia i od których może być się trudno odwołać w razie potrzeby. Ponadto sztuczna inteligencja zwiększa możliwość śledzenia i analizowania codziennych poczynań ludzi [podkr. M.R.]. Na przykład istnieje potencjalne ryzyko, że sztuczna inteligencja może być wykorzystywana – z naruszeniem unijnych przepisów dotyczących ochrony danych i innych – przez organy państwowe lub inne podmioty prowadzące masowy nadzór oraz przez pracodawców obserwujących zachowanie pracowników.

Poprzez dokonywanie analizy dużych ilości danych i identyfikację powiązań między nimi sztuczna inteligencja może być również wykorzystywana do znajdowania źródeł pochodzenia danych i deanonimizacji danych dotyczących osób, co stwarza nowe zagrożenie dla ochrony danych osobowych, nawet w odniesieniu do zbiorów danych, które same w sobie nie obejmują danych osobowych. Sztuczna inteligencja jest również wykorzystywana przez pośredników internetowych do priorytetowego traktowania informacji dla swoich użytkowników i moderacji treści. Przetwarzane dane, projekt aplikacji i możliwość interwencji człowieka mogą mieć wpływ na prawo do wolności słowa, ochrony danych osobowych, prywatności i swobód politycznych".

Dalej o zagrożeniach powodowanych przez AI w omawianej księdze napisano:

„Szczególne cechy technologii sztucznej inteligencji, w tym nieprzejrzystość (efekt czarnej skrzynki), złożoność, nieprzewidywalność i częściowo samodzielne działanie mogą utrudniać weryfikację zgodności oraz egzekwowanie istniejących przepisów UE służących ochronie praw podstawowych. Organy egzekwowania prawa i zainteresowane osoby mogą nie mieć możliwości sprawdzenia, w jaki sposób dana decyzja, w którą zaangażowana była AI, została podjęta, a zatem czy obowiązujące przepisy były przestrzegane. Osoby fizyczne i prawne mogą mieć trudności z faktycznym dostępem do wymiaru sprawiedliwości w sytuacjach, w których takie decyzje mogą mieć na nie negatywny wpływ".

BKUEws.AI i trzymiesięczne konsultacje w sprawie europejskich problemów z AI są, a przyszła dyrektywa europejska w sprawie AI (przede wszystkim) będzie próbą wprowadzenia do zasobu przepisów prawnych UE regulacji, które ograniczą, a być może usuną wspomniane wyżej obawy przed AI, albo może chociaż ograniczą je do minimum.

Komisja Europejska jest zdania, że można ulepszyć europejskie ramy legislacyjne, aby uwzględnić następujące zagrożenia i sytuacje:

- **Skuteczne stosowanie i egzekwowanie obowiązujących przepisów unijnych i krajowych:** najważniejsze cechy sztucznej inteligencji stanowią wyzwanie dla zapewnienia właściwego stosowania i egzekwowania przepisów unijnych i krajowych. Brak przejrzystości AI sprawia, że trudno jest określić i udowodnić ewentualne naruszenia prawa, w tym przepisów, które chronią prawa podstawowe, przypisują odpowiedzialność i określają warunki konieczne do dochodzenia odszkodowania. W związku z tym, aby zapewnić skuteczne stosowanie i egzekwowanie przepisów, konieczne może być dostosowanie lub doprecyzowanie obowiązujących przepisów w niektórych obszarach, np. w odniesieniu do odpowiedzialności, jak szczegółowo opisano w sprawozdaniu towarzyszącym niniejszej Białej Księdze.
- **Zmieniająca się funkcjonalność systemów sztucznej inteligencji:** włączenie oprogramowania, w tym sztucznej inteligencji, do produktów może zmienić funkcjonowanie takich produktów i systemów w trakcie ich cyklu życia. Dotyczy to w szczególności systemów, które wymagają częstych aktualizacji oprogramowania lub opierają się na uczeniu maszynowym. Cechy te mogą wiązać się z nowymi zagrożeniami, które nie występowały w momencie wprowadzenia systemu na rynek. Zagrożenia te nie są odpowiednio uwzględnione w obowiązującym prawodawstwie, które koncentruje się głównie na ryzyku związanym z bezpieczeństwem produktów w momencie wprowadzania ich do obrotu.
- **Zmiany pojęcia bezpieczeństwa:** wykorzystywanie sztucznej inteligencji w produktach i usługach może stwarzać zagrożenia, które obecnie nie są przedmiotem przepisów UE. Zagrożenia te mogą dotyczyć cyberbezpieczeństwa, bezpieczeństwa osobistego (np. w związku z nowymi zastosowaniami sztucznej inteligencji, takimi jak w urządzeniach gospodarstwa domowego), utraty łączności itd. Zagrożenia te mogą występować w momencie wprowadzania produktów do obrotu lub powstawać w wyniku aktualizacji oprogramowania lub uczenia się maszyn w trakcie stosowania produktu. UE powinna w pełni wykorzystać dostępne jej narzędzia, aby zwiększyć bazę dowodową na temat potencjalnych zagrożeń związanych z zastosowaniami AI, w tym wykorzystać doświadczenia Agencji UE ds. Cyberbezpieczeństwa (ENISA) do oceny krajobrazu zagrożeń związanych ze sztuczną inteligencją..

W Białej Księdze poinformowano: *„Kilka tylko państw członkowskich UE analizuje już możliwości związane z prawodawstwem krajowym, w celu sprostania wyzwaniom stwarzanym przez AI. Zwiększa to ryzyko rozdrobnienia jednolitego rynku europejskiego."*

Rozbieżne przepisy krajowe mogą stwarzać przeszkody dla przedsiębiorstw, które chcą sprzedawać i eksploatować systemy AI na europejskim jednolitym rynku. Zapewnienie wspólnego podejścia na szczeblu UE przyniosłoby europejskim przedsiębiorstwom korzyści wynikające ze sprawnego dostępu do tego jednolitego rynku i zwiększyłoby ich konkurencyjność na rynkach światowych. Zamieszczając tę uwagę w BKUEws.AI, Komisja Europejska zachęca wszystkie kraje członkowskie, zwłaszcza te, które dotychczas mało interesował problem AI, do udziału w analizowaniu i dostosowywaniu prawa krajowego do wymagań przyszłego prawa unijnego. □

BIO

Marek Ryszkowski

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

KAMERY w (NIE)BEZPIECZEŃSTWIE!

BEZPIECZEŃSTWO, OCHRONA DANYCH, KWESTIE PRZEJĘCIA DOSTĘPU DO URZĄDZEŃ TO DZISIAJ TEMATY ŻYWO INTERESUJĄCE ZARÓWNO OSOBY CHCĄCE ZDOBYĆ NASZE DANE, JAK I FIRMY OFERUJĄCE WSZELKIEJ MAŚCI ZABEZPIECZENIA. NA CO ZATEM ZWRACAĆ UWAGĘ W FAZIE PROJEKTOWANIA SYSTEMU WIZYJNEGO I CO NALEŻY SPRAWDZIĆ W DZIAŁAJĄCYM SYSTEMIE WIZYJNYM, ABY ZMINIMALIZOWAĆ RYZYKO NIEUPRAWNIONEGO DOSTĘPU?

TEKST
Michał Marciniak

Większość systemów telewizji dozorowej IP składa się z podobnych komponentów, jednakże skala rozwiązania może wymuszać zastosowanie odmiennego podejścia, a co za tym idzie będzie wymagać indywidualnej oceny praktycznie w każdym przypadku. Są jednak pewne cechy wspólne, które można wskazać jako „pierwszą linię" w trakcie weryfikacji poszczególnych elementów.

Kamery IP/rejestrator

Rdzeniem każdego systemu wizyjnego są oczywiście kamery. Obecne systemy stawiają wysokie wymagania dotyczące zabezpieczenia tych urządzeń, gdyż nie każdy zdaje sobie sprawę z tego, iż obecna moc obliczeniowa tych urządzeń dorównuje niekiedy mocy przeciętnych komputerów PC na naszych biurkach (niektóre z nich są nawet wyposażone w procesory graficzne – GPU – wspomagające procesy inteligentnej analizy obrazu). Kluczową kwestią jest dostęp do samej kamery – stosowanie domyślnych haseł jest niedopuszczalne, jedyną opcją jest hasło niezwiązane z innymi usługami lub systemami w danej sieci. Powiązaną czynnością powinno być dodanie użytkowników, którzy będą korzystali z systemu. Użytkownik „admin" stosowany jako autoryzacja u wszystkich operatorów może doprowadzić do przejęcia hasła i tym samym w prosty sposób uzyskania dostępu do danych.
Powinno się również wyłączyć wszelkie nieużywane serwisy (np. SSH, Telnet, SNMP, UPNP), jeśli nie planujemy z nich korzystać w przyszłości. Idąc dalej, można skorzystać z listy wykluczeń adresów IP i zawęzić dostęp do kamery tylko dla rejestratora i np. administratora. Dodatkową kwestią są certyfikaty HTTPS zwiększające bezpieczeństwo podczas korzystania z menu kamery, jednakże konfiguracja jest dość pracochłonna (generowanie i dodawanie certyfikatów), a korzyści (szczególnie w rozwiązaniach na bazie sieci lokalnej LAN) niewspółmierne do pracy, jaką należy w to włożyć.
Dobrą praktyką jest zmiana domyślnych portów HTTP/UDP/TCP/RTSP na niestandardowe, co wprawdzie nie wykluczy niebezpieczeństwa próby włamania, ale ograniczy próby skanowania przez niepowołane osoby po znanych portach (*well known port*).
Ostatnim ważnym obszarem do weryfikacji (często pomijanym ze względu na wysoki poziom zaufania do lokalizacji, w jakiej instalowane są kamery) jest bezpieczeństwo fizyczne. Na ten temat napisano już bardzo dużo (np. cykl artykułów opublikowanych w A&S dotyczących ochrony perymetrycznej obiektów infrastruktury krytycznej), jednakże za każdym razem problem wraca jak bumerang z powodu licznych błędów po stronie wszystkich uczestników projektu: projektanta i dostawcy sprzętu, instalatora, podmiotu zlecającego i odbierającego rozwiązanie.

Kluczowym elementem jest wizja lokalna i skrupulatna analiza potrzeb (i możliwości) klienta. Wskazanie odpowiednich punktów montażu zarówno kamer, jak i rejestratora często wymusza kompromis pomiędzy ograniczonymi środkami finansowymi, limitami nałożonymi przez rozkład pomieszczeń w budynku i otoczeniu, ale nierzadko też kwestiami estetycznymi i wizualnymi (na które nie wyraża zgody architekt lub klient). Znalezienie wspólnego mianownika wymaga ścisłej kooperacji pomiędzy wszystkimi stronami – tylko takie podejście gwarantuje profesjonalne i rzetelne wdrożenie bezpiecznego rozwiązania.

Sieć LAN/WAN

Nie każdy ma bezpośredni dostęp do tego poziomu, gdyż najczęściej switche/routery znajdują się w serwerowni, która powinna być dostępna tylko dla wskazanych osób. Jest jednak kilka kwestii, które warto poruszyć w aspekcie ruchu sieciowego dotyczącego systemów wizyjnych. W przeciwieństwie do standardowego przepływu pakietów pomiędzy komputerem PC a serwerem, najczęściej odbywającego się z określoną częstotliwością, strumień danych z kamery płynie praktycznie nieustannie do miejsca przeznaczenia (rejestrator). Powoduje to naturalnie zwiększone zapotrzebowanie na pasmo sieciowe, co z pewnością musi zostać uwzględnione na etapie projektowania systemu, wraz z założeniem marginesu na ewentualną rozbudowę o kolejne sekcje.
Z punktu widzenia bezpieczeństwa urządzenia sieciowe również należy chronić przed niepowołanym dostępem od strony konfiguracyjnej (każdy switch zarządzalny lub router ma mniej lub bardziej bogate menu, umożliwiające zmianę różnych parametrów portów i wielu innych ustawień).
Jednym z sugerowanych zaleceń jest oddzielenie sieci firmowej od sieci dla ruchu wizyjnego – daje to ogrom korzyści z wielu powodów:

- fizyczne oddzielenie na poziomie osobnych urządzeń gwarantuje możliwość zastosowania dedykowanych switchy PoE pracujących (i testowanych) w warunkach ciągłego przepływu danych związanych z ruchem w sieci monitoringu,
- wydzielenie portów VLAN tylko dla kamer lub rejestratorów w istniejącej infrastrukturze spowoduje rozdzielenie obu środowisk, jednakże ta forma wymaga większej wiedzy, uwagi, nadzoru (i poprawnej dokumentacji) ze strony specjalisty od spraw sieciowych, gdyż działamy na tym samym urządzeniu, na którym odbywa się firmowy przepływ danych.

Bardziej dogłębnym zabezpieczeniem, z którym współpracuje spora część kamer, jest protokół 802.1x. Dzięki niemu do portu sieciowego switcha jest w stanie podłączyć się tylko uwierzytelnione urządzenie, co minimalizuje problemy związane z nieautoryzowanym dostępem poprzez inne niż firmowe (autoryzowane) komponenty.
To nie koniec niespodzianek, z jakimi przyjdzie nam się zmierzyć w kwestii spraw sieciowych. Zataczając szerszy krąg – wychodzimy poza obszar naszej firmy i np. z hotelowego zacisza planujemy sprawdzić aktualny stan produkcji dzięki zainstalowanym tam kamerom. Obecny trend bezpieczeństwa wymusza coraz częściej stosowanie połączeń VPN (minimum L2TP, a najlepiej SSL VPN do pracy z danymi lokalnymi (serwer plików, połączenia Remote Desktop itd.). Dlaczego zatem nie stosować tego połączenia również do przeglądania danych z kamer/rejestratora? Należy pamiętać, że na rynku jest niewiele narzędzi szyfrujących całą ścieżkę przepływu (od kamery/rejestratora do zdalnego klienta) –

mało jeszcze popularne rozwiązania powoli wchodzą na rynek, np. Axis/Genetec Secure Real-time Protocol (SRTP), ale cena i niska dostępność ograniczają jeszcze te propozycje. Połączenie VPN daje nam pewne i szybkie rozwiązanie, niwelując tym samym skutki wpuszczania nieszyfrowanego ruchu wizyjnego bezpośrednio do Internetu.
Istotnym elementem, jaki należy mieć na uwadze, jest utrzymywanie aktualnych wersji oprogramowania (firmware) środowiska sprzętowego – dotyczy to wszystkich urządzeń, gdyż podatności na wszelkiego rodzaju *malware* dotykają każdy system informatyczny.

Pamięć – bezpieczne miejsce na dane

Wiele rozwiązań opartych na platformach rejestratorów stacjonarnych (NVR/DVR) nie zapewnia pożądanego poziomu zabezpieczenia zarejestrowanych danych z bardzo prostego powodu – są one nieszyfrowane. Składowane dane zawierające nagrania z kamer można najczęściej łatwo przenieść do innego rejestratora lub odzyskać bezpośrednio z podłączonego dysku twardego do komputera za pomocą odpowiedniego oprogramowania.
Dzisiejsze standardy zalecają szyfrowanie dysków w komputerach lub serwerach, co minimalizuje ryzyko przejęcia, a tym samym odczytu danych, ponieważ dane z rejestratorów są często wrażliwe (np. dane biometryczne) lub mogą stanowić łakomy kąsek dla potencjalnej konkurencji (procesy produkcyjne). Użytkownicy tych urządzeń muszą postawić dzisiaj na fizyczną ochronę, gdyż wymogi stawiane procesowi szyfrowania opierają się najczęściej na wykorzystaniu procesora głównego (lub dedykowanego), który obecnie skupia się wyłącznie na procesach związanych z analizą i przetwarzaniem obrazu. Najbliższy czas zmusi wiodących producentów do zweryfikowania swojej oferty i począwszy od topowych modeli oferujących wielodyskowe rejestratory, aż po najprostsze urządzenia jednodyskowe cała gama otrzyma dedykowaną opcję szyfrowania sprzętowego, podnoszącą bezpieczeństwo na nowy poziom.
Obecnie powyższą niedogodność można rozwiązać na kilka sposobów – z pewnością bardziej kosztownych niż prosty NVR, jednak gdy w grę wchodzi bezpieczeństwo danych i ochrona przed konkurencją, koszty schodzą na drugi plan. Można zastosować:

- Dedykowane platformy NAS wraz z wbudowanym oprogramowaniem do rejestracji obrazu z kamer (np. Qnap – QVR Pro, Synology – *Surveillance Station*, Asustor – *Surveillance Center*) - wszystkie te urządzenia z powodzeniem zastąpią dedykowany rejestrator (NVR), dając w zamian nadmiarowość dyskową (RAID), szyfrowanie dysków (AES), szerokie portfolio obsługiwanych kamer itd.
- Programowanie dedykowanie (VMS –*Video Management Software*) do zarządzania i rejestrowania środowiskiem wizyjnym, instalowane na serwerach (najczęściej bazujących na Windows Server). To podejście gwarantuje wykorzystanie narzędzi szyfrujących, oferowanych przez Microsoft (Bitlocker) lub dostawców firm trzecich (np. VeraCrypt). Część producentów oprogramowania VMS oferuje rozwiązania zwiększające bezpieczeństwo własnych archiwów, np. Axxon Next ma dedykowany system plików SolidStore oferujący dostęp tylko dla konkretnej instancji/użytkownika.

Czy to już wszystko?

Z pewnością nie. Proces zabezpieczania danych i środowiska to niekończąca się „walka" z wieloma nowymi zagrożeniami. Przedstawione w artykule zalecenia to tylko czubek góry lodowej, jednak często może to być dobry początek na uświadomienie sobie, iż nie stanowimy zamkniętej enklawy, do której nikt nie ma wstępu. Z pewnością zachowanie rozsądku i niepopadanie w paranoję będzie bardzo wskazane (monitoring wizyjny sklepu osiedlowego nie wymaga stosowania sieciowych urządzeń ochronnych klasy UTM lub szyfrowania dysków), jednak każdorazowa weryfikacja posiadanego (bądź planowanego) systemu dozoru wizyjnego będzie wiązała się ze ścisłą współpracą wielu działów i ludzi.
Zlecenie tego tylko działowi IT spowoduje skupienie uwagi wyłącznie na kwestiach technicznych. Dział Security może wnieść wiele w obszarze ogólnego bezpieczeństwa, ale pominie detale konfiguracji i zarządzania sprzętem. Wiele cennych informacji związanych z potencjalnymi zagrożeniami są w stanie dostarczyć kierownicy/managerowie zespołów na co dzień borykający się z problemami lub zagrożeniami. Wszystko to stanowi materiał do dyskusji i podejmowania decyzji nt. bezpieczeństwa i zagrożeń (w kontekście rozwiązań CCTV) z dystrybutorem i instalatorem.

Jednakże najważniejszym czynnikiem jest ciągła praca nad właściwymi zachowaniami osób, które mają kontakt z systemem wizyjnym – zarówno operatorów, jak i osób nadzorowanych. Czynnik ludzki (niestety jak zwykle) stanowi najsłabsze ogniwo w całym procesie i może doprowadzić do przejęcia istotnych danych pomimo stosowania rygorystycznych norm i obostrzeń. Edukacja, spotkania, szkolenia stanowią klucz do zachowania wysokiego stopnia świadomości każdego pracownika nie tylko w kwestii systemów wizyjnych, ale również wszystkich innych krytycznych rozwiązań istotnych dla firmy. □

BIO

Michał Marciniak

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

Kamera termowizyjna – wojskowa technologia w zastosowaniu cywilnym

Kamery termowizyjne mogą być użyte do różnych zastosowań, m.in. działań związanych z wykrywaniem i gaszeniem pożaru (szybka lokalizacja źródła pożaru), poszukiwawczych (obraz termiczny człowieka pomaga w określeniu jego położenia, np. pod zaspami śniegu) czy do oceny stanu zdrowia poprzez pomiar temperatury ciała zarówno ludzi, jak i zwierząt.

Możliwości zastosowania kamer termowizyjnych jest wiele. Pojawienie się pandemii koronawirusa (SARS-CoV-2) zaskoczyło nas, społeczeństwa nie były gotowe na tego rodzaju wyzwania. Teraz staje się oczywiste, że rozwiązanie problemu wymaga zintegrowanego podejścia oraz kolosalnej odpowiedzialności ze strony państw, obywateli i biznesu. W związku z tym postanowiliśmy wnieść swój wkład, co zaowocowało opracowaniem przez nas nowatorskiego rozwiązania w sektorze zabezpieczeń – mówi Maksym Dzherikhov, prezes Zarządu Secur Global.

Kamera termowizyjna Tecsar IPCT-PANDEMIC a koronawirus (SARS-CoV-2)

Nikt nie spodziewał się, że koronawirus zaledwie po kilku tygodniach, w czasie których pandemia rozwijała się na terenie Chin, trafi do Europy, a w końcu także do Polski. Szybko stało się jasne, że aby zapobiec rozprzestrzenianiu się choroby, trzeba podjąć nadzwyczajne działania przy wykorzystaniu wszelkich dostępnych metod. Idealnym rozwiązaniem okazało się zastosowanie kamer termowizyjnych w celu wykrywania pierwszych objawów COVID-19. Jak to możliwe?

Jednym z głównych objawów zarażenia się chorobą COVID-19 wywołaną przez koronawirusa (SARS-CoV-2) jest gorączka powyżej 38 C. Zadaniem kamery termowizyjnej Tecsar IPCT-PANDEMIC jest obrazowanie promieniowania podczerwonego emitowanego przez dany obiekt. Dzięki połączeniu rozdzielczości obrazu 400 x 300 pikseli z odpowiednią kalibracją termicznego modelu ciała czarnego uzyskuje się bardzo szczegółowy odczyt temperatury ciała osoby znajdującej się w jej zasięgu.

Ta metoda już została zaimplementowana na największym międzynarodowym i krajowym lotnisku na Ukrainie – Kijów-Boryspol. Miejscowe władze podjęły decyzję o wykorzystaniu technologii termowizyjnej do wykrywania wczesnych oznak koronawirusa (SARS-CoV-2) u osób podróżujących między krajami. Technologia ta sprawdzi się też na przejściach granicznych, przyczyniając się do zatrzymania wzrostu przypadków zakażenia, jednocześnie przyspieszając kontrolę przepływu ruchu na granicach państw.

Odpowiednia selekcja osób, u których podejrzewa się wystąpienie pierwszych oznak choroby COVID-19, odbywa się za pomocą ustawienia skali temperatury, którą kamera będzie uwzględniać w czasie monitorowania na obszarze od 3 do 5 m. Dzięki możliwości badania do 16 osób jednocześnie, z czasem pomiaru wynoszącym zaledwie 30 s, można w znacznym stopniu zwiększyć przepustowość podczas kontroli na granicach państw.

Kamery termowizyjne dają wiarygodne źródło informacji do prowadzenia właściwych działań w walce z koronawirusem (SARS-CoV-2). Dzięki temu służby bezpieczeństwa mogą reagować znacznie szybciej i podejmować właściwe decyzje mające na celu zminimalizowanie rozprzestrzeniania się pandemii. W przypadku działań na tak szeroką skalę rozwój technologii związanych z termowizją jest znaczącym i dość istotnym krokiem wpływającym na skuteczność prowadzonych działań. □

Infrastruktura sieciowa pod systemy monitoringu wizyjnego

Planując inwestycję w systemy zabezpieczeń, dużą wagę przywiązujemy do wyboru kamer, systemu przeciwpożarowego czy też kontroli dostępu, pomijając przy tym infrastrukturę IT. To częsty błąd. Choć na pozór jej nie widać, infrastruktura sieciowa jest tym elementem systemów zabezpieczeń, który je łączy. Jest zatem elementem niezwykle ważnym do poprawnego i bezawaryjnego ich działania. Dotyczy to m.in. systemów dozoru wizyjnego (VSS/CCTV) – zarówno kamer IP, jak i urządzeń do rejestracji obrazu oraz komputerów przeznaczonych do ich obsługi.

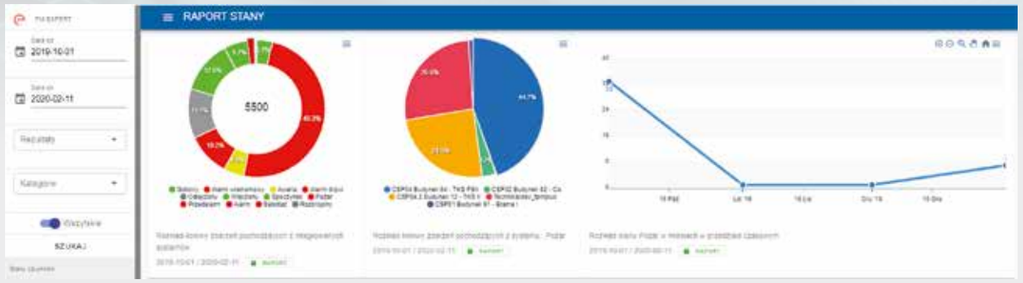
Systemy zabezpieczeń są w dużej mierze oparte na komunikacji IP. Warto dopasować infrastrukturę sieciową i dobrać optymalne rozwiązanie już na etapie projektowania, w momencie gdy znamy wszystkie systemy zabezpieczeń, które będą instalowane w obiekcie. Pozwala to zaplanować zarówno rozmieszczenie punktów dystrybucyjnych, jak i wymagane funkcjonalności zaimplementowanych w nich przełączników.

TP-Link posiada szerokie portfolio przełączników z zasilaniem PoE/PoE+, które świetnie sprawdzą się jako infrastruktura pod systemy monitoringu. W ofercie producenta znajdują się zarówno proste niezarządzalne przełączniki pięcio-, ośmio- i szesnastoportowe, jak również w pełni zarządzalne i większe 24- i 48-portowe switche.
Co ważne, producent posiada w Polsce dział wsparcia przed- i posprzedażowego, co umożliwia m.in. bieżące aktualizacje oprogramowania, a także szybką i sprawną pomoc techniczną. Wszystkie urządzenia biznesowe TP-Link, w tym przełączniki PoE i punkty dostępowe, są objęte minimum pięcioletnią gwarancją producenta.

Jedną z ciekawszych propozycji z portfolio TP-Link jest przełącznik TL-SL1218MP, który świetnie sprawdzi w małych systemach VSS/CCTV lub jako przełącznik dostępowy do kamer. Switch zawiera 16 portów Fast Ethernet z zasilaniem PoE+ oraz dwa porty UPLINK Gigabit Ethernet pozwalające na integrację systemu kamer z resztą infrastruktury sieciowej.
TL-SL1218MP cechuje się wysokim budżetem mocy PoE – do 30 W/port, 192 W łącznej mocy zasilanych urządzeń. Przełącznik ma funkcję PoE Extend Mode pozwalającą zwiększyć odległość od przełącznika do zasilanego urządzenia końcowego aż do 250 metrów. Funkcja ta upraszcza rozmieszczenie punktów dystrybucyjnych w większych obiektach. Kolejnym wartym uwagi urządzeniem jest 24-portowy przełącznik TP-Link TL-SL1226MP. Podobnie jak TL-SL1218MP, jest to model dysponujący portami Fast Ethernet o budżecie mocy 30 W/port (łączny budżet mocy 250 W), dwoma gigabitowymi portami UPLINK oraz trybem PoE Extend Mode.
W przypadku integracji systemu dozoru wizyjnego z siecią dla pracowników lub gości obiektu warto zdecydować się na przełączniki zarządzalne, umożliwiające tworzenie m.in. osobnych wirtualnych, odseparowanych sieci – VLAN. Takie rozwiązanie znacząco poprawia bezpieczeństwo całej infrastruktury i daje pewność, że wrażliwe dane z kamer nie dostaną się w niepowołane ręce.
Przykładem takiego przełącznika jest 24-portowy TP-Link T1600G-28PS. Urządzenie jest wyposażone w porty Gigabit Ethernet zgodne ze standardami 802.3at/af, mogące łącznie dostarczyć 192 W mocy oraz cztery gigabitowe porty SFP. Jego większym bratem jest 48-portowy przełącznik TP-Link T1600G-52PS o całkowitej mocy podłączonych urządzeń do 384 W, który świetnie sprawdzi się, gdy musimy podłączyć nie tylko kamery IP, ale także telefony IP czy punkty dostępowe.
Więcej informacji:
Robert Gawroński, SMB Channel Manager
robert.gawronski@tp-link.com

TP-Link Polska
Ul. Ożarowska 40/42,
05-850 Duchnice
www.tp-link.com.pl

FM EXPERT – narzędzie dla zarządców budynków



CZY MASZ PROBLEM Z:
- **fałszywymi alarmami?**
- **ze sprawdzeniem, jak operatorzy realizują procedury?**
- **rozliczaniem prac konserwacyjnych?**
- **raportowaniem tego, co się dzieje w obiekcie?**
- **oszacowaniem kosztów, których można uniknąć?**

MODUŁ FM EXPERT POZWOLI CI W PROSTY I ZAUTOMATYZOWANY SPOSÓB ZARZĄDZAĆ OBIEKTEM.

FM Expert to intuicyjny w obsłudze, dedykowany moduł systemu GEMOS, który został opracowany na podstawie rzeczywistych potrzeb i oczekiwań użytkowników rozwiązania oraz przy ich współudziale. Jego zadaniem jest wsparcie procesu decyzyjnego zarządców obiektów – moduł dostarcza w przejrzystej i czytelnej formie dane gromadzone w centralnej bazie systemu zarządzania budynkiem GEMOS, także te pochodzące ze zintegrowanych przez niego systemów technicznych budynku.
Nagminne wzbudzanie alarmów przez zainstalowane systemy jest uciążliwe i odczula personel od szybkiego reagowania na pojawiające się ostrzeżenia. Istnieje zatem niebezpieczeństwo, że w przypadku prawidłowo zasygnalizowanego alarmu nie zostaną podjęte właściwe i adekwatnie zrealizowane procedury przewidziane na daną okoliczność. Taka sytuacja stanowi zagrożenie dla osób przebywających na terenie obiektu, w którym dochodzi do częstego alarmowania. Fałszywe czy tzw. bezsensowne alarmy, oprócz oczywistego zagrożenia, mają fatalny wpływ na wizerunek danej instytucji, a bardzo często tworzą także niepotrzebne koszty.
Każdemu zarządzającemu obiektem zależy na zachowaniu ciągłości bezawaryjnej pracy. Każda awaria wiąże się z określonymi kosztami, które odpowiednia konserwacja może zredukować do akceptowalnego minimum. Obiektywna ocena przeprowadzanych prac konserwacyjnych umożliwia racjonalne zarządzanie budżetem. Jak dotąd trudno było zmierzyć jakość wykonywanych prac konserwacyjnych. Problem polegał na tym, aby uchwycić w jednym miejscu liczbę awarii, wyłączeń systemu czy generowanych alarmów.

Moduł FM Expert pozwala poznać powiązania pomiędzy gromadzonymi danymi, analizować je oraz identyfikować niewidoczne na pierwszy rzut oka zależności. Stanowi wiarygodną podstawę do analizy i oceny prac służb technicznych, pracowników ochrony oraz firm odpowiedzialnych za konserwację urządzeń. FM Expert zapewnia zarządcy obiektu pełen pakiet informacji o stanie instalacji i urządzeń w budynku. Zgromadzone informacje są przedstawiane w formie wykresów kołowych i słupkowych lub zestawień tabelarycznych. Dane te można również wyeksportować do popularnych formatów .xls czy .pdf.

Ela-compil
ul. Szczepanowskiego 8,
60-541 Poznań
www.ela.pl
office@ela.pl

Swinkels Family Brewers

CASE STUDY

Gdy przybędziesz do Swinkels Family Brewers, znanego na całym świecie producenta piwa bawarskiego i 25 innych marek, szlaban parkingowy podnosi się swobodnie. Następnie zgłaszasz się do sympatycznej recepcjonistki, która prosi cię o zarejestrowanie się przy wskazanym stanowisku, w przyjemnym holu. W ramach rejestracji poprosimy cię o zapoznanie się z kilkoma zasadami dotyczącymi bezpieczeństwa i ochrony. Kiedy to potwierdzisz, twoja karta gościa zostanie wydrukowana automatycznie, a osoba, z którą jesteś umówiony, zostanie poinformowana o twoim przybyciu.

Pobyt jest dobrze zorganizowany, mija w przyjaznej atmosferze. To jest to, czego pragnie firma Swinkels Family Brewers. Tu, podobnie jak w Nedap, ludzie są najważniejsi, a gościnność głęboko zakorzeniła się w naszej kulturze korporacyjnej.

WIĘKSZE BEZPIECZEŃSTWO Z ZACHOWANIEM OTWARTOŚCI

Browary Swinkels Family Brewers rozwinęły się w szybkim tempie – zarówno w kraju, jak i za granicą – a ich siedzibę w Lieshout w Holandii rozbudowano. Konieczny był przegląd zabezpieczeń i zastosowanie bardziej rygorystycznych środków, ale z jednoczesnym zachowaniem panującej w firmie atmosfery ciepła i otwartości. Zrozumiałe jest, że firma Swinkels musi wiedzieć, kto wchodzi i gdzie przebywa na terenie zakładu, ale nie chce, by goście widzieli przed sobą wysokie ogrodzenie. Zamiast tego szlaban ma się podnosić automatycznie. Gościnność jest częścią kultury korporacyjnej browaru Swinkels. Browar tworzy emocje i doświadczenie, a my chcemy je odzwierciedlać w naszych systemach kontroli dostępu i bezpieczeństwa.

Dawniej na wejściu było kilka kamer dozorowych i dość nieustrukturyzowany system rejestrowania obecności gości. Polityka bezpieczeństwa nie nadążała za rozwojem organizacji, a fakt stosowania przez Swinkels Family Brewers dwóch systemów kontroli dostępu powodował dalsze komplikacje. Przeprowadzano coraz większą liczbę audytów dla głównych klientów, które dotyczyły również kontroli dostępu i zabezpieczeń. Dla firmy cieszącej się wieloletnią historią, a jednocześnie poważnie myślącej o przyszłości poprawa bezpieczeństwa stała się koniecznością.

JEDNOLITE PODEJŚCIE

W celu rozwiązania problemów związanych z bezpieczeństwem firma Swinkels Family Brewers powołała grupę projektową. Objęła ona przedstawicieli jej zakładu, działu informatyki i inżynierii oraz biura konstrukcyjnego, a także instalatora i konsultanta zewnętrznego. Grupa rozpoczęła poszukiwania odpowiednich rozwiązań, ale szybko zdała sobie sprawę, że najpierw będzie potrzebna polityka bezpieczeństwa. Sporządzono więc listę zagrożeń, przed którymi miano zabezpieczyć firmę, i wykorzystano ją do utworzenia stref w całym zakładzie. Z założenia nie chciano tworzyć czegoś na wzór Fortu Knox – celem było zachowanie wizerunku otwartości i gościnności, przy jednoczesnym zapewnieniu bezpieczeństwa.

Potrzebowaliśmy systemu skalowalnego, przyjaznego dla użytkownika, dającego się połączyć z innymi systemami zarządzania, opartego na adresie IP. Wszystkie te wymagania doprowadziły do wyboru systemu AEOS.

SWINKELS FAMILY BREWERS W LICZBACH

- 1 rodzina
- 27 marek
- 130 państw
- ponad 1800 pracowników
- 300 lat doświadczenia
- 8 mln hektolitrów piwa rocznie
- ponad 713,1 mln euro rocznego obrotu oraz 2 zakłady chronione za pomocą jednego systemu kontroli dostępu – AEOS firmy Nedap

AEOS SPEŁNIA WYDŁUŻAJĄCĄ SIĘ LISTĘ WYMAGAŃ

Po przyjęciu polityki bezpieczeństwa grupa projektowa przystąpiła do poszukiwań odpowiedniego rozwiązania. Specyfikacje zawierały długą listę wymagań, które nowy system będzie musiał spełnić. Wiele z nich włączano do projektu w miarę jego realizacji, ponieważ wgląd w to, co było potrzebne, rozwijał się stopniowo. Ostatecznie zespół doszedł do wniosku, że potrzebny jest system skalowalny, przyjazny dla użytkownika, który można połączyć z innymi systemami zarządzania, wykorzystujący protokół IP. Wszystkie te wymagania przesądziły o wyborze systemu AEOS firmy Nedap.

ELASTYCZNOŚĆ TO KLUCZ

Kolejne lata stosowania systemu AEOS potwierdziły, że doskonale wpasował się do browarów Swinkels Family Brewers pod względem zarówno kultury korporacyjnej, jak i potrzeb w zakresie bezpieczeństwa. Doceniana jest szczególnie elastyczność oferowana przez system AEOS – ułatwia on konfigurację, dodawanie nowych funkcjonalności do nowych lokalizacji oraz integrację z innymi systemami i procesami. Przykładowo, już po jego zainstalowaniu firma zdecydowała się na dodanie interfejsu graficznego AEOS. Wszystkie raporty o incydentach trafiają teraz do centralnej lokalizacji, dzięki czemu ochrona zakładu może się z nimi zapoznać. Firma Swinkels może też z łatwością dodać więcej funkcji, np. rejestrowanie danych pojazdu wg różnych kryteriów wyboru. W celu zapewnienia jeszcze bardziej rygorystycznej kontroli dostępu i rozpoczęcia prac nad przepisami dotyczącymi *anti-passback*, firma planuje usunięcie automatów na monety na szlabanach wyjazdowych i zastąpienie ich urządzeniami do poboru kart i czytnikami identyfikatorów. Można to łatwo uregulować za pomocą systemu AEOS.

ŁATWA INTEGRACJA

Zdaniem kierownika zakładu Swinkels, Stefana Fehlhabera, łatwość integracji systemu AEOS z innymi systemami stanowi istotną korzyść. – *Jestem naprawdę zadowolony z integracji systemów AEOS i Geutebruck* – mówi. – *W przypadku pojawienia się nieautoryzowanej karty lub połączenia domofonowego kamera włączy się automatycznie. Będziemy również korzystać z możliwości integracyjnych systemu AEOS z naszym systemem rejestracji gości.*

WSZYSTKO NA JEDNEJ, STALE UDOSKONALANEJ PLATFORMIE

System AEOS doskonale spełnia początkowe wymagania postawione przez Swinkels Family Brewers, by móc wykonywać jak najwięcej zadań na jednej otwartej platformie bezpieczeństwa. Tak został zaprojektowany.

S. Fehlhaber kontynuuje: *Jesteśmy pod dużym wrażeniem skalowalności, stabilności i solidności systemu AEOS. Jest on bardzo praktyczny w codziennym użyciu i łatwy w obsłudze dla naszych pracowników ochrony. Ogromnym ułatwieniem jest również możliwość używania jednej plakietki w różnych miejscach.*

AEOS stanowi doskonałą podstawę do wszelkiego rodzaju fizycznej kontroli dostępu, w dowolnym miejscu, a Nedap nadal wzbogaca go o cechy charakterystyczne dla danej branży.

NAJPIERW LUDZIE, POTEM TECHNOLOGIA

Dla wielu organizacji wdrożenie nowego systemu kontroli dostępu może powodować pewien opór. Firma Swinkels Family Brewers przewidziała to i w ramach zarządzania zastosowała podejście stawiające ludzi na pierwszym miejscu. W okresie poprzedzającym wdrożenie AEOS zapewniła, jasno to komunikując, że jej pracownicy wiedzą, czego mogą się spodziewać i dlaczego ta zmiana ma miejsce. Na etapie planowania zaangażowała również kierowników działów, pytając ich, jakie obszary należałoby zabezpieczyć, a jakie powinny pozostać dostępne. Nie tylko podniosło to poziom bezpieczeństwa, ale także zapewniło wsparcie dla zmian w przyszłości.

BEZPIECZEŃSTWO NA CAŁE ŻYCIE

Takie podejście jest zbieżne ze standardami pracy w Nedap i m.in. dlatego tak dobrze dopasowaliśmy się do potrzeb firmy Swinkels Family Brewers. Potwierdza to Fehlhaber: *Naprawdę cieszy nas fakt, że firma Nedap trzyma się blisko użytkowników końcowych, dzięki czemu są oni świadomi nowych rozwiązań w zakresie potrzeb, chęci i preferencji.* Robimy tak, ponieważ dla nas bezpieczeństwo to nie tylko technologia – również ludzie i to, jak żyją. Dążymy do zaspokojenia podstawowych potrzeb w zakresie bezpieczeństwa i poczucia bezpieczeństwa innych, by mogli jak najlepiej wykorzystać każdy dzień i skupić się na swoich podstawowych zadaniach. Nazywamy to **„Bezpieczeństwem na całe życie”**, ponieważ wolność oferowana przez AEOS to o wiele więcej, niż tylko kontrola dostępu – to możliwość poprawy wydajności, kreatywności i osiągnięć.

Zachowanie jednolitych standardów bezpieczeństwa we wszystkich filiach przedsiębiorstwa wielooddziałowego (np. banku, sieci handlowej) jest prawdziwym wyzwaniem. Proces administrowania rozproszonymi instalacjami bezpieczeństwa usprawniają specjalne integrujące rozwiązania informatyczne.

Zintegrowane zarządzanie SSWiN w organizacjach o strukturze rozproszonej

Przykładem oprogramowania, dzięki któremu administrowanie systemami sygnalizacji włamania i napadu pracującymi w obiektach instytucji wielooddziałowej staje się łatwiejsze, wygodniejsze i bardziej efektywne, jest INTEGRUM. Zarządza ono systemami alarmowymi bazującymi na centralach INTEGRA lub INTEGRA Plus (z dołączonymi dedykowanymi modułami komunikacyjnymi, np. ETHM-1 Plus lub INT-GSM), pracującymi w obiektach rozmieszczonych na dowolnym obszarze. Informacje o stanie instalacji są zbierane na bieżąco – zdalny wgląd w te dane umożliwia natychmiastową reakcję na określony typ zdarzeń, np. alarmy czy awarie.

Struktura

Każdy z nadzorowanych obiektów jest przypisany do konkretnej gałęzi (regionu) w drzewiastej strukturze systemu. Daje to możliwość przejrzystego odwzorowania schematu organizacyjnego nawet dużej organizacji. INTEGRUM jest systemem skalowalnym – dodawanie nowych obiektów (np. podczas rozbudowy firmy) odbywa się w wygodny, szybki i nieskomplikowany sposób.

Administrowanie uprawnieniami

Możliwe jest utworzenie scentralizowanej bazy wszystkich użytkowników systemu. INTEGRUM oferuje szerokie możliwości zarządzania ich uprawnieniami. Dostępne jest także delegowanie uprawnień dla osób odpowiedzialnych za personel w danym obiekcie (np. kierownik, dyrektor) – nie musi się tym zajmować administrator.

Intuicyjna obsługa

Aplikacja jest obsługiwana z poziomu przeglądarki internetowej, dzięki czemu systemem można zarządzać z dowolnego miejsca. Aby ułatwić administratorom analizę informacji o systemie, utworzony został podział na: użytkownicy, centrale, zdarzenia. Dostępne są też różne szczegółowe filtry.

Jeden z paneli służy do przeglądania danych użytkowników poszczególnych central i zarządzania bazą osób, z których każda może być powiązana z wieloma obiektami. Użytkownikom można zdalnie przydzielać identyfikatory (np. karty). Panele dotyczące central umożliwiają edycję istniejących obiektów i dodawanie nowych. Ponadto operator ma wgląd w aktualny stan central, ich partycji, stref czy pojedynczych wejść. Możliwe jest też zdalne załączenie/wyłączenie czuwania, sterowanie wyjściami, przejściami itp. Lista „Zdarzenia" zawiera informacje o tym, co dzieje się w systemie – z podziałem na lokalizację, typ zdarzenia i powiązanego użytkownika. Zgromadzone dane można opatrywać komentarzami, co ułatwia późniejszą identyfikację.

Kontrola konfiguracji

INTEGRUM zawiera moduł kontroli konfiguracji centrali alarmowej. Okresowo na serwer jest pobierany pełen zbiór ustawień central alarmowych, a następnie przygotowywany jest raport wskazujący rozbieżności między wcześniejszą a bieżącą wersją konfiguracji.

Wszystko w jednym miejscu

Panel sterowania to ekran pozwalający na bieżąco śledzić, co dzieje się w systemie. W razie alarmu lub awarii pojawiają się wyskakujące okna z opcją umieszczenia komentarza. Ponadto wskazane osoby mogą być powiadamiane o określonych zdarzeniach drogą mailową. Operator, mając do dyspozycji widok map, oprócz bezpośredniego wglądu w sytuację systemu, może wyzwalać dostępne dla różnych obiektów akcje i otwierać podgląd obrazu z kamer. Podczas tworzenia map można uwzględniać szczegółowe odwzorowanie układów pomieszczeń, planów itp. INTEGRUM oferuje szerokie możliwości zarządzania rozproszonymi systemami alarmowymi. Można dzięki niemu w prosty, czytelny sposób administrować siecią obiektów i ich użytkowników, jednocześnie optymalizując koszty i oszczędzając cenny czas.

SATEL

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

Rozwój technologii, a za nim postępujący coraz bardziej oczekiwany przez większość komfort życia sprawiły, że w naszych domach zaczęła pojawiać się automatyka, powszechnie nazywana *smart home*. Inteligentny dom ma za zadanie zapewnić jego mieszkańcom komfort i wygodę. Co to oznacza w praktyce?

Profesjonalny system alarmowy w parze z inteligentnym domem

AVA PRO

Zmęczeni codziennymi obowiązkami i nieustannym brakiem czasu, wracając do domu, oczekujemy pełnego relaksu i odpoczynku. Po przeczytaniu setek maili, odpowiedzeniu na dziesiątki pytań i zmaganiach z licznymi projektami chętnie skorzystamy z dobrodziejstw, jakie nam umożliwia dzisiejsza technika, a więc ze sterowania oświetleniem, temperaturą, żelazkiem czy roletami. Dzięki nowoczesnym rozwiązaniom chociaż część obowiązków przestanie zaprzątać nasze myśli i pozwoli skupić się na rzeczach bardziej dla nas przyjemnych. Dużą zaletą takiego systemu, z czego nie każdy zdaje sobie sprawę, jest zwiększenie bezpieczeństwa zarówno osób, jak i ich majątku. Integracja systemów *smart home* z systemami alarmowymi daje nowe możliwości zapewnienia ochrony, czego przykładem może być AVA PRO, najnowsze rozwiązanie firmy EBS.

Potencjał integracji profesjonalnych systemów zabezpieczeń z systemami *smart home* doskonale widać w liczbach i trendach rynkowych. Według raportu ResearchAndMarkets.com dotyczącego rynku *smart home security* na lata 2018 – 2023 przewidywany wzrost sprzedaży jest na poziomie 15,56% rok do roku. Firma szacuje, że w 2026 r. wartość rynku w ujęciu globalnym osiągnie poziom 3,2 mld dol., a są jeszcze bardziej optymistyczne raporty. Firma IDC prognozuje, że do 2023 r. samych urządzeń *smart home* na świecie będzie 1,5 mld. Wszystkie dane potwierdzają tylko, że ludzie coraz bardziej otwierają się na technologię „smart".

Jeszcze niedawno systemy automatyki musiały być dostosowane do systemów ochrony. Obecnie obserwujemy odwrotny trend. Wychodząc naprzeciw tym tendencjom, firma EBS wprowadziła na rynek AVA PRO, czyli połączenie profesjonalnego systemu alarmowego z nowoczesnością inteligentnego domu.
AVA Pro dzięki swojej modułowej architekturze łatwo może zostać wzbogacony o moduł pozwalający na komunikację z urządzeniami IoT (*Internet of Things*) oraz sektora *smart home* za pomocą protokołu Z-Wave. Dzięki wykorzystaniu międzynarodowego standardu radiowego, jakim niewątpliwie jest Z-Wave, mamy możliwość szybkiej instalacji urządzeń, niezależnie od struktury przewodowej budynku.

T E K S T
Maciej Górecki
Project Manager, EBS

Najpopularniejszymi elementami do sterowania zarówno w domu, jak i w biurze są trzy funkcjonalności:
- sterowanie oświetleniem,
- sterowanie gniazdami elektrycznymi,
- sterowanie ogrzewaniem.

Zapewniając te funkcjonalności, AVA PRO integruje ze sobą trzy urządzenia: *wall plug, dimmer* oraz termostat w postaci głowicy do montażu bezpośrednio na grzejniku.
Wall plug służy do sterowania gniazdami elektrycznymi i elementami do niego podłączonymi. Za pomocą AVA PRO można wyłączyć i włączyć lampę, odłączyć żelazko czy inne urządzenia potencjalnie niebezpiecznie lub po prostu oszczędzać energię.
Urządzenie typu *dimmer* (ściemniacz oświetlenia) jest montowane pod włącznikiem i pozwala na sterowanie natężeniem światła. Użytkownik może włączyć lub wyłączyć oświetlenie albo je przyciemnić lub rozjaśnić.
Termostat pozwala na utrzymywanie pożądanej temperatury w pomieszczeniu, tzw. temperatury zadanej. Dzięki temu zyskuje się większy komfort, wygodę, ale także znaczne oszczędności na ogrzewaniu.
Każdym z wymienionych urządzeń możemy sterować wygodnie za pomocą aplikacji EBS Security App dedykowanej do obsługi centrali AVA PRO. Jeśli zapomnimy wyłączyć żelazko, możemy to zrobić natychmiast z dowolnego miejsca na świecie. Wracając z wakacji, w łatwy sposób za pomocą aplikacji możemy podnieść temperaturę w swoim domu, dzięki czemu powrót będzie jeszcze bardziej przyjemny.

W celu efektywnego wykorzystania możliwości smart home w AVA PRO wprowadzono trzy funkcje:
Sceny
(zwane także scenariuszami) pozwalają na wysterowanie wielu urządzeń *smart home* za pomocą jednego przycisku lub jednej akcji. Przykładowo, wychodząc z domu kliknięciem jednego przycisku uruchamiamy scenę „Wyjście". W ten sposób automatycznie wyłączy się oświetlenie, wyłączą się wybrane gniazda elektryczne oraz zostanie obniżona temperatura wybranych urządzeń.

Funkcje czasowe
pozwalają na uzależnienie aktywności scen lub pojedynczych urządzeń od czasu. Przykładowo, tę funkcjonalność można wykorzystać do podświetlania witryny sklepowej w galerii handlowej, aby przykuć uwagę osób wychodzących z kina czy restauracji po godzinie zamknięcia sklepu, a następnie wyłączyć oświetlenie w celu oszczędności energii.

Harmonogramy
to połącznie funkcji sceny i funkcji czasowej. Harmonogram uzależnia wywoływanie różnych akcji i funkcji (np. scen) od pory dnia i tygodnia. Idealnym przykładem jest sterowanie ogrzewaniem z dostosowaniem do trybu życia jego użytkownika. Dzięki tej funkcjonalności przykładowy dzień Kowalskiego może wyglądać następująco:
- **6:00 Kowalski budzi się** – 5:30 ogrzewanie zostaje ustawione na 20°C, ogrzewanie podłogowe w łazience załączone – przyjemnie wstać, gdy jest ciepło
- **8:00 Kowalski wychodzi do pracy** – 7:30 zostaje ustawiona temperatura 18°C – generujemy oszczędności
- **16:30 Kowalski wraca do domu** – 16:00 ustawiona temperatura 21°C – idealna temperatura do odpoczynku po pracy
- **23:00 Kowalski idzie spać** – 23:00 ustawienie temperatury 19°C – według badań najlepsza do komfortowego snu.

AVA PRO to jednak przede wszystkim profesjonalny system zaprojektowany do ochrony ludzi i mienia, a dopiero na drugim miejscu system *smart home*. Połącznie tych dwóch cech daje jednak nowe możliwości dla jego użytkowników. Każda scenę można uzależnić od sygnałów alarmowych. I tak np. scena „Wyjście " może się uruchamiać dopiero po uzbrojeniu systemu alarmowego. Dzięki AVA Key wystarczy jeden przycisk na klawiaturze w celu celu uzbrojenia systemu alarmowego oraz wyłączenia oświetlenia w całym domu, zmniejszenia temperatury czy wyłączenia gniazd elektrycznych (oszczędność energii) podczas nieobecności domowników. Czujki ruchu mogą włączać oświetlenie na schodach, a czujka otwarcia okna (kontaktron) może wyłączać ogrzewanie w pokoju w przypadku wykrycia otwarcia okna. Ponadto dzięki połączeniu dwóch „światów", jakim są system ochrony i system *smart home*, zyskujemy wiele innych funkcjonalności:
- Wykrycie zalania (czujka zalania) – zamknięcie zaworu wody, powiadomienie mieszkańców poprzez aplikację EBS Security.
- Wykrycie pożaru (czujka dymu) – wyłączenie wentylatorów, powiadomienie użytkowników.
- Włamanie (czujka sswin) – funkcja „panika" – załączenie oświetlenia w całym domu w celu wypłoszenia intruza.

Spektrum zastosowań dla AVA Pro jest wręcz nieograniczone. Najwięcej korzyści odnoszą klienci z rynku SOHO, SMB i użytkownicy indywidualni. Bezpieczeństwo idące w parze z wygodą, większą kontrolą i oszczędnościami to cechy poszukiwane przez ten segment rynku.
AVA PRO jest zarówno profesjonalnym systemem alarmowym, jak i systemem *smart home*. Zaopatrując się w niego, użytkownik zyskuje funkcjonalność dwóch różnych systemów. Mieszkanie, dom, domek letniskowy czy biuro – bez względu na to, co chcemy ochronić, AVA Pro zapewnia mieszkańcom i użytkownikom poczucie bezpieczeństwa, a także komfort, pozwalając na zdalne sterowanie i kontrolę na odległość, z poziomu aplikacji mobilnej.

EBS
ul. Bronisława Czecha 59
04-555 Warszawa
https://ebssmart.com

AJAX

Nowoczesny bezprzewodowy system alarmowy z funkcjami smart home

Komfort, wygoda i bezpieczeństwo to kluczowe cechy, którymi kierujemy się podczas zakupu lub budowy własnego domu. Każdy chciałby mieszkać w takich warunkach, co w dobie dzisiejszych rozwiązań nie jest trudne – wystarczy zainstalować system, który to umożliwi. Firma Ajax Systems posiada w ofercie pełną gamę urządzeń radiowych, które to zapewniają.

Innowacje w zakresie bezpieczeństwa

Firma Ajax Systems, która działa już w ponad dziewięćdziesięciu krajach, w tym w większości krajów Europy Środkowo-Wschodniej, wkracza na polski rynek ze swoimi urządzeniami bezprzewodowego systemu alarmowego Ajax, realizującymi funkcje „inteligentnego domu".

Ajax jest najczęściej nagradzanym bezprzewodowym systemem alarmowym w Europie mającym takie wyróżnienia, jak:
– *The Best Innovative Product* – nagroda dla najbardziej innowacyjnego produktu, przyznana podczas międzynarodowej wystawy zabezpieczeń Securika w Moskwie w 2017 r.,
– *Intruder Alarm of the Year* – nagroda dla najlepszego produktu roku 2017 (*Security & Fire Excellence Awards*), przyznana podczas targów IFSEC International w Londynie.
System Ajax znalazł się także w grupie finalistów na wiodących w Europie międzynarodowych na targach Expoprotection w 2018 r.

Wykorzystując najnowsze technologie z dziedziny zabezpieczeń, firma Ajax Systems opracowała i oferuje rozwiązania, które można dopasować do konkretnych, rzeczywistych potrzeb każdego użytkownika. Wszystkie urządzenia systemu (czujki) komunikują się z centralą sterowania systemu alarmowego drogą radiową (w pasmie częstotliwości 868,0–868,6 MHz) poprzez hub 2 (patent) z wykorzystaniem protokołu Jaweller. Zasięg pomiędzy współpracującymi z centralą czujkami wynosi 1700 m, natomiast wykorzystanie protokołu Wings pozwala przesyłać, również drogą radiową, zdjęcia z czujki ruchu z wbudowaną kamerą Ajax MotionCam w czasie krótszym niż 9 s.

Większość urządzeń radiowych Ajax jest gotowa do użycia od razu po wyjęciu z pudełka. Innowacyjny system montażu SmartBracket pozwala na szybkie zainstalowanie danego urządzenia w zaledwie kilka minut.

Bezpieczeństwo przede wszystkim

Centrale SSWiN Ajax z serii Motion w sytuacji wykrycia obecności potencjalnego zagrożenia uruchamiają sygnalizację alarmową mającą za zadanie odstraszyć potencjalnych intruzów i jednocześnie przyciągnąć uwagę sąsiadów. Następnie wysyłają informacje do użytkownika oraz firmy ochroniarskiej o naruszeniu wyznaczonej strefy, także w formie zdjęć, w celu weryfikacji zagrożenia.
We współczesnych gospodarstwach domowych zagrożenie może nadejść z każdej strony. Dom ma wiele elementów, które nieodpowiednio chronione bądź niewłaściwie monitorowane mogą doprowadzić do poważnych szkód materialnych, a nawet ofiar w ludziach. Integracja systemów zabezpieczeń z systemami inteligentnego domu pozwala skutecznie zwiększyć poziom bezpieczeństwa nie tylko wewnątrz budynku, ale także na zewnątrz.
Równie groźne mogą być też straty wynikające z pożaru lub awarii technicznych. Dzięki współpracy czujek pożarowych (*Ajax FireProtect*) oraz zalania (*Ajax LeaksProtect*) z przekaźnikami (*Relay* oraz *WallSwitch*) system alarmowy Ajax będzie w stanie podjąć odpowiednie działania. Wszystkie zawory zostaną automatycznie zamknięte, a użytkownik uzyska błyskawiczną informację o zaistniałej sytuacji za pomocą alertów bezpieczeństwa z poziomu aplikacji.

Inteligentny dom na wyciągnięcie ręki

Ajax Systems, oprócz realizacji funkcji systemów SSWiN, może też sterować urządzeniami domu z poziomu jednej aplikacji poprzez podłączenie wszystkich urządzeń gospodarstwa domowego do bezprzewodowej inteligentnej wtyczki Ajax. Zaletą takich rozwiązań jest możliwość kontroli tego, co aktualnie dzieje się w domu, bez konieczności przebywania w nim. Zautomatyzowane procesy sterowania dbają o nasz komfort, wykonując wiele czynności samodzielnie, dzięki czemu oszczędzamy czas, który możemy wykorzystać w inny sposób.

Za pomocą aplikacji można wyznaczać role (scenariusze) dla poszczególnych urządzeń: sterować roletami, aby podnosiły się bądź opuszczały automatycznie w zależności od pory dnia i nocy, ustawiać ogrzewanie na odpowiednim poziomie czy też włączać lub wyłączać oświetlenie, kiedy wracamy do domu albo wychodzimy z niego.
Takie rozwiązanie pozwala także znacząco zredukować koszty utrzymania domu. Dzięki pełnej integracji oraz automatyzacji wielu urządzeń jesteśmy w stanie uzyskać znaczący zwrot kosztów zużycia energii. System „inteligentnego domu" dba nie tylko o bezpieczeństwo i komfort użytkowania, ale także o finanse i środowisko naturalne. Możliwości jest naprawdę wiele i tylko od nas zależy, jak skonfigurujemy swój „inteligentny dom".

Wszystkie urządzenia wchodzące w skład innowacyjnych bezprzewodowych systemów alarmowych z funkcją „inteligentnego domu" marki Ajax mają certyfikaty na zgodność z wymaganiami normy EN 50131 Grade 2.

Wprowadzenie na polski rynek urządzeń radiowych systemu alarmowego z funkcją „inteligentnego domu" Ajax jest krokiem ku rozwojowi. Zaawansowana technologia idąca w parze z inteligentnym oprogramowaniem wspiera użytkowników, poprawiając ich komfort życia, optymalizując koszty energii elektrycznej i zapewniając pełne bezpieczeństwo.

Cash-in-Transit: pożegnanie z bronią?

Już od wielu lat w przedsiębiorstwach działających w sektorze transportu gotówki promuje się systemy znakowania banknotów (IBNS – *Intelligent Banknote Neutralization System* – inteligentny system neutralizacji banknotów) jako technologię ochronną.

Firma StrongPoint Cash Security wielokrotnie podkreślała, że jej celem nie jest po prostu znakowanie banknotów za pomocą inteligentnych i zaawansowanych technologicznie urządzeń. Podejmuje większe wyzwanie. Zależy jej na tym, aby zarówno Tomasz w Gdańsku, jak i Siergiej w Tuli, Mykoła w Odessie, Sebastien w Marsylii, Mathias w Monachium, Linda i Helena w Sztokholmie czy Björn w Trondheim wrócili po pracy do swoich bliskich cali i zdrowi.
Wspólnie z wiodącymi firmami Cash-In-Transit i ekspertami w dziedzinie ergonomii, opierając się na kilku opatentowanych rozwiązaniach technologicznych, StrongPoint Cash Security opracowała portfolio bezpiecznych walizek. Są to obecnie najbardziej zaawansowane tego typu urządzenia zabezpieczające dostępne na rynku. Wykonane z kompozytów z włókna węglowego, lekkich stopów i wysokiej jakości polimerów charakteryzują się najlepszym stosunkiem nośności do masy własnej. Bezpieczne walizki zajmują mało miejsca, ergonomiczna konstrukcja ładowania od góry zapewnia dużą ładowność przy małej powierzchni, a mała masa minimalizuje wysiłek użytkownika w trakcie transportu.

Tradycyjnie działalność związana z transportem gotówki jest uważana za niebezpieczną, dlatego nadal w niektórych krajach transport cennych ładunków może się odbywać wyłącznie pojazdami opancerzonymi z uzbrojonymi pracownikami ochrony. Taka forma zabezpieczenia zawsze musi być niezawodna i bezpieczna, jednak co roku pojawiają się wiadomości z dokładnie tymi samymi nagłówkami, że „doszło do ataku, pracownicy są ranni, a kosztowności skradziono". Czy wobec tego można mówić o niezawodności i bezpieczeństwie tradycyjnego rozwiązania?
W porównaniu z dotychczasowymi wymaganiami ostatnio obserwuje się dużą elastyczność w podejściu do taktyki zabezpieczeń transportu przedmiotów wartościowych. Coraz więcej krajów dopuszcza stosowanie inteligentnych systemów neutralizacji banknotów, a także specjalnych pojazdów i uzbrojonych strażników. Przykładem takiego podejścia jest stanowisko Europejskiego Banku Centralnego.
Badania przeprowadzone przez europejską organizację branżową EURICPA (*European Intelligent Cash Protection Association*) wskazują na ponad 65-proc. wzrost wykorzystania inteligentnych systemów neutralizacji banknotów w całej Unii Europejskiej i blisko 90-proc. wzrost w krajach strefy euro. Są też kraje, w których zezwala się na transport cennych przedmiotów, tylko pod warunkiem że w procesie operacyjnym wykorzystuje się urządzenia zawierające rozwiązania IBNS.

Podsumowując, możliwość neutralizacji banknotów stwarza warunki do bezpieczniejszej pracy w sektorze transportu gotówki oraz znacznie zmniejsza ryzyko wystąpienia niebezpiecznych sytuacji będących zagrożeniem dla pracowników ochrony i społeczeństwa. Metoda ta wyklucza możliwość osiągnięcia zysku z przestępstwa. Nigdy nie zostawiajmy niczego napastnikom!

W listopadzie 2020 r. StrongPoint Cash Security bedzie gościć na targach Securex w Poznaniu. Będzie nam miło spotkać się z Państwem i omówić możliwości współpracy. Zapraszamy do kontaktu: Alexey.Kvashnin@strongpoint.com.

StrongPoint Cash Security

Maskinvägen 13
931 37 Skellefteå,
Sweden
info.security@strongpoint.com

Bezpieczeństwo pożarowe w obiektach służby zdrowia

PANDEMIA KORONAWIRUSA Z WUHAN STANOWI JEDNO Z NAJWIĘKSZYCH WYZWAŃ DLA SYSTEMU SZEROKO POJMOWANEGO BEZPIECZEŃSTWA I OBRONY CYWILNEJ NA CAŁYM ŚWIECIE. W TYM KONTEKŚCIE WARTO PRZEANALIZOWAĆ WYTYCZNE DOTYCZĄCE SYSTEMÓW OCHRONY PRZECIWPOŻAROWEJ W OBIEKTACH SŁUŻBY ZDROWIA I ROLĘ, JAKĄ MOGĄ ODEGRAĆ PODCZAS EWENTUALNEJ EWAKUACJI.

Infrastruktura krytyczna (IK) to, wg ustawy o zarządzaniu kryzysowym, systemy i wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania administracji publicznej, instytucji i przedsiębiorców.

Infrastruktura krytyczna odgrywa kluczową rolę w funkcjonowaniu państwa i życiu jego obywateli. W wyniku zdarzeń spowodowanych siłami natury lub będących konsekwencją działań człowieka może zostać zniszczona, uszkodzona, a jej działanie może ulec zakłóceniu, przez co zagrożone może być życie i mienie obywateli. Równocześnie tego typu wydarzenia negatywnie wpływają na rozwój gospodarczy państwa. Stąd też ochrona infrastruktury krytycznej jest jednym z priorytetów stojących przed państwem polskim. Istota zadań sprowadza się nie tylko do zapewnienia jej ochrony przed zagrożeniami, ale również do tego, aby ewentualne uszkodzenia i zakłócenia w jej funkcjonowaniu były możliwie krótkotrwałe, łatwe do usunięcia i nie wywoływały dodatkowych strat dla obywateli i gospodarki [1].

11 marca br. Światowa Organizacja Zdrowia (WHO) ogłosiła stan pandemii, dwa dni później minister zdrowia Łukasz Szumowski poinformował, że w drodze rozporządzenia został w Polsce wprowadzony stan zagrożenia epidemicznego zgodnie z ustawą o zapobieganiu oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi, a dziewiętnaście szpitali przekształcono w szpitale zakaźne. Natomiast od piątku 20 marca od godziny 18:30 w całej Polsce obowiązuje już stan epidemii. Według komunikatu przekształcenie szpitala w szpital zakaźny ma usprawnić diagnostykę, hospitalizację i leczenie osób zakażonych koronawirusem.

A co z bezpieczeństwem pacjentów i pracowników, jeśli dojdzie do zagrożenia pożarem?

Zabezpieczenia przeciwpożarowe mają chronić przed powstaniem i rozprzestrzenianiem się ognia w obiekcie, powinny więc być wykonane z zachowaniem wymagań budowlanych oraz mieć odpowiednią klasę odporności pożarowej.

Jakie zabezpieczenia przeciwpożarowe stosuje się obecnie? W takich obiektach jak szpitale, gdzie ewentualna ewakuacja pacjentów może być szczególnie trudna, należy z wyjątkową precyzją przewidzieć wszystkie możliwe scenariusze. Szczegółowe uzgodnienia z użytkownikami obiektu dotyczą m.in. sposobu powiadamiania o alarmie pożarowym oraz zasad organizacyjnych samej ewakuacji, z uwzględnieniem obostrzeń dotyczących sal operacyjnych i sal intensywnej opieki medycznej.

Placówki opieki zdrowotnej lub ich części są zazwyczaj zaliczane do ZL II, czyli kategorii obiektów przeznaczonych przede wszystkim do użytku osób o ograniczonej zdolności poruszania się. Mogą się w nich pojawić także przestrzenie zakwalifikowane do kategorii ZL I (pomieszczenia, w których może przebywać ponad 50 osób niebędących ich stałymi użytkownikami ani osobami o ograniczonej zdolności poruszania się), jak i ZL III (użyteczności publicznej, niezakwalifikowane do ZL I i ZL II – pomieszczenia administracyjne). Po przypisaniu obiektowi opieki zdrowotnej odpowiedniej kategorii, zgodnie z przepisami [2], [3], [4] określa się wymagania dot. zabezpieczeń przeciwpożarowych.
Dopuszczalna wielkość powierzchni strefy pożarowej w obiekcie opieki zdrowotnej o jednej kondygnacji nadziemnej (bez ograniczenia wysokości) nie powinna przekraczać 8000 m², dla niskiego – 5000 m², średnio wysokiego – 3500 m², a wysokiego i wysokościowego – 2000 m². Zgodnie z § 28.1 rozporządzenia MSWiA [3] stosowanie systemów sygnalizacji pożarowej jest wymagane w budynkach szpitalnych o liczbie łóżek powyżej 200.
Brak tego typu rozwiązań dopuszcza się w obiektach wyposażonych w stałe urządzenia gaśnicze, chyba że system sygnalizacji pożarowej jest wymagany do uruchomienia urządzeń przewidzianych do funkcjonowania podczas pożaru, np. systemów oddymiania czy dźwiękowych systemów ostrzegawczych (DSO). W obiektach służby zdrowia taka zamiana jest rzadkością ze względu na brak konieczności montażu stałych urządzeń gaśniczych – wymóg ten dotyczy obiektów wysokościowych lub wynika z wprowadzenia rozwiązań zamiennych.

Trudno jest myśleć o zapewnieniu bezpieczeństwa bez analizy ryzyka wystąpienia pożaru i doboru pod tym względem odpowiedniego systemu sygnalizacji pożarowej (SSP). Głównym elementem systemu jest centrala sygnalizacji pożarowej (lub sieć central dla większych obiektów). Od jej parametrów technicznych, takich jak niezawodność działania, elastyczność, zdolność przetwarzania dużej ilości danych związanych z obsługą podłączonych elementów peryferyjnych (np. czujek pożarowych), zależy zapewnienie wymaganego bezpieczeństwa pożarowego w celu realizacji założeń scenariusza pożarowego,

INFRASTRUKTURA KRYTYCZNA OBEJMUJE SYSTEMY:

- zaopatrzenia w energię, surowce energetyczne i paliwa,
- łączności,
- sieci teleinformatycznych,
- finansowe,
- zaopatrzenia w żywność,
- zaopatrzenia w wodę,
- ochrony zdrowia,
- transportowe,
- ratownicze,
- zapewniające ciągłość działania administracji publicznej,
- produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych.

Centrale sygnalizacji pożarowej współpracujące z urządzeniami peryferyjnymi mają przede wszystkim za zadanie powiadomić i wskazać miejsce wystąpienia pożaru oraz uruchomić urządzenia alarmujące oraz inne urządzenia i systemy przeciwpożarowe zgodnie z matrycą sterowań powstałą na bazie scenariusza pożarowego. System sygnalizacji pożarowej realizuje następujące funkcje:

- detekcja pożaru za pomocą czujek automatycznych i ręcznych ostrzegaczy pożarowych,
- zaalarmowanie osób o zagrożeniu poprzez uruchomienie sygnalizatorów alarmowych akustycznych, optycznych czy optyczno-akustycznych lub wysterowania dźwiękowego systemu ostrzegawczego (DSO) w celu nadania komunikatów ewakuacyjnych,
- wydzielenie stref pożarowych poprzez zamknięcie klap na wentylacji bytowej,
- wyłączenie systemów wentylacji i klimatyzacji,
- uruchamianie systemu wentylacji pożarowej, w tym sterowanie i monitoring klap odcinających wentylacji pożarowej,
- odblokowanie rygli systemu kontroli dostępu na drogach ewakuacyjnych,
- zamknięcie bram pożarowych, załączenie pracy pożarowej dźwigów windowych.

Skuteczność realizacji wymienionych funkcji wpływa bezpośrednio na zapewnienie ewakuacji ludzi z obiektu oraz ograniczenia strat mienia w wyniku pożaru. Centrale mają funkcję autodiagnostyki własnych komponentów, a także monitorują stan pracy i uszkodzenia innych urządzeń ppoż. oraz urządzeń technicznych współdziałających z SSP. Dzięki temu zapewnione jest wykrycie wszelkich nieprawidłowości w funkcjonowaniu elementów składowych całego systemu bezpieczeństwa pożarowego obiektu.

W ramach oferowanego przez Schrack Seconet systemu sygnalizacji pożarowej Integral IP dostępne są trzy typy central do zastosowania w różnych wielkościach instalacji sygnalizacji pożarowej: Integral IP MX, Integral IP CX oraz Integral IP BXF. Centrale Integral IP MX i CX mogą być dodatkowo wykorzystywane jako centrale sterujące stałymi urządzeniami gaśniczymi (SUG). Uzupełnieniem paneli wbudowanych w centrale są wyniesione panele wskazań i obsługi, które można zainstalować w miejscu dogodnym dla personelu ochrony obiektu czy też z punktu widzenia działań prowadzonych przez służby ratowniczo-gaśnicze. System Integral IP obejmuje całą gamę urządzeń przeznaczonych do nadzoru i obsługi, np. system wizualizacji SecoLOG IP czy urządzenia zdalnego dostępu pakietu Integral Remote. Pozwalają one na informowanie o krytycznych zdarzeniach poprzez urządzenia mobilne (smartfon czy tablet) nie tylko osoby zlokalizowane w obiekcie, ale również innych użytkowników/zarządców obiektu.

W wyznaczonych obiektach służby zdrowia wymagane są urządzenia, których zadaniem jest powiadomienie przebywających w nim osób o zagrożeniu – pożarze. Działanie systemów ma wspomóc proces ewakuacji ludzi na zewnątrz budynku lub do strefy bezpiecznej. Zgodnie z Rozporządzeniem MSWiA [3] instalacja DSO jest wymagana w szpitalach o liczbie łóżek powyżej 200, z wyłączeniem pomieszczeń intensywnej opieki medycznej, sal operacyjnych i sal z chorymi. Jak widać, należy tak rozmieścić głośniki instalacji DSO, aby działający system nie wywoływał stresu lub wręcz paniki wśród przebywających w szpitalu pacjentów.
W tego typu obiektach prawidłowe przygotowanie projektu instalacji i działania DSO ma bardzo duże znaczenie. Zgodnie z wymaganiami ww. rozporządzenia należy przede wszystkim dokładnie przeanalizować cały obiekt pod kątem lokalizacji i przeznaczenia pomieszczeń. Korzystając z rzutów architektonicznych dla poszczególnych kondygnacji szpitala, jesteśmy w stanie precyzyjnie rozmieścić głośniki oraz prawidłowo dobrać ich moc. Kolejną sprawą jest dobór liczby i prowadzenie linii głośnikowych, co może przełożyć się później na samą funkcjonalność systemu, np. na podział obiektu na strefy nagłośnieniowe. Ważnym zadaniem jest odpowiednie przygotowanie komunikatów głosowych, tzw. kodowanych. Powinny być tak skonstruowane, aby ich treść nie wzbudzała niepokoju/paniki wśród pacjentów, a przy tym precyzyjnie przekazywała polecenia personelowi szpitala. Tylko takie podejście umożliwi przeprowadzenie bezpiecznej ewakuacji z zagrożonych przestrzeni obiektu.
System APS®-APROSYS umożliwia wgranie wielu komunikatów automatycznych różnej treści, których aktywacja może być dowolnie zaprogramowana, co daje wiele różnych scenariuszy. W ramach pojedynczego modułu komunikatów APS-19.2 można wgrać do 30 plików po 1MB każdy, a w pojedynczym systemie można zastosować kilka takich modułów. Kolejnym ciekawym i unikatowym na naszym rynku rozwiązaniem jest moduł APS-18.3. W sytuacjach nadzwyczajnych (np. zagrożenia związane z nieuprawnionym wtargnięciem osób na teren szpitala lub atak agresywnego pacjenta) pozwala on przeszkolonemu personelowi na bezpośrednie wdzwonienie się do systemu i nadanie komunikatu na żywo, bez konieczności korzystania z pulpitu mikrofonowego. To cenna i przydatna funkcja systemu APS®-APROSYS, która zdecydowanie wspomaga i przyspiesza przeprowadzenie ewakuacji lub poinformowanie o zaistniałym zagrożeniu.

Zaprojektowanie niezawodnego, inteligentnego systemu SSP może również uchronić przed zbędną ewakuacją z obiektu, a to pozwala uniknąć kolejnych zagrożeń i niepotrzebnych, często bardzo wysokich kosztów.
Rozwiązania Schrack Seconet umożliwiają lokalne monitorowanie stanu ich pracy, a tym samym ułatwiają kontrolę nad całym obiektem. Estetyczne, bezakumulatorowe, wyniesione panele obsługi Integral MAP lub panele wskazań Integral PIP zamontowane w pobliżu miejsc dyżuru pielęgniarskiego pozwalają na szybszą weryfikację pojawiających się komunikatów oraz ich ewentualne skasowanie na panelu obsługi, bez wywoływania niepotrzebnej ewakuacji. Z kolei w sytuacji prawdziwego zagrożenia panele wskazań i obsługi zdecydowanie przyspieszają działania interwencyjne.

Specyfiką obiektów służby zdrowia, przede wszystkim szpitali, są specjalne wymogi dotyczące wyposażenia sal operacyjnych i zabiegowych. Ze względu na sterylność tych pomieszczeń zaleca się stosowanie jak najmniejszej liczby zbędnych, widocznych urządzeń. Schrack Seconet wychodzi naprzeciw i takim wymaganiom, zabezpieczając sale operacyjne czujkami w osłonie przeciwwietrznej LKM 593X, montowanymi w kanałach wyciągowych systemu wentylacji i działającymi na zasadzie dozorowania czystości powietrza w pomieszczeniach. Standardowym już rozwiązaniem jest zabezpieczenie sal operacyjnych czujkami specjalnymi, np. czujkami zasysającymi dymu serii AirSCREEN ASD 53x. Ich najważniejszą cechą jest możliwość montażu układu orurowania, a tym samym i punktów próbkujących, w suficie i w przestrzeni międzystropowej, co umożliwia wyniesienie układu detekcyjnego do innego pomieszczenia. System ten charakteryzuje bardzo wysoka czułość i wykrywanie pożaru w bardzo wczesnym stadium, co zdecydowanie zmniejsza ryzyko zagrożenia i daje czas potrzebny na działania, np. ewakuacyjne.
Systemy zasysające w szpitalach stosuje się również do zabezpieczania szybów windowych i stacji transformatorowych ze względu na ich parametry techniczne i późniejsze uproszczenie eksploatacji.
Dla zapewnienia optymalnej obsługi, zarządzania i sterowania zintegrowanymi systemami bezpieczeństwa pożarowego i innych instalacji technicznych obiektu Schrack Seconet oferuje certyfikowany system integrujący urządzenia przeciwpożarowe SIS-FIRE, ściśle współpracujący z systemem Integral IP. Dzięki zastosowaniu intuicyjnego interfejsu użytkownika i wdrożeniu procedur/instrukcji postępowania w momencie wystąpienia alarmu pożarowego operator systemu może błyskawicznie zareagować na powstałe zagrożenie, zidentyfikować jego miejsce oraz nadzorować skuteczność działania urządzeń ppoż. zgodnie ze scenariuszem pożarowym. Dla uprawnionego personelu i służb ratowniczo-gaśniczych dostępne jest również sterowanie ręczne, zmieniające scenariusz automatyczny w sytuacji niekontrolowanego rozwoju pożaru.

Ważnym systemem w placówkach opieki zdrowotnej są także nowoczesne systemy przyzywowe, gwarantujące pacjentom bezpieczeństwo dzięki wzajemnej komunikacji z personelem medycznym. Sieciowy system VISOCALL IP realizuje różne scenariusze opieki. W pokojach montowane są specjalne przyciski, po których naciśnięciu wysyłany jest sygnał do miejsca, w którym przebywa personel. Na wyświetlaczach terminali systemowych w pobliżu personelu i telefonach przenośnych DECT/VoIP pojawia się informacja, z której sali nadano sygnał. Lekarz, pielęgniarka lub inne osoby z personelu od razu wiedzą, kto potrzebuje pomocy (pacjent albo osoba z personelu) oraz znają dokładną lokalizację miejsca przywołania. Mogą niezwłocznie porozmawiać z pacjentem i dowiedzieć się, czego dotyczy przywołanie, a następnie udać się na miejsce lub oddelegować inną osobę albo też zdalnie skasować przywołanie.
System przyzywowy i system telefonów medycznych można zintegrować z systemem sygnalizacji pożarowej w celu przekazywania szczegółowych informacji o zagrożeniu pożarowym. Ze względu na brak w salach chorych dźwiękowego systemu ostrzegawczego (DSO) umożliwi to grupowe ogłaszanie komunikatów bezpośrednio przy łóżkach pacjentów, a także na terminalach zainstalowanych przy drzwiach wejściowych do sal i pomieszczeń personelu. Personel będzie mógł szybciej otrzymać informację o zagrożeniu pożarowym, by przygotować pacjentów do ewakuacji.

Opisane w artykule systemy odpowiadają za ochronę przeciwpożarową obiektu oraz bezpieczeństwo personelu i pacjentów w nim przebywających. Integracja systemów zwiększa bezpieczeństwo pacjentów chociażby dzięki usprawnieniu procedury przygotowania personelu do podjęcia czynności związanych z ewakuacją chorych ze szpitala podczas pożaru. □

LITERATURA

[1] https://rcb.gov.pl/infrastruktura-krytyczna/
[2] Rozporządzenie Ministra Infrastruktury z 12 kwietnia 2002 r. w sprawie warunków technicznych, jakim powinny odpowiadać budynki i ich usytuowanie (Dz.U. z dn. 18.09.2015 poz. 1422).
[3] Rozporządzenie MSWiA z 7 czerwca 2010 r. w sprawie ochrony przeciwpożarowej budynków, innych obiektów budowlanych i terenów (Dz.U. z dn. 22.06.2010 nr 109, poz. 719).
[4] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 24 lipca 2009 r. w sprawie przeciwpożarowego zaopatrzenia w wodę oraz dróg pożarowych (Dz.U. 2009 nr 124, poz. 1030).

Schrack Seconet Polska

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

Wyjątkowa liniowa czujka dymu FireBeam *Xtra* CR

Ruchy i drgania konstrukcji budynków wielkokubaturowych są źródłem problemów w eksploatacji liniowych czujek dymu. Systemy wykorzystujące czujki starej technologii są uciążliwe w użytkowaniu i powodują liczne fałszywe alarmy. Czujka FireBeam Xtra CR pozwala na eliminację tych problemów.

Co mamy na myśli, mówiąc o wyjątkowych rozwiązaniach zastosowanych w czujce FireBeam Xtra CR?

To najbardziej zaawansowana technologicznie liniowa czujka dymu dostępna obecnie na rynku. Należy przede wszystkim podkreślić możliwość automatycznej kompensacji odchylenia wiązki pomiarowej aż o ±5° na nieosiągalnym dla innych optycznych czujek liniowych dystansie 160 m. Dzięki temu nie ma potrzeby dokonywania ręcznych korekt pozycji wysoko zawieszonej czujki po każdej zmianie geometrii konstrukcji budynku powodowanej ciągle zmieniającymi się warunkami atmosferycznymi lub drganiami występującymi w czasie normalnej eksploatacji obiektu.

Dostępny z poziomu podłogi panel wyniesiony czujki FireBeam Xtra pozwala znacząco zmniejszyć koszty eksploatacji. Co ważne, jego obecność nie jest potrzebna do pracy czujki po jej uruchomieniu. Za pomocą panelu operator systemu może szybko i sprawnie skontrolować stan urządzeń oraz przeprowadzić okresowe testy bez potrzeby użycia podnośnika, kolejno podłączając się do zainstalowanych czujek. Wyeliminowano tym samym problemy związane z pracą na wysokości i kosztowne przerwy w użytkowaniu chronionego obiektu. Dodajmy, że przeszkolony instalator może jednocześnie uruchamiać i kalibrować nawet do 25 czujek (ok. 56 tys. m² chronionej powierzchni) w średnim czasie 14 min przypadającym na urządzenie!

Dzięki redukcji liczby czujek na obiekcie dbamy o środowisko naturalne – jedna czujka FireBeam Xtra CR może zastąpić nawet do 26 czujek punktowych bez obawy o pogorszenie bezpieczeństwa.

Dlaczego Xtra?

Xtra uniwersalność: Dzięki zastosowaniu otwartej platformy oraz prostej parametryzacji bezproblemowo współpracujemy z dowolnym systemem SAP obecnym na europejskim rynku.

Xtra zgodność: Spełniamy wszystkie najnowsze wymagania normy EN54-12!

Xtra niezawodność: Czujka FireBeam Xtra CR o stopniu ochrony IP65 jest odporna na działanie czynników zewnętrznych. Dzięki temu można ją stosować w miejscach, gdzie warunki środowiskowe są nadzwyczaj wymagające.

Możemy pochwalić się m.in. jej bezawaryjnym działaniem w hali produkcyjnej przetwórni żywności regularnie czyszczonej strumieniami wody. IP65 oznacza nie tylko barierę dla wilgoci czy zapylenia, ale również dla owadów mogących zakłócić pracę czujki.

Xtra ekologia: Czujka ma ledwie zauważalne zużycie prądu niezależnie od stanu pracy – podczas dozoru, alarmowania czy sygnalizacji uszkodzenia pobór prądu jest stały i wynosi jedynie 3,5 mA. Dzięki temu w instalacji można zastosować mniejszą liczbę zasilaczy, co wpływa na redukcję kosztów zasilania i optymalizację energetyczną obiektu.

Xtra obsługa: Zrezygnowaliśmy z niezrozumiałych piktogramów, ponieważ komfort użytkownika jest dla nas równie ważny jak jego bezpieczeństwo – wszystkie komunikaty są wyświetlane w formie tekstowej w języku polskim.

Xtra kalibracja: Kalibracja wstępna jest dokonywana na podstawie zastanych warunków środowiskowych pomieszczenia, czyli tła. Uwzględnia się wszelkie niuanse chronionego obiektu, od sposobu ułożenia ścian i legarów, aż po rodzaj materiału, z którego wykonano pomieszczenie. Po kalibracji wstępnej przeprowadzana jest kalibracja właściwa – już z użyciem odbłyśnika.

Xtra unikatowość: Urządzenie jest dostępne również w wykonaniu AntiFog, co oznacza, że para wodna nie będzie osiadała na elementach optycznych czujki.

–

Podczas targów Securex 2020 oficjalnie zaprezentujemy możliwości czujki FireBeam Xtra CR po raz pierwszy w Europie. Zapraszamy na nasze stoisko w listopadzie.

CREATIO
ul. Różyckiego 1c p.229
51-608 Wrocław
www.creatioindustry.pl

PRYWATNOŚĆ BY DESIGN KONTRA OCHRONA DANYCH BY DESIGN

Dlaczego nadinterpretujemy RODO?

WARTO PORUSZYĆ DWA ZAGADNIENIA ZWIĄZANE ZE STOSOWANIEM RODO I PRZEPISÓW ZWIĄZANYCH: POWSZECHNEJ, CZASAMI PROWADZĄCEJ DO ABSURDÓW, NADINTERPRETACJI RODO ORAZ PEWNEJ NONSZALANCJI W STOSOWANIU POJĘĆ: PRYWATNOŚĆ I OCHRONA DANYCH.

TEKST

Waldemar Więckowski

O RODO – ogólnym rozporządzeniu o ochronie danych – w a&s Polska pisano już kilkakrotnie. Wcześniej w numerach 5/2017 [1], 6/2017 [2], 3/2018 oraz 4/2018 [3] [4], ostatnio w nr 6/2019 [5] i 1/2020 [6] – piórem zarówno autorów zawodowo funkcjonujących głównie w branży zabezpieczeń, jak i poza nią.

Tematykę RODO przedstawiano – co oczywiste – zasadniczo w ujęciu praktyki stosowania przepisów tego prawa w dziedzinie zabezpieczeń, głównie w dozorze (monitoringu) wizyjnym i kontroli dostępu, czasami stawiając na pierwszym planie zagadnienie ochrony prywatności (praw osób fizycznych), a czasami uwypuklając konieczność uzyskania balansu pomiędzy ochroną danych a zapewnieniem bezpieczeństwa. Odwołania do RODO zawarto także w wielu artykułach firmowych, odnosząc je do prezentowanych wyrobów i rozwiązań. W każdym razie Czytelnik a&s Polska, praktykujący w zabezpieczeniach, otrzymał rzeczową informację o przepisach. Nie poruszono jednak dwóch ważnych zagadnień: powszechnej nadinterpretacji RODO i pewnej nonszalancji w stosowaniu pojęć: prywatność i ochrona danych.

Dlaczego nadinterpretujemy RODO

Zjawisko nadinterpretacji RODO było i nadal jest dyskutowane dosyć szeroko w przestrzeni publicznej, ponieważ mamy z nim powszechnie do czynienia w sprawach codziennych. Nadinterpretacja RODO występuje również w praktyce branży zabezpieczeń, i to na dwóch płaszczyznach. Pierwsza to relacje biznesowe pomiędzy zamawiającym a dostawcą. Ponieważ te relacje w zabezpieczeniach nie różnią się niczym od takich relacji w innych branżach, w razie różnicy zdań można odwołać się do argumentów przedstawionych w dyskusji publicznej, zwłaszcza że odnośne organy państwa przedstawiły szereg wyjaśnień i komentarzy [7] [8]. Druga płaszczyzna to dostarczany przez branżę zabezpieczeń produkt. Ponieważ jest on specyficzny dla branży (co oczywiste), to w kwestii, czy spełnia on wymagania RODO, zasadniczo nie można się odwołać do praktyki innych branż. Musimy sobie radzić sami, wypracowując własną praktykę.

Rzeczą oczywistą jest, jakie znaczenie dla jego stron ma właściwie sformułowany kontrakt. Właściwie, tzn. tak, że po jego zrealizowaniu zyskują obie strony. Aby nie popełnić błędu przy opisie przedmiotu dostaw, a także by wiedzieć u kogo – w razie konieczności – szukać porady w kwestiach RODO, dobrze jest mieć świadomość, jakie jest powszechne podejście do tych przepisów. W tej kwestii interesującą opinię sformułował w rozmowie radiowej przeprowadzonej przez Przemysława Iwańczyka dr Maciej Kawecki, dziekan Wyższej Szkoły Bankowej w Warszawie, w latach 2017–2019 koordynator krajowej reformy ochrony danych osobowych, a w latach 2018–2019 dyrektor departamentu zarządzania danymi w Ministerstwie Cyfryzacji:

My w ogóle jako Polacy bardzo literalnie podchodzimy do prawa, tzn. jeżeli mamy pewną regulację, to bardzo lubimy ją nadinterpretować. To jest nasza narodowa bolączka. (...) W temacie RODO wynika to z pewnego kryzysu na rynku usług prawniczych, tzn. wejście w życie w Polsce RODO trafiło na okres bardzo dużego krachu na rynku usług prawniczych. To spowodowało, że wejście w życie tej regulacji urodziło stworzenie gigantycznej ilości różnych firm konsultingowych, doradczych, czasami na lepszym poziomie, czasami na gorszym poziomie, które troszkę podsycały tę atmosferę. Czyli trochę absurdy rozdmuchiwały, jakby szukając trochę wyjścia do zarobku. (...) To jest przyczyna w Polsce. Plus taka jakaś nasza cecha takiego literalnego bardzo podchodzenia do przepisów. To nie oznacza przestrzeganie przepisów, to oznacza czasami nadinterpretację, wyinterpretowywanie treści, których w nich nie ma. I z taką sytuacją mamy do czynienia w RODO. (...)

(Fragment w transkrypcji własnej autora niniejszego artykułu; całość do odsłuchania na [9].)

Wchodząc w relacje biznesowe, raczej nie możemy mieć wpływu na mentalność i podejście naszych rodaków do prawa, ale na wybór kontrahentów, w tym przede wszystkim konsultantów i doradców, już tak.

Czym innym jest prywatność, a czym innym ochrona danych osobowych

Słowo prywatność jest przy okazji RODO „odmieniane przez wszystkie przypadki" i niemal nie ma kontekstu ochrony danych osobowych, w którym by się nie pojawiło. Nader często – również w branży zabezpieczeń – jest stosowane zamiennie do danych osobowych. Czy słusznie?

W cytowanej wyżej rozmowie dr Maciej Kawecki stwierdza: (...) *prywatność jest wartością, którą my jako ludzie chronimy od zawsze (...). Więc ta prywatność jest gdzieś w nas bardzo głęboko zakorzeniona. I potrzeba prywatności. Ale czym innym są dane osobowe. I nie do końca jest tak, że dane osobowe są wartością bezwzględną, a dzisiaj są lansowane jako wartość bezwzględna. Natomiast musimy cały czas pamiętać o tym, że obok danych osobowych mamy jeszcze szereg przeróżnych wartości, które bardzo często w konflikcie wygrywają.*

W uzasadnieniu do ustawy o ochronie danych osobowych, dokumencie datowanym 13.09.2017, ujęto tę różnicę w sposób następujący: *W doktrynie i orzecznictwie nie budzi wątpliwości, iż naruszenie danych osobowych stanowi jednocześnie naruszenie dóbr osobistych. Art. 23 k.c. zawiera otwarty katalog dóbr osobistych. Natomiast dane osobowe ujmowane są jako kategoria dobra osobistego – prywatności. Dane osobowe nie mają więc charakteru samoistnego dobra osobistego. (...) Jednocześnie w piśmiennictwie podkreśla się, iż prywatność jest pojęciem wieloznacznym, trudnym do zdefiniowania (...).*

Jak się wydaje, już tylko te przywołane stanowiska powinny wystarczyć jako uzasadnienie, dlaczego nie powinniśmy stosować zamiennie pojęć „ochrona danych" i „prywatność".

Nie ma *prywatności* w RODO

Termin „prywatność" nie występuje w RODO (Rozporządzeniu Parlamentu Europejskiego i Rady UE2016/679 z 27 kwietnia 2016 r.) ani w krajowej Ustawie z 10 maja 2018 r. o ochronie danych osobowych. Ten termin był stosowany w dokumentach poprzedzających RODO, obecnie wycofanych, tj. w:

1) Dyrektywie 95/46/WE Parlamentu Europejskiego i Rady z 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, data końca ważności 24/05/2018;

2) Ustawie z 29 sierpnia 1997 r. o ochronie danych osobowych, uchylonej 25.05.2018.

Termin prywatność w odniesieniu do ochrony danych osobowych po raz ostatni pojawił się w dokumencie bezpośrednio poprzedzającym RODO, tj. we Wniosku Rozporządzenia Parlamentu Europejskiego i Rady (UE) w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych). Ten wniosek został złożony 25.01.2012 z terminem zakończenia jego ważności 27.04.2016.

Skoro po tak długim okresie stosowania terminu prywatność w odniesieniu do ochrony danych osobowych Parlament Europejski i Rada (UE) zdecydowały się ostatecznie usunąć go z RODO, to przyczyny nie mogą być drugorzędne.

Privacy by design czy Data Protection by Design

Informacja o *Privacy by Design* znajduje się w wielu różnych źródłach. Jednak z punktu widzenia branży zabezpieczeń najbardziej przydatny opis – moim zdaniem – znalazł się w Opinii 5/2018 r. Europejskiego Inspektora Ochrony Danych [10]. (Opinia 5/2018 nie została opublikowana w wersji polskojęzycznej – tłumaczenie fragmentów własne). W dokumencie tym *Privacy by Design* określono jako „szerokie pojęcie odnoszące się do środków technologicznych służących zapewnieniu prywatności" *(the broad concept of technological measures for ensuring privacy)*, zaś *Data Protection by Design* jako „określone obowiązki prawne ustanowione w Artykule 25 RODO" *(the specific legal obligations established by Article 25 of the GDPR)*. I dalej: „Chociaż środki podjęte celem spełnienia tych obowiązków również przyczynią się do osiągnięcia bardziej ogólnego celu *privacy by design*, uważamy, że szersze spektrum przedsięwzięć może być wzięte pod uwagę dla osiągnięcia celu *privacy by design*, który posiada wymiar wizjonerski i etyczny, spójny z zasadami i wartościami zapisanymi w Karcie praw podstawowych Unii Europejskiej" *(While measures taken under these obligations will also contribute to achieving the more general objective of „privacy by design", we consider that a wider spectrum of approaches may be taken into account for the objective of „privacy by design" which includes a visionary and ethical dimension, consistent with the principles and values enshrined in the EU Charter of Fundamental Rights of the EU)*.

(Syntetyczna informacja o *Privacy by Design* znajduje się także w publikacji GIODO „Czy jesteś gotowy na RODO?"[11])

Byty wirtualne: uwzględnienie ochrony danych w fazie projektowania (*Privacy by Design*)

Różnica pomiędzy *Privacy by Design* i *Data Protection by Design* została najbardziej czytelnie przedstawiona przez Europejskiego Inspektora Ochrony Danych we wspomnianej już Opinii opublikowanej w maju 2018 r. Tymczasem po prawie 4 latach od ogłoszenia RODO i ponad 1,5 roku jego obowiązywania, nadal powszechny jest przekaz, że aby dany system, w którym dochodzi do przetwarzania danych osobowych, spełniał wymagania RODO, powinien zapewnić *Privacy by design* i *Privacy by default*. Jest to uprawnione wymaganie w dyskusji o prawach podstawowych EU, ale nie przy formułowaniu wymagań użytkowych stawianych konkretnym urządzeniom i systemom. Z kolei w kontekście rozróżnienia przedstawionego przez Europejskiego Inspektora Ochrony Danych określenia typu „uwzględnienie ochrony danych w fazie projektowania (*Privacy by Design*)" są bytem wirtualnym, już choćby z tego najprostszego powodu, że „uwzględnienie ochrony danych w fazie projektowania" to po angielsku zgodnie z art. 25 RODO *Data protection by design a nie Privacy by design*.

Branża zabezpieczeń spod tego przekazu nie jest wyjęta, nawet jeżeli nie jest on kierowany bezpośrednio do niej. Niewątpliwie nasza branża oferuje systemy, w których dochodzi do przetwarzania danych osobowych (np. systemy dozoru wizyjnego czy systemy kontroli dostępu), choć na co dzień nazywamy je (zgodnie z ustawą) systemami technicznej ochrony osób i mienia. W tej sytuacji istotne jest wiedzieć, które wymagania stawiane przed systemami securi-

Fot. 1 i 2. Privacy by design. Fizyczny ekran przysłaniający pole widzenia kamery jako skuteczny sposób zapewnienia „strefy prywatności" i przekazania informacji o jej stworzeniu

ty są rzeczywistymi wymaganiami stawianymi przez RODO, a które wirtualnymi, wymyślonymi przy okazji pod kątem innych potrzeb.

RODO Art. 25: Data protection by design and by default

W tytule niniejszego rozdziału celowo przytaczam angielskojęzyczny nagłówek tego artykułu RODO, ponieważ zawarte w nim wymaganie pojawia się w kraju częściej w tej wersji niż w jej oficjalnym polskojęzycznym odpowiedniku: Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych.

Z treści art. 25 jednoznacznie wynika, że wymaganie to dotyczy administratora (!) danych – produkt branży zabezpieczeń jest uwzględniony pod określeniem „odpowiednie środki techniczne", które wdraża administrator. Zadaniem branży zabezpieczeń jest więc dostarczyć owe odpowiednie środki techniczne. Tylko tyle i aż tyle.

Na pytanie, dlaczego nadal w odniesieniu do ujętego w RODO prawnego wymagania ochrony danych osobowych powszechnie powielane są wymagania *Privacy by design* i *Privacy by default*, jest wiele możliwych odpowiedzi. Pierwsza – skrajna – to nienależyta staranność autora wymagania, w którym te określenia występują. Tak bardzo przyzwyczajono się do terminu prywatność stosowanego w odniesieniu do ochrony danych w poprzednio obowiązujących regulacjach, że nie zauważono, że RODO już go nie stosuje.

Pewnym dysonansem w tej wersji odpowiedzi jest fakt, że w poprzedniej regulacji nie stosowano pojęć *privacy by design* i *privacy by default* (w specjalistycznej dyskusji pojawiły się one w latach 90., ale odnosiły się nie do wymagań prawnych, lecz do domyślnego sposobu funkcjonowania organizacji) [12]. Druga skrajna odpowiedź to działanie intencjonalne. Jak napisano w (cytowanym wyżej) uzasadnieniu do ustawy o ochronie danych osobowych „Jednocześnie w piśmiennictwie podkreśla się, iż (...) Prywatność jest pojęciem wieloznacznym, trudnym do zdefiniowania (...) A skoro tak, to szkolić, konsultować i doradzać można będzie bez końca". Wskazuje na to dr Kawecki w cytowanej rozmowie, odnosząc to do praktyki krajowej. Ale wystarczy wrzucić w Google hasło *Privacy by design* lub *Privacy by default*, żeby przekonać się, jak wielu jest chętnych do przeszkolenia nas z tego tematu i tu, i za granicą.

Guidelines 4/2019 on Article 25 Data protection by design and by default

Bardzo dobra wiadomość dla dostawców rozwiązań security (a niekoniecznie dla wyżej wymienionych konsultantów i doradców) jest taka, że Europejska Rada Ochrony Danych [13] przygotowała dokument *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*. Do 16 stycznia 2020 trwały konsultacje publiczne (projektu) tych wytycznych. Na razie nie wiadomo, jaka będzie ostateczna (!) treść tych wytycznych i kiedy się one ukażą w wersji przyjętej po konsultacjach publicznych. Tym niemniej już teraz można pobrać udostępnioną treść projektu (ze strony EDPB) i skorzystać z wiedzy źródłowej.

Guidelines 3/2019 on processing of personal data through video devices

Druga bardzo dobra wiadomość, w szczególności dla branży zabezpieczeń, również pochodząca ze strony Europejskiej Rady Ochrony Danych to publikacja wytycznych wskazanych w tytule niniejszego rozdziału. Wersję w języku angielskim (2.0) przyjęto 29 stycznia 2020 r., na razie nie wiadomo, kiedy będzie wersja polskojęzyczna.

RODO wymyśliliśmy już w 1997 r.

Prowadzący cytowaną rozmowę radiową Przemysław Iwańczyk postawił – przyjętą przez obu rozmówców jako żart – tezę, że Polacy, zanim powstała jakakolwiek regulacja, już RODO wymyślili. A było to w czasie, kiedy w budynkach wielomieszkaniowych likwidowano listy lokatorów, a z ogólnego użytku wycofano książki telefoniczne (zawierające także adresy i nazwiska właścicieli numerów telefonicznych). Jak przypomniał dr Kawecki, uczyniono to w sierpniu 1997 r., implementując pakiet regulacyjny, który miał Polskę wprowadzić do Unii Europejskiej. Jednym z objętych tym pakietem obszarów była właśnie prywatność.

Panowie nie przywołali nazwy wprowadzonej w Polsce w 1997 r. regulacji dotyczącej prywatności, ale łatwo można się domyślić, że chodzi o Ustawę z 29 sierpnia 1997 r. o ochronie danych osobowych, która była wdrożeniem Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych.

Ponieważ ta dyrektywa dotyczyła wszystkich państw członków Unii Europejskiej, to czym, jak nie skłonnością do nadinterpretacji, wytłumaczyć fakt, że listy lokatorów zniknęły u nas z klatek schodowych w roku 1997 (7 lat przed naszym wejściem do UE), a np. w Wiedniu jeszcze 28 sierpnia 2018 r. nadal wisiały (*fot. 3*). □

Fot. 3. Lista lokatorów z budynku w Wiedniu (28.08.2018 r.)

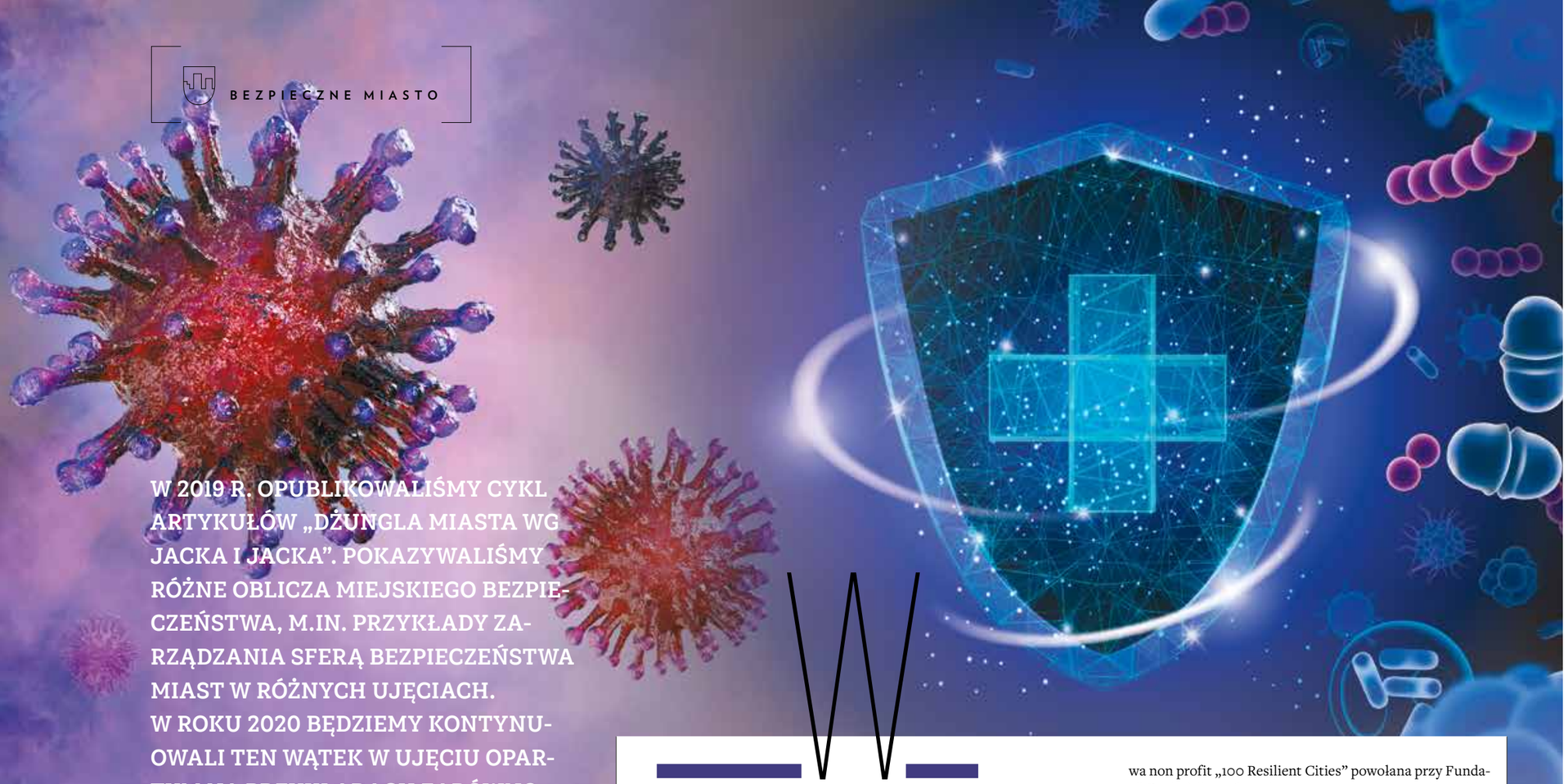
LITERATURA:

[1] M. Blim, RODO – jak nadzorować prowadzenie i ochronę zbiorów danych osobowych, a&s Polska, nr 5/2017.
[2] M. Blim, NUODO projekt polskiej ustawy i zmiany wobec dotychczasowych wymagań UODO, a&s Polska, nr 6/2017.
[3] P. Wittich, Nie bój się RODO w monitoringu! a&s Polska, nr 4/2018.
[4] A. Popielski, Kamery w świetle RODO, a&s Polska, nr 4/2018.
[5] P. Powązka, RODO w monitoringu wizyjnym, a&s Polska, nr 6/2019.
[6] A. Marcinkowska, A. Żyrek, Komunikacja za pomocą systemów przyzywowych a ochrona prywatności i godności pacjenta, a&s Polska, nr 1/2020.
[7] MIiR wprowadza program RODOracjonalność. Celem obalenie mitów o RODO, https://biznes.gazetaprawna.pl/artykuly/1196905,rodo-mity-i-stereotypy-ministerstwo-rozwoju.html [data dostępu: 30.07.2018].
[8] K. Żaczkiewicz-Zborska, M. Kawecki, Ustawa wprowadzająca porządkuje niejasności wokół RODO, https://www.prawo.pl/prawo/grozenie-kara-finansowa-staje-sie-karalne,375611.html, [data dostępu: 22.02.2019].
[9] O bezpieczeństwie w sieci mówi dr Maciej Kawecki, audycja TOKFM, data emisji 31.12.019, godz. 10:00, prowadzący Przemysław Iwańczyk, https://audycje.tokfm.pl/podcast/84776,Kawecki-Wartosc-danych-osobowych-po-raz-pierwszy-przekroczyla-wartosc-ropy-naftowej-Polacy-kroluja-w-swiadomosci-czym-one-sa-ale-tez-w-absurdalnym-podejsciu-do-tego-na-co-pozwala-RODO.
[10] Preliminary opinion on privacy by design, European Data Protection Supervisor, Opinion 5/2018, 31 May 2018
[11] Czy jesteś gotowy na RODO? Generalny Inspektor Ochrony Danych Osobowych (GIODO), 2017-12-04, https://archiwum.giodo.gov.pl/pl/1520281/10255
[12] Privacy by Design, The 7 Foundational Principles Ann Cavoukian, Information & Privacy Commissioner of Ontario, Canada, Originally Published: August 2009
[13] https://edpb.europa.eu/about-edpb/about-edpb_pl

BIO

Waldemar Więckowski

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



W 2019 R. OPUBLIKOWALIŚMY CYKL ARTYKUŁÓW „DŻUNGLA MIASTA WG JACKA I JACKA". POKAZYWALIŚMY RÓŻNE OBLICZA MIEJSKIEGO BEZPIECZEŃSTWA, M.IN. PRZYKŁADY ZARZĄDZANIA SFERĄ BEZPIECZEŃSTWA MIAST W RÓŻNYCH UJĘCIACH. W ROKU 2020 BĘDZIEMY KONTYNUOWALI TEN WĄTEK W UJĘCIU OPARTYM NA PRZYKŁADACH ZARÓWNO ZASTOSOWAŃ W WYBRANYCH MIASTACH, JAK I NARZĘDZI TEN PROCES WSPIERAJĄCYCH.

Przetrwają odporni!

Niech „wirusy słabości" odbiją się od tarczy zabezpieczeń

Wszyscy przeżywamy bardzo groźny kryzys związany z rozprzestrzeniającą się pandemią koronawirusa z Wuhan. To miasto jest stolicą prowincji Hubei, znaczącego ośrodka biznesowego i administracyjnego. Wuhan z liczbą 11 mln mieszkańców swoją skalą być może nie robi wrażenia w Chinach, ale w Europie byłaby to ogromna mietropolia (w pierwszej trójce największych), przekraczająca liczbą ludności co najmniej kilka Państw europejskich.

Z przerażaniem czytamy o rozprzestrzeniającej się chorobie i zgonach, o zamknięciu miasta dla podróżujących, budowanych naprędce szpitalach i licznych narzędziach kontroli. Teraz sami zmagamy się z epidemią. Po pewnym czasie dowiemy się, jakie narzędzia kontroli społecznej musiały być zastosowane w Wuhan, żeby opanować rozwój choroby. „Bezpiecznik" to ktoś, kto musi być liderem w czasie trudnym, kryzysowym. Z pewnością będziemy się uczyć na tym przykładzie.

Na początku roku Australia borykała się z katastroficznymi pożarami, które wstrząsnęły światem. Wszyscy podziwialiśmy poświęcenie strażaków, żołnierzy i zwykłych obywateli, którzy walczyli z żywiołem. Na szczęście spadł deszcz i poradzono sobie z pożarami.

Od kilku lat obserwujemy dynamicznie rozwijający się model analizy i zarządzania miejskim życiem, nazywany odpornością lub, posługując się terminem angielskim, *Urban resilience*.

Jedną z pierwszych organizacji zajmujących się w sposób metodyczny miejską odpornością była inicjatywa non profit „100 Resilient Cities" powołana przy Fundacji Rockefellera. Stosuje ona opracowane przez brytyjską pracownię urbanistyczno-architektoniczną Arup narzędzie znane jako City Resilient Index. Metodologia ta pomaga miastom na całym świecie zbadać ich poziom odporności na różne zagrożenia i wyzwania. Co ciekawe, tradycyjnie postrzegane przez „bezpieczników" zagrożenia kryminalne, terrorystyczne, ważą w tym rankingu mniej niż wyzwania z obszaru zanieczyszczenia środowiska, pandemii, dostaw wody, prądu oraz cyberprzestępstw.

Odporność miejska staje się również przedmiotem zainteresowania państw i ich organizacji, takich jak Organizacja Narodów Zjednoczonych czy Unia Europejska. ONZ ma swoją agendę badawczą UNHABITAT monitorującą kwestie wyzwań w przestrzeni miejskiej, głównie w krajach słabo rozwiniętych. Z tego powodu uczestnicy finansowanego z funduszy UE projektu TURAS (*Transitioning towards urban resilience and sustainability*) nawiązali współpracę z podmiotami miejskimi, aby wspólnie stawić czoło wyzwaniom związanym ze zrównoważonym rozwojem miast.

W cyklu artykułów zaprezentujemy zarówno programy i strategie wybranych miast, jak i narzędzia, technologie i rozwiązania metodologiczne. Przybliżymy czytelnikom strategie i narzędzia stosowane w Bangkoku, Glasgow, Nowym Jorku, Rotterdamie, Rio de Janeiro. Z naszego krajowego podwórka pokażemy przykład Krakowa, który co prawda nie ma strategii odporności w rozumieniu metodologii „100RC", ale grupa badawcza z UJ wraz z władzami miasta od lat prowadzi badania nad miejskim bezpieczeństwem. Każde z miast ma własne priorytety odporności wynikające z ich specyfiki, każde buduje własne indywidualne strategie spełniające ich cele.

TEKST
Jacek Tyburek

Bangkok
to 8-milionowe miasto z zespołem metropolitalnym przekraczającym 14 mln mieszkańców. Cała Tajlandia, w tym Bangkok, jest najpopularniejszą turystyczną destynacją na świecie. Królestwo bije rekord za rekordem i wg szacunków w 2019 r. odwiedziło je blisko 40 mln zagranicznych turystów. To już prawie trzykrotnie więcej niż jeszcze 10 lat temu, gdy tajską granicę przekraczało 14,6 mln obcokrajowców. Tego rodzaju skok jest powodem do zadowolenia, ale również zmartwieniem dla władz. Przychody z turystyki są ogromne, ale jednocześnie istnieje spore zagrożenie, że ten raj na ziemi zostanie zniszczony przez turystów.

Dlatego też strategia odporności Bangkoku jest ukierunkowana, a jej ciężar gatunkowy przeniesiony na kwestie środowiskowe. Strategia odporności ma trzy zasadnicze obszary działania:

1. Podnoszenie jakości życia w mieście poprzez:
- zapewnienie zdrowia i dobrostanu wszystkim mieszkańcom (nie tylko Tajów) obecnie i w przyszłości,
- bezpieczną, dostępną i wygodną sieć transportu miejskiego,
- urbanizację terenów włączanych do miasta w sposób przyjazny dla środowiska.

2. Ograniczanie ryzyka i podnoszenie poziomu dostosowania się do wyzwań poprzez:
- lepsze przygotowanie przed powodziami,
- poprawę miejskich i społecznościowych przygotowań do akcji kryzysowych,
- wzmocnienie instytucji odpowiedzialnych za przeciwdziałanie ryzyku i kryzysom.

3. Stałe dbanie o ekonomiczną atrakcyjność miasta i jego przewagi konkurencyjne:
- wdrożenie ułatwień w prowadzeniu biznesu,
- ciągłe rozwijanie turystyki, sfery usług turystycznych i podniesienie jakości pobytu turystów w Bangkoku.

Glasgow,
najważniejsze miasto Szkocji, liczące blisko 600 tys. mieszkańców, przeszło dogłębny proces konsultacji wewnętrznych z grupą ponad 3,5 tys. mieszkańców wytypowanych do partycypacji w tworzeniu założeń strategii odporności miejskiej. Opiera się ona na czterech „strategicznych filarach" i piętnastu „celach" wyznaczających długoterminową trajektorię odporności Glasgow. W związku z tym zidentyfikowano 49 działań, które zostaną wdrożone w ciągu najbliższych dwóch lat.

FILAR PIERWSZY:	DRUGI FILAR	TRZECI FILAR	CZWARTY FILAR
Poprawienie i zagwarantowanie równego dostępu do usług lokalnych przy wzmocnieniu pozycji liderów społeczności oraz stworzenie bezpiecznej przestrzeni. Filar ten ma się zmaterializować w następujących działaniach:	strategii zawiera się w postulacie stworzenia przykładu odporności, zmierzenia się z lokalnymi skutkami zmian klimatu i uwolnienia potencjału pustych miejsc. Ma on zostać zrealizowany poprzez:	jest ukierunkowany na ekonomiczny rozwój Glasgow. Jego zadaniem jest wspieranie nowych rozwiązań miasta i firm oraz uczenie się na podstawie najlepszych praktyk i zwiększanie umiejętności mieszkańców. Cel ma zostać zrealizowany poprzez:	strategii Glasgow koncentruje się wokół aktywizacji mieszkańców do ich głębszej partycypacji w budowę odpornego miasta.
– zapewnienie równego dostępu do wysokiej jakości lokalnych usług, które sprzyjają dobrobytowi, – wzmocnienie pozycji liderów społeczności we współpracy między partnerami miast i trzecim sektorem, – wykorzystanie istniejących zasobów, aby stworzyć zdrowe, bezpieczne i sprzyjające integracji miejsca dla społeczności w sieci, pomagające zmniejszyć izolację społeczną, – wpływ na program rządu szkockiego w zakresie odporności społecznej i społecznej.	– poprawę jakości powietrza i zmniejszenie emisji węgla, – połączenie infrastruktury transportowej dla firm i społeczności, – udostępnienie niedrogich i ekologicznych sposobów przemieszczania się w Glasgow, – efektywną energetycznie przyszłość, – inwestycje i miejsca pracy w społecznościach lokalnych, – dobry dostęp do infrastruktury fizycznej i cyfrowej.	– ułatwienie rozwoju kreatywnych i innowacyjnych rozwiązań miejskich zwiększających wartość fizyczną, społeczną i ekonomiczną tkanki Glasgow, – wspieranie rozwoju nowych i istniejących firm dzięki nowemu podejściu do przedsiębiorstwa, – założenie postindustrialnej podgrupy miasta z partnerami „100RC", by dzielić się najlepszymi praktykami i uczyć się na nich, – przeciwdziałanie ubóstwu, m.in. ubóstwu pracujących, zapobieganie skutkom ubóstwa mieszkańców razem z mieszkańcami Glasgow oraz łagodzenie ich skutków, – podnoszenie poziomu umiejętności ludności w wieku produkcyjnym.	

Nowy Jork

Tej metropolii nie trzeba przedstawiać. O Nowym Jorku Frank Sinatra śpiewał, że nigdy nie śpi. Organizacja „100RC" ma tu swoją siedzibę, więc siłą rzeczy Wielkie Jabłko jest wzorcem i inspiracją zarządzania miastem z perspektywy odporności. Jednak od lat przegrywa wyścigi wśród światowych megapolis. Strategia odporności Nowego Jorku opiera się na czterech założeniach:

1. pozostania najbardziej dynamiczną gospodarką miejską na świecie, w której kwitną rodziny, firmy i dzielnice. Aby zaspokoić potrzeby zwiększającej się populacji w czasach rosnących kosztów, miasto wdroży najbardziej ambitny w kraju program dotyczący tworzenia i zachowania tanich mieszkań. Będzie wspierać ten najważniejszy sektor komercyjny XXI w.;
2. wprowadzenia integracyjnej, sprawiedliwej gospodarki oferującej dobrze płatne miejsca pracy oraz możliwości, godność i bezpieczeństwo dla wszystkich. Do 2025 r. miasto zamierza wydobyć z ubóstwa lub bliskiego ubóstwa 800 tys. nowojorczyków, walcząc o podwyżkę płacy minimalnej i podejmując ważne inicjatywy wspierające edukację i wzrost zatrudnienia. Będzie dążyć do zmniejszenia przedwczesnej śmiertelności o 25 proc. do 2040 r., zapewniając wszystkim nowojorczykom dostęp do usług opieki fizycznej i psychicznej, zajmując się zagrożeniami w domach i ich bezpośrednim otoczeniu;
3. osiągnięcia pozycji najbardziej zrównoważonego dużego miasta na świecie i tytułu światowego lidera w walce ze zmianami klimatu;
4. przygotowania na niekorzystne zdarzenia, takie jak huragan Sandy, reagowania na nie, zapewnienia podstawowych funkcji i usług wszystkim mieszkańcom, a także wzmocnienia się jako wspólnota w celu wyeliminowania długoterminowego wysiedlenia z domów i miejsc pracy po zdarzeniach szokowych do 2050 r.

Rotterdam,

portowe miasto w Holandii, jest jednym z najważniejszych ośrodków miejskich zarówno w kraju, jak i całej Europie. Wynika to z wysokiego poziomu gospodarki tego kraju oraz jego kulturowej, naukowej i biznesowej atrakcyjności. Twórcy strategii odporności Rotterdamu zastosowali pewne założenie, stanowiące manifest i jednocześnie adresujące cele do zrealizowania przez miasto. W 2030 r. Rotterdam będzie miastem, w którym:

- silni obywatele szanują się nawzajem, stale się rozwijając,
- infrastruktura energetyczna zapewnia wydajne i zrównoważone dostawy energii w porcie i mieście,
- dostosowanie klimatu znalazło się w głównym nurcie działań miasta, woda stanowi wartość dodaną dla miasta, a system zarządzania wodą jest cyberoodporny,
- wykorzystuje się tereny podziemne, by wspierały rozwój miasta,
- wdrażając szeroko cyfryzację, nie uzależniając się od niej, miasto zapewni najwyższy poziom najlepszych praktyk w zakresie bezpieczeństwa cybernetycznego,
- samoorganizacja w mieście jest wystarczająca, a elastyczny rząd samorządowy wspiera ją,
- odporność miejska jest częścią codziennego myślenia, planowania i działania.

Rio de Janeiro

Ta metropolia w Brazylii wielu kojarzy się z faweli, wysoką przestępczością, karnawałem oraz jego ciemną stroną przestępczą. Kinomani być może wciąż są pod wrażeniem kultowego filmu „Elitarni", który w dwóch odsłonach ukazywał pracę jednostki specjalnej policji „Bope". Jego strategia rozwoju odporności, podobnie jak w innych miastach, koncentruje się wokół trzech filarów.

W ujęciu środowiskowym miasto wymaga dostosowania się do zmian klimatu, ograniczenia zanieczyszczeń i umożliwienia ponownego wykorzystywania zbiorników wodnych, aby dostarczyć mieszkańcom wodę pitną i rekreację.

Rio de Janeiro to miasto o zaniedbanej infrastrukturze, wymagającej pilnych inwestycji. Inicjatywa zastąpienia 75 proc. oświetlenia publicznego żarówkami LED sprawi, że oświetlone obszary publiczne staną się bezpieczniejsze, a jednocześnie zmniejszą się koszty energii. Nowe oświetlenie będzie stanowić część „inteligentnej sieci", która finalnie może obejmować także czujniki informujące organy miasta np. o warunkach drogowych, mikroklimacie w okolicy, nasyceniu infrastruktury drogowej czy działalności przestępczej.

Niepowtarzalny klimat tego pięknego miasta tworzą jego mieszkańcy. Trzecim celem strategii odporności jest zmobilizowanie obywateli do działań na rzecz Rio, edukacja w zakresie odporności miejskiej i zachęty do przemysłu niskoemisyjnego. Aby następne pokolenie żyło w pełnej świadomości proekologicznej, trzeba zacząć od najmłodszych. W ramach programu „Odporna młodzież" zostanie opracowany i wdrożony program dotyczący odporności w miastach. Celem jest edukacja dzieci w zakresie zagrożeń, na jakie narażone jest ich miasto, oraz promowanie kultury świadomości ekologicznej, zapobiegania i łagodzenia wstrząsów i stresów.

Strategie wymienionych hasłowo miast mają różną strukturę, stawiają sobie różne cele oraz daty graniczne wypełnienia postulatów. Za każdym z nich stoją opisane zadania szczegółowe oraz narzędzia i technologie wspierające procesy. Patrząc na opisy, można odnieść wrażenie, że są daleko w tle lub wręcz niewidoczne. Tak jest tylko pozornie, gdyż celem zapewnienia odporności jest wysoki standard życia mieszkańców. A ten wymóg jest zawsze ściśle powiązany z bezpieczeństwem osobistym i bezpieczeństwem biznesu. Niemniej należy go postrzegać jako wyzwanie już w niedalekiej przyszłości. Wyzwaniem dla dzisiejszych security managerów, którzy – ze względu na rozbudowaną w ostatnich latach różnorodność wykonywanych zadań w dużych organizacjach – są jakby naturalnymi kandydatami na objęcie stanowisk resilience managerów zarówno organizacji, jak i miast. Trzeba jednak mieć świadomość, że status kandydata nie oznacza objęcia wakatu. Do tego należy się bardzo gruntownie przygotować.

W kolejnych odcinkach cyklu pokażemy, w jakim kierunku podąża strategia dotycząca kształtowania odporności miejskiej, oraz wskażemy konkretne narzędzia wykorzystywane do osiągnięcia celów. Zapraszamy do lektury. W następnym numerze opiszemy Bangkok. □

BIO

Jacek Tyburek

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

Security Forum Bezpieczne Miasto 2020

W konferencji Bezpieczne Miasto 2020 wzięło udział ponad 100 przedstawicieli urzędów miejskich, straży miejskich oraz instytucji samorządowych z całej Polski. Najnowsze i najciekawsze systemy z zakresu bezpieczeństwa miast, ochrony mienia, osób i budynków zaprezentowało siedmiu partnerów branżowych A&S Polska.

Swoją wiedzą i doświadczeniem podzielili się eksperci w zakresie zarządzania bezpieczeństwem, zabezpieczeń technicznych i *smart city*.
Temat zarządzania bezpieczeństwem miast w pierwszej prelekcji konferencji poruszył były komendant wojewódzki policji na Mazowszu i w Wielkopolsce dr Rafał Batkowski. W swoim wystąpieniu pokazywał, jak zróżnicowana i wielopoziomowa musi być strategia zarządzania bezpieczeństwem w XXI wieku, tak by samorząd, policja i służby miejskie działały sprawnie. O nowej koncepcji i nowym podejściu do bezpieczeństwa opowiadał Rafał Łupkowski z Trustman. W myśl New Security Concept, o której mówił, strategia zarządzania bezpieczeństwem w mieście musi się zawierać w trzech kluczowych słowach: zarządzaj, monitoruj i nie przepłacaj.
Wiele uwagi w trakcie Security Forum Bezpieczne Miasto poświęcono monitoringowi wizyjnemu i jego wykorzystaniu. Paweł Wittich z Miejskiego Zarządu Dróg i Mostów w Bytomiu pokazał, że system zabezpieczeń w mieście musi być adekwatny, czyli „uszyty na miarę". Kluczowe powinno być to, jak technologia, której używamy do zabezpieczenia powierzchni miejskich, ma współgrać z innymi środkami zabezpieczenia stosowanymi w mieście. Sam monitoring nie byłby efektywny, gdyby nagrania nie były odpowiednio przechowywane i gromadzone, szczególnie w erze RODO – mówił w czasie swojej prelekcji Karol Narojczyk z Seagate.
Dozór wizyjny to nie tylko monitorowanie ulic, by te były wolne od przestępstw. To świetne narzędzie do organizacji życia w ośrodkach miejskich. Udowodnił to Konrad Badowski z Axis Communications. W czasie bloku poświęconego monitoringowi uczestnicy konferencji mogli też posłuchać, jak działa istniejące rozwiązanie na dużym osiedlu mieszkaniowym. Stały i zdalny monitoring na przykładzie krakowskiego osiedla „Na Kozłówce" zaprezentował Marcin Gromko z Securitas.
Smart City to Safe City – tych dwóch koncepcji w XXI w. nie da się traktować oddzielnie. Jak mówił Bartosz Dominiak, zastępca burmistrza Dzielnicy Ursynów m.st. Warszawy, obecnie miasta powinny skoncentrować się na zarządzaniu w duchu zrównoważonego rozwoju angażującego możliwie największą liczbę mieszkańców, by stać się nie tylko nowoczesne (*smart*), ale i bezpieczne (*safe*). Jacek Tyburek w swoim wystąpieniu mówił o rezyliencji, czyli odporności w kontekście bezpieczeństwa miast. Goście mogli posłuchać, jak budować odporność na przykładach 100 najbardziej odpornych miast świata. Nie zabrakło też zagadnień z zakresu bezpieczeństwa pożarowego, które w mieście jest bardzo ważne. O projektowaniu bezpieczeństwa pożarowego w swoim wystąpieniu mówił Marcin Barnat z Polon Alfa.

W strefie expo zostały zaprezentowane najnowsze rozwiązania z zakresu zabezpieczeń technicznych i technologii dla miast. Partnerami technologicznymi konferencji byli:
- **Axis Communications** – lider na rynku sieciowego dozoru wizyjnego: https://www.axis.com/pl-pl
- **DFE Security** – inteligentne rozwiązania z zakresu kontroli wejścia i dostępu do obiektów: https://www.dfes.pl/
- **Dilectro** – drony w wykorzystaniu miejskim: https://dilectro.pl/o-nas/
- **Next!** – inteligentne rozwiązania informatyczne do integracji systemów bezpieczeństwa: http://www.next.biz.pl/
- **Polon-Alfa** – największy polski producent systemów sygnalizacji przeciwpożarowej: https://www.polon-alfa.pl/pl
- **Seagate** – światowej klasy rozwiązania w zakresie ochrony danych: https://www.seagate.com/pl/pl/consumer/#
- **Securitas** – lider w zakresie ochrony osób i mienia: https://www.securitas.pl/

Konferencja Bezpieczne Miasto 2020 odbyła się 27 lutego w warszawskim hotelu Novotel Centrum. Była pierwszym spotkaniem z cyklu Security Forum – każde wydarzenie z cyklu będzie dotyczyło tematyki zarządzania bezpieczeństwem i zabezpieczeń technicznych w poszczególnych sektorach gospodarki. □

Dzień Kobiet Security

Trzecia edycja spotkania najbardziej wpływowych kobiet branży security. Panie z całej Polski spotkały się w Folwarku Białych Bocianów w Kamionce pod Warszawą. Dzień Kobiet Security wraz z redakcją A&S Polska zorganizowały firmy partnerskie: Axis Communications i Nedap Security Management.

Anna Twardowska

PARTNER WYDARZENIA
Nedap Security Management

→ ***Tym, co charakteryzuje spotkania, była także duża dawka wiedzy merytorycznej.*** *W tym roku było to szkolenie z komunikacji. Pokazało nam, jak ważna jest wiedza, aby dobrze się komunikować i być dobrze rozumianą.*

Dagmara Pomirska

PARTNER WYDARZENIA
Axis Communications

→ ***Dla nas to możliwość zbudowania relacji z różnymi kobietami, zarówno wśród naszych partnerów,*** *jak i firm konkurencyjnych. To także szansa na to, żeby jako kobiety rozwijać swoje pasje, zainteresowania, dlatego bardzo cieszymy się z warsztatów, ze spotkań i z rozmów, które towarzyszą temu Dniu Kobiet.*

W tym roku szkolenie z zakresu komunikacji poprowadzili znakomici trenerzy Kamilla Dąbrowska i Witold Casetti. Dzięki warsztatom o kolorach osobowości uczestniczki spotkania dowiedziały się, dlaczego niebieski szef czeka na tabele, a zielony na uśmiech. Popołudniowe szkolenie poświęcone było autoprezentacji. Jolanta Kucharska podzieliła się z kobietami z branży security kilkoma złotymi radami na temat wystąpień publicznych. Po spotkaniu nagrany został film, na którym gołym okiem widać, że wszystkie panie były pilnymi uczennicami warsztatów i zdobytą wiedzę potrafią znakomicie wykorzystać. Film można obejrzeć na portalu www.aspolska.pl. Zapraszamy!

Kamilla Dąbrowska i Witold Casetti

trenerzy

→ ***Rozmawialiśmy o tym, że komunikacja powinna być kolorowa każdy człowiek jest inny, każdy ma inne potrzeby.*** *Wszystko ma podłoże naukowe, a żyje się dużo lepiej, gdy jesteśmy świadomi tego, kim jesteśmy!*

Angelika Prokop-Grey

ASIS

→ ***Kompetencje i zaufanie*** *– to wszystko dziś tu zobaczyliśmy i to pokazuje, że na tym oparta jest kobieca współpraca w branży bezpieczeństwa.*

Aleksandra Krause

Konica-Minolta

→ ***Biorę udział w takim spotkaniu po raz pierwszy.*** *Cieszę się, że mogłam dołączyć do grona tak kompetentnych kobiet z niesamowitą energią.*

Agnieszka Bilska

EBS

→ ***Bardzo się cieszę, że idea takich kobiecych spotkań powstała****. Dzięki temu możemy budować również nasze relacje, doskonałą atmosferę i świetny klimat.*

Katarzyna Grudniewska

Anixter

→ ***Czujemy się tu jak na spotkaniu dobrych przyjaciółek,*** *gdzie możemy wymienić się doświadczeniami i nauczyć się nowych rzeczy.*

Nowe kamery Axis dla lotnisk, logistyki i transportu publicznego

Axis Communications wprowadza nowe kamery sieciowe z serii AXIS P13. Te solidne i szybkie w działaniu stałopozycyjne kamery typu box z wymiennymi obiektywami umożliwiają obserwację osób i obiektów na rozległych obszarach, pełniąc jednocześnie funkcję odstraszającą.

Kamery są dostępne w dwóch wersjach: wewnętrznej i zewnętrznej. Zapewniają znakomite odwzorowanie szczegółów (rozdzielczość 5 Mpix i 4K). Modele wewnętrzne AXIS P1377 i AXIS P1378 nie zawierają środków wykorzystywanych często do zmniejszania palności, są więc przyjazne dla środowiska. Świetnie sprawdzą się w portach lotniczych, w strefach przeładunku towarów i systemach transportu publicznego. Zaimplementowana w kamerach technologia Axis Forensic WDR pozwala uzyskiwać wysokiej jakości obraz, gdy obserwowana scena obejmuje zarówno ciemne, jak i jasne fragmenty. Natomiast technologia Axis Lightfinder zapewnia ostry kolorowy obraz nawet w słabych warunkach oświetleniowych. Modele zewnętrzne AXIS P1377-LE i AXIS P1378-LE są dodatkowo wyposażone w technologię Axis OptimizedIR umożliwiającą dozór w całkowitej ciemności. Wydajna technologia Axis Zipstream obsługująca formaty H.264 i H.265 zmniejsza zapotrzebowanie na przepustowość i pamięć masową..

Nowoczesny procesor Axis zastosowany w kamerach pozwala na zastosowanie udoskonalonych funkcji zabezpieczeń, zapewniających integralność i autentyczność oprogramowania sprzętowego kamery.

Nowe głośniki sieciowe od Axis sprawdzą się w każdym środowisku

Axis Communications wprowadza do oferty przystępny cenowo minigłośnik sieciowy o niewielkich rozmiarach oraz megafon, który może pracować w każdym środowisku zewnętrznym, w dowolnych warunkach atmosferycznych. Dzięki rozwiązaniom audio użytkownicy mogą szybko reagować na zdarzenia wykryte przez kamery i za pomocą komunikatów głosowych zapobiegać sytuacjom niepożądanym.

AXIS C1410 Network Mini Speaker

Minigłośnik sieciowy AXIS C1410 Network Mini Speaker to dyskretne urządzenie, które zajmuje niewiele miejsca. Opiera się ono na otwartych standardach, dzięki czemu można je łatwo zintegrować z innymi systemami, takimi jak telefonia VoIP oraz kamery wideo i narzędzia analityczne Axis oraz firm trzecich. Możliwość reagowania na obserwowane zdarzenia przy użyciu komunikatów głosowych podnosi poziom bezpieczeństwa – system emituje gotowy komunikat lub powiadamia pracowników ochrony, którzy mogą zwrócić się do intruzów bezpośrednio przez głośnik. Urządzenie może służyć również do emitowania ogólnych komunikatów, instrukcji oraz odtwarzania tła muzycznego. Głośnik można zainstalować na ścianie, na suficie, w korytarzu lub w innym dowolnym miejscu.

NAJWAŻNIEJSZE CECHY URZĄDZENIA:
- Łatwa integracja z sieciowymi systemami wizyjnymi, systemami kontroli dostępu i telefonią VoIP
- Przystępna cena i szerokie pokrycie dźwiękiem
- Wbudowany, fabrycznie skonfigurowany cyfrowy procesor sygnału, zapewniający wyraźne brzmienie każdego komunikatu głosowego
- Zdalne testowanie stanu technicznego głośników
- Wbudowana pamięć do przechowywania nagranych komunikatów audio
- Wbudowana czujka PIR do detekcji ruchu

AXIS C1310-E Network Horn Speaker

Wzmocniony megafon sieciowy AXIS C1310-E Network Horn Speaker wytrzymuje temperatury od -40 do 60°C. Dzięki zgodności z otwartymi standardami można go łatwo zintegrować z innymi systemami, takimi jak telefonia VoIP oraz kamery wideo i aplikacje analityczne Axis i firm trzecich. Umożliwia łatwe odstraszenie intruzów wykrytych przez kamery za pomocą przekazywanych na żywo lub nagranych komunikatów głosowych. Elastyczna konstrukcja megafonu AXIS C1310-E umożliwia jego montaż na ścianie lub słupie, co przekłada się na maksymalną użyteczność i wygodę. Urządzenie może służyć także do emitowania ogólnych powiadomień.

NAJWAŻNIEJSZE CECHY URZĄDZENIA:
- Łatwa integracja z sieciowymi systemami wizyjnymi, systemami kontroli dostępu i telefonią VoIP
- Możliwość pracy w temperaturze od -40 do 60°C
- Wbudowany, fabrycznie skonfigurowany cyfrowy procesor sygnału, zapewniający wyraźne brzmienie każdego komunikatu głosowego
- Zdalne testowanie stanu technicznego głośników
- Dwa wbudowane wejścia/wyjścia ogólnego przeznaczenia

Nowe głośniki sieciowe są dostępne w kanałach dystrybucyjnych Axis od I kwartału br.

Rejestratory Wisenet Pentabrid – rozwiązanie przyszłościowe

Nowe 4-, 8- i 16-kanałowe rejestratory Wisenet Pentabrid firmy Hanwha Techwin mogą przedłużyć czas użytkowania analogowych systemów CCTV, umożliwiając płynną i ekonomiczną migrację do rozwiązań IP. Można do nich podłączyć kamery analogowe i IP o rozdzielczości do 4K (Ultra HD), oprogramowanie rejestratora automatycznie rozpozna rodzaj kamery.

Zalety rozwiązań do dozoru wizyjnego opartych na sieci IP są powszechnie znane, ale użytkownicy nadal wybierają systemy analogowe i chcą zachować dotychczas używane rozwiązania, gdyż nie są gotowi na migrację do świata IP. Przyczyny mogą być różne – infrastruktura sieciowa może nie obsługiwać systemu dozoru wizyjnego lub przepustowość łącza może być nieodpowiednia. Ale jeśli dotychczasowe systemy analogowe nadal spełniają wymagania użytkowników, umotywowanie inwestycji w modernizację instalacji kablowej i wymianę urządzeń może być trudne – mówi Uri Guterman, szef Działu Produktów i Marketingu firmy Hanwha Techwin Europe.

Sześć nowych modeli rejestratorów wyposażono w wiele funkcji inteligentnej analizy wideo (detekcja dźwięku, twarzy, zmiany ostrości, wejścia/wyjścia do/ze strefy i sabotaż kamery). Można je skonfigurować tak, aby po wystąpieniu zdarzenia reagowały w różny sposób, np. automatycznie wysyłając powiadomienia e-mail do określonych osób lub wywołując zmianę widoku kamery PTZ.

Nowe rejestratory są kompatybilne z oprogramowaniem do zarządzania systemem dozoru wizyjnego, np. Wisenet WAVE. Obsługują wszystkie kamery sieciowe Wisenet oraz kamery analogowe Wisenet HD+, które rejestrują i przesyłają obraz i dźwięk bez opóźnień na odległość do 500 m przez standardowe okablowanie koncentryczne. Pomagają też w uproszczeniu przejścia na kolejną generację produktów Wisenet i mogą obsługiwać kamery niektórych innych producentów.

Nowa wersja VMS Wisenet WAVE 4.0

Hanwha Techwin wprowadziła czwartą, znacznie ulepszoną wersję oprogramowania do zarządzania systemem dozoru wizyjnego (VMS) Wisenet WAVE. Zawierające wiele nowych funkcji i zaprojektowane z myślą o ułatwieniu obsługi, poprawieniu zgodności operacyjnej i cyberbezpieczeństwie, oprogramowanie Wisenet WAVE 4.0 ma udoskonaloną architekturę systemu, która zapewnia wysoką dostępność i pozwala na wdrożenia skalowalnego systemu opartego nawet na 100 serwerach.

Łatwa obsługa

Wisenet WAVE 4.0 umożliwia połączenie systemów zarejestrowanych na platformie WAVE Sync z poziomu panelu nawigacyjnego online, co eliminuje konieczność konfiguracji przekierowania portów do zdalnego zarządzania serwerami. Nowy zaktualizowany interfejs użytkownika Wisenet WAVE zapewnia prostą i niezwykle intuicyjną obsługę. Nowa funkcja „Layout-as-an-Action" umożliwia automatyczne wyświetlenie wcześniej zdefiniowanego układu/widoku jako regułę dla wystąpienia zdarzenia alarmowego. Dodatkowo WAVE 4.0 obsługuje teraz takie funkcje analizy obrazu, jak zarządzanie kolejkami działające w kamerach Wisenet, a także wykrywanie uderzeń w kamerach z serii Wisenet X Plus i detekcję zmian temperatury w kamerach termowizyjnych Wisenet.

Większe bezpieczeństwo

W zastosowaniach wymagających wysokiego poziomu bezpieczeństwa Wisenet WAVE 4.0 można skonfigurować tak, aby system używał tylko protokołu HTTPS i szyfrował ruch wideo. Oprócz tego dodano opcję ochrony hasłem plików w formatach .nov i .exe.

Zestaw Metadata SDK i wtyczki

Nowy zestaw SDK do oprogramowania WAVE 4.0 umożliwia integrację urządzeń i systemów firm trzecich. Zawiera kompleksowy zestaw funkcji zaprojektowany do zewnętrznych systemów lub aplikacji, włączając oprogramowanie do analizy obrazu oparte na technologiach *deep learning* oraz sztucznej inteligencji (SI), jak również rozpoznawanie obiektów i szeroko pojętą automatyzację.

HotSpots mobilny system detekcji pożarów

Wieża HotSpots to nowoczesna koncepcja mobilnego systemu detekcji pożarów na rozległych obszarach, dostosowana do najbardziej wymagających zastosowań. Wieżę można wyposażyć w odpowiednią kamerę radiometryczną dostosowaną do określonego terenu i warunków. Połączenie kamer termowizyjnych umożliwiających monitoring i pomiar temperatury wraz z systemem transmisji obrazu w czasie rzeczywistym pozwala na szybką reakcję na pojawiające się zagrożenie.

Bardzo często wdrożenie systemu monitoringu pożarowego jest nieopłacalne lub niemożliwe ze względu na zbyt wysokie koszty instalacji lub brak wymaganej infrastruktury. Odpowiedzią na potrzeby rynku jest możliwość zakupu wieży HotSpots lub jej wynajęcia na czas określony. Dzięki temu klient nie ponosi kosztów związanych z budową odpowiedniej infrastruktury. Jest to rozwiązanie plug & play, czyli gotowe do zabezpieczenia wyznaczonego obszaru w ciągu kilku minut po dostarczeniu na miejsce. Ponieważ miejsce instalacji może nie posiadać infrastruktury energetycznej i sieciowej, wieża HotSpots może być zasilania z akumulatora lub innego alternatywnego źródła energii. Ze względu na elastyczność wyposażenia i zastosowania (wysypiska śmieci, place magazynowe, kopalnie itp.) jest to produkt funkcjonalny pod kątem użyteczności i możliwości zastosowań. **Więcej na: www.linc.pl**

Bazujący na rozwiązaniach IP system konferencyjny DICENTIS firmy Bosch

Wraz z pojawieniem się wersji 3.2 oprogramowania, system konferencyjny DICENTIS firmy Bosch oferuje nowy, niezależny od platformy, bezpieczny i skalowalny interfejs bazujący na *JSON (JavaScript Object Notation)* i komunikacji websocket.

Obsługuje płynnie łączność z urządzeniami do zarządzania i sterowania konferencją (panele dotykowe, krosownice wizyjne) innych producentów za pośrednictwem interfejsu, który działa niezależnie od systemu operacyjnego, w tym Microsoft Windows.

Dzięki integracji dotykowych paneli sterowania system umożliwia organizatorom konferencji sterowanie projektorami wideo, systemami audio czy oświetleniem za pomocą jednego urządzenia i zapewnia lepszą widoczność statusu wszystkich podłączonych urządzeń. Obsługując tłumaczenia nawet 100 języków, DICENTIS wyznacza nowy standard wśród systemów konferencyjnych, zaspokajając zróżnicowane potrzeby: zarządzanie dyskusją, tłumaczenia symultaniczne, wybór języka, głosowania, funkcje multimedialne, transmisje wideo na żywo, dostęp do Internetu, przeglądanie dokumentów, aplikacje innych producentów i wiele innych funkcjonalności. System bazuje na architekturze sieciowej IP OMNEO, obsługuje technologie Dante™ i PoE oraz umożliwia szybką i łatwą integrację z systemami innych producentów.

Jednym z pierwszych producentów paneli dotykowych, który dostosował interfejsy sterujące do oferty produktów DICENTIS, jest kalifornijska firma Extron, znany globalny dostawca profesjonalnych rozwiązań audio-wideo, w tym m.in. systemów sterowania.

C&C Partners dzieli się wiedzą

Intensywny, szybki rozwój nowoczesnych technologii generuje wśród naszych klientów potrzebę przyswajania coraz bardziej wyspecjalizowanej wiedzy. W odpowiedzi na te potrzeby uruchomiliśmy projekt szkoleniowy na miarę ich wymagań. Dzielimy się naszym wieloletnim doświadczeniem na rynku polskim oraz myślą inżynieryjną, które wzbogacamy podczas szkoleń i seminariów z naszymi partnerami działającymi w ramach Grupy TKH.

Akademia Technologii C&C, w której ramach prowadzimy szkolenia dla naszych partnerów – inżynierów, projektantów, instalatorów i klientów końcowych – jest doskonałym miejscem do podnoszenia kwalifikacji technicznych dla państwa i państwa pracowników. W C&C kładziemy nacisk na przekaz wiedzy na zaawansowanym poziomie. Oferujemy doskonałe warunki szkoleniowe, szeroki wybór tematyki i dostępnych terminów.

Akademia Technologii C&C zyskała nowy wymiar dzięki platformie szkoleniowej. Teraz dostęp do portfolio naszych szkoleń jest jeszcze łatwiejszy. Platforma daje uczestnikom możliwość m.in. zapisania się na szkolenie, zapoznania się z ich zakresem, liczbą dostępnych miejsc, terminem, kosztem oraz lokalizacją szkolenia. Zapraszamy do zapoznania się z ofertą szkoleń na 2020 rok! **www.ccpartners.pl**

NOWY TERMIN

24.09.2020

Warsaw Security Summit

#zostańwdomu

W trosce o bezpieczeństwo uczestników zmieniliśmy termin konferencji.

Zapewniamy, że będziemy reagowali na zmieniające się warunki sanitarno-epidemiologiczne. Zależy nam przede wszystkim na bezpieczeństwie naszych gości. Liczymy, że do września sytuacja będzie opanowana. **Życzymy zdrowia i wytrwałości. Do zobaczenia!**

AX-HUB
868MHZ

BEZPRZEWODOWY SYSTEM AX HUB

INTRUSION PROTECTION WITH VISION

HIGHLIGHTS

- AX Hub jest kompatybilny z kamerami ONVIF, zapewniając wideoweryfikację dla użytkowników i stacji monitoringu, aby szybko i efektywnie potwierdzać zdarzenia.
- Kiedy wystąpi kryterium alarmu, powiadomienia mogą zostać wysłane do użytkowników różnymi kanałami: poprzez powiadomienia PUSH do aplikacji, e-mail, połączenie głosowe oraz SMS.
- AX Hub jest łatwy w konfiguracji oraz posiada intuicyjny, przyjazny dla użytkownika interfejs.
- System można rozbudować do 32 czujek bezprzewodowych, 32 wyjść bezprzewodowych, 4 klawiatur bezprzewodowych, 4 czytników bezprzewodowych i 4 syren bezprzewodowych.
- AX Hub jest kompatybilny z aplikacją Hik-Connect, pozwalając na łatwe zarządzanie systemem, udostępnianie urządzenia członkom rodziny oraz tworzenie różnych poziomów uprawnień.