a&S POLSKA
www.aspolska.pl

CZASOPISMO RYNKU SECURITY
nr 2/2018 (8)
marzec/kwiecień
15 zł (w tym 8% VAT)

BEZPIECZNA INFRASTRUKTURA KRYTYCZNA

CYBER SECURITY

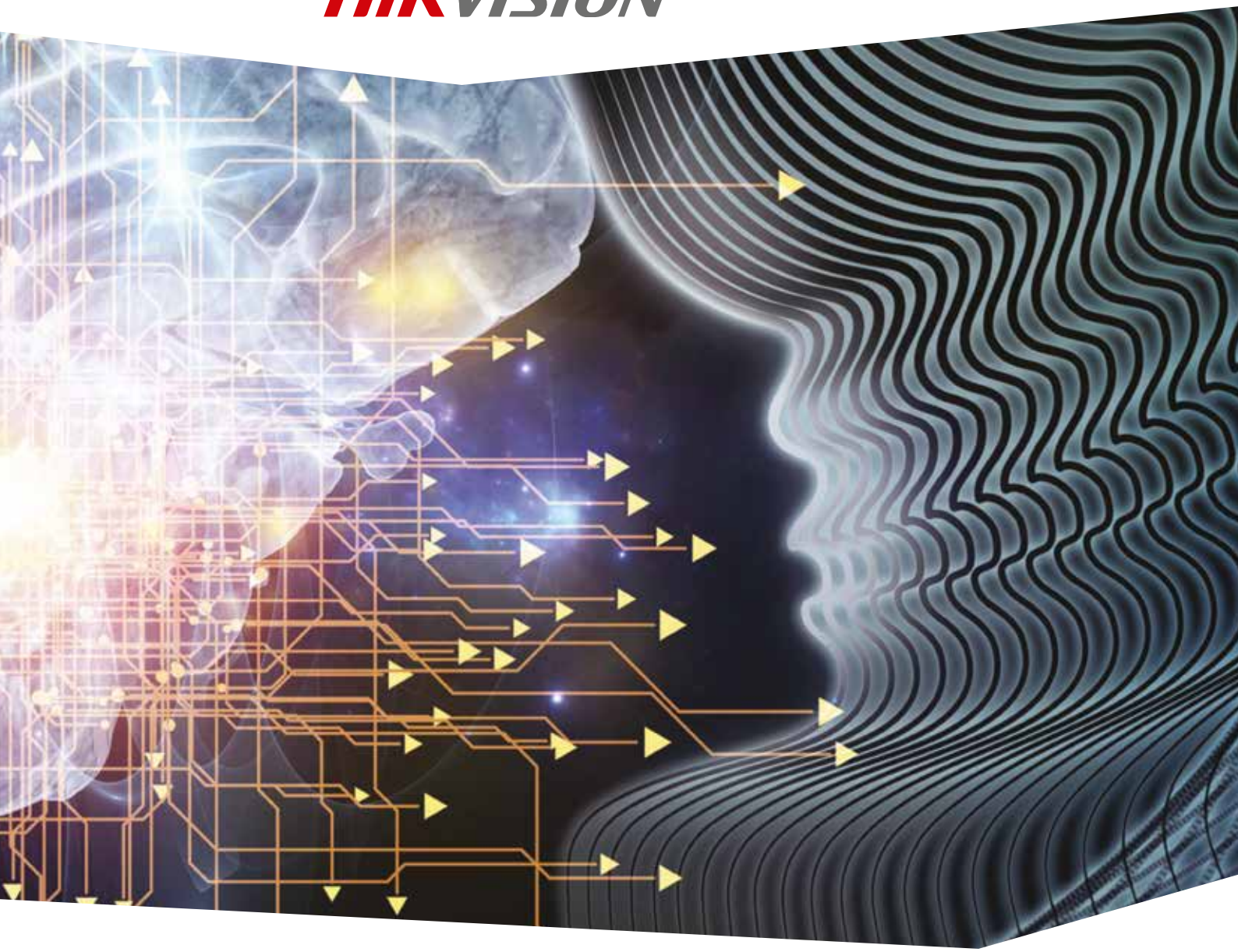
ISSN 2451-5175
9 772451 517703 03

WIĘKSZA INTELIGENCJA.
WIĘKSZE BEZPIECZEŃSTWO.
TECHNOLOGIA DEEP LEARNING FIRMY HIKVISION

Hikvision Poland Sp. z o.o.
ul. Krakowiaków 50
02-255 Warszawa

T +48 22 4600150
info.pl@hikvision.com

HIKVISION



Hikvision patrzy w przyszłość i stale rozwija swoje technologie.
Jedna z nich - Deep Learning - zapewnia zupełnie nowe możliwości. Detekcja twarzy, zliczanie osób, identyfikacja pojazdów - wszystko to jest możliwe z nowymi produktami dostarczanymi przez firmę Hikvision.

Sprawdź te i inne technologie na stosiku Hikvision podczas Targów Securex – pawilon 7A, stoisko 7.

Detekcja twarzy

Filtrowanie fałszywych alarmów

Zliczanie osób

Identyfikacja pojazdów

Rozpoznawanie osób

@HikvisionPoland
www.hikvision.com/pl/

Drodzy Czytelnicy

Cyberbezpieczeństwo to jedno z większych, jeśli nie największe wyzwanie współczesności. Szczególnie wrażliwa jest branża security, dostarczająca elektroniczne (sieciowe!) zabezpieczenia techniczne. Czy zatem systemy security są odporne na cyberzagrożenia? Jak pisze Jan T. Grusznic (s. 26), **cyberdefilada ruszyła na całego!** Zapewnienie bezpieczeństwa cyfrowego jest coraz trudniejsze, gdyż z tych samych środków korzystają obie strony cyberwojny – zarówno specjaliści security, jak i cyberintruzi. Do tej walki coraz częściej zaprzega się tzw. **sztuczną inteligencję, co stanowi szansę, ale niesie także zagrożenia** (s. 18).

Szczególnie chronione – nie tylko przed cyberatakami, ale także zagrożeniami innego typu – są **obiekty infrastruktury krytycznej.** Odpowiedzialni za ich bezpieczeństwo podzielili się z nami swoimi doświadczeniami, wskazując na coraz większe wyzwania (s. 38). Właśnie w odpowiedzi na rosnące zagrożenia **Rządowe Centrum Bezpieczeństwa zmienia podejście do ochrony IK,** o czym opowiedział nam w wywiadzie przedstawiciel RCB (s. 34).

W zabezpieczaniu obiektów (nie tylko krytycznych) niezbędna może się okazać termowizja. Dlatego poruszamy problemy związane z **projektowaniem systemów termowizyjnych** (s. 58), odpowiadamy na **najczęstsze pytania dot. termowizji z analizą obrazu** (s. 62), prezentujemy **ofertę rynkową kamer termowizyjnych i bispektralnych** (s. 64). Projektantom i instalatorom polecamy też artykuł **o promiennikach podczerwieni w systemach CCTV** (s. 74).

Wiosna obfituje w wydarzenia branżowe. Spośród wielu, w których uczestniczyliśmy, należy wymienić szczególne – 8 marca gościliśmy piękniejszą część naszej branży na pierwszym **Dniu Kobiet Security** (s. 112). Przed nami z kolei najważniejsze wydarzenia w tym roku – kwietniowe **targi Securex** (s. 107) oraz czerwcowa **konferencja Warsaw Security Summit** (s. 119).

Z radością informujemy także o powołaniu **Instytutu Bezpieczeństwa RESCON**, którego jesteśmy partnerem strategicznym (s. 110).

Witamy także w naszym zespole wyjątkową osobę! Po wielu latach współpracy autorskiej **Jan T. Grusznic został zastępcą redaktora naczelnego *a&s Polska.*** Będzie dla nas ogromnym wsparciem merytorycznym. Wspólnie podejmiemy wiele ciekawych i niezwykle wartościowych inicjatyw! Szczegóły wkrótce...

Marta Dynakowska
redaktor naczelna

Mariusz Kucharski
dyrektor zarządzający

Od mojej pierwszej publikacji w prasie branżowej (na łamach *Systemów Alarmowych*) minęło 8 lat. Z tej perspektywy dostrzegam, że nasza branża, aby się rozwijać, musi poprawić komunikację, być otwarta na nowe wyzwania i wsłuchiwać się w potrzeby i oczekiwania użytkowników. **Potrzebne są publikacje**, które omawiają realne problemy i sposoby na ich rozwiązanie, opisują światowe trendy elektronicznych systemów zabezpieczeń oraz wymagania rodzimego rynku. **Potrzebne są też działania** wykraczające poza artykuły prasowe, odpowiadające na oczekiwania współczesnych odbiorców.

Dlatego po latach współpracy z redakcją *Systemów Alarmowych*, a teraz *a&s Polska* zdecydowałem się **objąć stanowisko zastępcy redaktora naczelnego** i podjąć się realizacji **ambitnych przedsięwzięć**, które dotychczas pozostawały jedynie w sferze planów. **Będzie się działo!**

Jan T. Grusznic
z-ca redaktora naczelnego

Wydawca
a&s Polska Sp. z o.o.

Adres wydawcy i redakcji
a&s Polska
Rondo1 (10. piętro)
Rondo ONZ 1, 00-124 Warszawa
tel. +48 22 418 71 59
e-mail: info@aspolska.pl
www.aspolska.pl

Dyrektor zarządzający
Mariusz Kucharski

Redaktor naczelna
Marta Dynakowska

Z-ca redaktora naczelnego
Jan T. Grusznic

Dział reportażu
Andrzej Popielski

Dział marketingu i reklamy
Iwona Krawiec

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

Korekta
Jolanta Kucharska

Projekt graficzny
Sylwester Dmowski

Skład
Dorota Cybulska
Sylwester Dmowski

Prenumerata
www.aspolska.pl/prenumerata

BCS-PHC3X2M-IR

PANORAMIC 180° HDCVI IR BULLET CAMERA

- TRZY 2-MEGAPIKSELOWE PRZETWORNIKI 1/2.8" CMOS
- TECHNOLOGIA HDCVI STARLIGHT
- 1 OBRAZ PANORAMICZNY 3 OBRAZY 2 MPX
- WIELOPRZETWORNIKOWA KAMERA PANORAMICZNA HDCVI

Wieloprzetwornikowa kamera panoramiczna **HDCVI** daje nowe możliwości obserwacji , w miejscach gdzie konieczny jest **monitoring wielkich powierzchni**. Zastosowanie **trzech 2-megapikselowych** przetworników pracujących równolegle pozwala na stworzenie obrazu o wysokiej rozdzielczości i kącie widzenia **180°** przy zachowaniu wysokiej jakości szczegółów. Jednocześnie otrzymujemy również **3 kanały HDCVI** o rozdzielczości **2-megapikseli**. Dzięki takiej funkcjonlności możemy wyeliminować **martwe strefy monitoringu**. Razem mamy zatem do dyspozycji **4 wysokiej jakości** źródła obrazu przy wykorzystaniu tylko jednej kamery, dzięki czemu możemy w znacznym stopniu zredukować koszty samej instalacji jak i późniejszej eksploatacji systemu monitoringu. Dodatkowo kamera **wspiera** funkcję zaawansowanej elektronicznej **analizy obrazu** takiej jak **śledzenie obiektów** i **wielopunktową detekcję ruchu**. Wykorzystanie możliwości **obrazu panoramicznego** sprawia, że tego typu kamera znajdzie zastosowanie i świetnie sprawdzi się na obiektach gdzie zachodzi potrzeba **obserwacji dużych powierzchni** takich jak hale magazynowe, lotniska, parkingi, stadiony i hale sportowe, obiekty użyteczności publicznej czy monitoring miejski.

BCS®

www.bcscctv.pl

W numerze...

BEZPIECZEŃSTWO BIZNESU

SERWIS INFORMACYJNY

STR. 64

Przegląd kamer termowizyjnych

Kamera sieciowa AXIS Q3517-LV

AXIS
www.axis.com/pl

- Rozdzielczość 5 Mpix przy pełnej poklatkowości
- *Forensic WDR, Lightfinder* i *OptimizedIR*
- Technologia *Zipstream* firmy Axis
- Elektroniczna stabilizacja obrazu (EIS), obudowa IP52 (ochrona przed kurzem i wodą) oraz IK10
- Zasilanie redundantne i konfigurowalne porty we./wy.

Dyskretna i wandaloodporna kamera sieciowa zapewnia doskonałej jakości obrazy nawet w trudnych warunkach oświetlenia, niezależnie od pory dnia i nocy oraz zastosowania. Wyposażono ją w zaawansowane funkcje:

- *Forensic WDR* oznacza, że obraz charakteryzuje się wysoką szczegółowością, a sceny z obszarami kontrastowo oświetlonymi są doskonale widoczne.
- Technologia *Lightfinder* zapewnia ostre kolorowe obrazy przy słabym oświetleniu.
- Funkcja *OptimizedIR* zapewnia obraz wideo bez szumu nawet w całkowitej ciemności.
- Technologia *Zipstream* firmy Axis zmniejsza zapotrzebowanie na przepustowość i pamięć nawet o 50%, zapewniając przechwytywanie szczegółów w pełnej jakości obrazu.

Kamerę AXIS Q3517-LV zaprojektowano tak, by była odporna na drgania i wstrząsy. Ochronę przed wnikaniem kurzu i wody zapewnia obudowa o klasie IP52, która jest również odporna na akty wandalizmu (klasa IK10). Elektroniczna stabilizacja obrazu umożliwia uzyskanie niezakłóconego obrazu nawet w przypadku narażenia kamery na drgania. Dzięki redundantnemu zasilaniu prądem stałym oraz PoE dozór kluczowych obiektów można prowadzić nieprzerwanie nawet w przypadku awarii zasilania.

Kamera panoramiczna BCS-PHC3X2M-IR

BCS
www.bcscctv.pl

Wieloprzetwornikowa kamera panoramiczna HDCVI daje nowe możliwości obserwacji wielkich powierzchni.

Zastosowanie trzech 2-megapikselowych przetworników pracujących równolegle pozwala wygenerować obraz o wysokiej rozdzielczości i kącie widzenia 180°, przy zachowaniu wysokiej jakości szczegółów.

Jednocześnie są również dostępne trzy kanały HDCVI o rozdzielczości 2 Mpix. Dzięki takiej funkcji można wyeliminować martwe strefy monitoringu.

Łącznie mamy zatem do dyspozycji cztery wysokiej jakości źródła obrazu przy użyciu tylko jednej kamery. Pozwala to w znacznym stopniu zredukować koszty instalacji oraz późniejszej eksploatacji systemu dozoru wizyjnego.

Ta wieloprzetwornikowa kamera panoramiczna wspiera funkcje zaawansowanej elektronicznej analizy obrazu: śledzenie obiektów i wielopunktową detekcję ruchu.

Wykorzystanie możliwości obrazu panoramicznego sprawia, że tego typu kamera znajdzie zastosowanie i świetnie sprawdzi się w obiektach wymagających obserwacji dużych powierzchni, takich jak hale magazynowe, lotniska, parkingi, stadiony i hale sportowe, obiekty użyteczności publicznej czy miejskie systemy monitoringu.

GANZ CORTROL oprogramowanie VMS klasy Enterprise

CBC (Poland)
www.cbcpoland.pl

Skalowalność, uniwersalność i prostota to cechy najnowszego oprogramowania centralnego zarządzania obrazem VMS GANZ CORTROL.
Dostępne w trzech wersjach: *Prime*, *Premiere* i *Global* zapewnia bardzo wydajny dozór wizyjny. Wspiera kodeki H.264, H.265, MJPEG, MPEG-4, ma intuicyjny interfejs użytkownika i gwarantowaną wydajność. Dzięki centralnej strukturze hierarchicznej i wielu specjalistycznym modułom wersja *Global* jest idealnym rozwiązaniem dla systemów CCTV o dużej, rozproszonej architekturze.
Kluczowe funkcjonalności systemu to: platforma 64-bitowa, gotowość do odbioru strumienia 4K i 8K z możliwością nagrywania i odtwarzania, pełna kontrola i automatyzacja dozoru wizyjnego (menedżer zdarzeń), dostęp z aplikacji mobilnych, możliwość tworzenia własnych widoków oraz e-map i geomap, możliwość dodania niegraniczonej liczby serwerów na jednej aplikacji klienckiej, funkcja strumieniowania wideo i dwukierunkowa komunikacja za pomocą telefonu komórkowego, ciągłe monitorowanie stanu serwerów i centralne zarządzanie pracą awaryjną (*failover*), replikacja danych archiwalnych, strumieniowanie RTMP (np. na www lub YouTube), zaawansowane funkcje wyszukiwania materiału wizyjnego, wbudowany serwer WWW z multicastem.
Ma potężne możliwości analityczne (identyfikacja numerów rejestracyjnych, identyfikacja twarzy, wbudowany silnik *deep learning* VCA), zestaw (API/SDK) umożliwia integrację z innymi systemami VMS.

PCX46 APP

Pyronix
HIKVISION

Hybrydowy system alarmowy z aplikacją

Adaptowalny, funkcjonalny i pełen cech

PCX 46 APP jest profesjonalnym rozwiązaniem wysokiej klasy bezpieczeństwa z komunikacją IP. Przewodowe i bezprzewodowe, dwukierunkowe akcesoria powodują, że instalacja jest szybka i łatwa, a wszystko z obsługą przez aplikację HomeControl+, dającą użytkownikom pełną kontrolę nad ich systemem z dowolnego miejsca świata!

www.facebook.com/pyronix @pyronix Dołącz do nas na LinkedIn

Hikvision Poland, The Park, Office Building A Krakowiaków 50, 02-255 Warsaw
Tel: +48 22 460 01 50 E-Mail: info.pl@hikvision.com Website: www.pyronix.com

Energooszczędne zasilanie awaryjne

CyberPower
www.cyberpower.com/eu/pl

Energooszczędne urządzenia zasilania awaryjnego CyberPower są przykładem zaawansowanych rozwiązań do zabezpieczenia infrastruktury IT i security. Produktem wartym uwagi jest kompaktowy model OR600ELDRM1U (600 VA/360 W), którego niezwykle małe rozmiary 4,4 x 43,3 x 23,5 cm stanowią ciekawą propozycję do zasilania w lokalizacjach, gdzie nie stosuje się klasycznych szaf typu *rack*, a miejsca na zasilanie awaryjne jest niewiele. Jego pobór mocy na potrzeby własne wynosi zaledwie 4 W – jest jednym z najbardziej energooszczędnych urządzeń tej klasy na rynku.
Przyjmując, że cena energii elektrycznej wynosi ok. 50 gr za kilowat, w ciągu roku koszt użytkowania tego UPS-a zamknie się kwotą 22 zł. W połączeniu z bezpłatnym oprogramowaniem *PowerPanel Business Edition* zapewnia administratorowi ogromne możliwości w zakresie monitoringu i zarządzania do 250 urządzeń UPS.
Warto podkreślić, że oprogramowanie ma certyfikację zgodności m.in. z Cisco EnergyWise™, Vmware czy QNAP.
Uzupełniając system o czujnik środowiskowy *Envirosensor*, mierzący temperaturę i wilgotność otoczenia, mamy pewność, że urządzenia pracują w optymalnych warunkach, a o niepożądanych sytuacjach zostaniemy powiadomieni. Wykorzystując cztery wejścia bezprądowe *Envirosensora*, można podłączyć dowolne czujniki, dzięki czemu można łatwo zintegrować je w jeden system powiadamiania o zdarzeniach.

Wszechstronna kamera DH-SD56230V-HNI

Dahua Technology Poland
www.dahuasecurity.com/pl

Rynek urządzeń do systemów telewizji dozorowej jest niezmiernie szeroki. Wyjątkiem nie jest też rodzina kamer obrotowych PTZ. Mnogość dostępnych rozwiązań zaspokoi praktycznie wszystkie potrzeby. O ile jednak nie stanowi problemu dobór kamer pod kątem ogniskowych, zastosowanych przetworników obrazu czy klasy szczelności obudowy, o tyle dostępność interfejsów wyjściowych jest zazwyczaj mocno ograniczona. W większości przypadków nie będzie to stanowiło problemu, jednak niektórzy klienci mogą oczekiwać czegoś więcej niż tylko sygnału w postaci strumienia sieciowego czy sygnału HDCVI.
Dahua Technology wychodzi naprzeciw tym oczekiwaniom, wzbogacając portfolio kamer PTZ o model DH-SD56230V-HNI. Na pierwszy rzut oka specyfikacja nie zwiastuje niczego nadzwyczajnego: rozdzielczość 1080P, wysokoczuły przetwornik obrazu Sony Starvis 2,8'' (technologia *Starlight*), 30x zoom optyczny o zakresie 4,5–135 mm czy kompresja H.265 to dziś dość popularne cechy, spotykane również w innych produktach. Czym zatem wyróżnia się ta wyjątkowa konstrukcja na tle innych dostępnych obecnie na rynku?
Przede wszystkim liczbą dostępnych interfejsów wyjściowych, mamy tu bowiem ich duży wybór: HD-CVI, HD-SDI, DVI, HDMI, VGA i RJ45. Pozwala to na integrację z większością istniejących instalacji. Problemem nie będzie również brak instalacji kablowej, gdyż kamera jest wyposażona w kartę bezprzewodową Wi-Fi.
Te cechy plasują DH-SD56230V-HNI w gronie najbardziej elastycznych produktów dostępnych na rynku.

Nowe czytniki kontroli dostępu marki ViDiLine

Genway
www.genway.pl

Oferta produktów kontroli dostępu marki ViDiLine powiększa się o trzy nowe. Pierwszym z nich jest czytnik kart i linii papilarnych VIDI-AC-F007. To wodoodporne urządzenie (klasa szczelności obudowy IP66) może obsłużyć do 1000 odcisków i 2000 kart. Czytnik jest wyposażony w wyjście Wiegand i może pracować w szerokim zakresie temperatury od -30°C do 50°C. Wyjście przekaźnikowe typu NO/NC ma obciążalność prądową do 2 A. Solidna obudowa została wykonana ze stopu aluminium.

System uzupełniają czytniki kart i breloków zbliżeniowych VIDI-AC-3CSS oraz VIDI-AC-3CSW. Mogą pracować w trzech trybach: samodzielnym, kontrolera Wiegand lub czytnika Wiegand. Urządzenia mają identyczne parametry techniczne, ale różnią się wyglądem zewnętrznym. Obsługują do 1000 kart lub breloków zbliżeniowych, przy czym dwa transpondery mogą funkcjonować jako napadowe lub pod przymusem – ich użycie otworzy drzwi, ale jednocześnie wywoła cichy alarm.
Wbudowane wyjście przekaźnikowe ma dwa tryby pracy: monostabilny i bistabilny. Wejście i wyjście w formacie Wiegand może mieć od 26 do 37 bitów, a kody użytkowników są transmitowane jako 4-bitowe, 8-bitowe (ASCII) lub 10-cyfrowe numery wirtualne. Czytniki pracują w zakresie temperatury od -40°C do 60°C. Ich solidna obudowa, łącznie z klawiszami, również została wykonana z metalu.

OPTEX
Sensing Innovation

NIC CI NIE UMKNIE

Dwie niezależne strefy detekcji w czujce BX Shield

BX Shield
Zewnętrzna kurtyna PIR
Dwie niezależne strefy detekcji po 12 m
Modele przewodowe / bezprzewodowe
z antymaskingiem

Czujki z serii BX Shield łączą w sobie niezawodną technologię z nowoczesnym wzornictwem. Linia produktów składa się z łatwych w instalacji i konfiguracji detektorów kurtynowych niskiego montażu. Urządzenia z serii BX Shield idealnie sprawdzają się przy zabezpieczeniu wąskiego obszaru bezpośrednio przyległego do zewnętrznych ścian budynku.

Technologia czterech piroelementów zastosowanych w czujce umożliwia ustawienie dwóch niezależnych obszarów detekcji (lewego i prawego). Strefy mają regulowany zasięg do 12 m każdy. Czujka jest odporna na obecność małych zwierząt i niekorzystne warunki środowiskowe.

Aktywacja alarmu w detektorze niezależnie dla prawego i lewego obszaru detekcji jest przydatna w wypadku połączenia z kamerami CCTV. Rozwiązanie to wykorzystujemy w wideoweryfikacji alarmów, zarówno w zastosowaniach indywidualnych jak i komercyjmych.

Więcej informacji na www.optex-europe.com

Nowe kamery PTZ serii Wisenet Q od Hanwha Techwin

Hanwha Techwin Europe
www.hanwha-security.eu

Hanwha Techwin wprowadza do oferty dwa nowe modele kamer PTZ o rozdzielczości full HD, z 23-krotnym zoomem optycznym. QNP-6230 i QNP-6230H to, odpowiednio, modele do montażu wewnątrz i na zewnątrz pomieszczeń. Model zewnętrzny ma obudowę o klasie szczelności IP66 i odporności udarowej IK10. Kamery wspierają kompresję H.265, H.264 i MJPEG oraz transmisję wielostrumieniową. Oba modele są wyposażone w mechanicznie przesuwany filtr IR oraz WDR 120 dB. Stabilizację obrazu wspomaga sensor żyroskopowy.
Technologia transmisji *Wisestream II* z kompresją H.265 oraz doskonała cyfrowa redukcja szumów 2D i 3D zmniejszają generowany strumień danych nawet do 75% w porównaniu ze standardową kompresją H.264, co wydatnie redukuje koszt dysków twardych w systemach zapisu.
Wbudowane gniazdo na karty SD pozwala na zapis równoległy lub awaryjny do 256 GB danych, co w połączeniu z funkcją ARB (automatyczne odzyskiwanie kopii zapasowej przez rejestratory *Wisenet*) gwarantuje najwyższy poziom bezpieczeństwa danych. Funkcja ta, a także alarmowanie o sabotażu, szyfrowane pliki konfiguracji, oprogramowanie układowe i programowana retencja danych na karcie SD czynią z kamer serii *Wisenet Q* produkty wspierające klientów w dostosowaniu się do rozporządzenia RODO. Doskonała, konkurencyjna cena nowych kamer jest idealnym uzupełnieniem ich świetnych parametrów funkcjonalnych.

Inspekcyjna kamera Hikvision DS-2TP03-15VM/W

Hikvision
www.hikvision.com/pl/

Model DS-2TP03-15VM/W to termograficzna kamera inspekcyjna firmy Hikvision, zaprojektowana do pomiaru temperatury z dużą dokładnością ±2°C. Zakres pomiarowy kamery wynosi od -20°C do 650°C.
Przetwornik termowizyjny zastosowany w kamerze generuje obraz o rozdzielczości 384 x 288, natomiast obraz z modułu optycznego ma rozdzielczość 1920 x 1080 pikseli. Ponadto kamera została wyposażona w 3,5” ekran dotykowy, na którym można wyświetlać obrazy z poszczególnych przetworników oraz nakładać je na siebie (obraz w obrazie, fuzja obrazów).
Wbudowana pamięć 64 GB umożliwia zapisywanie nagrań i zrzutów obrazu. Ponadto kamera zawiera slot na kartę pamięci micro SD, która umożliwia zwiększenie czasu zapisu.
Kamera ma wbudowany moduł GPS, *Bluetooth*, elektroniczny kompas. Obsługuje także Wi-Fi, dzięki czemu możliwy jest zdalny podgląd na żywo obrazu z kamery.
Kamera inspekcyjna świetnie sprawdza się jako narzędzie diagnostyczne. Umożliwia w sposób bezdotykowy wykrywanie wad, uszkodzeń lub miejsc potencjalnych awarii, np. instalacji elektrycznych, bez konieczności wyłączeń i nie powodując przerwy w pracy przedsiębiorstwa.
Ten model kamery jest wyposażony w baterię litową umożliwiającą ciągłą pracę przez ponad 4 godziny.

Eagle Eye Networks – bezpieczny monitoring w chmurze

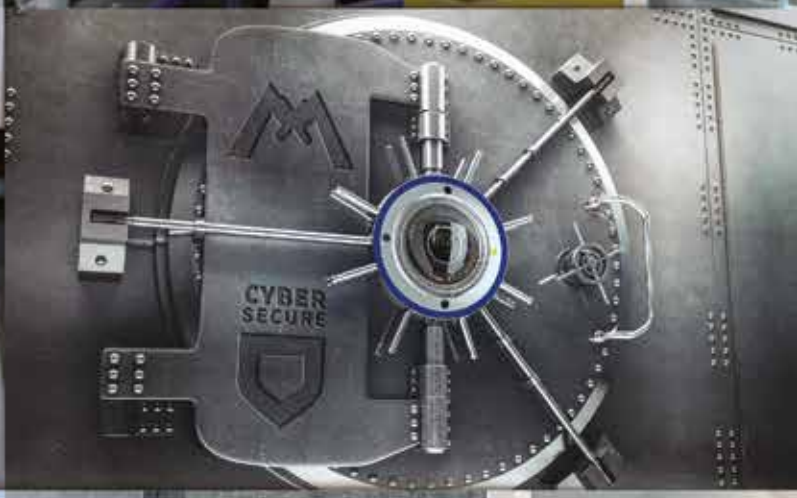
Linc Polska
www.linc.pl

Usługi *Video Surveillance as a Service* (VSaaS) stają się coraz bardziej popularne. Możliwość zastosowania dowolnych kamer IP lub analogowych oraz archiwizacja w chmurze sprawiają, że zyskały duże grono zwolenników. Dokonując wyboru ich dostawcy, należy zwrócić uwagę przede wszystkim na zapewnienie bezpieczeństwa danych w sieci.
Eagle Eye Networks przechowuje informacje w tych samych centrach danych, które obsługują strategiczne instytucje, np. banki i firmy telekomunikacyjne, dla których bezpieczeństwo jest również kwestią priorytetową.
Rozwój technologii sprawia, że systemy dozoru wizyjnego stają się coraz bardziej precyzyjne i skuteczne. Eagle Eye Networks umożliwia zarządzanie strumieniem danych pomiędzy kamerami a rejestratorem oraz rejestratorem a chmurą, jednocześnie kontrolując rozdzielczość obrazu i wymaganą przestrzeń dyskową. Dostęp do obrazu z kamer jest możliwy w każdej chwili (365/7/24).
Rozwiązanie oferuje funkcjonalności pozwalające w wymierny sposób obniżyć miesięczny koszt ochrony. Można np. ustawić funkcje analityczne w chmurze (zliczanie obiektów, przekroczenie linii, wejścia w obszar). Każda z nich generuje alarm, który można zdalnie zweryfikować i podjąć decyzję co do dalszych działań. Wybór abonamentów umożliwia dostosowanie usługi do indywidualnych potrzeb. Eagle Eye Networks to bezpieczny i ekonomiczny monitoring w chmurze.

MOBOTIX

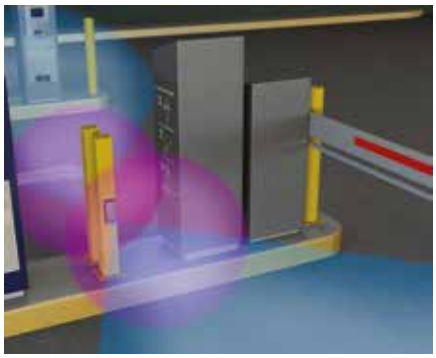
BeyondHumanVision

Linc Polska Sp. z o.o.



www.linc.pl

Skuteczne zarządzanie ruchem na parkingu



Optex Security
www.optex.com.pl

OPTEX w swoim nowym produkcie wykorzystał dwie technologie: mikrofalową i ultradźwiękową, tworząc linię bardzo skutecznych czujek parkingowych.
Głównym zastosowaniem modelu OVS-01GT jest zautomatyzowanie podnoszenia szlabanu. Dwustopniowy algorytm wykrywa pojazd, który zatrzymał się przed szlabanem. Czujka ma łatwo konfigurowalne wyjścia przekaźnikowe (o parametrach obciążalności 30 V, 300 mA), które można łatwo zintegrować z istniejącym systemem parkingowym.
Drugi model OVS-01CC jest przeznaczony do liczenia pojazdów poruszających się z prędkością do 60 km/h. Dane te można wykorzystać do efektywnego informowania o wolnych miejscach parkingowych.
Największą przewagą czujek jest to, że stanowią alternatywę dla pętli indukcyjnej. Ich montaż nie sprawia kłopotów nawet na nierównym lub miękkim podłożu czy posadzce garażu. Koniec z kuciem betonu i niedogodnościami związanymi z zatrzymaniem ruchu na czas prac remontowych. Wystarczy postawić słupek w odpowiednim miejscu i zamontować na nim detektor, a na panelu sterowania ustawić czułość i zasięg detekcji. Proces kalibracji jest zautomatyzowany, wymaga tylko naciśnięcia jednego przycisku.
Czujki parkingowe OPTEX skutecznie rozpoznają pojazdy, ignorując jednocześnie ruch pieszych. Wbudowana grzałka usuwa śnieg i lód, który mógłby wpłynąć na poprawność działania urządzenia.
Detektory OVS-01 sprawdzą się we wszystkich obiektach, gdzie ważne jest odpowiednie zarządzanie ruchem pojazdów.

SIS-FIRE: Zintegrowany system zarządzania bezpieczeństwem pożarowym

Schrack Seconet Polska
www.schrack-seconet.pl

System SIS-FIRE jest przeznaczony do wizualizacji, sterowania i zarządzania urządzeniami ppoż., a także innych systemów i urządzeń mających wpływ na bezpieczeństwo pożarowe (kryzysowe) obiektu – zapewnia maks. poziom ochrony, tworząc spójne, w pełni kompatybilne i kompleksowe narzędzie nadzoru nad budynkiem. SIS-FIRE powstał na bazie wieloletnich doświadczeń Schrack Seconet w produkcji systemów bezpieczeństwa pożarowego.
W skład systemu wchodzą:
• 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 z modułami we/wy techniki X-LINE,
• sterowniki urządzeń technicznych i ppoż. SF-CONTROL (w różnych wersjach).
Podstawową zaletą systemu jest elastyczność umożliwiająca optymalny (dla konkretnego obiektu) dobór elementów i funkcji, z zapewnieniem ścisłej współpracy i podziału kompetencji pomiędzy nimi. Redundancja komponentów bazujących na systemie Integral IP MX oraz (opcjonalnie) platformy informatycznej SIS-FIRE zapewnia ciągłość działania nawet w przypadku awarii pojedynczych elementów całego układu.
Istotną cechą systemu integrującego (w przeciwieństwie do standardowego systemu SSP) jest możliwość spełnienia nieograniczonej liczby zadań i funkcji logicznych związanych z obsługą, sterowaniem i nadzorowaniem zintegrowanych systemów w obiekcie.

TP-Link EAP225 – punkt dostępowy Wi-Fi do zastosowań biznesowych

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

Zapewnienie stabilnych i szybkich połączeń sieciowych to wyzwanie, któremu muszą sprostać dostawcy Internetu, producenci sprzętu sieciowego oraz administratorzy w takich obiektach, jak szkoły, kampusy, centra handlowe, hotele czy biura. Każde z nich wymaga jak najlepszego dostępu do sieci. TP-Link ułatwia to zadanie – oferowany punkt dostępowy EAP225 to bezpieczne, łatwe w instalacji i zarządzaniu rozwiązanie do budowy sieci bezprzewodowej na dużych powierzchniach. Sprawdzi się jako bezpieczne rozwiązanie w miejscach, w których z Wi-Fi korzystają nie tylko stali użytkownicy, ponieważ umożliwia stworzenie sieci dla gości – z logowaniem przez stronę powitalną, vouchery lub jednorazowe hasła dostępu.
EAP225 zapewnia duże prędkości transmisji (pracuje w standardzie 802.11ac) nawet do 1350 Mb/s w dwóch pasmach. Zastosowanie technologii MU-MIMO *(Multi User-MIMO)* pozwala osiągnąć szybkość połączeń do 867 Mb/s wielu urządzeniom jednocześnie. Jeszcze szybsze połączenie zapewnia funkcja *Band Steering,* automatycznie wybierająca optymalne pasmo transmisji w przypadku urządzeń dwuzakresowych. Model wyposażono w gigabitowy port Ethernet. Bezpłatne oprogramowanie TP-Link EAP Controller pozwala z dowolnego komputera zarządzać centralnie siecią bezprzewodową złożoną z setek urządzeń. Zasilanie w standardzie PoE 802.3af lub z wykorzystaniem pasywnego PoE z dołączonym do zestawu injectorem ułatwia instalację i obniża jej koszty.

ZETTLER

Tradycja tworzenia nowatorskich rozwiązań z zakresu wykrywania pożaru

ZETTLER z dumą prezentuje wieloletnią tradycję w kreowaniu nowatorskich technologii wykrywania pożaru. Oferta ZETTLER została stworzona w oparciu o technologię MZX, która zapewnia najbardziej zaawansowane funkcje wykrywania pożaru.

Więcej informacji na stronie:
www.zettlerfire.com

ŚNIADANIE EKSPERTÓW

Transport i logistyka

Specyficzne rozwiązania security dla transportu czy problemy w zapewnieniu bezpieczeństwa łańcucha logistycznego...
Rozmawiali o tym uczestnicy kolejnego śniadania ekspertów „a&s Polska".

Film ze spotkania na:
http://aspolska.pl/sniadanie_transport

Przedstawiciele firm z branży zabezpieczeń z odbiorcami i użytkownikami systemów security spotkali się w warszawskim hotelu Westin 2 marca. Podczas wspólnego śniadania w luźnej atmosferze rozmawiali o ważnym temacie bezpieczeństwa w transporcie i logistyce.
To spotkanie zainaugurowało drugi rok organizowanych cyklicznie „Śniadań ekspertów", które na stałe wpisały się w kalendarz wydarzeń branżowych. O sukcesie świadczy nie tylko duże zainteresowanie spotkaniami, ale także komentarze uczestników.

Kolejne „Śniadanie ekspertów" o bezpieczeństwie infrastruktury krytycznej odbędzie się 25 maja. Szczegóły na s. 52.

Jakub Kozak
Axis Communications

Spotkanie było bardzo owocne – tego typu wydarzenia są bardzo potrzebne. Jeśli strona producenta (vendorzy i producenci) nie będą mieli kontaktu z klientami, nie będą znali realnych potrzeb użytkowników i ich produkty nie będą miały szansy rozwijać się tak dobrze i tak skutecznie, jak to jest potrzebne.

Spotykają się tutaj ludzie z branży, zarówno ze strony oferenta, jak i klienta końcowego. Wymiana informacji i – mówiąc wprost – wizytówek pomaga nam, klientom docelowym, prowadzić nasze biznesy.

Krzysztof Wilczyński
Ceva Logistics Poland

Robert Jakubowski
Linc Polska

Takie spotkania są bardzo istotne – szczególnie dla dystrybutorów i dostawców rozwiązań technicznych. Dzięki uczestnictwu w takich wydarzeniach możemy znaleźć pomysł na dostosowanie systemów do potrzeb użytkowników.

Tego typu spotkania, gdzie spotykają się wszystkie strony zainteresowane logistyką i transportem, są jak najbardziej wskazane. Nie jesteśmy jedynie dostawcami urządzeń, ale także klientami firm transportowych i logistycznych, które się tutaj pojawiły. Mamy więc pełną synergię – my dowiadujemy się od nich wiele, ale i oni od nas mogą się czegoś dowiedzieć.

Piotr Świder
Hikvision Poland

Tomasz Siwicki
GEFCO Polska

Ciekawe spotkanie. Można tu spotkać producentów z branży security, którzy okazują się naszymi klientami. Świetne wydarzenie – mam nadzieję, że w kolejnym też uda mi się uczestniczyć.

Całą branżę security czeka jeszcze wiele pracy, aby dostosować się do zmieniających się zagrożeń w zakresie ochrony transportu. Myślę, że ścisła współpraca między producentami i klientami w niedalekiej przyszłości może zaowocować bardzo ciekawymi rozwiązaniami.

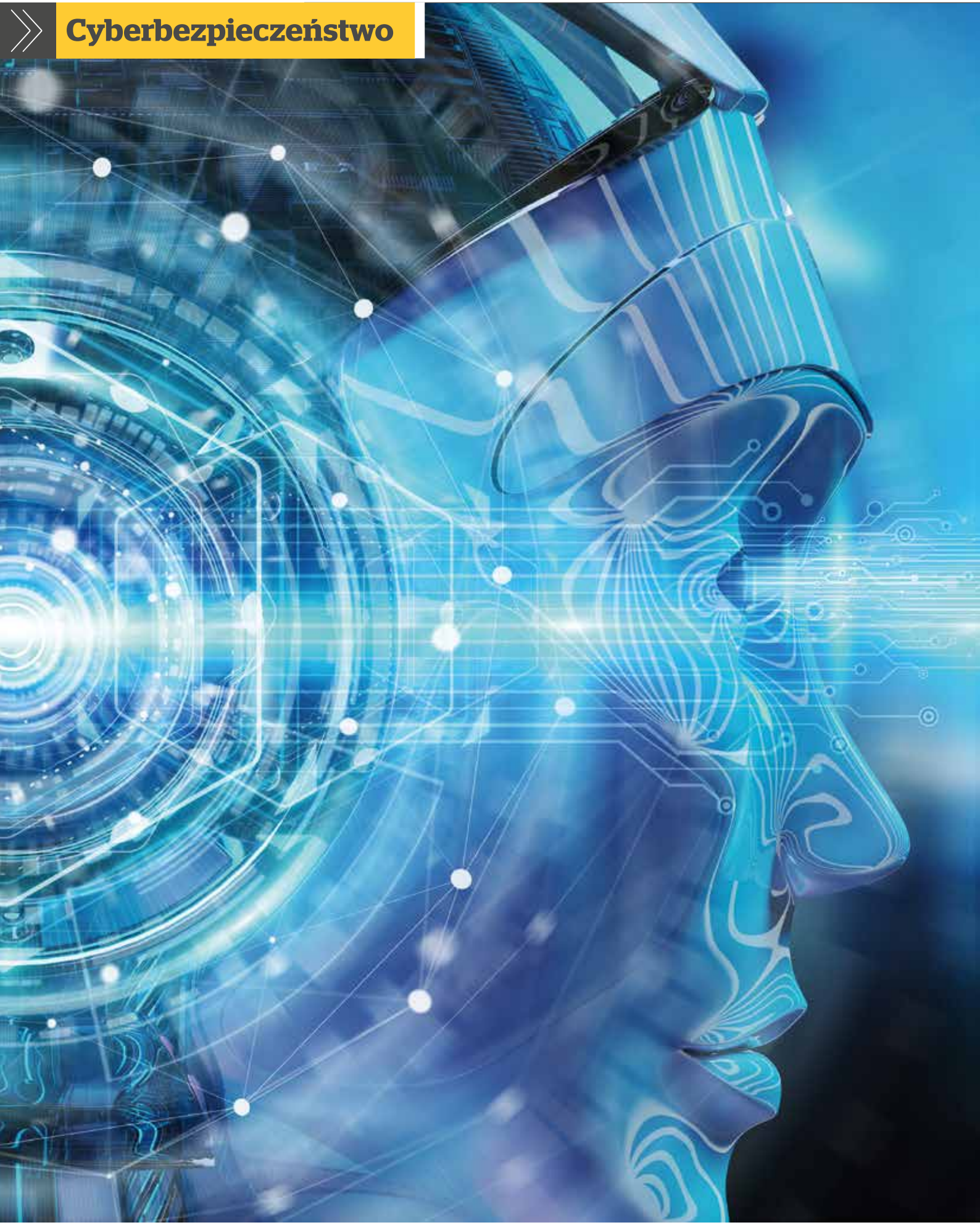
Marcin Ruciński
Dahua Technology Poland

Witold Safarzyński
Omtech

Bardzo interesujące spotkanie. Zainspirowało mnie i zaowocuje kilkoma pomysłami na to, w jakim kierunku moglibyśmy pójść w rozwoju naszych produktów.

Andrzej Żochowski
TNT EXPRESS

Spotkanie ma bardzo ciekawą formułę. Jest to wymiana doświadczeń zarówno po stronie osób czy firm dostarczających rozwiązania, jak również po stronie branży i security managerów. Uważam, że jest to bardzo dobra formuła i powinna być z całą pewnością kontynuowana.



Sztuczna inteligencja

w służbie cyberbezpieczeństwu infrastruktury krytycznej

SZANSE I ZAGROŻENIA

Tempo rozwoju świata wymusza coraz większą automatyzację zadań wykonywanych dotychczas albo manualnie, albo przez sterowniki analogowe. Z perspektywy optymalizacji procesu jest to trend, którego nie da się już zawrócić.

Dla specjalisty do spraw bezpieczeństwa automatyzacja jest większym problemem i bólem głowy, poczynając od potrzeby zapewnienia interoperacyjności narzędzi, których wyprodukowanie niejednokrotnie dzielą dekady, do ciągłego śledzenia potencjalnych zagrożeń dla zainstalowanej infrastruktury, które są odkrywane każdego dnia. A to tylko przy założeniu, że taki proces śledzenia podatności jest w przedsiębiorstwie realizowany oraz że podatność da się wykryć zdalnie, a nie przez odwiedzenie wszystkich jednostek organizacyjnych firmy.

Dla przykładu na konferencji *Black Hat 2017* przedstawiciel firmy IOActive pokazał wyniki badań nad oprogramowaniem stacji do wykrywania promieniowania radioaktywnego. Odkrycia są równie szokujące, co proste do niewłaściwego wykorzystania. Dla przykładu – jedna z bramek do wykrywania promieniowania miała wprowadzonych kilka poziomów uprawnień. Badanie kodu programu ujawniło jednak, że producent pozostawił również tylną furtkę dającą maksymalne uprawnienia. Konstrukcja kodu pokazuje, że było to działanie jak najbardziej celowe a konsekwencją wykorzystania takiego dostępu jest na przykład możliwość wyłączenia alarmu radiacyjnego, czyli głównej funkcjonalności całego mechanizmu.

W tym momencie przez głowę specjalisty do spraw zabezpieczeń infrastruktury krytycznej przelatuje tornado emocji. Od ulgi związanej z faktem, że ktoś wykrył tę podatność, przez ciekawość, ile takich podatności jest nieznanych, przez niepewność związaną z pytaniem, czy w zarządzanej infrastrukturze są takie tylne furtki, aby w końcu zatrzymać się na uczuciu przytłoczenia związanego z koniecznością zapewnienia ciągłości bezpieczeństwa nie tylko dla infrastruktury jako całości, ale również dla każdego komponentu z osobna wiedząc, że jedna rzecz od 24 lat na pewno się nie zmieniła. W dalszym ciągu zorganizowane grupy przestępcze stają się bardziej aktywne w próbie uzyskania dużych partii cennych materiałów z przedsiębiorstw. Kontaktują się z personelem, badają słabe punkty systemu i możliwości kradzieży lub zakłócenia działalności na wielką skalę.

Czy sztuczna inteligencja może przyjść tu z pomocą? Gdzie już jest wykorzystywana a gdzie powinniśmy ją zacząć wykorzystywać w najbliższej przyszłości? Co ze skutkami działań systemów autonomicznych posiadających funkcje samouczące? Jakie korzyści a jakie zagrożenia niesie za sobą wykorzystanie sztucznej inteligencji nie tylko do wykrywania, ale również do zwalczania cyberataków? Nie bez znaczenia będzie też wyciągnięcie wniosków z istniejących już wdrożeń systemów bezpieczeństwa wspomaganych sztuczną inteligencją.

Przykłady zastosowań

Głównym celem badań nad sztuczną inteligencją jest stworzenie technologii pozwalającej komputerom i maszynom

W zależności od tego czyje cele realizuje system sztucznej inteligencji (korporacji, socjopatów, dyktatorów, wojska, przemysłu, terrorystów itd.) możemy mieć do czynienia z konsekwencjami bezprecedensowymi w historii ludzkości.

funkcjonować w inteligentny sposób. Całość wyzwań można rozbić na podkategorie w następujący sposób:

- uczenie się,
- rozumienie języka naturalnego,
- wnioskowanie i rozwiązywanie problemów,
- planowanie,
- kreatywność,
- inteligencja społeczna,
- generyczna inteligencja,
- prezentowanie wiedzy,
- percepcja,
- motywacja i manipulacja.

W niedalekiej przyszłości, gdy systemy sztucznej inteligencji staną się bardziej skuteczne, zaczniemy widzieć bardziej zautomatyzowane i coraz bardziej wyrafinowane ataki socjotechniczne. Wzrost liczby cyberataków wspieranych sztuczną inteligencją spowoduje eksplozję włamań do sieci, kradzieży danych osobowych i rozprzestrzeniania się inteligentnych wirusów komputerowych na skalę epidemii. Ironicznie, naszą najlepszą nadzieją, aby bronić się przed włamaniami wspieranymi funkcją sztucznej inteligencji, jest użycie sztucznej inteligencji. Prawdopodobnie jednak doprowadzi to do wyścigu zbrojeń, którego konsekwencje mogą być bardzo kłopotliwe w dłuższej perspektywie, zwłaszcza gdy aktorzy rządowi dołączą w większej skali do cyberataków na cele komercyjne.

Biorąc pod uwagę ilość zastosowań sztucznej inteligencji w codziennym życiu (Siri, Netflix, Nest, Alexa, chatboty, autonomiczne samochody itp.) oczekiwania wobec zastosowania sztucznej inteligencji do walki z cyberprzestępczością są uprawnione. Niektóre raporty szacują, że wielkość rynku sztucznej inteligencji i robotyki osiągnie 153 miliardy dolarów do 2020 roku. Rozwój tego obszaru w ostatnich latach jest fenomenem. Google przewiduje, że roboty osiągną poziom ludzkiej inteligencji do roku 2029 a analitycy z McKinsey&Company dowiedli, że prawie 50% amerykańskich i europejskich miejsc pracy może być całkowicie zautomatyzowanych.

Czy można przyjąć więc, że mamy do czynienia ze zmierzchem cyberprzestępczości i świtem zautomatyzowanej ochrony opartej na sztucznej inteligencji? Tylko druga teza ma poparcie w analizowanych faktach. W związku z faktem, że cyberzagrożenia robią się coraz bardziej zaawansowane i również wspierane przez sztuczną inteligencję, należy dobrze zrozumieć, co sztuczna inteligencja może zrobić, czego nie może i czego wręcz nie powinna robić, aby zminimalizować płaszczyznę potencjalnego ataku. Zwłaszcza że zgodnie z tezą ortogonalności Bostroma dowolny system sztucznej inteligencji może charakteryzować się dowolną konfiguracją inteligencji i celów. Takie cele mogą zostać zdefiniowane na etapie projektu, przez włamania przestępców lub w późniejszym etapie przy użytkowaniu systemów. W konsekwencji, w zależności od tego czyje cele realizuje system sztucznej inteligencji (korporacji, socjopatów, dyktatorów, wojska, przemysłu, terrorystów itd.) możemy mieć do czynienia z konsekwencjami bezprecedensowymi w historii ludzkości.

Obecnie systemy automatyzujące prace analityków bezpieczeństwa czy automatycznie zabezpieczające infrastrukturę krytyczną bez udziału człowieka są już dostępne. W dalszej części analizie poddane zostaną możliwości w kontekście potencjalnych zastosowań.

Ochrona przed atakiem i przed błędami w oprogramowaniu

Oprogramowanie zarządzające komputerami, sterownikami i urządzeniami typu „smart" w infrastrukturze jest naturalnie podatne zarówno na błędy w kodzie, jak i błędy ludzkie, które mogą być wykorzystane przez przestępców. Potencjał konsekwencji jest praktycznie nieskończony i może dotyczyć bezpieczeństwa jednostki, regionu czy całego kraju. Środki ochrony muszą więc być przystosowane do wykrywania pojedynczego hakera, grupy przestępczej oraz coraz częściej oprogramowania samodzielnie wspieranego przez systemy sztucznej inteligencji z mechanizmami polimorficznymi lub zmieniać sposób zachowania w zależności od konieczności i dostępnych wektorów ataku. Rozwój systemów, które mogą wyszukiwać i naprawiać te błędy i luki w zabezpieczeniach, a także bronić przed atakami wyrósł z tej pilnej potrzeby, a wiele firm, które pracują nad autonomicznymi systemami, jest finansowana przez wojsko (DARPA) i przez uznane uniwersytety na całym świecie.

Najczęściej podawanym przykładem samodzielnego systemu zabezpieczającego jest rozwiązanie Mayhem tworzone w startupie ForAllSecure wspólnie z Uniwersytetem Carnegie Mellon – zwycięzca zawodów autonomicznych systemów bezpieczeństwa – *Cyber Grand Challenge*, które odbyły się 4 sierpnia 2016 r. w Las Vegas. Ich organizatorem jest amerykańska agencja zaawansowanych projektów obronnych DARPA podlegająca Pentagonowi. Autonomiczne programy miały bronić się przed włamaniami i próbować zaatakować przeciwników, wykorzystując wiedzę o lukach. DARPA wprowadziła jednak nowy element – serwery, na których uruchomiono e-hakerów, musiały cały czas normalnie funkcjonować. Analiza kodu, obrona i atak nie mogły znacząco spowolnić normalnej pracy. Jak się okazało, miało to znaczenie dla ostatecznej klasyfikacji.

Tego typu systemy, autonomicznie analizujące luki w oprogramowaniu i potrafiące je automatycznie zabezpieczać to bliska przyszłość każdego centrum cyberbezpieczeństwa. Na chwilę obecną jednak są jeszcze niedoskonałe, co pokazała późniejsza konferencja *Def Con 2016,* gdzie Mayhem jako pierwszy w historii autonomiczny „haker" przystąpił do zawodów typu *Capture the*

Flag. Mimo że ostatecznie finiszował na ostatnim miejscu, to w trakcie rozgrywki parokrotnie wyprzedzał zespoły ludzkie. W ostatecznej klasyfikacji zabrakło mu jedynie 1,8% punktu, żeby wyprzedzić zespół sklasyfikowany na przedostatnim miejscu. To pokazuje, jak niewielki postęp jest potrzebny, by wprowadzić autonomiczne systemy do użytku komercyjnego.

Inteligentne systemy wsparcia analityków bezpieczeństwa

Podczas gdy autonomiczne systemy bezpieczeństwa są jeszcze (niedaleką) przyszłością, większość specjalistów do spraw bezpieczeństwa prędzej czy później będzie miała do czynienia z kilkoma problemami obrazującymi prozę współczesnego przedsiębiorstwa w tak dynamicznie rozwijającym się technologicznie środowisku.

Po pierwsze, przedsiębiorstwom zaczynają doskwierać konsekwencje dotychczasowego braku praktyk typu *security by design*. Innymi słowy, większość systemów komercyjnych, a zwłaszcza systemów dziedzinowych, była pisana nie uwzględniając współczesnych zagrożeń cybernetycznych. Konsekwencją takich wieloletnich zaniedbań jest konieczność *de facto* monitorowania całości infrastruktury informatycznej, anomalii w zachowaniu użytkowników oraz korelowania informacji między systemami w celu identyfikacji zagrożeń dla infrastruktury i danych firmy. Wykrywać należy również takie niespodziewane tylne furtki jak we wspomnianych systemach do monitorowania radiacji, których zresztą producent odmówił załatania twierdząc, że systemy wykrywania radiacji są instalowane w bezpiecznych lokalizacjach. Pytaniem otwartym pozostaje, co się stanie, jeśli w systemach chroniących te lokalizacje również znajdą się tylne furtki lub błędy w algorytmach zabezpieczeń.

Drugim wyzwaniem dla każdego działu bezpieczeństwa jest efektywne wykorzystanie całości wiedzy dostępnej w Internecie i w sieciach zanonimizowanych typu Tor czy I2P. Każdy analityk bez wątpienia chciałby działać proaktywnie i wykrywać luki w zabezpie-

czeniach zanim zagrożenie nadejdzie. Praktyka jednak pokazuje, że większość czasu specjaliści spędzają raczej na gaszeniu pożarów, niż na systematycznym przyswajaniu dostępnej wiedzy. Zresztą istniejąca, i wciąż rosnąca ilość dostępnej wiedzy jest nie do przyswojenia przez człowieka. Co więcej, jej realne wykorzystanie w momencie zagrożenia, pod presją czasu i odpowiedzialności, jest mocno ograniczone.
Trzecim problemem, który zaczyna być coraz bardziej widoczny, jest powiększający się niedobór doświadczonych specjalistów ds. bezpieczeństwa. Szacuje się, że na rynku brakuje około 1,5 miliona specjalistów i liczba ta się powiększa.
Odpowiedzią na wszystkie trzy problemy jest efektywne wykorzystanie dostępnych już na rynku systemów kognitywnych, opracowanych (czyt. nauczonych) aby rozumiały zagadnienia z zakresu cyberbezpieczeństwa. Narzędzia kognitywne mają na celu wesprzeć analityków bezpieczeństwa w analizie zdarzeń i korelacji informacji z wewnątrz przedsiębiorstwa z wiedzą dostępną w sieci. Dzięki takiemu podejściu analityk, który zidentyfikuje podejrzane zachowania w infrastrukturze, będzie automatycznie wsparty całą dostępną w sieci wiedzą na temat tego konkretnego zagrożenia. Praktyka pokazuje, że współcześnie systemy kognitywne potrafią oszczędzić analitykom bezpieczeństwa i analitykom SOC do 50% czasu związanego z wyszukiwaniem i klasyfikowaniem informacji.

Ochrona prywatności i bezpieczna komunikacja

W przypadku każdej infrastruktury, ale w szczególności w przypadku infrastruktury krytycznej, zapewnienie bezpiecznej komunikacji pomiędzy komponentami systemu oraz zabezpieczenie danych wrażliwych staje się coraz większym wyzwaniem. Zwłaszcza w przypadku, gdy nadchodząca era komputerów kwantowych zaczyna poważnie zagrażać skuteczności części algorytmów szyfrowania.
Z tym większym zainteresowaniem świat obserwował jeden z najciekawszych eksperymentów przeprowadzonych prze badaczy z Google Brain,

którzy oprogramowali dwie uczące się maszyny (a konkretnie dwie sieci neuronowe) Bob i Alice, aby same wymyśliły bezpieczny sposób komunikacji, oraz zlecili trzeciej maszynie (Eve) przechwycić i rozkodować przekaz. W skrócie, naukowcy z Google Brain odkryli, że odpowiednio oprogramowana sztuczna inteligencja, tworzy dziwnie nieludzkie schematy kryptograficzne i że lepiej radzi sobie z szyfrowaniem niż deszyfracją. Ostatecznie naukowcy stwierdzili, że Bob i Alice opracowały solidny protokół szyfrowania. Eve z drugiej strony po początkowych sukcesach nie potrafiła już odszyfrować komunikacji systemów, które nieustannie się uczyły i poprawiały swój algorytm. Oznacza to, że już dzisiaj roboty mogą ze sobą rozmawiać w sposób, którego ani inne roboty ani, co za tym idzie, ludzie, nie są w stanie zrozumieć i złamać.

Mimo że na pierwszy rzut oka taka perspektywa może się wydawać niekomfortowa lub wręcz niebezpieczna, to niesie ze sobą kolosalne możliwości w zakresie zabezpieczania danych, a zwłaszcza w zakresie bezpiecznej pracy na danych zaszyfrowanych. Odkąd w 2009 roku Craig Gentry udowodnił, że pełne szyfrowanie homomorficzne jest możliwe w praktyce – badania nad tym obszarem przybliżają nas z każdym dniem do zastosowań komercyjnych. W skrócie – pełne szyfrowanie homomorficzne umożliwia dowolne działania na danych zaszyfrowanych. Dzięki zastosowaniu takiego szyfrowania oraz bezpiecznej komunikacji stworzonej przez samouczące się sieci neuronowe jesteśmy w stanie pracować na najważniejszych danych dla firmy nie tylko w szerszej skali, ale przede wszystkim bez strachu o to, że te dane wpadną w ręce przestępców lub konkurencji. Przez wielu szyfrowanie homomorficzne postrzegane jest jako Święty Graal kryptografii, a przez dostawców rozwiązań przetwarzania w chmurze wyczekiwana jest pełna komercjalizacja rozwiązań w oparciu o szyfrowanie homomorficzne.

Zabezpieczanie urządzeń IoT

Według Gartnera, do końca roku konsumenci będą korzystać z ponad 8 miliardów podłączonych urządzeń.

> Wielu producentów inteligentnych urządzeń nie wie, jak zabezpieczyć urządzenia IOT przed cyberatakiem, a wielu to nie interesuje, bo koncentrują się na funkcjonalności.

Te urządzenia IoT, takie jak inteligentne telewizory, tablety, smartfony, notebooki, urządzenia do noszenia, czujniki, termostaty, asystenci itd, sprawią, że nasze życie będzie bardziej efektywne, oszczędzające energię, bardziej komfortowe i mniej kosztowne. Jak pokazał przykład botnetu Mirai z 2016 roku – życie będzie również bardziej wygodne dla przestępców mogących wykorzystać niezabezpieczone (czyli większość) urządzeń IoT do swoich celów.

Rzeczywistość bezpieczeństwa IoT jest dość mizerna: wielu producentów inteligentnych urządzeń nie wie, jak zabezpieczyć urządzenia IOT przed cyberatakiem, a wielu to nie interesuje, bo koncentrują się na funkcjonalności. Przez to jednak ogromna liczba urządzeń IoT nie ma nawet infrastruktury wspierającej do uruchamiania rozwiązań zabezpieczających, a całkiem sporo również nie ma nawet mechanizmów aktualizacji.

Nie bez powodów Senat USA przyjął w sierpniu 2017 r. pierwszą legislację dotyczącą urządzeń IoT – The Internet of Things Cybersecurity Improvement Act. Prawo dotyczy wprawdzie urządzeń IoT używanych i kupowanych w ramach administracji rządowej, ale wprowadzone przez nie standardy będą prawdopodobnie podstawą do stworzenia standardów sektorowych. Tym bardziej przeraża fakt, że w 2017 r. potrzebne jest prawo, które wprowadza dla urządzeń cyfrowych:

a) możliwość aktualizacji;
b) zakazuje wpisywanych „na sztywno" haseł w kodzie;
c) nakazuje, aby urządzenia nie były podatne na znane podatności.

Ten ostatni wymóg jest zresztą trudny do wdrożenia, gdyż znając mechanizm zakupów w administracji udowodnienie, że urządzenie jest podatne, stanie się standardowym mechanizmem walki konkurencyjnej.

Z perspektywy infrastruktury krytycznej pojedynczy smartwatch czy telewizor wiszący w sali konferencyjnej nie jest może zagrożeniem krytycznym (chyba że są połączone w sieć i wykorzystane do przeprowadzenia ataku typu DoS na infrastrukturę firmy), ale nawet takie pojedyncze urządzenia świetnie się sprawdzają w fazie rekonesansu poprzedzającej atak właściwy. Dzieje się tak, ponieważ większość systemów bezpieczeństwa przedsiębiorstwa nie traktuje sprzętu IoT jako części infrastruktury informatycznej, którą należy zabezpieczać. W związku z tym nadają się one idealnie do wykorzystania nie tylko podczas rekonesansu, ale również (jeśli nie przede wszystkim) w atakach z wewnątrz firmy.

Zabezpieczenia przeciwko zagrożeniom wewnętrznym (*insider threat*)

Niezadowolony pracownik wynoszący w tajemnicy poufne informacje, niedbały kierownik klikający na link ze złośliwym oprogramowaniem, czy może przestępca uzyskujący dostęp do infrastruktury krytycznej za pomocą skradzionych poświadczeń: to wszystko dzieje się na co dzień i stanowi jedno z największych wyzwań cyberbezpieczeństwa w 2017 roku.

Alphabet, firma matka Google, złożyła ostatnio sprawę przeciwko byłemu inżynierowi Anthony'owi Levandowskiemu, który obecnie współpracuje z Uberem. Firma oskarżyła Levandowskiego o kopiowanie ponad 14 000 plików wewnętrznych i przekazanie ich bezpośrednio do swojego nowego pracodawcy.

Co jest zagrożeniem dla bezpieczeństwa spowodowanym przez wewnętrznych użytkowników? Prawdą jest, że typowe zagrożenia, takie jak ataki złośliwego oprogramowania, włamania do sieci, ataki typu „odmowa usługi" i *ransomware*, są znacznie częstsze niż ataki wewnętrzne. Takie przeświadczenie panuje przynajmniej w więk-

szości firm, dopóki nie przeprowadzona zostanie właściwa analiza. Podczas gdy wewnętrzne zagrożenia bezpieczeństwa cybernetycznego często są związane ze złośliwymi użytkownikami, w rzeczywistości zwykli pracownicy nieumyślnie powodują naruszenia i wycieki danych firmowych praktycznie codziennie

Utrata poświadczeń następuje z powodu phishingu, kradzieży lub nieświadomego wpuszczania złośliwego oprogramowania do systemu, gdy pracownik kliknie łącze w wiadomości e-mail lub przynosi zainfekowane urządzenie. Nie obejmuje to zwykłych błędów, takich jak wysyłanie poufnych plików na niewłaściwy adres. Wszystko to jest tylko małą listą sposobów, w jaki pracownicy mogą mniej lub bardziej nieświadomie narażać firmy zarówno na straty finansowe, jak i wizerunkowe.

Urządzenia IoT, a także zachowania pracowników na chwilę obecną wymykają się klasyfikacji jako zasoby wymagające monitorowania z uwagi na zagrożenia cybernetyczne. Na szczęście te niedociągnięcia można już zacząć adresować za pomocą sztucznej inteligencji i analityki, a także wykorzystywać matematykę i technologię rozpoznawania wzorów, aby poznać wzorce zachowań pracowników, przewidywać przyszłość i podejmować bardziej efektywne decyzje. Jest to trend, który sprawdził się już w różnych dziedzinach bezpieczeństwa i może poprawić skuteczność walki z zagrożeniami wewnętrznymi poprzez redukcję fałszywych alarmów i znalezienie przysłowiowej igły w stogu siana.

Kluczową technologią wydaje się tutaj być *User Behaviour Analytics* (UBA). Gartner definiuje UBA jako rozwiązania analizujące wzorce zachowań człowieka, a następnie stosujące algorytmy i analizę statystyczną w celu wykrycia znaczących anomalii z tych wzorców – anomalii, które wskazują potencjalne zagrożenia. Tym samym rozwiązania UBA nie tyle skupiają się na analizie informacji z systemów informatycznych, co pozyskanych od ich użytkowników. Systemy typu UBA docelowo mogą bardzo ułatwić również procesy audytu wewnętrznego. Zwłaszcza że nie muszą się przejmować potencjalnymi reperkusjami dla swojej kariery. Co więcej, takie systemy z definicji badają zachowania wszystkich pracowników, podwykonawców i pracowników czasowych mających dostęp do infrastruktury przedsiębiorstwa, a w sytuacji wykrycia niebezpieczeństwa mogą automatycznie zareagować w zaprogramowany sposób.

Zabezpieczanie przed włamaniami do systemów SCADA

Metody zabezpieczania systemów nadzorujących przebieg procesu technologicznego jest tematem na osobne opracowanie, zwłaszcza że jest obciążone wszystkimi wadami struktur tworzonych przez lata. Właściwe zabezpieczenie infrastruktury będzie miało kluczowe znaczenie nie tylko w siedzibie przedsiębiorstwa, ale również (jeśli nie przede wszystkim) w ramach struktur, które znamy pod nazwą smart cities. Inteligentne miasta polegają na wzajemnie połączonych urządzeniach, aby usprawnić usługi miejskie w oparciu o dane uzyskiwane w czasie rzeczywistym. Systemy te łączą sprzęt, oprogramowanie i analizę geoprzestrzenną w celu polepszenia usług komunalnych i optymalizacji wykorzystania przestrzeni miejskiej. Wraz z rozwojem tych technologii stawka ochrony cyfrowych fundamentów miasta będzie coraz wyższa. Tym bardziej że inwestycje w inteligentną infrastrukturę wzrosły, ale wiele z innowacji jest wdrażanych bez solidnych testów, a cyberbezpieczeństwo jest często zaniedbywane. Miasta obecnie wykorzystujące system typu SCADA do kontroli i nadzoru nad swoją infrastrukturą są szczególnie podatne na częste ataki ze względu na słabe protokoły bezpieczeństwa. Choć systemy SCADA sterują procesami na dużą skalę i łączą zdecentralizowane obiekty, rzadko wykorzystują kryptografię na poziomie protokołu i uwierzytelniania.

W ramach europejskich projektów badawczych FP7-SEC-2011-1 Project 285647 i H2020-DS-2015-1 Project 700581 grupa inżynierów przedstawiła pełen zestaw ataków na infrastrukturę opartą na protokole Modbus over TCP/IP. Dlatego też biorąc pod uwagę całą złożoność i historyczne obciążenie systemów SCADA i IASC lepszym pomysłem wydaje się być nie tyle stały i obciążający monitoring całości infrastruktury, co zwłaszcza w przypadku rozproszonego środowiska niesie również problemy związane z opóźnieniami w komunikacji, ale raczej zdefiniowanie standardów inteligentnego analizotora ruchu umożliwiającego zaadresowanie problemu nieprzystosowania systemów SCADA do łączenia się z Internetem. Skoro SCADA jednak jest połączona z Internetem, podstawowym celem takiego inteligentnego filtra jest ochrona przed atakami, które mogłyby doprowadzić do braku ciągłości działania. Grupa naukowców z University of Michigan opracowała techniczną architekturę takiego samouczącego się systemu mającego na celu dopuszczanie do systemu wyłącznie zachowań o znanych parametrach, weryfikując pochodzenie ruchu płynącego przez system oraz przechwytując i buforując podejrzany ruch wykryty w systemie, równolegle testując wykorzystanie przydzielonego pasma. Takie podejście może nie rozwiązuje problemów w sposób systemowy ani nie zwalnia działu bezpieczeństwa od ciągłego monitoringu zagrożeń, ale umożliwia bezpieczne działanie systemu, gdzie bezpieczeństwo jest nadzorowane przez algorytmy samouczące.

Wsparcie procesu uwierzytelniania

Zarządzanie tożsamością i dostępem jest już obecnie jedną z kluczowych broni w arsenale bezpieczeństwa wielu organizacji w celu złagodzenia przypadków naruszania i wycieku danych oraz zaadresowania wyzwań wynikających z przyjęcia nowych trendów, takich jak BYOD. Często za naruszenie danych odpowiada nie tyle system zarządzania tożsamością, co wykorzystanie danych poświadczających tożsamość przez niewłaściwą osobę. Naturalnym kierunkiem migracji wydaje się być więc przejście od haseł biometrycznych do systemu sztucznej inteligencji, dodatkowo weryfikującego tożsamość przy użyciu bodźców wizualnych i dźwiękowych. Zamiast więc uwierzytelniać dostęp opierając

się na wcześniej zdefiniowanych i możliwych do wykradzenia danych, takich jak identyfikator i hasło, maszyna może zidentyfikować osobę na podstawie wskazówek wizualnych i fonologicznych, nauczyć się, kiedy taki dostęp może być przydzielony i zachowywać się konsekwentnie w oparciu o zestaw wyuczonych wzorców zachowań użytkowników systemu. Taka sztuczna inteligencja posiada też potencjał w zapewnianiu inteligentnej i ścisłej kontroli dostępu. Dla przykładu – tylko dlatego, że użytkownik poświadczył swoją tożsamość 10 minut temu, system nadal powinien uważać, że to ten sam użytkownik korzysta z dostępu? Systemy sztucznej inteligencji mogą tutaj zarządzać dostępem użytkownika wykorzystując parametry biometrii dynamicznej nawet gdy przemieszcza się on po sieci czy terenie przedsiębiorstwa.

Światowi liderzy i szefowie bezpieczeństwa przedsiębiorstw powinni zapoznać się z najnowocześniejszymi zagadnieniami związanymi z bezpiecznym wykorzystaniem sztucznej inteligencji przy zapewnianiu cyberbezpieczeństwa. Uzbrojeni w tę wiedzę liderzy będą mogli świadomie zadecydować, jak dodanie sztucznej inteligencji do swojego produktu lub usługi pozwoli zapewnić pozytywne doświadczenia użytkowników, przy jednoczesnym wyważeniu kosztów potencjalnych zagrożeń związanych z dodatkowym ryzykiem wycieku danych i innymi, opisanymi powyżej zagrożeniami. Zatrudnienie dedykowanego specjalisty do spraw sztucznej inteligencji może być naturalnym krokiem, ponieważ większość specjalistów do spraw bezpieczeństwa cybernetycznego nie jest przeszkolona (a co dopiero doświadczona) w zakresie przewidywania lub zapobiegania atakom wspieranych przez systemy inteligentne. Pozostaje mieć nadzieje, że obecnie trwające badania oraz prace legislacyjne pomogą włączyć sztuczną inteligencję w globalne i lokalne struktury zabezpieczeń z jak największym sukcesem.

Artykuł pochodzi z raportu Instytutu Kościuszki *Cyberbezpieczeństwo polskiego przemysłu. Sektor energetyczny.*

BIO

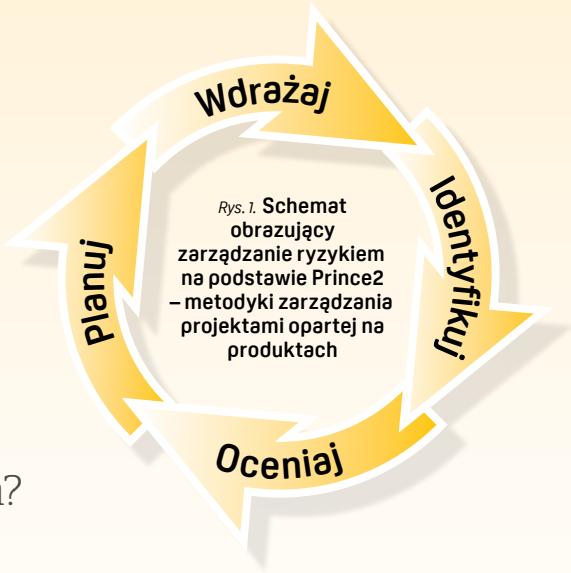
Marcin Spychała
jest doświadczonym ekspertem ds. cyberbezpieczeństwa, pracującym dla IBM Security Practice. Przez ostatnie lata był odpowiedzialny za projektowanie rozwiązań z zakresu bezpieczeństwa teleinformatycznego.

ZABEZPIECZANIE ZABEZPIECZEŃ

Cyberdefilada ruszyła na całego. Rynek ciągle nienasycony literaturą omawiającą dobre praktyki w zakresie cyberbezpieczeństwa domaga się kolejnych informacji. Działalność marketingowa firm z branży security pokazuje, jak istotna to pozycja w portofolio produktowym, którym producent może się szczycić.

Jan T. Grusznic

W zabezpieczaniu sens ma tylko podejście całościowe. Jaki bowiem może być pożytek z drzwi antywłamaniowych osadzonych w karton-gipsie lub kamer wandaloodpornych instalowanych na suficie podwieszanym?



Rys. 1. **Schemat obrazujący zarządzanie ryzykiem na podstawie Prince2 – metodyki zarządzania projektami opartej na produktach**

Na podstawie docierających z rynku przekazów można wywnioskować, że niektórzy dostawcy zmienili zakres swojej działalności na rzecz rozwoju produktów zwiększających bezpieczeństwo sieciowe. Dzielni handlowcy sprzedają cyberbezpieczeństwo jako kolejny produkt, który można dostarczyć „w pakiecie", ponieważ wpisuje się w trend obecnych oczekiwań posiadania bezpiecznego rozwiązania.

Z moich obserwacji wynika, że z cyberbezpieczeństwem na rynku zabezpieczeń technicznych jest trochę jak z kolejną funkcją na liście życzeń użytkownika, którą musi spełnić urządzenie – *WDR: jest, super(światło)czułość: jest, megarozdzielczość: obecna, cyberbezpieczeństwo: zaimplementowane*. I szafa gra...

Chciałbym, aby tak było – niestety nie jest. Stosowanie zabezpieczeń przed atakami sieciowymi zbytnio się nie różni od reguł, jakie od dekad stosujemy w zabezpieczaniu mienia za pomocą rozwiązań technicznych. Najpierw tworzymy listę potencjalnych zagrożeń, uwzględniając charakter obiektu, jego otoczenie, działania biznesowe itp. (identyfikacja). Następnie analizujemy je pod kątem prawdopodobieństwa wystąpienia i skutków z tym związanych (ocena). Na tej podstawie tworzymy potencjalne rozwiązanie lub kilka rozwiązań, które mają za zadanie zmniejszyć ryzyko pojawienia się prawdopodobnych zagrożeń (planowanie) i je wdrażamy (*rys. 1*)[1] Co istotne, cała procedura powinna być powtarzana cyklicznie lub wg potrzeb i bynajmniej nie ograniczać się do rozwiązań technicznych – dotyczy całego rozwiązania, przedsiębiorstwa, ludzi czy procesów. Tylko podejście całościowe ma sens, jaki bowiem może być pożytek z drzwi antywłamaniowych osadzonych w karton-gipsie czy kamer wandaloodpornych instalowanych na suficie podwieszanym?

Z cyberbezpieczeństwem nie jest inaczej – jedynie holistyczne podejście do problemu ma szansę na uzyskanie solidnego zabezpieczenia. Dobrze skonfigurowana kamera nie zapewni właściwej ochrony przed atakiem, jeśli pozostałe urządzenia podłączone do tej samej sieci będą pracowały w ustawieniach domyślnych (czytaj: będą niezabezpieczone).

Istnieje kilka podstawowych kroków, które pozwalają, aby system mógł być traktowany jako zabezpieczony. Zastrzegam, że głębokość wprowadzanych zmian zależy od kontekstu i przeprowadzonej analizy ryzyka. Nie ma jednej recepty na wszystkie potencjalne zagrożenia. Tych kilka kroków prowadzących do uzyskania świadomego minimalnego poziomu bezpieczeństwa, które wpajam już od kilku lat podczas szkoleń lub wizyt w obiektach, są niczym porządne okna i drzwi z solidnymi okuciami chroniące mienie.

Czas

Podstawą utrzymania bezpieczeństwa w sieci jest czas. To zmienna istotna z kilku powodów – od czasu, tj. sparametryzowanych daty, godziny, strefy czasowej, zależą uprawnienia dostępu do urządzeń, odtworzenie logów lub nagrań wizji/fonii czy automatyzacja procesów, takich jak wyzwalanie akcji w reakcji na wystąpienie zależnych od siebie zdarzeń. Technikom synchronizacja wszystkich elementów systemu względem jednej sygnatury czasu pozwala na szybkie ustalenie przyczyn awarii. Administratorzy sieci na podstawie oprogramowania analizującego ruch w sieci oraz logów urządzeń brzegowych reagują na anomalie, które mogą wskazywać na obecność niechcianego oprogramowania. Aby wymienione działania były efektywne, wszystkie te elementy systemu muszą synchronizować się z autorytatywnym serwerem czasu. Brak synchronizacji wśród urządzeń może stanowić przyczynę poważnego „bólu głowy". Urządzenie pracujące w sieci wydzielonej na ogół w jakimś stopniu jest dozorowane przez narzędzia SIEM[2]. Efektywność tego narzędzia polega na przetwarzaniu logów z urządzeń, których wpisy są wprowadzane zgodnie z kolejnością momentu wygenerowania wpisu, nie zaś dostarczenia. Bez dokładnego znacznika czasu w plikach dzienników SIEM nie jest w stanie ponownie utworzyć dokładnej sekwencji wzoru dla proaktywnego ostrzegania i wyjaśnienia anomalii po awarii.

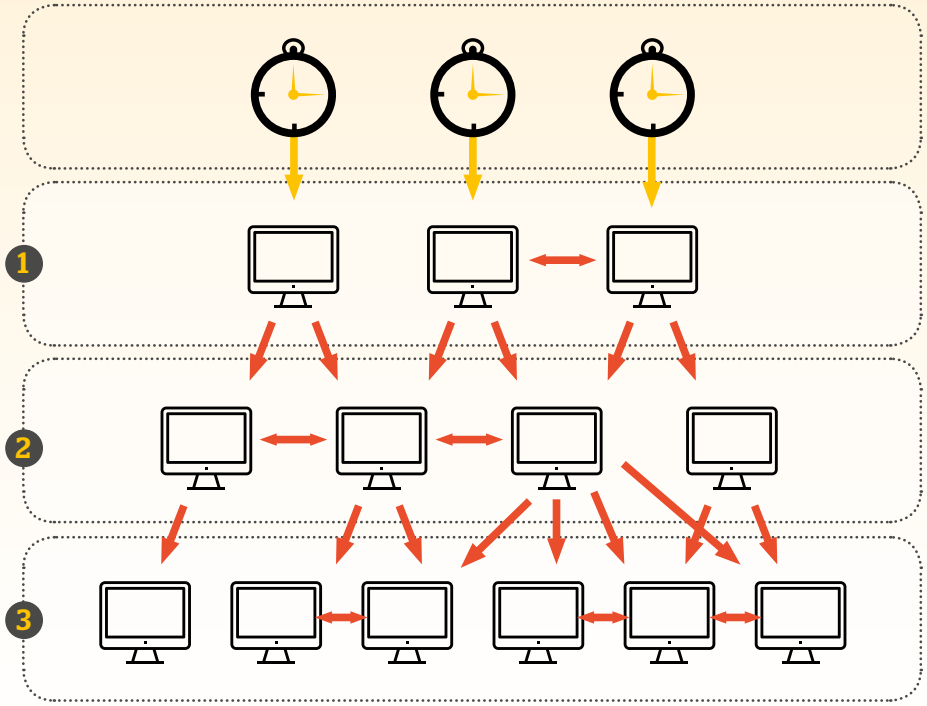
Niektórzy z nas uważają, że synchronizacja jest zbyteczna, skoro wszystko działa... O ile utrzymanie synchroniza-

[1] Sprawa jest bardziej złożona. Nawiązanie do analizy ryzyka ma na celu uzmysłowienie, że ten proces zachodzi niemal niezauważalnie i jest naturalny dla branży zabezpieczeń technicznych. Wszystkich zainteresowanych kieruję do literatury poświęconej temu zagadnieniu.

[2] *Security Information and Event Management* – zarządzanie informacją związaną z bezpieczeństwem i zdarzeniami. Warstwa technologiczna rozwiązań klasy SIEM pozwala na centralne zarządzanie dziennikami zdarzeń generowanymi z wielu urządzeń w jednym czasie oraz ich archiwizację. W tym celu wszystkie informacje generowane przez urządzenia są przesyłane, gromadzone i scentralizowane. Ponadto silnik SIEM przechowuje informacje i udostępnia je zespołowi bezpieczeństwa w celu analizy, mapowania oraz generowania raportów i zarządzania w sytuacjach kryzysowych, zgodnie z określonymi procedurami. Możliwość korelacji, czyli szukania zależności pomiędzy nimi, daje działom bezpieczeństwa niespotykany dotychczas poziom wiedzy.

cji sygnałów fonii i wizji z dwóch różnych urządzeń na serwerze zapisu nie wymaga synchronizacji czasu[3], o tyle do osiągnięcia podstawowego poziomu bezpieczeństwa jest kluczowe. Aby nie być gołosłownym, posłużę się przykładem sprawy hakerskiej opisanej później przez Clifforda Stolla w książce „Kukułcze jajo". Na podstawie informacji zawartych w logach autor odtwarza niewinny błąd w rachunkach na 75 centów, aż do wykorzystania komputerów przez 9 sekund, co nie zostało odnotowane. Dane z logów i zastosowanie różnych technik dochodzeniowych pozwoliły Stollowi prześledzić atak Markusa Hessa z Hanoweru w Niemczech, który zbierał informacje z amerykańskich komputerów i sprzedawał je sowieckiemu KGB. Niesamowita rozgrywka, która swój początek ma w 9 sekundach nieodnotowanych w dziennikach systemowych.

Historia ta pokazuje jednocześnie, że jeśli nie wiesz, czego szukasz, odnalezienie tego wśród niezsynchronizowanych danych będzie niewiarygodnie trudne. Dlatego po pierwsze, zacznij od kompleksowego spisu systemów, usług i aplikacji w środowisku zarządzania dziennikami/SIEM. Sprawdź, czy są one synchronizowane i z jakim serwerem. Gdy wiesz, skąd pochodzi informacja o sygnaturze czasowej (lokalizacja geograficzna, strefa czasowa, system, aplikacja i/lub usługa), zastosuj techniki normalizacji w systemie zarządzania dziennikami aplikacji. Jeśli log jest pobierany z urządzenia, o którym wiadomo że ma bardzo dokładne i wiarygodne zewnętrzne źródło czasu, oryginalny znacznik czasu w dzienniku można uznać za akceptowalny. Należy jednak pamiętać, że mechanizm zarządzania dziennikami może nadal wymagać normalizacji informacji o czasie, by odtworzyć pojedynczy meta-czas dla wszystkich urządzeń, aby reguły korelacji mogły działać efektywnie. Weźmy dla przykładu firmy z firewallami w ich biurach w Londynie, Nowym Jorku i San Jose. Dane dziennika z zapór są analizowane przez silnik i ostrzegają, że 15 stycznia 2018 r.



Rys. 2. Wszystkie komputery uczestniczące w procesie synchronizacji NTP można uporządkować w strukturze gałęziowej STRATUM. Zasada przekazywania informacji o czasie jest następująca: komputery warstwy STRATUM N mogą być serwerami czasu dla warstwy STRATUM N+1, ale nie na odwrót. Komputery STRATUM N mogą być jednocześnie klientami komputerów warstwy STRATUM N-1 itd.
Wielowarstwowa struktura STRATUM ma na celu uporządkowanie i wprowadzenie pewnej hierarchii ważności komputerów, zgodnie z ich rzeczywistym przeznaczeniem i funkcją. Aby ograniczyć dodatkowe opóźnienia w propagacji czasu, wynikające z rozgałęzionej struktury NTP, wprowadzono ograniczenie łącznej liczby warstw do 16 (STRATUM 0-15).
Żółte strzałki oznaczają bezpośrednie połączenie; czerwone – połączenia sieciowe
Źródło: *https://pl.wikipedia.org/wiki/Network_Time_Protocol*

o godz. 15:45, 13:45 i 10:45 wykryto odmowę usługi. W przypadku ich stref lokalnych są to poprawne znaczniki czasu, ale jeśli mechanizm zarządzania dziennikami normalizuje czas geograficzny w pojedynczy meta-czas lub uniwersalny czas koordynowany (UTC), jasne jest, że wszystkie trzy zapory zostały zaatakowane w tym samym czasie. Innym podejściem jest dostrojenie raportowania czasu w plikach dziennika urządzeń, aby odzwierciedlić pożądany czas uniwersalny w silniku korelacji zamiast prawidłowego czasu lokalnego.

Bez względu na rodzaj normalizacji niezawodność źródła czasu ma znaczenie kluczowe. Podczas odtwarzania zdarzeń znaczniki czasu w sieci organizacji mogą być porównywane z urządzeniami zewnętrznymi. Z tego powodu należy mieć pewność, że źródło, z którego korzystasz, jest tak dokładne, jak to tylko możliwe. Jednym z najpopularniejszych protokołów używanych do synchronizacji czasu jest NTP (*Network Time Protocol*), wersja 3[4], który dostarcza informacji o czasie w UTC. Systemy Microsoft Windows implementują NTP jako WTS (*Windows Time Service*)[5], a niektóre zegary atomowe dostarczają danych do Internetu w celu synchronizacji NTP. Jednym z przykładów jest Tempus udostępniony nieodpłatnie przez Główny Urząd Miar[6].

Co prawda istnieją pewne obawy związane z bezpieczeństwem NTP, ponieważ używa on protokołu bezstanowego do transportu i nie jest w żaden sposób uwierzytelniany. Zdarzały się także

[3] RFC3550 – RTP: *A Transport Protocol for Real-Time Applications.*
[4] RFC 1305, *Network Time Protocol (Version 3) Specification, Implementation and Analysis.*
[5] https://docs.microsoft.com/en-us/windows-server/networking/windows-time-service/windows-time-service-top
[6] https://www.gum.gov.pl/pl/uslugi/zegar/524,Zegar.html.

przypadki ataków typu *Denial of Service* (DoS) na serwery NTP, przez co stały się one czasowo niedostępne na potrzeby dostarczania informacji o czasie. Co możemy z tym zrobić? Niewiele, pomimo drobnych problemów związanych z bezpieczeństwem NTP jest najczęściej stosowanym (i szeroko obsługiwanym) protokołem do synchronizacji czasu urządzeń sieciowych. Można więc dołożyć wszelkich starań, aby obejść te problemy, tworząc strukturę drzewa rozpinającego serwerów (*rys. 2*). Dzięki takiemu podejściu urządzenia w wydzielonej sieci będą miały dostęp do odseparowanych serwerów czasu. Można też rozważyć dodanie dodatkowego monitorowania i segregacji sieci do autorytatywnych źródeł czasu tam, gdzie to możliwe.

Hasła

Nie od dziś wiadomo, że odpowiednio zbudowane i wykorzystywane hasła dostępowe to jeden z podstawowych i najważniejszych elementów budowania bezpieczeństwa teleinformatycznego w organizacji. Większość z nas doskonale zdaje sobie sprawę, jak ważnym elementem bezpieczeństwa jest odpowiednie zarządzanie takimi poświadczeniami uwierzytelniającymi. Mimo wszystko często nie przykładamy do tego wielkiej wagi, bagatelizujemy takie zabezpieczenie, żyjąc w przekonaniu, że ponieważ to wydzielona instalacja, więc co wielkiego może się zdarzyć? Tymczasem, jak podano w raportach[7], coraz poważniejszym problem stają się „wewnętrzni intruzi".

Formalnie w zakresie złożoności, długości oraz częstotliwości zmiany haseł dostępowych do systemów informatycznych, w których zachodzi proces przetwarzania danych osobowych (a do takich należy zaliczyć obrazy z monitoringu wizyjnego ukazujące wizerunki osób)[8], do 25 maja 2018 r. obowiązują przepisy rozporządzenia MSWiA. Wskazują one jednoznacznie, iż w sytuacji, gdy przynajmniej jedno urządzenie infrastruktury sieci lokalnej jest podłączone do sieci publicznej, hasła dostępowe do takich systemów powinny składać się z co najmniej 8 znaków, w tym muszą wystąpić małe i duże litery, cyfra lub znak specjalny oraz być zmieniane nie rzadziej niż co 30 dni. Po wejściu RODO wymóg częstotliwości zmiany, odpowiedniej złożoności i długości hasła zostanie zniesiony. Uważam rekomendowaną przez MSWiA częstotliwość zmiany hasła za zbyt dużą, tym bardziej że większość systemów jest odizolowana od sieci zewnętrznych. Nie mam natomiast wątpliwości, że hasło powinno być na tyle bezpieczne, aby czas jego odgadnięcia *(tabela)* był niewspółmierny do korzyści wynikających z uzyskania dostępu do zasobów.

W przypadku branży security oznacza to, że powinno:

- **składać się z co najmniej 8 znaków,**
- **zawierać zarówno małe, jak i duże litery,**
- **zawierać cyfry,**
- **zawierać również znaki specjalne (np. &, @, !).**

Optymalnym rozwiązaniem jest utworzenie unikatowej pary: użytkownik, hasło, które będzie używane przez systemy współkorzystające z danych zasobów. Korzystanie z fabrycznego użytkownika na prawach administratora, takiego jak *admin* czy *root*, jest mniej bezpieczne nie tylko ze względu na wymóg odgadnięcia samego hasła użytkownika w celu uzyskania dostępu. Większość fabrycznych „administratorów" zezwala na nieograniczony dostęp do urządzeń w porównaniu do użytkowników stworzonych zgodnie z prawami administratora. Ten dostęp to np. możliwość debugowania (kontrolowane wykonywanie poleceń programu, w tym włączanie i wyłączanie usług), zmiany plików wykonawczych, ładowanie plików specjalnych (np. testowe niepodpisane oprogramowanie układowe) czy dostęp przez telnet, ssh lub ftp.

W celu wymiany standardowych informacji często wystarczą nawet uprawnienia na prawach niższych niż administrator. Jeśli jednak są wymagane wyższe, zachęcam do tworzenia unikalnych par: użytkownik, hasło.

Wraz z upływem czasu hasła są coraz słabsze

Czas potrzebny do złamania hasła:

security1

Lata	Mies.	Tygodni	Dni	Godzin	Minut	Sekund
rok 2000						
3	10	1	5	14	54	19
rok 2001						
2	9	0	5	11	28	35
rok 2002						
2	1	3	0	22	20	41
rok 2003						
1	9	1	6	18	22	50
rok 2004						
1	0	1	2	1	57	49
rok 2005						
0	7	1	5	6	6	52
rok 2006						
0	6	2	3	13	26	6
rok 2007						
0	4	0	5	15	26	39
rok 2008						
0	4	3	4	1	26	2
rok 2009						
0	4	3	2	8	9	8
rok 2010						
0	4	1	4	19	7	57
rok 2011						
0	4	1	2	12	25	23
rok 2012						
0	4	0	0	21	11	42
rok 2013						
0	3	3	5	23	36	29
rok 2014						
0	3	3	1	0	39	45
rok 2015						
0	3	1	6	14	44	19
rok 2016						
0	2	4	1	10	12	11

[7] 2018 *Cybersecurity Predictions A Shift to Managing Cyber as an Enterprise Risk*, styczeń 2018, Stroz Friedberg an AON Company.

[8] Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dn. 9.04.2013 r., II SA/Wa 211/13.

Protokoły

Jedną z zasad bezpieczeństwa, jaką wyniosłem po nauce administracji sieci w banku, jest wyłączaj, jeśli nie używasz. I stosuję ją wszędzie, również w technicznych systemach zabezpieczeń, a zwłaszcza w opartych na komunikacji IP. Wyłączanie dotyczy przede wszystkich niebezpiecznych lub nieużywanych protokołów, które są niczym bramy, przez które można się dostać do urządzenia.

Niewątpliwie wszystkie są użyteczne. Dzięki nim proces wykrycia, instalacji i konfiguracji przebiega szybciej. Dla większości ich użyteczność kończy się jednak wraz z zakończeniem procesu wdrażania i odbiorem systemu. Wówczas należałoby pozamykać furtki, które mogłyby posłużyć innym do niecnych celów, a które nie są wymagane do stabilnego działania systemu. Są to wszelkiego rodzaju protokoły *Discovery,* które służą do wykrywania urządzeń w sieci za pomocą oprogramowania dostępnego powszechnie lub ze strony producenta. Co ciekawe, jest to jedno ze skuteczniejszych sposobów zabezpieczania urządzeń przed niechcianą próbą ingerencji przez osoby nieuprawnione.

Jestem również za absolutnym zakazem wykorzystania protokołu UPnP (*Universal Plug and Play*), który umożliwia przesyłanie danych między dwoma urządzeniami bez autoryzacji i jakichkolwiek zabezpieczeń. FBI i inni eksperci od cyberbezpieczeństwa sugerują wyłączenie tego protokołu nawet we wszystkich urządzeniach domowych.

Urządzenie wykorzystujące UPnP potrafi przekierować porty komunikacyjne oraz adresy serwerów DNS w innym urządzeniu (również z uruchomionym UPnP) bez konieczności potwierdzania swojej tożsamości. Natomiast takie protokoły, jak ftp, ssh czy telnet według moich doświadczeń są pomocne w rozwiązaniu problemu, gdy taki pojawi się w systemie. Nie jestem zatem taki skory do ich całkowitego wyłączania. Jednocześnie dają zbyt wiele możliwości „napsucia" ustawień urządzenia i powinny być dostępne tylko dla przeszkolonego

AON O (CYBER)RYZYKU

Firma doradcza AON w swoich raportach wskazuje na wzrost ryzyka cybernetycznego w związku z uzależnieniem się przedsiębiorstw od technologii cyfrowych, większym naciskiem na ochronę danych i wzrostem wartości aktywów niematerialnych.

Do ataków z zewnątrz będą wykorzystywane urządzenia IoT, będą też rosły zagrożenia płynące z wewnątrz organizacji. Według AON ma to być związane ze zbyt niskimi inwestycjami w proaktywne programy zapobiegające takim rodzajom ryzyka. Przedsiębiorstwa nie inwestują w rozwój świadomości swoich pracowników o zagrożeniach w zakresie bezpieczeństwa informatycznego.

Brak danych dotyczących udziału czynnika ludzkiego, który przyczynił się do udanego ataku, a następnie utrzymywanie tego faktu w tajemnicy powoduje i będzie powodowało, że firma podchodzi do takich incydentów *ex post*.

To niemały problem, zwłaszcza gdy zestawić ten wniosek z badaniami przeprowadzonymi przez Cisco *2018 Security Capabilities Benchmark Study,* które wyraźnie wskazują, że można się spodziewać ataków od wewnątrz na technologię operacyjną (OT – *Operation Technology*), urządzenia przemysłowe ICS (*Industrial Control Systems*) oraz IoT. Są one jeszcze dość rzadkie, wielu specjalistów ds. zabezpieczeń jeszcze ich nie doświadczyło.

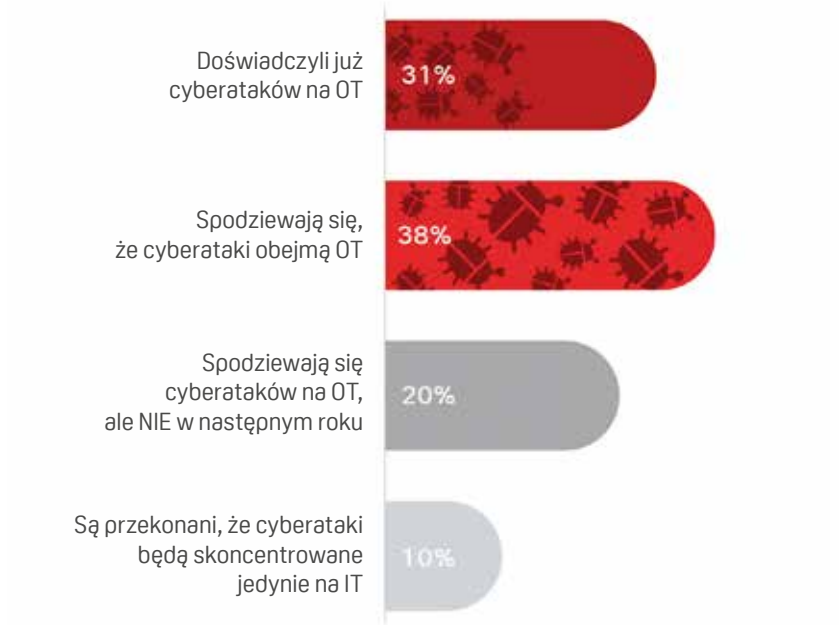
Tajemnicą poliszynela jest to, że systemy te często są słabo zabezpieczone i mają nieaktualne oprogramowanie, co czyni je podatnymi na ataki. Jeden z respondentów badania stwierdził, że *wciąż mamy infrastrukturę OT, która pracuje 25 lat, oraz kompresory i maszyny, które mają 40 lat.*

Tymczasem w świecie IT specjaliści są przyzwyczajeni do harmonogramu, znają datę wycofania produktu ze sprzedaży i spodziewaną datę zakończenia wsparcia. W środowisku OT nie ma czegoś takiego... Niewielu specjalistów ds. bezpieczeństwa ma dostateczną wiedzę o kwestiach związanych z zabezpieczeniem infrastruktury urządzeń OT w ich organizacjach. Nie musieli wykonywać takich działań w przeszłości ani ich nie planują, a implementacje technologii IoT są po prostu zbyt nowe.

Spośród tych specjalistów 31% stwierdziło, że ich organizacje już doświadczyły cyberataków na infrastrukturę OT, a 38% spodziewa się, że w tym roku nastąpi atak z sieci IT na OT.

Ryzyko cyberataków w ocenie firm

źródło: Cisco 2018 Security Capabilities Benchmark Study



Więcej na: **cisco.com/go/acr2018**

personelu. Inną kwestią jest to, że korzystając z niezabezpieczonych kanałów, takich jak ftp i telnet, nazwy użytkowników i hasła są wysyłane jawnie przez sieć lub kodowane tzw. base64 (kodowanie transportowe), które można bez problemu odkodować.
Bezpieczniejsze jest korzystanie z protokołu ssh (*secure shell*), następcy telnetu, które na szczęście coraz większa liczba producentów wprowadziła w elektronicznych systemach zabezpieczeń. Protokół ten wykorzystuje AES (*Advanced Encryption Standard*) – symetryczny (do szyfrowania i odszyfrowywania stosuje się ten sam klucz) szyfr blokowy o różnych długościach klucza. Dzięki temu wymiana danych między urządzeniami jest bezpieczna.

Izolacja

Zasadę „wyłączaj, jeśli nie używasz" należy stosować nie tylko do protokołów komunikacyjnych, ale także do wszystkich pozostałych elementów systemu. W przypadku przełączników sieciowych (oczywiście umieszczonych w zabezpieczonych przed nieautoryzowanym dostępem pomieszczeniach) dotyczy to portów, które nieobciążone powinny być trwale wyłączone. W tym celu należy stosować zarządzalne przełączniki sieciowe. Gdy trzeba podłączyć dodatkowe urządzenie do infrastruktury, administrator sieci aktywuje port w przełączniku. Nie jest to najszybsza metoda, ale skuteczna, ze względu na naturalną weryfikację tego, co i w jakim celu jest podłączane.
Dla niecierpliwych istnieją inne rozwiązania. W switchach dostępowych warstwy drugiej można również stosować polisy bezpieczeństwa lub listy dostępowe (ACL – *Access Control List*) opartych na adresach fizycznych urządzeń (adres MAC – *Media Access Control*). MAC jest adresem sprzętowym karty sieciowej Ethernet, unikatowym w skali światowej, nadawanym przez producenta danej karty podczas produkcji. Każdy port przełącznika może być zaprogramowany do obsługi tylko jednego urządzenia z jednym adresem MAC. Jeśli zostanie do niego podłączone inne urządzenie, port przekieruje ruch do specjalnie utworzonej sieci wirtualnej (VLAN – *Virtual Local Area Network*) odseparowanej od sieci bezpieczeństwa. Niestety takie rozwiązanie nie jest bez wad. Urządzeniom można chwilowo zmienić adres MAC, tak aby „udawały" inny produkt. Zatem możliwe jest podłączenie komputera jako kamery, jeśli komputerowi wprowadzimy adres fizyczny tej kamery. Wtedy przełącznik zaakceptuje komputer jako element systemu bezpieczeństwa i wprowadzi do sieci zabezpieczonej.
Z tego też powodu bardziej skuteczne są polisy bezpieczeństwa, które w przypadku odłączenia urządzenia natychmiast wyłączają port w przełączniku, a także stosowanie zabezpieczeń IEEE802.1x opartych na certyfikatach uwierzytelniających. Wymaga to jednak zastosowania sprzętu o odpowiedniej klasie i zarządzania certyfikatami wszystkich elementów systemu, co wiąże się z wyższymi kosztami.
A co z bezpieczeństwem urządzeń klienckich? Wnioskując po wynikach badań przeprowadzonych przez Cisco 2018 *Security Capabilities Benchmark Study*, największym zagrożeniem cybernetycznym dla przemysłowych systemów sterowania (w tym systemów bezpieczeństwa) jest nieprzeszkolony personel i błędy ludzkie, które często pozostają nieujawnione. Dlatego należy tak przygotować środowisko użytkownika, aby zminimalizować prawdopodobieństwo popełnienia błędu z powodu choćby nieuwagi.
Nie mam na myśli interfejsu użytkownika aplikacji – to jest zrozumiałe. Chodzi mi o uprawnienia w systemie operacyjnym komputera używanego jako stacja klienckа systemu.
Optymalnym rozwiązaniem jest odizolowanie jednostki roboczej od użytkownika, w ten sposób można ograniczyć możliwość uruchamiania zewnętrznych plików z pamięci przenośnych. Natomiast jeśli nie jest to możliwe, sugerowałbym wyłączanie dostępu do napędów i portów USB, ograniczenie wykorzystania skrótów klawiszowych oraz zmianę konfiguracji sieciowej. W środowisku Windows można za pomocą zasad grupy (*group policy*) poważnie ograniczyć dostęp do zasobów nawet użytkownikowi na prawach administratora.

7 KROKÓW DO ZABEZPIECZENIA ELEKTRONICZNYCH SYSTEMÓW ZABEZPIECZEŃ

1. Ustaw serwer czasu - niech wszystkie elementy systemu zsynchronizują się do tej samej sygnatury.
2. Ustaw silne hasła dla użytkownika na prawach administratora. Jeśli to możliwe, utwórz drugiego użytkownika na takich prawach i wykorzystuj go do komunikacji z urządzeniami w systemie. Jeśli nie jest to konieczne, nie używaj użytkownika na prawach administratora do wykonywania zadań, do których ma dostęp użytkownik o niższych uprawnieniach.
3. Wyłącz protokoły niezabezpieczone (telnet, ftp) i te, których nie używasz.
4. Używaj wyłącznie zweryfikowanego oprogramowania układowego (np. przez sygnaturę md5), pochodzącego z zaufanego źródła lub podpisanego cyfrowo.
5. Wyłącz nieużywane porty w przełącznikach sieciowych, aby nikt fizycznie nie mógł dostać się do sieci, lub ustaw je w odseparowanych wirtualnych sieciach (VLAN-ach).
6. Ogranicz fizyczny dostęp do urządzeń zbiorczych (szafy teletechniczne, w których zainstalowano switche, serwery, macierze dyskowe i inne) tylko do osób zaufanych.
7. Ogranicz prawa użytkownika na komputerze z zainstalowanym oprogramowaniem klienckim. Jeśli to możliwie, odseparuj sieciowo (VLAN) stację roboczą od pozostałych urządzeń.

BIO

Jan T. Grusznic, z-ca red. naczelnego „a&s Polska". Z branżą wizyjnych systemów zabezpieczeń związany od 2004 r. Ma bogate doświadczenie w zakresie projektowania i wdrażania rozwiązań dozoru wizyjnego w aplikacjach o rozproszonej strukturze i skomplikowanej dystrybucji sygnałów. Ceniony diagnosta zintegrowanych systemów wspomagających bezpieczeństwo.

Jak zapewnić bezpieczeństwo danych w firmie?

Kilkanaście lat temu przedsiębiorstwa posiadały hermetyczne systemy informatyczne, w większości mające własną, odseparowaną sieć. Były więc mniej podatne na działania związane z pozyskaniem danych przez osoby nieuprawnione. **W dobie wszechobecnej informatyzacji pojawia się coraz więcej zagrożeń bezpieczeństwa. Ochrona danych przesyłanych w sieciach komputerowych należy do najważniejszych zadań nie tylko pracowników działów IT.**

Michał Chodnicki

Fundamentalnym pojęciem związanym z bezpieczeństwem, które nie powinno być obce kadrze zarządzającej przedsiębiorstwem, jest System Zarządzania Bezpieczeństwem Informacji (SZBI), czyli szczegółowo opracowany plan działania w zakresie zapewnienia właściwej ochrony informacji. Jego podstawowymi założeniami są analiza, planowanie, wykonanie, sprawdzenie oraz zapewnienie ciągłego doskonalenia podjętych działań i procedur w celu optymalizacji ryzyka związanego z naruszeniem poufności, zgodnie z zaleceniami normy ISO 27001.

Dane w firmie są istotnymi zasobami zarówno dla niej, jak i jej klientów. Celem polityki bezpieczeństwa jest zapewnienie ochrony zasobów danych, rozumianej jako ochrona ich integralności, dostępności oraz poufności bez względu na formę zapisu. Uwzględnienie regulacji prawnych i wymogów biznesowych, przy jednoczesnej rzetelnej ochronie informacji to klucz do wzmocnienia pozycji firmy na rynku, odbieranej przez potencjalnych klientów jako rzetelna i godna zaufania.

Na jakie elementy systemów sieciowych w aspekcie bezpieczeństwa warto zwrócić uwagę? **Najsłabsze ogniwo nie ma tu niestety bezpośredniego związku z technologią – tym ogniwem są pracownicy.** Wystarczy hasło zapisane na kartce przyczepionej pod monitorem, hasło do sieci wydrukowane i powieszone na ścianie, „bo ciągle ktoś o nie pyta" czy też poufne dane nagrane na dysk przenośny, by można było coś jeszcze z nimi zrobić w domu…

Takie sytuacje z punktu widzenia bezpieczeństwa danych są niedopuszczalne. Zdarzają się jednak zbyt często, i to nie tylko w małych czy średnich firmach. Wprowadzenie i przestrzeganie procedur zawartych w SZBI nabiera szczególnego znaczenia. Trzeba pamiętać, że zasoby, które staramy się chronić, będą tak bezpieczne, jak najsłabsze ogniwo pancerza, którym je otaczamy.

Kolejnym ważnym czynnikiem jest oprogramowanie systemowe i uprawnienia użytkowników. Przy wyborze systemu nie mamy niestety wielkiego pola manewru, jednak niezależnie od platformy,

na którą się zdecydujemy, musimy zapewnić firmie spójną politykę bezpieczeństwa, minimalizując w ten sposób luki w systemie. Budując system informatyczny, należy zakładać uprawnienia oparte na rolach. Każdy użytkownik powinien posiadać tylko i wyłącznie takie uprawnienia, jakie są mu niezbędne do wykonywania powierzonych zadań. W przypadku oprogramowania pracującego na produkcyjnych systemach operacyjnych żaden ze „standardowych" użytkowników nie powinien mieć uprawnień do instalowania lub aktualizacji oprogramowania. Ograniczenie dostępu do określonych zasobów najłatwiej przeprowadzić w środowisku domenowym, gdzie prawa dostępu zostaną przypisane do wszystkich stacji roboczych, wykorzystując ustanowione przez nas reguły. Bardzo istotna jest dbałość o aktualizacje zabezpieczeń przewidzianych do danego systemu operacyjnego oraz wybór odpowiedniego systemu antywirusowego. Niekiedy aktualizacje systemowe mogą zakłócić działanie innych programów, może dojść do konieczności restartu systemów operacyjnych i oprogramowania procesowego.
Warto korzystać z takich rozwiązań, jak wirtualizacja i redundancja, które w znacznym stopniu ograniczają skutki uboczne wynikające z przerw lub ewentualnych awarii, jak również próby pozyskania danych przez osoby do tego nieupoważnione. Bez względu jednak na to, jak dobrze sieć wydaje się zabezpieczona, o skuteczności tej ochrony przekonamy się dopiero po bezpośredniej próbie ataku.

Oprócz wspomnianej wcześniej kartki z zapisanym hasłem pozostawionej pod

Celem polityki bezpieczeństwa jest zapewnienie ochrony zasobów danych, rozumianej jako ochrona ich integralności, dostępności oraz poufności bez względu na formę zapisu.

monitorem **użytkownik komputera może paść ofiarą próby wyłudzenia danych *(phishing).*** Niestety wracamy do najsłabszego ogniwa w postaci samych użytkowników. Nawet najbardziej zaawansowany program strzegący stacji roboczej nie uchroni przed kłopotami, jeśli nie zachowamy zdrowego rozsądku. Możliwości ataków na sieć, system czy zasoby baz danych jest wiele. Można je podzielić na ataki wewnętrzne, zewnętrzne, rozproszone lub dokonane przy użyciu węzłów pośrednich. Niektóre z nich, np. mające na celu kradzież tożsamości, danych finansowych czy innych poufnych danych, mogą być wykonywane na zlecenie. Ten scenariusz raczej nie dotyczy małych i średnich przedsiębiorców. W takich przypadkach większym zagrożeniem będzie ciekawość atakującego, czasem chęć sprawdzenia swoich umiejętności. I właśnie chęć sprawdzenia swoich umiejętności często prowadzi do ataków takich jak zmiany czy wykasowanie danych bezpośrednio na komputerze ofiary czy też ataki DoS *(Ping of Death)* w celu blokady usług. Spamowanie skrzynek poczty elektronicznej to również zmora dzisiejszych czasów.
Osoby pragnące sprawdzić się w roli hakera zazwyczaj nie są świadome konsekwencji swoich czynów, w tym także odpowiedzialności karnej. Dlatego tak istotna jest nie tylko szeroko zakrojona edukacja na poziomie zabezpieczania przed potencjalnymi atakami, ale także uświadamianie konsekwencji tego typu działań.

Na etapie projektowania czy późniejszej rozbudowy infrastruktury sieciowej w firmie nie można zapomnieć o **poprawnej konfiguracji narzędzi mających za zadanie pomoc w zapobieganiu nieautoryzowanemu dostępowi do jej zasobów.** Oprogramowanie antywirusowe, *spyware, adware* to nie wszystko. Elementy sieci, takie jak zapory ogniowe czy systemy IDS, powinny być konfigurowane i administrowane jedynie przez osoby upoważnione, posiadające odpowiednią wiedzę umożliwiającą bezpieczną konfigurację, przy zachowaniu pełnej funkcjonalności systemów firmy dla wszystkich pracowników, w tym pracujących zdalnie na poufnych zasobach danych.

Mówiąc o bezpieczeństwie, nie można pominąć zagadnienia związanego z kopiami zapasowymi. Redundancja i wirtualizacja w znacznym stopniu ułatwiają procesy kopiowania i przywracania danych. Polityka kopii zapasowych jest jedną ze składowych SZBI. Kopie zapasowe powinny być wykonywane z zachowaniem historii dokonywanych zmian, a więc zgodnie z hierarchią GFS (dziadek – ojciec – syn). Poziom „syn" oznacza dni tygodnia, w których jest wykonywana kopia przyrostowa; poziom „ojciec" – tygodnie miesiąca, w których jest wykonywana pełna kopia; poziom „dziadek" to z kolei liczba miesięcy, na koniec których jest wykonywana pełna kopia całej zawartości wskazanych zasobów. Kopie zapasowe w zależności od polityki firmy mogą być przechowywane na zewnętrznych nośnikach lub w chmurze. Zawsze jednak powinny pozostawać odpowiednio zabezpieczone, najlepiej zaszyfrowane, np. przy użyciu algorytmu 3DS.

Niezależnie od tego, z jakich zasobów sieciowych korzystamy na co dzień, należy pamiętać, że coraz więcej czasu spędzamy w cyfrowym świecie, umieszczamy w nim również mnóstwo prywatnych informacji. Informacje te wykorzystane przez niepowołane osoby mogą przysporzyć wielu problemów – o tym zdają się wiedzieć wszyscy. Nie wszyscy jednak przestrzegają podstawowych zasad bezpieczeństwa, które przyswajają sobie, ale z reguły już po fakcie.

Zalecenia dotyczące bezpieczeństwa – oprócz zawartych w procedurach firm – są umieszczane na portalach społecznościowych czy forach internetowych. W znacznym stopniu poszerza to grono świadomych użytkowników, którzy wiedzą, co i kiedy im wolno, a czego nie.
Wiedza oparta na radach i zaleceniach jest zawsze łatwiej przyswajana niż bazująca na zakazach i nakazach. Jej posiadanie jest najlepszą drogą do tego, aby w cyfrowej rzeczywistości uniknąć zagrożeń – żadne, nawet najlepsze technologie nie zastąpią zdrowego rozsądku użytkownika.

BIO

Michał Chodnicki
Z branżą IT związany od ponad 20 lat. Realizował liczne projekty obejmujące bezpieczeństwo danych dla takich instytucji, jak Uniwersytet Warszawski, AmRest czy ambasada Kanady. Od 2011 r. pracuje w TP-Link Polska jako szef działu technicznego na Polskę, Węgry i kraje bałtyckie.

Ochrona infrastruktury krytycznej

Rząd zmienia podejście

z Maciejem Pyznarem, szefem Wydziału Ochrony Infrastruktury Krytycznej w RCB, rozmawiają Marta Dynakowska i Mariusz Kucharski.

Ochrona infrastruktury krytycznej jest obowiązkiem jej właściciela. Przypomnijmy Czytelnikom jaką rolę w systemie ochrony IK pełni RCB? W jaki sposób wspiera operatorów IK?

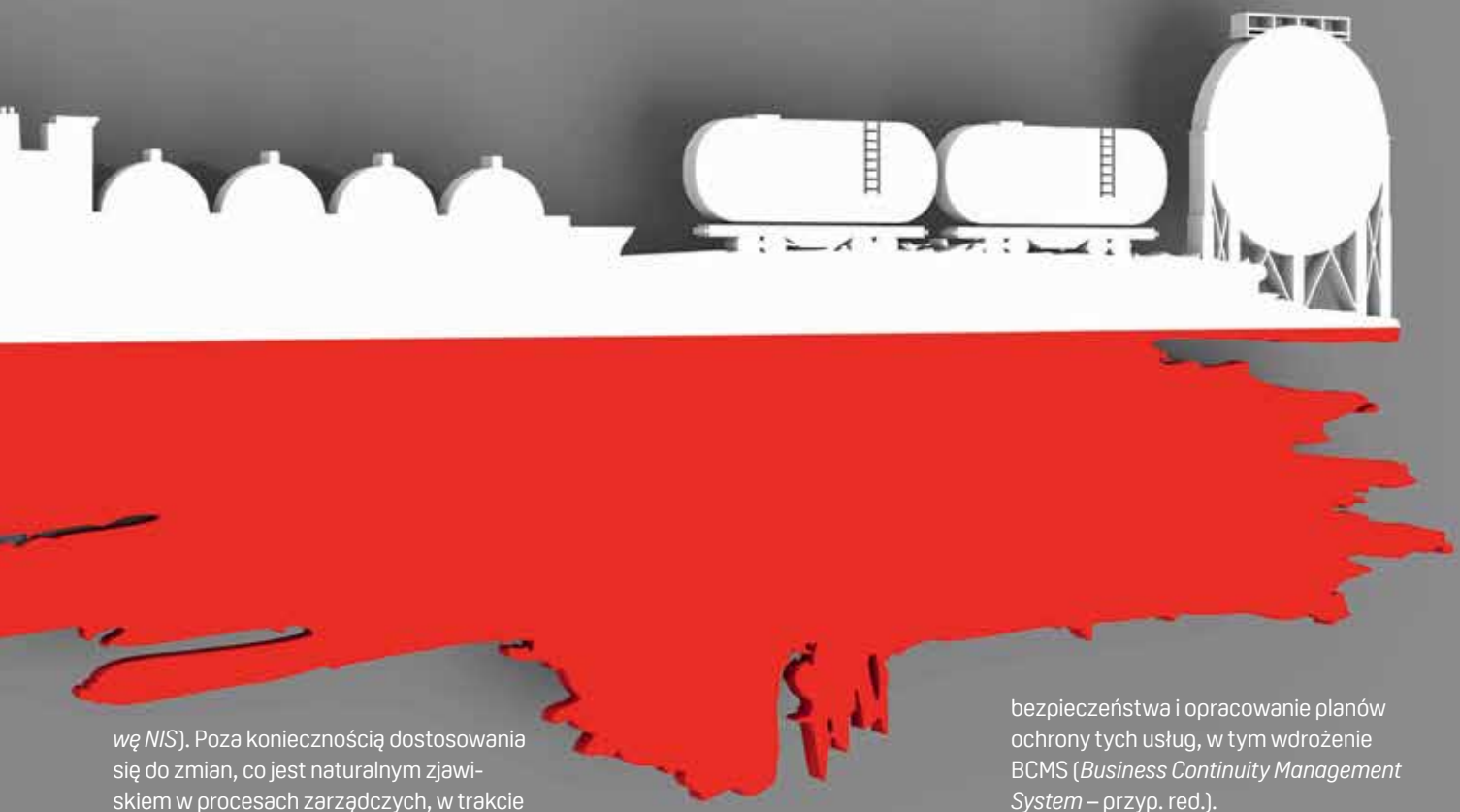
– Rządowe Centrum Bezpieczeństwa, jako państwowa jednostka budżetowa, realizuje zadania określone w ustawie z dn. 26 kwietnia 2007 r. o zarządzaniu kryzysowym. W obszarze ochrony IK, RCB realizuje zadania planistyczne i programowe z zakresu ochrony infrastruktury krytycznej oraz europejskiej infrastruktury krytycznej, w tym opracowuje i aktualizuje załącznik funkcjonalny do Krajowego Planu Zarządzania Kryzysowego dotyczący ochrony IK. Współpracuje także, jako krajowy punkt kontaktowy, z instytucjami Unii Europejskiej i NATO oraz krajami członkowskimi w zakresie ochrony IK. Ponadto dyrektor RCB opracowuje, we współpracy z ministrami i kierownikami urzędów centralnych odpowiedzialnymi za systemy IK, Narodowy Program Ochrony Infrastruktury Krytycznej (w Programie zawarte są kryteria identyfikacji IK) i realizuje zadania w nim określone oraz (już samodzielnie) zatwierdza plany ochrony IK opracowane przez jej operatorów.

Przedstawiając założenia zmian, spotkaliśmy się z przychylnym przyjęciem. Operatorzy również zauważają niedoskonałości systemu.

Z praktycznego punktu widzenia, RCB dba o to, by opisane wyżej zadania zostały zrealizowane najlepiej jak to możliwe. Wydział Ochrony Infrastruktury Krytycznej najwięcej czasu poświęca na wspieranie operatorów IK przy opracowaniu planów ochrony oraz organizację szkoleń i pomoc w rozwiązywaniu problemów przy współpracy z administracją.

W wywiadzie udzielonym nam przed rokiem zastępca dyrektora RCB Krzysztof Malesa zaznaczył, że jednym z ważniejszych zadań RCB w ramach ochrony IK jest przejście z systemu obiektowego do usługowego. Jakie są założenia i cele tego nowego podejścia?

– Podstawowym celem zmiany podejścia jest dostosowanie do zmian w środowisku bezpieczeństwa. Po szczycie NATO w Warszawie Polska, podobnie jak pozostałe państwa członkowskie, złożyła zobowiązanie do wzmocnienia odporności, które w znacznej części wpisuje się w obszar infrastruktury krytycznej i szeroko pojętego zarządzania kryzysowego. Z punktu widzenia NATO odporność państwa na zagrożenia jest funkcją m.in. zapewnienia ciągłości świadczenia podstawowych usług. Odradzające się w Europie zagrożenie terrorystyczne to kolejna zmiana w środowisku bezpieczeństwa, którą musimy brać pod uwagę. Nie możemy również pominąć regulacji unijnych, które odnoszą się do usług kluczowych (mam tu na myśli Dyrektywę Parlamentu i Rady UE w sprawie zapewnienia wysokiego bezpieczeństwa sieci i systemów teleinformatycznych tzw. *Dyrekty-*



wę NIS). Poza koniecznością dostosowania się do zmian, co jest naturalnym zjawiskiem w procesach zarządczych, w trakcie naszej pracy zidentyfikowaliśmy rozwiązania, które nie do końca sprawdziły się w praktyce i wymagają korekty.
Doświadczenia z ubiegłorocznych, tragicznych wydarzeń w Polsce potwierdzają, że zapewnienie ciągłości dostaw podstawowych dóbr i usług dla obywateli i przedsiębiorców jest jednym z najważniejszych zadań państwa. Myśląc o ochronie obywateli powinniśmy się skupić na ochronie przed skutkami zaprzestania świadczenia usług podstawowych. Zmiana podejścia na usługowe ma więc przede wszystkim umożliwić objęcie ochroną tych zasobów, które są niezbędne do świadczenia usług, a które dotychczas nie były uwzględniane w ochronie IK.

Jakie to usługi?
– Przede wszystkim zamierzamy identyfikować usługi krytyczne jak w definicji IK – kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców. Z kolei operatorów identyfikujemy na trzech poziomach w zależności od kryteriów ilościowych i jakościowych zakłócenia tej usługi – proszę nie sugerować się nazwami, są robocze, nie chcieliśmy po prostu używać pojęcia „kategoria". I tak na poziomie krajowym będzie to usługa, której zakłócenie świadczenia ma niekorzystny wpływ na bezpieczeństwo całego państwa, na poziomie regionalnym – usługa, której zakłócenie świadczenia ma niekorzystny wpływ na dany sektor/system IK lub kilka województw, zaś na poziomie lokalnym – usługa, której zakłócenie świadczenia ma niekorzystny wpływ na lokalną społeczność.

Podstawowym celem zmiany podejścia jest dostosowanie do zmian w środowisku bezpieczeństwa.

Konsekwencją takiego podziału będzie, w założeniu, przeniesienie części odpowiedzialności za IK na niższe poziomy administracji. Zatem na poziomie lokalnym za identyfikację operatorów IK, prowadzenie ich wykazu, zatwierdzanie planów ochrony usług krytycznych, współpracę z operatorami oraz zarządzanie kryzysowe na wypadek zakłócenia świadczenia danej usługi byłby odpowiedzialny wojewoda, natomiast na poziomie systemowym/regionalnym – ministrowie odpowiedzialni za systemy IK, a na poziomie krajowym – te zadania realizowałby dyrektor RCB.
Poza tym operatorzy usług krytycznych byliby odpowiedzialni za zapewnienie ich bezpieczeństwa i opracowanie planów ochrony tych usług, w tym wdrożenie BCMS (*Business Continuity Management System* – przyp. red.).
Chcemy także wprowadzić wymogi w zakresie zapewnienia bezpieczeństwa fizycznego, osobowego i teleinformatycznego na poziomie minimalnym i podwyższonym. Wymogi minimalne musiałby spełnić każdy operator usługi krytycznej, a podwyższone, w zależności od stopnia ryzyka, na poziomie krajowym.
Do obowiązków operatora IK należałoby cykliczne przeprowadzanie audytu wewnętrznego i przekazywanie jego wyników (w tym zaleceń poaudytowych) do właściwych organów. Organy mogłyby nakazywać usunięcie spostrzeżeń audytowych w określonym czasie. Obowiązkiem operatora byłoby również zgłaszanie zakłóceń w świadczeniu usług – progi zgłaszania określałby, we współpracy z dyrektorem RCB, organ właściwy dla danego poziomu IK.
W końcu chcemy dać właściwym organom możliwości kontroli po wystąpieniu zakłócenia świadczenia usługi lub w przypadku niezrealizowania zaleceń poaudytowych, a także możliwość karania za notoryczne uchylanie się od realizacji obowiązków. Niestety, po upływie 4 lat od przyjęcia pierwszego Programu i powiadomieniu operatorów o ujęciu ich infrastruktury w wykazie IK, wciąż zdarzają się przypadki niesporządzenia przez nich planu, i to

pomimo ponagleń... Pamiętajmy również, że część z tych zmian będzie wymagała zmian w ustawie o zarządzaniu kryzysowym.

Jak zmieni się lista obiektów IK po zmianie podejścia z obiektowego na usługowe?
– Trudno jednoznacznie odpowiedzieć na to pytanie. Jako że wykaz będzie obejmował trzy poziomy, część usług (obiektów świadczących usługi krytycznej), które teraz znajdują się w wykazie przejdzie do innego poziomu, będzie to dotyczyć przede wszystkim usług świadczonych w systemie zaopatrzenia w wodę, które z reguły są świadczone lokalnie. Część obiektów „zwinie się" w jedną usługę (np. w systemach elektroenergetycznym czy łączności), pojawią się również nowe usługi. Jesteśmy jeszcze w trakcie opracowywania szczegółowych kryteriów, dlatego pytania o szacowaną liczbę usług będzie można formułować dopiero po zakończeniu tego procesu.

RCB opracowało NPOIK w roku 2013 i 2015. Kiedy można spodziewać się kolejnego?
– Kolejnego Programu można spodziewać się w połowie tego roku. Jako że NPOIK zawiera kryteria identyfikacji IK, opracowanie kryteriów determinuje czas wprowadzenia aktualizacji Programu.

Nad nowym podejściem do ochrony IK oraz o standardach jej ochrony dyskutowano podczas V Krajowego Forum Ochrony Obiektów Infrastruktury Krytycznej w grudniu ub.r. Jakie są konkluzje tego spotkania?
– Przedstawiając na Forum założenia zmian, spotkaliśmy się z przychylnym przyjęciem. Operatorzy również zauważają niedoskonałości systemu. W opinii uczestników kierunek zmian jest dobry, ale o ostatecznej akceptacji będziemy mogli mówić, gdy opracujemy szczegóły zaproponowanych rozwiązań, które jak wiadomo decydują również o skuteczności.

Program NPOIK przewiduje również organizację forów na szczeblu branżowym. Czy odbyły się takie spotkania z branżą security?
– Program przewiduje spotkania branżowe dla forów na poziomie wojewódzkim, ale w rozumieniu spotkania przedstawicieli wybranego systemu (sektora) IK. Oczywiście na fora organizatorzy mogą zapraszać przedstawicieli innych sektorów czy świata nauki, jeśli przyczyni się to do podniesienia poziomu wiedzy uczestników lub rozwiązania konkretnego problemu. Z mojej wiedzy wynika, że dotychczas nie odbyło się żadne spotkanie z udziałem przedstawicieli branży security.

O problemach związanych z zabezpieczeniem IK rozmawiali w maju ub.r. uczestnicy organizowanego przez nas* śniadania ekspertów a&s Polska. *Obok oferentów techniki zabezpieczającej i security managerów operatorów IK, obecni byli także przedstawiciele RCB. Po spotkaniu uczestnicy przyznali, że była to dobra okazja do wymiany doświadczeń w zakresie nowości technicznych, przepisów prawa i postrzegania bezpieczeństwa. W maju tego roku zorganizujemy podobne spotkanie – czy do tego czasu będą znane szczegóły dot. nowego NPOIK?
– Mam nadzieję. Jak powiedziałem wcześniej, intensywnie pracujemy nad kryteriami identyfikacji usług krytycznych oraz założeniami do zmiany ustawy o zarządzaniu kryzysowym. Jeśli będziemy mogli, na pewno w trakcie kolejnego spotkania przedstawiciel RCB podzieli się najświeższymi informacjami w tym zakresie.

Potrzebą krytyczną jest edukacja wszystkich stron systemu ochrony IK - w szczególności w dziedzinie cyberbezpieczeństwa. Jakie są zalecenia w tym zakresie?
– Podczas posiedzenia Międzyresortowego Zespołu ds. Zagrożeń Terrorystycznych, które odbyło się 14 marca, zostało przyjęte sprawozdanie *Zespołu zadaniowego do spraw opracowania standardów zabezpieczeń antyterrorystycznych i reguł współdziałania dotyczących infrastruktury krytycznej oraz zasad dokonywania sprawdzenia zabezpieczeń obiektów infrastruktury krytycznej, zgodnie z przepisami ustawy o działaniach antyterrorystycznych*. Jednym z wyników prac zespołu zadaniowego było opracowanie minimalnych wymagań w obszarach zapewnienia bezpieczeństwa fizycznego, osobowego i właśnie teleinformatycznego. W obszarze bezpieczeństwa teleinformatycznego dokument bazuje na rozpowszechnionych w Polsce normach PN-EN ISO serii 27000, wzbogaconych o komentarze i uwagi dotyczące praktycznego stosowania tych wymagań. Mam nadzieję, że dokument w niedługim czasie stanie się publicznie dostępny. Obecnie trwają prace nad propozycją jego wdrożenia. Biorąc to pod uwagę, w przypadku bezpieczeństwa teleinformatycznego zalecić mogę wdrożenie systemu lub wybranych elementów systemu zarządzania bezpieczeństwem informacji opisanego w tych normach.

W opinii operatorów IK kierunek zmian jest dobry, ale o ostatecznej akceptacji będziemy mogli mówić, gdy opracujemy szczegóły zaproponowanych rozwiązań, które decydują również o skuteczności.

Czy zaleca się stosowanie rozwiązań Internetu Rzeczy - z jednej strony oferujących nowe „inteligentne" funkcje, z drugiej zaś są podatne na ataki hakerskie?
– Jako RCB koncentrujemy się raczej na bezpieczeństwie świadczenia usług i pracy IK. Przy okazji wdrażania czy stosowania wszelkich nowych rozwiązań, wskazujemy na konieczność przeprowadzenia oceny wpływu danego rozwiązania właśnie na bezpieczeństwo świadczenia usługi i pracy IK. Wydaje się, że w tym obszarze producenci rozwiązań z zakresu Internetu Rzeczy mają jeszcze dużo do nadrobienia.

Kolejne kontrowersyjne narzędzie ochrony to drony. Z jednej strony zapewniają bezpieczeństwo (np. na dużych przestrzeniach), z drugiej jednak – mogą stanowić zewnętrzne zagrożenie. Jak RCB widzi ten problem?
– Dokładnie w ten sam sposób jak Państwo, czyli jako szansę i zagrożenie zarazem. W związku z tym, że otrzymujemy od operatorów informacje o pojawiających się próbach nieuprawnionego użycia dronów, staramy się pomóc w tym obszarze. Razem z Urzędem Lotnictwa Cywilnego, w ramach prac Międzyresortowego Zespołu ds. Zagrożeń Terrorystycznych, staramy się wyposażyć operatorów IK w narzędzia, przede wszystkim prawne, pozwalające na skuteczną reakcję na tego typu incydenty.

Dziękujemy za rozmowę.

Experience The Next®

OTWARTA PLATFORMA INTEGRUJĄCA
SYSTEMY BEZPIECZEŃSTWA

Pobierz darmową wersję na axxonsoft.com/pl

AxxonSoft Polska Sp. z o.o.
ul. Olszańska 5H
31-513 Kraków

Tel.: +48 12 393 58 01
E-mail: **poland@axxonsoft.com**
www.axxonsoft.com/pl

Każdego dnia jesteśmy bombardowani przez media informacjami o różnych zagrożeniach, ale niewiele osób zwraca na nie uwagę, wychodząc z założenia, że dopóki nas to nie dotyka, dopóty nie ma potrzeby się tym przejmować. Nawet jeśli skutki tych zagrożeń odczujemy bezpośrednio, to gdy emocje opadną, i tak o nich zapominamy.

Zagrożenia bezpieczeństwa

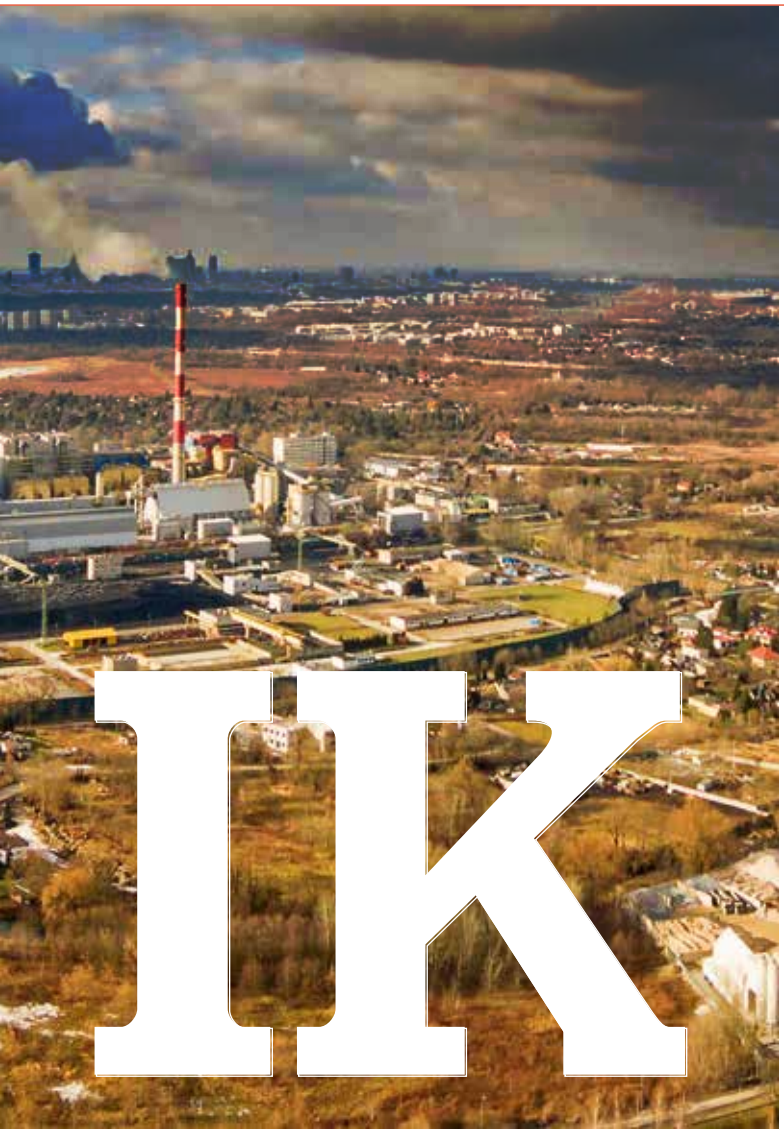
Andrzej Kozłowski
Biuro Bezpieczeństwa
PGNiG TERMIKA

Lekceważącą postawę wobec zagrożeń kreują nawet osoby wysoko postawione w strukturach organizacji, odpowiedzialne za bezpieczeństwo infrastruktury krytycznej (IK). Wynika ono często z koncentrowania się na realizacji założonych celów ekonomicznych (lub własnych), ale również braku podstawowej wiedzy z zakresu ochrony infrastruktury krytycznej oraz świadomości możliwych skutków ich nieodpowiedzialności.

Na całym świecie występuje stan ciągłego zagrożenia bezpieczeństwa, któremu ludzie starają się przeciwstawić. Aby ich działania były skuteczne, potrzebna jest wiedza na temat przyczyn powstawania tych zagrożeń, możliwych skutków ich wystąpienia, struktury i natury niebezpiecznych zjawisk oraz ich wczesnej i skutecznej identyfikacji. Dzięki niej możliwe jest opracowanie odpowiednich procedur postępowania na wypadek zagrożenia, które będą w stanie zminimalizować prawdopodobieństwo jego wystąpienia, złagodzą jego przebieg oraz ograniczą skutki. Dlatego podmioty zainteresowane utrzymaniem stabilnego poziomu bezpieczeństwa, a zwłaszcza podmioty o strategicznym znaczeniu dla bezpieczeństwa państwa i jego obywateli powinny korzystać z wiedzy o możliwych zagrożeniach do budowania indywidualnych systemów zarządzania bezpieczeństwem IK.

Obecnie największym wyzwaniem dla osób zajmujących się zapewnieniem bezpieczeństwa IK jest przeciwdziałanie zagrożeniom cywilizacyjnym, zwłaszcza tym, które zostały wywołane przez człowieka i postęp techniczny. To one są najczęstszymi przyczynami awarii i katastrof. Zazwyczaj wynikają z błędów projektowych i różnych wad (materiału, wykonania, montażu), a także niewłaściwej eksploatacji urządzeń i ich nadmiernego zużycia.

Skutki awarii są często nieprzewidywalne, mogą obejmować zasięgiem tereny zarówno lokalne, jak i oddalone o setki kilometrów. Szczególnie niebezpieczne są awarie elektrowni i elektrociepłowni, które mogą doprowadzić do *blackoutu*[1)], oraz awarie zakładów, w których znajdują się niebezpieczne środki chemiczne mogące skazić środowisko naturalne. Przyczyną skażeń mogą być zamierzone działania ludzi, a więc akty przemocy o charakterze terrorystycznym, których celem jest wywołanie przerażenia w społeczeństwie. Szczególnie niebezpieczne są akty terroryzmu zbiorowego o podłożu politycznym, których ofiarami są zazwyczaj przypadkowe osoby. Terroryści do ataków wykorzystują wszelkie możliwe środki, które mogą wywołać nie tylko skutek śmiertelny, ale także choroby zakaźne, skażenie śro-



dowiska, zniszczenie budynków, urządzeń technicznych, linii komunikacyjnych oraz infrastruktury gospodarczej i przemysłowej.

Zagrożenie bezpieczeństwa IK stanowią również procesy migracyjne ludności z terenów słabiej rozwiniętych lub dotkniętych działaniami wojennymi do dużych aglomeracji, gdzie łatwiej o pracę. Efektem jest uzależnienie się od „scentralizowanych dostaw: żywności, wody, gazu, energii elektrycznej oraz odprowadzania ścieków i wywozu odpadów", a także duże prawdopodobieństwo wystąpienia poważnych awarii technicznych, zagrażających mieszkańcom aglomeracji i środowisku naturalnemu. Skutki niewłaściwej urbanizacji aglomeracji miejskich można zaobserwować właściwie w każdym dużym mieście. Są nimi nasilające się korki na ulicach, zanieczyszczenie powietrza, nadmierne zużycie wody, powstawanie ogromnych ilości śmieci i innych odpadów oraz ubożenie terenów zielonych.

We współczesnym świecie przedsiębiorstwa i społeczeństwo są coraz bardziej narażone na akty przemocy, konieczne jest zatem zastosowanie odpowiednich środków zaradczych w obrębie jednostek ważnych dla bezpieczeństwa państwa i obywateli. Należy przygotować pracowników tych jednostek na wypadek wystąpienia takich sytuacji, jak napad, włamanie, wzięcie zakładników, podłożenie ładunku wybuchowego, skażenie terenu środkami biologicznymi, chemicznymi, promieniotwórczymi. Trzeba przede wszystkim dokonać analizy i oceny możliwości pojawienia się tego typu zagrożeń, następnie opracować i wdrożyć procedury postępowania w celu zminimalizowania ryzyka wystąpienia tego typu przestępstw oraz złagodzenia konsekwencji ich ewentualnego zaistnienia. Środkami zaradczymi może być zastosowanie ochrony fizycznej i technicznej na różnych poziomach, a także działania informacyjne, szkolenia i treningi.

Olbrzymim zagrożeniem dla obiektów IK jest obecnie globalny rozwój sieci internetowej, powodujący przenikanie niepożądanych zjawisk ze świata wirtualnego do realnego. Rozwój ten doprowadził do powstania nowego rodzaju zagrożeń związanych z cyberprzestępczością. W związku z tym działania przedsiębiorstw IK powinny opierać się na czynnych i systematycznie aktualizowanych zasadach bezpieczeństwa, mających na celu zapewnienie ochrony personelu, majątku, działalności operacyjnej i ich wyników.

Wartością, która powinna podlegać szczególnej ochronie, jest wiedza pracowników na tematy związane z funkcjonowaniem przedsiębiorstwa. Bardzo ważna jest przy tym ochrona przepływu informacji, zwłaszcza przetwarzanych w systemach informatycznych.

Pracownicy przedsiębiorstw IK powinni mieć świadomość dużego prawdopodobieństwa zagrożenia związanego z próbami pozyskania przez agentów obcego wywiadu i ugrupowania terrorystyczne informacji o stanie ochrony i organizacji ich jednostek, systemach zabezpieczeń technicznych, stosowanej technologii oraz systemach operacyjnych odpowiedzialnych za produkcję. Cyberprzestępcom do zainfekowania systemów operacyjnych wystarczy zwykły laptop z dostępem do sieci online. Natomiast walka z cyberterroryzmem jest bardzo trudna ze względu na brak jakichkolwiek granic w cyberprzestrzeni.

Każdy pracownik powinien wiedzieć, że aby przedsiębiorstwo mogło skutecznie prowadzić działalność w wymiarze wewnętrznym, a także kontaktach z klientami i kontrahentami, musi posiadać odpowiedni system wsparcia informatycznego, który niestety może być narażony na ataki hakerów. Pracownicy w trakcie korzystania z systemów i łączności informatycznej muszą zatem przestrzegać wymogów operacyjnych związanych z ochroną: informacji przed nieupoważnionym dostępem i manipulacją, danych o działalności przedsiębiorstwa, systemów sterowania odpowiedzialnych za utrzymanie ruchu urządzeń technologicznych, systemów finansowych i administracyjnych.

Przedsiębiorstwa powinny posiadać szczegółowe instrukcje i procedury postępowania zapobiegające możliwości wystąpienia tego typu ryzyka oraz wy-

[1] *Blackout* – utrata napięcia w sieci elektroenergetycznej na znacznym obszarze w wyniku nałożenia się kilku zdarzeń losowych (awarie sieci, wyłączenia elektrowni, ekstremalne warunki atmosferyczne), gdzie dochodzi do przekroczenia krytycznych wartości parametrów technicznych (częstotliwość, napięcie) oraz odłączenia od sieci elektrowni, co skutkuje utratą napięcia na całym obszarze objętym zakłóceniem.

kształcić wśród pracowników zachowania ukierunkowane na stworzenie kultury bezpieczeństwa informatycznego.
Kolejnym zagrożeniem związanym z postępem technicznym i cywilizacyjnym jest możliwość użycia do ataku terrorystycznego bezzałogowych statków, aparatów powietrznych zwanych potocznie dronami. Urządzenia te są dostępne prawie w każdym kraju za niewielkie pieniądze, a ich unikalne cechy użytkowe sprawiają, że są chętnie wykorzystywane do działań przestępczych. W rękach terrorystów mogą się stać bardzo niebezpieczną bronią umożliwiającą inwigilację terenu oraz przenoszenie i zrzut niebezpiecznego ładunku w dowolne miejsce.
Drony są tym bardziej groźne, że ich wykrycie przez obecnie stosowane systemy ochrony obwodowej jest właściwie niemożliwe. Co prawda istnieją systemy antydronowe, ale nie dają one pełnej gwarancji bezpiecznego unieszkodliwienia drona, zanim osiągnie on zakładany cel (najczęściej ze względu na ograniczony zasięg ich działania). Jeśli nawet uda się przejąć kontrolę nad sterowaniem drona i sprowadzić go na ziemię, to pozostaje jeszcze kwestia dezaktywowania ładunku, o którym nie ma żadnych informacji (a możliwość zastosowanych mechanizmów aktywacji i środków rażenia jest ograniczona jedynie pomysłowością konstruktora).
Skuteczne zarządzanie bezpieczeństwem obiektów IK jest coraz trudniejsze, wymaga bowiem specjalistycznej wiedzy z różnych obszarów działalności człowieka. Jest ona niezbędna do identyfikacji i prognozowania ewentualnych stanów zagrożeń, przygotowania adekwatnych scenariuszy postępowania na takie sytuacje oraz sporządzenia i uzgodnienia planów ochrony, a także planów obrony cywilnej tych obiektów.
Aby zapobiegać i przeciwdziałać zagrożeniom związanym z przestępczą działalnością człowieka nie należy zapominać o bezpośredniej ochronie fizycznej obiektów, ani o ich odpowiednim zabezpieczeniu technicznym. Chodzi o inwestycje w zabezpieczenia budowlane oraz elektroniczne systemy sygnalizacji włamania i napadu, kontroli dostępu, ochrony obwodowej, telewizji dozorowej, zabezpieczeń informatycznych, dźwiękowego ostrzegania czy ochrony przeciwpożarowej.
Zastosowanie najnowocześniejszej techniki nie daje jednak pewności, że uda się zapobiec aktom zagrażającym bezpieczeństwu. Zwiększa się natomiast szansa ich wykrycia i ograniczenia skutków, m.in. dzięki identyfikacji osoby, śledzeniu rejonów przemieszczania się, zasygnalizowaniu przedostania się do wydzielonej strefy lub próby włamania do systemu informatycznego lub identyfikacji przeszukiwanych lub kopiowanych obszarów z danymi.
Nawet najprostsze zabezpieczenie mechaniczne (np. zamek z zasuwą), budowlane (krata, płot, ściana itp.) lub interwencja pracownika ochrony może skutecznie podnieść poziom bezpieczeństwa.

BIO

Andrzej Kozłowski Specjalista ds. bezpieczeństwa w Biurze Bezpieczeństwa PGNiG TERMIKA SA. Ekspert od zarządzania kryzysowego i organizacji ochrony w obiektach energetycznych. Autor książki „Zarządzanie bezpieczeństwem w obiektach energetycznych" i publikacji o zagrożeniach bezpieczeństwa energetycznego.

Wojna

Zagrożenie bezzałogowymi statkami powietrznymi dla infrastruktury krytycznej jest realne. Drony to temat świeży, ale rynek technologiczny jest już na tyle rozwinięty, że pojawiają się nowsze i bardziej dopracowane konstrukcje. W rezultacie może to stanowić problem nawet dla najnowocześniejszych systemów antydronowych.

Łukasz Wieczorek
specjalista ds. bezpieczeństwa, PGNiG TERMIKA

To dopiero początek „wojny na drony". Coraz rzadsze będą ataki organizowane bezpośrednio przez ludzi i z udziałem ludzi, gdyż to oni wykorzystują technikę i naukę do różnych celów zarówno pozytywnych (leczenie różnych chorób, ułatwienie życia codziennego), jak i zniszczenia ładu i pokoju na świecie.
Bezzałogowe statki powietrzne, potocznie nazywane dronami, są pilotowane z centrum dowodzenia przez przeszkolonego operatora lub mają zakodowane konkretne cele do osiągnięcia (są w pełni autonomiczne). Dzięki temu, że są kierowane zdalnie, nie ma strat w ludziach, np. po zestrzeleniu takowego drona.
Można je sklasyfikować wg kilku kategorii, np. ich masy, czasu działania, maksymalnej wysokości lotu.
W kategorii masy można wyróżnić bardzo lekki dron, którego masa nie przekracza 5 kg, lekki ważący między 5 a 50 kg, średniej wagi dron ma masę w zakresie między 50 a 200 kg, do kategorii ciężkich dronów zaliczamy o masie od 200 do 2 tys. kg (2 ton), a hierarchię wagową zamykają drony bardzo ciężkie przekraczające 2 tys. kg (2 tony).
Czas lotu drona może wynosić od 6 nawet do 40 godzin, a jego zastosowaniem może być np. wsparcie wojska w operacjach taktycznych i strategicznych.
Ostatnia kategoria działania bezzałogowych statków powietrznych to maksymalna wysokość lotu: niska (poniżej 1000 m n.p.m.) lub wysoka (nawet powyżej 10 tys. m n.p.m.)
Potencjalni terroryści, którzy dopuszczają się ataku na obiekty IK, najprawdopodobniej posłużą się dronami bardzo lekkimi lub lekkimi. Są one dostępne niemal wszędzie i bez większych problemów. Nie sprawiają także kłopotów

na drony

z obsługą, a ich cena jest na tyle niska, że nawet ich zniszczenie przy niepowodzeniu potencjalnego aktu terroru nie jest w żaden sposób odczuwalne. Drony lekkie nie przeniosą wprawdzie ciężkich ładunków, ale jak wiadomo już niewielka ilość bakterii wąglika jest w stanie zabić wiele osób. Można również doczepić do drona kamerę cyfrową, która pozwoli potencjalnym terrorystom na zapoznanie się z topografią terenu danego obiektu IK, który jest ich celem.

Czym jest infrastruktura krytyczna? Właściwie jest to termin używany w odniesieniu do zasobów mających podstawowe znaczenie dla funkcjonowania społeczeństwa i gospodarki. Najczęściej kojarzy się z nim przemysł energetyczny i przemysł paliwowy, sektor telekomunikacji, gospodarkę wodną (ścieki, woda pitna, woda powierzchniowa), dystrybucję żywności, ochronę zdrowia, transport, instytucje finansowe czy służby bezpieczeństwa. Jednym z największych zagrożeń IK jest zagrożenie chemiczne. Przedostanie się do wód gruntowych czy dużych zbiorników wodnych groźnych wirusów oraz bakterii powoduje narażenie dużej liczby ludności na utratę zdrowia, a nawet życia. Dron może przenieść substancję niebezpieczną (np. wirusy czy bakterie) nad większe skupisko ludzi (np. podczas imprez masowych czy demonstracji). Kolejnym przykładem może być pojawienie się drona z niewielkim ładunkiem wybuchowym, np. nad lotniskiem czy dużym zbiornikiem substancji ropopochodnych w bazie paliwowej. Niezauważony niewielki bezzałogowy obiekt latający potrafi sparaliżować ruch portu lotniczego czy narazić zdrowie i życie ludzi podczas podłożenia ładunku w porcie naftowym, co dodatkowo niesie ogromne straty finansowe. Bezzałogowych statków powietrznych wyposażonych w dobrą optykę z rejestracją obrazu (na wewnętrznym dysku lub z możliwością bezpośredniego przesyłu obrazu do operatora) potencjalni terroryści mogą używać do sporządzenia mapy lokalizacyjnej punktu, na który atak będzie najbardziej odczuwalny i powodujący najwięcej zniszczeń. Takie skutki miałby atak na obiekt z sektora przemysłu paliwowego i energetycznego. Przykładowo podczas ataku terrorystycznego z użyciem drona na sektor energetyczny może dojść do tzw. *blackoutu*, czyli braku napięcia w sieci elektroenergetycznej na znacznym obszarze.

Czy jest możliwa obrona przed atakiem dokonanym za pomocą bezzałogowego statku powietrznego? Moim zdaniem żadna ochrona obwodowa nie jest w stanie zagwarantować 100% skuteczności... Oczywiście sektor odpowiedzialny za bezpieczeństwo rozwija się i powstają różnego rodzaju systemy antydronowe. W ich skład wchodzą podsystemy wykrywania (sensory optyczne, radiolokacyjne czy akustyczne) oraz reagowania, mające na celu zakłócenie i trwałe uszkodzenie układów elektronicznych lub takie, które niszczą drony w sposób mechaniczny. Cena takich systemów jest jednak (jeszcze) na tyle wysoka, że niewielu operatorów infrastruktury krytycznej zdecyduje się dołączyć taką formę obrony do swojej ochrony obwodowej.

BIO

Łukasz Wieczorek
Specjalista ds. bezpieczeństwa w PGNiG TERMIKA SA, doktorant na Wydziale Bezpieczeństwa Narodowego Akademii Sztuki Wojennej.

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

Nowe rozwiązania w ochronie perymetrycznej dzięki zaawansowanej analizie obrazu

Istotą ochrony perymetrycznej nie jest zastosowanie systemu dozoru wizyjnego, lecz dostarczenie obrazu, który pozwoli dokonać najbardziej trafnej oceny sytuacji.

John Merlino

Znaczna część materiału zarejestrowanego bądź obrazu na żywo nigdy nie zostanie obejrzana przez operatora. Powód? Duża liczba kamer w systemie dozorującym np. obiekty MON czy agencji rządowych zapewnia obraz na żywo w trybie ciągłym, ale prześledzenie jego zapisu w całości jest praktycznie niewykonalne, ponieważ zgromadzony materiał jest zbyt obszerny.

Analiza obrazu, sztuczna inteligencja i uczenie maszynowe – technologie te pozwalają z olbrzymich ilości danych wyłuskać użyteczne informacje i na ich podstawie operator może szybciej podejmować właściwe działania. W poddanym analizie zapisie zachowywane są w formie danych jedynie odpowiednio przefiltrowane fragmenty. Aplikacje oparte na sztucznej inteligencji i uczeniu maszynowym umożliwiają dodawanie do materiału wizyjnego metadanych i takie ich przetwarzanie, by stanowiły funkcjonalne narzędzia w zastosowaniach publicznych i prywatnych.

AI, *machine learning*: jak można z nich korzystać w systemach dozorowych

Na początku zdefiniujmy sztuczną inteligencję (AI) i uczenie maszynowe.

Sztuczna inteligencja – szersze pojęcie – jest elementem informatyki umożliwiającym inteligentne wykonywanie przez komputer zadań z reguły realizowanych przez człowieka. Uczenie maszynowe przenosi tę koncepcję na wyższy poziom, jest zastosowaniem sztucznej inteligencji umożliwiającym komputerom analizę danych oraz najlepszy możliwy sposób „uczenia". Stanowi właściwie automatyzację tworzenia modelu analitycznego – komputer „ustala" optymalne rozwiązanie bez potrzeby wcześniejszego zaprogramowania. Wszystko to przekłada się na dozór wizyjny, w szczególności gdy ochroną obwodową są objęte rozległe obszary. Oprogramowanie sztucznej inteligencji i uczenia maszynowego jest nie tylko w stanie wyodrębnić różne typy obrazu, ale także umożliwia przeglądanie wszystkich danych wizyjnych w celu dokonania wyboru materiału do dalszej analizy na podstawie danych fizycznych, ruchu, zachowania obiektów i innych kryteriów.

System może np. wysyłać alarmy, gdy w obszarze ograniczonym, takim jak strefy zastrzeżone na lotnisku, wystąpi ruch. Sztuczna inteligencja pozwala określić, czy ruch ten został spowodowany przez człowieka, pojazd, czy zwierzę, a może na skutek drobnych zawirowań atmosferycznych. Na podstawie posiadanego „doświadczenia" uczenie maszynowe proponuje podjęcie określonej reakcji.

Sztuczna inteligencja i uczenie maszynowe są czymś na kształt „zwielokrotnionej siły działania", umożliwiającej zoptymalizowanie działań personelu ochrony. Dzięki temu, że monitorowanie obrazu wymaga mniejszej liczby operatorów, organizacje są w stanie pracować wydajniej.

Inteligentne funkcje obrazu: udoskonalanie ochrony obwodowej

Analiza obrazu wykorzystuje trzy podstawowe rodzaje technologii informatycznych:

- **analizę opartą na pikselu** – najbardziej podstawowy format z wymienionych, wysyła alarmy w przypadku pogorszenia jakości obrazu (spowodowanego np. sabotażem sprzętowym) lub wykrycia ruchu w obrazie;
- **analizę opartą na obiekcie** – bardziej zaawansowana, jako że potrafi rozpoznawać obiekty typu samochody, ludzie, drzewa, budynki itp. Obejmuje dwie kategorie analizy: śledzenie obiektów i rozpoznawanie obiektów;
- **analizę specjalistyczną,** która korzysta z informacji opartych na pikselach i obiektach w celu sprawdzenia obrazu pod kątem specjalistycznych zastosowań, czyli rozpoznawania tablic rejestracyjnych, rozpoznawania twarzy czy wykrywania pożaru.

Wymienione narzędzia analityczne znajdują wiele zastosowań w ochronie obwodowej, m.in. algorytmy:

- **przekroczenia linii** – aplikacje sygnalizujące przekroczenie linii (nazywane również linką rozciągniętą nisko nad ziemią) tworzące wirtualne ogrodzenia lub obszary zastrzeżone. Dla tak określonych granic możliwe jest wygenerowanie reguł, np. po przekroczeniu przez samochód określonej uprzednio granicy zostaje wysłany alarm;
- **sygnalizacji włamania** – inny rodzaj śledzenia obiektów, określający, czy do zastrzeżonej strefy dostały się niepowołane osoby bądź pojazdy. Śledzony jest ruch z jednej strefy do innej, a w momencie wykrycia ruchu w określonym obszarze zostaje uruchomiony zapis;
- **pozostawienia obiektu** – obiekt ruchomy jest umieszczany na stałe w polu widzenia kamer i pozostaje tam przez określony czas. Obiektem może być bomba, torba z pieniędzmi albo zbiór tajnych informacji;
- **wykrywania podejrzanego zachowania** – rejestruje się czas przebywania osób na określonym obszarze. Po wykryciu podejrzanego zachowania na obrazie ukazuje się dokładny czas i miejsce detekcji. Zostaje też podjęta próba identyfikacji osób.

Analiza obrazu odgrywa i nadal będzie odgrywać kluczową rolę w ochronie granic oraz ochronie obwodowej.

Sztuczna inteligencja i uczenie maszynowe umożliwiają optymalizację działań personelu.

Gdy personel otrzyma informację o niecodziennym ruchu bądź zachowaniu i zaklasyfikuje te zdarzenia, funkcja inteligentnej analizy obrazu umożliwi rozpoznanie potencjalnych zagrożeń, o ile nadal występują w obszarze, i tym samym podjęcie sprawnej reakcji.

Innym zastosowaniem jest powstrzymywanie nielegalnego przekraczania granic – w tym przypadku z kilkoma poziomami detekcji. Powszechnie stosuje się kamery termowizyjne. Analiza obrazu wsparta naziemną techniką radarową i zoptymalizowaną technologią kamer HD jest stosowana do kontroli obszarów detekcji, określenia poziomu zagrożenia oraz podjęcia odpowiednich działań.

W ochronie rozległych obszarów i granic coraz większą rolę odgrywa rozpoznawanie twarzy oraz rozpoznawanie tablic rejestracyjnych.

Analiza predykcyjna zgromadzonych danych

Należy też zwrócić uwagę na możliwość wykorzystania analizy treści obrazu w przewidywaniu potencjalnych zdarzeń. Analiza predykcyjna obejmuje zastosowanie metadanych pochodzących z aplikacji uczenia maszynowego i sztucznej inteligencji, pomocnych w dokładniejszym przewidywaniu zdarzeń i zachowań. Jest to szczególnie istotne dla personelu ochrony, który powinien działać proaktywnie.

System kontroli dostępu w obiektach infrastruktury krytycznej

Infrastruktura krytyczna (IK) to – jak można przeczytać na stronie Rządowego Centrum Bezpieczeństwa – systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty (w tym budowlane), urządzenia, instalacje oraz usługi, które są kluczowe dla bezpieczeństwa państwa i obywateli.

Błażej Ożga

Opracowany przez Rządowe Centrum Bezpieczeństwa Narodowy Program Ochrony Infrastruktury Krytycznej wskazuje na wzrost świadomości różnego rodzaju zagrożeń w tym obszarze. Dokument *Standardy służące zapewnieniu sprawnego funkcjonowania IK – dobre praktyki i rekomendacje* wzmacnia to poczucie.

Brak wiedzy, brak świadomości

Amerykańska agencja GAO (*Government Accountability Office*) w swoim raporcie zwraca uwagę Departamentowi Bezpieczeństwa Wewnętrznego USA (*Department of Homeland Security*) na brak strategii i personelu, aby móc zdefiniować, oszacować oraz zaadresować rodzaje ryzyka wynikające z cyberataków, których celem mogą być systemy kontroli dostępu w ponad 9 tys. obiektach federalnych. Amerykański instytut ICS-CERT (*Industrial Control Systems Cyber Emergency Response Team*) w 2016 r. odnotował 290 incydentów cyberataków na infrastrukturę krytyczną. Najbardziej narażone były sektory produkcji krytycznej – 63 ataki, sektor telekomunikacyjny – 62 ataki oraz energetyczny, w którym odnotowano aż 59 ataków.

Technologia IT

Infrastruktura IT to nie tylko komputery, serwery czy systemy operacyjne. Technologia IT już dawno została zaadaptowana przez producentów systemów zabezpieczeń i automatyki przemysłowej. Jest też powszechnie stosowana do zarządzania sieciami w sektorach: energetycznym, transportowym czy telekomunikacyjnym. Połączone w sieci IP sterowniki stają się coraz częściej celem ataków. Cyberataki na systemy IT mogą zagrażać bezpieczeństwu całego kraju. Jednak w odróżnieniu od działów IT, gdzie świadomość zagrożeń jest w miarę wysoka, w branży security wiedza na temat cyberbezpieczeństwa jest znikoma.

Stuxnet

W roku 2010 został wykryty robak stuxnet, który dokonał spustoszenia w systemie teleinformatycznym elektrowni atomowej w Iranie, atakując sterowniki PLC odpowiedzialne za procesy w systemie automatyki przemysłowej. Stuxnet to pierwszy w historii PCL *rootkit* rozprzestrzeniający się w systemach Windows, w szczególności WinCE, bardzo popularnym systemie operacyjnym typu *embedded*. Taki system operacyjny jest wykorzystywany również w systemach zabezpieczeń.

> Według statystyk PwC średnio 4 godziny zajmuje hakerowi uzyskanie dostępu do systemów i danych, 70% incydentów jest powodowanych działaniami pracowników, a 31% cyberataków kończy się ujawnieniem lub modyfikacją danych firmowych.

Jak to się ma do systemów kontroli dostępu?

Obiekty infrastruktury krytycznej muszą podlegać szczególnej ochronie. Stosowane systemy powinny spełniać najwyższe standardy bezpieczeństwa nie tylko w odniesieniu do norm odwołujących się do systemów zabezpieczeń, ale także wymogów stawianych systemom IT. Standardowo obiekty IK są chronione przez zabezpieczenia mechaniczne (ogrodzenia, bramy) oraz elektroniczne – systemy kontroli dostępu, telewizji dozorowej, sygnalizacji włamania i napadu oraz zarządzający bezpieczeństwem SMS (*Security Management System*). Częstą praktyką jest też integracja systemów elektronicznych z systemami budynkowymi BMS (*Building Management System*) i sterowania windami. Wszystkie te elementy są spięte za pomocą sieci TCP/IP przy użyciu switchy i routerów. Praktycznie każde podłączone urządzenie jest oparte na protokole IP. Z tego względu występuje kilka podstawowych zagrożeń:

- **Elementy systemu są dostępne z zewnątrz, w związku z czym są podatne na ataki.**
- **Brak świadomości – szefowie bezpieczeństwa zakładają, że sieć LAN, do której są podłączone urządzenia, jest odseparowana i bezpieczna.**
- **Brak wiedzy – wielu szefów bezpieczeństwa, instalatorów czy też serwisantów nie ma dostatecznej wiedzy z obszaru IT, a więc i cyberbezpieczeństwa.**
- **Luki w systemie BMS/SCADA i możliwość ich wykorzystania w ataku na system bezpieczeństwa.**

Do głośnych incydentów, które miały miejsce w 2017 r., związanych z systemem kontroli dostępu należy atak na kurort narciarski w austriackich Alpach. Atak *ransomware* spowodował paraliż hotelu, uniemożliwiając obsłudze wydawanie gościom kart dostępu. Właściciele hotelu byli zmuszeni rozważyć zamianę elektronicznych

identyfikatorów na klucze mechaniczne. Jak podaje magazyn „Wired", powołując się na raport firmy Symantec, w 2017 r. w ponad 20 incydentach hakerom udało się dostać do sieci różnych firm, w tym należących do sektora infrastruktury krytycznej w USA. Analitycy, którzy wykryli te ataki, stwierdzili, że hakerzy uzyskali kontrolę nad interfejsami stosowanymi przez inżynierów do wysyłania komend, np. do wyłączników prądu. Umożliwiło to hakerom m.in. odcięcie zasilania w sektorach zarówno prywatnym, jak i biznesowym.

Kontroler jak PC

W ciągu ostatnich 15 lat w wyniku rewolucyjnych przemian systemy zabezpieczeń, także kontroli dostępu, stały się systemami IT. Teraz kontroler systemu KD jest jak komputer PC podłączony do sieci IP w celu komunikacji z serwerem oraz innymi elementami w sieci. Oznacza to, że jest narażony na takie same metody ataku jak każdy komputer. W obszarze IT standardy bezpieczeństwa z roku na rok są wyższe. Branża security natomiast nie ma takiej wiedzy na temat cyberataków. To pokazuje olbrzymie potencjalne zagrożenie systemów kontroli dostępu.

Z punktu widzenia cyberprzestępcy niedostatecznie zabezpieczony kontroler może być celem ataku, może też zostać wykorzystany jako brama do całej sieci. Staje się więc słabym jej ogniwem. Przeanalizujmy możliwości techniczne, jakie mogą być stosowane do zabezpieczenia tego urządzenia.

Szyfrowanie komunikacji

Zabrzmi to co najmniej dziwnie, ale nawet we współczesnych systemach KD nie zawsze jest stosowane szyfrowanie danych przesyłanych pomiędzy kontrolerem a serwerem lub w komunikacji *peer-to-peer*.

W rozwiązaniach wspierających szyfrowanie standardem powinno być wykorzystywanie publicznych algorytmów szyfrowania (np. TLS), bo tylko one są uznawane za bezpieczne. Zabezpieczenie TLS polega na tym, iż dwa urządzenia akceptują klucze szyfrujące przed nawiązaniem komunikacji. Od momentu, gdy zaakceptują klucze, za każdym razem, kiedy konfigurują połączenie, klucze deszyfrujące znane są tylko tym dwóm urządzeniom. W związku z tym, gdy ktoś przechwyci dane zaszyfrowane przez TLS, nie będzie w stanie ich odszyfrować.

Certyfikaty i autentykacja

Istnieją sposoby weryfikacji osób, stosuje się paszporty, dokumenty tożsamości. W środowisku IT wykorzystywane jest podobne podejście w postaci cyfrowych paszportów nazywanych certyfikatami. Oznacza to, że urządzenia muszą się nawzajem sprawdzić przed rozpoczęciem szyfrowania. Tylko wtedy wiedzą, że mogą sobie nawzajem zaufać. Taką operację określamy mianem autentykacji. Jedynie po przeprowadzeniu poprawnej autentykacji urządzenia mogą zgodzić się na wymianę kluczy szyfrujących. Ponieważ komputer atakującego nie posiada ważnego certyfikatu, nie może być podłączony do kontrolera. Takie podejście rodem z branży IT jest bardzo często pomijane w systemach zabezpieczeń. A jest to jedyny sposób, aby uniemożliwić przestępcom dostęp do kontrolera.

Środowisko IT to nie wszystko

Stosując zaawansowane systemy kontroli dostępu, które zapewniają połączenia szyfrowane pomiędzy kontrolerami a serwerem w sieci LAN, należy również zwrócić uwagę na zagrożenia, jakie niosą ze sobą pozostałe elementy systemu.

Karty RFID – w czym tkwi problem?

W przypadku obiektów należących do infrastruktury krytycznej szczególną uwagę należy zwrócić na bezpieczeństwo kart dostępu, ponieważ dane w nich zapisane są bezpośrednio narażone na ataki. Niestety świadomość zagrożeń wynikających ze stosowania kart, których technologie zabezpieczania zostały dawno złamane (np. Mifare Classic), lub takich, które zapewniają podobne bezpieczeństwo, jakie daje użycie kodu QR – czyli żadne (EM Marin 125 kHz). Karty bezpieczne to takie, w których do zaszyfrowania informacji stosuje się publiczne algorytmy, np. AES-128 lub wyższy, np. Mifare Desfire Ev1 czy HID SEOS.

Podwójna autoryzacja

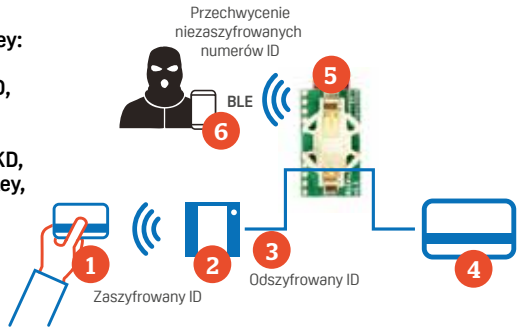
Nietrudno zgodzić się z wytycznymi dotyczącymi obiektów IK, które zostały zawarte we wspomnianym załączniku. Dobrą praktyką jest stosowanie podwójnej autoryzacji w celu wejścia do stref szczególnie chronionych. Może być ona realizowana jako *karta + pin*, *karta + cecha biometryczna*. Niektóre systemy oferują również bardziej złożone procedury, włącznie z mierzeniem masy ciała osoby wchodzącej.

Wiegand i BLEKey

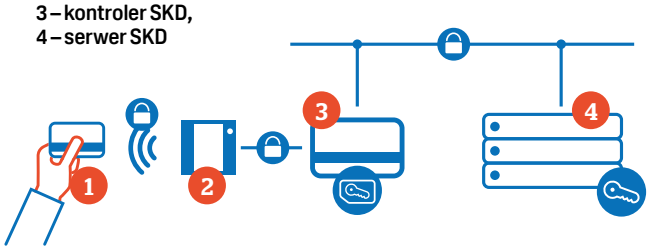
Nawet najnowocześniejsza technologia zastosowana w kontrolerach, kartach RFID czy też czytnikach nie zapewnia, że system KD chroni przed dostępem osób nieuprawnionych, jeżeli nie zostanie zabezpieczone tak słabe ogniwo, jakim jest niewątpliwie technologia rodem z lat 80. XX wieku. Mowa o interfejsie Wiegand. Jest on niezwykle popularny, ponieważ umożliwia podłączenie niemal każdego czytnika do niemal każdego kontrolera. Protokół Wiegand pozwala na przesyłanie informacji tylko w jednym kierunku, a ponadto nie zapewnia jakiegokolwiek szyfrowania transmitowanych danych.

O tym, jak niebezpieczne może być stosowanie protokołu Wiegand, przekonali się uczestnicy corocznej konferencji *Black Hat*, która odbyła się w Las Vegas w 2015 r. Architekt systemów wbudowanych (*embedded*) Eric Evenchick oraz Mark Baseggio zaprezentowali urządzenie kosztujące 35 USD, umożliwiające zhakowanie systemu SKD w około 60 s. Tym urządzeniem jest BLEkey, a jego zasada działania została pokazana na *rys. 1*. Wpięcie tego urządzenia w system zajmuje niewiele czasu, a jego wykrycie jest niemal niemożliwe. Na szczęście na rynku są rozwiązania, które umożliwiają bezpieczne przesłanie numeru ID karty do kontrolera. Przykładem może być nowy standard kodowania OSDP (*Open Supervised Device*

Rys 1. Zasada działania BLEkey:
1 – karta RFID
2 – czytnik RFID,
3 – magistrala Wiegand,
4 – kontroler SKD,
5 – moduł BLEkey,
6 – aplikacja na smartfonie



Rys. 2. Zasada działania SKD z szyfrowaniem danych:
1 – karta RFID,
2 – czytnik RFID,
3 – kontroler SKD,
4 – serwer SKD



Protocol) v2 czy też rozwiązania producenckie korzystające z interfejsu RS485 i oferujące szyfrowanie danych.

Procedury i świadomość zagrożeń. Wiedza o systemie

Wybierając system kontroli dostępu dla obiektów infrastruktury krytycznej, szczególną uwagę należy zwrócić na wszystkie podzespoły oraz zasadę działania. Jak odczytywany jest numer ID z karty, jak i gdzie jest on odszyfrowywany, następnie jak jest on przesyłany do jednostki decyzyjnej. Z punktu widzenia bezpieczeństwa system kontroli dostępu powinien zapewniać szyfrowanie danych na każdym z tych etapów (*rys. 2*).
Ważnym aspektem bezpieczeństwa danych jest miejsce przechowywania kluczy deszyfrujących. Najnowszym trendem jest lokalizowanie kluczy deszyfrujących informacje podbierane z karty RFID nie w czytniku, lecz w kontrolerze. Czytniki często są umieszczane po niezabezpieczonej stronie i mogą być celem ataku.

Instalacja, serwis

Osoby zarządzające bezpieczeństwem w obiektach IK powinny mieć pełną świadomość, kto instaluje, uruchamia, a potem serwisuje systemy zabezpieczeń, w tym system kontroli dostępu. Należy odpowiedzieć na następujące pytania:

1. Czy wiem, jaka technologia kart została użyta?
2. Czy mam świadomość, kto programuje karty dostępu?
3. Czy wiem, kto jest w posiadaniu kluczy do programowania kart?
4. Czy wszystkie urządzenia mają podłączony styk sabotażowy?
5. Czy mam świadomość, że komputer serwisanta, który jest wpinany do kontrolera/sieci w celu zmiany konfiguracji, może być źródłem cyberataku, nawet gdy jego właściciel nie jest tego świadomy?
6. Czy instalatorzy/serwisanci posiadają umiejętności i wiedzę, która pozwala im zabezpieczyć system kontroli dostępu od strony IT?
7. Czy po uruchomieniu systemu zostały zmienione hasła domyślne?
8. Kto jest w posiadaniu haseł do systemu?
9. Czy sieć LAN systemu SKD jest odizolowana od sieci biznesowej?
10. Czy firma serwisująca ma dostęp zdalny i jak go zabezpieczono?
11. Czy wiem, z jakimi systemami łączy się system kontroli dostępu, po jakich protokołach, jakie dane są wymieniane?
12. Czy tworzona jest kopia zapasowa systemu, bazy danych, konfiguracji?
13. Czy była dokonywana próba odtworzenia systemu z kopii?

Okazuje się bowiem, że po zakończonych odbiorach i wdrożeniu systemu w życie systemy budynkowe pozostają „wystawione na świat". Na taki scenariusz czekają osoby o niecnych zamiarach.
Bill Rios, *Director of Threat Intelligence* w firmie Qualys, za pomocą prezentacji *Owning a Building* uświadomił innym, że zhakowanie systemów budynkowych nie jest trudne. Zademonstrował sposób „włamania" do systemu BMS jednej z aren w Soczi, wykorzystując otwarte porty i serwisy oraz używając haseł domyślnych, by móc przeglądać dane, a nawet sterować systemem.

Automatyzacja – eliminacja błędu ludzkiego

Wdrażając automatyzacje procesów w systemach kontroli dostępu, można zniwelować błąd człowieka. Wyobraźmy sobie sytuację, w której połączenie wyżej wymienionego systemu z systemem kadrowym umożliwia automatyczne nadawanie uprawnień w zależności od departamentu, w którym dana osoba ma pracować. Dostanie ona tylko takie uprawnienia, jakie są jej niezbędne, a gdy zostanie zwolniona, jej karta zostanie zablokowana. Innym przykładem, gdy błąd ludzki może odgrywać ważną rolę w bezpieczeństwie obiektu, jest zgłoszenie przez pracownika zgubienia karty. Osoba przyjmująca taką informację wystawia kartę zastępczą, ale powinna również zablokować kartę zgubioną. System powinien robić to automatycznie.

Aktualizacja

Jak dowodzą liczne sytuacje w ostatnich latach, w większości ataków na infrastrukturę krytyczną wykorzystano luki w oprogramowaniu. Dotyczy to zarówno systemów operacyjnych, jak i aplikacji, np. kontroli dostępu. Dlatego też przy wyborze systemu kontroli dostępu należy brać pod uwagę to, jak często są wydawane aktualizacje aplikacji.

Bezpieczeństwo w IK

System kontroli dostępu bierze bezpośredni udział w podejmowaniu decyzji o przebywaniu uprawnionych osób w danych strefach infrastruktury krytycznej. Z tego względu bardzo ważny jest system i jego funkcje, a także poziom zapewnianego bezpieczeństwa oraz to, czy jest przygotowany do przeprowadzania aktualizacji.

BIO

Błażej Ożga W branży security od ponad 13. lat, nie tylko jako specjalista, lecz również jako autor kilku innowacyjnych rozwiązań. W firmie Nedap Security Management odpowiedzialny za budowanie kanału wsparcia dla projektantów, architektów i konsultantów.

Przemysł naftowy i gazowy: wymogi bezpieczeństwa wciąż rosną

Przemysł naftowy i gazowy należy do branż dysponujących największą infrastrukturą krytyczną. To także jeden z kluczowych sektorów światowej gospodarki. Nic dziwnego, że jego bezpieczeństwo i ochrona zarówno przed atakami fizycznymi, jak i cyberzagrożeniami ma tak duże znaczenie.

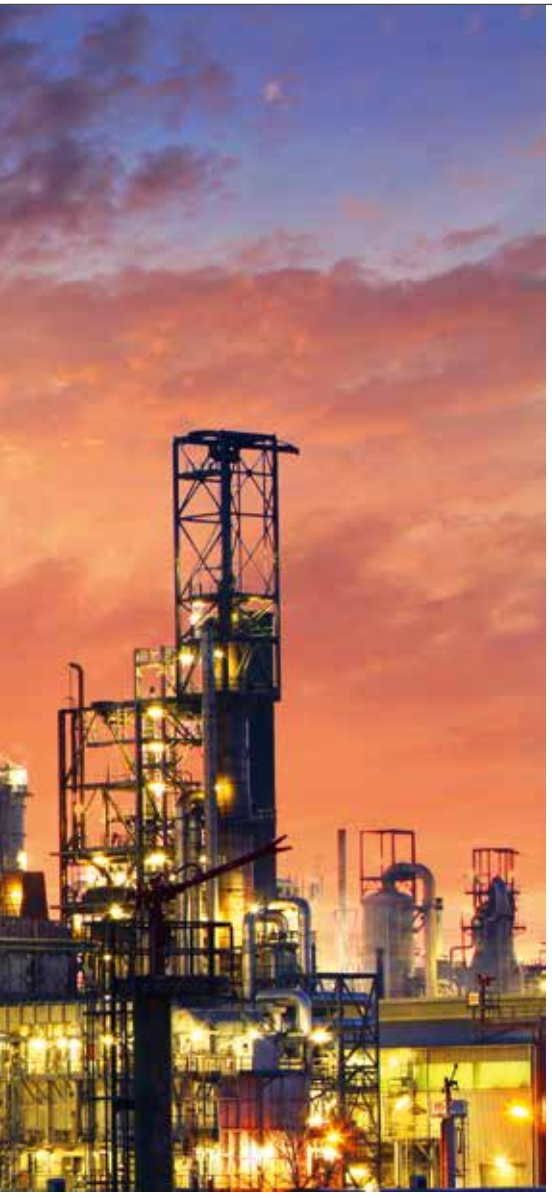
Eifeh Strom
a&s International

Czasy nie sprzyjają branży naftowej i gazowej. Od załamania cen ropy w 2014 r. światowy sektor O&G (*Oil and Gas*) stara się ograniczać koszty operacyjne, a jednocześnie zwiększać wydajność i efektywność. Musi jednak pamiętać o coraz ostrzejszych wymogach związanych z bezpieczeństwem. Choć niełatwo zwiększać wydatki na ochronę, gdy marże spadają i trzeba ciąć koszty, to niedawne cyberataki i ataki terrorystyczne wymierzone w globalną infrastrukturę O&G pokazały, że branża potrzebuje silniejszej ochrony zarówno fizycznej, jak i informatycznej.

RYNEK ROŚNIE

Według analityków z Markets and Markets do 2020 r. wartość globalnego rynku security oraz usług związanych z branżą naftową i gazową ma osiągnąć 33,9 mld USD, przy rocznej stopie wzrostu w latach 2015–2020 szacowanej na 5,2 proc.

33,9
mld USD



CYBERATAKI

Przemysł naftowy i gazowy musi zabezpieczyć się przed cyberatakami i poradzić sobie z ryzykiem wynikającym z cyfrowej transformacji.

Trudna sytuacja na rynku

W obszarze bezpieczeństwa branży O&G w ostatnich latach zaszły duże zmiany. Według Boba Fryklunda, analityka z IHS Markit Energy, są one wynikiem ewolucji tego sektora w następstwie globalizacji biznesu oraz cyfryzacji. Bezpieczeństwo wciąż opiera się na pięciu podstawowych elementach: operacyjnym, finansowym, środowiskowym, ludzkim i informacyjnym. Problemy stały się jednak bardziej rozległe i połączone. W obszarze ryzyka operacyjnego można obecnie wyróżnić komponenty związane z cyberbezpieczeństwem i urządzeniami przemysłowymi, obiektami produkcyjnymi, firmami zewnętrznymi, środowiskiem i pracownikami. Mamy więc do czynienia ze znacznym wzrostem skali ryzyka i odpowiedzialności.

Większość sytuacji zagrażających bezpieczeństwu była następstwem wtargnięć albo ataków terrorystycznych, do których dochodziło lokalnie lub w odległych lokalizacjach. Większa potrzeba ochrony wynikała więc z bezpośredniej reakcji na te działania i przekonania, że zabezpieczenia muszą zostać wzmocnione – tłumaczy David Montague, dyrektor sprzedaży w dziale bezpieczeństwa firmy FLIR Systems, odpowiedzialny za region EMEA.

Z kolei Derek Tan, dyrektor ds. technologii zabezpieczeń w firmie Johnson Controls, odpowiedzialny za region APAC (region Azji i Pacyfiku), uważa, że choć globalny rynek rośnie, to jego wzrost jest ograniczany przez nowe regulacje, polityczne zawirowania i niestabilną sytuację na Bliskim Wschodzie, a także rozwój alternatywnych źródeł energii oraz niedostosowanie starszych technologii do obecnych potrzeb i wyzwań operacyjnych.

Ameryka Północna liderem

Analitycy z firmy badawczej Markets and Markets szacują, że największe udziały w rynku zabezpieczeń sektora O&G ma Ameryka Północna, ale największą roczną stopę wzrostu w latach 2015–2020 osiągną kraje Ameryki Łacińskiej.

Rynek w Ameryce Północnej rozwinął się wraz ze wzrostem eksploracji ropy naftowej i gazu na tym kontynencie w ostatnich kilku latach. *W ubiegłej dekadzie wzrosła tam liczba odwiertów na morzu i lądzie oraz rurociągów, a amerykańska ropa wniosła największy procentowy wkład do światowych źródeł energii* – twierdzi Rob Borsch, przewodzący zespołowi Oil and Gas Practices w firmie Genetec. Pod względem technologicznym firmy branży O&G Ameryki Północnej przewodzą we wdrażaniu rozwiązań chmurowych i mobilnych.

Większe potrzeby na Bliskim Wschodzie i w Afryce

Pomimo politycznej i lokalnej niestabilności w regionie MEA (*Middle East and Africa*) firmy branży security odnotowują wzrost popytu w tamtejszych krajach, m.in. w Iraku. *Gdy skończyły się problemy i rośnie zaufanie, zwiększają się inwestycje. Obserwujemy wzrost zainteresowania naszymi rozwiązaniami w tym regionie* – twierdzi D. Montague z FLIR Systems. Zwraca przy tym uwagę na ożywienie rynku w Afryce, związane z morskimi platformami wiertniczymi. Platformom wiertniczym w Afryce zagrażają przede wszystkim piraci. *W przypadku platform najczęściej spotykamy się z pytaniami klientów o radary. Odnotowujemy zapotrzebowanie na detekcję obejmującą większy obszar – radary i kamery termowizyjne dalekiego zasięgu. Dzięki nim mogą być wykrywani ludzie zbliżający się do platformy w niewielkich łodziach, a tak działają piraci* – dodaje D. Montague.

Dzięki zdolności do integrowania różnych systemów i czujników platformy PSIM (*Physical Security Information Management*) oraz VMS (*Video Management Systems*) nieustannie cieszą się dużym zainteresowaniem sektora O&G.

PSIM i VMS przenikają się, gdy chodzi o ich funkcjonalności, skupiając się na obrazie (świadomości sytuacyjnej) i zarządzaniu incydentami w obiektach infrastruktury krytycznej. Zapotrzebowanie klientów wymusi też zwiększenie zasięgu integracji PSIM i VMS o systemy DCS i SCADA – twierdzi Andrea Sorri, dyrektor ds. rozwoju biznesu w Axis Communications.

Korzyści z zastosowania zaawansowanego rozwiązania VMS/PSIM przedstawia też Erez Goldstein, dyrektor marketingu w Qognify. *Pewna firma, zanim zdecydowała się na zastosowanie rozwiązania VMS/PSIM, wydawała rocznie 8 mln USD na zabezpieczanie swoich rozległych lokalizacji, w tym magazynów, węzłów transportowych, centrów logistycznych, zakładów produkcyjnych, biur i ośrodków szkoleniowych. Dzięki przeniesieniu zadań wcześniej wykonywanych przez lokalnych pracowników ochrony do globalnego centrum bezpieczeństwa GSOC (Global Security Operations Center) firmie udało się ograniczyć koszty o 15 proc.*

Wymogi bezpieczeństwa

Zagrożenia w branży O&G wciąż rosną. Sprawą kluczową staje się zapewnienie, by zabezpieczenia były stale aktualizowane i chroniły przed wszystkimi możliwymi incydentami. Jednak z powodu malejących zysków i coraz większych wyzwań rynkowych budżety, jakimi dysponują działy bezpieczeństwa, mogą być niewystarczające. *Specjaliści ds. bezpieczeństwa muszą kłaść większy nacisk na wykorzystanie posiadanych zasobów niż na budowę nowych systemów* – twierdzi Paul Barker, konsultant w zajmującej się bezpieczeństwem brytyjskiej firmie doradczej Linx International Group. *– Dlatego firmy automatycznie nie będą się pozbywać starszych technologii zabezpieczeń, tylko szukać sposobów na integrowanie ich z nowszymi systemami wszędzie tam, gdzie jest to możliwe.*
Podobnie uważa Andrea Sorri z Axis Communications. *Gdy rynek ewoluuje, obserwujemy łączenie tradycyjnych zabezpieczeń z rozwiązaniami bezpieczeństwa i ochrony środowiska pracy. Praktycznie polega to na integrowaniu nowych urządzeń z dotychczas wykorzystywanymi platformami. Dzięki temu możliwe stają się zdalne działanie, testowanie, nieprzerwana produkcja i rozszerzony dozór z jednego centrum kontroli* – wyjaśnia. Kluczową sprawą staje się zrozumienie całego środowiskowego otoczenia. Przykładowo, dużą rolę odgrywa poznanie rzeczywistych problemów występujących w danej lokalizacji, ostatnich incydentów, a także posunięć udziałowców, partnerów i konkurentów firmy w celu określenia i ograniczenia bieżących zagrożeń.

Konieczne jest także zabezpieczenie pojazdów i rurociągów, którymi transportowane są ropa i gaz, przed różnej natury zagrożeniami na lądzie, w powietrzu czy na morzu. Instalacje naftowe i gazowe, w szczególności rurociągi biegnące przez wielkie obszary, są narażone na ataki terrorystyczne, akty sabotażu i kradzieże. Infrastruktura naftowa i gazowa może także stać się celem prób sabotażu będącego formą protestu. Dlatego coraz ważniejsze jest monitorowanie rozległych terenów infrastruktury krytycznej, takiej jak rurociągi.

Dostęp do obiektów jest najczęściej nadzorowany przez systemy dozoru wizyjnego i operatorów, na znaczeniu zyskują także integracja i automatyzacja kontroli dostępu.

W poszukiwaniu rozwiązań

Wykorzystanie systemów dozoru wizyjnego w branży O&G przez lata ewoluowało. Zastosowanie zautomatyzowanej analizy wizyjnej, wdrożenia czujników Internetu Rzeczy (IoT) do monitorowania rurociągów oraz centra dozoru, z których można zarządzać wieloma systemami zabezpieczeń obejmującymi wielkie obszary geograficzne – to rozwiązania poszukiwane dziś przez przemysł naftowy i gazowy.
Kluczowym elementem każdego systemu dozoru wizyjnego są kamery. W branży O&G powszechnie wykorzystuje się kamery działające w świetle widzialnym i termowizyjne – zarówno do monitorowania, jak i ochrony obwodowej (perymetrycznej). Rośnie też znaczenie innych technologii, takich jak radary dalekiego zasięgu. *W przypadku lądowych instalacji O&G rozwiązania muszą mieć duży zasięg, by pracować na coraz większym obszarze. Wcześniej stosowaliśmy czujki ochrony obwodowej, ale obecnie jest zapotrzebowanie na detekcję dalekiego zasięgu* – twierdzi D. Montague. *– Oczekuje się też, że jeśli jakiś obiekt zostanie wykryty, to następnie będzie obserwowany. W momencie wyzwolenia alarmu musimy więc zapewnić skierowanie na ten obiekt kamery PTZ i dalsze jego śledzenie.*
Dużym zainteresowaniem branży O&G cieszy się nowej generacji analiza wizyjna w czasie rzeczywistym, która wykorzystuje sztuczną inteligencję i technologię *deep learning*. W ciągu kilku sekund umożliwia ona lokalizowanie i monitorowanie miejsca pobytu osoby (i jej wcześniejszych lokalizacji) przy użyciu inteligentnego i automatycznego przeszukiwania całej sieci dozoru wizyjnego. Okazuje się to przydatne w zarządzaniu zdarzeniami *na żywo*, stanowiąc jednocześnie dużą pomoc w dochodzeniach prowadzonych po wystąpieniu incydentu.

Rewizja kontroli dostępu

Wiele firm z branży O&G modernizuje swoje systemy kontroli dostępu, zastępując urządzenia analogowe rozwiązaniami wykorzystującymi protokół IP.
Rob Borsch wskazuje na konieczność stosowania rozwiązań kontroli dostępu zgodnych z programem TWIC. *Program TWIC (Transportation Worker Identification Credential) umożliwia posługiwanie się odpornymi na manipulacje biometryczne danymi*

DRONY DOZORUJĄ INFRASTRUKTURĘ KRYTYCZNĄ

Drony są wykorzystywane do monitorowania rurociągów naftowych i gazowych, zapewniając ich operatorom widok *z lotu ptaka* na rozległe obszary.

Drony to dość kontrowersyjne narzędzie ochrony. Są uważane za rozwiązanie o ogromnym potencjale, ale też postrzegane jako zagrożenie zewnętrzne.
Coraz więcej jest doniesień o obcych dronach krążących nad rafineriami, obiektami produkcyjnymi i magazynowymi, dlatego firmy z branży O&G powinny mieć możliwość identyfikowania tego rodzaju zewnętrznego zagrożenia i reagowania na nie.
Rośnie jednocześnie potrzeba wykorzystania dronów do ochrony i monitorowania rurociągów naftowych i gazowych. Bardzo trudnym zadaniem jest zabezpieczenie rozległych obiektów przy użyciu kamer stacjonarnych, które zawsze są narażone na atak – napastnicy mogą łatwo zniszczyć tego rodzaju sprzęt. Dlatego obserwuje się coraz większe zainteresowanie użyciem dronów do monitorowania rurociągów, ich automatycznym wysyłaniem, sprowadzaniem z powrotem do stacji, a także uzyskiwaniem raportów z akcji.
Wykorzystanie dronów może jednak stać się problematyczne. Coraz więcej jest przeciwników wykorzystania dronów do patrolowania rurociągów i granic obiektów. Rośnie przy tym presja na prawne ograniczenie powszechnego użycia dronów.

uwierzytelniającymi, np. przez pracowników pracujących na morzu, którzy muszą mieć dostęp (bez eskorty) do stref zastrzeżonych lub niebezpiecznych. Program ma kluczowe znaczenie z punktu widzenia rozproszonych i rozległych instalacji naftowych oraz gazowych, a także ze względu na wyjątkowo rygorystyczne standardy zarządzania dostępem – wyjaśnia przedstawiciel Genetec.

Dostęp do obiektów O&G jest najczęściej nadzorowany przez systemy dozoru wizyjnego i operatorów, na znaczeniu zyskują także integracja i automatyzacja kontroli dostępu. Automatyzacja ogranicza manualną pracę związaną z zarządzaniem dostępem do lokalizacji, można też zdalnie zarządzać dostępem, w ten sposób ograniczając liczbę potrzebnych operatorów.

Wyraźnym trendem jest rosnące wykorzystanie technologii LPR (*Licence Plate Recognition*) – identyfikacji tablic rejestracyjnych do zarządzania dostępem do bram wjazdowych. Możliwość odczytywania numerów rejestracyjnych pojazdu, sprawdzenia jego uprawnień w bazie danych, a następnie przydzielenie prawa do wjazdu automatyzuje zarządzanie dostępem.

Jak sobie radzić z cyberzagrożeniami

Cyberzagrożenia to nie żarty – hakerzy potrafią przejmować kontrolę nad krytycznymi systemami, a ich celem stają się nie tylko dane. Niedawne cyberataki na struktury państwowe i organizacje, których celem były zarówno systemy SCADA, jak i IT, pokazały, jak groźne mogą być ich konsekwencje. Prawdopodobieństwo przełamania zabezpieczeń systemów, które może prowadzić do bardzo poważnych awarii, jest coraz większe. Ryzyko rośnie wraz ze wzrostem konwergencji systemów zabezpieczeń i IT, które mogą być podatne na ataki z powodu ludzkich błędów, wykorzystywania przestarzałych systemów oraz urządzeń mobilnych, takich jak tablety i smartfony.

Problem cyberzagrożeń jest tym większy, im większa jest automatyzacja i liczba danych operacyjnych przesyłanych przez Internet – a w ten sposób jest obecnie przesyłana większość danych produkcyjnych w branży O&G, m.in. w rafineriach i zakładach chemicznych dane operacyjne są wysyłane przez Internet. Możliwość zdalnego dostępu zwiększa więc ryzyko wystąpienia zakłóceń, wyłączenia zasilania lub przerwania komunikacji.

Branża O&G stoi zatem przed koniecznością ochrony przed cyberatakami i ryzykiem, jakie niesie transformacja cyfrowa. Amerykański NIST (*National Institute of Standards and Technology*) opracował zalecenia dotyczące zwiększenia cyberbezpieczeństwa infrastruktury krytycznej. Jest to zestaw standardów i najlepszych praktyk mających pomóc operatorom infrastruktury krytycznej w radzeniu sobie z ryzykiem cyberzagrożeń. Zalecenia te ułatwiają firmom wdrażanie najlepszych praktyk zarządzania ryzykiem i tworzenie indywidualnych wytycznych dotyczących cyberbezpieczeństwa.

Z punktu widzenia zabezpieczeń technicznych, np. kamer sieciowych – jeśli nie są odpowiednio zabezpieczone, tworzą lukę w systemie ochrony. *Zhakowane kamery sieciowe mogą umożliwiać przeprowadzanie ataków typu DDoS, których celem stają się aplikacje oraz usługi bezpieczeństwa* – przestrzega Andrea Sorri. – *Ważna jest więc współpraca z takim dostawcą, który zapewnia wsparcie na każdym poziomie. Cyberbezpieczeństwo powinno być w centrum wszelkich działań – konieczne są rygorystyczne wymogi dla produktów i współpraca z partnerami w zakresie przeciwdziałania zagrożeniom.*

Bezpieczeństwo to konieczność

Zapewnienie bezpieczeństwa infrastruktury w branży O&G jest niezbędne do prawidłowego jej funkcjonowania. Właściwe podejście wymaga nie tylko zastosowania najnowszych urządzeń i aktualizacji oprogramowania, ale także wprowadzenia w życie najlepszych praktyk. Samo zaprojektowanie i wdrożenie systemu dozoru wizyjnego jeszcze nie gwarantuje sukcesu. Ważny jest cały proces zarządzania zmianami, który obejmuje szkolenia, bieżące wsparcie użytkowników przez dostawcę oraz okresowe kontrole aplikacji.

Jedynie stosując najlepsze praktyki, firmy z branży O&G mogą sprawić, by ich systemy bezpieczeństwa były przygotowane i odporne na zagrożenia nie tylko obecne, ale także przyszłe.

a&S POLSKA

ŚNIADANIE EKSPERTÓW

Bezpieczeństwo infrastruktury krytycznej

dyskusja o bezpieczeństwie w luźnej atmosferze

ZAPRASZAMY PRZEDSTAWICIELI:

- security managerów obiektów infrastruktury krytycznej
- security managerów obiektów przemysłowych
- przedstawicieli firm i instytucji o strategicznym znaczeniu dla funkcjonowania państwa:
  m.in. zaopatrzenia w energię, surowce energetyczne i paliwa, łączności, sieci teleinformatycznych, finansowych, ochrony zdrowia, transportowych, ratowniczych oraz produkcji, składowania i stosowania substancji niebezpiecznych

Hotel Westin Warszawa
25 maja 2018 r.
godz. 9.00-12.00

Uczestnictwo w śniadaniu jest **bezpłatne!**

Rejestracja: www.aspolska.pl/sniadanie

organizator: a&S POLSKA

partnerzy: AXIS COMMUNICATIONS, BCS, dahua TECHNOLOGY, HIKVISION, Linc Polska Sp. z o.o., SCHRACK SECONET

Głos branży

Infrastruktura krytyczna wymaga krytycznych zabezpieczeń. Systemy security w takich zastosowaniach muszą spełniać najwyższe wymogi bezpieczeństwa.

Nowe technologie do ochrony infrastruktury krytycznej

Tomasz Goljaszewski
Project Engineer,
Hikvision Poland

Nakłady na ochronę infrastruktury krytycznej w Polsce są ciągle relatywnie niskie. W okresie gorszej koniunktury gospodarczej namnożyły się wieloletnie zaniechania i pozorne oszczędności, które obniżyły poziom bezpieczeństwa tych obiektów. Luki w technicznych systemach zabezpieczeń łatano ochroną fizyczną, ale ta, pozbawiona dobrych narzędzi wczesnego wykrywania zagrożenia i systemu powiadamiania, nie jest w stanie skutecznie i odpowiednio szybko reagować. Na szczęście wraz ze wzrostem świadomości zagrożeń coraz częściej mówi się o podniesieniu poziomu bezpieczeństwa obiektów infrastruktury krytycznej.

System CCTV jest kluczowym elementem systemu zabezpieczeń ważnych obiektów. Rozwój w sektorze dozoru wizyjnego odpowiada na rosnące oczekiwania dotyczące zwiększenia poziomu bezpieczeństwa.

Firma Hikvision w ciągu kilku ostatnich lat rozwinęła dwie unikalne technologie związane z jakością obserwacji w nocy: *DarkFighter* opartą na dużych przetwornikach o specjalnej światłoczułej konstrukcji oraz *DarkFighterX* opartą na rozwiązaniu dwusensorowym (jeden przetwornik odpowiada wyłącznie za rozpoznanie kształtów, a drugi za rozpoznanie koloru). Obie technologie zostały opracowane pod kątem zapewnienia bardzo dobrego obrazu w warunkach nocnych przy minimalnym poziomie oświetlenia (np. światło gwiazd), przy czym technologia *DarkFighterX* koncentruje się na odwzorowaniu obrazu w kolorze. Nowością są kamery 4 Mpix i 8 Mpix w technologii *DarkFighter*.

W ochronie obiektów infrastruktury krytycznej sprawdzą się też kamery termowizyjne oraz zaawansowana analiza obrazu. Hikvision oferuje pełną gamę kamer termowizyjnych w rozdzielczości CIF, 4CIF oraz 1 Mpix poprzez cyfrowe przeskalowanie. Mają prędkość wyświetlania do 50 kl./s, co jest bardzo istotne dla skuteczności działania algorytmów analizy treści obrazu. Pod koniec ub.r. firma opracowała też nowe oprogramowanie (*firmware*) do kamer termowizyjnych, które automatycznie rozpoznaje w obrazie źródło pożaru, a także wejście człowieka, zwierzęcia i pojazdu w chronioną strefę. Skutecznie podnosi to wykrywalność niebezpiecznych zdarzeń i ogranicza lub eliminuje liczbę fałszywych alarmów. Jest to możliwe dzięki nowej technologii *deep learning*, opartej na uczeniu i tworzeniu wielu wzorców rozpoznawanych obiektów czy zdarzeń. Technologia ta została zaimplementowana w nowych kamerach linii 7 oraz w systemach rejestracji Hikvision. Urządzenia te posiadają algorytmy pod kątem ochrony perymetrycznej i potrafią filtrować alarmy po wykryciu człowieka czy pojazdu. Istotne, że detekcja człowieka nie wynika z określenia wielkości obiektu czy prędkości poruszania się, co jest najczęściej spotykane i mało skuteczne, ale właśnie poprzez rozpoznawanie wzorca.

Hikvision opracował również nową, profesjonalną platformę klient-serwer *HikCentral*. Może ona skutecznie scentralizować w jeden system wszystkie obiekty infrastruktury krytycznej na bardzo dużym obszarze – umożliwia zarządzanie niemal nieograniczoną liczbą systemów lokalnych.

Infrastruktura krytyczna – bezpieczeństwo nie tylko państwa

Marcin Morzyk
BCS

Infrastruktura krytyczna w rozumieniu ogólnym to systemy powiązane ze sobą oraz wchodzące w ich skład obiekty. Rozumienie infrastruktury krytycznej może być różne w zależności od funkcjonalności i przeznaczenia obiektów, systemów czy urządzeń. Dla funkcjonowania państwa będzie to kilkanaście sektorów takich jak energia, woda, banki i finanse, telekomunikacja, transport itp. Przygotowanie zabezpieczeń dla każdego z tych sektorów jest różne i wymaga zróżnicowanych urządzeń, które powinny być zintegrowane w jeden system bezpieczeństwa np. dla jednego typu obiektów. Firmy prywatne, które nie są kluczowe w rozumieniu funkcjonowania państwa mają własną infrastrukturę krytyczną dla funkcjonowania ich działalności, którą również należy zabezpieczać zgodnie z ich wymogami.
Systemy monitoringu wizyjnego idealnie wpisują się w zabezpieczanie praktycznie wszystkich obiektów infrastruktury krytycznej zarówno państwowej, jak i prywatnej. Jednym z najważniejszych systemów dla funkcjonowania państwa jest energetyka. Dobrym przykładem mogą być elektrownie lub elektrociepłownie, gdzie wykorzystanie kamer termowizyjnych BCS pozwala zabezpieczyć obiekt przed ewentualnym wtargnięciem na teren z dużej odległości. Zabezpieczenie kamerami termowizyjnymi zwiększa pewność wykrycia intruza oraz dodatkowo może działać prewencyjnie, informując użytkownika systemu o wzroście temperatury powyżej zadanej wartości w krytycznych elementach systemu przesyłu produkowanej energii.
Zabezpieczanie infrastruktury krytycznej prywatnych obiektów może być wspomagane inteligentną analizą obrazu zaimplementowaną w kamerach. Przykładem może być zakład produkcyjny, gdzie na drogach komunikacyjnych można poruszać się tylko w wyznaczonym kierunku, a jakiekolwiek odstępstwa mają być komunikowane jako alarm do ochrony czy też innych osób odpowiedzialnych za bezpieczeństwo. Korzystanie z inteligentnej analizy i dobra konfiguracja na obiekcie pozwoli zminimalizować czas reakcji na zaistniałe zdarzenia, a w przypadku dużej liczby kamer zapewni znaczną skuteczność.
Głównym wyznacznikiem dla ochrony państwowych obiektów infrastruktury krytycznej (i nie tylko) realizowanej przy pomocy systemów telewizji dozorowej powinna być jakość i funkcjonalność urządzeń. Wybór rozwiązań BCS, oprócz jakości i funkcjonalności daje również szerokie spektrum asortymentu i wsparcie przy uruchomieniu systemu, co niejednokrotnie jest ważnym elementem przy dokonywaniu wyboru dostawcy urządzeń.

Chroń firmę przed cyberatakami!

Agnieszka Gołędowska
Junior Product Manager,
Dahua Technology Poland

Możliwość wyszukania, przesłania i odbioru informacji z niemal każdego miejsca sprawia, że przedsiębiorstwa, poszukując nowych rozwiązań, które zautomatyzują ich pracę, coraz częściej przenoszą swój biznes do sieci. Dlatego ochrona cyberprzestrzeni jest ostatnio jednym z głównych tematów podejmowanych zarówno przez wielkie, jak i małe firmy.

Cyberataki stanowią coraz większe zagrożenie dla wszystkich. Inwestycje w technologię i innowacyjne produkty umożliwiające wzrost i rozwój firmy niestety narażają ją także na większe ryzyko ataku i wycieku danych. Każdy taki atak wiąże się ze stratą finansową przedsiębiorstwa i osłabieniem marki na rynku.

Według raportu PwC Polska 70% incydentów[1] jest wynikiem działania pracowników, dlatego warto prowadzić szkolenia i uświadamiać o roli i skutkach ich działań. Firmy, mając świadomość zagrożenia, inwestują także w systemy monitoringu wizyjnego i kontroli dostępu, zwiększając w ten sposob swoje szanse w walce z cyberatakami.
Aby stworzyć bardziej bezpieczne miejsce pracy Dahua Technology na każdym szkoleniu przypomina, żeby nigdy nie używać domyślnego hasła, tylko tworzyć własne i zmieniać je cyklicznie. Najsilniejsze hasła powinny zawierać co najmniej 8 znaków wraz z kombinacją znaków specjalnych, cyfr, małych i wielkich liter.
Co więcej, aktualizacja oprogramowania zapewni nie

[1] PwC Polska, raport ze stycznia 2016 r. *www.pwc.pl/badaniebezpieczenstwa*

Zarządzanie bezpieczeństwem pożarowym w obiektach infrastruktury krytycznej

Krzysztof Kunecki
dyrektor ds. technicznych, Schrack Seconet Polska

Zapewnienie najwyższego poziomu bezpieczeństwa pożarowego w każdym zabezpieczanym obiekcie, a szczególnie w obiektach infrastruktury krytycznej, takich jak elektrownia, wymaga przede wszystkim przeprowadzenia szczegółowej analizy i identyfikacji potencjalnych źródeł zagrożeń powstałych w wyniku pożaru i oceny ich wpływu na newralgiczne zasoby i procesy obiektu istotne z punktu widzenia zapewnienia ciągłości działania całej organizacji.
Wyniki przeprowadzonej analizy funkcjonowania obiektu z uwzględnieniem potencjalnie najgorszych scenariuszy rozwoju pożaru jednoznacznie wskazują na ogromną rolę nie tylko urządzeń przeciwpożarowych w zakresie detekcji i zwalczania (ograniczania) pożaru. Ale także pokazują, jak istotne jest odpowiednie zarządzanie obiektem w zakresie koordynacji działań po stronie służb ochrony i personelu odpowiedzialnego za cykl produkcyjny. W takiej sytuacji nieodzowne jest zastosowanie dedykowanego systemu do zarządzania bezpieczeństwem pożarowym, aktywnie wspomagającego użytkownika w zakresie zarządzania bezpieczeństwem ludzi i mienia dzięki centralnej wizualizacji, sterowaniu, integracji systemów i urządzeń przeciwpożarowych oraz wszystkich innych instalacji mających wpływ na bezpieczeństwo pożarowe obiektu.
W przypadku sytuacji kryzysowej, jaką jest alarm pożarowy, wszystkie najważniejsze informacje o stanach pracy zintegrowanych urządzeń są błyskawicznie przesyłane i przetwarzane na poziomie platformy zarządzającej systemem oraz przedstawiane operatorowi – za pomocą graficznego interfejsu użytkownika – na planach obiektowych lub schematach instalacji produkcyjnych.
Co najważniejsze, system dodatkowo wyświetla instrukcje postępowania dla użytkownika, wskazując niezbędne czynności do wykonania. Treść instrukcji/procedur postępowania może być indywidulanie dostosowywana dla konkretnego operatora systemu odpowiedzialnego za dany proces produkcyjny, aby tym samym zapewnić skoordynowane działanie personelu technicznego w zagrożonych miejscach obiektu.
Wspomagany przez system personel techniczny może szybko zidentyfikować zagrożenie, a wykonując właściwe operacje, znacznie ograniczyć ewentualne straty w obiekcie.
Podsumowując, zintegrowany system zarządzania bezpieczeństwem pożarowym może znacznie podnieść poziom bezpieczeństwa pożarowego obiektu. Aby to osiągnąć, wymagana jest ścisła współpraca użytkownika z instalatorem/producentem – począwszy od etapu tworzenia koncepcji i projektu, poprzez wdrożenie, a skończywszy na eksploatacji systemu.

---

tylko dodatkowe funkcjonalności, ale także nowsze rozwiązania zabezpieczenia sprzętu przed atakami. Zmiana portów domyślnych pozwoli uniknąć włamania do sieci i możliwości zdalnego podglądu kanałów wideo. Stosując bezpieczny protokół https ze sprawdzonym certyfikatem bezpieczeństwa ssl i poprawnie skonfigurowany serwer www, zaszyfrujemy komunikację między urządzeniami. Uchroni to sieć przed przechwyceniem wrażliwych danych.

Jeśli podejrzewasz, że ktoś uzyskał nieautoryzowany dostęp do twojego systemu, możesz sprawdzić dziennik systemowy pokaże, które adresy IP zostały użyte podczas logowania do twojego systemu i do czego uzyskano dostęp.

Firma, która nie chce czekać na atak, tylko bierze sprawy w swoje ręce, może liczyć na pomoc pentesterów.
Czym jest test penetracyjny i dlaczego warto go przeprowadzić w przedsiębiorstwie? Jest to kontrolowany proces, którego celem jest atak na systemy teleinformatyczne i praktyczną ocenę bieżącego stanu jego bezpieczeństwa. Test pozwala sprawdzić i ujawnić podatności i odporności na próby przełamania zabezpieczeń. Zidentyfikuje niebezpieczeństwo i wesprze w procesie tworzenia odpowiednich zabezpieczeń udostępnionych aplikacji i usług, chroniąc przed niepożądanym dostępem czy przerwaniem ich poprawnego funkcjonowania.

Pracując w Dahua Technology, mamy świadomość, że współpraca z profesjonalistami z całego świata jest dobrym sposobem na poprawę wykrywania luk w zabezpieczeniach. W tym celu powstało *Dahua Cybersecurity Center* (DHCC), którego zadaniem jest rozwiązywanie problemów i zapewnienie jak najlepszej ochrony dla naszych rozwiązań.

Jak każda technologia sieciowa, systemy dozoru wizyjnego są również narażone na cyberataki. Nawet najlepsze urządzenia nie będą w stanie uchronić sieci przed atakami, jeśli nie zabezpieczymy jej odpowiednim firewallem, a na styku produkt-sieć nie będzie użytkownika świadomego zagrożeń i skutków, jakie niosą cyberataki.

Firma Dahua Technology cały czas prowadzi badania i podejmuje walkę z hakerami, aby każdy jej produkt miał solidną barierę przed cyberatakami.
Zapraszamy czytelników do odwiedzenia naszej strony, gdzie dokładnie opisujemy działania i radzimy, w jaki sposób uchronić sieć przed cyberatakami.

Zapewnienie ciągłości działania jest kluczowe

Bogumił Szymanek
Inside Sales Manager Poland and Baltics, Axis Communications

Kiedy odpowiadasz za obiekt o kluczowym znaczeniu, musisz być przygotowany na różnorodne zagrożenia i problemy. Zaburzenia ciągłości procesów technologicznych i zagrożenia bezpieczeństwa mogą być wywołane wieloma czynnikami, takimi jak wypadki, kradzieże, akty terroryzmu czy klęski żywiołowe. Rozwiązania firmy Axis z zakresu sieciowych systemów dozoru wizyjnego z takimi wyzwaniami sobie radzą i zapewniają bezproblemowe funkcjonowanie obiektu.
System ochrony obwodowej służy do wykrywania potencjalnych i rzeczywistych zagrożeń związanych z wtargnięciem intruza na teren chroniony i umożliwia szybkie działanie w sytuacji rzeczywistego zagrożenia.
Rozwiązania firmy Axis przeznaczone do ochrony obwodowej opierają się na kamerach termowizyjnych z wbudowanym oprogramowaniem do analizy obrazu. Ich zaletą jest to, że „widzą" także w zupełnej ciemności i automatycznie wysyłają alarm, gdy ktoś wejdzie na określony obszar w polu widzenia kamery. Detekcja podejrzanych zachowań jeszcze przed wtargnięciem intruza na teren oraz wizyjne potwierdzenie (weryfikacja) zdarzeń umożliwia wczesne podjęcie odpowiednich czynności.
Rozwiązanie można łatwo zintegrować z innymi kamerami IP, reflektorami, głośnikami i istniejącymi systemami zabezpieczeń, zapewniając optymalne działanie systemu.
Tym, co wyróżnia rozwiązania Axis, jest analiza treści obrazu, usprawniająca działanie całego systemu ochrony. *AXIS Perimeter Defender* to wszechstronna, skalowalna aplikacja analityczna – obraz jest analizowany w czasie rzeczywistym. Aplikacja pozwala rozróżniać ludzi, zwierzęta i pojazdy oraz jest w stanie wskazać zdarzenia w rodzaju włamania, przekroczenia strefy i podejrzanego zachowania.

Monitoring obiektów bez zasilania

W latach 2015-2016 Najwyższa Izba Kontroli przeprowadziła kontrolę i audyt, którego celem była weryfikacja skuteczności zabezpieczeń technicznych obiektów infrastruktury krytycznej. Obiekty te mają priorytetowe znaczenie dla funkcjonowania i bezpieczeństwa państwa i dlatego w pierwszej kolejności skupiono się na nich. W przedstawionym raporcie wskazano wiele nieprawidłowości, m.in.:

- ochroną fizyczną nie obejmowano wszystkich obiektów infrastruktury krytycznej;
- część terenów, na których znajdowały się obiekty infrastruktury krytycznej, nie była właściwie zabezpieczona;
- wejścia do części obiektów nie spełniały norm bezpieczeństwa i nie były objęte systemem kontroli dostępu, a bramy wjazdowe nie zostały wyposażone w zapory zabezpieczające przed wtargnięciem;
- we wszystkich skontrolowanych podmiotach nie wyodrębniono personelu, kluczowego dla przestrzegania zasad bezpieczeństwa infrastruktury krytycznej.

Raport sprawił, że w ostatnim czasie coraz częściej obserwujemy zmianę w podejściu do zabezpieczenia obiektów IK. Pierwsze efekty tego zjawiska można było zauważyć w 2017 r. W tym roku zapewne zostaną podjęte kolejne działania. Trzeba pamiętać, że opracowanie koncepcji ochrony takich obiektów, a następnie przeprowadzenie wdrożenia całego systemu jest procesem długim i złożonym. Obiekty infrastruktury krytycznej to jedne z najbardziej skomplikowanych obiektów do zabezpieczenia. Często standardowe systemy i rozwiązania są tutaj niewystarczające. Dlatego coraz częściej projektanci sięgają po technologie, które jeszcze nie tak dawno były zarezerwowane dla wojska lub były na tyle kosztowne, że dla wielu użytkowników stały się niedostępne. Jednym z rozwiązań, które przeszło z wojskowych obszarów zastosowań do obszaru cywilnego, jest radar. Popularyzacja tego rozwiązania widoczna jest także w innych segmentach. Coraz częściej właśnie radary krótkiego zasięgu montuje się w samochodach. Masowa produkcja tych rozwiązań przyczynia się do sukcesywnego spadku cen tej technologii.
W obiektach infrastruktury krytycznej są stosowane bardziej profesjonalne radary o większym zasięgu detekcji, które wykrywają intruza z dużej odległości, a po wykryciu mogą go śledzić. Mogą być stosowane do detekcji różnych obiektów ruchomych: czołgających się lub wędrujących osób, poruszających się pojazdów lądowych oraz łodzi, nisko latających samolotów, w tym dronów. Radary wykorzystują

Jakub Sobek
certyfikowany trener techniczny, Linc Polska

mikrofale do skanowania powierzchni ziemi lub wody na dystansie aż do 32 km, przy azymucie 360°. Radar można zintegrować z kamerą termowizyjną dalekiego zasięgu, co zapewnia operatom bardzo dobrą świadomość sytuacyjną. Dzięki tak dużym zasięgom działania, w systemie można zaprojektować niewielką liczbę urządzeń, co stanowi dużą zaletę takich projektów. Tak zaprojektowane systemy przy kolejnej kontroli NIK z pewnością zasłużą na pochwałę!

Międzynarodowe Targi Poznańskie

securex®
POLAND

Międzynarodowe Targi Zabezpieczeń

23-26.04.2018
POZNAŃ

Zabezpiecz swój sukces!

www.securex.pl

Projektowanie systemów termowizyjnych

Jak dobrać właściwe do danego projektu rozwiązanie i uniknąć najczęściej popełnianych błędów projektowych.

Jakub Sobek

Tradycyjne kamery są obecnie naturalnym elementem wielu systemów zabezpieczenia technicznego, często jednak służą jedynie do dokumentowania zdarzeń, a nie do aktywnego wykrywania intruza, zanim jeszcze zdąży dokonać kradzieży czy zniszczenia. Dlatego projektanci systemów coraz częściej zwracają się w stronę bardziej zaawansowanych rozwiązań – takich systemów, które pozwolą zrezygnować z ochrony fizycznej na rzecz rozwiązań technicznych.

Angielska firma Trigion świadcząca usługi ochrony obiektów i patrolowania zauważa na swojej stronie internetowej, że termowizja jest jedną z technologii, która pozwala świadczyć usługi na zupełnie nowym poziomie. Jako przykład przywołuje jeden ze swoich projektów: zabezpieczenie dużego złomowiska. Chroniony obszar jest rozległy, a na jego terenie składuje się mnóstwo materiałów różnego typu. Taka złożoność monitorowanej sceny sprawia, że trudno zauważyć intruza za pomocą tradycyjnych kamer CCTV. Trzeba też pamiętać, że jeśli ludzkim okiem trudno dostrzec np. osobę na ekranie, tym trudniejsze będzie to dla algorytmów analizy wizyjnej. Niejednokrotnie to rozwiązanie stanie się nieskuteczne.

Kamera termowizyjna pozwala natomiast na zauważenie obiektu cieplejszego od tła i precyzyjne określenie sposobu jego przemieszczania się. Dobry kontrast między tłem a obiektem zapewnia skuteczniejsze działanie analizy wideo. Obszary detekcji można modyfikować wraz ze zmianą rozkładu materiału w obrębie złomowiska, co sprawia, że cały system jest bardzo elastyczny.

Termowizja coraz częściej staje się elementem oferty czołowych producentów kamer. Jeszcze kilka lat temu rozwiązania te były dostępne jedynie w kilku firmach, które specjalizowały się tylko w tej technologii. Ta zmiana dowodzi, że rynek zauważył ten trend i docenił skuteczność takich rozwiązań. Kamery termowizyjne coraz chętniej są używane także na rynku polskim. Wiele osób podchodzi jednak do tej technologii z pewną obawą, wynikającą zazwyczaj z niewiedzy w tej materii. W projektach są często popełniane te same podstawowe błędy.

Przyjrzyjmy się zatem głównym aspektom technicznym kamer termowizyjnych.

Technologia kamer termowizyjnych

Pierwsze kamery termowizyjne pojawiły się na przełomie lat 40. i 50. ubiegłego wieku. Początkowo działały na zasadzie skanowania liniowego. Na uzyskanie pojedynczego obrazu kamera potrzebowała około godziny. Były to w tamtych czasach rozwiązania tworzone na potrzeby amerykańskiego wojska i miały stanowić jeden z elementów wyposażenia systemów obrony przeciwlotniczej. Od lat 50. można zauważyć znaczny postęp w rozwoju nowoczesnych materiałów i wiele innowacji w zakresie produkcji oraz projektowania urządzeń termowizyjnych. Przez te wszystkie lata nastąpił także duży rozwój w dziedzinie optoelektroniki, który stanowi podstawę technologii termowizyjnej. Pojawienie się nowych materiałów i nanostruktur sprawiło, że nowe rozwiązania są znacznie mniejsze i wydajniejsze niż te sprzed lat.

Podczerwień to część widma elektromagnetycznego znajdująca się poza zakresem światła widzialnego dla ludzkiego oka. Z promieniowaniem podczerwonym wiąże się kilka praw opisujących jego charakter. Najważniejsze z nich to prawo Kirchhoffa, prawo Stefana-Boltzmanna, prawo Plancka oraz prawo Wiena. Nie wchodząc głębiej w szczegółowe ich opisy, warto zaznaczyć podstawowe założenia. Pozwalają one lepiej zrozumieć działanie kamer termowizyjnych oraz wszelkich aspektów związanych z obrazowaniem w tym paśmie.

W roku 1859 Gustav Kirchhoff zauważył, że każdy materiał, który dobrze pochłania promieniowanie podczerwone jest także dobrym radiatorem. Ciało pochłaniające

całe promieniowanie nazywa się ciałem doskonale czarnym. Odwrotnością jest ciało doskonale białe, czyli takie, które całkowicie odbija promieniowanie. Ciała takie w przyrodzie praktycznie nie występują, przyjmowane są do budowania teoretycznych modeli fizycznych.
Prawo Stefana-Boltzmanna opisuje całkowitą energię wypromieniowywaną przez ciało doskonale czarne w danej temperaturze. Łatwo zauważyć, że nie zależy ona od długości fali, a jedynie od temperatury tego ciała:

$$E = \sigma \cdot T^4 \quad [W/m^2]$$

gdzie: E jest energią promieniowania,
σ stałą Stefana-Boltzmanna,
T temperaturą w skali Kelwina.

Szczegółową znajomość zagadnień fizycznych związanych z termowizją powinny posiadać osoby, które zajmują się konstrukcją kamer termowizyjnych, wykonują ich kalibrację lub prowadzą badania naukowe dotyczące radiometrii. Dla stosujących kamery w systemach zabezpieczenia technicznego wiedza ta może okazać się pomocna, ale nie jest konieczna. Takie podstawy fizyczne na tym etapie są wystarczające.
Podczerwień to obszar widma elektromagnetycznego obejmujący 0,7–1000 µm. Jest to zakres fal leżący pomiędzy światłem widzialnym a promieniowaniem mikrofalowym. Znaczna część tego spektrum nie jest jednak dostępna dla kamer termowizyjnych. Wiele długości fal jest pochłanianych przez gazy znajdujące się w atmosferze ziemskiej. Istotne są nazywane potocznie tzw. okna widmowe lub okna transmisji atmosferycznej. Określają pasma, które mogą zostać wykorzystane. Wyróżniamy cztery podstawowe pasma: bliska podczerwień NIR, 0,8–1,1 µm, krótka podczerwień SWIR, 0,9–2,5 µm, średnia podczerwień MWIR 3–5 µm oraz daleka podczerwień LWIR 7–14 µm.
Pasma NIR i SWIR są zbliżone do pasma światła widzialnego (od strony jego najdłuższych fal). Fale te zachowują się podobnie jak światło widzialne. Promieniowanie w tych pasmach musi zostać wyemitowane z jakiegoś źródła, aby następnie odbić się od obiektu, na który pada, i trafić do obiektywu kamery. Dopiero wtedy można uzyskać obraz dobrej jakości. Dotyczy to wszystkich kamer CCTV, które mają wbudowane oświetlacze podczerwieni.
Z powodu braku zrozumienia różnic związanych z długościami fal wiele osób potocznie nazywa kamery różnego typu, stosując wymiennie określenie „kamery na podczerwień" i „kamery termowizyjne". Trzeba zaznaczyć, że istnieje wyraźna granica pomiędzy rozwiązaniami tego typu. Kamery termowizyjne to (dopiero) te kamery, które operują w pasmach MWIR oraz LWIR. Ze względu na inne długości fal niż światło widzialne kamery muszą być wyposażone w inny detektor promieniowania niż tradycyjnie używane kamery. To główny element różnicujący je.
Czujnik podczerwieni jest elementem, który przez lata ewoluował. Na początku był to pojedynczy detektor ze skanowaniem optyczno-mechanicznym. W latach 70. zaczęto produkować pierwsze kamery oparte na matrycach wielopikselowych FPA (*Focal Plane Array*). Obecnie dostępne na rynku przetworniki obrazu można podzielić na dwa typy: chłodzone i niechłodzone. Przetworniki niechłodzone są przystosowane do pracy w oknie widmowym LWIR, chłodzone zaś w oknie MWIR. Poza wieloma różnicami technicznymi w sposobie działania i budowie tych detektorów niestety najczęściej kluczowa jest różnica ich ceny. Detektory niechłodzone są wielokrotnie tańsze od tych dla fal MWIR. W wielu aplikacjach nie stanowi to jednak większego problemu, ponieważ obecnie jakość niechłodzonych przetworników jest tak wysoka, że mogą one pracować na dystansach nawet do 8000 m. Zatem jedynie wtedy, kiedy monitorowane są bardzo duże odległości (np. ochrona granic, portów, lotnisk, obiektów wojskowych) czy przy bojowych zastosowaniach wojskowych wykorzystuje się kamery chłodzone.

Jeszcze kilka lat temu kamery termowizyjne oferowało tylko kilka firm, które specjalizowały się jedynie w tej technologii. Rynek zauważył i docenił skuteczność takich rozwiązań.

Kolejnym elementem różnicującym kamery tradycyjne od termowizyjnych jest stosowana w nich optyka. Promieniowanie podczerwone jest blokowane przez szkło, przez co w kamerach termowizyjnych nie można używać tradycyjnej optyki. Istnieje wiele pierwiastków, z których wykonuje się obiektywy do takich kamer. Jednym z nich jest german, który ma bardzo dobre parametry fizyczne. Materiał ten jest nieprzepuszczalny dla światła widzialnego, a przepuszcza fale o długości 2–14 µm. Oprócz kamer german jest także stosowany w czujkach podczerwieni, pirometrach czy medycznych przyrządach pomiarowych. Ważnymi jego cechami są nietoksyczność, duża twardość i wytrzymałość. Dzięki temu dobrze wykonane obiektywy kamer są bardziej odporne na uszkodzenia. Dodatkowe warstwy powlekające german zwiększają wytrzymałość i zmniejszają refleksyjność ich powierzchni. Dzięki temu więcej energii podczerwieni trafia do wnętrza kamery. W efekcie obraz jest lepszej jakości, ma wyższy kontrast nawet w przypadku niskiej różnicy temperaturowej pomiędzy tłem a obiektem.
Trzecim elementem każdej kamery termowizyjnej jest procesor sygnałowy – DSP (*Digital Signal Processor*). Wcześniej ten element kamery był odpowiedzialny za przeprowadzanie prostych operacji na obrazie, takich jak zmiana jasności obrazu, kontrastu czy np. wyostrzanie krawędzi na obrazie. Dzisiaj DSP jest wyposażany w dodatkowe funkcje znacząco rozszerzające funkcjonalność kamer, w tym także termowizyjnych. Współczesne procesory stosowane w kamerach termowizyjnych stanowią tak naprawdę połączenie procesorów graficznych z procesorami DSP oraz RISC (*Reduced Instruction Set Computing*). Umożliwia to budowanie rozwiązań łączących architekturę 8-, 16- oraz 32-bitową wraz ze zmiennoprzecinkową arytmetyką 16- i 32-bitową. Wielordzeniowa architektura takich procesorów oraz kontrolowana przez oprogramowanie pamięć podręczna tworzą konfigurację, która pozwala osiągnąć wysoką wydajność. Wszystko to przy zachowaniu niskiego poboru mocy. Niskie zapotrzebowanie energetyczne jest szczególnie istotne, gdyż projektanci zawsze starają się zasilać kamery IP za pomocą PoE, a w klasie 3. występują ograniczenia do 15,4 W.

Nowe procesory wzbogacają kamery termowizyjne o nowe funkcje, które jeszcze kilka lat temu w urządzeniach brzegowych nie istniały. Nową technologią w takich rozwiązaniach jest np. *deep learning,* czyli uczenie głębokie, funkcjonalność szczególnie istotna we współczesnej analizie wizyjnej. Usprawnia nie tylko detekcję uprzednio zdefiniowanych wzorców, ale także uczenie się kamery nowych wzorców na przestrzeni czasu. Takie funkcje jak *deep learning* potrzebują dużych mocy obliczeniowych, ponieważ w trakcie działania wykonuje się wiele złożonych operacji związanych chociażby z mnożeniem dużych macierzy liczbowych, co jest wymagane przy uczeniu się sieci neuronowych. Z tego powodu wydajność na poziomie kilku GFlops (1 GFlop = 1 mld operacji/s) jest tak ważna.

Zastosowanie dużych pamięci RAM w procesorze pozwala na przechowywanie tymczasowych danych, które powstają w trakcie uczenia głębokich sieci neuronowych. Technologia *deep learning,* która do niedawna mogła być implementowana tylko na serwerach lub w chmurze, teraz może znaleźć się w kamerze. Jedną z bardzo pomocnych funkcji, szczególnie przy analityce wideo, jest zdolność budowania modeli 3D. Na podstawie ruchu obiektów, analizy głębi, czasem też przy wsparciu dodatkowych sensorów kamera buduje sobie model monitorowanej sceny. Dzięki temu możliwa jest korelacja wielkości obiektu i miejsca, w którym się on znajduje i porusza. Ułatwia to także śledzenie zauważonych obiektów nawet w bardzo złożonych scenach.

Za kilka lat, kiedy roboty do patrolowania obiektów staną się bardziej popularne, także kamery termowizyjne będą jednym z wielu „zmysłów", w które zostanie wyposażony robot. Takie algorytmy będą niezbędne w jego codziennej pracy, zatem szybki rozwój w kolejnych latach to rzecz raczej pewna.

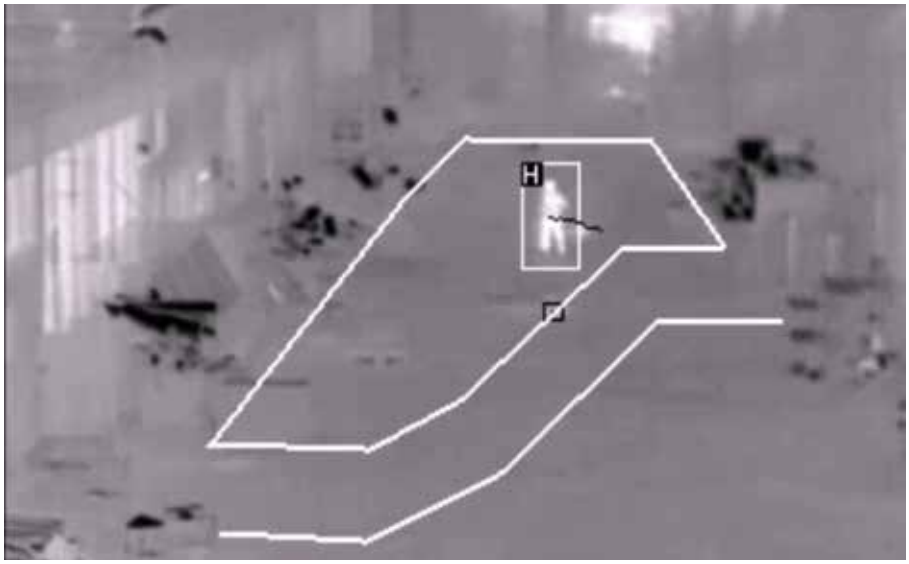
Termowizja i analiza obrazu

W zależności od tego, z jakiego algorytmu analizy wizyjnej chcemy korzystać, należy dobrać właściwą kamerę termowizyjną. Szczególnie jest to istotne, gdy planujemy stosowanie algorytmów wizyjnych innego producenta niż producent kamery. Wiele osób, dobierając kamerę do swojego projektu, posługuje się zasięgami podawanymi przez producentów kamer, które opierają się na kryterium detekcji, rozpoznania i identyfikacji. Kryteria te są wyliczane na podstawie opracowania Johna Johnsona z końca lat 50. XX wieku (*rys. 1*). W swojej pracy scharakteryzował on prawdopodobieństwo DRI (detekcja, rozpoznawanie, identyfikacja), opierając się na efektywnej rozdzielczości kamery. Obecnie dla kryterium detekcji przyjmuje się, że obiekt musi mieć wielkość minimum 1,5 x 1,5 piksela. Wielkość 1,5 piksela jest odpowiednikiem 0,75 cyklu dla przestrzennej rozdzielczości celu. W kryterium rozpoznania minimalna liczba pikseli wynosi 6 x 6, a dla identyfikacji 12 x 12 pikseli.

Rys. 1. **Graficzne przedstawienie kryterium Johnsona**

Projektanci dobierający kamery do systemów zabezpieczenia technicznego posługują się niejednokrotnie materiałami marketingowymi kamer termowizyjnych. Bez chwili refleksji nad tym, jaka jest różnica pomiędzy poszczególnymi kryteriami. Dobierają kamery w swoich projektach, opierając się właśnie na najniższym kryterium detekcji. Zapominają, że na końcu deklarowanego zasięgu obiekt wielkości człowieka będzie reprezentowany przez pojedyncze piksele. W przypadku trudnych warunków atmosferycznych będzie to nie do osiągnięcia. Bardzo gęsta mgła, ulewny deszcz lub gęsty śnieg skracają skuteczny zasięg działania. Nie można zakładać, że system analizy wizji zadziała prawidłowo, gdy na obrazie obiekt będzie miał wielkość 3–4 piksele. Tak mała liczba punktów nie pozwala także na określenie charakterystyki obiektu, czyli prawidłowe zakwalifikowanie do jakiegokolwiek wzorca. Często współczesne algorytmy wizyjne pozwalają określić, czy obserwowany obiekt to osoba, pojazd, czy zwierzę (*rys. 2*). Prawidłowa kategoryzacja obiektu umożliwia eliminowanie niepożądanych alarmów spowodowanych np. przez przelatujące ptaki.

Jeśli stosując kamery termowizyjne, zamierzamy korzystać z algorytmów analizy wizyjnej, musimy zacząć od zapoznania się z dokumentacją techniczną tego rozwiązania. Najważniejsze są dwa podstawowe parametry działania danego algorytmu. Pierwszym z nich jest wielkość obiektu, jaki może zostać wykryty. Wartość ta jest podawana w pikselach lub procentowo, określając wysokość obiektu w stosunku do wysokości całego obrazu. W przypadku różnych algorytmów można znaleźć różne wartości. Producenci podają w swoich rozwiązaniach, że cel wielkości człowieka powinien mieć minimum 10 x 10 pikse-



Rys. 2. **Przykład działania analizy wizji z klasyfikacją zauważonego obiektu. Litera H oznacza Human, czyli człowiek.**

li. U innego producenta można spotkać wymóg mówiący o liczbie pikseli na cel (POT – *Pixel on Target*), według którego cel wielkości człowieka powinien generować minimum 60 pikseli na obrazie. Taki opis jest oczywiście poprawny i ostatnio właśnie parametr POT staje się coraz bardziej popularny. Mimo prawidłowego wyliczenia liczby pikseli na cel przy planowanej odległości nie należy zapominać o warunkach atmosferycznych, które mogą wpływać na kontrast obrazu oraz widoczność celu. Z tego powodu trzeba pamiętać, że określany zakres wykrywania obiektu jest oceną statystyczną, która takie warunki powinna uwzględniać. Zatem przyjmowane w kalkulacjach graniczne wartości POT dla danego algorytmu mogą sprawić, że przy gorszej pogodzie obiekt nie zostanie prawidłowo zakwalifikowany lub nawet nie zostanie wykryty.

Drugim istotnym parametrem, który musimy sprawdzić, wybierając algorytm analizy wizji, jest rozdzielczość strumienia, na jakim pracuje. Niewiele algorytmów działa w wysokich rozdzielczościach. Często obraz wysyłany z kamery np. o rozdzielczości VGA (640 x 480 pikseli) jest przez algorytm skalowany do rozdzielczości niższej, np. CIF (352 x 288 pikseli) lub nawet QCIF (144 x 176 pikseli). To bardzo istotna kwestia przy obliczeniach POT, ponieważ nawet jeśli przetwornik kamery ma np. rozdzielczość VGA, a algorytm pracuje w rozdzielczości QCIF, to wszystkie wyliczenia liczby pikseli na cel powinny zostać wykonane właśnie dla tej niższej rozdzielczości. W przeciwnym wypadku, tzn. przy wyliczeniach dla wyższej rozdzielczości, zawyżamy nie tylko liczbę otrzymywanych pikseli, ale także skuteczny zasięg detekcji danej kamery i zastosowanego algorytmu analizy wizyjnej. W rezultacie w projekcie kamery zostaną umieszczone w zbyt dużych odległościach między sobą. Już na początku tworzymy wirtualne ogrodzenie, które będzie miało „olbrzymie dziury". Trzeba także pamiętać o pewnym aspekcie ekonomicznym, który się tutaj pojawia. Im wyższa rozdzielczość kamery termowizyjnej, tym większa jej cena. Choć ta zależność nie jest w pełni liniowa, nie ma sensu stosować kamer o bardzo wysokich rozdzielczościach, jeśli wybrany algorytm i tak pracuje na obrazach mniejszej wielkości. Nie przyniesie to bowiem żadnej poprawy skuteczności detekcji intruza, a przecież jest to cel stawiany najczęściej przed kamerami pracującymi w systemach ochrony perymetrycznej.

Rys. 3. **Przykład POPRAWNEGO rozmieszczenia kamer.** Martwa strefa kamery nr 2 znajduje się w strefie efektywnego działania kamery nr 1.

Rys. 4. **Przykład BŁĘDNEGO rozmieszczenia kamer.** Martwa strefa kamery nr 2 znajduje się poza strefą efektywnego działania kamery nr 1.

Wyższa rozdzielczość kamer ma przeważnie sens, gdy wybieramy kamery termowizyjne z wbudowaną analizą obrazu na pokładzie samej kamery. Wszystko to jest już obecnie możliwe dzięki coraz lepszym procesorom umieszczanym w kamerach. Producenci dostosowują działający na pokładzie kamery algorytm do jej rzeczywistej rozdzielczości, dzięki czemu wyższa rozdzielczość poprawia zasięg działania kamery.

Tworząc koncepcję systemów ochrony perymetrycznej, należy mieć na względzie kilka podstawowych aspektów. Budowany system ma na celu stworzenie wirtualnego ogrodzenia, które oddziela obszar zewnętrzny od właściwego obszaru chronionego obiektu. Zazwyczaj intruz ma być wykryty właśnie na etapie przekraczania tej wirtualnej linii. W niektórych przypadkach może być także wykrywany na zdefiniowanych obszarach. W takich aplikacjach kamery termowizyjne z niechłodzonym przetwornikiem obrazu dają zazwyczaj wystarczająco dobry obraz do wykorzystania wraz z analizą wizji. Oczywiście należy przy wyborze zwracać uwagę na parametry techniczne danego rozwiązania oraz na to, co może zaoferować wbudowany procesor.

Poza tym należy pamiętać o takim pozycjonowaniu kamer, aby wyeliminować wszystkie ewentualne martwe strefy, przez które intruz może przejść niezauważony (*rys. 3* i *rys. 4*), a także o policzeniu wielkości celu dla zakładanych zasięgów pracy, aby spełniać kryteria wydajności wybranej analizy od początku do końca planowanego obszaru działania. Jeśli podczas projektowania przestrzegamy tych podstawowych zasad, szybko docenimy skuteczność działania systemów opartych na kamerach termowizyjnych, tak jak doceniła to firma Trigion. Wraz ze wzrostem świadomości na temat tej technologii będziemy obserwować ciągły wzrost jej popularności. Zapewne kolejne lata zaskoczą nas niejednokrotnie rozwojem tej technologii.

Literatura:

[1] *The Truth about range data: How to assess thermal camera range capability for site design purposes,* John Love, DRS Commercial Infrared Systems White Paper, 2014
[2] *Infrared: A Key Technology for Security Systems, "Advances in Optical Technologies"*, Carlo Corsi 2012
[3] *Advances in Infrared Detector Array Technology*, Nibir K. Dhar, Ravi Dat and Ashok K. Sood 2013
[4] *Best Practices Guide for Perimeter Security Applications* – FLIR Systems
[5] *Fundamentals of Infrared and Visible Detector Operation and Testing, Second Edition,* – John David Vincent 2016
[6] https://trigion.co.uk/trigion-proves-its-mettle-at-scrap-yard
[7] http://www.iiviinfrared.com/Optical-Materials/ge.html
[8] https://www.movidius.com/technology

5 pytań o termowizję z analizą obrazu

Termowizja i analiza obrazu są znane od wielu lat, jednak dla wielu wciąż skrywają tajemnice i nieodkryte zalety w zastosowaniach security. Podobne pytania słyszę podczas spotkań i rozmów z wieloma osobami z branży.

Krzysztof Skowroński

1 W jaki sposób kamera termowizyjna „widzi" promieniowanie podczerwone?

Termowizja jest metodą obrazowania rozkładu temperatury obserwowanych obiektów, opartej na detekcji promieniowania podczerwonego. W uproszczeniu kamera termowizyjna jest rodzajem termometru działającego na odległość. Mierząc różnice temperatury na powierzchni obserwowanych obiektów, tworzy ich obraz temperaturowy. Każdy piksel obrazuje różnicę temperaturową wyrażoną odpowiednią barwą lub odcieniem szarości. Działanie kamery termowizyjnej nie ma zatem nic wspólnego z tworzeniem obrazu w tradycyjnych kamerach wizyjnych.

2 Na czym polega różnica pomiędzy kamerą termowizyjną a kamerą wizyjną?

Kamera termowizyjna zapewnia obrazowanie niewidzialnego promieniowania podczerwonego (tzw. energii termicznej), czyli wykrywa energię fal elektromagnetycznych o określonej długości w zakresie pomiędzy światłem widzialnym a falami radiowymi. Ze względu na charakterystykę przepuszczalności powietrza zależną od długości fali producenci kamer termowizyjnych wykorzystują głównie zakres LWIR (8–14 um), który ulega nieznacznemu tłumieniu w atmosferze.

W odróżnieniu od klasycznych kamer wizyjnych, których przetworniki CMOS/CCD wykrywają fotony promieniowania widzialnego (lub też bliskiej podczerwieni, np. z oświetlaczy podczerwieni), docierające po odbiciu od obserwowanych obiektów do przetwornika, kamera termowizyjna jest wyposażona w detektor promieniowania podczerwonego wyemitowanego (nie odbitego!) przez obiekt. Z reguły jest to niechłodzona matryca bolometryczna, której zadaniem jest pomiar temperatury docierającego do kamery promieniowania cieplnego. Padające promieniowanie jest absorbowane w materiale detektora, co powoduje podniesienie temperatury elementów matrycy bolometrycznej i zmianę ich rezystancji.

3 Jakie obiekty wykrywa kamera termowizyjna?

Każdy obiekt o temperaturze powyżej zera bezwzględnego 0°K (czyli powyżej -273,15°C) emituje energię. Zatem praktycznie każde ciało fizyczne znajdujące się na Ziemi emituje energię termiczną (np. człowiek emituje promieniowanie podczerwone o temperaturze ok. 309°K). Czyli każdy obiekt spełniający powyższy warunek jest wykrywany przez kamerę termowizyjną.

4 Co stanowi o wyższości kamery termowizyjnej w systemie monitoringu?

Kamera termowizyjna do uzyskania obrazu nie wymaga doświetlenia sceny aktywnym źródłem światła. Działa dyskretnie w całkowitej ciemności i ta cecha stanowi istotną zaletę oraz przewagę pod względem skuteczności działania. Ponadto działa skutecznie w trudnych warunkach widoczności, takich jak zadymienie, opady deszczu lub śniegu. Jest równie skuteczna latem w pełnym słońcu, gdyż wykrywa nawet najmniejsze różnice temperatury pomiędzy tłem a obiektami znajdującymi się w zasięgu obserwacji.

Opisane właściwości termowizji sprawiają, że znajduje ona szerokie zastosowanie w systemach ochrony zewnętrznej i perymetrycznej. Kamery termowizyjne monitorują rozległe tereny, place magazynowe, parkingi, obszary o słabej lub „zerowej" dla tradycyjnych kamer widoczności, w terenach zalesionych, w przemyśle, transporcie itd. Są niezastąpione i najskuteczniejsze w sytuacjach, gdy nie ma konieczności identyfikacji obiektów, a wymagane jest jedynie szybkie wykrycie i stwierdzenie ich obecności. Stanowią swoisty rodzaj detektora dalekiego zasięgu. Utrudniona widoczność czy niekorzystne warunki atmosferyczne to statystycznie warunki największego nasilenia czynów przestępczych. Tymczasem w takich właśnie warunkach termowizja zapewnia skuteczną, a przy tym dyskretną detekcję potencjalnych intruzów bez konieczności doświetlania obszarów monitorowanych.

BIO

Krzysztof Skowroński
Od 20 lat związany z branżą security, od 2001 r. pracuje w firmie CBC Poland. Ma bogate doświadczenie w zakresie systemów VSS i rozwiązań technologicznych stosowanych w systemach monitoringu wizyjnego.

5 Jakie korzyści zapewnia kamera termowizyjna z analizą wizji?

Określenie *analiza wizji* jest zbyt uogólniane i nadużywane do celów marketingowych, stosuje się je nawet w kontekście najprostszych rozwiązań nieznacznie odbiegających od zwykłej detekcji ruchu.

Klient ma utrudnione zadanie, stojąc przed wyborem konkretnego algorytmu analizy treści obrazu (VCA) tego czy innego producenta. Brak norm i uregulowań mogących stanowić zasadnicze narzędzie do klasyfikacji czy oceny jakościowej algorytmów analizy spowodowało swobodę w zakresie propagandy marketingowej.

Tymczasem wystarczy przeprowadzić rzetelny test w rzeczywistych (nie laboratoryjnych!) warunkach, aby się przekonać, jaki poziom jakości (czytaj: skuteczności) prezentuje badany algorytm.

Zachęcam również do zwrócenia uwagi na różnice, jakie prezentuje analiza wizji posiadająca certyfikację *i-LIDS* – brytyjskiego instytutu naukowego powołanego przez rządowy organ *Home Office* i zajmującego się badaniem oraz oceną skuteczności algorytmów analitycznych w systemach wizyjnych. Wielka Brytania, niekwestionowany pionier i europejski lider pod względem skali wdrożonych systemów wizyjnych, już wiele lat temu usankcjonowała kwestie oceny jakościowej analizy wizyjnej. Nadanie certyfikatu *i-LIDS* oznacza jedno – przebadany algorytm zdał trudny egzamin i prezentuje bardzo wysoki poziom skuteczności.

Wracając do postawionego pytania, obraz z kamery termowizyjnej w odpowiednich trybach palety barw, np. w trybie *white-hot,* charakteryzuje się czytelnym odróżnieniem (kontrastem) obiektów ciepłych od tła. Poddanie takiego obrazu analizie sprawia, że obiekty o temperaturze innej niż temperatura tła są bardzo szybko wykrywane i bezbłędnie śledzone. Wykrycie i sklasyfikowanie obiektu jako zagrożenie (np. człowiek -> ALARMUJ, zwierzę -> IGNORUJ) powoduje natychmiastowe powiadomienie o alarmie, a przy tym nie generuje fałszywych alarmów.

Wykrycie z dużym prawdopodobieństwem realnego zagrożenia i natychmiastowa reakcja stanowią kluczową zaletę termowizji połączonej z analizą obrazu. Narząd wzroku operatora wykorzystywany dotychczas jako podstawowe i często jedyne narzędzie detekcji sytuacji alarmowych może być wyręczony z konieczności ciągłej obserwacji obrazów.

Połączenie tych dwóch technologii stanowi zatem silne narzędzie w ochronie zewnętrznej i obwodowej. Biorąc pod uwagę kilkukilometrowe zasięgi detekcji uzyskiwane przez kamery termowizyjne, można z powodzeniem określić te urządzenia mianem detektorów intruza o dalekim zasięgu i wysokiej skuteczności.

Przegląd kamer termowizyjnych

AXIS Q1942-E

Wyjątkowo skuteczna detekcja i szybka weryfikacja:

- Obsługa wielu rozwiązań analizy wizyjnej
- VGA 640x480 dla dalekiego zasięgu detekcji i szerokiego pola widzenia
- Wyjątkowy kontrast i elektroniczna stabilizacja obrazu
- Technologia *Zipstream* firmy Axis mniejsza przepustowość przy zachowaniu jakości
- Wydajny procesor w kamerze

AXIS Q1942-E umożliwia dołączenie do systemu dozoru wizyjnego najszerszego na rynku pakietu algorytmów w zakresie analizy wizyjnej. Aplikacje analizy treści obrazu firmy Axis i partnerów dostarczają danych, na podstawie których podejmowane są działania według scenariusza w odpowiedzi na wykryte zdarzenia: analiza, automatyczne odrzucenie zdarzeń niestanowiących zagrożenia i natychmiastowe powiadomienie personelu ochrony o sytuacjach potencjalnie krytycznych. Personel może wtedy obejrzeć wyraźne, szczegółowe nagranie, aby określić precyzyjnie charakter zagrożenia i zadziałać we właściwy sposób.

Kamera AXIS Q1942-E ma rozdzielczość termowizyjną 640 x 480 VGA przy pokryciu dozorem dużych obszarów i dużym zasięgu – jedna kamera rejestruje zdarzenia na dużym obszarze i z dużej odległości. Ponadto, dzięki połączeniu funkcji dynamicznego histogramu, wzmocnienia kontrastu i dynamicznego wyostrzania obrazu, kamera AXIS Q1942-E poprawia kontrast obrazu, zapewniając ostrość i wyraźne detale w każdych warunkach. Z kolei elektroniczna stabilizacja obrazu eliminuje zakłócenia nawet w przypadku narażenia kamery na drgania. W rezultacie otrzymujemy wyjątkowe możliwości detekcji i szybką weryfikację charakteru wykrytych zdarzeń. Zdarzenia można odrzucić lub podjąć konieczne działania, aby zminimalizować liczbę fałszywych alarmów.

AXIS P1280-E

Mała, dyskretna termowizyjna kamera sieciowa AXIS P1280-E sprawdza się wtedy, gdy konieczna jest niezawodna detekcja w dzień i w nocy.

Można ją zamontować za elementami konstrukcyjnymi, we wnękach, na ścianach lub w obudowie typu *bullet* w zależności od potrzeb. Akcesoria dostępne są dla każdej opcji montażu.

Kamera AXIS P1280-E ma wszystkie zalety kamery termowizyjnej w przystępnej cenie. Dzięki wbudowanym funkcjom analizy (lub zastosowaniu zaawansowanych aplikacji analitycznych Axis lub partnerów firmy) sprawdza się podczas detekcji osób, pojazdów lub obiektów niezależnie od warunków oświetlenia czy prób kamuflażu. Może służyć jako niedrogi detektor zapewniający potwierdzenie identyfikacji osób i przedmiotów w różnym otoczeniu, a także do zmniejszenia częstotliwości fałszywych alarmów.

- Niezawodna i niedroga detekcja ruchu
- Technologia termowizyjna obniżająca częstotliwość fałszywych alarmów
- Funkcjonalny i nierzucający się w oczy design
- Do użytku wewnątrz i na zewnątrz pomieszczeń

CBC Poland: GANZ mini-bullet serii GXi

Połączenie technologii VCA z termowizją wyznacza nowe standardy skutecznych systemów monitorowania. Wysoki odsetek incydentów związanych z bezpieczeństwem zdarza się w warunkach słabego oświetlenia lub słabej widoczności. Kamera termowizyjna ZNX1-BBT55G3xA z analizą wizyjną VCA działa skutecznie zarówno w dzień, w nocy, jak i w warunkach utrudniających widoczność.
Mini-bullet ZNX1-BBT55G3xA oferuje bardzo atrakcyjne i skuteczne rozwiązanie monitorowania, w porównaniu do konwencjonalnych metod łączenia standardowych kamer z czujnikami pasywnymi detekcji obwodowej, zapewniając bardzo skuteczną detekcję włamań, wejścia potencjalnego intruza do strefy zabronionej niezależnie od warunków widoczności (noc, dym, śnieg, ulewny deszcz, mgła), a dzięki zaimplementowanej analizie VCA jest potężnym narzędziem dla operatorów centrum monitoringu, gwarantującym skuteczną pomoc w wykrywaniu podejrzanych działań bez generowania fałszywych alarmów.
Analiza VCA może skutecznie wykrywać ruch w minimalnych obszarach obrazu. Czyni to poprzez analizę metadanych związanych z ruchem i właściwościami obiektów w treści strumienia wizji. Wynikiem takiego działania jest bardzo wysoki wskaźnik wykrywalności zdarzeń i skuteczna redukcja fałszywych alarmów, generowanych zwykle przez tradycyjne urządzenia bazujące na detekcji ruchu.
Kamera oferuje ponadto dodatkowe usługi, takie jak zliczanie pojazdów i osób, alarmy oparte na kryteriach prędkości, kontroli temperatury itp. Kamera jest również wyposażona w funkcję monitorowania temperatury, która może być skonfigurowana do wykrywania anomalii temperaturowych (np. procesy przemysłowe, logistyka, składy magazynowe), czy też wczesnego wykrycia zagrożenia pożarem. Określone „widełki" temperaturowe mogą być przypisane do czterech niezależnych stref pomiaru w polu widzenia kamery. Wykrycie zmiany temperatury wykraczającej poza zdefiniowany zakres wywołuje akcję alarmową.
Kamera jest dostępna w dwóch wersjach: z obiektywem 4 mm oraz 6,8 mm, temperatura pracy kamery to -40°C... +50°C, działa w oparciu o przetwornik mikrobolometryczny niechłodzony z tlenku wanadu, zasięg detekcji kamery wynosi 400 m.

Dahua: nowe kamery bispektralne

Kamery termowizyjne długo były kojarzone z technologią dostępną jedynie dla wojska lub ochroną dużych obiektów infrastruktury krytycznej. Mimo że ta technologia sprawdza się rewelacyjnie przy obserwacji rozległych, nieoświetlonych terenów, mało kto decydował się na stosowanie takich kamer ze względu na wysokie ceny urządzeń.
W 2017 r. nastąpiła ogromna zmiana w tej technologii. Dahua Technology wprowadziła do oferty nowe bispektralne kamery termowizyjne z funkcją *fusion*, która w unikalny sposób na obraz o rozdzielczości full HD nakłada obraz z modułu termowizyjnego. Model TPC-BF2120 łączy zalety kamer termowizyjnych i kamer tradycyjnych, niwelując ich potencjalne wady, a powstała technologia jest dostępna nawet dla odbiorców indywidualnych.
Opracowanie nowego, bardzo czułego detektora (czułość 40 mK), pracującego w zakresie 7-14 µm zaowocowało nową linią profesjonalnych kamer tulejowych – TPC-BF5400. Matryca detektora o wymiarach 400 x 300 pikseli rozwiązuje częsty problem zbyt małej szczegółowości popularnych detektorów o rozdzielczości CIF i zbyt wysokiej ceny detektorów o rozdzielczości VGA.
Kamery nowej linii mogą być wyposażane w obiektywy szerokokątne umożliwiające detekcję obiektów z odległości nawet 4000 m oraz w funkcje analizy treści obrazu, m.in. wykrycie intruza, przekroczenie linii czy detekcja źródeł ognia.
Zadbano także o interfejs użytkownika. Model TPC-BF5400 wykorzystuje komunikację zarówno IP, jak i analogową. Standard HDCVI umożliwia pracę kamery z wykorzystaniem istniejącego okablowania koncentrycznego, zapewnia też zdalne sterowanie kamerą i zmiany trybów prezentacji kolorów.
Firma Dahua Technology rozwija segment kamer termowizyjnych – podstawę doskonalszych systemów ochrony, dostępnych dla większej liczby odbiorców.

Hikvision DS-2TA13-6VI/H1

To najnowsza bispektralna kamera termograficzna zaprojektowana do pomiaru temperatury ciała człowieka. W urządzeniu znajduje się przetwornik mikrobolometryczny wykonany w technologii Vox o rozdzielczości 384 x 288, wspomagany przez kamerę pasma widzialnego o rozdzielczości 1280 x 960.
Kamera jest w stanie wykryć twarz i śledzić człowieka o podwyższonej temperaturze ciała w zatłoczonym obszarze publicznym, a dokładność pomiaru w czasie rzeczywistym może osiągnąć ± 0,3° C . W zestawie z kamerą otrzymujemy *ciało czarne* do kalibracji.
Niewielkie rozmiary ułatwiają montaż i integrację, zapewniając dyskretny monitoring. Kamera może być stosowana w celu kontroli czy kwarantanny w takich miejscach, jak przejścia graniczne, lotniska, szkoły i szpitale.

Hikvision DS-2TD2636-10

Model ten łączy zalety kamery termowizyjnej z kamerą pasma widzialnego. Dzięki nowej technologii urządzenie jest wyposażone w funkcję *fuzji obrazów*, która pozwala nakładać na siebie obrazy termowizyjne i światła widzialnego, tworząc z nich spójny widok. To sprawia, że widzimy więcej szczegółów, łatwiej dostrzegamy przedmioty i możemy skuteczniej potwierdzać wystąpienie nietypowych zdarzeń.
Moduł termowizyjny ma przetwornik typu Vox 50 Hz o rozdzielczości 384 x 288, o NETD: <40mK (@25°C,F#=0.9). Moduł pasma widzialnego zawiera przetwornik CMOS o rozdzielczości 1920 x 1080 wzmocniony technologią *DarkFighter*.
Na pokładzie kamery nie mogło zabraknąć promiennika podczerwieni o zasięgu do 40 m. W urządzeniu zaimplementowano funkcje PIP, pomiaru temperatury czy wykrycia ognia, co czyni ją uniwersalnym rozwiązaniem w ochronie obwodowej oraz ochronie obiektów infrastruktury krytycznej.

Hikvision DS-2TS03-25UM/W

Coraz większą popularnością cieszą się ręczne kamery termowizyjne, np. w postaci monokularu. Przedstawicielem tego typu urządzeń jest model DS-2TS03--25UM/W. Obiektyw 25 mm, przetwornik termowizyjny o rozdzielczości 384 x 288 i wyświetlacz OLED 1024x768 w połączeniu z niewielkimi rozmiarami dają duże możliwości w przypadku poszukiwań, patrolowania czy polowań.
Kamera ma własne Wi-Fi i aplikację na smartfon, dzięki czemu obraz można na żywo wyświetlać na smartfonie, co jest bardzo pomocne zarówno podczas marszu (osoba nie musi iść np. w lesie z kamerą przy oku), jak i w czasie stacjonarnego *czatowania*, można ją wtedy umieścić na statywie i całość obserwować z poziomu laptopa czy tabletu. W kamerze znajduje się też moduł GPS oraz wbudowana pamięć 16 GB umożliwiająca robienie zdjęć i nagrywanie filmów.

Linc Polska: Mobotix M16 Thermal TR

Kamera termowizyjna M16 Thermal TR marki Mobotix umożliwia zarówno monitoring wizyjny, jak i pomiar temperatury w zakresie od -40°C do 500°C.
Kamery TR *(Thermal Radiometry)* cechuje wykorzystanie skalibrowanego przetwornika termowizyjnego z dokładnością pomiaru ± 10°K. Możliwość weryfikowania wartości temperatury w każdym punkcie obrazu pozwala na zdefiniowanie zdarzenia bazującego na wzroście lub spadku temperatury we wskazanym obszarze (z możliwością tworzenia do 20 stref z indywidualnie dobranymi wartościami). Może to posłużyć do wysłania informacji sieciowej lub wysterowania wyjścia sygnałowego z powiadomieniem o danym zdarzeniu.
Kamera może być stosowana do zabezpieczenia ppoż. wewnątrz pomieszczeń, np. w przemyśle (zakłady produkcyjne), szeroko rozumianej logistyce lub na zewnątrz, np. przy detekcji pożarów lasów, obserwacji składowisk odpadów i produktów chemicznych.
Zastosowanie w kamerze dwóch przetworników: termowizyjnego i światła widzialnego (6 Mpix) zapewni operatorowi pełną świadomość sytuacji. Przetwornik termowizyjny można też wykorzystać do monitoringu. Dzięki wbudowanej funkcji analizy MxAcitivitySensor stanowi idealne uzupełnienie tradycyjnej kamery. Nałożenie na siebie obrazów termowizyjnego i światła widzialnego zapewnia wysoką szczegółowość.
Nowa platforma Mx6 z kompresją H.264 wspiera protokół ONVIF, dzięki czemu integracja kamery z istniejącymi systemami jest szybka i łatwa. Kamera ma wbudowany mikrofon i głośnik, można też rejestrować obraz na wbudowanej karcie microSD. Atutem kamery jest niski pobór mocy rzędu 8 W oraz zasilanie ze switcha PoE.
Rozwiązania Mobotix gwarantują bezpieczeństwo danych w sieci m.in. poprzez szyfrowanie SSL, tworzenie grup użytkowników, ochronę przed botami oraz kodowanie nagrań.
Model MOBOTIX M16 Thermal TR jest wszechstronnym narzędziem o wielu zastosowaniach, zarówno w zakresie pomiarów temperatury, jak i w ochronie perymetrycznej.

Linc Polska: FLIR FB-O

FLIR FB-O to najnowsza seria kamer termowizyjnych typu *bullet*, które sprawdzają się w wykrywaniu zagrożeń zarówno w dzień, jak i w nocy. Szczególnie polecane są w ochronie perymetrycznej różnych obiektów – prywatnych i przemysłowych. To połączenie wysokiej jakości z atrakcyjną ceną.
Przy odświeżaniu na poziomie 25 kl./s kamera generuje płynny obraz, a technologie *Auto AGC* czy *DDE* gwarantują, że jest on wyraźny i kontrastowy. Seria FB-O obejmuje kilka modeli różniących się zakresem obserwacji, zależnie od wybranego obiektywu i rozdzielczości przetwornika. Interesująca jest możliwość wyposażenia kamery w obiektyw szerokokątny (93°). Wszystkie modele serii są przystosowane do instalacji na zewnątrz (IP66).
Uniwersalność tego rozwiązania polega nie tylko na możliwości jego wszechstronnego zastosowania w różnego typu projektach. W przypadku tej serii elastyczność jest rozumiana również jako możliwość integracji kamer z systemami czy rozwiązaniami firm trzecich. Przykładowo współdziałanie z oprogramowaniem *FLIR United VMS* umożliwia precyzyjną konfigurację i zarządzanie alarmami.
Kamery serii FB-O można też integrować z inną zewnętrzną analizą obrazu, np. *IntrusionTrace* (detekcja wtargnięcia) czy *LoiterTrace* (detekcja osób i czasu ich przebywania w strefie) marki Xtralis, a już wkrótce seria FB zostanie wzbogacona o kamery z wbudowaną analizą.
Dwa niezależne strumienie, obsługa protokołów sieciowych, zgodność z ONVIF, a także wyjścia analogowe oraz IP to tylko niektóre z cech umożliwiających zastosowanie kamer serii FB-O w nowych oraz już istniejących systemach zabezpieczeń.
W modelach serii FB-O wykorzystano tę samą, wielokrotnie nagradzaną technologię termowizyjną, wcześniej stosowaną w innych kamerach termowizyjnych marki FLIR przeznaczonych do ochrony obiektów. Niezawodność tych rozwiązań potwierdza 10-letnia gwarancja producenta na sensor i 3-letnia gwarancja na kamerę.

Linc Polska: Silent Sentinel

Silent Sentinel jest brytyjskim producentem obrotowych kamer termowizyjnych. Firma słynie z głowic PTZ o wzmocnionej konstrukcji, na których są umieszczane kamery. Mogą to być kamery termowizyjne chłodzone lub niechłodzone, a także kamery dualne – termowizyjna w połączeniu z kamerą światła widzialnego.
Cechą wyróżniającą kamery niechłodzone marki Silent Sentinel są obiektywy o ogniskowej nawet 300 mm, co sprawia, że kamery mogą być stosowane do obserwacji na bardzo dalekich dystansach.
Przykładem jest kamera serii Jaegar Ranger, przystosowana do wymagających systemów zabezpieczeń. Wyposażona w obiektyw o długiej ogniskowej idealnie sprawdzi się w ochronie dużych obszarów. Umieszczenie kamery na walcu obrotowym umożliwia ruch ciągły o kącie 360° i równocześnie utrzymanie kamery na tym samym poziomie. Dzięki temu staje się idealnym narzędziem do pracy z radarem. Kamera termowizyjna wyposażona w przetwornik VOx o rozdzielczości 640x480 połączona z kamerą dzienną SD lub HD z zoomem optycznym pozwala operatorowi na wykrycie, a następnie weryfikację danego zdarzenia w zdefiniowanej strefie. Obrazy termowizyjny i dzienny są generowane w tym samym czasie.
Obudowa wykonana z odpornego aluminium malowanego proszkowo o klasie szczelności IP67 (opcjonalnie nawet IP68) zapewnia stabilną pracę w najbardziej wymagającym środowisku. Mechanizm obrotu oparty na kołach zębatych i optycznym enkoderze zapewnia precyzyjne sterowanie, a nawet korektę położenia z szybkością obrotu do 45°/s. Kamera Jaegar Ranger zintegrowana z dowolnym systemem zabezpieczeń stanowi idealne uzupełnienie systemów radarowych zamontowanych powyżej kamery, co umożliwia pełną detekcję wtargnięć. To profesjonalne rozwiązanie dla wymagających użytkowników.

Tiandy 视界为世界
Vision For World

X-NVR

SUPER MÓZG W TWOIM CENTRUM BEZPIECZEŃSTWA

- Obsługa do 320 kamer
- Obsługa 24 dysków + macierz na kolejne 24
- Redundantne zasilanie
- Tryby RAID 0, 1, 5, 6
- Inteligentna Analiza Obrazu IVA
- Obsługa kamer 4K

Tiandy Technologies Co.,Ltd.

Email: sales@tiandy.com
Website: en.tiandy.com
Phone: +86-22-58596065
Fax : +86-22-58596048

Normy Obronne

W Polsce działają dwa podstawowe ośrodki wprowadzające normy: Polski Komitet Normalizacyjny (PKN) oraz Wojskowe Centrum Normalizacji, Jakości i Kodyfikacji (WCNJiK). Regulacje prawne dotyczące normalizacji są zapisane w Ustawie z 12 września 2002 r., a więc z czasów, gdy Polska już była w NATO, lecz zanim stała się członkiem UE.

Stefan Jerzy Siudalski

Polski Komitet Normalizacyjny wprowadza normy międzynarodowych organizacji CEN i CENELEC[1]. Normy te:

- są oznaczane literami PN EN i odpowiednimi cyframi, zgodnymi z oznaczeniami oryginalnymi,
- są wprowadzane do spisu polskich norm albo w wersji językowej oryginalnej (angielskiej), albo po przetłumaczeniu w j. polskim,
- nie są do obowiązkowego stosowania, chyba że ustawodawca ustali inaczej, np. w rozporządzeniach lub w konkretnych inwestycjach, gdy normy lub część ich wymagań zostaną zapisane w SIWZ,
- w wielu arkuszach zawierają wymagania także dla obiektów militarnych,
- mają zapisane dokładnie te same wymagania dla wszystkich krajów członkowskich CEN i CENELEC, czyli urządzenia sprowadzane z zagranicy, a spełniające np. we Francji czy Niemczech wymagania konkretnych norm będą również spełniały wymagania odpowiednich, polskich norm serii PN[2],
- są dostępne dla każdego, lecz trzeba za nie zapłacić – prawa autorskie do norm ma PKN.

Wojskowe Centrum Normalizacji, Jakości i Kodyfikacji wprowadza i tworzy normy dot. sfery obronności kraju. Normy Obronne:

- są oznaczane kolejno: literami NO – cyframi – literą i cyframi – cyframi porządkowymi i oznaczeniem roku wydania,
- normy dotyczące systemów alarmowych i zabezpieczeń mechanicznych nie mają swoich dokładnych odpowiedników w normach zagranicznych[3],
- są tworzone w WCNiK, lecz zdarza się, że zawierają odwołania do norm serii PN EN,
- dostęp do nich jest ograniczony dla osób fizycznych, ale redakcje i instytucje mogą je kupić lub dostać, po zatwierdzeniu podania, za darmo.

Oprócz wymienionych różnic między tymi dwiema grupami norm można wskazać kilka istotnych, zdecydowanie odmiennych cech:

- normy grupy PN zawierają wiedzę zsumowaną, wielokrotnie przekonsultowaną i zatwierdzoną w pewnego rodzaju głosowaniu fachowców z dziedziny ochrony wszystkich krajów członkowskich CENELEC lub CEN – przed zatwierdzeniem ostatecznego kształtu każdej z norm mogły wypowiadać się setki fachowców i zgłaszać swoje uwagi,
- normy NO (przynajmniej tu omawiane) powstają w wąskim gronie fachowców tylko z Polski i tylko, jak mniemam, z wojska, a informacje nt. konsultacji z ekspertami spoza wojska podczas procesu tworzenia norm wskazują, że te możliwości nie są w pełni wykorzystywane[4].

Obecnie mamy ponad 950 norm obronnych, z tego dziewięć dotyczy zabezpieczeń elektronicznych (NO-04-A004 *Obiekty wojskowe – Systemy Alarmowe* z kwietnia 2016 r.) i jedna zabezpieczeń mechanicznych, w tym płotów (NO-04-A009:2017). Te dziewięć arkuszy Normy Obronnej dotyczącej systemów alarmowych liczy około 100 stron, a około 100 Polskich Norm dotyczących podobnego zakresu zawiera ponad 1000 stron. Już sam ten fakt sugeruje, że normy „cywilne" są znacznie bardziej rozbudowane i uszczegółowione niż Normy Obronne.

Jak to wpływa na poziom ochrony obiektów zabezpieczanych wg NO w stosunku do obiektów ochranianych wg zasad zawartych w normach PN EN?

Zanim odpowiem na to pytanie, przedstawię w skrócie, co zawierają powoływane tu arkusze Norm Obronnych *(tab.)*.

[1] Zostały pominięte ISO i IEC, ponieważ w przypadku omawianych tu norm te organizacje nie mają znaczenia.

[2] „Członkami CENELEC są krajowe jednostki normalizacyjne następujących państw: Austrii, Belgii, Bułgarii, Cypru, Danii, Estonii, Finlandii, Francji, Grecji, Hiszpanii, Holandii, Irlandii, Islandii, Litwy, Luksemburga, Łotwy, Malty, Niemiec, Norwegii, **Polski**, Portugalii, Republiki Czeskiej, Rumunii, Słowacji, Słowenii, Szwajcarii, Szwecji, Węgier, Włoch i Zjednoczonego Królestwa" i tych państwach normy, które w Polsce występują jako PN-EN, mają swoje dokładne odpowiedniki - oznaczenia literowe różnią się w zależności od kraju, ale cyfry w nazwie norm są takie same.

[3] Nie mają odpowiedników w NATO.

[4] Przykładowo Polska Izba Systemów Alarmowych (PISA) po zapoznaniu się projektami norm proponowała w 2015 r. daleko idące poprawki, które w większości nie zostały uwzględnione.

Numer normy, tytuł i liczba stron	Istotne zapisy	Uwagi
NO-04-A004-1:2016 Wymagania ogólne (10 stron)	– zawiera definicje w zakresie systemów alarmowych, w normie znajdują się odwołania do norm NO-04-A004-3, NO-04-A004-4, – podane są definicje stref ochrony, wymagania środowiskowe i wymagania na zasilanie, – zdefiniowano dwa z trzech rodzajów centrów monitorowania[5]: LCN – lokalne centrum nadzoru umieszczone wewnątrz chronionego obiektu, GCMA – garnizonowe centrum monitorowania obejmujące kompleks obiektów	podział na cztery strefy ochrony: peryferyjna – poza ogrodzeniem – zwykle bez systemów alarmowych, zewnętrzna obwodowa – obszar między ogrodzeniem zewnętrznym i wewnętrznym, gdzie znajdują się systemy elektronicznej ochrony, systemy łączności, wieże wartownicze, pas zabronowany, droga dla patroli, zewnętrzna bezpośrednia – obszar o szerokości 15 m przyległy do budynków, gdzie są montowane zarówno systemy alarmowe, jak i kamery, wewnętrzna[6] – obszar wewnątrz budynków łącznie ze wszystkimi otworami, gdzie montuje się systemy ochrony elektroniczne
NO-04-A004-2:2016 Wymagania techniczno-użytkowe (7 stron)	wymagania dot. ochrony systemów alarmowych w magazynach, pomieszczeniach wojskowych podlegających szczególnej ochronie z uwzględnieniem ich rodzajów	– wprowadza wymóg dwustopniowego sterowania pracą systemów alarmowych, – narzuca wymóg na pojemność pamięci zdarzeń przynajmniej na okres trzech miesięcy, – określa wymagania dot. linii dozorowych, testowania urządzeń, dopuszczalnego zmniejszenia zasięgu wykrywania itd., – wskazuje (bez wchodzenia w szczegóły) na wymagania dotyczące wytrzymałości na impulsy, wysokie napięcie, drgania itd., – brak odniesień do podziału na stop
NO-04-A004-3:2016 Metody określania liczby urządzeń (10 stron)	podział chronionych obiektów na trzy grupy w zależności od wagi tego, co ma być chronione	– brak w bibliografii powołania na normy PN-E-08390-1:1996, z której skopiowano i umieszczono w tym arkuszu kilka definicji. – narzuca liczbę i rodzaje czujek w zależności od powierzchni obiektów
NO-04-A004-4:2016 Wymagania dotyczące urządzeń zewnętrznych (12 stron)	podziały na strefy, klasyfikacje systemów wykrywania	– zawiera listę zalecanych do ochrony zewnętrznej czujek i systemów wraz z takimi parametrami jak długość strefy wykrywania, szerokość, wysokość itd.
NO-04-A004-5:2016 Wymagania dotyczące tablicy synoptycznej (5 stron)	wymagania dot. tablic synoptycznych wraz z definicją	– zawiera wymagania, co ma być na tablicy wskazywane i jakie kolory co sygnalizują
NO-04-A004-6:2016 Wymagania dotyczące systemów kontroli dostępu (12 stron)	wymagania środowiskowe i wymagania na zasilanie	– zawiera definicje oraz wymagania na czytniki, bramki, śluzy, drzwi, a także przepustowość i dopuszczalne błędne interpretacje, – zawiera wymagania konstrukcyjne i środowiskowe, – wymagania na zasilanie są rozszerzone w stosunku do wymagań w pozostałych arkuszach normy
NO-04-A004-7:2016 Wymagania dotyczące telewizyjnych systemów nadzoru (17 stron)	m.in. wymagania na zasilanie	– normy serii PN EN łącznie zawierają ponad 1100 stron, co po porównaniu ze 17 stronami arkusza 7 NO wskazuje, że wymagania ustanowione przez wojsko są bardzo ograniczone
NO-04-A004-8:2016 Eksploatacja (30 stron)	definicje dla garnizonowego, lokalnego i oddalonego centrum monitorowania, a także wymagania dot. podmiotów gospodarczych realizujących zadania w zakresie ochrony fizycznej	– zawarte są wymagania dla trzeciego rodzaju centrów monitorowania, tzw. oddalonych centrów monitorowania prowadzonych przez podmioty gospodarcze świadczące usługi na rzecz wojska
NO-04-A009:2017 Zabezpieczenia mechaniczne i ogrodzenia. Wymagania ogólne	definicje zabezpieczeń mechanicznych, ich klasyfikacja, wymagania w zależności od miejsc stosowania zabezpieczeń, m.in. drzwi, okien, płotów, bram, barier zaporowych itp.	– są zawarte wymagania dot. klas zabezpieczeń w zależności od strefy, w której mają być montowane

W normach serii PN EN 50131 w klasyfikacjach systemów występują także kategorie wymagań dla obiektów militarnych. Przy tworzeniu Norm Obronnych nie można więc wyważać otwartych drzwi, tylko skorzystać z istniejących zapisów. W przypadku omawianych tu NO skorzystano z tej możliwości w minimalnym stopniu:

- skopiowano co prawda wymagania na zasilanie, ale z wycofanej dziewięć lat temu normy PN E 08390, a nie z aktualnych norm serii PN EN 50131. Znacznie ogranicza to zatem możliwość wyboru centralek alarmowych tylko do tych, które spełniają stare (sprzed wielu lat), a nie najnowsze wymagania co do zasilania,
- zgubiono przy tym kopiowaniu wymagań co do zasilania bardzo istotny zapis, a mianowicie wymagania na czas pełnego nała-

[5] Trzeci rodzaj centrum monitorowania pojawia się w arkuszu dziewiątym NO pod nazwą „oddalone centrum monitorowania" i dotyczy centrum komercyjnego.

[6] Wymagania dla „strefy wewnętrznej" pokrywają się z wymogiem wykrywania agresji na wszystkie otwory z normą PN EN 50131-7 Grade 3.

dowania się akumulatorów rozładowanych po zaniku zasilania sieciowego,
- pominięto, poza jednym przypadkiem przycisków napadowych[7], możliwość stosowania urządzeń zasilanych tylko z baterii,
- nie przewidziano stosowania systemów bezprzewodowych, a przecież są od wielu lat oferowane systemy spełniające wysokie wymagania „cywilnej" klasy Grade 3 (stopnia zabezpieczeń 3), czyli odpowiedniej dla wojska,
- wymagania środowiskowe zawarte w NO tylko w jednej z czterech kategorii są tożsame z wymaganiami norm PN EN. Wywołuje to problemy przy doborze urządzeń pracujących w wojsku, ponieważ większość urządzeń dostępnych na rynku jest klasyfikowana wg wymagań norm PN EN.

Nie „zauważono" w NO zapisów PN EN dotyczących zmienności stref czułości czujek i ich sposobów testowania, tworząc wymagania, które w wielu punktach budzą wątpliwości.

Pozytywy

Dobrze się stało, że podjęto próbę opracowania dokumentów – w postaci norm mających za zadanie uporządkować i ułatwić zarówno projektowanie, jak i użytkowanie, a więc także konserwację systemów alarmowych i zabezpieczeń mechanicznych. Bardzo ważne są zapisy w NO dotyczące systemów ochrony na zewnątrz budynków, ponieważ normy serii PN-EN zawierają tylko wymagania dla systemów pracujących wewnątrz obiektów. Co prawda klasy środowiskowe III i IV w normach serii PN EN dotyczą urządzeń pracujących na zewnątrz obiektów, ale brakuje wymagań i metod testowania czujek i systemów wykrywających przeznaczonych z zasady do pracy na zewnątrz.

Bardzo pożyteczne są zapisy zawarte w:
- arkuszu 8 NO – resursy urządzeń (tylko kilka drobnych błędów) oraz harmonogramy konserwacji i przeglądów,
- arkuszu 4 NO – wymagania dotyczące systemów zewnętrznych.

Problemy i wątpliwości

Twórcy omawianych norm mieli już na starcie pewne ograniczenia, których nie do końca potrafili pokonać. W polskim prawie istnieje zapis wykluczający powoływanie się w dokumentach państwowych na dokumenty w innym języku niż polski. Oznacza to, że normy wprowadzone do spisu polskich norm jako tzw. normy okładkowe (czyli z przetłumaczoną tylko pierwszą stroną, ale z zawartością w języku angielskim) nie mogą być jako normy powoływane.

Obecnie z ponad stu norm dotyczących elektronicznych systemów zabezpieczeń przetłumaczono na język polski tylko niecałe dwadzieścia. Tak więc baza, którą można zgodnie z prawem cytować, jest bardzo ograniczona. Można było tę barierę ominąć, wybierając fragmenty wymagań i wskazując wymagane prawem autorskim źródła, z których one pochodzą, bez odwoływania się do normy jako całości. Nie wykorzystano tej możliwości w pełni. Pojawia się pytanie, dlaczego tylko niewielki procent norm został przetłumaczony. Przez sześć lat uczestniczyłem w pracach komitetów technicznych KT52 i KT306 PKN. Zrezygnowałem z nich, ponieważ mimo że wchodziły nowe normy europejskie dotyczące ochrony, proces ich tłumaczenia praktycznie został zawieszony. Z każdym rokiem rosną więc zaległości w tłumaczeniu norm.

To jedna z przyczyn, które mogły wpłynąć na kształt Norm Obronnych. Nie omówię wszystkich wątpliwości, które zostały zauważone w normach. Zajęłoby to nawet kilkadziesiąt stron[8], ponieważ wątpliwy zapis wymaga wytłumaczenia, dlaczego jest błędny. Wskażę przykładowo kilka zapisów w kilku grupach wątpliwości.

Omawiane Normy Obronne zawierają zróżnicowany poziom wiedzy – od fragmentów cennych i na wysokim poziomie po zapisy, które powinny być skorygowane.

Deklaracje i „zawieszone" definicje

- W arkuszu 8 zawarty jest, jako dokument alternatywny, wymóg „świadectwa kwalifikacyjnego". Może się okazać, że zapis ten jest „wskazaniem produktu" konkretnej firmy, która jako jedyna wydaje takie dokumenty w Polsce.
- W arkuszu 2 pojawia się niewyjaśnione hasło, które nie ma odpowiednika w znanych normach: *automatyczną regulację tła szumowego w przypadku złych warunków atmosferycznych.*
- W normie NO-04-A009:2017 *Zabezpieczenia mechaniczne i ogrodzenia* w bibliografii powołano normę PN-EN 1303:2007 *Okucia budowlane – Wkładki bębenkowe do zamków – Wymagania*

[7] Ostrzegacz napadowy.

[8] W 2015 r. eksperci z PISA sformułowali zastrzeżenia do zapisów w Normach Obronnych na 24 stronach, większość zastrzeżeń została odrzucona przez Wojskowy Komitet Normalizacyjny (WKN).

i metody badań, lecz w tabelach wymagań nie ma odwołań do wkładek i ich klasyfikacji.

„Zagubienia" wymagań

- **Wymagania na zasilanie** – powtarzane w kilku arkuszach NO zostały zaczerpnięte praktycznie dosłownie z norm wycofanych dziesięć lat temu, przy czym kopiując wymagania, „zgubiono" bardzo istotny zapis określający czas naładowania akumulatorów. Zapis ten istniał w wycofanych już normach, znalazł się też w zmienionym brzmieniu w aktualnych normach serii PN EN. Uważam ten błąd w NO za bardzo groźny.
- Zapis w normie: *W przypadku uszkodzenia systemów alarmowych naprawa ich powinna być podjęta w czasie nie dłuższym niż 4 h…* wydaje się logiczny, ale bez określenia dopuszczalnego czasu naprawy (i co należy zrobić, gdy się przedłuża) naprawa może trwać miesiącami[9].

Odwołania do nieistniejących klasyfikacji

- Wymagania na szyby w normie NO-04-A009:2017 – *Zabezpieczenia mechaniczne i ogrodzenia. Wymagania ogólne – Wymagania na szyby – Klasy 01-P2A*. Otóż klasyfikacja 01 szyb nie występuje od ponad osiemnastu lat, znikła w chwili pojawienia się klasyfikacji P2A, więc albo powołujemy się na klasy 01 do P2 z zaznaczeniem nieaktualności normy, albo jeśli jest zapis P2A, rezygnujemy z klasyfikacji 01[10]. Wprowadzenie klasy 01 jest wg mnie błędem.

Nieprecyzyjne wymagania

- Nie jest zrozumiały zapis – i to w kilku miejscach – co do klasy szczelności i wodoodporności obudów kamer: *Zaleca się stosowanie obudów IP 65 i IP 66, a w warunkach dużej wilgotności IP 67 lub IP 68*. Z wymagań na klasę obudowy wynika, że klasa IP 65 jest wystarczająca nawet w miejscach bezpośredniego wystawienia kamer na deszcz. Obudowa o klasie IP 66 zabezpiecza kamerę nawet przed **silnym strumieniem wody**, natomiast klasy IP67 i IP68 dotyczą kamer zanurzanych w wodzie. Większość kamer w obudowach klasy IP65 będzie pracowała poprawnie, a w obudowach IP66 nawet w silnych strugach wody. Co więcej, w zacytowanym zdaniu raz występuje spójnik „i", raz „lub" (z których pierwszy oznacza „i to, i to", a drugi „to lub to") – w obu miejscach wg mnie powinno być „**lub**".
- Cytat: *Pkt 3.3 System alarmowy w strefie zewnętrznej obwodowej powinien wykrywać: poruszanie się w strefie chronionej…*

W przypadku czujek ruchu mogą występować różne wymagania co do wykrywania ruchu w zależności od:
– pozycji (postawy) osoby poruszającej się,
– szybkości poruszania, i to zarówno minimalnej, a już wykrywanej, jak i maksymalnej jeszcze wykrywanej
– rodzaju obiektu, np. typowa sylwetka człowieka, pojazd, koty, psy, ptaki, fruwające śmieci itd.,
i dopiero na ich podstawie można ustalić dokładnie wymagania na wykrywanie poruszania się. Przykładowo bariera mikrofalowa może mieć zasięg:
– 500 m przy sylwetce wyprostowanej,
– 300 m przy sylwetce pochylonej,
– 150 m, gdy osoba czołga się.
Tak ogólnikowy wymóg zapisany w normie może być dowolnie interpretowany.

Umieszczenie w normie wymagań dot. urządzeń, których użytkowanie jest już mało prawdopodobne

W systemach telewizji dozorowej dziś nie używa się już multiplekserów, przełączników wizji i magnetowidów, a w NO takie urządzenia wciąż występują. Przy narzuconych na nie resursach jest mało prawdopodobne, aby obecnie mogły być użytkowane zgodnie z wymaganiami.

Nadmierne, niepotrzebne wymagania

1. W algorytmach czynności dotyczących sprawdzania funkcjonowania kamery (załącznik D) jest zapis o sprawdzaniu stanu wnętrza kamery. To wymaganie uważam za ryzykowne, a wręcz niepotrzebne. Wielokrotne otwieranie kamery, która pracuje poprawnie, wprowadza ryzyko złego skręcenia obudowy lub jej rozszczelnienia.
2. W załączniku F jest wymóg, aby sprawdzać odporność centralki na zmianę polaryzacji. Takie sprawdzenie systemu podczas pierwszego przyjmowania jest uzasadnione, ale jego powtarzanie, gdy w systemie nic nie było zmieniane, wydaje się pozbawione sensu.

> Normy powinny jeszcze raz przejść procedury konsultacji – jest do nich zbyt wiele wątpliwości.

Klasyfikacja urządzeń a resursy

Dwa zapisy: „**Kamery TV**" – i przedział pracy od 5 do 7 lat oraz „**Cyfrowe wizyjne detektory ruchu**" – resurs od 10 do 15 lat są sprzeczne, ponieważ detekcja ruchu:
– może być zaimplementowana w oprogramowaniu kamery, a więc odbywać się w kamerze,
– lub może odbywać się już przy zapisie sygnałów, a więc poza kamerą.

Wątpliwości merytoryczne

1. *W celu wyeliminowania odblasków światła na szybach, ścianach lub na podłodze ochranianych pomieszczeń należy stosować filtry polaryzacyjne…* – ten wymóg w większości sytuacji jest pozbawiony sensu, ponieważ filtry polaryzacyjne ustawia się za każdym razem do konkretnego oświetlenia padającego z konkretnego, niezmieniającego się kierunku, a większość kamer jest w zasięgu wędrującego światła słonecznego.
2. W normie dotyczącej zabezpieczeń mechanicznych nie zachowano zasady mówiącej, że *o wytrzymałości łańcucha decyduje jego najsłabsze ogniwo* – przykład w tabeli B.1 wymagania na drzwi to klasa RC-3 – wg norm PN EN dla tej klasy równoważną szybą jest szyba klasy P5A, a nie klasa P2A.
3. W tej samej normie zawarto wymagania na zamki, ale zapomniano, że są także zamki z wkładkami i one też powinny mieć podaną klasę ze wskazaniem normy.

BIO

Stefan Jerzy Siudalski
Autor ponad 340 artykułów i 8 książek oraz ponad 200 opinii (dla ubezpieczycieli, agencji ochrony i sądów) nt. systemów ochrony. Przez ponad 27 lat był biegłym sądowym z dziedziny systemów alarmowych i systemów ochrony. Szkolił agentów ochrony, instalatorów systemów i inwestorów.

[9] Znam takie przypadki z sali sądowej.
[10] W domyśle także 02.

Promienniki podczerwieni w systemach CCTV

Błogosławieństwo czy przekleństwo instalatorów Cz.1

Oświetlacze podczerwieni zaczynały swoją karierę w telewizji dozorowej kilkanaście lat temu. Od tego czasu technologia w tej dziedzinie ogromnie się rozwinęła i wydawałoby się, że zestaw promiennik oraz kamera nie powinien sprawiać instalatorom żadnych problemów. **Praktyka wskazuje jednak na coś innego. Wielu współcześnie budowanym systemom telewizji dozorowej promiennik zdaje się bardziej przeszkadzać, niż pomagać.**

Maciej Grzondkowski

Możliwość wykorzystania promienników podczerwieni opiera się na standardowej właściwości przetworników fotoelektrycznych (zarówno typu CCD, jak i CMOS) stosowanych we współczesnych kamerach CCTV. Czułość widmowa przetwornika nie ogranicza się bowiem do standardowego zakresu promieniowania widzialnego (od 400 do 700 nm), lecz jest znacznie szersza. Korzystając z tej cechy, można na planie obserwacyjnym zastosować niewidzialne dla ludzkiego oka, ale widzialne dla kamery promieniowanie z zakresu podczerwieni.

W odróżnieniu od konstrukcji sprzed kilku lat, kiedy to projektant lub instalator musiał dobierać odpowiedni typ kamery lepiej lub gorzej dostosowanej do pracy z podczerwienią, w zasadzie wszystkie obecnie produkowane kamery są w stanie efektywnie wykorzystywać promieniowane podczerwone. Co więcej, producenci opanowali do perfekcji wytwarzanie punktów kamerowych zintegrowanych z promiennikami IR, a to spowodowało, że współczesne systemy telewizji dozorowej praktycznie w 100% są oparte na takich konstrukcjach.

Wybór modeli, rodzaju obudów, sposobu ich montażu, miejsca zastosowania, parametrów i dostępnych funkcji jest bogaty. Projektant przystępujący do tworzenia koncepcji systemu wizyjnego nie powinien mieć najmniejszego problemu, aby dobrać odpowiedni typ do jego instalacji.
Na co więc powinien zwracać uwagę, aby nie popełnić błędu i stworzyć optymalny pod względem funkcjonalności i kosztów system CCTV? W artykule skupię się na kilku istotnych aspektach związanych z konstrukcją zintegrowanych punktów kamerowych oraz parametrach promienników podczerwieni. Wydaje się, że to właśnie one w największym stopniu decydują o ostatecznym powodzeniu projektu.

Parametry promiennika

Każdy promiennik charakteryzuje się kilkoma podstawowymi cechami (parametrami), na które należy zwrócić szczególną uwagę:

· Zasięg świecenia

Trzeba wiedzieć, co wpływa na zasięg świecenia promiennika i w jaki sposób jest on określany przez producentów. Wbrew utartym opiniom zasięg promiennika nie oznacza, że dany punkt kamerowy doskonale oświetli każdy plan czy obiekt na tym planie w zakresie podanym w karcie katalogowej. Mówi on natomiast o maksymalnej odległości, z jakiej ten konkretny punkt kamerowy będzie w stanie zaobserwować obiekt, którego powierzchnia czy materiał ma współczynnik odbicia (reflektancję) równy lub większy niż 90%. Taką wartość współczynnika odbicia ma np. biała ściana. Jeśli planem obserwacyjnym będzie ściana pomalowana na kolor ciemnoszary (współczynnik odbicia poniżej 30%), **to skuteczny zasięg świecenia zmniejszy się nawet o 50%**.
Brak tej wiedzy jest bardzo często powodem nieuzasadnionych reklamacji. Niejednokrotnie byłem świadkiem zarzutów instalatorów lub ostatecznych użytkowników, kiedy nieprawidłowo dobrana kamera (o zbyt małej mocy promiennika) nie była w stanie skutecznie oświetlić scen, na których były zlokalizowane ciemne obiekty typu asfalt, trawnik czy ściana z cegły. Po prostu zasięg promiennika dobierano do projektu z kart katalogowych, nie uwzględniając współczynnika odbicia, jakim charakteryzuje się dany obiekt na planie.

· Kąt świecenia

To niezwykle istotny parametr, mówiący o tym, w jakim kącie przestrzennym dany promiennik będzie emitował podczerwień. Kąt świecenia powinien być zbliżony do kąta widzenia kamery, aby promiennik możliwie równomiernie oświetlał plan obserwacyjny. Niestety ten parametr jest bardzo rzadko podawany przez producentów, a bez specjalistycznego sprzętu trudno go oszacować. Pozostaje jedynie zaufać wytwórcom, że kąt świecenia zestawu diod został prawidłowo dobrany do danego rodzaju kamery i użytego obiektywu.
Trzeba pamiętać, że im dłuższa ogniskowa, tym zazwyczaj węższy kąt świecenia promiennika. I odwrotnie, krótka ogniskowa powinna współgrać z szeroko świecącym promiennikiem. Aczkolwiek nie zawsze jest to regułą. Gdy nie jesteśmy pewni parametrów, przed ostatecznym montażem warto przeprowadzić test na planie pozwalający stwierdzić, czy zastosowany promiennik ma dostatecznie szeroki lub wąski kąt świecenia i czy pokrywa się on z kątem widzenia kamery.
Takie testy powinniśmy przeprowadzić, jeśli zamierzamy stosować kamery ze zmienną ogniskową. Promienniki zazwyczaj mają konkretny kąt świecenia, który nie będzie się zmieniał wraz ze zmianą ogniskowej i kąta widzenia kamery. Można przyjąć z dużym prawdopodobieństwem, że promiennik będzie ustawiony na wartość średnią i pokryje plan obserwacyjny dla obiektywów z ogniskową 4–6 mm. Stąd dla ogniskowych krótszych uzyskamy prawdopodobnie silnie oświetlone centrum kadru i niedoświetlone krawędzie (*fot. 1*).
Warto również pamiętać o pewnej zależności, która występuje w większości obecnie produkowanych punktów kamerowych. Szeroki kąt świecenia oznacza zazwyczaj mniejszy zasięg. I odwrotnie, daleki zasięg świecenia oznacza wąski kąt (*fot. 2*). Aczkolwiek na rynku są dostępne także konstrukcje punktów ka-

fot. 1 **Kamera ze zbyt wąskim kątem świecenia**

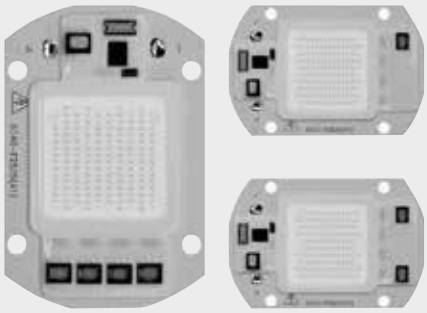
fot. 2 **Efekt latarki**

fot. 3 **Promiennik sprzężony z obiektywem**

fot. 5 **Kamera z sekcją diod LED szerokokątnych**

fot. 7 **Miniaturowa kamera z diodami COB**

fot. 4 **SMD LED**



fot. 6 **COB LED**

fot. 8 **Diody LED dużej mocy z soczewką**

merowych, w szczególności kamer typu PTZ, w których, w zależności od zbliżenia optycznego obiektywu, są włączane lub wyłączane dane sekcje diod w promienniku. Przy kącie szerokim świecą diody szerokokątne, a przy dużym zbliżeniu świeci sekcja silnych diod o skupionej wiązce. Ciekawe rozwiązania spotyka się również w niektórych kamerach stacjonarnych, np. obiektyw jest mechanicznie zsynchronizowany z soczewką promiennika. Niestety jest to funkcja dostępna w droższych modelach (*fot. 3*).

· Żywotność

Wszystkie źródła światła, nawet współczesne bardzo trwałe diody LED, mają ograniczoną żywotność. W zależności od użytej technologii typowy okres pracy waha się od 10 tys. do 30 tys. godz. Konstrukcje tańsze, zazwyczaj bardziej „wysilone", rzadko są w stanie pracować dłużej niż 2 lata, konstrukcje zaawansowane z kontrolą prądu pracy diod osiągają swoje maksima w okresie od 3 do 5 lat, przy założeniu typowych warunków pracy promienników, kiedy diody są załączane średnio na 50% czasu na dobę. Gdy kamery pracują np. w ciemnych pomieszczeniach i promienniki świecą ciągle, zdarza się, że wymagają wymiany już po 10–12 miesiącach pracy.

Wraz z dłuższym czasem świecenia strumień świetlny diod ulega zmniejszeniu (diody wypalają się), a co za tym idzie – zasięg promiennika zdecydowanie spada. Ten efekt jest doskonale znany każdemu właścicielowi samochodu, kiedy w reflektorach są zamontowane jednocześnie stare i nowe żarówki. Należy go uwzględniać na etapie projektu – mając plan o wielkości np. 20 m, warto zainwestować w promiennik o zasięgu 30 m, aby po kilkunastu miesiącach pracy nadal móc skutecznie oświetlić scenę!

· Zakres widmowy promieniowania IR

W większości przypadków stosuje się diody emitujące podczerwień o długości fali ok. 880 nm. Jest to tzw. bliska podczerwień niewidoczna dla ludzkiego oka, ale jednak jesteśmy w stanie dostrzec działające diody LED w kamerze. Dlatego gdy projektantowi zależy na wyjątkowej dyskrecji, stosuje się promienniki wykorzystujące podczerwień o długości fali 940 nm. W tym przypadku nie można już dostrzec nawet samych diod. Warto wówczas zwrócić uwagę na rodzaj kamer, gdyż niektóre konstrukcje mogą być zdecydowanie mniej czułe na ten zakres promieniowania lub wręcz go zupełnie nie widzieć.

Technologia i rodzaj użytych diod LED

Od kilku lat w ofercie producentów źródeł światła widać technologiczną zmianę pokoleniową z lamp tradycyjnych żarowych lub wyładowczych na półprzewodnikowe (LED). Diody LED jeszcze niedawno spotykane tylko w specjalistycznych zastosowaniach zadomowiły się w naszym życiu jako wydajne i niezawodne źródła światła. Również branża security nie oparła się tym zmianom i współczesne punkty kamerowe są wyposażane w najnowsze typy diod LED, które różnią się:

· rodzajem złącza emisyjnego i jego konstrukcją

Można wyróżnić dwie główne grupy:

– pojedyncze diody SMD (*fot. 4, fot. 5*). Takie rozwiązanie ma dwie ważne zalety. Pierwszą jest możliwość precyzyjnego tworzenia wiązki świetlnej poprzez dobór różnych typów diod i ich układu, drugą – zdecydowanie większa niezawodność. Tego typu zestaw jest bardzo dobrym rozwiązaniem pozwalającym uzyskać szerokie kąty świecenia przy zachowaniu wysokiej równomierności oświetlenia sceny;

– moduły typu COB *(chip-on-board)* (*fot. 6*). To rozwiązanie wygodne, gdy chcemy uzyskać daleki zasięg świece-

fot. 9 **Diody COB dużej mocy**

fot. 11 **Diody z odbłyśnikiem w obudowie typu *flat-face***

fot. 10 **Promiennik z odbłyśnikiem**

Diody LED, jeszcze niedawno spotykane tylko w specjalistycznych zastosowaniach, zadomowiły się jako wydajne i niezawodne źródła światła również w branży security.

nia, wykorzystując efektywne źródło podczerwieni oraz w przypadku miniaturyzacji samej kamery (*fot. 7*).

· typem zastosowanej optyki

W tym przypadku wyróżnikiem jest rodzaj układu optycznego, który odpowiednio kieruje promieniowane emitowane ze złącza diody.

Producenci najczęściej korzystają z dwóch rozwiązań – soczewek zintegrowanych z pojedynczą diodą (*fot. 8*) oraz układów z odbłyśnikami i modułami typu COB (*fot. 9 i fot. 10*). Wybór jest duży, warto więc dokładnie zapoznać się z kartami katalogowymi danego urządzenia, gdyż każda z tych technologii oferuje inne funkcjonalności, a co za tym idzie ma unikalne zalety, ale również wady.

Na przykład stosowane od kilku lat moduły COB z dedykowanymi odbłyśnikami prostokątnymi mają bardzo równomierny rozkład strumienia świetlnego w całym zaprojektowanym kącie świecenia, ale w przypadku złego dopasowania odbłyśnika do użytego obiektywu tworzą bardzo wyraźny efekt latarki w centrum kadru i wyraźnie niedoświetlone krawędzie obrazu. Efekt jest szczególnie widoczny, gdy kamera została wyposażona w obiektyw o bardzo szerokim kącie widzenia (powyżej 80 stopni).

Stosowanie diod o dedykowanej optyce wymogło na producentach skonstruowanie innych rodzajów obudów (*fot. 11*), ale w tym przypadku okazało się to korzystne dla takiej konstrukcji, gdyż zdecydowanie ograniczyło poświatę i odblaski powstające podczas pracy promiennika zamontowanego w tradycyjnych obudowach kopułowych lub cylindrycznych.

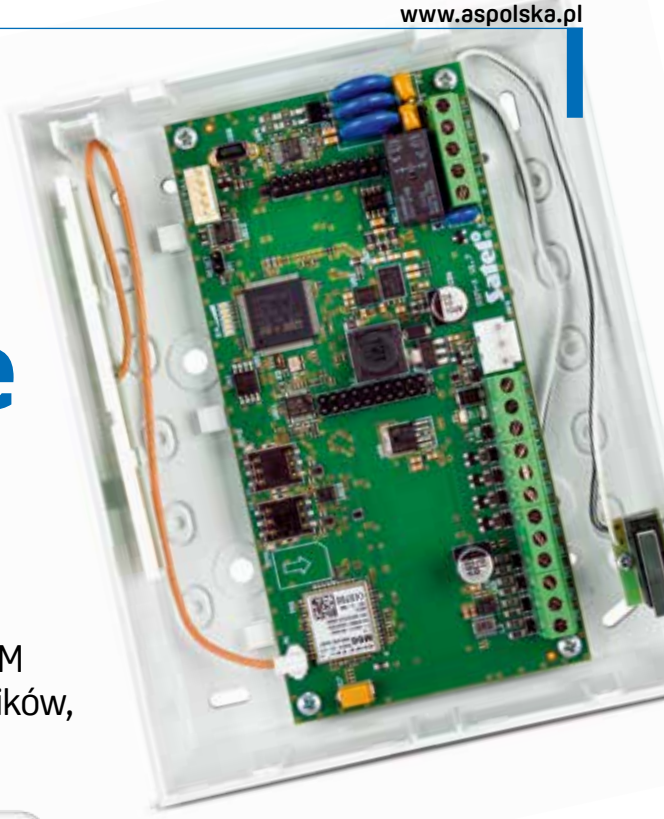
Od kilku lat na rynku, głównie w przypadku promienników o zasięgu przekraczającym 100 m, stosuje się również oświetlacze wykorzystujące światło laserowe. Ze względu na łatwość tworzenia wiązki świetlnej rozwiązanie to jest szczególnie popularne w zaawansowanych kamerach PTZ. Należy jedynie pamiętać o prawidłowym oznakowaniu takich punktów kamerowych, gdyż stosowanie światła laserowego o tak dużych mocach może być szkodliwe dla osób i zwierząt przebywających na planie.

W kolejnej części więcej o rodzajach kamer z promiennikami, ich miejscu montażu oraz najczęściej spotykanych problemach, jakie zdarzają się na instalacjach wykorzystujących podczerwień.

BIO

Maciej Grzondkowski
W branży security od ponad 17 lat, związany przede wszystkim z systemami wizyjnymi. Wdrożył wiele produktów i linii produktowych na rynek krajowy. Krzewi dobre zasady projektowania oświetlenia w systemach telewizji dozorowej.

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



Nowe moduły komunikacyjne SATEL

W drugiej połowie lutego 2018 r. SATEL wprowadził na rynek urządzenia GSM-X oraz GPRS-A zastępujące dotychczasową grupę modułów komunikacyjnych GSM i GPRS. Nowe modele łączą funkcjonalności poprzedników, oferując przy tym wiele dodatkowych, ciekawych rozwiązań.

Bartosz Piotrowski
ekspert ds. technicznych **SATEL**

Tym, co łączy obie nowości, jest możliwość współpracy z dowolnymi centralami alarmowymi, realizacji monitoringu, powiadamiania oraz zdalnego sterowania, np. czuwaniem systemu alarmowego czy funkcjami automatyki budynkowej. Co jeszcze kryją nowe produkty SATEL?

Uniwersalny moduł monitorujący

GPRS-A to moduł, który może monitorować szeroki zakres czujników: NO, NC i analogowych. Posiada też magistralę 1-Wire dla czujników temperatury. Może on automatycznie reagować na przekroczenie zaprogramowanych limitów monitorowanych wartości, zmieniając stan swoich wyjść i/lub informując o takim zdarzeniu. Zgodnie z koncepcją Internetu Rzeczy zbierane przez moduł dane mogą być przesyłane do innych urządzeń. Informacje te są przekazywane przez GPRS z użyciem otwartych protokołów MQTT, JSON lub MODBUS RTU. Mogą być przetwarzane, gromadzone i wizualizowane zarówno w rozwiązaniach dostępnych na rynku, jak i w aplikacjach tworzonych od podstaw. Wgląd w dane zbierane z wielu modułów zamontowanych w różnych obiektach może być przydatny np. przy nadzorowaniu farmy wiatrowej.

Uniwersalny moduł komunikacyjny...

GSM-X, w odróżnieniu od GPRS-A, ma wbudowany moduł głosowy, dzięki czemu może prowadzić monitoring i powiadamianie także torem *audio*. Moduł ten może pracować jako bramka GSM, a także stanowić zapasowy tor łączności na wypadek awarii naziemnej linii telefonicznej. Może być zastosowany jako modem do central INTEGRA lub odbiornik stacji monitorującej STAM-2. Urządzenie ma dwa gniazda kart nano-SIM – w przypadku problemów z siecią operatora pierwszej karty moduł automatycznie przełącza się na drugą, zachowując ciągłość komunikacji.

...i jego rozszerzenie

Do GSM-X można dołączyć dedykowany moduł ethernetowy GSM-X-ETH, uzyskując w ten sposób dodatkowy kanał komunikacji – sieć Ethernet. Takie rozwiązanie umożliwia realizację niezwykle skutecznego monitoringu dwutorowego (*Dual Path Reporting*; zgodnie z wymaganiami kategorii DP4 normy EN 50136), wymaganego w obiektach o najwyższym stopniu zabezpieczenia, takich jak banki, infrastruktura krytyczna itp.

Zdalna konfiguracja i aktualizacja urządzeń

Nowe urządzenia konfiguruje się z użyciem programu GX Soft posiadającego przejrzysty i intuicyjny interfejs. Z jego poziomu jest też dostępne sterowanie wyjściami modułów oraz blokowanie ich wejść.
Komunikacja z modułami, zarówno na czas programowania, jak i aktualizacji firmware'u przez program UpServ może odbywać się zdalnie. Instalator może dzięki temu przeprowadzić natychmiastową kontrolę stanu urządzeń i niezwłocznie zmodyfikować ustawienia lub zaktualizować oprogramowanie, bez konieczności dojazdu do obiektu.

Aplikacja na iOS i Android

Do współpracy z nowymi modułami komunikacyjnymi SATEL została stworzona aplikacja GX CONTROL. Za jej pomocą można sterować wyjściami modułów (kontrolować podłączone do nich urządzenia lub instalacje), sprawdzać stan wejść i wyjść czy przeglądać zapisane zdarzenia wewnętrzne modułów. Służy ona także do konfiguracji powiadomień *push*, informujących użytkownika urządzenia mobilnego o zdarzeniach.

Satel®
MADE TO PROTECT

NOWE MODUŁY KOMUNIKACYJNE

współpracują z dowolną centralą alarmową i obsługują wiele torów transmisji.

GPRS-A

uniwersalny moduł monitorujący

GSM-X

uniwersalny, wielozadaniowy moduł komunikacyjny

Oferują pewność powiadamiania i skuteczny monitoring, zdalne sterowanie z aplikacji mobilnej **GX CONTROL** oraz wiele innych ciekawych funkcji.

Wśród nich:

- Dual Path Reporting oraz funkcja bramki GSM (GSM-X)
- Obsługa sygnałów analogowych oraz cyfrowych czujników temperatury 1-Wire (GPRS-A)

Program **GX Soft** z intuicyjnym i przejrzystym interfejsem umożliwia sprawną konfigurację modułów.

www.**satel**.pl

Hikvision Poland
ul. Krakowiaków 50, 02-255 Warszawa
tel. 22 460 01 50, faks 22 464 32 11
e-mail: info.pl@hikvision.com

CASE STUDY

Nowoczesny dozór Politechniki Białostockiej

Planując modernizację systemu dozoru wizyjnego uczelni, władze Politechniki Białostockiej stanęły przed trudnym zadaniem. Obiekty są rozproszone na dużym obszarze i zlokalizowane w kilku oddalonych od siebie miejscach.

W skład kampusu wchodzi 14 budynków w Białymstoku, w tym m.in. rektorat, klub studencki, hala sportowa i akademiki, a także gmach Zamiejscowego Wydziału Leśnego w Hajnówce. Planowane jest również podłączenie do systemu kolejnych trzech budynków Wydziału Architektury w Białymstoku oraz czterech budynków Wydziału Zarządzania z Kleosinie.

Przed modernizacją

Zanim zdecydowano się na modernizację systemu dozoru wizyjnego, funkcjonowało wiele wydzielonych systemów z lokalną rejestracją. W kampusie Politechniki Białostockiej działało 46 kamer analogowych różnych producentów (m.in. Samsung i Sanyo), a także 72 kamery IP (m.in. Sanyo, Geovision, Acti i Novus). Dozór nie obejmował Wydziału Architektury oraz Zamiejscowego Wydziału Leśnego w Hajnówce.

Wraz z modernizacją i integracją urządzeń dozoru wizyjnego władze uczelni zaplanowały wdrożenie całodobowego dozoru straży akademickiej, która miałaby podgląd na wszystkie obiekty kampusu. Ze względu na duże rozproszenie geograficzne budynków istotną kwestią było również ujednolicenie zarządzania dozorem, pozwalając zmniejszyć obciążenia administracyjne związane z utrzymaniem systemów lokalnych i zarządzaniem nimi.

Wybór rozwiązania

Po przeprowadzeniu serii testów zdecydowano, że w tych warunkach najlepszą propozycją są rozwiązania firmy Hikvision. Dotychczasowy system został uzupełniony o 32 kamery stałopozycyjne

DS-2CD4A26FWD-IZS (2,8–12 mm), 9 kamer DS-2CD4A-25FWD-IZS (8–32 mm), 12 kamer DS-2CD4526FWD-IZS (2,8–12 mm) oraz 8 kamer obrotowych DS-2DF8223I-AEL. Ponadto system został wyposażony w dwa rejestratory DS-96128NI-F16 z obsługą macierzy RAID5 i pamięć dyskową (48 TB) oraz rejestratory, które integrują zainstalowane już kamery analogowe DS-7204HGHI-SH/A (5 szt.), DS-7208HGHI-SH/A (3 szt.) i DS-7216HGHI-SH/A (1 szt.). Na potrzeby Uczelnianej Straży Akademickiej do podglądu obrazów z kamer zainstalowano trzy dekodery DS-6408HDI-T oraz manipulator do obsługi kamer obrotowych DS-1100KI.

Komunikacja i integracja

Komunikacja pomiędzy urządzeniami jest oparta na istniejącej infrastrukturze teleinformatycznej i łączach światłowodowych, które są zarządzane i nadzorowane przez Centrum Komputerowych Sieci Rozległych Politechniki Białostockiej i operatora Miejskiej Sieci Komputerowej BIAMAN. Infrastruktura wykorzystuje 22 węzły sieciowe rozlokowane w obiektach kampusu. Do transmisji obrazów z kamer znajdujących się poza budynkami (pod zadaszonym ciągiem komunikacyjnym pomiędzy budynkami wydziałów oraz na słupach) wykorzystano 8 szaf dystrybucyjnych.

Zarządzanie systemem

Zarządzanie zostało ujednolicone i scentralizowane. Serwery znajdują się w serwerowni MSK BIAMAN wyposażonej w systemy kontroli dostępu, monitoringu wizyjnego, przeciwpożarowy oraz wczesnego wykrywania zalaniem wodą. Ciągłość gwarantowanego zasilania zapewniają system UPS i agregat prądotwórczy.
Poszczególne centra monitoringu są usytuowane w portierniach każdego wydziału, a główne centrum całodobowego nadzoru ze stanowiskami straży akademickiej mieści się w akademiku. Do podglądu obrazów w portierniach wydziałów wykorzystano komputery, w całodobowym centrum natomiast zastosowano dekodery sprzętowe odpowiedzialne za wyświetlanie strumieni wizyjnych na 19 monitorach.

Funkcje systemu

W rozległym i rozbudowanym systemie z tak dużą liczbą kamer (przekłada się to na dużą liczbę obserwowanych obrazów) operator centrum monitoringu nie jest w stanie wychwycić wszystkich zdarzeń. W tym celu wybrane kamery wyposażono w funkcje inteligentnej analizy wizyjnej, np. rozpoznawanie numerów tablic rejestracyjnych. W przyszłości może się okazać pomocna m.in. detekcja przekroczenia wirtualnej linii, która w znacznym stopniu ułatwi operatorowi wychwycenie zdarzeń związanych z aktami wandalizmu na ścianach budynków.
Pomocna może się okazać również funkcja detekcji twarzy, dzięki której proces poszukiwania potencjalnego sprawcy może się znacząco skrócić i ograniczyć do przeszukiwania galerii twarzy zamiast wielogodzinnego przeglądania nagranego materiału. W kamerach obrotowych sprawdzi się funkcjonalność automatycznego śledzenia obiektów będących w ruchu, potencjalnie wyłapując istotne zdarzenia – mówi Kamil Guryn z Centrum Komputerowych Sieci Rozległych Politechniki Białostockiej. Hikvision zaproponował rozwiązanie integrujące kamery analogowe oraz IP różnych producentów w spójny system. Dzięki temu stało się możliwe scentralizowane zarządzanie całym systemem oraz podgląd wszystkich obiektów Politechniki Białostockiej z jednego miejsca.
Zainstalowane kamery spełniają nasze oczekiwania. Mamy urządzenia działające sprawnie nawet w warunkach słabego oświetlenia. Dzięki technologii Darkfighter uzyskiwane obrazy są wyraźne i czytelne nawet w nocy. A wszystko to w konkurencyjnej cenie – dodaje Kamil Guryn.
Z kolei Łukasz Lik, dyrektor ds. technicznych w Hikvision Poland, podkreśla, że największym wyzwaniem w tym projekcie była integracja kamer innych producentów.
Nie korzystaliśmy tu z rozwiązań software'owych, a zdecydowaliśmy się zastosować rejestratory IP. Z tym zadaniem doskonale poradziły sobie nasze „Super NVR-y" DS-96128NI-F16. Duża liczba kanałów i szerokie pasmo wejściowe umożliwiają jednoczesne podłączenie nawet 128 kamer. Dzięki zintegrowaniu protokołów innych producentów, zgodności z Onvif i możliwości bezpośredniej implementacji strumienia RTSP udało nam się spiąć sygnały ze wszystkich kamer w jednym miejscu.

UTC Fire & Security Polska
ul. Sadowa 8, 80-771 Gdańsk
tel.: 58 301 38 31, 58 760 64 80, faks: 58 301 14 36
www.utcfssecurityproducts.pl, piotr.ejma-multanski@fs.utc.com

System zabezpieczeń technicznych

Lenel OnGuard cz. 1

Marka Lenel – jedna z najsilniejszych w segmencie tzw. korporacyjnych systemów zabezpieczeń *(enterprise security systems)* – **nie jest jeszcze znana na polskim rynku security.** Prezentację marki rozpoczynamy od jej historii, w kolejnych wydaniach przybliżymy charakterystykę rozwiązania i jego mocne strony oraz model dystrybucji i najnowsze propozycje.

Piotr Ejma-Multański
UTC Fire & Security Polska

W latach 80. XX w. zarówno systemy zarządzania bezpieczeństwem, jak i pozostałe systemy informatyczne były oparte głównie na minikomputerach, które zastąpiły komputery typu *mainframe*. Oprogramowanie użytkowe miało charakter zamknięty – było tworzone pod jednym systemem operacyjnym, dla konkretnego typu sterowników.

W tym okresie w USA powstała firma Lenel. Założyło ją w 1991 r. grono informatyków pochodzenia ukraińskiego. Ambicją firmy było opracowanie oprogramowania otwartego, współpracującego z urządzeniami obiektowymi wielu producentów. Zwieńczeniem starań było wprowadzenie w 1995 r. pierwszej wersji oprogramowania OnGuard®, opartego na relacyjnej bazie danych systemu zarządzania systemami KD i SWiN ze zintegrowaną telewizją dozorową.

W tym innowacyjnym rozwiązaniu wykorzystano kontrolery firmy Mercury oraz upubliczniony kod pozwalający na tworzenie interfejsów do kolejnych urządzeń. W 1998 r. powstał *Open Application Alliance Program* – system rejestracji, testowania i certyfikacji interfejsów między oprogramowaniem OnGuard a systemami innych producentów. Dzięki niemu Lenel ma największą na świecie bibliotekę interfejsów, dostępną w Internecie pod hasłem Lenel OAAP. W 2005 r. firma stała się częścią United Technologies, a marka Lenel – globalną marką koncernu, wzmocnioną po zakupie GE Security (właściciela m.in. Casi Rusco i Aritech).

Dzięki otwartej polityce i ciągłemu rozwojowi oprogramowania Lenel, z ponad 20 tys. wdrożeń, stał się głównym graczem na rynku amerykańskim, a potem światowym. Systemy Lenel OnGuard pracują w największych firmach informatycznych, konsultingowych i przemysłowych, w administracji publicznej i wojsku.

Do niedawna produkty Lenel były stosowane w Polsce i krajach ościennych jedynie przez firmy globalne, które podłączały przez sieć WAN do serwerów centralnego systemu nadzoru OnGuard na świecie urządzenia peryferyjne (czytniki, kamery, kontrolery itp.) w nowych zakładach czy biurowcach . Od kilku lat pojawiają się „lokalne" instalacje, realizowane przez polskie firmy. Złożyło się na to kilka czynników:

– transfer *know-how* i technologii do Europy, w tym do Polski. Od 2010 r. w Gdańsku działają Centrum Badań i Rozwoju oraz Dział Wsparcia Technicznego Lenel na Europę. Dzięki temu zarówno wiedza techniczna, jak i wsparcie oraz szkolenia są bardziej dostępne;
– obecność przeszkolonych polskich firm, certyfikowanych partnerów Lenela, potrafiących zrealizować wdrożenie „pod klucz";
– rosnące wymagania klientów poszukujących najlepszego rozwiązania na potrzeby swoich przedsiębiorstw.

UTC Fire & Security
A United Technologies Company

Marka Lenel jest częścią UTC Fire & Security Products

– światowej korporacji oferującej innowacyjne systemy zabezpieczeń elektronicznych służące do ochrony bezpieczeństwa ludzi, budynków, urządzeń i infrastruktury. UTC Fire & Security ma w swojej ofercie rozwiązania wykorzystywane do wykrywania pożarów, włamań i napadów oraz kontroli dostępu i dozoru wizyjnego.

UTC Fire & Security Products to część firmy UTC Climate, Controls & Security

– wiodącego producenta systemów bezpieczeństwa, automatyki budynkowej, klimatyzacji i ochrony pożarowej.

UTC CLIMATE, CONTROLS & SECURITY W LICZBACH

16 800 000 000 dolarów rocznego obrotu
201 000 pracowników w **70** krajach świata
53 000 pracowników
600 oddziałów
39 własnych zakładów
9 centrów badań

- Sercem systemu bezpieczeństwa **Lenel** jest komputerowe oprogramowanie **OnGuard®**, integrujące kompletny pakiet funkcji i technologii zabezpieczeń elektronicznych; kontroli dostępu, wydawania i personalizacji identyfikatorów, monitoringu alarmowego, identyfikacji opartej o karty typu smart oraz wzorce biometryczne, nadzoru wizyjnego, analityki obrazu w czasie rzeczywistym i połączenia z wieloma systemami innych producentów.
- Siłą **marki Lenel** jest globalna sieć autoryzowanych partnerów, tzw. VAR (Value added Reseller), stale szkolonych i podnoszących swoje kwalifikacje.
- Obecnie sieć liczy ponad **800** przedsiębiorstw, z czego około **200** w same Europie, a **5** w Polsce.
- Lenel, od lat wspiera otwartość rozwiązań informatycznych i publikuje dokumentację pozwalającą na tworzenie interfejsów do **systemu OnGuard® (API)**.
- W ramach programu **OpenAccess Alliance (OAAP)**, działającego od roku 1998, każdy dostawca może stworzyć interfejs do swojego systemu, a następnie przedłożyć go w celu sprawdzenia i certyfikacji przez **markę Lenel**.

REGIONAL SALES MANAGER LENEL
UTC CLIMATE, CONTROLS & SECURITY | FIRE & SECURITY PRODUCTS
Mobile +48 691 04 05 64 | Email piotr.ejma-multanski@fs.utc.com

LENEL
United Technologies

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

PROTEGE GX

Zintegrowany system zarządzania bezpieczeństwem klasy Enterprise

PROTEGE GX jest przeznaczony do obiektów różnej skali – od najmniejszych, po rozbudowane i rozległe systemy pracujące w wielu lokalizacjach. Należy do grupy systemów SMS (*Security Management Systems*), ale wyróżnia go podstawowa i bardzo istotna zaleta – sprzętowa realizacja zadań.

PROTEGE GX jest systemem bezpieczeństwa i automatyki składającym się z oprogramowania i urządzeń. Oferuje szeroką funkcjonalność, na którą składają się: kontrola dostępu, sygnalizacja włamania i napadu, telewizja dozorowa, automatyka budynkowa, komunikacja interkomowa, rejestracja czasu pracy, rejestracja gości, zarządzanie windami, obsługa urządzeń biometrycznych SUPREMA, integracja urządzeń bezprzewodowych INOVONICS, integracja czujek REDWALL/REDSCAN.

Oprócz wymienionych funkcjonalności umożliwia on także integrację z wieloma systemami i urządzeniami innych producentów. Są to:

- Zewnętrzne systemy BMS
- Systemy zamków offline (np. Salto Sallis, ASSA Abloy Aperio, Kaba Cencon)
- Systemy CCTV wielu producentów
- Systemy interkomowe SIP wielu producentów
- Bezpośrednia integracja z systemami zarządzania windami OTIS, KONE, Schindler i Thyssen Krupp
- Modbus
- *Automation & Control Protocol*
- *Data Sync* – integracja baz danych
- WebSOAP
- MSMQ (*Microsoft Message Queue*)
- *Active Directory* (LDAP)

Cechą charakterystyczną systemu i wyróżniającą go na tle innych dostępnych na rynku rozwiązań jest sprzętowa realizacja zadań. Polega ona na zapewnieniu użytkownikowi pełnej funkcjonalności systemu na poziomie urządzeń (kontrolerów). Dzięki takiemu rozwiązaniu system działa (udziela dostępu, zabezpiecza strefy alarmowe, steruje windami, zapewnia integrację z CCTV, BMS itp.) bez udziału serwera i oprogramowania.
Możliwość stosowania szerokiej gamy urządzeń, w tym kontrolerów z pełną funkcjonalnością pracy offline, pozwala na stworzenie systemu zabezpieczeń, który może pracować nieprzerwanie dzięki w pełni rozproszonej logice. Dopóki pojedynczy kontroler będzie działał, dopóty elementy do niego podłączone będą spełniały swoje zadanie.

Ta unikalna właściwość PROTEGE GX rozwiązuje bardzo ważny problem, z którym często spotykają się użytkownicy innych systemów. Jego działanie jest stale zapewnione, niezależnie od infrastruktury IT czy też sprzętu komputerowego i oprogramowania.
Oprogramowanie systemu PROTEGE GX pozwala na aktywne oraz intuicyjne zarządzanie systemem. Występuje ono zarówno w wersji aplikacji dla systemu Windows, jak i w formie interfejsu WEB dostępnego za pośrednictwem przeglądarki internetowej. Umożliwia łatwe dopasowanie wyświetlanych treści w zależności od zalogowanego użytkownika. Nawet podstawowe wersje oprogramowania oferują więcej niż systemy klasy Enterprise. To, a także brak kosztów związanych z aktualizacją oprogramowania sprawia, że całkowity koszt posiadania i utrzymania systemu jest niezwykle niski.

Do systemu dostępna jest aplikacja na smartfony i tablety, działająca na systemach zarówno Android, jak i iOS. Pozwala ona na łatwą obsługę systemu z dowolnego miejsca. Aplikacja oferuje powiadomienia *push*, dzięki którym użytkownik jest na bieżąco informowany o najważniejszych zdarzeniach w systemie. Aplikacja zawiera również mobilny identyfikator, umożliwiający identyfikację użytkownika na czytnikach Bluetooth/NFC dostępnych dla systemu PROTEGE.
Skalowalność systemu jest jednym z jego atutów. Pojedynczy kontroler systemowy może obsłużyć nawet 5 mln użytkowników, 248 przejść kontroli dostępu, ponad 5 tys. wejść alarmowych, 200 klawiatur itd. Liczba takich kontrolerów w systemie jest nieograniczona. Nielimitowana liczba stref, poziomów dostępu, kontrolerów w systemie, a także globalny i lokalny *anti-pass back* sprawiają, że wielkość systemu jest nieograniczona.

System PROTEGE GX jest zgodny z wymaganiami normy PN-EN50131 stopień zabezpieczenia 3 (SSWiN) oraz EN50133 Klasa Rozpoznania 2 (czytniki bez klawiatury), Klasa Rozpoznania 3 (czytniki z klawiaturą), Klasa Dostępu B (KD).

urmet
MIWI

IndigoVision

Zintegrowany System Video IP

Miwi Urmet Sp. z o.o. | 91-341 Łódź, ul. Pojezierska 90 A
tel: 42 616 21 00 | miwi@miwiurmet.pl

www.miwiurmet.pl

Bosch Security Systems
ul. Jutrzenki 105, 02-231 Warszawa
tel. 22 715 41 00
www.pl.boschsecurity.com/pl/

REMOTE SERVICES

USŁUGI ZDALNEGO NADZORU I KONSERWACJI

Koncepcja Internetu Rzeczy podlega dynamicznemu rozwojowi i obejmuje coraz szerzy zakres urządzeń. Inteligentne domy, urządzenia pomiarowe czy linie produkcyjne stają się standardem.

Zdalny dostęp do informacji, na którym opiera się koncepcja IoT, pozwala podejmować szybkie i trafne decyzje, zwiększa wydajność pracy oraz poprawia jej komfort. Wszystko po to, aby optymalizować wykonywane procesy i zadania oraz szybciej podejmować właściwe decyzje na podstawie aktualnych danych.

Systemy bezpieczeństwa stanowią podstawę automatyki nowoczesnych budynków. Aby w pełni efektywnie nimi zarządzać, potrzebne są narzędzia ułatwiające analizę danych. Obecnie zadanie to pełnią systemy BMS *(Building Management System)* oraz SMS *(Security Management System)*. Te jednak są przeznaczone dla obsługi przebywającej na stałe w obiekcie.

Dostęp do bieżących informacji przez firmy zewnętrzne, zajmujące się instalacją czy konserwacją systemu, dotychczas był zaniedbywany. Idące za tym wydłużenie czasu instalacji czy opóźnienie reakcji serwisowej negatywnie wpływa na satysfakcję klienta końcowego.

W jaki sposób można temu zaradzić?

Remote Services to pakiet trzech usług zapewniających stały dostęp do aktualnych informacji dotyczących m.in. systemów sygnalizacji pożarowej.

Remote Connect

Usługa zdalnego połączenia się z centralą systemu sygnalizacji pożarowej. Dzięki temu można z dowolnego miejsca połączyć się i uzyskać bieżące informacje dotyczące stanu pracy systemu (pełny podgląd ekranu kontrolera). Narzędzie to znajduje zastosowanie na każdym etapie korzystania z systemu. Podczas instalacji umożliwia programowanie centrali pożarowej nie tylko w bezpośrednim kontakcie z nią, ale także zdalnie z dowolnego miejsca, wykorzystując łącze internetowe. Dzięki temu wraz z obejmowaniem przez instalację kolejnych stref budynku aktualizację i testy programu centrali można prowadzić bezpośrednio w miejscu, którego dotyczą. W znacznym stopniu przyspiesza to programowanie centrali.

Na wyciągnięcie ręki jest również dostępna funkcja *Automatyczne sczytywanie*, umożliwiająca ponowne sczytywanie i diagnostykę błędów okablowania pętli dozorowej w dowolnym miejscu budynku, bez konieczności udania się do pomieszczenia z centralą. Remote Connect i wbudowana w program funkcja *Zapal diodę LED* pozwala z kolei na ręczną aktywację diody poszczególnych czujek. Dzięki temu opis czujki w programie można łatwo zweryfikować z miejscem instalacji.

Narzędzie ułatwia również konserwację systemu. W razie wystąpienia awarii serwisant potrafi z dowolnego miejsca dokonać diagnozy problemu zgłaszanego przez centralę dzięki zdalnemu wglądowi do szczegółów usterki. Pozwala to ograniczyć zbędne wyjazdy do odszukania źródła problemu, umożliwiając pełne przygotowanie się na naprawę awarii już podczas pierwszej wizyty w obiekcie. Modyfikacje istniejącego systemu, np. dodawanie czujek w środku pętli, dzięki wymienionym narzędziom instalacyjnym również staje się szybsze.

Remote Maintenance

Usługa zdalnego serwisu to narzędzia dostępne przez portal w chmurze. Szczegółowe dane dotyczące systemu, obejmujące m.in. listę zainstalowanych urządzeń wraz ze szczegółami na temat aktualnego stanu pracy, są dostępne w dowolnym urządzeniu typu smartfon, tablet z wykorzystaniem przeglądarki internetowej.

Użytkownik może generować automatyczne raporty serwisowe na podstawie informacji zbieranych przez system, obejmujących m.in. numery seryjne czujek czy ich stan zabrudzenia. Znacząco ogranicza to czas wymagany na tworzenie dokumentacji i raportów, a użytkownik końcowy zyskuje wiarygodne i aktualne dane.

Remote Alert

Ta usługa zapewnia stały i natychmiastowy dostęp do informacji nt. stanu pracy systemu. W przypadku wystąpienia zdarzenia alarmowego, awarii lub utraty łączności z chmurą danych zdefiniowani użytkownicy otrzymują automatyczne powiadomienia SMS oraz e-mail. Serwisant jest w stanie reagować natychmiast po pojawieniu się problemu, niezależnie od miejsca występowania i pracy obsługi systemu w budynku. Z kolei użytkownik końcowy wie, czy system pracuje poprawnie, a w przypadku wykrycia zagrożenia pożarowego natychmiast otrzymuje informacje.

BOSCH
Technologia bliżej nas

Inni czują się bezpieczniej

Remote Services

Ty czujesz, że kontrolujesz wszystkie zainstalowane systemy sygnalizacji pożaru.

Bosch umożliwia budowanie bezpieczniejszego świata. Remote Services oferuje trzy skuteczne i nowatorskie rozwiązania.

Usługi zdalnego nadzoru i konserwacji to większa łączność, pełna ciągłość działania i nieprzerwana dostępność z każdego miejsca na świecie.

Dowiesz się więcej na: boschsecurity.pl

Profesjonalne wykrywacze podsłuchów

oraz technicznych środków inwigilacji

Cayman oraz Piranha to wykrywacze przeznaczone dla jednostek, służb i firm, które cenią sobie precyzję i optymalizację. W połączeniu z dobrym stosunkiem jakości do ceny okazuje się, że na rynku trudno znaleźć lepsze i skuteczniejsze urządzenia.

Wiercenie dziury w ścianach, prucie sufitu, odrywanie wykładziny od podłogi to tylko niektóre sposoby umożliwiające wykrycie i zlokalizowanie różnego typu środków technicznych stosowanych do nieautoryzowanego pozyskania informacji... W ofercie Spy Shop pojawiły się urządzenia, które nie tylko pozwalają oszczędzić czas detekcji, ale także pozostawiają sprawdzone pomieszczenie w stanie nienaruszonym.
Wykrywacz urządzeń inwigilujących ST-031M Piranha-M oraz wykrywacz złączy nieliniowych ST-402 Cayman zostały opracowane pod kątem służb porządku publicznego, służb specjalnych, technik operacyjnych czy profesjonalnych firm ochroniarskich i detektywistycznych. Wykrywacze nie tylko ułatwiają pracę, ale też optymalizują jej czas i koszt, dając pełną gwarancję, że nawet najmniejszy podsłuch, telefon czy fala radiowa zostaną wykryte.

Wykrywacz podsłuchów

Selcom ST-402 Cayman jest wykrywaczem złączy nieliniowych, który służy do detekcji i lokalizacji każdego rodzaju urządzeń podsłuchowych rejestrujących i transmitujących sygnał drogą radiową. Zasada działania detektora opiera się na właściwości charakterystycznej dla układów półprzewodnikowych – pobudzone sygnałem elektromagnetycznym emitują drugą i trzecią harmoniczną, detektor je analizuje, prezentując siłę odbicia sygnału od elementów metalowych. Dzięki wieloczęstotliwościowemu sygnałowi w paśmie 2–3 GHz Cayman wykrywa nawet bardzo małe elementy, np. kartę SIM, z wysoką skutecznością pracy w obecności zakłóceń. Wykrywacz podsłuchów i kamer jest zasilany dwoma standardowymi akumulatorami Li-Ion typu 18650, a jego konstrukcja jest lekka oraz poręczna.

Wykrywacz technicznych środków inwigilacji

ST-31M Piranha to urządzenie wielofunkcyjne umożliwiające detekcję i lokalizację różnego typu środków technicznych stosowanych do nieautoryzowanego pozyskiwania informacji. Mierzy efektywność podjętych środków technicznych służących zabezpieczeniu przed ich wyciekiem.
Do zestawu są dołączone sondy i akcesoria wykrywające większość urządzeń na podstawie różnych zjawisk fizycznych. Piranha wykrywa i lokalizuje:
• analogowe podsłuchy radiowe FM, WFM, AM oraz hybrydowe, z możliwością demodulacji fonii oraz funkcją wspomagającą lokalizację źródła • urządzenia komunikujące się w sieciach komórkowych GSM, UMTS, CDMA, 3G, LTE, z rozróżnieniem sygnałów stacji BTS • nadajniki wielkich częstotliwości.
Każde pomieszczenie jest dzisiaj „nafaszerowane" urządzeniami elektronicznymi, a ST-31M bez problemu wykrywa sieci Wi-Fi, wyłączone telefony komórkowe, podsłuchy i kamery PLC, nieautoryzowane stacje radiowe, a także wiele innych transmisji radiowych, które są najtrudniejsze do zlokalizowania.

ViDiLine®

Wideodomofon IP

w najniższej cenie w Europie

Łączność bezprzewodowa | Zasilanie PoE | Integracja z kamerami IP | Łączność przewodowa

Genway
ul. Chopina 37, Płock
tel.: +48 24 264 77 33
e-mail: info@genway.pl

ViDiLine®

www.c5.genway.pl

* Szczegóły u naszych handlowców pod numerem telefonu: +48 24 264 77 33.

Consorcium STS
al. Krakowska 219, 02-180 Warszawa
tel./faks: 22 868 15 25
www.consorciumsts.com

Trzeźwość pod kontrolą

Consorcium STS, jako integrator systemów security, przygotował autorskie rozwiązanie, pozwalające znacząco **poprawić bezpieczeństwo pracy i zabezpieczyć teren obiektu przed wejściem osób nietrzeźwych lub nieposiadających stosownych uprawnień.**

Kontrola trzeźwości za pomocą alkomatu EBS Platinium, który jest zintegrowany z bramkami typu tripod oraz systemami kontroli dostępu i dozoru wizyjnego, pozwala na skuteczne zatrzymanie zarówno osób nietrzeźwych (wchodzących i wychodzących), jak i pracowników nieposiadających wymaganych uprawnień, np. do poruszania się pojazdami zakładowymi itp.

Wbudowany generator losowy umożliwia kontrolowanie wszystkich lub tylko losowo wybranych osób, co ma doskonałe działanie prewencyjne.

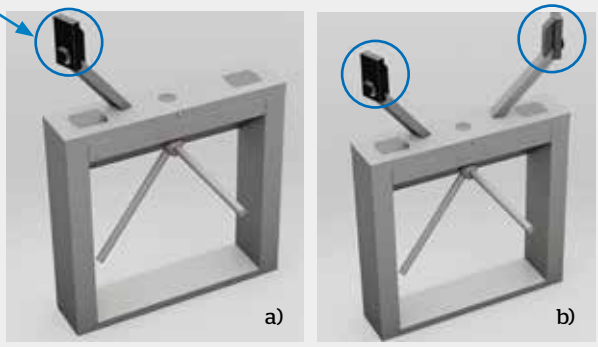
Nad alkomatem można zainstalować wyświetlacz LCD, na którym pojawiają są informacje, np. o kończących się badaniach BHP pracownika, potrzebie przedłużenia przepustki czy innych uprawnieniach. Urządzenie jest bezdotykowe, nie wymaga żadnych ustników czy rurek, a pomiar trwa tylko 2 s.

Zaprojektowano go w sposób uniemożliwiający podmianę kart czy „dmuchanie" przez inną osobę. Nie ma potrzeby ograniczenia liczby pracowników poddających się kontroli, ponieważ kalibracja czujnika odbywa się w cyklu 80 tys. pomiarów. Eksploatacja jest więc ekonomiczna. Alkomat EBS Platinium został zaprojektowany do weryfikacji dostępu osób wchodzących do chronionej strefy. Pomiar jest szybki i wiarygodny, a to gwarantuje pełną ochronę przed wejściem nietrzeźwych pracowników.

TEST TRZEŹWOŚCI

OPCJE MONTAŻU

Alkomat EBS Platinium montuje się na bramkach w opcjach jednostronnej (a) lub dwustronnej (b) kontroli trzeźwości



Urządzenie zintegrowano z systemem kontroli dostępu. Aby przejść przez bramkę, pracownik musi poddać się testowi na trzeźwość. System nie przepuści osoby, która nie wykona testu lub jest nietrzeźwa.

Alkomat EBS Platinium jest montowany na bramkach w opcjach jedno- lub dwustronnej kontroli trzeźwości. Alkomat można również montować w śluzach osobowych lub kołowrotach typu furta stadionowa. Takie rozwiązanie pozwala wyeliminować konieczność angażowania do dozoru pracowników ochrony.

POLON-ALFA NAJNOWSZA TECHNOLOGIA. NAJWYŻSZA JAKOŚĆ

PROJEKTUJEMY

zgodnie ze sztuką

SYSTEMY SYGNALIZACJI POŻAROWEJ

- innowacyjnie rozproszony **POLON 6000**
- interaktywny **POLON 4000**
- konwencjonalny **IGNIS 1000/2000**

UNIWERSALNE CENTRALE STERUJĄCE UCS 6000

SYSTEM DETEKCJI GAZÓW SDG 6000

POLON-ALFA S.A. (dawniej Polon-Alfa Spółka z ograniczoną odpowiedzialnością Sp. k.)
85-861 Bydgoszcz, ul. Glinki 155 | www.polon-alfa.pl

NUODO

PROJEKT POLSKIEJ USTAWY I ZMIANY WOBEC DOTYCHCZASOWYCH WYMAGAŃ UODO

OCHRONA DANYCH OSOBOWYCH CZ. 6

To kolejny artykuł **poświęcony projektowi Nowej Ustawy ODO udostępnionemu 12 września 2017 r.** przez Ministerstwo Cyfryzacji do publicznej dyskusji. Kontynuuje tematykę poruszaną w poprzednich wydaniach „a&s Polska".

Marek Blim

1. Czego przedsiębiorca branży security nie może zaniedbać wg wymagań RODO

Grupa Robocza Art. 29 UE w swojej opinii z 27 lipca 2017 podała, że stosowanie nowych technologii informacyjnych w miejscu pracy w zakresie infrastruktury, aplikacji oraz inteligentnych urządzeń umożliwia nowe sposoby systematycznego i potencjalnie inwazyjnego przetwarzania danych osobowych. Podkreśla, że nowe sposoby przetwarzania danych (np. śledzenie korzystania z usług internetowych) są znacznie mniej zauważalne przez pracowników niż tradycyjne formy, takie jak kamery monitoringu wizyjnego umieszczone w widocznych miejscach. W przypadku pracy zdalnej może też dochodzić do monitorowania ich aktywności poza fizycznym miejscem pracy. Nasuwa to pytanie, **w jakim stopniu pracownicy są świadomi konsekwencji stosowania takich technologii, ponieważ pracodawcy mogą niezgodnie z prawem przetwarzać dane bez wcześniejszego poinformowania pracowników.**

Nowe technologie mogą być pomocne w zapobieganiu i wykrywaniu kradzieży własności intelektualnej i mienia firmy, zwiększeniu produktywności pracowników oraz ochrony danych osobowych, za którą odpowiedzialność ponosi sprawujący kontrolę. Stawia jednak poważne wyzwania w kwestii ochrony danych i prywatności. W efekcie potrzebna jest nowa ocena, biorąca pod uwagę zachowanie równowagi między uzasadnionymi interesami pracodawcy chroniącego swoją firmę a uzasadnionymi oczekiwaniami pracowników w kwestii prywatności.

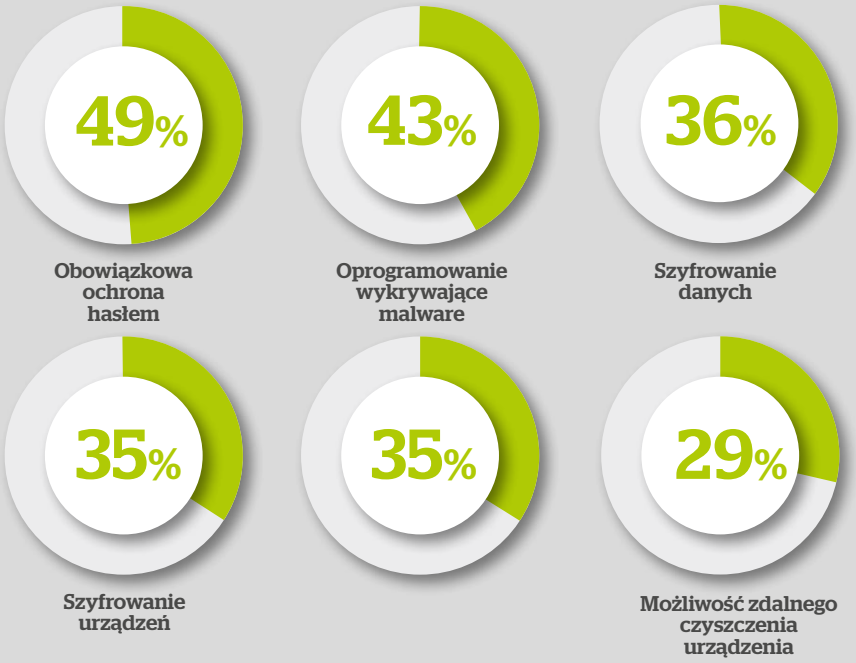
1.1. Zadania pracodawców

Rozwój nowych technologii i metod przetwarzania danych sprawił, że pracodawcy muszą zwracać większą uwagę na podstawowe zasady dotyczące ochrony danych osobowych. Zdaniem Grupy Roboczej Art. 29 pracodawcy powinni:

- zapewnić, że dane są przetwarzane w określonych, zgodnych z prawem celach, które są proporcjonalne i konieczne;
- kierować się zasadą ograniczenia celu, zapewniając, że dane są wystarczające, od-

BYOD w polskich firmach i organizacjach

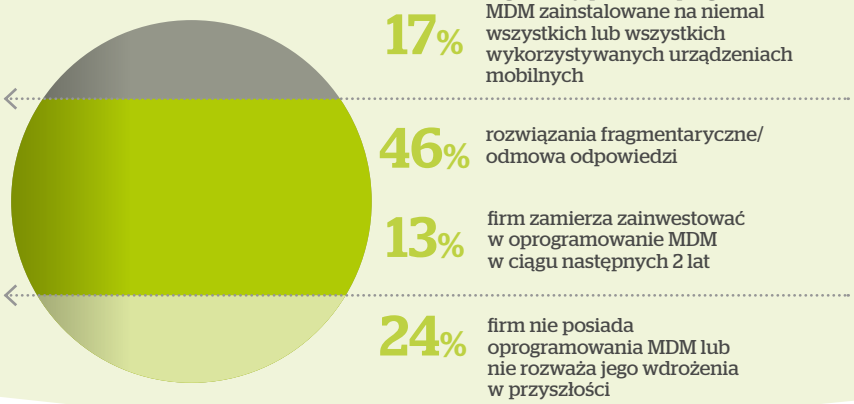
NARZĘDZIA WYKORZYSTYWANE DO OCHRONY URZĄDZEŃ MOBILNYCH



DO KOGO NALEŻĄ URZĄDZENIA MOBILNE WYKORZYSTYWANE W FIRMIE?

- urządzenia należą tylko do pracowników
- urządzenia należą tylko do organizacji
- część urządzeń należy do firmy, a część do pracowników
- odmowa odpowiedzi/brak danych

JAKI PROCENT URZĄDZEŃ W FIRMIE POSIADA ZAINSTALOWANE OPROGRAMOWANIE MDM?



Źródło: IBM, „Computerworld"

powiednie i proporcjonalne do uzasadnionego celu;
- zastosować zasadę proporcjonalności i pomocniczości bez względu na mającą zastosowanie podstawę prawną;
- zachować transparentność w relacji z pracownikiem w związku z zastosowaniem i celami technologii monitorowania;
- umożliwić osobom, których dane dotyczą, korzystanie ze swoich praw, w tym z prawa do dostępu, a także korektę, usunięcie lub zablokowanie danych osobowych;
- zapewniać, aby dane były dokładne, i nie przechowywać ich dłużej, niż jest to konieczne;
- podejmować wszelkie niezbędne działania, aby chronić dane przed nieautoryzowanym dostępem i zapewnić, by inni pracownicy mieli dostateczną wiedzę na temat obowiązków wynikających z ochrony danych.

1.2. Zgoda jako podstawa prawna przetwarzania danych pracowników

Grupa Robocza Art. 29 stwierdza, że podstawą prawną przetwarzania danych pracowników nie może i nie powinna być zgoda pracowników. Jeśli pracodawca wymaga zgody, a jej brak może spowodować w stosunku do pracownika jakąś szkodę (np. groźbę zwolnienia), zgoda nie ma ważnej podstawy prawnej, ponieważ nie została udzielona dobrowolnie.

Nawet w przypadkach, gdy uważa się, że zgoda stanowi ważną podstawę prawną przetwarzania (jest dobrowolna), wymagane jest konkretne, świadome i dobrowolne wskazanie zgody pracownika. Domyślna konfiguracja urządzeń oraz/lub instalacja oprogramowania umożliwiającego elektroniczne przetwarzanie danych osobowych nie są traktowane jako zgoda pracowników, ponieważ **zgoda wymaga czynnego wyrażenia woli**. Brak aktywności (gdy domyślne ustawienia nie zostaną zmienione) może nie być traktowane jako specjalna zgoda na umożliwienie takiego przetwarzania.

1.3. Realizacja umowy jako podstawa prawna przetwarzania danych pracowników

W niektórych przypadkach przetwarzanie danych może być konieczne do realizacji umowy – pracodawca musi np. przetwarzać

dane osobowe pracownika, aby wypełnić jakiekolwiek zobowiązania, m.in. wypłata wynagrodzenia.

1.3.1. Obowiązek wynikający z przepisu prawa

Zdarza się też, że prawo zatrudnienia może nakładać obowiązki prawne, które wymagają przetwarzania danych osobowych (np. do celów wyliczenia podatków oraz zarządzania wynagrodzeniami). To podstawa prawna przetwarzania danych, ale pracownik musi być w pełni i jasno poinformowany o takim przetwarzaniu (jeśli nie ma zastosowania wyjątek).

1.3.2. Uzasadniony interes pracodawcy

Jeśli pracodawca chce powołać się na swój uzasadniony interes, cel przetwarzania musi być zasadny, wybrana metoda lub dana technologia muszą być konieczne, proporcjonalne i wdrożone przy zastosowaniu możliwie najmniej uciążliwych środków, umożliwiając pracodawcy wykazanie, że zastosowano odpowiednie środki, aby zapewnić równowagę z poszanowaniem podstawowych praw i wolności pracowników. Operacje przetwarzania muszą być zgodne z wymogami w zakresie przejrzystości, a pracownicy powinni być w jasny i wyczerpujący sposób poinformowani o przetwarzaniu ich danych osobowych, w tym o istnieniu systemów monitorowania – podkreśla Grupa Robocza Art. 29. Należy zastosować odpowiednie środki techniczne i organizacyjne zapewniające bezpieczeństwo przetwarzania. Przetwarzanie danych w pracy powinno być przeprowadzane w możliwie najmniej uciążliwy sposób i uwzględniać obszary szczególnego ryzyka. Pracownik może wyrazić sprzeciw wobec przetwarzania, które odbywa się na podstawie prawnie uzasadnionego celu.

1.4. Jak RODO/GDPR odnosi się *in corpore* do przetwarzania danych pracowników

Rozporządzenie o ochronie danych zaostrza wymogi dotyczące ochrony danych osobowych i wprowadza nowe obowiązki dla wszystkich administratorów danych, w tym pracodawców. Wymaga od administratorów danych m.in. wdrożenia ochrony danych domyślnie już w fazie projektowania. Przykładowo, jeśli pracodawca, wydając urządzenia

NUODO – Nowa Ustawa o Ochronie Danych Osobowych
PUODO – Prezes Urzędu Ochrony Danych Osobowych
UODO – Urząd Ochrony Danych Osobowych
IOD – Inspektor Ochrony Danych

pracownikom, wykorzystuje technologie śledzenia, należy wybrać najlepsze technologie chroniące prywatność. Powinien też przetwarzać tylko niezbędne dane. Ponadto rozporządzenie zobowiązuje administratorów do przeprowadzania oceny skutków przetwarzania danych na ich ochronę. Jeśli taka ocena wykaże, że zidentyfikowanych zagrożeń administrator danych nie może w odpowiedni sposób ograniczyć – tj. ryzyko pozostaje wysokie – musi się skonsultować z organem nadzorującym, zanim rozpocznie procedurę przetwarzania.
Zgodnie z rozporządzeniem UE nr 679/2016 (RODO/GDPR) państwa członkowskie mogą ustalić konkretne zasady, aby zapewnić ochronę praw i wolności w zakresie przetwarzania danych osobowych pracowników w związku z zatrudnieniem (np. na potrzeby rekrutacji, wykonywania umowy o pracę czy zarządzania, planowania i organizacji pracy). Wszelkie te przepisy powinny jednak zawierać odpowiednie i konkretne środki gwarantujące godność oraz poszanowanie podstawowych praw osoby, której dane dotyczą, w szczególności w związku z:

- transparentnością przetwarzania,
- przekazywaniem danych osobowych w ramach grupy przedsiębiorstw prowadzących wspólną działalność gospodarczą,
- systemami monitorowania w miejscu pracy.

1.5. Przetwarzanie danych osobowych w procesie rekrutacji

Podczas rekrutacji często wykorzystuje się media społecznościowe. Pracodawcy sprawdzają np. profile kandydatów do pracy. Zdaniem Grupy Roboczej Art. 29 nie powinni zakładać, że ze względu na powszechną dostępność informacji na profilach społecznościowych mogą przetwarzać te dane do własnych celów. Do tego jest wymagana podstawa prawna, taka jak uzasadniony interes. Pracodawca powinien więc przed przeglądaniem profilu na portalu społecznościowym upewnić się, czy dany profil osoby aplikującej ma charakter prywatny, czy związany z pracą, co może stanowić istotną wskazówkę w odpowiedzi na pytanie, czy takie przeglądanie jest legalne. Ponadto pracodawcy mogą gromadzić i przetwarzać dane osób aplikujących jedynie, gdy jest konieczne i istotne z punktu widzenia wykonywanej pracy, o którą kandydat się ubiega.

1.5.1. Przetwarzanie danych osobowych wynikające z weryfikacji pracownika

Za sprawą dostępności profili w mediach społecznościowych i rozwoju nowych technologii analitycznych pracodawcy mają techniczną możliwość stałego sprawdzania pracowników poprzez zbieranie informacji obejmujących ich przyjaciół, opinie, zainteresowania, zwyczaje, miejsce przebywania, poglądy i zachowanie. W ten sposób pozyskują dane zawierające informacje poufne, związane z prywatnym i rodzinnym życiem pracownika.

1.5.2. Przetwarzanie danych osobowych wynikające z monitorowania technologii informacyjnych i komunikacyjnych w miejscu pracy

Zmiany technologiczne umożliwiają nowe, ingerujące w prywatność i powszechne sposoby monitorowania pracowników, np. zastosowanie w miejscu pracy aplikacji biurowych w chmurze, co w teorii umożliwia dokładny zapis aktywności pracowników. Pracodawcy, stosując takie rozwiązania, powołują się na swój prawnie uzasadniony cel i np. konieczność ochrony przed wyciekiem danych osobowych. Jednak zdaniem Grupy Roboczej Art. 29 monitorowanie każdej aktywności pracowników w tym celu jest reakcją nieproporcjonalną. Pracodawca powinien najpierw upewnić się, czy nie istnieją inne, mniej inwazyjne środki zapewniające ochronę poufności danych.
Pracodawca powinien poinformować pracowników o dopuszczalnym i niedopuszczalnym korzystaniu z sieci i urządzeń. Będą wtedy mogli korzystać z urządzeń IT w taki sposób, aby zapobiec byciu monitorowanym podczas korzystania z sieci w celach pry-

watnych. W ramach dobrych praktyk co najmniej raz w roku należy opracować politykę, która pozwoli ocenić, czy wybrane rozwiązania w zakresie monitorowania przynosi pożądane rezultaty, a także czy są dostępne inne, mniej inwazyjne narzędzia lub środki, które mogą posłużyć do osiągnięcia tego samego celu.

1.5.3. Przetwarzanie danych osobowych wynikające z monitorowania technologii informacyjnych i komunikacyjnych poza miejscem pracy

Korzystanie z technologii informacyjnych i komunikacyjnych poza miejscem pracy staje się coraz bardziej powszechne wraz z rozwojem telepracy i używaniem przez pracowników własnych urządzeń. Może to stwarzać zagrożenie prywatności pracowników, ponieważ systemy monitorowania działające w miejscu pracy funkcjonują także w środowisku domowym podczas korzystania z takich urządzeń.

Praca zdalna może stanowić dla pracodawcy potencjalne ryzyko – pracownicy mogą mieć zdalny dostęp do infrastruktury firmy, która nie jest ograniczona w wymiarze fizycznym tak, jak w siedzibie firmy. Bez implementacji odpowiednich środków technicznych ryzyko nieautoryzowanego dostępu wzrasta i może skutkować utratą bądź zniszczeniem informacji, w tym danych osobowych pracowników lub klientów, którymi dysponuje pracodawca.

Pracodawcy muszą więc przeanalizować, czy uzasadnione jest korzystanie z pakietów oprogramowania, które umożliwiają rejestrowanie naciśnięcia klawiszy czy ruchów myszą, zrzutów ekranów, rejestrację użytych aplikacji na kompatybilnym urządzeniu, dostęp do kamery i gromadzenie zarejestrowanego materiału. Jak zauważa Grupa Robocza Art. 29, przetwarzanie danych, do którego dochodzi podczas wykorzystywania nowoczesnych technologii, jest nieproporcjonalne i pracodawca ma małe szanse, aby uzyskać podstawę prawną, na którą mógłby się powołać, wykazując swój uzasadniony interes, np. podczas rejestracji naciśnięcia klawiszy czy ruchów myszą przez pracownika.

Pod względem liczby aktów prawnych zmienianych w związku z RODO/GDPR ta reforma jest jedną z największych w naszej historii.

1.5.4. Przetwarzanie danych osobowych w celu rejestracji czasu i obecności

Systemy, które umożliwiają pracodawcom kontrolę osób wchodzących na teren firmy lub do określonych obszarów w swojej siedzibie, również mogą umożliwiać śledzenie aktywności pracowników. Chociaż takie systemy istniały przez wiele lat, nowe technologie kontrolowania czasu i obecności pracowników (w tym przetwarzające dane biometryczne), a także inne umożliwiające śledzenie urządzeń mobilnych, są obecnie coraz szerzej stosowane. Mogą one stanowić istotną część ścieżki kontroli w firmie, stanowią także ryzyko dostarczania wiedzy i kontroli na poziomie, który może mieć charakter inwazyjny. Dotyczy to aktywności pracownika w miejscu pracy. Jeśli przetwarzanie jest konieczne i nie narusza prywatności pracowników, może stanowić uzasadniony interes pracodawcy, gdy pracownicy zostali odpowiednio poinformowani o operacji przetwarzania. Jednak ciągły monitoring częstotliwości i dokładnego czasu wejść i wyjść pracowników nie może być uzasadniony innym celem jak oceną wydajności pracownika.

1.5.5. Przetwarzanie danych osobowych z użyciem systemów monitoringu wizyjnego

Dzięki możliwościom, jakie zapewnia analiza materiału wizyjnego, pracodawca może monitorować mimikę pracownika w sposób zautomatyzowany w celu zidentyfikowania odchyleń od wcześniej określonego wzoru. Jest to nieproporcjonalne w stosunku do praw i wolności pracownika, a zatem zazwyczaj niezgodne z prawem. Przetwarzanie z dużą dozą prawdopodobieństwa może objąć profilowanie oraz zautomatyzowane podejmowanie decyzji. Pracodawcy powinni więc unikać stosowania technologii rozpoznawania twarzy. Mogą istnieć pewne odstępstwa od tej reguły, ale takie scenariusze nie mogą odwoływać się do ogólnego uprawomocnienia stosowania takich technologii.

2. RODO/GDPR a zadania dla pracodawców wykorzystujących BOYD

Część pracowników korzysta w pracy z własnych urządzeń. Może to spowodować, że pracodawca zyska dostęp do informacji o pracowniku niezwiązanych z pracą zawodową. Monitorowanie lokalizacji i ruchu prywatnych urządzeń wykorzystywanych w pracy może zostać uznane za służące uzasadnionemu interesowi, by chronić dane osobowe, za które odpowiedzialny jest pracodawca jako administrator danych. Jednak może być niezgodne z prawem, jeśli takie monitorowanie pozwoli pozyskać dane związane z życiem prywatnym i rodzinnym pracownika. Aby zapobiec monitorowaniu prywatnych informacji, należy podjąć odpowiednie kroki pozwalające rozróżnić pomiędzy prywatnym a biznesowym zastosowaniem urządzenia. Pracodawcy powinni wdrożyć metody, które umożliwią bezpieczny transfer ich danych pomiędzy urządzeniem a siecią firmy.

2.1. Praktyczne użycie urządzeń mobilnych

Już w 2015 r. urządzenia mobilne odpowiadały w Polsce za 60% ruchu internetowego. Dla porównania StatCounter wskazuje, że na świecie proporcje rozkładały się następująco: 51,3% – urządzenia mobilne i 48,7% – desktopy. Oznacza to, że nasz kraj dostosowuje się do nowych technologii szybciej niż reszta świata.

Liczba użytkowników smartfonów w 2016 r. przekroczyła 2 mld, a liczba mobilnych pobrań do końca 2017 r. przekroczy 268 mld – mówi Robert Włodarski, odpowiedzialny w IBM za współpracę z klientami w zakresie zarządzania mobilnością[1)].

2.2. Oczekiwania od pracowników

W sytuacji, gdy większość dorosłych ma smartfon w kieszeni, rosnąca popularność trendu BYOD (*Bring Your Own Device* – Przynieś Swoje Własne Urządzenie) nie jest zaskakująca. Najczęściej oznacza instalowanie aplikacji służbowych na własnym urządzeniu, np. do przeglądania poczty firmowej lub obsługi systemu CRM. Elementem tego zjawiska jest także BYOA (*Bring Your Own Ap-*

[1)] *http://odkryjibm.pl/.../kon-trojanski-czy-czarny-kon-produktywnosci-urzadzenia-mobilne*

plication – Przynieś Swoją Własną Aplikację). Wykorzystywanie aplikacji prywatnych w celach służbowych może mieć formę instalowania ulubionych narzędzi do zarządzania czasem lub produktywnością na służbowym telefonie, aby wszystkie swoje zadania, zarówno prywatne, jak i zawodowe, mieć uporządkowane w jednym miejscu. Czy i w jakim zakresie pracodawcy powinni to akceptować – wymaga przemyślenia stosownie do sytuacji *tu i teraz*.

2.3. Jak to wygląda w statystykach

Raport Harvard Business Review wskazuje, że wprawdzie tolerancja korzystania z własnego sprzętu mobilnego w pracy wzrasta, to spada liczba firm, które oficjalnie zachęcają do tej praktyki swoich pracowników. Z danych HBR wynika, że wprawdzie w 2014 r. już 90% firm zezwalało na przynoszenie własnego smartfonu i wykorzystywanie go w pracy, to w tym samym czasie odsetek przedsiębiorstw zachęcających do tej praktyki spadł o 18 punktów procentowych. Wynika to z niebezpieczeństw, jakie niesie ze sobą trend BYOD. Raport Crowd Research Partners wskazuje, że obawa o bezpieczeństwo (39% wskazań) oraz prywatność pracowników (12%) to najważniejsze problemy, dla których firmy nie decydują się na sięgnięcie po BYOD.

Z danych firmy McAfee wynika, że obecnie w każdej minucie pojawia się 387 nowych zagrożeń bezpieczeństwa teleinformatycznego – mówi Robert Włodarski[2]. Spośród niebezpieczeństw, jakie wiążą się ze stosowaniem urządzeń pracowników w środowisku firmowym, najczęściej wskazuje się ryzyko wycieku lub utraty firmowych danych (72%), nieautoryzowany dostęp do tych danych (56%), aplikacje lub treści niosące ze sobą niebezpieczeństwo dla firmowych zasobów (54%) lub po prostu *malware* działające na urządzeniach mobilnych (52%). Dane McAfee wskazują, że w ostatnim kwartale 2016 roku zebrano 72% więcej próbek unikatowego oprogramowania *malware* skierowanego na urządzenia mobilne wykorzystywane w systemach firm[3].

[2] *http://odkryjibm.pl/.../kon-trojanski-czy-czarny-kon-produktywnosci-urzadzenia-mobilne*

[3] *https://www.bankier.pl/wiadomosc/McAfee-Raport-na-temat-zagrozen-w-Internecie-2145098.html*

W podsumowaniu

Polskie przepisy dotyczące ochrony danych osobowych były już kilkakrotnie aktualizowane, ale mimo wprowadzanych zmian wciąż nie nadążały za zmieniającą się technologią. Tym samym nie gwarantowały właściwej ochrony obywatelom. Podobnie przedstawiała się sytuacja w innych państwach UE. Stało się to powodem podjęcia wieloletnich prac UE ukierunkowanych na reformę przepisów w celu zwiększenia poziomu ochrony prywatności obywateli, przy jednoczesnym uwzględnieniu interesów przedsiębiorców.

Po czterech latach intensywnych prac i konsultacji 4 maja 2016 r. opublikowano ogólne rozporządzenie o ochronie danych osobowych (GDPR/RODO), które będzie stosowane (również w Polsce) od 25 maja 2018 r.

Długi, bo dwuletni okres od opublikowania, po którym nowe prawo będzie stosowane, wynika z ogromu zmian, jakich wymaga dostosowanie się państw członkowskich do nowych zaleceń prawnych. Projekty opublikowane przez Ministerstwo Cyfryzacji są jednym z elementów dostosowania Polski do nowej regulacji. Pod względem liczby aktów prawnych, które ulegną zmianie w związku RODO/GDPR, reforma przepisów ochrony danych osobowych jest jedną z największych w naszej historii.

Wkrótce przekonamy się, jakie zmiany są akceptowane i czego naprawdę oczekują od ustawodawcy nasi przedsiębiorcy…

Literatura

[1] BOYD: *http://odkryjibm.pl/.../kon-trojanski-czy-czarny-kon-produktywnosci-urzadzenia-mobilne*

[2] „*Cyberdoktryna RP*", CIIP Focus RCB, styczeń 2015 str.14-15, za: *http://rcb.gov.pl/wp-content/uploads/ciip-focus-9.pdf*

[3] „*Opinia nr 2/2017 Grupy Art.29 w sprawie przetwarzania danych w związku z zatrudnieniem*", Euro-lex, 2017-07-27

[4] Projekt NUODO: *https://www.gov.pl/cyfryzacja/projekt-ustawy-o-ochronie-danych-osobowych*

[5] Raporty: *https://www.bankier.pl/wiadomosc/McAfee-Raport-na-temat-zagrozen-w-Internecie-2145098.html*

BIO

dr inż. Marek Blim

Europejski menedżer systemu zarządzania jakością EOQ, certyfikowany audytor systemów jakości i zarządzania bezpieczeństwem informacji, ekspert systemowy ISO 9000 INTERCERT/TüV Rheinland Polska. Rzeczoznawca systemów technicznej ochrony osób i mienia oraz zarządzania bezpieczeństwem. Projektant systemów ochrony. Czynny zawodowo konsultant, rzeczoznawca, audytor.

KORUPCJA?

WYZWANIE NAJBLIŻSZYCH MIESIĘCY...

Korupcja jest tematem wielu dyskusji w różnych gremiach. Słowo to pada ostatnio zdecydowanie częściej w związku z tym, iż po kilku turach konsultacji społecznych, podczas których zgłoszono około 1000 szczegółowych uwag, opinii i propozycji, **12 grudnia 2017 r. na stronie Rządowego Centrum Legislacji została opublikowana najnowsza wersja projektu ustawy o jawności życia publicznego.**

Michał Czuma

Korupcja od lat jest ważnym tematem życia publicznego, poruszanym zarówno przez zwolenników, jak i przeciwników każdej władzy. Sporo uwagi poświęca się jej w mediach, przeciwnicy polityczni przerzucają się podejrzeniami o sprzyjanie jej albo iluzoryczną z nią walkę.

Najczęściej wymienianą wśród respondentów różnych sondaży formą korupcji jest łapownictwo. W prawie karnym wyróżniono jego dwie odmiany: bierną (*Kto w związku z pełnieniem funkcji publicznej przyjmuje korzyść majątkową lub osobistą albo jej obietnicę,* o czym mówi art. 228 § 1) i czynną (*Kto udziela lub obiecuje udzielić korzyści majątkowej lub osobistej osobie pełniącej funkcję publiczną w związku z pełnieniem tej funkcji podlega karze…*, art. 229 kk). Korupcją jest również płatna protekcja (*Kto, powołując się na wpływy w instytucji państwowej, samorządowej, organizacji międzynarodowej albo krajowej lub w zagranicznej jednostce organizacyjnej dysponującej środkami publicznymi albo wywołującymi przekonanie innej osoby lub utwierdzającej ją w przekonaniu o istnieniu takich wpływów, podejmuje się pośrednictwa w załatwieniu sprawy w zamian za korzyść majątkową lub osobistą albo jej obietnicę,* art. 230 i 230a kk).

Rzadko się o tym mówi, ale korupcją jest także tzw. nadużycie władzy (art. 231 kk) polegające na tym, iż przekraczając swoje uprawnienia lub nie dopełniając obowiązków, funkcjonariusz publiczny działa na szkodę interesu publicznego lub prywatnego. Za to można trafić za kratki nawet na 3 lata. Korupcji dotyczą też przepisy związane z tzw. nadużyciem zaufania (art. 296 oraz art. 296a i 296b kk), gdy ktoś, zajmując się sprawami majątkowymi lub prowadząc działalność gospodarczą osoby prawnej nieposiadającej osobowości prawnej (np. szkoły, przedszkola), nie dopełnia obowiązków czy działa na szkodę, powinien mieć świadomość odpowiedzialności karnej na nim ciążącej. Do tego można dodać wszelkie formy przekupstwa.

Jak widać, jest sporo przepisów pozwalających na pociągnięcie do odpowiedzialności każdego, kto pozycję, wpływy i posiadane zaufanie społeczne wykorzystuje nieetycznie do uzyskania korzyści osobistych.

Ciekawy jest źródłosłów słowa korupcja. Pochodzi ono od łacińskiego *corrumpere* oznaczającego dwie czynności: niemoralnego łamania lub psucia. Korupcja rzeczywiście łamie ludziom charaktery i kariery, psuje biznes, życie publiczne i politykę. Uznaje się ją za jedną z wielu nieuczciwych, najstarszych praktyk w historii ludzkości, za coś nagannego, chociaż historycznie i politycznie można wskazać okresy i miejsca, kiedy bywała prawie legalną, a na pewno akceptowalną formą regulującą różne kwestie polityczne, gospodarcze czy historyczne.

Zastanawiać może jeszcze jedno zjawisko dostrzegalne w badaniach sondażowych. W ciągu ostatnich niespełna czterech lat odsetek badanych uważających, że korupcja stanowi bardzo duży problem, zmniejszył się o 8 punktów procentowych – do 31 proc.; respondentów twierdzących, że jest on duży, także ubyło – z 87 proc. do 76 proc. Liczba osób przekonanych, że zjawisko to nie jest szczególnie znaczące wzrosła z 8 proc. do 15 proc. (badanie CBOS, 2016 r.). To, że zjawisko korupcji istnieje, nie podlega dyskusji – publicznie znane fakty to potwier-

NAJWIĘKSZE AFERY KORUPCYJNE NA ŚWIECIE

- Pomimo restrykcji prawnych oraz sporych kompetencji i możliwości danym organom ścigania amerykański koncern Johnson & Johnson miał płacić lekarzom (także w Polsce, Rumunii i Grecji) za promowanie swoich produktów medycznych. Sprawa ujrzała światło dzienne w 2011 r. dzięki informacji, jaka wpłynęła m.in. poprzez uruchomiony przez Departament Sprawiedliwości USA kanał powiadamiania. Ten jeden z największych farmaceutyczno-kosmetycznych koncernów na świecie zgodził się na zawarcie ugody, która kosztowała go 70 mln dolarów.

- Inna afera dotyczyła **Panalpina World Transport**, szwajcarskiego koncernu świadczącego usługi transportowe na całym świecie. Niektórzy jej menedżerowie mieli wręczyć tysiące łapówek w wysokości 27 mln dolarów politykom z co najmniej siedmiu krajów (m.in. Brazylii, Rosji i Nigerii). Ostatecznie Szwajcarzy zawarli ugodę, która kosztowała ich 76 mln dolarów.

- **Francuska firma Alcatel-Lucent** była podejrzana o korumpowanie polityków z Kostaryki, Hondurasu, Malezji, Tajwanu i Kenii w zamian za korzystne kontrakty telekomunikacyjne. Ostatecznie Francuzom przyszło zapłacić 137 mln dolarów w ramach zawartej ugody.

- Problemy związane z korupcją nie ominęły także **niemieckiego koncernu motoryzacyjnego Daimler,** oskarżanego o korumpowanie polityków w 22 krajach (m.in. w Austrii, Rosji i na Węgrzech). W zamian za milionowe łapówki lokalni oficjele gwarantowali firmie zwycięstwo w przetargach na zakup samochodów często po cenach, które trudno nazwać rynkowymi. Ugoda z wymiarem sprawiedliwości kosztowała Daimlera 195 mln dolarów.

- **Japoński koncern JGC Corp.** miał korumpować nigeryjskich oficjeli w zamian za korzystne kontrakty budowlane – ugoda z wymiarem sprawiedliwości kosztowała Japończyków aż 219 mln dolarów. Nigeria ma opinię najbardziej skorumpowanego kraju na świecie.

- Nigeryjskich polityków korumpował również **francuski koncern Technip S.A.,** który miał chrapkę na wart ponad 6 mld dolarów kontrakt na budowę zakładów skroplonego gazu. W ramach ugody Francuzi zapłacili karę w wysokości 240 mln dolarów.

- Jedna z najgłośniejszych afer korupcyjnych, chociaż sięgała 1997 r., ale jej apogeum miało miejsce 7 lat temu i nadal jest w zainteresowaniu francuskich służb – w 2010 r. **francuski koncern paliwowy Total** został oskarżony o korumpowanie irańskich polityków. W grę miało wchodzić nawet 60 mln dolarów łapówek. W zamian Francuzi mieli otrzymać lukratywne kontrakty na irańskim rynku naftowym. Ostatecznie Total zgodził się na zawarcie ugody opiewającej na gigantyczną kwotę 398 mln dolarów. Sędzia prowadzący dochodzenie ustalił, że osoby ze świecznika tego koncernu przekazywały znaczne kwoty byłym dostojnikom z reżimu Saddama Husajna w zamian za dostarczanie Totalowi ropy naftowej w ilościach przekraczających ONZ-owski program „Ropa za żywność".

- **Brytyjski koncern zbrojeniowy BEA Systems** został oskarżony o korumpowanie polityków w Arabii Saudyjskiej, Czechach i na Węgrzech w zamian za zdobycie kontraktów na dostawy samolotów. Przedstawiciele koncernu mieli m.in. wręczyć gigantyczną łapówkę w wysokości 2 mld dolarów saudyjskiemu ambasadorowi Bandarowi bin Sultanowi. Ugoda z wymiarem sprawiedliwości kosztowała Brytyjczyków 448 mln dolarów.

- Szerzej opisywana w mediach sprawa dotycząca **niemieckiego koncernu Siemens**, który wydaje się weteranem afer korupcyjnych. Największa z nich, dotycząca korumpowania urzędników państwowych w Niemczech, USA i wielu innych krajach, kosztowała Siemensa aż 1,3 mld dolarów wniesionych w ramach ugody. Koncern był również bohaterem głośnej afery korupcyjnej w Rosji (wręczenie łapówek przedstawicielom Gazpromu). Ostatecznie Siemens został poddany wielu procesom mającym na celu oczyszczenie firmy z działań prowadzonych przez niektórych menedżerów, a które przez wiele lat nie schodziły z łam prasy i mediów. Sprawa korupcji w koncernie pokazuje, jak wielowątkowe są sprawy korupcyjne i jak wiele innych patologii może być z nimi związanych.

Niemcy były jednym z tych krajów, które do 1999 r. uznawały praktyki gratyfikacyjne (jak nazywano wtedy łapówki) za zgodne z prawem niemieckim. Ale Siemens nie zmienił swojej polityki, gdy decyzją władz niemieckich stały się one nielegalne. Podczas śledztwa znaleziono dane wskazujące, iż przedstawiciel firmy w Moskwie ostrzegał, że bez „bakszyszów" obroty koncernu w Rosji spadną o 40 proc. Oficjalnie dyrektorzy zarządzający koncernem polecili w tym okresie przedstawicielom w innych krajach postępowanie zgodne z prawem. Śledztwo wykazało jednak, że patrzyli przez palce na finansowe machinacje. Gdy wybuchł skandal, zapewniali, że o niczym nie wiedzieli, przyjęli tylko „odpowiedzialność polityczną" i nie wyrazili skruchy. W Nigerii korupcję krzewił i wspierał dyktator Sani Abacha, który konsekwentnie pobierał połowę każdej „prowizji" wypłaconej przez Siemensa.
W toczących się śledztwach wiele informacji ujawniono prasie, dzięki czemu można przekazać jeszcze kilka ciekawostek.
W 2004 r. łapówkę od Siemensa w wysokości 1,7 mln dolarów zainkasował minister komunikacji Bangladeszu w zamian za kontrakt telefonii komórkowej opiewający na 40,9 mln dolarów. Władze Bangladeszu powołały komisję śledczą, która sprawdzała, czy minister nie przeznaczył części pieniędzy od Siemensa na finansowanie organizacji terrorystów islamskich Dżamaat ul-Mudżahedin Bangladesz. Został skazany na 31 lat więzienia za wspieranie terrorystów i 10 lat za przestępstwa finansowe. Jak widać, korupcja generuje kolejne przestępstwa, niepowstrzymana powoduje kolejne patologie.
Z kolei w Rosji kontrakt z przedsiębiorstwem telefonicznym podpisano na następujących zasadach: *50% „prowizji" dla dyrektora generalnego, 40% dla dyrektora technicznego i koniecznie 10% dla głównego księgowego, aby nie „zapomniał" zapłacić przelewem za dostarczoną przez Siemensa technologię.*
Ta i wiele innych spraw ciągnęły się przed niemiecką Temidą wiele lat. Sąd w Monachium dopiero 4 lata temu orzekł, że były dyrektor ds. finansowych Siemensa musi zapłacić dawnemu pracodawcy 15 mln euro odszkodowania. Według sądu nie dopełnił obowiązków i nie zapobiegł ani nie zwalczał korupcji. Zmiany, jakie władze Siemensa zaczęły wdrażać na całym świecie, by ukrócić powyższe praktyki, trwają do dzisiaj. Obecny Siemens pod względem transparentności niewiele ma wspólnego z tym, jakim był jeszcze kilka lat temu.

dzają. Nie budzi również większych wątpliwości, że z tym procederem należy walczyć. Jednak w tej walce zalecam daleko posuniętą ostrożność.

Korupcja jest zjawiskiem trudnym do badania, czymś ulotnym. Tak naprawdę wiedzę o stopniu skorumpowania i zakresu korupcji mają nie ci, którzy o niej czytają czy nawet opowiadają, ale ci, którzy dają łapówki i korumpują, oraz ci, którzy biorą je i dają się skorumpować. A także ci, którzy z racji obowiązków zajmują się jej zwalczaniem i przeciwdziałaniem. Osoby korumpujące i dające się korumpować raczej nie piszą pamiętników i nie chwalą się tym w mediach społecznościowych. Ale obserwując wyniki śledztw, w tym dziennikarskich, można się o tym procederze sporo dowiedzieć.

Jeszcze kilkadziesiąt lat temu przekupywanie polityków i ludzi władzy było powszechnie stosowaną i… dozwoloną praktyką. W wielu krajach, w tym np. w Europie, łapówki można było odliczyć od podatku, wpisując je w koszty prowadzenia działalności gospodarczej. Nadal są kraje, gdzie funkcjonariusze państwa mają niewielkie pensje i włos nie spadnie im z głowy, jeśli dorabią sobie, biorąc „w łapę". Jednym z krajów, który mocno „ucierpiał" z powodu korupcji i gdzie doszło i nadal dochodzi do wielu głośnych afer korupcyjnych, są Stany Zjednoczone Ameryki Płn. Jednocześnie to jeden z krajów, w którym od lat toczy się bezkompromisowa walka z wszelkimi formami korupcji. Wszystko zmieniło się tam za sprawą głośnej afery Watergate, która pociągnęła na dno amerykańskiego prezydenta Richarda Nixona. Tym, którzy nie wiedzą, co tak zbulwersowało Amerykanów, przypomnę, że dochodzenie w sprawie nielegalnych wpłat na kampanię Nixona doprowadziło do ujawnienia *slush funds** w setkach amerykańskich firm. Komisja Papierów Wartościowych i Giełd (*Securities and Exchange Commission* – SEC) wykazała, że 400 przedsiębiorstw wydało setki milionów dolarów, przekupując zagranicą kogo się tylko dało, poczynając od premierów, kończąc na szeregowych policjantach. Po ujawnieniu afery w 1977 r. USA przyjęły pierwszą na świecie ustawę antykorupcyjną (*Foreign Corrupt Practices Act* – FCPA). Na jej mocy przekupywanie zagranicznego funkcjonariusza państwowego lub polityka w celu zawarcia kontraktu stało się nielegalne. Śladem USA podążyły kolejne kraje. Dziś korupcja jest już zjawiskiem powszechnie nieakceptowanym, wręcz piętnowanym. Nie przeszkadza to jednak wielu w „wynagradzaniu" polityków za wprowadzenie korzystnych rozwiązań, rozstrzygnięcie przetargu czy też usunięcie określonych przeszkód prawnych.

Czy więc wprowadzanie wszelkich barier i mechanizmów korupcyjnych pozwala skutecznie zwalczać korupcję? Warto poznać kilka faktów. Po pierwsze minęło ponad 20 lat od czasu, kiedy inne kraje podążyły tą samą drogą co USA i zakazały przekupstwa, uchwalając Konwencję OECD przeciw korupcji. Obecnie ratyfikowało ją 37 krajów, a na całym świecie toczy się 245 spraw dotyczących złamania jej zapisów. Zmiana przepisów i uchwalanie kolejnych ustaw czy zapisów kodeksowych nie eliminuje jednak pokusy sięgania po korupcję. Po drugie zmiana prawa to nie wszystko, zwalczanie korupcji wymaga zmiany mentalności wielu ludzi, od menedżerów po funkcjonariuszy państwa i służb zajmujących się zwalczaniem korupcji. Po trzecie same przepisy nie wystarczą. Przypadki głośnych afer korupcyjnych pozostałyby tajemnicą kilku wpływowych osób, gdyby nie dobra wola odpowiedzialnych za biznes oraz współpraca odpowiedzialnych za wykrywanie i zwalczanie korupcji z tymi, którzy w firmach stali na straży przestrzegania zasad przejrzystości w biznesie.

Czy w Polsce były afery podobnego kalibru? Najgłośniejsza i znana z mediów dotyczyła „nieprawidłowości w przetargach z lat 2007–2010 na zakup sprzętu i usług teleinformatycznych przez CPI (Centrum Projektów i Usług Informatycznych MSWiA). Prokuratura po długim postępowaniu postawiła zarzuty ośmiu osobom, którym groziło do 12 lat pozbawienia wolności. Główny oskarżony w tzw. Infoaferze, czyli Andrzej M., otrzymał 4,5 roku więzienia w zawieszeniu na 8 lat, 93 tys. zł grzywny i przepadek przyjętych korzyści. Doszło do tego w wyniku dobrowolnego poddania się przez A.M. karze, na co zgodziła się prokuratura. Wyrok wydał sąd okręgowy w Warszawie wobec uznawanego za mózg afery byłego szefa CPI, który od przedstawicieli firm informatycznych wziął 1,6 mln zł i 110 tys. zł w postaci komputerów i sprzętu RTV oraz dostał obietnicę kolejnej łapówki 2,5 mln zł. Według prokuratury apelacyjnej w Warszawie A.M. zasłużył na nadzwyczajne złagodzenie kary, ponieważ w śledztwie składał obszerne wyjaśnienia i ujawnił fakty nieznane śledczym. Ponadto orzeczono wobec niego o przepadku korzyści uzyskanych z przestępstw przez niego i troje członków jego rodziny, w tym mieszkania o wartości 800 tys. zł, auta, pieniędzy na kontach oraz wielu luksusowych przedmiotów AGD i RTV. Karom w zawieszeniu wraz z M. poddali się jego żona, ojciec i siostra. Do dzisiaj sprawa nie znalazła finału.

W rodzimych aferach zaskakuje kilka rzeczy – bardzo długi tryb prowadzenia dochodzeń (w ub.r. wyroki zapadające w sprawach korupcyjnych dotyczyły głównie spraw z lat 1999–2014). Głośno jest o śledztwie CBA prowadzonym w Krakowie. Dotyczy ono powoływania się na wpływy w instytucjach państwowych i samorządowych woj. małopolskiego oraz udzielania korzyści majątkowych osobom pełniącym funkcje publiczne w związku z pełnieniem tych funkcji. Wiadomość o zatrzymaniu znalazła się we wszystkich mediach. Ale czy dojdzie do procesu i jakie zapadną wyroki?

Informacja o zatrzymaniu podejrzanych nie oznacza, że są oni winni zarzucanych im czynów, a na pewno nie oznacza, że zgromadzony materiał dowodowy udało się w toku czynności procesowych udowodnić. W przypadku korupcji jest to wyjątkowo trudne. A to niestety sprawia, że korupcja wciąż jest atrakcyjną metodą, tym bardziej że niezmiernie rzadko dochodzi do niej w kraju, w którym potem podejmowane są decyzje i zamieszkują uczestnicy procederu. Dla służb stanowi to sporą przeszkodę, gdyż nie mogą one działać w innych krajach bez współpracy z władzami lokalnymi, które bez przedstawienia twardych dowodów i poszlak mogą odmówić współdziałania.

Informacje o zatrzymaniach nietrudno znaleźć, szczególnie gdy w sprawę są zamieszane głośne nazwiska. Później jednak na

* Termin zaczerpnięty z marynistyki, dosłownie oznacza „fundusz błotny" – na statkach wielorybniczych, gdzie wytapiano tłuszcz, oficerowie sprzedawali producentom łoju zanieczyszczony tłuszcz, który pozostawał na dnie kotłów, a uzyskane z tego dochody były przechowywane w funduszach „błotnych" na dokonywanie niewielkich zakupów na potrzeby załóg statków.

lata zapada milczenie, z wielkim trudem do opinii publicznej przedostają się informacje o skazaniu. To skutkuje bezkarnością i brakiem obaw o konsekwencje.

Ustawa „o jawności życia publicznego" weszła w życie 1 marca. Firmy mają 6 miesięcy na wdrożenie procedur antykorupcyjnych.

Projekt ustawy

Sprawy korupcyjne są bardzo trudne do wykrycia, a jeszcze trudniejsze w aspekcie procesowego udokumentowania. Dlatego nie może dziwić, że w pracach nad tzw. ustawą o jawności życia publicznego kładzie się nacisk na tworzenie w przedsiębiorstwach obowiązkowych procedur antykorupcyjnych, a w konsekwencji pobudzenie właścicieli biznesu do podejmowania praktycznych, namacalnych działań mających eliminować korupcję. Ma to sens, jeśli właściciel przedsiębiorstwa rozumie, iż korupcja jest przejawem patologii wewnątrz organizacji.

Skoro z problemem nie radzą sobie organy państwa, nic dziwnego, że część obowiązków państwo przerzuca na właścicieli i zarządy firm. Nałożony np. na firmy obowiązek opracowania i wdrożenia wewnętrznych procedur postępowania w sprawie zgłaszania nieprawidłowości pozwala na podjęcie innych działań uzdrawiających biznes i tworzących nowe możliwości przeciwdziałania np. wyłudzeniom oraz oszustwom pracowniczym. Warto łączyć przeciwdziałanie korupcji ze szkoleniem, poprawą jakości zarządzania oraz podejmowaniem działań zmierzających do eliminowania strat z tytułu nieuczciwości pracowniczej i likwidacji kosztów z tytułu oszustw.

Na firmy (tylko średnie i duże) wkrótce zostanie nałożony obowiązek wdrożenia programu antykorupcyjnego, który powinien zawierać co najmniej następujące elementy:

- kodeks etyki – podpisany przez każdego pracownika, współpracownika i inny podmiot gospodarczy działający na rzecz przedsiębiorcy,
- klauzule antykorupcyjne – umieszczane obowiązkowo w umowach jako klauzule stanowiące, iż żadna część wynagrodzenia z tytułu wykonania umowy nie zostanie przeznaczona na pokrycie kosztów udzielania korzyści majątkowych i osobistych,
- procedury i wytyczne dotyczące otrzymywanych prezentów,
- szkolenia – zapoznawanie osób zatrudnianych przez przedsiębiorcę z zasadami odpowiedzialności karnej za przestępstwa korupcyjne,
- procedury związane z *whistleblowingiem*, w tym opracowanie procedur informowania właściwych organów przedsiębiorcy o propozycjach korupcyjnych,
- dochodzenia wewnętrzne – opracowanie wewnętrznych procedur postępowania w sprawie zgłoszenia nieprawidłowości oraz prowadzenia dochodzeń,
- niedopuszczanie do tworzenia tzw. funduszy korupcyjnych,
- niepodejmowanie decyzji w oparciu o działania korupcyjne.

W projekcie ustawy utrzymano sankcje za brak, pozorność lub nieskuteczność systemów antykorupcyjnych, czyli karę pieniężną do 10 mln zł i zakaz ubiegania się o zamówienia publiczne przez 5 lat. Dla firm, które z takich przetargów się utrzymują, samo ustanowienie powyższych procedur i zapisów oraz klauzul w umowach z klientami nie będzie wystarczające. Niezbędne będzie powołanie własnych komórek zajmujących się korupcją albo wynajęcie profesjonalnych firm zewnętrznych zajmujących się m.in. przeciwdziałaniem praktykom korupcyjnym, które przejmą obowiązek kontrolowania tej sfery działalności przedsiębiorstw w Polsce. Istnieje obawa, iż nasz rynek, nierzadko branżowo skonfliktowany, w walce o kontrakty i zamówienia może sięgnąć po ostre i niezbyt „sympatyczne" środki – wykorzystując np. anonimowe donosy, które mogą uderzyć w biznes. Już dzisiaj wiele firm może mieć problemy z powodu zemsty niezadowolonych i zawiedzionych pracowników, kontrahentów czy wrogo nastawionych konkurentów. Urzędy skarbowe potwierdzają, że mają obowiązek sprawdzenia każdej informacji, jaka do nich spływa kanałami operacyjnymi, w tym poprzez przesyłane donosy. Do jednostek Ministerstwa Finansów niedługo dołączy CBA.

Nowe przepisy również mogą tworzyć nowe rodzaje ryzyka, uderzając nie tylko w korumpujących i skorumpowanych, ale także w nieprzygotowanych do obrony i uczciwych przedsiębiorców. Już dzisiaj wielu z nich ma obawy, czy czyjaś zła wola nie spowoduje, że firma zostanie postawiona w trudnej sytuacji tylko dlatego, że ktoś wie więcej niż zarząd czy właściciel i wykorzysta to, by uderzyć w firmę. Ale na to jest tylko jedna rada – trzeba temu przeciwdziałać i nie czekać na ostatni moment, kiedy do firmy zapuka fiskus czy CBA.

Ustawa „o jawności" jest poprawiana, na etapie dyskusji w sejmie może ulec zmianie. Ustawa powinna weść w życie 1 marca 2018 r., ale ta data jest wciąż przesuwana. Firmy będą miały sześć miesięcy na wdrożenie lub dostosowanie swoich procedur antykorupcyjnych. To niewiele czasu. Z korupcją należy walczyć i państwo nie może rezygnować ze swojej w tym roli. Przenoszenie na obywateli ciężarów związanych z walką z korupcją będzie generować zagrożenia i ryzyko u tych, którzy transparentnie prowadzą biznes. Czy utrudnią tworzenie *slush funds*? Czy korupcja stanie się mniej opłacalna? Czy ryzyko „wpadki" się zwiększy? Czy obywatele skorzystają z nowych możliwości, by dzielić się swoimi spostrzeżeniami? Czy zwalczanie korupcji w firmach znajdzie wsparcie i nowe siły? Wkrótce się o tym przekonamy. W innych krajach nawet najbardziej doskonałe przepisy prawne oraz coraz lepiej wyszkolone i wyposażone organy ścigania częściej wykrywają działania korupcyjne. Ale korupcja, łapownictwo czy płatna protekcja nadal znajdują chętnych mimo kar za to grożących.

Jedno jest pewne – problem, który niedawno interesował dziennikarzy i opinię publiczną oraz część przedstawicieli biznesu, dzisiaj stał się problemem wszystkich. Problemem, obok którego nie można przejść obojętnie, ale trzeba podjąć odpowiednie działania. Konsekwencje zaniechania mogą być dolegliwe.

BIO

Michał Czuma
Wiceprezes i współwłaściciel G+C Kancelaria Doradców Biznesowych. Wcześniej stworzył i zarządzał pierwszymi w kraju Biurami Antyfraudowymi w spółkach grupy PKO BP. Były wieloletni z-ca dyrektora Departamentu Bezpieczeństwa PKO BP.

CYWILNY NADZÓR POLITYCZNY

nad

SŁUŻBAMI SPECJALNYMI

W PAŃSTWACH DEMOKRATYCZNYCH

Marek Ryszkowski

Przedstawiony w zarysie problem być może zainteresuje Czytelników „a&s Polska”, choć jest odstępstwem od głównej tematyki czasopisma, która dotyczy przede wszystkim problemów funkcjonowania polskiej branży ochrony osób i mienia.

Cywilny nadzór polityczny nad służbami specjalnymi jest niezbędny. Problemem jest to, by był skuteczny. Służby muszą być nadzorowane, w demokratycznym państwie prawnym bowiem powinny one – a nawet są do tego prawnie zobowiązane – działać w granicach prawa i zgodnie z prawem. Tymczasem wielu zorientowanych głosi tezę, że to nie służby są nadzorowane przez polityków, lecz politycy przez służby, a bywa, że niektórzy z nich z pomocą służb specjalnych są wynoszeni do władzy i potem sterowani przez ich funkcjonariuszy podczas pełnienia swoich funkcji/obowiązków politycznych lub administracyjnych.

W wielu państwach demokratycznych, zwłaszcza tych o statusie mocarstwa światowego mającego interesy polityczne, gospodarcze, wojskowe i inne w wielu regionach naszego globu, służb specjalnych posiadających uprawnienia do prowadzenia czynności operacyjnych (w tym inwigilacyjnych) bywa nawet kilkanaście. Koordynacja i nadzór polityczny nad ich poczynaniami jest problemem niemal równie skomplikowanym, jak rozwiązanie węzła gordyjskiego. Aleksander Wielki, sławny król i wódz macedoński, pokazał, jak „rozwiązać" węzeł gordyjski – rozciął go mieczem. Może jest to metoda na skuteczny „nadzór polityczny nad służbami specjalnymi w państwach demokratycznych", oczywiście bez użycia miecza w stosunku do tych szefów służb i wszystkich innych, nie tylko funkcjonariuszy służb, którzy sabotują funkcjonowanie tego nadzoru.

Historia wielu służb specjalnych, nazywanych często specsłużbami, dostarcza argumentów na uzasadnienie tezy, że powinny one podlegać ścisłej kontroli, najlepiej specjalnych komisji parlamentarnych o rozległych kompetencjach nadzorczo-kontrolnych. W państwach, gdzie istnieje więcej niż jedna służba specjalna, niezbędna jest ścisła koordynacja ich poczynań, mająca na celu pobudzanie zdrowego ich współzawodnictwa, rozgraniczenie sfer ich działania oraz łagodzenie nieuniknionych konfliktów i nieporozumień.

Służby muszą być nadzorowane, w demokratycznym państwie prawnym powinny one (a nawet są do tego prawnie zobowiązane) działać w granicach prawa i zgodnie z prawem.

Brak ścisłego nadzoru i koordynacji poczynań służb specjalnych może mieć niekiedy katastrofalne następstwa. Wiele napisano na ten temat, krytykując za brak koordynacji działań i wymiany informacji wywiadowczych amerykańskie oraz rosyjskie służby specjalne (których w każdym z tych państw jest wiele) po zamachach terrorystycznych w Nowym Jorku i Waszyngtonie we wrześniu 2001 r.[1] oraz w Moskwie w październiku 2002 r. Sięgając natomiast do przeszłości, można zaryzykować tezę, iż konflikt między hitlerowskimi Abwehrą[2] a Sicherheitsdienstem[3] (SD), wynikający zapewne z braku należytej kontroli i koordynacji ich poczynań, nieporozumień i ambicji personalnych ich szefów (admirała Wilhelma Canarisa i SS-obergruppenführera Reinharda Tristana Eugena Heydricha), a może z celowej polityki w tym względzie Adolfa Hitlera[4], z pewnością *sprawiał, że i tak już dostatecznie niewdzięczne zadanie – walka z agentami brytyjskimi, radzieckimi i amerykańskimi w kraju i za granicą – stawała się dla Niemców jeszcze trudniejsza*[5].

Konflikt zakończył się likwidacją Abwehry oraz aresztowaniem i zamordowaniem jej szefa, admirała Wilhelma Canarisa. Aresztował go osobiście SS-brigadeführer, Walter Schellenberg, szef wywiadu SD, co zupełnie nie zdziwiło Canarisa, który w chwili aresztowania miał zauważyć: *Wiedziałem, że to będzie pan*[6].

W tym miejscu nie od rzeczy będzie zamieszczenie, jako dygresji, dwu informacji. Pierwsza mówi o tym, że W. Schellenberg rozgłaszał, iż to Nicolai[7] zasugerował, żeby wysłać Lenina do Rosji w zaplombowanym[8] wagonie kolejowym przez Niemcy po tym, jak ówczesny habsburski cesarz Karol, drażliwy na punkcie rosyjskiej rewolucji i jej wpływu na jego imperium, nie zgodził się, by Lenin dotarł do Rosji najkrótszą drogą ze Szwajcarii do Rosji przez Austrię[9].

Druga sugeruje, że W. Canarisa cechowało pewne dziwactwo, będąc już bowiem szefem Abwehry, okazywał podobno niechęć, a niekiedy nienawiść do ludzi z małymi uszami i o okazałej posturze, co mogło wynikać stąd, że sam był wzrostu niezbyt okazałego, a jego uszy nie należały do małych[10]. Zdaniem autora duże uszy i nierzucająca się w oczy postura są raczej zaletą niż wadą, zwłaszcza u człowieka zajmującego się tym, czym przez wiele lat zajmował się Wilhelm Canaris. W Polsce pracowników specsłużb określa się potocznie mianem „gumowe ucho". Duże ucho, co potwierdzi każdy laryngolog, słyszy lepiej niż ucho małe.

Polityczny (parlamentarny) nadzór cywilny nad służbami specjalnymi w Wielkiej Brytanii

Organizacja skutecznego, politycznego (parlamentarnego) nadzoru i kontroli nad służbami specjalnymi jest z pewnością nie tylko problemem polskim, ale także światowym. Warto zatem prześledzić, jak radzili i radzą sobie z nim – a może nie radzą – w Wielkiej Brytanii, która szczyci się jed-

1) Patrz szerzej [w:] J.F. Hoge (red.) i G. Rose, 11 września 2001. *Jak to się stało i co dalej?* Wyd. AMBER, Warszawa 2001.
2) Wojskowy wywiad i kontrwywiad III Rzeszy Niemieckiej.
3) Służba bezpieczeństwa partii hitlerowskiej NSDAP.
4) Może to przypadek stosowania przez tego wodza starożytnej zasady „dziel i rządź"; (łac. *divide et impera*).
5) Praca zb. (red.). Z. Foniok, *Wojna szpiegów 1939 - 1945*, Wydawnictwo AMBER, Warszawa 2001, str. 51.
6) W. Kozaczuk, *II wojna światowa - wywiad i kontrwywiad.* Krajowa Agencja Wydawnicza, Warszawa 1986. Zeszyt 23, str. 78.
7) Płk Walter Nicolai, od 1912 roku szef wywiadu cesarskiej armii niemieckiej.
8) Wagon podobno nie był zaplombowany.
9) Szerzej [w:] R. Bassett, *Arcyszpieg Hitlera,* Wydawnictwo AMBER, Warszawa 2006, str. 35.
10) Tamże, str. 80

nymi z najstarszych i najskuteczniejszych w Europie służbami wywiadu i kontrwywiadu. W tym celu warto zajrzeć do książki Sebastiana Michalaka, *O służbach specjalnych w brytyjskim parlamencie. Dzieje parlamentarnej kontroli służb specjalnych Wielkiej Brytanii* (1909–1994), którą wydało Wydawnictwo Trio, Warszawa 2006. Książka ta, oparta na badaniach naukowych, przeprowadzonych przez jej autora na potrzeby rozprawy doktorskiej, została przez polski rynek wydawniczy prawie niezauważona. A szkoda, zawiera bowiem niemało informacji przydatnych tym, którzy interesują się i/lub próbują wykonywać nadzór polityczny (parlamentarny) nad polskimi służbami specjalnymi.
Na stronie 44 książki Sebastian Michalak zawarł następującą myśl, z którą nie zamierzam polemizować:
Najistotniejszym problemem dotyczącym kontroli nad służbami wywiadowczymi jest zapewnienie środowiska koniecznego do realizacji ich zadań. Tajne służby prowadzą działania w tajemnicy, dlatego że oddziałuje to bezpośrednio na ich skuteczność. Ta okoliczność wpływa na tworzone ciała kontrolne, które powinny zapewnić służbom możliwość pracy adekwatną do jej specyfiki, a jednocześnie gwarantować, by nie naruszała prawa. Oprócz poszanowania prawa równie istotnym warunkiem jest ochrona zasadniczych w systemie demokratycznym wolności obywatelskich, z którymi służby [specjalne – przyp. aut.] *nieuchronnie i wielokrotnie wchodzą w kolizję.*
Wywiad działający poza granicami kraju, który go powołał, narusza prawa krajów, w których prowadzi swoje operacje. Z kolei kontrwywiad, działający przede wszystkim w kraju, który go powołał, narusza – jeżeli to czyni – prawa kraju macierzystego, zatem – w odniesieniu do działań kontrwywiadu – powyższa uwaga wydaje się bardziej trafna.

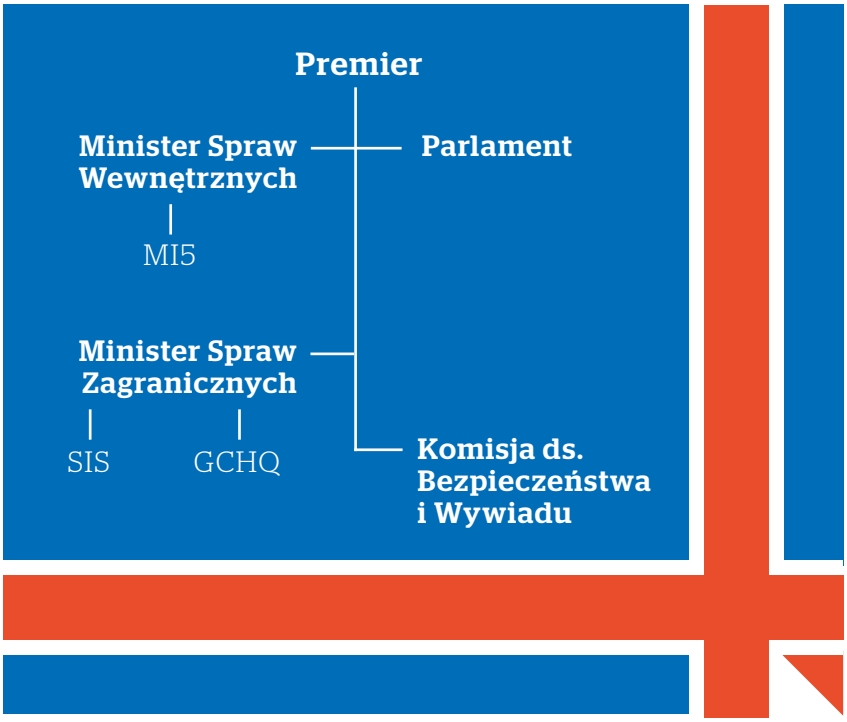
* * *

Zamiast szczegółowo przedstawiać historię parlamentarnej – i nie tylko – kontroli politycznej nad brytyjskimi służbami specjalnymi zostanie zamieszczony schemat tej kontroli oraz kilka uwag natury ogólnej, którymi autor cytowanej książki zakończył swoje rozważania nad dziejami parlamentarnej (politycznej) kontroli specsłużb w Wielkiej Brytanii.

Oto uwagi natury ogólnej, o których była mowa:

1. W latach 1909–1994[11] parlament brytyjski sprawował bezpośrednią kontrolę nad służbami specjalnymi. Była to jednak kontrola śladowa i zasadniczo ograniczała się do sprawdzania preliminarzy[12] ich funduszy.
2. W drugiej połowie lat 50. XX wieku posłowie laburzystowscy[13] podejmowali w izbie niższej (Izba Gmin) problematykę związaną z przejawami ingerencji specsłużb w życie codzienne obywateli, zwłaszcza poprzez stosowanie podsłuchów telefonicznych.
3. Afery szpiegowskie z lat 1945–1965 wykazały niewystarczającą skuteczność brytyjskiego kontrwywiadu i spowodowały wzrost zainteresowania parlamentarzystów informacjami o powodach tego stanu. Świadczą o tym liczne wystąpienia przed parlamentem przedstawicieli rządu brytyjskiego, wyjaśniających rolę i zasady ministerialnego nadzoru nad specsłużbami.
4. W trakcie dyskusji parlamentarnych po wystąpieniach przedstawicieli rządu oceniono, że stan parlamentarnej kontroli nad służbami specjalnymi […] wskazuje, że […] była ona znikoma (str. 279–280).
5. W latach 1966–1978 dominującą formą parlamentarnej kontroli nad służbami specjalnymi były tzw. pytania pisemne, kierowane przez parlamentarzystów do przedstawicieli rządu, głównie w sprawach działania kontrwywiadu. Taka forma kontroli utrzymywała się do 1994 r.

System parlamentarnej i ministerialnej kontroli nad służbami specjalnymi w Wielkiej Brytanii



LEGENDA:
MI5 – Służba Bezpieczeństwa (*Security Service*); kontrwywiad brytyjski.
SIS – Tajna Służba Wywiadowcza (*Secret Intelligence Service*), wywiad brytyjski, określany także jako MI6.
GCHQ – Zarząd Główny Łączności Rządowej (*Government Communications Headquarters*), następca Rządowej Szkoły Kodów i Szyfrów (*Government Code and Cipher School*).

Źródło: Michalak S., *O służbach specjalnych w brytyjskim parlamencie. Dzieje parlamentarnej kontroli służb specjalnych Wielkiej Brytanii (1909–1994)*, str. 273.

6. W latach 1979–1983 działała grupa studyjna Partii Pracy, która zbadała zagadnienia kontroli parlamentarnej nad służbami specjalnymi. Grupa ta postulowała powołanie specjalnej komisji parlamentarnej w celu kontrolowania specsłużb, uregulowania zasad wykorzystywania przez nie technicznych środków operacyjnych i zintensyfikowania bezpośredniej kontroli władzy ustawodawczej nad tymi służbami. Postulaty te uzyskały poparcie wszystkich w zasadzie sił politycznych reprezentowanych w brytyjskim parlamencie, z wyjątkiem posłów[14] i parów z Partii Konserwatywnej.
7. W latach 1986–1988 dyskusje parlamentarne nt. służb specjalnych były zdominowane rewelacjami na ich temat, zawartymi w książce Petera Wrighta *Łowca szpiegów*[15], który opisał w niej wiele przypadków działania brytyjskich specsłużb na granicy prawa lub jej przekraczania. Ich ciężar gatunkowy powodował, że dostrzegano silną potrzebę zintensyfikowania kontroli parlamentarnej nad tymi służbami, zwłaszcza nad kontrwywiadem.
8. W roku 1994 główne siły polityczne w parlamencie brytyjskim zaakceptowały powołanie komisji ds. wywiadu i bezpieczeństwa, organu pośredniej kontroli i nadzoru służb specjalnych. W skład komisji weszli parlamentarzyści obu izb parlamentu, jednak nie podlegali oni w swoich działaniach parlamentowi, lecz premierowi.
9. W roku 1998, a więc już poza okresem, który objął badaniami naukowymi S. Michalak, rząd brytyjski zrealizował propozycję komisji ds. wywiadu i bezpieczeństwa, powołując oficera śledczego, którego zadaniem miało być wspieranie czynności kontrolnych komisji. Wspomina o tym autor książki na str. 283–284.
10. Ostateczna ocena przez S. Michalaka skuteczności wszystkich wspomnianych zabiegów, mających na celu zintensyfikowanie i zwiększenie skuteczności parla-

Organizacja skutecznego politycznego (parlamentarnego) nadzoru i kontroli nad służbami specjalnymi jest z pewnością problemem światowym.

mentarnej i ministerialnej kontroli/nadzoru nad brytyjskimi służbami specjalnymi brzmi pesymistycznie: *W świetle badań nad dziejami parlamentarnej kontroli* (nad specsłużbami – przyp. aut.) *widać, że właściwie od lat sześćdziesiątych* (XX wieku – przyp. aut.) *brytyjski parlament tracił na znaczeniu* (str. 282).

Dla polskiego czytelnika brzmi to tym bardziej pesymistycznie, bo skoro tak „stary" i doświadczony parlamentaryzm brytyjski nie poradził sobie z tym problemem, jak możemy oczekiwać, że nasz parlament upora się z tym problemem lepiej niż brytyjski. W Wielkiej Brytanii podejmowano także, zwłaszcza w okresach wojen, liczne działania na szczeblu rządowym, ukierunkowane na polepszenie sprawności wywiadu w zdobywaniu danych o przeciwnikach wojennych, a także kontrwywiadu, od którego oczekiwano uniemożliwienia agentom wrogich wywiadów przeciwników wojennych działania na terenie wysp macierzystych i wszędzie tam, gdzie mogli oni naruszyć swoimi działaniami brytyjskie interesy wojenne i inne.

Parlamentarna (polityczna) kontrola służb specjalnych w Stanach Zjednoczonych Ameryki Północnej (USA)

W USA o profesjonalnym i skutecznym wywiadzie zagranicznym można mówić dopiero od momentu, gdy zostały one uwikłane w działania zbrojne I wojny światowej. Jednak zaraz po jej zwycięskim zakończeniu tę służbę specjalną zdegradowano i pozbawiono możliwości sprawnego działania, podobnie jak całe siły zbrojne. Przyczyną takiego stanu rzeczy była zapewne polityka rządu USA, polegająca na niemieszaniu się w sprawy europejskie i inne, jeżeli nie naruszały one interesów tego państwa (polityka izolacjonizmu). Dopiero wybuch II wojny światowej, zwłaszcza zaatakowanie USA przez Japonię i w następstwie tego aktu agresji wypowiedzenie USA wojny przez Niemcy, spowodował szybki rozwój w tym państwie wywiadu zagranicznego, w tym wojskowego. W roku 1942 powołano OSS – Biuro Służb Strategicznych (*Office of Strategic Services*), które istniało do 1946 r. Po zwycięskim dla USA zakończeniu II wojny światowej ponownie zdegradowano działający dość sprawnie podczas wojny wywiad zagraniczny, w tym wojskowy, likwidując OSS. Ze względu jednak na pogarszanie się sytuacji międzynarodowej (narastanie konfliktów między niedawnymi sojusznikami wojennymi, zwłaszcza USA i ZSRR) szybko zaprzestano degradowania wywiadu i przystąpiono do jego rozbudowy. Jeszcze w 1946 r. w miejsce OSS powołano organizację CIG – Grupę Centrali Wywiadu (*Central Intelligence Group*), która istniała jedynie kilkanaście miesięcy. Już w roku 1947 utworzono CIA – Centralną Agencję Wywiadowczą (*Central Intelligence Agency*), która szybko osiągnęła olbrzymie rozmiary i zasięg działania, stając się jedną z największych i najważniejszych na świecie służb specjalnych drugiej połowy XX wieku i w wieku XXI. Istnieje ona i aktywnie działa do dzisiaj.
Za działania kontrwywiadowcze na terenie USA odpowiada FBI – Federalne Biuro Śledcze (*Federal Bureau of Investigation*), które powołano w 1908 r. (pod inną nazwą). Obecną nazwę nadano FBI w 1935 r. Przez lata działania FBI i innych organizacji o charakterze specsłużb, np. CIA, trudno mówić o parlamentarnej (politycznej) kontroli/nadzorze ich poczynań w kraju i poza granicami USA. Pomimo licznych sygnałów, które docierały do

11) Taki okres kontroli działalności brytyjskich służb specjalnych objął badaniem naukowym Sebastian Michalak.
12) Preliminarz – wykaz przewidywanych dochodów i rozchodów; projekt jednostkowego planu finansowego danej specsłużby.
13) Posłowie lewicy parlamentarnej z Partii Pracy (ang. *Labour Party*).
14) Członków Izby Lordów.
15) Wydanie polskie – Wydawnictwo Officina, Warszawa 1991.

Historia wielu służb specjalnych dostarcza argumentów na uzasadnienie tezy, że powinny one podlegać ścisłej kontroli, najlepiej specjalnych komisji parlamentarnych o rozległych kompetencjach nadzorczo-kontrolnych.

opinii publicznej w USA – i nie tylko – o różnych uchybieniach, w tym prawnych, popełnianych przez funkcjonariuszy tych służb, z jakichś powodów takiej kontroli/nadzoru parlamentarnego nie zorganizowano.

Dopiero w latach 1975–1976 Kongres USA przeprowadził dochodzenia w sprawie nadużyć CIA, które wzburzały od lat opinię publiczną w USA. W następstwie tego dochodzenia obie izby Kongresu USA (Izba Reprezentantów i Senat) powołały stałe komisje ds. wywiadu, których zadaniem miało być m.in. kontrolowanie FBI i CIA. Do tego celu Senat powołał w 1976 r. Komisję Specjalną Senatu ds. Wywiadu (*Senate Select Committee on Intelligence*). Izba Reprezentantów natomiast dokonała tego w 1977 r., powołując Komisję Specjalną Izby Reprezentantów ds. Wywiadu (*House Permanent Select Committee on Intelligence*).

Od 1980 r., z mocy przepisów ustawy o kontroli wywiadu (*The Intelligence Oversight Act*), finansowanie wszystkich tajnych operacji wywiadu USA wymaga zgody obu ww. komisji. Ponadto komisja senacka na mocy tego aktu uzyskała prawo do zatwierdzania nominacji na dyrektora CIA[16].

Tak zorganizowana kontrola parlamentarna i nadzór polityczny nad amerykańskimi specsłużbami mają szansę być skuteczniejsze. Ale czy takie są? Na to pytanie mogą odpowiedzieć jedynie kongresmeni i senatorowie wchodzący w skład tych komisji.

Kontrola parlamentarna i nadzór polityczny nad służbami specjalnymi w Australii

W Australii kontrolę parlamentarną i nadzór polityczny nad służbami specjalnymi wprowadzono w 1979 r. na podstawie regulacji ustawy o Australijskiej Organizacji Bezpieczeństwa i Wywiadu (ASIO – *Australian Security and Intelligence Organisation*). W celu prowadzenia tej kontroli i nadzoru utworzono Połączoną Parlamentarną Komisję ds. Australijskiej Organizacji Bezpieczeństwa i Wywiadu (*Parliamentary Joint Committee on the Australian Security and Intelligence Organisation*). W jej skład wchodzi siedmiu członków – trzech z Senatu i czterech z Izby Reprezentantów. Senatorów powoływał przywódca partii rządzącej w Senacie (*Leader of the Government in the Senate*), natomiast członków Izby Reprezentantów wybranych rezolucją tej izby – premier, po konsultacji z przywódcami partii opozycyjnych mających reprezentację w izbie. Komisja miała prawo badać określone formy funkcjonowania ASIO na polecenie ministra sprawiedliwości, który odpowiadał za kontrwywiad ASIO, lub na mocy uchwały jednej z izb parlamentu. Komisja, o której mowa, nie mogła badać źródeł i metod gromadzenia przez ASIO informacji niejawnych.

Wiedza o tym, jak skuteczny w działaniach kontrolno-nadzorczych jest ww. system nadzoru parlamentarnego i politycznego nad australijskimi służbami specjalnymi, jest w Polsce niewielka.

* * *

Z danych, które w trakcie badań naukowych problemów z nadzorem parlamentarnym (politycznym) nad służbami specjalnymi Wielkiej Brytanii i niektórych innych państw demokratycznych, które przeprowadził S. Michalak, wynika, że przez wiele dziesięcioleci były one zapewne poddane jakimś formom kontroli i nadzoru, wykonywanym jednak raczej przez organy rządowe tych państw i tylko doraźnie przez ich parlamenty. Dopiero chyba pod presją opinii publicznej, która reagowała coraz ostrzej na ujawniane przez wolne media przypadki afer o różnym charakterze w służbach specjalnych, powołano w parlamentach lub złożone z parlamentarzystów komisje kontrolno-nadzorcze, uprawnione do stałej lub okresowej obserwacji poczynań specsłużb pod kątem ich zgodności z prawem, zwłaszcza kraju macierzystego, który je powołał. Niestety w dostępnych źródłach brak danych o sukcesach tych komisji w prowadzonych przez nie czynnościach nadzorczo-kontrolnych.

Opis systemu parlamentarnej (politycznej) kontroli polskich służb specjalnych i ocena jego skuteczności wykraczają poza ramy tego artykułu. Jest to zagadnienie domagające się naukowego zbadania i opracowania. Może podejmie się tego zadania jakiś doktorant z wyższej uczelni, w której funkcjonuje wydział bezpieczeństwa narodowego lub kierunek studiów o takiej specjalności, i znajdzie promotora, który pokieruje naukowo tym badaniem.

[16] Patrz: S. Michalak S.: *O służbach specjalnych w brytyjskim parlamencie...*, dz. cyt. str. 154.

SECUREX 2018 – Złote Medale MTP

Międzynarodowe Targi Zabezpieczeń SECUREX 2018 w Poznaniu to jedno z najważniejszych wydarzeń branży security w Europie Środkowej. Odbywają się w cyklu dwuletnim, w tym roku 23-26 kwietnia. Wystawie towarzyszą konferencje branżowe oraz uroczyste wręczenie Złotych Medali Międzynarodowych Targów Poznańskich. Oto lista nagrodzonych produktów:

Wszystkie przyznane Złote Medale MTP są równoważne. Lista ułożona alfabetycznie wg nazw producentów.

AFG Elektronika Przemysłowa Maciej Garczarek, Poznań
- Centrala sterująca automatyką pożarową typu AFG-3

AMBIENT SYSTEM, Gdańsk
- MiniVES – zintegrowany kompaktowy system

ARGUS Security, Włochy (zgłaszający: Creatio Arkadiusz Waligóra, Milicz)
- SAGITTARIUS® – bezprzewodowy system detekcji pożaru

BT ELECTRONICS, Kraków
- SAIK TUBE – zabezpieczone klucze do drzwi wejściowych

Dahua Technology Poland
- HAC-PFW3601-A180 – kamera multisensorowa tulejowa 180° HDCVI, 3 x 2 Mpix.
- TPC-BF2120 – kamera bispektralna
- NKB5000 – klawiatura sieciowa
- XVR5216AN-4KL-16P – rejestrator wielosystemowy

DMSI Software, Warszawa
- SAFESTAR – oprogramowanie

EBS, Warszawa
- Zestaw do mobilnego programowania central alarmowych z aplikacją ava install app

G+M Elektronik, Szwajcaria (zgłaszający: Schrack Seconet Polska)
- APS-180-LOOP. Moduł linii pętlowych z izolatorami

Hikvision Poland
- DS-2DF6A236X–AEL – kamera sieciowa PTZ
- DS-2TD2636–10/15 – kamera bispektralna typu *bullet*
- DS-2TD8166–180ZE2F – kamera bispektralna sieciowa na głowicy pozycjonującej
- 2DF8250I5X–AEL(W) – kamera obrotowa
- DS-2DF8225IH–AEL – kamera obrotowa *DarkFighterX*

- DS-2CD6A64F–IHSNFC2 – kamera panoramiczna
- iDS–96128NXI – I24 – rejestrator sieciowy
- iDS–2CD8426G0/F-I + iDS–9632NXI – I8/4F – rozwiązanie do rozpoznawania twarzy

LINC Polska, Poznań
- FFT AURA Ai-2 – światłowodowy system ochrony perymetrycznej

PULSAR Krzysztof Bogusz, Łapczyca
- System zasilania DSO 24 V do systemu Paviro firmy Bosch

RABAN, Swarzędz
- Senstar LM100 – napłotowy, hybrydowy system detekcji intruza

RONYO Technologies, Czechy, (zgłaszający: RCS Engineering, Czechy)
- VARYA PERIMETER – bezprzewodowy system ochrony perymetrycznej wykorzystujący RFID

SATEL, Gdańsk
- INTEGRUM oprogramowanie zarządzające rozproszonymi instalacjami elektronicznych systemów zabezpieczeń

Schrack Seconet Polska
- Integral WAN – sieć central sygnalizacji pożarowej i sterowania urządzeniami przeciwpożarowymi serii Integral IP. Integracja obiektów rozproszonych

Somfy, Warszawa
- SOMFY ONE+ – system alarmowy ze zintegrowaną kamerą

TELBUD, Poznań
- ARGUS 3D – profesjonalny system sterowania i nadzoru klasy PSIM

UAVS Poland, Kraków
- Bezzałogowy Statek Powietrzny DC-01 Mucha wraz z głowicą obserwacyjną oraz Lekką Mobilną Stacją Kierowania i Kontroli

W2 Włodzimierz Wyrzykowski, Białe Błota
- Sygnalizator głosowy pożarowy SGPgw2

XTRALIS, Australia (zgłaszający: XTRALIS UK, Wielka Brytania)
- Detektor zasysający VESDA-E, model VEA-040-A10

Do konkursu o Złoty Medal Międzynarodowych Targów Poznańskich rocznie startuje niemal 500 produktów. Jednak tylko te z nich, które spełnią regulaminowe kryteria i zyskają pozytywne rekomendacje profesjonalnego jury, otrzymują to prestiżowe wyróżnienie.

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

Złote medale dla Schrack Seconet

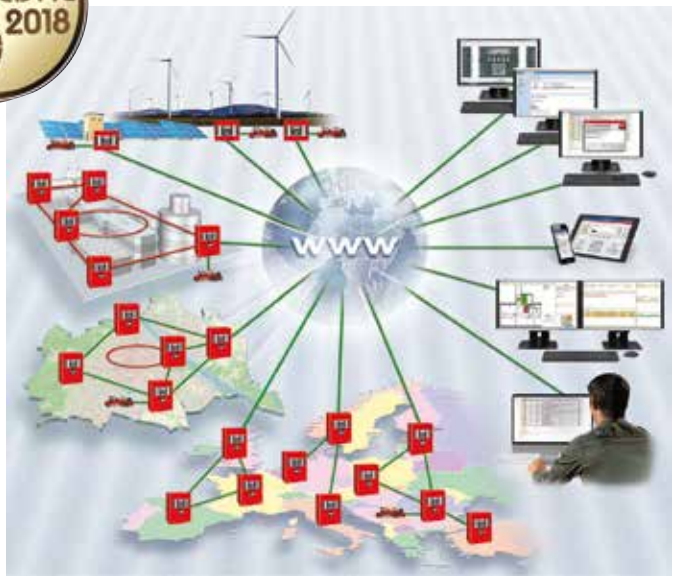
Firma Schrack Seconet Polska została podwójnym laureatem konkursu *Złoty Medal Międzynarodowych Targów Poznańskich – SECUREX 2018*. To jedna z najbardziej prestiżowych i rozpoznawalnych nagród na polskim rynku, którą otrzymują wyłącznie najlepsze produkty – najbardziej innowacyjne i wykonane przy użyciu najnowszych technologii.

Krzysztof Kunecki
dyrektor ds. technicznych,
Schrack Seconet Polska

Pierwszy Złoty Medal MTP został przyznany **Integral WAN – najnowszej sieci central sygnalizacji pożarowej/sterowania urządzeniami ppoż. serii Integral IP (MX, CX, BX)**, stosowanej do łączenia dużej liczby central w jeden spójny system bezpieczeństwa pożarowego, a także do integrowania obiektów rozproszonych (niezależnych instalacji) i centralnego zarządzania nimi.

Rozwiązanie charakteryzuje się bardzo wysoką niezawodnością działania m.in. ze względu na zastosowanie redundantnych kart sieciowych należących do nowej generacji platform B5A i B6A systemu Integral IP. Ponadto bardzo elastyczna architektura sieci pozwala na zastosowanie różnych topologii sieciowych (pierścień, drzewo lub sieć kratowa) spełniających wymagania konkretnego projektu. W zależności od zastosowanej topologii sieciowej i liczby torów komunikacyjnych system może być odporny na trzy niezależne uszkodzenia (topologia pierścienia) lub nawet siedem niezależnych uszkodzeń (topologia sieci kratowej).

Centrale łączy się przewodami miedzianymi (skrętką) lub łączami światłowodowymi jedno- i wielomodowymi. Przy zastosowaniu torów światłowodowych prędkość transmisji danych w sieci wynosi aż 100 Mb/s. W celu zintegrowania central w zakresie związanym z przekazywaniem informacji może zostać wykorzystana istniejąca infrastruktura IT danego obiektu (sieć LAN), a nawet sieć rozległa typu WAN.



Sieć Integral WAN umożliwia połączenie central najnowszych platform B5A i B6A ze starszymi (kompatybilność wstecz) w jeden spójny system. Do zarządzania całym układem sieciowym Integral WAN może być wykorzystywany system integrujący urządzenia ppoż. SIS-FIRE oraz rozwiązania technologii *Integral over IP*.

Drugim Złotym Medalem MTP eksperci wyróżnili **APS-180-LOOP – moduł linii pętlowych z izolatorami zwarć Dźwiękowego Systemu Ostrzegawczego APS®-APROSYS**.

Rozwiązanie to – dzięki zastosowaniu topologii pętli i dodatkowych izolatorów zwarć w linii – znacznie zwiększa bezpieczeństwo nagłaśnianych stref. W przypadku wystąpienia zwarcia lub przerwy w linii pętlowej izolatory zwarć izolują jedynie uszkodzony fragment linii pętlowej i poprzez obustronne zasilanie linii głośnikowych umożliwiają dalszą pracę sprawnej części instalacji. To decyduje o znacznej przewadze technicznej APS-180-LOOP w porównaniu ze standardowymi liniami otwartymi/promieniowymi, gdzie w przypadku wystąpienia zwarcia uszkodzeniu ulega cała linia, co z kolei często powoduje utratę 50% całkowitego nagłośnienia w danej strefie. Dzięki adresowalnym izolatorom zwarć można znacznie szybciej zlokalizować i naprawić uszkodzenie, które wystąpiło w linii, oraz szybciej przywrócić pełną sprawność instalacji.

Funkcja DSO (dźwiękowego systemu ostrzegawczego) APS®-APROSYS pozwala na podwyższenie niezawodności instalacji i – co za tym idzie – również bezpieczeństwa osób przebywających w obiekcie.

System APS®-APROSYS charakteryzuje się elastyczną, modułową architekturą zapewniającą dostosowanie systemu do wymagań użytkownika oraz możliwość łatwej i praktycznie nieograniczonej rozbudowy systemu w układach sieciowych.

APS®-APROSYS został wyposażony w fabrycznie zintegrowane zasilanie bateryjne oparte na akumulatorach o pojemności 24 Ah, co znacząco ułatwia eksploatację i konserwację systemu w obiekcie. Ponadto system umożliwia bezstratne, optymalne wykorzystanie mocy wzmacniaczy operacyjnych dzięki unikalnemu rozwiązaniu w postaci modułów kontroli linii głośnikowych z programowalnymi selektorami stref. Przesyłanie sygnałów audio oraz sygnałów sterujących odbywa się drogą cyfrową. Integracja cyfrowa jest dostępna zarówno z centralami sygnalizacji pożarowej Schrack Seconet Integral IP, jak i z systemem zarządzania bezpieczeństwem pożarowym SIS-FIRE.

Nowa inicjatywa:
Instytut Bezpieczeństwa RESCON

Na mapie polskich organizacji podejmujących problematykę zarządzania bezpieczeństwem pojawił się nowy gracz – Instytut Bezpieczeństwa RESCON. Redakcja „a&s Polska", jako partner strategiczny tej inicjatywy, odsłania plany na bliższą i dalszą przyszłość nowego przedsięwzięcia oraz przybliża sylwetki jego liderów. Z twórcami Instytutu – Grzegorzem Ćwiekiem i Krzysztofem Liedelem – rozmawia Mariusz Kucharski.

Instytut RESCON

Opowiedzmy, skąd pomysł utworzenia takiej organizacji i jaki jest cel jej działania.

Grzegorz Ćwiek (G.Ć.): Wizja utworzenia przedsięwzięcia, którego misją byłoby wspieranie i propagowanie idei rozwoju zarządzania bezpieczeństwem, a w szczególności odpornością organizacji na różnego rodzaju wydarzenia o charakterze kryzysowym, sięga końca lat 90. ubiegłego wieku. Wówczas jako młody człowiek zaangażowany w pierwsze projekty związane z bezpieczeństwem (głównie technicznym) i zafascynowany ideą zarządzania kryzysowego, próbując znaleźć jakiekolwiek informacje na ten temat, napotykałem głównie materiały w obcych językach. Cała wiedza, jaką ja i moi współpracownicy czerpaliśmy na temat standardów organizacyjnych i nowoczesnych koncepcji zabezpieczeń technicznych, pochodzi z instytucji zagranicznych, producentów urządzeń i oprogramowania, a także z prasy i książek pisarzy brytyjskich, amerykańskich czy niemieckich. W Polsce brakowało specjalistów, a nasze uczelnie wyższe nie były przygotowane do kształcenia w takich kierunkach, jak bezpieczeństwo informacji, zarządzanie ryzykiem czy komunikacja kryzysowa. Podczas gdy w Wlk. Brytanii czy USA już w latach 70. i 80. powstawały – uznawane do dzisiaj za niezbędne – kodeksy dobrych praktyk wspierające przedsiębiorców w walce ze zdarzeniami krytycznymi, my, u progu XXI wieku, poruszaliśmy się po podstawowych pojęciach w tym zakresie, a branża zabezpieczeń dopiero nabierała kształtu.

Podczas spotkań i rozmów z wieloma znajomymi ekspertami zauważyłem, że mają oni podobne zdania, obserwacje i wnioski. Obaj z Krzysztofem jesteśmy przekonani, że w ciągu ostatnich 20 lat wiele się w tym zakresie zmieniło, jednak nadal można dostrzec ogromne luki w poziomie świadomości i wiedzy społeczeństwa oraz mnóstwo potrzeb rynkowych w zakresie rzetelnych informacji na temat nowoczesnych technologii oraz rozwiązań organizacyjnych dotyczących szeroko rozumianego bezpieczeństwa. Dzisiaj, w dobie coraz powszechniejszego na świecie zagrożenia o różnym pochodzeniu – od ataków terrorystycznych po zagrożenia w sieci – znacznie bardziej niż kilkanaście lat temu potrzebujemy dobrych, sprawdzonych metod zarządzania bezpieczeństwem organizacji, wzorców kształtowania kultury bezpieczeństwa w całym naszym społeczeństwie. Cieszę się, że spotkałem na swojej drodze Krzysztofa, którego zaangażowanie w działania badawcze i edukacyjne tak świetnie wpisuje się w pomysł sprzed lat. Wspólnie doszliśmy do wniosku, że nie możemy dłużej czekać i należy działać. Potrzebny jest ktoś, kto będzie wspierał takie idee, prowadził aktywność badawczo-rozwojową, współpracował z ekspertami, dysponował wiedzą, by doradzać innym i tworzyć nowe standardy. Taki mamy wspólny cel!

Cieszę się także z nawiązania strategicznego partnerstwa z „a&s Polska". Jako liczące się w branży czasopismo macie szeroki ogląd sytuacji rynkowej i bliskie kontakty z uczestnikami tego rynku – od oferentów techniki zabezpieczeń po security managerów. Zainicjowaliście bardzo ważne dla branży spotkania, podczas których osoby odpowiedzialne za bezpieczeństwo w firmach i instytucjach mogą regularnie dyskutować i wymieniać się doświadczeniami z przedstawicielami branży zabezpieczeń. Takie zestawienie nowych technologii wraz z potrzebami rynku jest niezwykle istotne, pomaga bowiem spojrzeć na cały problem holistycznie. Macie już duże doświadczenie, daliście się poznać rynkowi security, dlatego cieszę się, że będziemy wspólnie podejmować ciekawe inicjatywy.

Wyjaśnijmy, skąd nazwa Instytutu…

G.Ć.: Nazwa RESCON powstała poprzez połączenie kilku słów, z jednej strony już znanych w Polsce, z drugiej – naszym zdaniem – jednak nierozumianych w taki sposób, w jaki według nas powinny być one przyswojone. O ile w języku angielskim bezpieczeństwo nie występuje jako termin ogólny i uniwersalny (służy temu kilka różnych określeń stosowanych w zależności od kontekstu), o tyle w Polsce jest swego rodzaju kluczem znaczeniowym, którego nie zawsze używamy poprawnie. Mówiąc o bezpieczeństwie, zwykle rozumiemy je bardziej jako poczucie bezpieczeństwa, jedną z najważniejszych i nieco ułudnych potrzeb ludzkich. Jednocze-

śnie jest to pojęcie, które nie obejmuje tylko konkretnej struktury znaczeniowej lub przyswojonego zestawu wymaganych działań, ale nie wyznacza żadnych konkretnych kierunków naszych aktywnych i świadomych decyzji. Słysząc czy mówiąc o zarządzaniu bezpieczeństwem, mamy także często raczej mglistą wizję pewnego stanu mającego zapewnić nam, jako ludziom, lub całej organizacji, np. firmie, spokój działania i pracy, realizacji celów. Tylko nie bardzo wiadomo, co zrobić, by ten spokój osiągnąć.
Dlatego też, tworząc nazwę naszego nowego przedsięwzięcia, połączyliśmy kilka wyrazów. Poza wskazaniem na obszar naszej działalności w ujęciu tradycyjnym (bezpieczeństwo), przywołujemy tu także takie wyrazy, jak: *resilience* (rezyliencja, odporność) oraz *continuity* (ciągłość), stawiając ich treść znaczeniową i związane z tym międzynarodowe standardy za symbol naszych działań oraz kierunek rozwoju Instytutu.

Krzysztof Liedel (K.L.): Naszym celem jest działanie ukierunkowane na praktykę – nie tylko wspieramy budowanie poczucia bezpieczeństwa, ale także jesteśmy zdeterminowani, by budować w odbiorcach naszych działań (usług) automatyzmy właściwych zachowań, a także wysoką świadomość i kulturę w zakresie rozumienia i codziennego stosowania zasad i mechanizmów bezpieczeństwa. Dotyczy to zarówno życia codziennego każdego mieszkańca naszego kraju i umiejętności szybkiego wyboru właściwych zachowań w warunkach zagrożenia życia i zdrowia (napad, atak terrorystyczny), jak i życia codziennego przedsiębiorstwa, które musi na co dzień zmagać się z szeregiem zagrożeń ze strony nieuczciwych kontrahentów i pracowników, ryzykiem prawnym, finansowym czy groźbą utraty danych lub zagrożeniem pożarowym. Zależy nam nie tylko na przekazywaniu wiedzy, lecz także na doradztwie i edukacji w zakresie zasad podejmowania aktywnych działań prewencyjnych, umiejętności wykrywania zagrożeń (wykorzystywania odpowiednich technik i narzędzi), właściwego reagowania na nie, ale również zdolności do odbudowania swoich aktywów i zasobów po wystąpieniu sytuacji krytycznej zagrażającej przetrwaniu organizacji prywatnej, publicznej, non profit.

Misja jest bardzo ambitna i mamy nadzieję, że spotka się z przychylnym przyjęciem przez rynek.

G.Ć.: Nasze działania podejmujemy z rozwagą, ale przede wszystkim wielką otwartością na wszelkie potrzeby i sugestie rynku. Co więcej, status Instytutu wskazuje na nasze poświęcenie ważnej misji i potrzebę właściwego zaangażowania potencjału rynkowego, który może wspomóc realizację postawionych przed nami celów. Chcielibyśmy, aby członkami naszej organizacji i naszymi współpracownikami stało się jak najwięcej ekspertów oraz specjalistów we wszystkich dziedzinach, jakimi zajmujemy się aktualnie oraz planujemy zająć się w najbliższej przyszłości.
K.L.: Chcemy integrować nasze środowisko i być także poza naszą działalnością rynkową postrzegani jako organizacja łącząca interesy i potrzeby wielu stron: potrzebujących wsparcia, doradztwa oraz posiadających kompetencje w tym zakresie.
G.Ć.: Dlatego, oprócz działalności doradczej i szkoleniowej, tworzymy specjalistyczny portal Biznesbezprzerwy.pl, którego zadaniem będzie udostępnianie specjalistom przestrzeni do prezentacji treści – artykułów merytorycznych, materiałów edukacyjnych czy promocji własnych działań spójnych z zakresem funkcjonowania Instytutu. Także dzięki zaangażowaniu w to przedsięwzięcie „a&s Polska" chcemy stworzyć kompendium wiedzy dotyczącej szeroko pojętego bezpieczeństwa. Portal w pełnej odsłonie będzie niebawem dostępny. Zapraszamy do współpracy wszystkich, którzy swoim działaniem, wiedzą, doświadczeniem i umiejętnościami chcą przyczyniać się do rozwoju kultury bezpieczeństwa w Polsce. Jesteśmy przekonani, że możemy wspólnie dokonać wiele dla rozwoju branży. Chcielibyśmy, aby nasza działalność była przede wszystkim potrzebna i pożyteczna.

Zapraszamy do współpracy!

BIO

Grzegorz Ćwiek – absolwent studiów doktoranckich Kolegium Zarządzania i Finansów Szkoły Głównej Handlowej, absolwent wydziału zarządzania brytyjskiego Bournemouth University, członek brytyjskiego The Business Continuity Institute, specjalista w zakresie zarządzania ciągłością działania, bezpieczeństwem technicznym i organizacyjnym. Od ponad dwudziestu lat związany z rynkiem systemów bezpieczeństwa oraz praktyką bezpieczeństwa biznesu. Wieloletni pracownik, członek zarządu i doradca wiodących w branży firm międzynarodowych oraz inwestorów polskich i zagranicznych. Autor i współautor wielu publikacji na temat zarządzania bezpieczeństwem technicznym, w tym pożarowym, komunikacją, odpornością organizacyjną, ciągłością procesów biznesowych i zarządzania ryzykiem.

dr Krzysztof Liedel – doktor w specjalności zarządzania bezpieczeństwem, prawnik, specjalista w zakresie terroryzmu międzynarodowego i jego zwalczania, ekspert w zakresie analizy informacji, szczególnie w obszarze analizy decyzyjnej. Stażysta w Narodowym Centrum Kontrterrorystycznym w USA. Były naczelnik Wydziału ds. Przeciwdziałania Zagrożeniom Terrorystycznym Departamentu Bezpieczeństwa Publicznego Ministerstwa Spraw Wewnętrznych i Administracji, były dyrektor Departamentu Bezpieczeństwa Pozamilitarnego Biura Bezpieczeństwa Narodowego. Kierownik Instytutu Analizy Informacji Collegium Civitas, dyrektor Centrum Badań nad Terroryzmem CC. Wykładowca Collegium Civitas i Uniwersytetu Warszawskiego. Autor i współautor wielu publikacji na temat terroryzmu międzynarodowego i jego zwalczania oraz analizy informacji.

Szczegółowe informacje o Instytucie Bezpieczeństwa RESCON:
www.rescon-instytut.org

Dzień Kobiet Security

8 marca to dzień wyjątkowy. Szczególnie w tym roku, kiedy odbyła się I edycja Dnia Kobiet Security. Spotkanie najbardziej wpływowych Pań branży zabezpieczeń technicznych zorganizowały wspólnie redakcja „a&s Polska" oraz firmy Axis Communications i Nedap Security Management. Uczestniczyło w nim ponad 30 przedstawicielek branży. W Pałacu Czosnowskich pod Warszawą Panie wzięły udział w warsztatach motywacyjnych prowadzonych przez znaną mentorkę i coacha Tatianę Mindewicz-Puacz oraz warsztatach emisji głosu przygotowanych przez dziennikarkę Jolantę Kucharską. Uzupełnieniem części mentoringowej były warsztaty wizerunkowe Marty Grusznic i Marty Michałko oraz pokaz kuchni molekularnej znanego szefa kuchni Marcina Jabłońskiego.

Niewiele jest kobiet w naszym gronie i dlatego wspólnie zorganizowaliśmy spotkanie, integrujące Panie z naszej branży. Osobiste relacje budują fantastyczną współpracę zarówno w ramach jednej firmy, jak i pomiędzy firmami.

Justyna Puławska
Axis Communications

Anna Twardowska
Nedap Security Management

Wszyscy jesteśmy za bardzo zajęci codziennymi sprawami, by poznać się i nawiązać ze sobą bliższe relacje. Dlatego takie spotkania są nam bardzo potrzebne.
Warsztaty rozwoju osobistego, które zaproponowaliśmy uczestniczkom, mogą się przydać w wielu sytuacjach, w życiu zarówno biznesowym, jak i prywatnym.

Mariusz Kucharski
a&s Polska

Zaprosiliśmy Panie pracujące w tej męskiej branży, by mogły się lepiej poznać, porozmawiać w luźnej i przyjaznej atmosferze. Od wielu uczestniczek słyszeliśmy, że mają niewiele okazji do takich spotkań, więc budowanie relacji i możliwość uczestniczenia w ciekawych warsztatach rozwoju osobistego wydały nam się interesujące. Jak się okazuje – sądząc po opiniach uczestniczek – mieliśmy rację!

Smart City Forum: Odkryj miasto na nowo

Już po raz siódmy podczas Smart City Forum w Warszawie spotkali się prezydenci polskich miast, zagraniczni eksperci, przedstawiciele administracji publicznej oraz biznesu.

Była to merytoryczna, dynamiczna konferencja pełna ciekawych dyskusji oraz dużej dawki wiedzy. Wydarzenie zgromadziło ponad 600 osób.
Uczestnicy spotkania mieli możliwość interakcji, wymiany myśli i doświadczeń z zakresu *smart city* w postaci innowacyjnej formuły *ROUND TABLES*. Każdemu stolikowi przewodniczyli eksperci w danej dziedzinie, przy tej edycji tematami przewodnimi były:

- energetyka rozproszona
- *sharing economy*
- normy ISO
- jakość powietrza
- systemy sterowania inteligentnymi miastami
- smartM2M –inteligentna komunikacja urządzeń w mieście

Wielka Gala Smart City
Podczas wieczornej gali wręczono statuetki przedstawicielom administracji publicznej i biznesu. Nagrody przyznała niezależna Kapituła Konkursowa, w kategoriach:

- Smart City powyżej 500 tys. mieszkańców – **Wrocław**
- Smart City od 100 do 500 tys. mieszkańców – **Rzeszów**
- Smart City do 100 tys. mieszkańców – **Jaworzno**
- wyróżnienie Smart City do 100 tys. mieszkańców – **Siemianowice Śląskie**
- Inteligentne rozwiązanie Smart City Solution – **Miejskie Wodociągi i Kanalizacja w Bydgoszczy**
- Człowiek Roku 2017 – **Wadim Tyszkiewicz, prezydent miasta Nowa Sól**

Smart City Forum to cykliczna konferencja dot. rozwoju inteligentnych miast, organizowana przez MMC Polska.
Redakcja „a&s Polska" była oficjalnym patronem medialnym wydarzenia.

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

Nagrody dla Dahua Technology Poland

Za nami pierwszy kwartał 2018 r., wiele osób ma już zaplanowaną majówkę, a nawet wakacje. Nie ma w tym nic dziwnego, skoro ubiegły rok był postrzegany przez większość osób jako najlepszy pod względem gospodarczym w Polsce od roku 1989. Doskonałym przykładem na potwierdzenie tego stanu rzeczy były wypowiedzi osób zarządzających w firmach branży security, cytowane na łamach 1/2018 „a&s Polska".

Wszyscy uznali rok 2017 za bardzo dobry, udało się w nim zrealizować większość celów biznesowych, powiększyć kapitał ludzki w firmie lub wprowadzić na rynek nowe marki. Dla Dahua Technology Poland był to pierwszy pełny rok działalności operacyjnej w Polsce – jak się okazuje, pełen sukcesów. Na początku lutego br. przedstawiciele polskiego biura Dahua zostali zaproszeni na spotkanie podsumowujące działania i wyniki koncernu Dahua Technology w roku 2017. Podczas wieczornej gali zostały wręczone nagrody za najlepsze osiągnięcia (w kilku kategoriach). Nagrodę dla **najlepszego zespołu sprzedażowego** w imieniu Dahua Technology Poland odebrał Andrzej Jarzyna wraz z Nicole Shi.

Nagroda, zwłaszcza tak zaszczytna, zawsze cieszy, ale kiedy otrzymujemy drugą, można już z całą pewnością stwierdzić, że to nie był przypadek. Chwilę później na scenę poproszono Artura Prusinowskiego, Mateusza Zapotocznego i Karola Narojczyka, którym wręczono nagrodę za **najlepszy plan sprzedażowy** w sekcji projektów.

Dziękujemy całemu zespołowi Dahua Technology Poland za ciężką pracę w minionym roku. To są wasze nagrody, my je tylko odbieraliśmy – powiedział Andrzej Jarzyna, Sales and Operations Director w Dahua Technology Poland. – *Obiecujemy, że nie spoczniemy na laurach i w tym roku także udowodnimy, że jesteśmy najlepszym zespołem Dahua Technology na świecie, a 2018 będzie rokiem Dahua.*

Dahua Technology Poland

Ticket to China z Dahua Technology Poland

***Przygoda, przygoda, każdej chwili szkoda…* Jeżeli praca jest tym, co lubimy robić, każdego dnia czeka nas nowa przygoda. Współpraca z Dahua Technology może być przygodą każdego dnia – w codziennej pracy lub… podczas odkrywania uroków Azji. Mogli się o tym przekonać uczestnicy drugiej edycji *Ticket to China* z Dahua Technology. W drugiej edycji szkoleniowej w centrali firmy w Hangzhou wzięło udział aż 29 osób, o 10 więcej niż w edycji ubiegłorocznej.**

Jak przystało na chińską gościnność, poniedziałek 12 marca rozpoczęto od oficjalnego spotkania z przedstawicielami Dahua Technology, po czym zaplanowano zwiedzanie okazałego, dwupoziomowego *showroomu*, w którym prezentowano najnowsze technologie, które wkrótce będą dostępne w ofercie Dahua Technology. Po południu odbyło się zwiedzanie fabryki, w której działają w pełni zautomatyzowane linie produkcyjne głowic szybkoobrotowych. Po dniu pełnym wrażeń i nowych doświadczeń w poniedziałkowy wieczór wylądowaliśmy w Chengdu.

Podczas kolejnych trzech dni uczestnicy odkrywali tajemnice tego niezwykłego miasta. Mieli okazję zwiedzać hodowlę pandy wielkiej, pływać po rzece Mingjiang, obejrzeć posąg Wielkiego Buddy z Leshan, podziwiać górę Qingcheng wpisaną na światową listę dziedzictwa UNESCO, a także obejrzeć system irygacyjny, który jest najstarszym i jedynym na świecie zachowanym bezzałogowym systemem nawadniającym. Nikt zapewne nie opuści Chengdu nie odwiedziwszy tradycyjnej herbaciarni w parku Wangjianglou. Przygoda z *Ticket to China* 2 zakończyła się w czwartek 15 marca. W godzinach nocnych samolot wylądował na lotnisku Chopina w Warszawie. Wszystkim, którzy towarzyszyli nam w tej wyprawie, serdecznie dziękujemy za wspólnie spędzony czas. Jeśli ktoś chciałby wziąć udział w kolejnej edycji *Ticket to China*, zapraszamy do współpracy. Szczegóły wkrótce.

Karol Narojczyk,
Marketing Manager, CEE & Nordic
Dahua Technology Poland

Truckshow Hikvision w 6 miastach w Polsce

Na początku 2018 roku ciężarówka firmy Hikvision ruszyła w trasę, by zaprezentować najnowocześniejsze rozwiązania z zakresu sztucznej inteligencji. Już w maju pojawi się w sześciu miastach w Polsce!

Uczestnicy wydarzenia będą mieli okazję odkryć najnowsze innowacyjne rozwiązania w zakresie technologii monitoringu wizyjnego i przekonać się, w jaki sposób sztuczną inteligencję można zastosować w praktyce.
Podczas *truckshow* będzie można przede wszystkim zwiedzić mobilny *showroom* Hikvision, a także uczestniczyć w ciekawych doświadczeniach na pokładzie ciężarówki. Organizatorzy pokazów zaplanowali również interesujące prelekcje.
Wydarzenie będzie zorganizowane w formie pikniku.

Rozkład jazdy:

8.05.2018 r.	Kraków, Tauron Arena
10.05.2018 r.	Warszawa, Stadion PGE Narodowy
15.05.2018 r.	Gdańsk, Dwór Oliwski
17.05.2018 r.	Szczecin, Binowo Park
21.05.2018 r.	Poznań, Inea Stadion
22.05.2018 r.	Wrocław, Hala Stulecia

Agenda:
od 9:30 – Rejestracja (czynna przez cały dzień)
10:00-10:30 – Prezentacja Sztuczna Inteligencja
11:15-11:35 – Prezentacja WD
11:35-12:05 – Prezentacja Seagate
13:15-13:35 – Prezentacja HikCentral
13:35-14:00 – Prezentacja Cybersecurity
16:00 – Zakończenie

Hikvision Poland

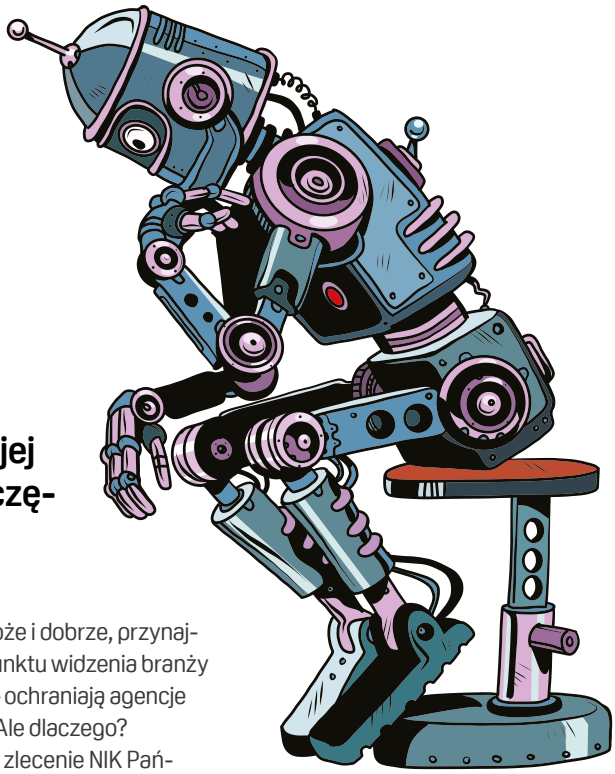
Moduł analizy obrazu IntelliVIX-DPS

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

IntelliVIX-DPS to wyjątkowe rozwiązanie inteligentnej analizy obrazu w czasie rzeczywistym. Pakiet IntelliVIX-DPS, oprócz modułu analizy obrazu, składa się z wodoodpornych kamer, tablicy elektronicznej oraz lampy ostrzegawczej z wbudowanym głośnikiem alarmowym. Moduł IntelliVIX-DPS w czasie rzeczywistym wykrywa tonięcie obiektu i w ciągu kilku sekund powiadamia ratownika o potencjalnym zagrożeniu. Dzięki integracji z lampą oraz dźwiękowym systemem ostrzegawczym pracownicy basenu oraz pozostałe osoby przebywające tam zauważą ostrzeżenie. Instalacja systemu IntelliVIX-DPS znacząco zwiększa szansę na szybkie zlokalizowanie osoby tonącej oraz skuteczne udzielenie jej pomocy. Rozwiązanie to znakomicie ułatwia pracę ratownikom oraz poprawia bezpieczeństwo w tego typu obiektach sportowych. Więcej informacji na temat IntelliVIX-DPS oraz pozostałych produktów IntelliVIX na: www.intellivixeu.com

Inf. IntelliVIX

Inteligentni inaczej



Sztuczna inteligencja. Jedni o niej marzą, inni się jej boją i przed nią ostrzegają – nie tylko Bill Gates czy nieżyjący już Stephen Hawking. **Mam własne myśli na jej temat. Bo co tu mówić o AI, kiedy ta prawdziwa jest często w głębokim deficycie, czyli w czarnej dziurze.**

To, co na temat sztucznej funkcjonuje w obiegu informacyjnym, to często marketing dla inteligentnych inaczej. Inteligencja w sensie ludzkim (emocjonalnym) nie jest do osiągnięcia przez technikę. Choć może kiedyś maszyna będzie mogła sama z siebie zachwycać się lotem i ubarwieniem motyla i mu współczuć, gdy straci skrzydło. Ale może też nie myśleć jak człowiek, mieć nieludzki sposób rozumowania – obcą inteligencję. Tymczasem problem faktycznie powstających, coraz więcej mogących maszyn imitujących ludzkie zachowania – nazywanych AI – nie jest wymyślony. Trzeba zachować ostrożność, np. taką, jak przy obchodzeniu się z „tępymi" narzędziami, choćby z ogniem. On może nam ugotować obiad lub go spalić, a kucharza przy okazji. Maszyna wybierze sobie działanie według jakichś przetworzonych przez nią wstępnych algorytmów programistycznych, bo przecież jest „inteligentna". Dajcie jej teraz możliwości np. bojowego drona.

Podczas bliskich już mistrzostw świata w piłce nożnej w Rosji zadebiutuje system *Video Assistant Referee (VAR)*, czyli powszechna już w ochronie wideoweryfikacja. Pojawił się na światowych boiskach w 2016 r., jest też na polskich stadionach Ekstraklasy. Gdy występuje sędziowska wątpliwość dotycząca strzelonego gola, rzutu karnego, czerwonej kartki lub ukarania niewłaściwego zawodnika, specjalni sędziowie VAR i asystenci wideo oglądają w multimedialnym pojeździe powtórkę nagrania z boiskowych kamer. Czy to problem związany z bezpieczeństwem? Oczywiście – a co podnieca do białej gorączki kiboli o wprost proporcjonalnym stosunku posiadanego poziomu agresywnego testosteronu do głupoty?

Ciekawostka z kontroli NIK o bezpieczeństwie przewozów kolejowych. Kto wie, że polskie dworce kolejowe obsługujące rocznie ok. 300 mln pasażerów nie zostały w ustawie o transporcie kolejowym zaliczone do elementów… infrastruktury kolejowej. Świat postawiony na głowie – przecież tory przez nie biegną. W konsekwencji dworce nie są objęte systemami zarządzania bezpieczeństwem na kolei, bo zarządcy infrastruktury i przewoźnicy nie są tym specjalnie zainteresowani. Druga ciekawostka: Straż Ochrony Kolei (SOK) nie jest samodzielną formacją ochronną, tylko zakładem pracy, składnikiem organizacyjnym PLK PKP, jednej ze spółek kolejowych. Jaki ma to wpływ na bezpieczeństwo? Wiele dworców – nie chcę powiedzieć, że to źle, bo może i dobrze, przynajmniej z punktu widzenia branży security – ochraniają agencje ochrony. Ale dlaczego?

W ub.r. na zlecenie NIK Państwowa Straż Pożarna skontrolowała 238 dworców i ujawniła dużo nieprawidłowości dotyczących nie tylko łamania przepisów ppoż. Wiele obiektów nie jest sprzętowo przygotowanych do prowadzenia działań ratunkowych i ewakuacji ludzi w przypadku pożaru lub innych zagrożeń, także terrorystycznych. Na prawie co piątym dworcu hydranty nie miały wystarczającego zasięgu. Często brakowało awaryjnego oświetlenia i zabezpieczenia przed zadymieniem dróg ewakuacyjnych. Ujawniono niesprawne dźwiękowe systemy ostrzegawcze i niedziałającą pożarową sygnalizację alarmową. NIK we wnioskach zasugerowała delikatnie, aby przynajmniej duże obiekty dworcowe wyposażać w defibrylatory, systemy monitoringu oraz szkolić pracowników obsługi i ochrony z zasad udzielania pierwszej pomocy.

Coś z bliskiej zagranicy. Inwestycje w bezpieczeństwo nie muszą kosztować kokosów, a ile mogą dać zadowolenia. Niestety dyscyplinarnie zwolniono racjonalizatora – wicedyrektora pewnego moskiewskiego więzienia. Potwierdziły się doniesienia o znajdujących się w nim specjalnych celach dla bogatych więźniów, podczas gdy w tym samym kryminale są też cele przepełnione i bez urządzeń sanitarnych. Za „Moskiewskim Komsomolcem" podaję, że owe miejsca dla VIP-ów są przestronne, ładne i nawet „modne", jakby w jakimś hotelu na Malediwach, a nie w Matrosskiej Tiszynie. Telewizor prawie na całą ścianę, lodówka wypełniona delikatesami – miejsce do odsiadywania kary można kupić za milion rubli (ok. 60 tys. zł). Kto by stamtąd uciekał? Tam nawet poziom frustracji i agresji może być mniejszy. Jak pokazuje ten obrazek, w tzw. niesprzyjających okolicznościach przyrody zarobić potrafi nie tylko Polak.

BIO

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

Więcej informacji na:

www.WarsawSecuritySummit.eu

alhua TECHNOLOGY

World Security Leader

securex® POLAND

23-26 kwietnia 2018 r.

PAWILON 8A
STOISKO 13

Serdecznie zapraszamy!

CE FC UL RoHS ISO 9001:2000

www.dahuasecurity.com/pl

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