CZASOPISMO RYNKU SECURITY

a&s POLSKA

02 (32) 03/04 2022

ZARZĄDZANIE BEZPIECZEŃSTWEM

W OBLICZU WOJNY W UKRAINIE

Utrzymanie ciągłości działania, zarządzanie personelem i ochrona łańcucha dostaw to wskazane przez Rządowe Centrum Bezpieczeństwa priorytetowe obecnie zadania dla menedżerów bezpieczeństwa.

CYBERBEZPIECZEŃSTWO

STOPNIE ALARMOWE

Co oznacza wprowadzenie w Polsce stopnia alarmowego BRAVO (zagrożenie atakiem terrorystycznym) i CHARLIE-CRP (zagrożenie terrorystyczne w cyberprzestrzeni)? Jak je odnieść do branży bezpieczeństwa fizycznego?

INFRASTRUKTURA KRYTYCZNA

W CZASACH TURBULENCJI

Wchodzimy dziś na inny poziom incydentów bezpieczeństwa infrastruktury krytycznej – poziom infiltracji i sabotażu jako zagrożeń realnych, o rosnącym ryzyku wystąpienia. Jak podejść do nowych wyzwań?

APLIKACJA MOBILNA

www.aspolska.pl

ISSN 2451-5175

9 772451 517703 05

15 zł (w tym 8% VAT)

Drodzy Czytelnicy

Po dwóch latach pandemii mieliśmy nadzieję na powrót do normalności i odbudowę gospodarki nadwątlonej lockdownami i rosnącą inflacją. Nasze plany zniweczyła wojna w Ukrainie, której konsekwencje trudno przewidzieć, a jej skutki będziemy odczuwać jeszcze długo. Dobrze i spokojnie już było...

W związku z obecną sytuacją RCB podniosło stopnie alarmowe w całym kraju, wydało rekomendacje dla security menedżerów i zidentyfikowało obszary wymagające szczególnej uwagi (s. 14). W momencie oddawania numeru do druku w Polsce obowiązują dwa stopnie alarmowe: BRAVO oraz CHARLIE-CRP, które różnią się obszarem obowiązywania i dotyczą różnych aspektów bezpieczeństwa. Jakie obowiązki nakładają na branżę ochrony? Jaki wpływ na życie osób niezwiązanych z obszarem security ma ich wprowadzenie? (s. 20).

Ciekawymi uwagami dzielą się branżowi specjaliści (s. 28). Wypowiadają się nie tylko w kwestiach bezpieczeństwa fizycznego, zwracając uwagę na potencjalne konsekwencje pandemii i wojny w Ukrainie (s. 16,), ale też ważnego dziś cyberbezpieczeństwa systemów teleinformatycznych, którego dotyczą stopnie alarmowe CRP. Jak się zabezpieczyć przed skutkami cyberataków skierowanych przeciwko Ukrainie i krajom sojuszniczym, co może nam zagrażać w sferze internetowej, przedstawiamy na s. 18.

Wchodzimy dziś na inny poziom incydentów bezpieczeństwa – poziom infiltracji i sabotażu jako zagrożeń realnych, o rosnącym ryzyku wystąpienia. Musimy zmienić dotychczasowe postrzeganie bezpieczeństwa IK w tradycyjnym rozumieniu, zacząć myśleć w kontekście konkretnej sytuacji, która zmienia priorytety. Jak podejść do nowych wyzwań, piszemy na s. 34. Ważnym elementem ochrony perymetrycznej IK są sieci telekomunikacyjne – sprawna komunikacja elektroniczna stanowi nerw całej gospodarki i funkcjonowania państwa. O sposobach ich zabezpieczania piszemy na s. 44.

Przed wielką szansą na rozbudowanie swoich usług o ochronę klientów przed cyberzagrożeniami stoją dziś firmy ochrony, które swoje działania coraz odważniej opierają na technologiach teleinformatycznych. Czy ją wykorzystają? (s. 76). Osobom zarządzającym w tym sektorze pomocne będą wskazówki, jak w przedsiębiorstwach wprowadzić system zarządzania ciągłością działania, aby zapewnić ich płynny rozwój – kolejne kroki opisujemy na s. 80.

Dużą uwagę w aspekcie IK poświęcamy systemom ochrony perymetrycznej. Podpowiadamy, jakie są najpopularniejsze technologie (s. 50), wskazujemy zalety analityki wizyjnej, której zastosowanie rośnie wykładniczo dzięki wspomaganiu przez AI (s. 54). W zabezpieczaniu dużych obszarów incydenty związane z nieautoryzowanym wtargnięciem są trudniej wykrywane. Radary i lidary stanowią w tym względzie niebagatelne wsparcie (s. 60).

Gorąco zapraszamy na konferencję Warsaw Security Summit zaplanowaną na 6 czerwca w Centrum Praskim KONESER w Warszawie. Agenda i formularz rejestracyjny będzie dostępny na www.warsawsecuritysummit.online.

Do zobaczenia!

Marta Dynakowska
REDAKTOR NACZELNA

Jan T. Grusznic
Z-CA REDAKTORA NACZELNEGO

Mariusz Kucharski
DYREKTOR ZARZĄDZAJĄCY

A&S POLSKA REDAKCJA

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

Prezes Zarządu
Mariusz Kucharski

Redaktor naczelna
Marta Dynakowska

Z-ca redaktora naczelnego
Jan T. Grusznic

Dział reklamy i marketingu
Iwona Krawiec

Dział projektów specjalnych
Jolanta A. Kucharska
Aleksandra Czapska

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

Korekta
Jolanta Kucharska

Projekt graficzny i skład
Kalwala Studio Sp. z o.o.

Adres redakcji
A&S Polska
ul. M. Rodziewiczówny 1 lok. 801
04-187 Warszawa
e-mail: info@aspolska.pl
www.aspolska.pl

Prenumerata
www.aspolska.pl/prenumerata

a&S POLSKA

02

32

03/04

2022

SPIS TREŚCI

WOJNA W UKRAINIE ZARZĄDZANIE BEZPIECZEŃSTWEM

WOJNA W UKRAINIE CYBERBEZPIECZEŃSTWO

CYBERBEZPIECZEŃSTWO

INFRASTRUKTURA KRYTYCZNA

SPIS TREŚCI

RYNEK SECURITY

BEZPIECZEŃSTWO BIZNESU

BEZPIECZEŃSTWO POŻAROWE

SERWIS INFORMACYJNY

PRODUKT NUMERU

AXIS COMMUNICATIONS

www.axis.com/pl

Kamera typu bullet AXIS M2036-LE

Przystępna cenowo kamera z funkcją głębokiego uczenia się

AXIS M2036-LE TO IDEALNE URZĄDZENIE DO PRACY W TRUDNYCH WARUNKACH ŚRODOWISKOWYCH I ATMOSFERYCZNYCH, ZAPEWNIA OBRAZ W ROZDZIELCZOŚCI QUAD HD 1440P/4 MPIX.

Zaawansowany procesor ma wyjątkowe możliwości analityczne oparte na mechanizmach głębokiego uczenia się, dostępne bezpośrednio w kamerze. Urządzenie zostało wyposażone w liczne funkcje. AXIS Object Analytics oferuje wykrywanie i klasyfikację ludzi, pojazdów i typów pojazdów. Z kolei Axis Edge Vault chroni identyfikator urządzenia Axis i upraszcza autoryzację urządzeń Axis w sieci. Ta kamera w obudowie typu bullet o klasie odporności mechanicznej IK08 oferuje elastyczną i ekonomiczną instalację, w tym zasilanie w standardzie PoE. Technologia Edge-to-Edge umożliwia inteligentne parowanie z głośnikami Axis Speakers. Ponadto przestronna, uszczelniona puszka tylna zapewnia bezpieczne zarządzanie kablami.

Najważniejsze cechy:
- Quad HD 1440p/4 MP
- Kompaktowa lekka konstrukcja
- Analityka wykorzystująca technikę głębokiego uczenia
- Technologia Zipstream wspierająca kompresję H.264/H.265
- Gotowość do pracy na zewnątrz z oświetlaczem podczerwieni.

BCS

www.bcscctv.pl

Kamery BCS Line serii 9000 w niższych rozdzielczościach

KAMERY BCS LINE SERII 9000, POCZĄTKOWO DOSTĘPNE JEDYNIE W WERSJACH O ROZDZIELCZOŚCI 12 MPIX, TERAZ POJAWIAJĄ SIĘ W DWÓCH KOLEJNYCH: 8 LUB 4 MPIX. DOTYCZY TO URZĄDZEŃ WE WSZYSTKICH TYPACH OBUDÓW, KLASYCZNEJ KOMPAKTOWEJ, TUBOWEJ ZE ZINTEGROWANĄ PUSZKĄ MONTAŻOWĄ I KOPUŁOWEJ Z KLOSZEM.

Rozszerzenie serii o nieco bardziej budżetowe modele o niższych rozdzielczościach pozwoli wykorzystać szerokie możliwości analizy wizyjnej, w które kamery te są wyposażone, w obiektach/miejscach, gdzie rozdzielczość 12 Mpix może być zdecydowanie na wyrost. Kamery tej serii stanowią wydajną platformę, którą dzięki aktualizacji oprogramowania można uzupełnić o kolejne funkcje analityczne do nowych zadań. Dalej dostępne jest gromadzenie metadanych o obiektach widocznych przed kamerą, pozwalające błyskawicznie wyszukać interesujące nas obiekty, a także zliczanie osób jednocześnie w 4 strefach czy kontrolę ruchu samochodów za pomocą LPR/ANPR. Analizę wizyjną uzupełniono o możliwość monitorowania, czy osoby przebywające w danej strefie lub przekraczające wirtualną linię są odpowiednio ubrane. Kamera rozpoznaje takie szczegóły ubioru, jak kamizelka ochronna, kask lub okulary ochronne oraz kolor, w jakim powinien być dany element. Dzięki zastosowaniu tak zaawansowanych kamer nie ma już konieczności zastanawiania się, jakiego typu kamery użyć do określonego zadania. Teraz jedynym problemem będzie dobór odpowiedniego typu obudowy, gdyż każda z kamer oferuje dokładnie taki sam wachlarz możliwości.

C&C PARTNERS

www.ccpartners.pl

Nowa seria kamer stałopozycyjnych TKH Security

Najnowsza seria kamer kopułkowych i tubowych FD2002v2M/FD2005v2M i BL2002v2M/BL2005v2M zapewnia doskonałą jakość obrazu zarówno w dzień, jak i w nocy.

Wbudowane w kamery inteligentne funkcje analityczne umożliwiają filtrowanie czynników środowiskowych (obecność zwierząt czy poruszające się na wietrze liście/gałęzie), minimalizując tym samym duże obciążenia związane z całodobowym monitorowaniem i nadmierną liczbą fałszywych alarmów.

PODSTAWOWE CECHY NOWYCH KAMER W OFERCIE C&C PARTNERS

- Rozdzielczość do 2592 x 1944 (5 Mpix)
- 2 Mpix – przy szybkości 25 lub 30 kl./s, 5 Mpix – przy 25 kl./s
- Kodowanie czterostrumieniowe H.264, H.265 i MJPEG
- Wbudowany oświetlacz IR o zasięgu do 60 m
- Wbudowana analiza wideo
- Profile ONVIF S, G i T
- Obudowy o klasie szczelności IP67 i odporności IK10

HIKVISION

www.hikvision.com/pl

Bezprzewodowa zewnętrzna czujka Tri-Tech AM

NOWA BEZPRZEWODOWA CZUJKA HIKVISION W OFERCIE PRODUKTÓW PRZEZNACZONYCH DO WSPÓŁPRACY Z CENTRALAMI ALARMOWYMI AX-PRO – CZUJKA TRI-TECH – WYKORZYSTUJE INNOWACYJNE TECHNOLOGIE W CELU ZREDUKOWANIA LICZBY FAŁSZYWYCH ALARMÓW.

Jak sama nazwa wskazuje, detektor Tri-tech jest zbudowany z trzech czujników wykorzystujących różne techniki detekcji: czujnika PIR na górze, czujnika mikrofalowego i czujnika PIR na dole. Oznacza to, że może wykrywać ruch ludzi i pojazdów na różnych wysokościach, z regulowanym obszarem wykrywania w obrębie 15 m i 90°, dokładniej identyfikując faktyczną przyczynę wyzwolenia alarmu.
Ponadto czujka jest wyposażona w opatentowaną technologię *Independent Floating Threshold* (IFT), pozwalającą na automatyczne i dynamiczne dostosowanie progów alarmu (czułości) w zależności od warunków zewnętrznych.

POZOSTAŁE CECHY:

- Cyfrowa kompensacja temperatury zapewnia wysoką odporność na trudne warunki atmosferyczne
- Wodoszczelność – klasa ochrony obudowy IP65
- Automatycznie regulowana czułość
- Łatwość instalacji i konfiguracji (brak przewodów zasilających i sieciowych).

Duże prawdopodobieństwo wykrycia intruza i ostrzeganie o zagrożeniach jest jedną z najważniejszych funkcjonalności urządzeń SSWiN. Możliwość weryfikacji zagrożenia (i eliminacji fałszywych alarmów) odgrywa ogromną rolę w skutecznej ochronie zewnętrznej. Czujka Tri-tech spełnia te wszystkie wymagania i może być stosowana w szerokim zakresie scenariuszy.

LINC POLSKA

www.linc.pl

Ogniwa paliwowe EFOY = czysta energia

OGNIWA PALIWOWE EFOY DOSTARCZAJĄ PRZYJAZNĄ DLA ŚRODOWISKA, CICHĄ ENERGIĘ ELEKTRYCZNĄ, KTÓRA UMOŻLIWIA BEZPIECZNĄ I NIEPRZERWANĄ PRACĘ ZASILANYCH URZĄDZEŃ.

Dzięki zastosowaniu rozwiązań odpornych na warunki atmosferyczne ogniwa mogą być używane samodzielnie w pojazdach, szafach sterowniczych lub w trybie hybrydowym z innymi generatorami prądu.
EFOY Hybrid Power tworzy kompletny pakiet energetyczny oparty na ogniwach paliwowych i nowych akumulatorach EFOY Li. Dzięki zintegrowanemu elementowi grzewczemu akumulator można ładować w temp. zewn. do -20°C.
Inteligentny system zarządzania kontroluje i monitoruje parametry ogniwa paliwowego i akumulatora, zapewniając maksymalną wydajność EFOY Hybrid Power.
Sercem ogniwa paliwowego jest rdzeń generujący energię. Przetwarza on metanol w czysty wodór, zamieniany w procesie elektrochemicznym na energię elektryczną. W wyniku reakcji wydalane są głównie ciepło i skroplona para wodna.

System może współpracować z innymi źródłami energii odnawialnej np. z panelami słonecznymi, ogniwami fotowoltaicznymi i turbinami wiatrowymi.
Ogniwa paliwowe EFOY działają automatycznie, cicho i są przyjazne dla środowiska. Platforma EFOY Cloud zapewnia bezpieczny i niezawodny zdalny dostęp do każdej jednostki. Ułatwia to monitorowanie i ogranicza prace konserwacyjno-serwisowe do absolutnego minimum. Moduł zdalnego powiadamiania informuje użytkownika, gdy np. kończy się paliwo.
Ogniwa paliwowe EFOY są kluczem do nowoczesnego i przyjaznego dla środowiska źródła zasilania.

NEDAP SECURITY MANAGEMENT

www.nedapsecurity.com/pl/

Integracja AEOS i SIS-FIRE

STALE ROZWIJANE INSTALACJE NISKOPRĄDOWE DOSTARCZAJĄ NOWYCH FUNKCJONALNOŚCI. IDZIE TO W PARZE ZE ZWIĘKSZENIEM BEZPIECZEŃSTWA OBIEKTU, DZIĘKI CZEMU KLIENT DOSTAJE PRODUKT FUNKCJONALNY, KTÓRY SPEŁNIA WSZYSTKIE OBOWIĄZUJĄCE NORMY.

Dzisiaj system kontroli dostępu nie tylko pełni funkcję rozstrzygającą o przyznaniu autoryzacji do wejścia, lecz jednocześnie staje się centrum zarządzania budynkiem i źródłem informacji dla innych systemów.

Dzięki otwartości na integrację zarówno systemu KD AEOS, jak i SIUP SIS-FIRE firmy Schrack Seconet, możliwe było połączenie obu rozwiązań w celu dostarczenia obsłudze obiektu dodatkowych informacji, pomocnych podczas normalnego użytkowania systemów oraz w trakcie zagrożenia, jakim w szczególności jest alarm pożarowy.

Protokolarna wymiana informacji pomiędzy systemami umożliwia m.in.
- monitorowanie skuteczności wysterowania przez SSP przejść na drodze ewakuacyjnej, zwiększające bezpieczeństwo przeprowadzenia sprawnej ewakuacji;
- monitorowanie położenia drzwi na drogach ewakuacyjnych. Operator SIUP ma dzięki temu pełny obraz sytuacji w obiekcie w trakcie alarmu pożarowego;
- automatyczną zmianę poziomu autoryzacji na wszystkich lub wybranych przejściach w przypadku alarmu pożarowego. Dzięki czemu system AEOS może działać zgodnie ze scenariuszem zaprogramowanym w SIS-FIRE;
- monitorowanie uruchomienia przycisków ewakuacyjnych podczas alarmu pożarowego, wskazujące możliwe miejsca zagrożenia podczas ewakuacji osób z obiektu.

OPTEX SECURITY

www.optex-europe.com/pl

Czujki laserowe OPTEX do zadań specjalnych

REDSCAN PRO, NAJNOWSZA CZUJKA LASEROWA Z NAGRADZANEJ SERII REDSCAN LIDAR, POTRAFI Z NIEZWYKŁĄ DOKŁADNOŚCIĄ WYKRYWAĆ INTRUZÓW NA OBSZARZE AŻ 50 X 100 M BEZ JAKICHKOLWIEK LUK I UTRATY SKUTECZNOŚCI DETEKCJI ZE WZROSTEM ODLEGŁOŚCI. ZASTOSOWANIE PÓL DETEKCJI W KSZTAŁCIE PROSTOKĄTA A NIE WACHLARZA ELIMINUJE ICH NAKŁADANIE SIĘ, DZIĘKI CZEMU CZUJKI DOSKONALE NADAJĄ SIĘ DO OCHRONY ELEWACJI I OGRODZEŃ PRZY UŻYCIU WIRTUALNYCH ŚCIAN I PŁASZCZYZN OBEJMUJĄCYCH OTWARTE PRZESTRZENIE, SUFITY I DACHY.

Czujka REDSCAN PRO bazuje na inteligentnych algorytmach wielostrefowych, by spełnić wymagania danej lokalizacji. Oznacza to, że dla każdej strefy detekcji można niezależnie określić czułość, rozmiar obiektu i sygnał wyjściowy, co pozwala na dostosowanie urządzenia do zagrożeń i specyfiki lokalizacji, gwarantuje maks. częstotliwość przechwytywania i ogranicza fałszywe alarmy.
Moduł kamery zapewnia wizualne wspomaganie na potrzeby konfiguracji i analizy zdarzenia, które wywołało alarm. W razie wystąpienia alarmu zapisywany jest plik dziennika zdarzeń i obraz wideo. Ułatwia to pracownikom ochrony analizę przyczyn alarmu.
Czujka charakteryzuje się nowym eleganckim wzornictwem, elastycznością montażu (można ją pochylić pod kątem od +5 do -95°), łatwością ustawień i prostotą konfiguracji za pomocą przeglądarki sieciowej. Seria REDSCAN Pro obejmuje dwa modele: RLS-3060V o maks. zasięgu 30 x 60 m oraz RLS-50100V o zasięgu do 50 x 100 m, zgodne z protokołem ONVIF S.

SCHRACK SECONET

www.schrack-seconet.pl

d-List – liniowa czujka ciepła z kablem sensorycznym SEC 15

SYSTEM D-LIST TO LINIOWA CZUJKA CIEPŁA DZIAŁAJĄCA NA ZASADZIE WIELOPUNKTOWEGO POMIARU TEMPERATURY Z WYKORZYSTANIEM KABLA SENSORYCZNEGO SEC 15. DZIĘKI BEZHALOGENOWEJ OBUDOWIE KABLA SEC 15, ODPORNEJ NA AGRESYWNE CZYNNIKI ZEWNĘTRZNE, ŚWIETNIE SPRAWDZA SIĘ W TRUDNYCH WARUNKACH ŚRODOWISKOWYCH.

Wprowadzany obecnie nowy kontroler SCU 835 pozwala na podłączenie dwóch kabli sensorycznych o długości maks. 350 m każdy. Standardowa odległość między czujnikami w kablu sensorycznym to 1, 2, 3, 4, 5, 8 lub 10 m. Istnieje możliwość zamówienia kabla z dowolnym rozstawem sensorów, z zachowaniem minimalnej odległości 0,25 m.
Kontroler SCU 835 wyposażony w moduł XLM35 umożliwia bezpośrednie podłączenie oraz integrację z pętlą X-Line. Ponadto kontroler możemy rozbudować o dodatkowe 16 wyjść przekaźnikowych dzięki zastosowaniu modułu REL 835. Do dyspozycji są również dodatkowe interfejsy komunikacyjne, co znacznie ułatwia proces programowania.
Poza obecnym już wcześniej złączem szeregowym kontroler ma złącza LAN oraz USB. Pamięć wewnętrzna została rozszerzona poprzez zastosowanie karty mini-SD, która umożliwia skopiowanie pamięci zdarzeń z kontrolera bez użycia oprogramowania.
Dzięki posiadanym certyfikatom ATEX system d-List może być również stosowany w strefach zagrożonych wybuchem. Kontroler SCU 835 ma możliwość komunikacji po protokole MODBUS TCP/RTU oraz pełnej integracji cyfrowej z systemem SIS-FIRE.

TP-LINK

www.tp-link.com.pl

TP-Link VIGI NVR1016H – 16-kanałowy sieciowy rejestrator wideo

TEN 16-KANAŁOWY SIECIOWY REJESTRATOR WIDEO SŁUŻY DO KOORDYNACJI PRACY KAMER Z SERII TP-LINK VIGI, A TAKŻE PRZEGLĄDANIA, PRZECHOWYWANIA I ODTWARZANIA ZAREJESTROWANYCH MATERIAŁÓW WIDEO. DZIĘKI ZGODNOŚCI ZE STANDARDEM ONVIF WSPÓŁPRACUJE Z KAMERAMI RÓŻNYCH PRODUCENTÓW, TWORZĄC KOMPLEKSOWY SYSTEM MONITORINGU.

Materiał z kamer jest rejestrowany na dysku SATA o pojemności do 10 TB. Rejestrator wspiera rozdzielczość rejestracji obrazów do 8 Mpix, a także standard kompresji H.265+ ograniczający nadmierne wykorzystanie przepustowości sieci. Dzięki temu zastosowanie dysku o maks. pojemności pozwala na przechowywanie nagrań nawet przez 720 dni.
Rejestrator umożliwia podgląd na żywo obrazów z 16 kamer jednocześnie oraz wyszukiwania zdarzeń w harmonogramach wideo w celu szybkiego przeglądania materiału. Obsługuje również dwukierunkową transmisję dźwięku.
Dzięki obsłudze interkomu z dowolnego miejsca można prowadzić rozmowy, widząc jednocześnie obraz z kamery.
W urządzeniu znajdują się: złącze zasilające, Audio In, Audio Out, VGA, HDMI, port Ethernet RJ45 10/100 Mb/s oraz dwa porty USB do podłączenia myszki, klawiatury lub zewnętrznego dysku twardego.
Mobilna aplikacja VIGI na urządzenia mobilne z systemem iOS i Android pozwala na monitorowanie zdalne.
Rejestrator NVR1016H uzupełnia system monitoringu wizyjnego TP-Link, w którego skład wchodzą wewnętrzne kamery typu turret oraz zewnętrzne typu bullet.

Produkt jest objęty 36-miesięczną gwarancją producenta.

W związku z aktualną sytuacją geopolityczną w Ukrainie Rządowe Centrum Bezpieczeństwa zidentyfikowało trzy obszary, na które menedżerowie bezpieczeństwa powinni zwrócić szczególną uwagę. Dotyczą one konieczności utrzymania ciągłości działania, zarządzania personelem oraz ochrony łańcucha dostaw.

Zarządzanie bezpieczeństwem

w obliczu wojny w Ukrainie

OD REDAKCJI: Ubiegły rok minął pod znakiem niedostępności towarów, wydłużających się terminów dostaw i wyzwań związanych z wyszukiwaniem nowych wytwórców komponentów. Nagłe zmiany wywołane pandemią obnażyły wiele słabości światowej gospodarki i globalnych łańcuchów dostaw, które posypały się w najmniej spodziewanym momencie. Jedną z tych słabości okazały się twarde realia rynku produkcji układów scalonych oraz uzależnienie rynków od stopnia skomplikowania otaczających nas urządzeń i rosnącego na nie zapotrzebowania. Szczegółowo pisaliśmy o tym w artykule: *Na układy nie ma rady. Kryzys w dostawach mikroprocesorów* w nr. 1/2022.
Dostępność chipów nadal jest ograniczona, a do ustabilizowania sytuacji potrzeba czasu. Tymczasem jak podaje Reuters, obecny konflikt zbrojny tylko pogorszy i tak złą sytuację na rynku. Powodem jest uzależnienie producentów od surowców z Ukrainy i Rosji. Chodzi o C4F6 wykorzystywanych m.in. w procesie wytrawiania wafli krzemowych. Jeszcze gorzej wygląda sytuacja z neonem (wykorzystywany do obróbki laserowej), którego 90 proc. pochodzi z Ukrainy. Zapasy wystarczą do maja, a producenci chipów nie mają zagwarantowanych dostaw z innych regionów świata, co prawdopodobnie oznaczać będzie dalsze ograniczenia w produkcji.

Dorota Duda

Wydział Ochrony Infrastruktury Krytycznej
Rządowe Centrum Bezpieczeństwa

1 UTRZYMANIE CIĄGŁOŚCI DZIAŁANIA

Konieczność utrzymania ciągłości działania wiąże się ze spodziewanymi zakłóceniami. Zakładamy, że będą miały one charakter cyberzagrożeń. Wprowadzenie na terytorium całego kraju trzeciego stopnia alarmowego CRP (Charlie-CRP) dotyczącego bezpieczeństwa w cyberprzestrzeni jest nie tylko sygnałem dla służb i administracji publicznej do zachowania szczególnej czujności, ale też dowodem na świadomość tych instytucji w zakresie wystąpienia cyberzagrożeń.

Działania, jakie należy wykonać w związku z wprowadzeniem stopnia Charlie-CRP, dotyczą m.in.

- konieczności zapewnienia dostępności kluczowego personelu niezbędnego do funkcjonowania danej organizacji,
- dokonania przeglądu zasobów zapasowych na wypadek konieczności ich wykorzystania,
- przygotowania się do uruchomienia planów umożliwiających zachowanie ciągłości działania po wystąpieniu potencjalnego ataku.

Wprawdzie wskazane obowiązki dotyczą administracji publicznej i operatorów infrastruktury krytycznej (IK), ale w ramach dobrych praktyk powinny być stosowane przez wszystkie inne zagrożone podmioty.

Biorąc pod uwagę sytuację w Ukrainie, RCB zarekomendowało operatorom IK podjęcie następujących działań:

- przegląd i aktualizację procedur bezpieczeństwa (w szczególności bezpieczeństwa teleinformatycznego, fizycznego, osobowego i technicznego),
- przegląd procedur na wypadek zmaterializowania się zagrożeń kinetycznych, w tym o charakterze terrorystycznym,
- przegląd i aktualizację planów ciągłości działania z uwzględnieniem zapasowego miejsca pracy czy też sprawdzenie działania środków łączności stosowanych w celu zapewnienia bezpieczeństwa.
- Te działania powinny być wykorzystane przez menedżerów bezpieczeństwa w ich organizacjach.

2 ZARZĄDZANIE PERSONELEM

Zarządzanie personelem w organizacji w obecnej sytuacji napiętego kryzysu jest kolejnym obszarem, w którym należy podjąć działania, aby zminimalizować zagrożenia mogące wystąpić w obszarze bezpieczeństwa osobowego. Odnosi się to nie tylko do ochrony kluczowego personelu, czyli osób posiadających newralgiczną wiedzę na temat funkcjonowania organizacji (w tym obszarze należy podejmować kroki dające możliwość zastępstwa o podobnych kwalifikacjach i uprawnieniach), ale także możliwości utraty pracowników. Należy podjąć kroki w zakresie oceny ryzyka funkcjonowania dla kluczowych procesów realizowanych przez organizację. Wielu obywateli Ukrainy opuściło swoje miejsca pracy w Polsce, udając się na wojnę. Najwięcej z nich pracowało w branży transportowej i budownictwie. Sektor transportu mierzy się z brakiem kierowców, co wiąże się z niemożnością wykonywania przewozów.

3 OCHRONA ŁAŃCUCHA DOSTAW

Taka sytuacja bezpośrednio przekłada się na kolejny obszar, jakim jest możliwość zakłóceń w łańcuchu dostaw. To z kolei może mieć poważne konsekwencje dla gospodarki. Zakłócenia dotyczą m.in. terminów dostaw przewożonych towarów i mają wpływ na wzrost cen usług transportowych.

Wszystkie opisane działania wpisują się w kulturę bezpieczeństwa, którą należy stale kształtować, utrzymać na wysokim poziomie i doskonalić. Wykorzystując cykl Deminga (zaplanuj–wykonaj–sprawdź–popraw), zarówno kierownictwo, jak i pracownicy powinni mieć świadomość i wiedzę nt. zagrożeń, obszarów ich występowania i wzajemnych powiązań oraz możliwości podejmowania działań prewencyjnych, które pozwolą na budowanie bezpieczeństwa organizacji.

Konsekwencje pandemii

i wojny w Ukrainie

Na co menedżerowie do spraw bezpieczeństwa powinni zwracać szczególną uwagę? Nad czym już teraz powinni pracować?

Jan Kapusta

Odpowiedź na tak sformułowane pytania jest trudna i wielowątkowa. Patrząc przez pryzmat bezpieczeństwa, „teraz" może być rozumiane jako reakcja na zdarzenia, incydenty mające miejsce obecnie. Ale „teraz" to też czas, który (oprócz reagowania i utrzymywania już wypracowanych metod i standardów działania) powinniśmy poświęcić głównie na dwie istotne kwestie. Po pierwsze powinniśmy zagospodarować wiedzę zdobytą zarówno podczas pandemii, jak i w okresie tuż przed i zaraz po wybuchu wojny w Ukrainie. Drugą kwestią jest próba rozważenia różnych scenariuszy w kontekście potencjalnych konsekwencji obu wydarzeń i przygotowanie się na zagrożenia będące ich pochodną.
W kwestiach związanych z bezpieczeństwem kluczowy jest kontekst organizacyjny, czyli profil i zasięg operacyjny konkretnej organizacji. W innej sytuacji są mniejsze organizacje lokalne, w innej duże, lecz nadal lokalne podmioty, w jeszcze innej gracze międzynarodowi. Podobnie innych konsekwencji mogą spodziewać się ci, którzy nie wycofali się z działalności na terenie i/lub z podmiotami z Federacji Rosyjskiej i Białorusi, a innych ci, którzy podjęli odmienną decyzję. Niezależnie od tego uważam, że jest kilka elementów wspólnych, które każdy menedżer ds. bezpieczeństwa powinien uwzględnić w swoich analizach czy rozważaniach. Zarówno pandemia, jak i wojna w Ukrainie będą miały konsekwencje finansowe. Co do tego nie ma wątpliwości. Pytanie dotyczy raczej skali i ciężaru, a nie samego faktu ich wystąpienia. Oba wydarzenia polaryzują społeczeństwo, choć w różnej skali.
Pandemia już dawno nas podzieliła. Wojna chwilowo wydaje się jednoczyć zarówno Polaków między sobą, jak i z uchodźcami i narodem ukraińskim. Jednak w dłuższej perspektywie obawiam się, że może Polaków coraz bardziej dzielić w opiniach co do tego, kto i w jakim zakresie powinien ponosić ciężar pomocy udzielanej uchodźcom. Innymi słowy, na rodzaj i skalę konsekwencji, z którymi przyjdzie nam się zmierzyć, będą miały wpływ negatywne kierunki rozwoju sytuacji co do zasobności portfela, sytuacji na rynku pracy i – wynikające z nich obu – nastroje społeczne. Z tego powodu, oprócz dobrze znanych zagrożeń przeciwko mieniu, wskazałbym na konieczność położenia w analizach większego niż dotychczas nacisku na:

1. zasady współpracy oparte na poszanowaniu godności i szacunku *(workplace civility)*,
2. świadome i odpowiedzialne posługiwanie się informacją,
3. bezpieczeństwo pracowników poza miejscem pracy,
4. współpraca między departamentami.

Nie są to zagadnienia nowe, wiele organizacji świetnie sobie z nimi radzi. Chcę jednak zwrócić uwagę na pewne specyficzne ich aspekty, które bezpośrednio łączą się z aktualnymi wydarzeniami.

ZASADY WSPÓŁPRACY OPARTE NA POSZANOWANIU GODNOŚCI I SZACUNKU

Na pierwszy rzut oka zagadnienie to wydaje się problemem czysto HR-owym. Mogę jednak wymienić przynajmniej trzy aspekty, które wprost dotyczą komórek ds. bezpieczeństwa. Pierwszym, najbardziej oczywistym jest skierowanie pracownika ochrony fizycznej w odpowiedzi na potencjalną przemoc w miejscu pracy czy asysty w niektórych przypadkach związanych ze zwolnieniem pracownika. Drugim aspektem jest prowadzenie postępowań wyjaśniających w określonych sytuacjach naruszenia zasad postępowania w miejscu pracy, trzecim – zapewnienie efektywnych mechanizmów i procedur wspierających dwa pierwsze zadania. Innymi słowy, musimy być zawczasu przygotowani, by dobrze zareagować na określone zdarzenie i zapewnić wsparcie HR pomocą doraźną i długofalową, gdyby np. zaszła konieczność udokumentowania zdarzenia przed wymiarem sprawiedliwości (polityki, procedury i inny materiał dowodowy).
Wyobraźmy sobie scenariusz, w którym sfrustrowany sytuacją pracownik, obywatel naszego kraju, wdaje się w kłótnię, a następnie przepychankę z pracownikiem pochodzenia ukraińskiego. Załóżmy, że pracownik ochrony zostaje wezwany w związku ze zdarzeniem na terenie zakładu pracy. Czy jesteśmy gotowi na taki scenariusz i potencjalne jego konsekwencje? Pominąwszy konsekwencje czysto ludzkie i związane z kodeksem pracy, nietrudno wyobrazić sobie, z jakimi jeszcze przyjdzie się zmierzyć organizacji, jeżeli niezależnie od prawdziwej natury konfliktu w Internecie czy prasie pojawi się nagłówek w stylu „Tak traktowani są uchodźcy w firmie X".
Przedstawiony scenariusz prowadzi do kolejnego zagadnienia, które zarówno organizacja, jak i komórki ds. bezpieczeństwa muszą uwzględnić w swoich strategiach.

ŚWIADOME I ODPOWIEDZIALNE POSŁUGIWANIE SIĘ INFORMACJĄ

Ponownie może się wydawać, że ma to niewiele wspólnego z komórkami odpowiedzialnymi za bezpieczeństwo. Wiele firm potrafi profesjonalnie zarządzać informacją, ma wyspecjalizowany personel, który troszczy się nie tylko o bezpieczeństwo informacji, ale także o jakość przekazu.
Osoby profesjonalnie zajmujące się bezpieczeństwem coraz wyraźniej zaczynają dostrzegać, że oprócz regularnej wojny w świecie fizycznym toczy się bardzo niebezpieczna wojna informacyjna, w której wszyscy mniej lub bardziej świadomie bierzemy udział. Publikujemy swoje przemyślenia, udostępniamy treści przekazywane przez innych czy własne zdjęcia czegoś, co wydaje się nam godne uwagi. Należy mieć świadomość, że jakaś część tego, co udostępniamy, może być użyta w sposób, który nie przyszedłby nam nawet do głowy.
Co ma organizacja do treści, jakie publikuję jako osoba prywatna i które nie mają nic wspólnego z działalnością organizacji, w której pracuję? Co do zasady – organizacji nic do tego, ale tu chodzi o to, że we współczesnej wojnie informacyjnej znaczenie ma nie tylko to, co piszesz, ale nawet kogo masz w znajomych na portalach społecznościowych. Im wyższe stanowisko zajmujesz, tym bardziej jesteś eksponowany na konsekwencje, które mogą cię dotknąć również na stopie zawodowej, a nawet postawić całą organizację w trudnej sytuacji. Masz prawo wyrażać swoje zdanie, ale staraj się robić to świadomie. Wyobraźmy sobie taki scenariusz: pracownik publikuje treść, która stoi jawnie w sprzeczności z wartościami deklarowanymi przez organizację. Wkrótce w mediach społecznościowych zaczyna krążyć wiadomość, że firma X zatrudnia pracownika, który prezentuje poglądy powszechnie uznawane za nieetyczne i brak w nich empatii dla ludzi, którzy nie ze swojej winy znaleźli się w obecnym położeniu.
Czy organizacja jest przygotowana na taki scenariusz? Czy pracownicy są gotowi na takie sytuacje? W świecie bezpieczeństwa wiemy, że najważniejsze są fakty i decyzje oparte na faktach (wiarygodnych, sprawdzonych informacjach). Wiemy też, jakie konsekwencje może przynieść nieodpowiedzialne posługiwanie się informacją opartą na swobodnej interpretacji zdarzeń dyktowanej emocjami. Uważam, że to właśnie menedżerowie bezpieczeństwa powinni zgłaszać do władz organizacji konieczność podnoszenia świadomości odpowiedzialnego wypowiadania się. Świadomość tego rodzaju pomoże nie tylko pracownikom, ale także organizacji.

BEZPIECZEŃSTWO PRACOWNIKÓW POZA MIEJSCEM PRACY

Znaczna część osób, które uciekły do Polski z Ukrainy, będzie (i słusznie) szukać i już szuka zatrudnienia w Polsce. I choć bardzo chciałbym się co do tego mylić, obawiam się, że po pierwszym odruchu pięknej i spontanicznej pomocy okazywanej uchodźcom z czasem mogą pojawiać się nastroje antyukraińskie. Nawet pojedyncze grupy wyładowujące swoje frustracje mogą stanowić realne zagrożenie dla naszych pracowników, w tym pochodzenia ukraińskiego.
Ważne będzie monitorowanie tego zjawiska w kontekście siły i lokalizacji występowania. Współpraca z organami ścigania i odpowiednie programy podnoszące świadomość naszych pracowników (zwłaszcza tych pochodzenia ukraińskiego, którzy nie zdążyli jeszcze dobrze poznać naszego kraju) co do potencjalnych zagrożeń, sposobu zachowania, rodzaju i dostępnej pomocy w sytuacji zagrożenia jest tym, nad czym należy pracować już teraz. Nie wykluczam, że w określonych lokalizacjach trzeba będzie pomyśleć o zapewnieniu bezpiecznego transportu do i z miejsca pracy.

WSPÓŁPRACA MIĘDZY DEPARTAMENTAMI

Zarysowane problemy wyraźnie pokazują, że komórki ds. bezpieczeństwa będą zaangażowane w większe wyzwania, których nie są adresatem. Organizacje, które jeszcze tego nie zrobiły, powinny możliwie szybko wzmocnić relacje między departamentami. Ponieważ wszystkie wskazane zagadnienia dotyczą pracowników i wrażliwych społecznie zagadnień, szczególną rolę przypisałbym konieczności ścisłej współpracy między komórkami HR, bezpieczeństwa i odpowiedzialnymi za komunikację wewnątrz i na zewnątrz organizacji.
Ze względu na specyfikę pracy menedżerów bezpieczeństwa i posiadane umiejętności szerszego analitycznego postrzegania zagrożeń i ich konsekwencji to oni powinni wyjść z inicjatywą i przedstawić w swoich organizacjach poruszoną tu problematykę. Mam świadomość, że siła przebicia może być różna, jednak wczesne zaadresowanie potencjalnych konsekwencji zwiększa szansę przygotowania organizacji na ich wystąpienie. Działania czysto reaktywne mogą być w tym zz

JAN KAPUSTA

mgr inż., Dip. CSMP®, M.ISMI®. Praktyk i wykładowca, od ponad 20 lat związany z branżą security i zarządzaniem bezpieczeństwem. Współtwórca i były przewodniczący Forum Bezpieczeństwa Fizycznego przy Radzie Bezpieczeństwa ZBP. Obecnie zarządza bezpieczeństwem operacyjnym z obszarem działania obejmującym Europę Środkową i Wschodnią, Rosję i Wspólnotę Niepodległych Państw.

Wojna w Ukrainie

a cyberbezpieczeństwo w Polsce

niebezpiecznik.pl

Jaki wpływ na bezpieczeństwo polskiego Internetu ma inwazja Rosji na Ukrainę i jak się zabezpieczyć przed ewentualnymi negatywnymi skutkami cyberataków skierowanych zarówno przeciwko Ukrainie, jak i krajom sojuszniczym? Oto kilka porad i opis tego, co może nam zagrażać w sferze internetowej.

DZISIAJ WOJNA TO NIE TYLKO BOMBY, TO TAKŻE WIRUSY, ATAKI DDOS CZY DEFACE

Bombardowanie Ukrainy zaczęło się 24 lutego, ale pierwszą fazą ataku w tej wojnie były działania w cyberprzestrzeni. Tak naprawdę zaczęły się one już 15 stycznia, kiedy zaatakowano kilkanaście sieci rządowych (tzw. Deface). Włamywacze, używając narzędzi powiązanych z tymi, które wykorzystują rosyjscy hakerzy, podmienili treści rządowych stron internetowych na komunikat. Treść sugerowała, że za atakiem mają stać nieprzychylni Ukraińcom Polacy... Tego samego dnia do niektórych rządowych ukraińskich sieci wpuszczono złośliwe oprogramowanie służące do kasowania danych (tzw. wiper).
Z kolei 23 lutego wieczorem informowaliśmy na naszym Twitterze, że ok. godz. 16:00 ESET powiadomił o kolejnej fali ataków na setki komputerów w ukraińskich firmach i instytucjach. Znów użyto tzw. wipera i sparaliżowano działania tych instytucji, wymuszając konieczność odtworzenia systemów z kopii bezpieczeństwa. Ten atak miał zapewne zająć i utrudnić reakcję w początkowej fazie inwazji zbrojnej, która nadeszła 10 godzin później. Ta wojna zaczęła się więc od cyberataku. Ukraińskie serwery regularnie były i są atakowane DDoS-ami. Nie powodują one wprawdzie utraty danych, ale budzą niepokój wśród ludzi, którzy ze względu na skutki ataku nie mogą dostać się np. do swoich kont bankowych. Również 23 lutego o godzinie 16:30 taki atak DDoS uruchomiono przeciwko kilku ukraińskim instytucjom. Co ciekawe, w tym samym czasie atak DDoS odnotowaliśmy także my i kilka innych sieci w Polsce. Atak nie był duży i trwał ok. 30 min, ale jego charakterystyka była ciekawa – proporcja złośliwego ruchu z polskich adresacji była wyższa niż we wcześniejszych atakach DDoS.

KONSEKWENCJE DLA POLSKI

Bazując na przedstawionym opisie tego, co się dzieje w ukraińskiej cyberprzestrzeni, daje się zauważyć trzy rodzaje zagrożeń.

1. ATAK ZŁOŚLIWYM OPROGRAMOWANIEM

Na razie wszystkie tego typu działania, o jakich wiemy, są skierowane przeciw sieciom i firmom w Ukrainie. Ale pamiętajmy, że Internet nie ma granic i wiele polskich firm ma oddziały lub w inny sposób jest ściśle połączone z firmami na Ukrainie. Oznacza to, że infekcja i atak na maszyny znajdujące się po stronie ukraińskiej może szybko rozpropagować się na połączone z nimi polskie siedziby. Wspomniany wiper został też użyty wobec firm na Litwie, a podobny atak już kilka lat temu był przeprowadzony także na firmy w Polsce świadczące usługi (czyli połączone) z firmami na Ukrainie. Polskie firmy utrzymujące sieciowy kontakt z Ukrainą powinny:

- upewnić się, że połączenia pomiędzy sieciami (oddziałami) są odpowiednio filtrowane,
- zweryfikować konfigurację rozwiązań bezpieczeństwa, zwłaszcza pod kątem propagacji wiperów,
- wprowadzić, gdzie to możliwe, dwuskładnikowe uwierzytelnienie, najlepiej oparte na kluczach U2F, aby ograniczyć ataki phishingowe i *credential stuffing*,
- zweryfikować poprawność wykonywania kopii bezpieczeństwa i zdolność przywracania z nich pracy systemów.

2. BEZPOŚREDNI ATAK NA INFRASTRUKTURĘ W POLSCE

Na razie nie ma informacji, aby Polska infrastruktura była bezpośrednim priorytetowym celem ataków ze strony Rosjan. Ale to może się zmienić, m.in. dlatego, że wraz z innymi państwami oficjalnie pomagamy Ukrainie w cyberkonflikcie, a więc Rosjanom może zależeć, aby związać nasze zasoby rodzimymi problemami.
W Polsce obowiązuje już stopień alarmowy CHARLIE-CRP. To oznacza, że przynajmniej obiekty infrastruktury krytycznej powinny być ściślej niż zwykle monitorowane pod kątem zagrożeń. Wprowadzono m.in. dyżury 24-godzinne i przetestowano procedury awaryjne. Nie uważamy, że grozi nam całkowity cyberparaliż w Polsce, ale na chwilowe awarie w dostępie do różnych usług warto się przygotować. I nie wpadać w panikę, kiedy nastąpią. W celu zminimalizowania skutków takich ataków:

- zadbaj o to, aby kluczowe dla siebie dane mieć lokalnie, a nie w chmurze (kontakty, klucze licencyjne itp.);
- ulokuj pieniądze w kilku bankach. Gdyby jeden miał problem, będziesz mógł skorzystać z drugiego;
- miej przy sobie gotówkę na wypadek awarii nie tylko banku, ale także pośredników w płatnościach obsługujących terminale w sklepach;
- zaktualizuj swój system operacyjny na komputerze, telefonie, telewizorze, kamerze monitoringu, lodówce. Wszędzie. W ten sposób zamykasz ewentualnym atakującym dostęp do twoich urządzeń za pomocą znanych, niezałatanych dziur, gdyż takie najczęściej się wykorzystuje w atakach internetowych;
- naładuj powerbanki;
- pamiętaj, że w trakcie wojny celem jest przede wszystkim paraliż infrastruktury krytycznej, gdyż jednym uderzeniem można zaszkodzić wielu osobom (co nie wyklucza ataków skierowanych na poszczególnych internautów). To prowadzi nas do trzeciego zagrożenia.

3. DEZINFORMACJA i PSYOP[1]

Od dawna obserwujemy działania dezinformacyjne ze strony Rosji i Białorusi, m.in. wymierzone przeciwko Polsce. Narracji jest sporo. Przytoczmy zwłaszcza dwa przykłady: kiepskie „dowody" na to, że za atakami na ukraińskie serwisy internetowe mają stać Polacy, oraz najświeższy tzw. *false-flag,* że to niby Polacy mieli wysadzić w powietrze zbiornik z chlorem na terenie oczyszczalni ścieków w Doniecku[2].
Celem tych działań jest poróżnienie sojuszników, ale w dobie Internetu zagrożenie dezinformacją jest zdecydowanie bardziej złożone i przerażające. Obserwujemy, jak w mediach społecznościowych pojawiają się fałszywe komunikaty (np. o tym, gdzie doszło do „tragicznego w skutkach ataku") albo ślady operacji PSYOP. Na przykład SMS-ów, które miały zostać wysłane do ukraińskich żołnierzy tuż przed inwazją, „zachęcające" do ucieczki i poddania się bez walki. Wspomnijmy podobne SMS-y, których nikt nie widział (krążyły same screenshoty) wysłane do Polaków w strefie przygranicznej informujące o mobilizacji wojskowej kilka lat temu.

[1] Operacje psychologiczne
[2] https://twitter.com/EliotHiggins/status/1495355366141534208

Takie działania i wpisy, często bardzo mocno nacechowane emocjonalnie, mają na celu szybko spolaryzować dyskusję i fałszywie kogoś o coś oskarżyć, wywołać niepokój. Są szybko udostępniane i podawane dalej. Bazując na półprawdach, mieszając fakty z fake newsami, skutecznie budują fałszywą narrację. Dlatego:

1. Nie wierz we wszystko, co widzisz w Internecie z obszaru „konfliktu". Bardzo często zdjęcia i materiały wideo pochodzą z innych lokalizacji i innej daty. Pamiętaj, że nie zawsze łatwo zweryfikować prawdziwość tych nagrań, a ich metadane można fałszować;
2. Bazuj na zaufanych źródłach. Preferuj rzetelnych dziennikarzy, którzy znają sytuację geopolityczną, są na miejscu i dokładnie weryfikują to, co podają, ponieważ od tego zależy ich reputacja. Listę takich osób piszących o Ukrainie na bieżąco znajdziesz w naszym serwisie niebezpiecznik.pl, ale pamiętaj, że i one mogą czasem dać się ponieść emocjom;
3. Zastanów się, zanim podasz informację dalej. Sprawdź „komentarze", może ktoś dostrzegł coś podejrzanego w danym przekazie;
4. Jeśli po fakcie zorientujesz się, że nowe informacje przeczą temu, co podałeś dalej, usuń lub odpowiednio skoryguj wcześniejszy wpis. To żaden wstyd. Sytuacja zmienia się dynamicznie, a wiele treści jest naprawdę profesjonalnymi manipulacjami. Ryzyko błędu jest wpisane w dyskusję internetową, ale rzetelnych dyskutantów poznaje się po tym, że przyznają się do błędów.

WAŻNA RADA DLA KAŻDEGO

Gdzie tylko możliwe włącz dwuskładnikowe uwierzytelnienie w oparciu o klucze U2F. To jedyne zabezpieczenie, które nie jest podatne na najbardziej popularne i wykierowane w każdego ataki phishingowe.

Zdecydowanie warto zabezpieczyć w ten sposób skrzynkę e-mail i konta w mediach społecznościowych. Przejęcie skrzynki oznacza dostęp do wszystkich kont, które zarejestrowaliśmy na ten adres e-mail, jeśli nie mamy na nich włączonego dwuskładnikowego zabezpieczenia. Przejęcie profili w mediach społecznościowych to ryzyko wycieku poufnych danych z prywatnych rozmów i wykorzystanie naszego konta do dezinformacji lub ataku na naszych przyjaciół (tzw. atak na BLIK).

Na naszym kanale na YouTubie zamieszczamy dziesiątki godzin merytorycznego materiału z zakresu cyberbezpieczeństwa.
Zdecydowanie częściej i więcej tego, co się dzieje w polskiej cyberprzestrzeni, publikujemy na naszych profilach na Twitterze[3] i Facebooku[4]. Tu na nasz serwis o bezpieczeństwie teleinformatycznym trafiają najpoważniejsze tematy.

[3] https://twitter.com/niebezpiecznik
[4] https://www.facebook.com/niebezpiecznik

Uwaga, stopień!

Tomasz Dacka

W momencie pisania artykułu w Polsce obowiązują dwa stopnie alarmowe: BRAVO oraz CHARLIE-CRP. Różnią się one obszarem obowiązywania i dotyczą różnych aspektów bezpieczeństwa. Co właściwie oznaczają? Jak je odnosić do branży bezpieczeństwa fizycznego? Jakie niosą konsekwencje dla obywateli Rzeczypospolitej Polskiej?

Wprowadzanie stopni alarmowych jest ściśle uregulowane (o czym w następnej części artykułu), a samo ich wprowadzenie nie musi oznaczać jakiegokolwiek ataku na terytorium RP. Zatem nie ma tu powodów do paniki czy pojawiania nadmiernych co do sytuacji działań (np. wypłacanie dużych ilości gotówki, przesadne zakupy). To, jaki stopień został wprowadzony, i dlaczego, można odczytać literalnie z regulacji prawnych. Chociaż konkretna przyczyna wprowadzenia zapewne pozostanie nieznana szerszemu gronu odbiorców, to metodyka wprowadzania stopni jest transparentna, co zdecydowanie odróżnia ją od zalewu dezinformacji mającej na celu wzbudzenie paniki, niepewności i strachu.

Niemniej jednak nadal pojawia się dużo pytań dotyczących stopni. Co oznaczają stopnie CRP i czy są tożsame ze stopniami bez CRP w nazwie? Jakie obowiązki nakładają na obszar bezpieczeństwa? Stopnie alarmowe są nie od dziś i już wcześniej, zazwyczaj przy okazji ważnych wydarzeń politycznych czy społecznych, były komunikowane i wprowadzane. Obecna sytuacja związana z wojną w Ukrainie jest jednak na tyle nadzwyczajna (poza działaniami wojennymi), że wprowadzono stopnie wyższe niż dotychczas (CHARLIE-CRP po raz pierwszy w historii) w tak długiej perspektywie czasowej.

KTO, JAK, DLACZEGO?

Aby zrozumieć istotę wprowadzania stopni alarmowych, należy zajrzeć do litery prawa. Zacznijmy od „fundamentu", czyli ustawy o ochronie osób i mienia[1], w której w art. 5 określono, co podlega obowiązkowej ochronie, tj. obszary, obiekty, urządzenia i transporty ważne dla obronności, interesu gospodarczego państwa, bezpieczeństwa publicznego i innych ważnych interesów państwa [...].
Koncepcję ochrony realizuje się za pomocą planów ochrony, które podlegają obligatoryjnym uzgodnieniom z właściwym terytorialnie komendantem wojewódzkim Policji, a w zakresie zagrożeń o charakterze terrorystycznym, z właściwym terytorialnie dyrektorem delegatury Agencji Bezpieczeństwa Wewnętrznego (art. 7 ust. 1).
W kontekście omawianego obszaru warto zwrócić szczególną uwagę na konieczność uzgodnień tematyki antyterrorystycznej. Odbywa się to za pomocą załącznika antyterrorystycznego (załącznika do planu ochrony), który jest uzgadniany z delegaturą ABW, i to w nim powinny znaleźć się informacje szczególnie nas interesujące.
Co zatem powinien taki załącznik zawierać? Najlepiej sprawdzić u źródła. Na stronie Biuletynu Informacji Publicznej ABW zamieszczono wytyczne co do zawartości omawianego załącznika. Można tam wyczytać, że załącznik powinien zawierać m.in. zakres przedsięwzięć wykonywanych w przypadku uruchomienia czterech kolejnych stopni alarmowych (nie dotyczy stopni alarmowych CRP) przewidzianych ustawą antyterrorystyczną, na obszarze administracyjnym, na którym zlokalizowany jest ochraniany obszar, obiekt, urządzenie podlegające ochronie. Jest tu zatem odnośnik do ustawy antyterrorystycznej, czyli ustawy o działaniach antyterrorystycznych[2]. To właśnie ten dokument odpowiada na gros pytań: kto, jak, dlaczego wprowadza stopnie alarmowe.

1 Ustawa z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz.U. z 2021 r. poz. 1995 ze zm.).

STOPIEŃ STOPNIOWI NIERÓWNY

Wspomniana ustawa o działaniach antyterrorystycznych wprowadza dwa rodzaje stopni alarmowych: stopnie alarmowe oraz stopnie alarmowe CRP. Nazewnictwo stopni rzeczywiście może wprowadzać niektórych w konsternację, stopnie różnią się bowiem jedynie członem nazwy CRP, a jakby tego było mało, nomenklaturę zachowano również przy nazewnictwie poszczególnych stopni. I tak, zgodnie z art. 15 ustawy o działaniach antyterrorystycznych, rozróżniamy:

1. W przypadku zagrożenia wystąpieniem zdarzenia o charakterze terrorystycznym albo w przypadku wystąpienia takiego zdarzenia można wprowadzić jeden z czterech stopni alarmowych:

- pierwszy stopień alarmowy (stopień ALFA);
- drugi stopień alarmowy (stopień BRAVO);
- trzeci stopień alarmowy (stopień CHARLIE);
- czwarty stopień alarmowy (stopień DELTA).

2. W przypadku zagrożenia wystąpieniem zdarzenia o charakterze terrorystycznym dotyczącego systemów teleinformatycznych organów administracji publicznej lub systemów teleinformatycznych wchodzących w skład infrastruktury krytycznej albo w przypadku wystąpienia takiego zdarzenia można wprowadzić jeden z czterech stopni alarmowych CRP:

- pierwszy stopień alarmowy CRP (stopień ALFA-CRP);
- drugi stopień alarmowy CRP (stopień BRAVO-CRP);
- trzeci stopień alarmowy CRP (stopień CHARLIE-CRP);
- czwarty stopień alarmowy CRP (stopień DELTA-CRP).

Łatwo zatem wywnioskować, że stopnie CRP dotyczą zagrożeń wymierzonych w infrastrukturę teleinformatyczną (poszczególnych podmiotów), podczas gdy stopnie alarmowe mówią o ogólnych zagrożeniach. Wprowadzanie poszczególnych stopni (zarówno stopni, jak i stopni CRP) jest podyktowane następującymi kwestiami:
Pierwszy stopień alarmowy – wprowadzany w momencie, kiedy istnieją przesłanki o możliwości wystąpienia zdarzenia o charakterze terrorystycznym, którego rodzaj i zakres jest trudny do przewidzenia.
Drugi stopień alarmowy – wprowadzany w momencie, kiedy oszacowane prawdopodobieństwo wystąpienia zdarzenia o charakterze terrorystycznym jest większe, ale trudno sprecyzować cel, w który zostanie wymierzone.
Trzeci stopień alarmowy – ustawa mówi już o wystąpieniu zdarzenia, które urealnia prawdopodobny cel ataku (model naczyń połączonych) wymierzony w bezpieczeństwo porządku publicznego, bezpieczeństwo RP lub bezpieczeństwo innego państwa, które może mieć przełożenie na bezpieczeństwo RP. Ponadto trzeci stopień wprowadza się w następujących sytuacjach:

- w momencie wejścia w posiadanie informacji (wiarygodnej i potwierdzonej) dotyczącej planowania zdarzenia o charakterze terrorystycznym na terytorium RP,
- w momencie wejścia w posiadanie informacji (wiarygodnej i potwierdzonej) dotyczącej planowania zdarzenia o charakterze terrorystycznym wymierzonym w obywateli RP przebywających za granicą oraz instytucji polskich, polskiej infrastruktury rozlokowanych poza granicami RP.

Czwarty stopień alarmowy – wprowadzany adekwatnie do założeń trzeciego stopnia, ale mowa tu już o wystąpieniu (bezpośredniego) zdarzenia o charakterze terrorystycznym lub w momencie wejścia w posiadanie informacji wskazującej jednoznacznie na zaawansowaną fazę przygotowań dotyczących zdarzeń wskazanych przy stopniu trzecim.

W celu doprecyzowania odnośnie do wprowadzania stopni (w tym stopni CRP) należy wskazać następujące elementy:

2 Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (Dz.U. z 2021 r. poz. 2234 ze zm.).

1. Można wprowadzać stopnie wyższe z pominięciem stopni niższych.
2. Stopnie mogą być wprowadzane rozłącznie lub wspólnie.
3. Stopnie można wprowadzać w dowolny sposób z podziałem na obszary, jednostki organizacyjne.
4. Odwołanie obowiązujących stopni odbywa się niezwłocznie po ustąpieniu przesłanek do ich wprowadzenia.
5. W momencie występowania różnych stopni należy wykonywać zadania przypisane do stopnia wyższego.
6. Stopnie wprowadza i odwołuje Prezes Rady Ministrów drogą rozporządzenia.

OBOWIĄZKI

Wprowadzenie samych stopni bez wskazania i przypisania im zadań do wykonania byłoby pozbawione sensu. W związku z tym wprowadzono drogą rozporządzenia Prezesa Rady Ministrów doprecyzowanie wymaganych przedsięwzięć. W poniższej tabeli omówiono wybrane obowiązki przy wprowadzeniu zarówno stopni alarmowych, jak i stopni alarmowych CRP zgodnie z Rozporządzeniem Prezesa RM w sprawie zakresu przedsięwzięć wykonywanych w poszczególnych stopniach alarmowych i stopniach alarmowych CRP[3].
Co ważne, rozporządzenie wskazuje, kogo dotyczą zapisy, wymieniając podmioty, tj. organy administracji publicznej, kierowników służb i instytucji właściwych w sprawach bezpieczeństwa i zarządzania kryzysowego, właściciele (posiadaczy) samoistnych oraz zależnych obiektów infrastruktury krytycznej w zakresie ochrony tych obiektów.

Tabela 1. Wybrane wymagania stopni alarmowych

	STOPIEŃ ALARMOWY	STOPIEŃ ALARMOWY CRP
ALFA	Prowadzenie wzmożonych kontroli obiektów użyteczności publicznej (np. za pomocą dozbrojonej obsady posterunków ochrony). Informowanie służb w momencie zauważenia podłożonych ładunków, nieznanych pojazdów lub wszelkich innych działań, które są nietypowe dla zapewnienia bezpieczeństwa danej strefy. Poinformowanie personelu o konieczności zachowania większej czujności, gdy cokolwiek wzbudza ich niepokój. Bycie przygotowanym na konieczność dozbrojenia posterunków ochrony w dodatkową siłę ludzką. Konieczność przeprowadzania kontroli pojazdów. Konieczność sprawdzenia działania systemów alarmowych, przepustowości dróg ewakuacyjnych, sprawności wizyjnych systemów dozoru wideo.	Wprowadzenie wzmożonego monitoringu stanu bezpieczeństwa systemów ICT, w tym zapewnienie, że nie doszło do naruszenia bezpieczeństwa komunikacji elektronicznej, zachowanie dostępności usług elektronicznych. Poinformowanie personelu o zaistniałej sytuacji i konieczności zachowania zwiększonej czujności. Sprawdzenie sprawności kanałów łączności, punktów kontaktowych z zespołami reagowania na incydenty cyberbezpieczeństwa. Dokonanie weryfikacji posiadanych kopii zapasowych wraz ze sprawdzeniem czasu przywrócenia działania usług.
BRAVO	Wprowadzenie dodatkowych kontroli pojazdów oraz osób. Sprawdzenie skuteczności działania zasilania awaryjnego. Zapewnienie w trybie alarmowym dostępności personelu odpowiedzialnego za wdrażanie procedur związanych z materializacją zdarzenia o charakterze terrorystycznym. Wzmocnienie ochrony ważnych obiektów publicznych. Sprawdzenie systemu ochrony obiektów obsługiwanych przez SUFO. Wprowadzenie kontroli przesyłek pocztowych. Zamknięcie nieużywanych pomieszczeń, budynków.	Zapewnienie w trybie alarmowym obecności personelu odpowiedzialnego za bezpieczeństwo systemów. Wprowadzenie całodobowych dyżurów administratorów systemów kluczowych oraz osób decyzyjnych w sprawach bezpieczeństwa systemów ICT.
CHARLIE	Wprowadzenie całodobowych dyżurów we wskazanych urzędach i jednostkach administracji publicznej (na wniosek ministra właściwego do spraw wewnętrznych). Wprowadzenie dyżurów personelu odpowiedzialnego za wdrażanie procedur związanych z materializacją zdarzenia o charakterze terrorystycznym. Ograniczenie do minimum liczby miejsc ogólnodostępnych w chronionych obiektach i ich rejonach. Wprowadzenie ścisłej kontroli osób i pojazdów. Wydanie broni i amunicji wraz ze środkami ochrony osobistej osobom uprawnionym do wykonywania zadań ochronnych. Wprowadzenie całodobowego nadzoru nad miejscami wskazanymi jako podatne, a do tej pory nieobjętymi nadzorem.	Dokonanie przeglądu zasobów zapasowych i ich skuteczności w momencie konieczności ich zastosowania. Dokonanie audytu planów awaryjnych. Przygotowanie się do ograniczenia pracy na serwerach w momencie konieczności ich nagłego wyłączenia.
DELTA	Wprowadzenie ograniczeń komunikacyjnych. Zapewnienie identyfikacji wszystkich pojazdów znajdujących się w chronionych strefach (uwzględniając w uzasadnionych przypadkach ich relokację). Wprowadzić kontrolę wszystkich pojazdów wraz z przewożonym ładunkiem. Wszystkie przedmioty wnoszone na teren obiektu podlegają kontroli. Należy przeprowadzać częste kontrole na zewnątrz budynków (w tym na parkingach). Przygotować się do konieczności świadczenia pracy w innym miejscu niż docelowym.	Uruchomienie planów awaryjnych, ciągłości działania w kontekście utraty ciągłości działania operacyjnej jednostki. Przystąpienie, w miarę możliwości, do procedur przywracania ciągłości działania.

Przy wprowadzaniu stopni wyższych (np. CHARLIE) należy spełnić wszystkie wymagania stopni niższych (w tym przypadku ALFA oraz BRAVO).
Jak widać z podanych przykładów, bardzo istotne jest nie tylko zrozumienie wymagań, ale także przełożenie ich na możliwe do zastosowania w rzeczywistości plany. Aby to osiągnąć, konieczne jest moim zdaniem:

- Zapewnienie odpowiednich środków finansowych na wypadek wystąpienia konieczności wdrażania działań zgodnie z poszczególnymi stopniami.
- Wcześniejsze wskazanie osób odpowiedzialnych za wdrożenie, rozliczenie i komunikację związaną z działaniami zaradczymi.
- Przygotowanie procedur postępowania w momencie ogłoszenia odpowiednich stopni alarmowych (nie tylko zapisy w załącznikach antyterrorystycznych, ale również wewnętrzne przepisy jednostki organizacyjnej zapewniające skuteczną, wewnętrzną i zewnętrzną, komunikację oraz jasno wskazujące odpowiedzialność).
- Zapewnienie odpowiedniej komunikacji pomiędzy zespołami wdrażającymi środki zgodnie ze stopniami alarmowymi oraz stopniami alarmowymi CRP (konwergencja bezpieczeństwa na styku z utrzymaniem i serwisem obiektów).
- Prowadzenie cyklicznych szkoleń, ćwiczeń i przeglądów planów ochrony.

Odpowiednie stopnie alarmowe wymagają od branży ochrony podejmowania działań z uwzględnieniem środków ochrony strukturalnej, elektronicznej, proceduralnej, a przede wszystkich zasobów ludzkich. We wdrażaniu niektórych wymagań pomocne mogą stać się np. analityka zawartości wideo (VCA) czy zastosowanie oprogramowania klasy PSIM, które uzbrojone w odpowiednie scenariusze wydatnie usprawni pracę posterunków ochrony w momencie ogłaszania poszczególnych stopni alarmowych.

DZIEŃ JAK CO DZIEŃ?

Jaki wpływ na życie osób niezwiązanych z obszarem security ma wprowadzenie stopni alarmowych? Czy wymaga się od nich podejmowania jakichkolwiek działań? Litera prawa nie wymaga, jednak zdrowy rozsądek już powinien. Należy zachować przede wszystkim spokój i pozwolić pracować ludziom bezpośrednio zaangażowanym w działania zaradcze. Na koniec wystosowałbym kilka osobistych rad:

- Jeśli nie musisz, ogranicz wizyty w urzędach i innych jednostkach administracji publicznej (szczególnie przy trzecim i czwartym stopniu alarmowym).
- To nie jest dobry czas na fotografowanie i wycieczki do ciekawych obiektów objętych zapisami wspomnianych w artykule ustaw.
- Zrewiduj swoje hasła do najważniejszych usług (w tym bankowości elektronicznej i poczty elektronicznej).
- Włącz mechanizm uwierzytelniania wieloskładnikowego w kontaktach z bankiem, w obsłudze poczty elektronicznej.
- Uważaj na próby wyłudzenia pieniędzy wykorzystujące zaistniałą sytuację.
- Weryfikuj źródła informacji, jeśli jest to dla ciebie problemem – w pierwszej kolejności czerp wiedzę ze źródeł oficjalnych.

3 Rozporządzenie Prezesa Rady Ministrów z dnia 25 lipca 2016 r. w sprawie zakresu przedsięwzięć wykonywanych w poszczególnych stopniach alarmowych i stopniach alarmowych CRP (Dz.U. z 2016 r. poz. 1101 ze zm.).

TOMASZ DACKA

Ekspert bezpieczeństwa fizycznego. Z branżą związany ponad 12-letnim doświadczeniem, zwolennik holistycznego podejścia do zarządzania bezpieczeństwem. Prywatnie entuzjasta architektury przedwojennej Warszawy.

Bezpieczeństwo cybernetyczne

w systemach zabezpieczeń technicznych

Piotr Rogalewski

Kamery i inne urządzenia security już dawno przestały być systemami zamkniętymi. W istocie są to specjalizowane komputery, które realizują mnóstwo zadań dodatkowych, z wykorzystaniem sztucznej inteligencji włącznie. Filtrowanie fałszywych alarmów, rozpoznawanie sylwetki człowieka lub pojazdu, rozpoznawanie twarzy czy numerów rejestracyjnych „na pokładzie” urządzeń to tylko kilka przykładów możliwości obecnych rozwiązań. W architekturze systemu traktujemy kamerę czy rejestrator jako sprzęt, ale tak naprawdę realizacja tych przykładowych zadań możliwa jest tylko dzięki oprogramowaniu działającemu wewnątrz tego sprzętu. Na rynku komercyjnym o podobnych systemach mówi się, że są „smart”.

JAKI MAMY PROBLEM?

Można przyjąć za pewnik, że jeśli coś jest „smart”, to jest podatne na atak cybernetyczny. Dlaczego? Ponieważ mylić się jest rzeczą ludzką, a współczesne metody inżynierii oprogramowania oparte na metodykach „zwinnych” (np. SCRUM) niestety sprawy nie ułatwiają. W 2015 r. międzynarodowa firma konsultingowa Roland Berger przeprowadziła badania, z których wynika, że średnia stopa błędów programistycznych zawiera się w granicach między 15 a 50 problemów na każde 1000 linii kodu programu. Samo jądro systemu operacyjnego Linux stosowanego powszechnie w urządzeniach security to obecnie kilkanaście milionów linii kodu. Oprogramowanie kamery IP to kolejne kilka, kilkanaście milionów linii.

Co więcej, twórcy oprogramowania wykorzystują w swoich projektach wiele gotowych komponentów, tzw. bibliotek, które realizują zadania typowe dla niemal każdego systemu komputerowego, np. szyfrowanie danych, transmisję czy obsługę dzienników zdarzeń. Pozwala to skupić czas i środki na samym „rdzeniu” oprogramowania, nie zajmując się od podstaw sprawami, które ktoś już dobrze opracował i napisał (doskonałym przykładem są biblioteki obsługujące autentykację SSL czy EAP-TLS).
Ale tu pojawia się problem, bo nawet jeśli producent dołożył maksymalnych starań, świetnie przetestował produkt i wprowadził go na rynek jako wolny od luk, to takie ukryte luki mogły istnieć w komponentach (bibliotekach), których producent użył w swoim projekcie.

CO MOŻE SIĘ WYDARZYĆ?

Na początku 2021 r. jedna z największych w USA firm oferujących chmurowe usługi zabezpieczeń technicznych padła ofiarą ataku hakerskiego. Przestępcy uzyskali dostęp do ponad 150 tys. kamer. Ofiarami ataku były szpitale, posterunki policji, szkoły, firmy, a nawet więzienia i areszty śledcze. Ten przykład doskonale oddaje wagę zagadnień bezpieczeństwa cybernetycznego w systemach zabezpieczeń technicznych.
Nawet gdyby skala ataku była mniejsza, to oprócz konsekwencji dla wizerunku firmy czy instytucji może wystąpić wprost zagrożenie dla bezpieczeństwa mienia i/lub osób tam pracujących. Mogą też pojawić się poważne konsekwencje prawne i finansowe, jeśli np. okaże się, że podmiot nie dołożył należytych starań związanych z implementacją zapisów RODO. Problem jest naprawdę poważny, a w aktualnej rzeczywistości geopolitycznej śmiało można stwierdzić, że zagadnienia te nigdy nie były istotniejsze niż obecnie.
Technik stosowanych przez hakerów jest wiele. *Exploit*, czyli wykorzystanie błędów (luk) systemu do przejęcia kontroli nad nim, metoda *brute force*, czyli łamanie hasła metodą podstawiania kolejnych kombinacji znaków, *middle man* (człowiek w środku) polegający na podsłuchaniu i/lub modyfikacji transmisji do odbiorcy to tylko kilka przykładów.
Do tych technik programistycznych dochodzą inne, czysto socjotechniczne, np. „phishing” (fałszywe wiadomości ze spreparowanymi linkami lub niebezpiecznymi załącznikami), czy nawet „haking” fizyczny (np. kradzieże nośników danych).
W walce z socjotechnikami każdy z nas jest na pierwszej linii ognia, ale zwykle czujność i rozsądek wystarczą do zneutralizowania zagrożenia. Nie otwieramy maili z nieznanego źródła, nie klikamy linków, nie otwieramy załączników. Usuwamy wiadomość i zwykle jest po kłopocie. Jednak zagrożenia innego typu są tak różnorodne i jest ich tak wiele, że wymagają bardziej kompleksowego podejścia do zagadnienia.

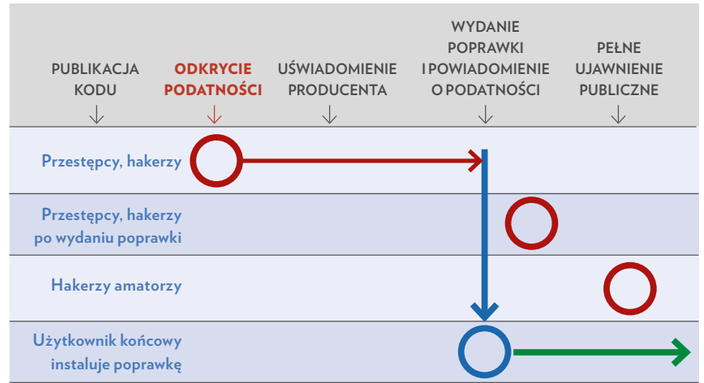
CO MOŻNA ZROBIĆ?

Po pierwsze – mieć świadomość zagrożeń. Skąd mamy wiedzieć, na jakie aktualne zagrożenia jest narażony nasz system zabezpieczeń technicznych? Pierwszoplanową rolę odgrywa tu jasna i szybka komunikacja ze strony producenta. Jeśli zidentyfikował on lukę w swoich produktach, musi jak najszybciej opracować odpowiednią poprawkę, przetestować ją i wydać np. w postaci nowej wersji firmware, jednocześnie powiadamiając swoich partnerów.
Ale producent sam nie jest w stanie rozwiązać problemu, gdyż uczestnikami procesu są też: klient końcowy, instalator/integrator i dystrybutor. Z różnych względów producent nie jest często w stanie dotrzeć do wszystkich podmiotów „na końcu łańcucha”. Dlatego komunikacja i szybkość działania mają tu kluczowe znaczenie. Zobaczmy scenariusz przedstawiony na *rys. 1*.
Hakerzy odkrywają podatność i wykorzystują ją do penetracji urządzenia. Producent urządzenia uzyskuje świadomość problemu albo samodzielnie go wykrywając, albo np. polegając na testach penetracyjnych realizowanych regularnie przez firmy zewnętrzne. Następnie producent przygotowuje poprawkę oprogramowania „łatającą” lukę i powiadamia o tym zainteresowanych partnerów/klientów.
I teraz rzecz zasadnicza: natychmiastowa instalacja poprawki powoduje „wyzerowanie” działań hakerskich, które będą musiały być uruchomione niejako od nowa w celu poszukiwania ewentualnej kolejnej (innej) luki lub próby obejścia wdrożonej poprawki. Hakerzy amatorzy, czyli grupa osób wykorzystująca publiczne już informacje o podatności, nie będzie mogła użyć ich do swoich celów.

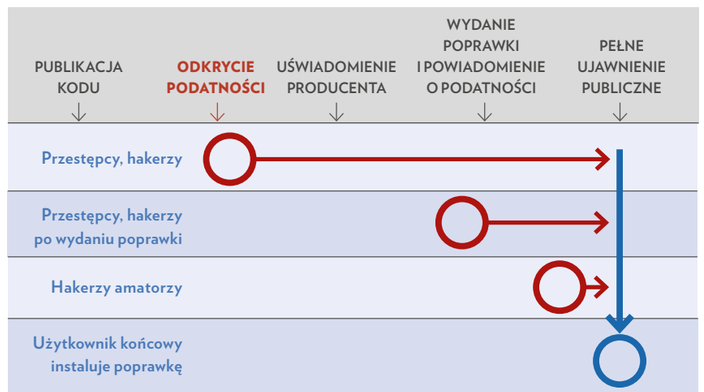
Co jednak dzieje się, gdy klient nie ma świadomości istnienia poprawki lub taką świadomość ma, ale z aktualizacją zwleka? Spójrzmy na wykres *z rys.2.* Sytuacja przed-

Przestępcy uzyskali dostęp do ponad **150 tys.** kamer

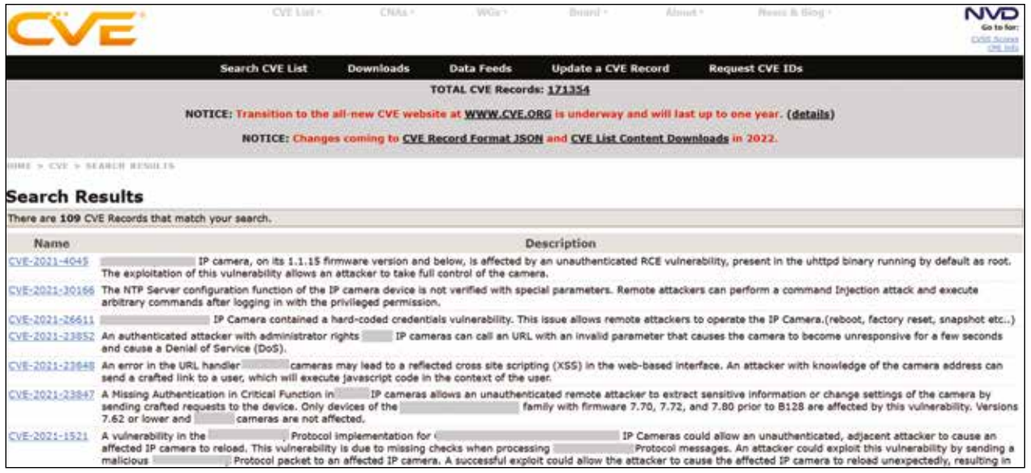
Rys. 1. Scenariusz „dzień zero” – klient instaluje poprawkę natychmiast po jej wydaniu



Rys. 2. Co się dzieje, gdy instalacja poprawki się opóźnia



Fot. 1. Publiczna baza podatności CVE. Na zdjęciu lista 109 podatności w odpowiedzi na wyszukiwanie hasła „IP camera”. Nazwy producentów sprzętu zostały zamaskowane.



stawia się tu o wiele gorzej – mimo wydania poprawki przez producenta hakerzy mogą operować bez żadnego dodatkowego nakładu pracy, wciąż wykorzystując „starą” lukę. Dodatkowo system jest narażony na działania hakerów amatorów, najczęściej wykorzystujących gotowe narzędzia typu *exploit*, zazwyczaj pojawiające się szybko po ujawnieniu podatności.

Tak więc skuteczny i szybki proces aktualizacji opiera się na ścisłej współpracy producenta, dystrybutorów, instalatorów/integratorów i klientów końcowych. Każdy z tych podmiotów może jednak zwiększyć sprawność swojej reakcji na zagrożenie, korzystając z publicznych baz danych wykrytych podatności. Najpopularniejszą chyba bazą tego typu jest strona http://cve.mitre.org. Zawiera ona wszystkie zgłoszone podatności, ich opis i stopień zagrożenia, jakie niosą.

JAK TO ROBI HIKVISION?

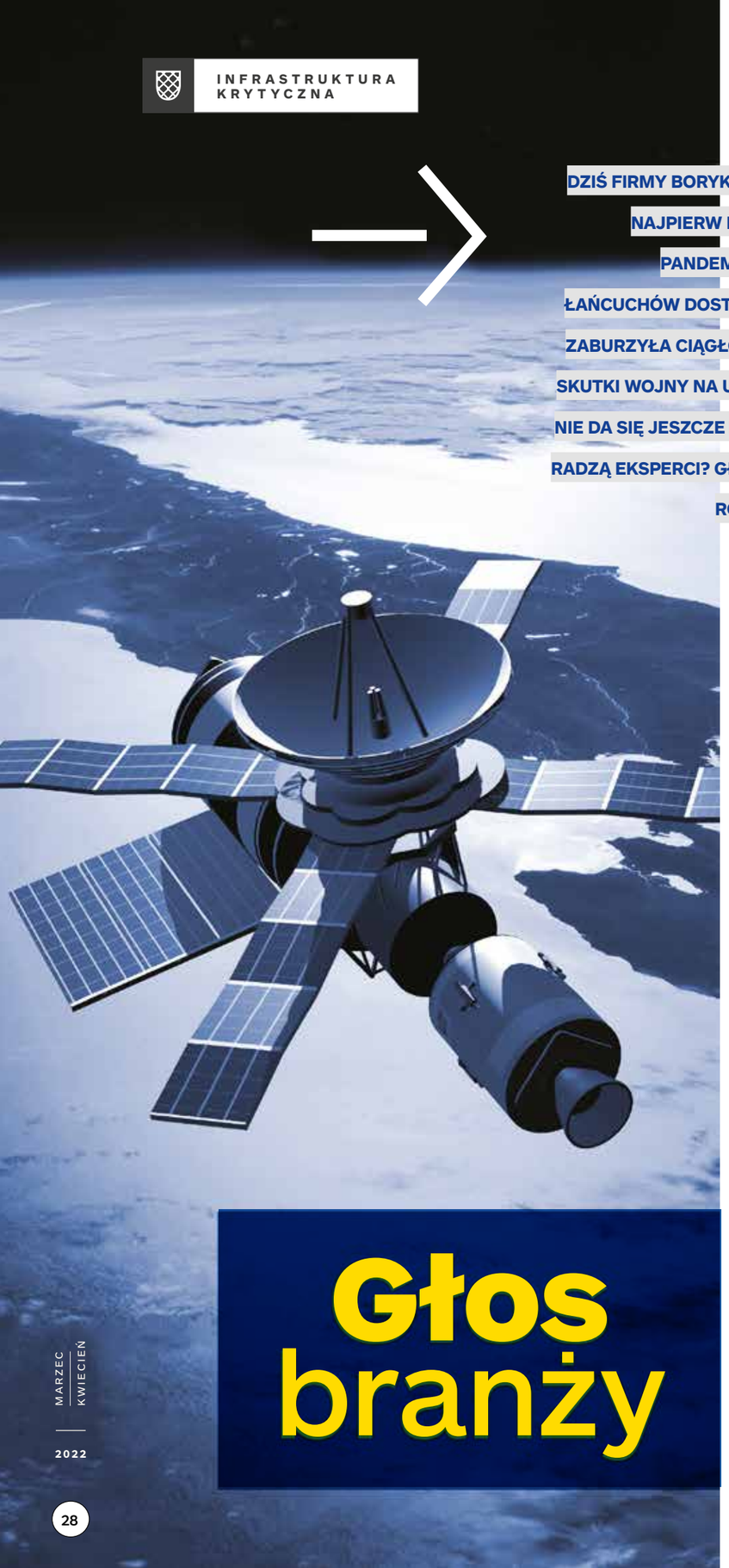
Zaufanie do urządzeń jako bezpiecznych elementów systemu jest nie do przecenienia. Hikvision podchodzi do tego zagadnienia kompleksowo. Przede wszystkim wdraża filozofię *Secure by design* i *Secure by default*. Ta pierwsza oznacza projektowanie urządzeń w taki sposób, by od momentu utworzenia miały bezpieczną architekturę i swoją konstrukcją logiczną i fizyczną minimalizowały ryzyko wystąpienia problemów. Drugi element oznacza taką domyślną konfigurację produktów, by urządzenie „wyjęte z pudełka” było możliwie najbardziej bezpieczne. W praktyce oznacza to np. brak haseł domyślnych, brak ukrytych funkcji (tzw. backdoor), wymuszanie wysokiej komplikacji hasła, brak możliwości użycia w haśle nazwy użytkownika, szyfrowanie plików z oprogramowaniem układowym (firmware), szyfrowanie plików konfiguracyjnych itd.

To także szereg zabezpieczeń na różnych poziomach – od fizycznych (np. zamek chroniący panel dostępu do dysków, podwójny zasilacz, niezależne porty sieciowe dla stacji roboczych i kamer), przez systemowe (autentykacja w protokole 802.1x EAP-TLS, szyfrowanie strumieni wizyjnych, kody weryfikacyjne w chmurze HikConnect, bezpieczna transmisja plików SFTP czy filtrowanie adresów IP), po bezpieczeństwo danych (zapis RAID, zapis awaryjny n+1, automatyczna kopia zapasowa, zarządzanie retencją danych, zapis awaryjny na kartach SD kamer i automatyczne kopiowanie tych danych do rejestratorów).

Ramy tego artykułu pozwalają zaledwie na bardzo ogólne zarysowanie istoty zagadnienia bezpieczeństwa cybernetycznego w systemach zabezpieczeń technicznych. Gorąco zachęcamy wszystkich zainteresowanych zgłębieniem tematu do bezpośredniego kontaktu z firmą Hikvision lub jej autoryzowanymi dystrybutorami.

HIKVISION POLAND

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



Głos branży

DZIŚ FIRMY BORYKAJĄ SIĘ Z WIELOMA PROBLEMAMI. NAJPIERW DZIAŁALNOŚĆ ZDESTABILIZOWAŁA PANDEMIA, KTÓRA PRZERWAŁA CIĄGŁOŚĆ ŁAŃCUCHÓW DOSTAW I WIELU PRZEDSIĘBIORSTWOM ZABURZYŁA CIĄGŁOŚĆ PRODUKCJI. DO TEGO DOSZŁY SKUTKI WOJNY NA UKRAINIE, KTÓREJ KONSEKWENCJI NIE DA SIĘ JESZCZE PRZEWIDZIEĆ. CO W TEJ SYTUACJI RADZĄ EKSPERCI? GŁOS ZABIERAJĄ PRZEDSTAWICIELE RÓŻNYCH SEKTORÓW GOSPODARKI.

Maksym Dzherikhov

Ajax Systems

Pomimo wojny w Ukrainie Ajax Systems zapowiada nowości

Od czasu wybuchu wojny w Ukrainie Ajax Systems nie czeka bezczynnie na pokój. Zamiast tego firma robi wszystko, co konieczne, by zapewnić ochronę i bezpieczeństwo swoim pracownikom oraz zagwarantować dostawy partnerom.
Do tej pory Ajax Systems przeniósł ponad 600 pracowników wraz z rodzinami do bezpiecznych regionów w Ukrainie i Europie. Producent robi również wszystko, aby jego oddziały i firmy partnerskie mogły normalnie funkcjonować. Obecnie jest w trakcie przenoszenia zapasów magazynowych wyrobów gotowych i ponownego uruchamiania produkcji. Regularne dostawy do partnerów zostały wznowione 9 marca.
Infrastruktura serwerowa Ajaxa działa bez zakłóceń, użytkownicy i partnerzy nie muszą się więc martwić o stabilność już zainstalowanych systemów. Serwery Ajaxa są geograficznie rozproszone w całej Europie, w centrach danych Amazon w Irlandii i Niemczech. Jest to sprawdzona ogólnoświatowa praktyka stosowana przez dużych producentów i organizacje.
Ajax kontynuuje również prace nad wprowadzeniem nowych produktów. Urządzenia, które firma zapowiedziała, będą wkrótce dostępne zgodnie z harmonogramem.

Janusz Syrówka

E.ON Polska

Test dla menedżerów bezpieczeństwa

Po pandemii koronawirusa wojna na Ukrainie to kolejny przykład, że prawdziwe wydarzenia prześcigają nawet najbardziej fantastyczne scenariusze. Co to oznacza dla ludzi z branży bezpieczeństwa – najprościej odpowiedzieć, że teoretycznie niewiele. Ta praca polega na mierzeniu się z takimi sytuacjami.
W ostatnim czasie pojawia się wiele analiz, opinii i oczywiście wypowiedzi ekspertów, z których płyną szerokim strumieniem dobre rady, co i jak teraz robić. Moim zdaniem osoby zajmujące się bezpieczeństwem przez cały czas są wystawione na oddziaływanie takiego czynnika jak niepewność, zwłaszcza w odniesieniu do nowych, nieprzewidzianych wcześniej scenariuszy. To jest test na to, co wnosimy do bezpieczeństwa. Test działań, które podejmowaliśmy w przeszłości, ale też test, jak my, ludzie, mierzymy się z nową sytuacją.
Największym wyzwaniem jest odwieczne i typowe dla branży bezpieczeństwa godzenie ognia z wodą. Chodzi mi o pewien naturalny konflikt polegający na maksymalnym sformalizowaniu zasad bezpieczeństwa – tworzenie procedur, regulaminów, list kontrolnych. To są ważne sprawy. Bardzo pomagają w tzw. sytuacji normalnej. Są również niezwykle pomocne w sytuacjach kryzysowych. Pozwalają działać na „autopilocie" w sytuacji presji czasu i stresu. Jednocześnie takie podejście może być „zabójcą" myślenia poza regułami. Takie godzenie ognia z wodą to umiejętność właściwej oceny sytuacji pomagająca nam znaleźć punkt krytyczny, gdzie procedury zamiast pomagać, przeszkadzają. To swoiste zdjęcie mentalnego „ogranicznika obrotów". Takie dylematy to dzisiaj największe wyzwanie.
W obecnym świecie wszyscy mamy porównywalny dostęp do informacji. Kluczowe jest, jak je zinterpretujemy i czy nasze wewnętrzne przekonania i blokady nie staną się główną przeszkodą w podjęciu właściwej decyzji. Występowanie w takiej roli jest obciążające i generuje duży stres.
Jakkolwiek potoczy się obecny kryzys związany z wojną na Ukrainie, jedno wydaje się pewne – potrwa długo. Dlatego moim zdaniem najważniejszą sprawą dla kierujących bezpieczeństwem jest dbanie o siebie. Znalezienie mimo wszystko czasu na odpoczynek i „reset" myśli. Będąc w dobrej formie, będziemy podejmować właściwe decyzje. Nieprawda, że jest to tak oczywiste, iż nie trzeba o tym mówić.
W dawnych dobrych i spokojnych czasach brałem udział w wielogodzinnych ćwiczeniach z zarządzania kryzysowego. Ćwiczenia, choć męczące, przebiegły pomyślnie, jednak wszystkich uczestników najbardziej zdziwiła jedna obserwacja asesorów ćwiczenia – tak skoncentrowali się na pracach, że zapomnieli o piciu wody. Taki stan rzeczy mógł w dalszej perspektywie doprowadzić do groźnego odwodnienia. Kończąc krótko, jeśli nie pomożesz sobie, to nie pomożesz też innym.

Mirosław Lukowski

ekspert ds. bezpieczeństwa

Testowanie procedur bezpieczeństwa

Dzisiaj, kiedy stoimy u progu kolejnego ogólnoświatowego kryzysu, wszystkie działania menedżerów ds. bezpieczeństwa muszą koncentrować się na szerokim spektrum obszarów bezpieczeństwa. Dostaję wiele zapytań o procedury na wypadek wojny, bo zarządy występują o takie opinie do działów bezpieczeństwa.
Według mnie głównym zadaniem powinno być teraz przetestowanie procedur pozwalających na utrzymanie procesów biznesowych, zachowanie ciągłości dostaw, utrzymanie ciągłości pracy i liczebności załogi. W tak trudnej sytuacji należy przeprowadzić testy podatności systemów na ataki hakerskie. Konieczna jest analiza sprzętu i oprogramowania. Nie można wykluczyć, że kraje, które dziś deklarują bądź darzą cichym poparciem reżim rosyjski, nie podejmą prób sabotowania prac ich urządzeń, z których my korzystamy. Przykładem jest PKP, której system integrujący był budowany na oprogramowaniu rosyjskim i jednego dnia wygenerował rozproszoną awarię, która sparaliżowała komunikację kolejową w całym kraju.
Ważnym krokiem jest też przetestowanie wszelkich procedur bezpieczeństwa, w tym ewakuacji osób. Podkreślę słowo „przetestowanie", a nie tylko „sprawdzenie dokumentacji". Działania praktyczne pozwalają ujawnić błędy i dziury, luki w procesie, a to daje możliwość usprawnienia i poprawę jakości działań.
Działy bezpieczeństwa stoją obecnie w obliczu nowych wyzwań, a tylko sprawnie działające mechanizmy mogą zapewnić poczucie stabilnego biznesu. Nowe wydarzenia wywołują też nowe zagrożenia. Ogromna tragedia naszych sąsiadów powoduje, iż jest już prawie 2 miliony uchodźców. Należy założyć, że jakiś odsetek z nich będzie brał udział w procesach kryminogennych. W związku z tym branża handlu detalicznego musi być gotowa na wzrost kradzieży w sklepach, a społeczeństwo na zwiększoną liczbę innych zdarzeń o podłożu kryminalnym, takich jak włamania, rozboje czy gwałty. To proces, na który musimy się przygotować.
Menedżerowie ds. bezpieczeństwa już dziś muszą pracować nad przywróceniem sprawności działania struktur ochrony do poziomu sprzed pandemii.

Tomasz Wojak

Seris Konsalnet Holding

Wyzwania dzisiejszych czasów

Jedną z konsekwencji trwającej za naszą wschodnią granicą wojny jest ogromny, niespotykany do tej pory przepływ imigrantów do naszego kraju. Może on być przyczyną zwiększonego zapotrzebowania na usługi firm ochrony w wielu formach.

Pracownicy ochrony, zabezpieczający budynki klientów, instytucje publiczne, galerie handlowe czy hale sportowe, pełnią często ważne i zróżnicowane funkcje związane nie tylko z zapewnieniem ochrony przed kradzieżami czy dewastacją mienia. Pracownicy ochrony są również odpowiedzialni za sprawną organizację ruchu osób i pojazdów na chronionym terenie, udzielają niezbędnych informacji oraz zapewniają przebywającym tam osobom poczucie bezpieczeństwa, które jest teraz szczególnie ważne.
Szacujemy, że w Polsce ochroną fizyczną zajmuje się 200-tysięczna grupa osób. Ta olbrzymia rzesza ludzi odgrywa zdecydowanie ważną rolę w organizacji porządku i bezpieczeństwa dla przybywających do naszego kraju ludzi szukających schronienia. Jesteśmy również ważnym wsparciem i partnerem państwowych służb mundurowych, które pracują z uchodźcami przybywającymi do Polski. Pomagamy na dworcach, punktach granicznych, środkach transportu, w centrach logistycznych i punktach zbiórek, m.in. dzięki pomocy pracowników ochrony wszystko odbywa się sprawnie i bezpiecznie.
Branża ochrony i bezpieczeństwa jest także otwarta na nowych pracowników z Ukrainy – zapraszamy osoby chętne (kobiety i mężczyzn) do pracy w ochronie i usługach cleaningu. Mamy nadzieję, że pozwoli im to szybciej stanąć na nogi i łatwiej odnaleźć się w nowej rzeczywistości.

Tomasz Olejniczak

Hikvision Poland

Inteligentny system wspomagania decyzji (IDSS)

Potrzeba postępu jest nieodzownym elementem ludzkiej natury. Ulepszamy i kształtujemy rzeczywistość dookoła nas. Odbieramy i przetwarzamy informacje, aby przy podejmowaniu decyzji wybierać najlepsze rozwiązania. Ilość generowanych informacji stale rośnie, dlatego potrzebne są odpowiednie narzędzia modelujące je i przedstawiające w przejrzysty i użyteczny sposób.
Połączone systemy zabezpieczeń (dozoru wizyjnego, kontroli dostępu, sygnalizacji włamania i napadu, sygnalizacji pożarowej) generują duże ilości informacji. Jak w przypadku każdego archiwum, największym wyzwaniem jest ustrukturyzowanie zarejestrowanych danych. Analizowanie danych tylko z jednego systemu przedstawia częściowy obraz sytuacji, co może prowadzić do niewystarczającej oceny zagrożeń i ryzyka, jakie mogą się pojawić w obiekcie.
Całościowa analiza na podstawie informacji z systemów zintegrowanych, dając pełny obraz sytuacji, pozwala dostosować procedury działania do zmieniającego się przeznaczenia pomieszczeń. W systemach zintegrowanych zebrane informacje z wielu systemów bezpieczeństwa tworzą modele danych oparte na zdefiniowanych regułach. W systemie integrującym pomaga w tym zastosowanie reguł logicznych pomiędzy odbieranymi informacjami a funkcjami wykonawczymi systemu. Część reguł jest predefiniowana zgodnie z przepisami prawa.
Celem integracji i zdefiniowanych reguł jest uzyskanie dodatkowych funkcji w istniejącym systemie. Najczęściej wykorzystywaną regułą przy połączeniu systemu CCTV/VSS z dowolnym systemem zabezpieczeń jest wizyjna weryfikacja zdarzenia, a dodatkową funkcją może być automatyczne zabezpieczenie powiązanego ze zdarzeniem materiału wideo przed nadpisaniem. Utworzone reguły zadziałają bez potrzeby wykonywania działań przez obsługę.
Inną funkcją integracji w sytuacji zagrożenia jest przeprowadzenie użytkownika systemu przez przygotowaną procedurę działania. Procedury mogą się różnić w odniesieniu do różnych zagrożeń, dlatego systemy integrujące pozwalają na tworzenie wielu procedur, dostosowując je do potrzeb obiektu, regulacji prawnych i norm bezpieczeństwa. Przygotowane procedury pomagają zoptymalizować reakcję obsługi na każde zagrożenie.
Ważnym elementem systemu zintegrowanego jest również możliwość prezentowania informacji w przyjaznym graficznym interfejsie. Użytkownik systemu może dzięki temu łatwo analizować zgromadzone dane na podstawie np. czasu wystąpienia zdarzeń, typu i źródła zdarzenia, lokalizacji miejsca jego wystąpienia czy korelacji pomiędzy zdarzeniami.
Podsumowując, systemy zintegrowane pozwalają lepiej ocenić każde zagrożenie. Wszystkie zdarzenia ze wszystkich podłączonych systemów są prezentowane w spójnym interfejsie, co skraca czas reakcji obsługi. Wiele zdarzeń dzięki zastosowaniu zdefiniowanych reguł jest obsługiwanych automatycznie przez system, najważniejsze z nich są podane do decyzji użytkownika w postaci przejrzystej procedury działania. Wszystkie zdarzenia i podjęte działania można łatwo przeanalizować w formie graficznej.
Big data zrewolucjonizowało podejście do zarchiwizowanych informacji, systemy integrujące zmieniają nasze podejście do bezpieczeństwa, wprowadzając je na wyższy poziom.

Daniel Kamiński

Smart-i

Konwergencja bezpieczeństwa fizycznego i cybernetycznego

Współczesny trend migracji zabezpieczeń technicznych w kierunku urządzeń sieciowych powoduje, że pod względem ochrony cybernetycznej należy je traktować podobnie jak rozwiązania IT. Można wręcz powiedzieć, że od strony zagrożeń systemy zabezpieczeń przypominają rozwiązania IT/IoT. To wynik cyfrowej transformacji, łączenia systemów w sieci, analizy dostarczanych danych z inteligentnych czujników i w efekcie zdalnego sterowania w zależności od potrzeby.
Nasilenie zagrożeń cybernetycznych dla urządzeń security będzie się pogłębiało. Wystarczy wpisać w przeglądarce hasła „kamera IP" oraz „DDoS", aby uzyskać setki artykułów o podatności kamer różnych producentów. O zgrozo, są tam gotowe przewodniki omawiające, jak przejąć kamerę i wykorzystać jej wbudowaną moc obliczeniową do ataku typu DDoS. Przy przejęciu kilku lub kilkudziesięciu tysięcy kamer moc takiego ataku jest porażająca. Teoretycznie to oczywiste, podobne artykuły dotyczą przejmowania routerów, drukarek, telewizorów i innych urządzeń podłączonych do sieci. Ale w przypadku sprzętu konsumenckiego wydźwięk społeczny nie jest tak duży. Niestety, gdy dotyczy to rozwiązań security lub automatyki przemysłowej wykorzystywanej do sterowania np. torami kolejowymi, wtedy opinia uderza w nas, specjalistów.
Warte uwagi jest również spojrzenie od strony bezpieczeństwa informacji opisane w normie ISO 27001. Widać tam efekt przenikania się kontroli dostępu, ochrony fizycznej, ochrony środowiskowej i ochrony cybernetycznej.
Wszakże podatność systemów teleinformatycznych na zagrożenia nie wynika tylko z powodu ataków wolumetrycznych, klikania na zarażone łącza czy podszywania się pod określone strony. Umożliwia je również fizyczny dostęp do serwerowni, komputera, telefonu, gdy patrzymy na to od strony klienta. Patrząc jednak od strony dostawcy telekomunikacyjnego, będzie to dostęp do studzienek telekomunikacyjnych, wież BTS, central telefonicznych czy data center. Ograniczenie dostępu za pomocą zamków, drzwi antywłamaniowych, czytników kontroli dostępu czy kamery wideo weryfikujące intruza staje się fizyczną ochroną na tyle mocną, że napastnicy wolą wykorzystywać słabości użytkowników, a nie słabości systemów zabezpieczeń.
Dziś jesteśmy świadkami konwergencji bezpieczeństwa fizycznego i cybernetycznego. Nie ma od tego ucieczki. Trzeba mieć świadomość dokonujących się zmian w rozwoju systemów zabezpieczeń technicznych, ich transformacji w kierunku sieciowych systemów teleinformatycznych oraz zagrożeń z tym związanych. Pilnujmy, aby ta transformacja nie przyniosła nam szkód. Szukając przyszłościowych rozwiązań, wybierajmy cyberbezpieczne systemy zabezpieczeń technicznych oraz przestrzegajmy „higieny cyfrowej". Nie korzystajmy z fabrycznych haseł, blokujmy otwarte porty, szyfrujmy komunikację, ograniczmy dostęp do konfiguracji, aktualizujmy oprogramowanie, łączmy się z zabezpieczonych komputerów i telefonów.

Jarosław Sapko

Axis Communications

Niezawodność infrastruktury krytycznej

Infrastruktura krytyczna to bardzo szerokie pojęcie, obejmujące m.in. przemysł energetyczny, gospodarkę wodną, terminale lotnicze, a także serwerownie czy też instytucje finansowe. Rozwiązania wspomagające bezpieczeństwo tych wszystkich obiektów IK będą się różniły, gdyż ich potrzeby są zróżnicowane. Na przykład lotniska czy elektrownie muszą monitorować rozległe tereny zewnętrzne, obiekty typu data center natomiast mają zabezpieczyć stosunkowo niewielkie powierzchnie.
Jednakże podstawowymi celami systemów bezpieczeństwa obiektów IK są ochrona przed wtargnięciem osoby nieuprawnionej na ich teren oraz zapewnienie ciągłości świadczonych usług. Z tego też względu w celu ochrony obiektów infrastruktury krytycznej wykorzystywane są coraz bardziej zaawansowane technologie łączące różne sposoby detekcji i analizy zachowania.
W obiektach strategicznych, oprócz parametrów technicznych urządzeń i systemów zabezpieczających, należy także zwrócić uwagę na ich niezawodność, łatwość integracji z innymi systemami oraz istniejącymi instalacjami, a także na czas wsparcia dla urządzeń, z uwzględnieniem aktualizacji oprogramowania sprzętowego. Z tego też względu, oprócz funkcji urządzeń związanych z zapewnieniem bezpieczeństwa, w systemach dedykowanych infrastrukturze krytycznej powinniśmy zwracać większą uwagę na dodatkowe narzędzia wspierające monitorowanie poszczególnych elementów systemów zabezpieczeń, a także ich codzienną obsługę w celu długotrwałej prawidłowej pracy.

Marcin Walczuk

BCS

Rozwiązania dla obiektów IK

Ostatnie wydarzenia na świecie zdecydowanie nas nie oszczędzają. Gdy już mieliśmy nadzieję, że towarzysząca nam od przeszło dwóch lat pandemia koronawirusa zaczyna odpuszczać i będziemy mogli zacząć wracać do „normalności", za naszą wschodnią granicą wybuchła wojna. To, szczególnie w pierwszych dniach, przełożyło się na kolejki na stacjach benzynowych i brak gotówki w większości bankomatów. Trudno sobie wyobrazić, jak szerzona dezinformacja mogłaby wpłynąć na zachowania ludzi w dłuższym okresie.
Aby nie potęgować uczucia strachu i paniki, niezwykle ważne w takich sytuacjach jest zagwarantowanie dostępu do prądu, bieżącej wody i gazu oraz zachowanie ciągłości dostaw i niezakłóconej łączności. Infrastruktura krytyczna – bo o niej mowa – jest niezbędna do prawidłowego i niezachwianego funkcjonowania państwa. Utrudniony dostęp do jej usług może skutkować pogłębiającą się paniką wśród ludności cywilnej, a w konsekwencji do destabilizacji gospodarczej i społecznej.
Obiekty IK są w dużej mierze własnością prywatnych przedsiębiorstw i to one powinny zapewnić ich bezpieczeństwo i niezakłócone dostawy. Zarządzający nie powinni szczędzić wydatków na systemy zabezpieczeń. Czy to będzie telewizja dozorowa, system alarmowy, kontroli dostępu, czy ppoż., liczy się zapewnienie bezpieczeństwa na odpowiednio wysokim poziomie, a nie oszczędności.
Nie wolno zapominać o osobach, które ten sprzęt mają obsługiwać. Muszą być odpowiednio przeszkolone, by móc w pełni wykorzystać możliwości, jakie dają elektroniczne systemy zabezpieczeń, i we właściwy sposób reagować na sytuacje kryzysowe. Konieczne jest stosowanie się do już istniejących procedur bezpieczeństwa oraz w razie potrzeby tworzenie nowych, które będą przygotowywać na nieuwzględnione do tej pory zagrożenia.
BCS proponuje rozwiązania dla każdego sektora i obiektów wchodzących

w skład infrastruktury krytycznej – zabezpieczenie dużych zakładów produkcyjnych, rozległych linii przesyłowych, gazociągów czy mniejszych ważnych placówek, takich jak banki lub urzędy. Korzystając z naszych produktów IP, można tworzyć rozproszone systemu CCTV obsługiwane z centralnej stacji monitoringu wizyjnego za pomocą stale rozwijanej aplikacji BCS Manager. Kamery termowizyjne, kamery i rejestratory korzystające z zaawansowanej analizy wideo pomogą szybko wykryć zagrożenie, którego nie widać gołym okiem, lub reagować jedynie na sytuacje, które takiej reakcji wymagają. Nie tylko dostarczamy rozwiązania techniczne najwyższej jakości, ale dbamy również o rozwój korzystających z nich osób. Dlatego prowadzimy szkolenia, podczas których przybliżamy wszystkie oferowane przez nas produkty.

Jakub Łukasik

Axis Communications

Działania związane z wojną w Ukrainie

W odpowiedzi na obecną sytuację związaną z wojną w Ukrainie szwedzka firma Axis Communications AB podjęła decyzję o zaprzestaniu wysyłania wszelkich produktów i usług do Rosji i Białorusi z dniem 24 lutego.
W Ukrainie firma nie zatrudnia pracowników, natomiast utrzymuje długotrwałe relacje biznesowe, np. z partnerami i dystrybutorami, którzy są obsługiwani z naszego biura w Polsce i krajach bałtyckich. Uważnie śledzimy rozwój sytuacji i podjęliśmy decyzję, by od 25 lutego wstrzymać wysyłkę towarów. Nadal zapewniamy wsparcie naszym klientom i partnerom Axis w Ukrainie z biura w Warszawie.
Gdy tylko będziemy mieli dodatkowe informacje lub zmiany decyzji, którymi będziemy mogli się podzielić, przekażemy je zainteresowanym.
Nie widzimy żadnych sygnałów, aby obecna sytuacja mogła mieć wpływ na polski rynek security. Kontynuujemy nasze działania zgodnie z przyjętą strategią.

PAWEŁ TROJAK

AxxonSoft Europe

Wpływ wojny na polski rynek security

Wojna w Ukrainie zasadniczo nie wpłynęła na naszą codzienną działalność, wszystkie aktywności i sprzedaż odbywają się jak dotychczas. Zaangażowaliśmy się w akcje pomocowe na rzecz uchodźców i to nieco zmieniło naszą codzienność. Odczuwalny jest też pewien niepokój, napięcie.
Wojna pobudziła także naszą konkurencję do propagowania nieprawdziwych informacji, jakoby AxxonSoft był firmą rosyjską. Od 2021 r. większościowym udziałowcem jest Streamlabs Corporation, beneficjentem rzeczywistym jest obywatel Tajwanu. Rozwój produktu prowadzony jest w krajach UE (Irlandia, Litwa, Polska, Estonia), Australii, Gruzji, Turcji i USA.
Działając wyłącznie na terytorium UE, nie mamy kontaktów handlowych z Rosją. Natomiast jesteśmy dumni, że AxxonSoft już w drugim dniu wojny zajął bardzo zdecydowane stanowisko, domagając się pokoju i poszanowania integralności terytorialnej Ukrainy.
Myślę, że jest jeszcze za wcześnie, by mówić o wpływie wojny na polski rynek security. Nie sądzę jednak, aby czekały nas bardzo głębokie zmiany. Oczywiście wiele będzie zależeć od tego, jak szybko i w jaki sposób konflikt zostanie rozwiązany, a także czy i do jakich przemian dojdzie w Rosji po wojnie. Dzisiaj (początek kwietnia) możemy tylko snuć hipotezy w kilku wariantach.

Anna Twardowska

Nedap Security Management

Wzrosło ryzyko cyberataków

Obecna sytuacja związana z wojną w Ukrainie powinna skłaniać osoby zajmujące się bezpieczeństwem w firmach do przyjrzenia się swoim organizacjom pod względem ryzyka, które pojawia się także w zakresie cyberataków na infrastrukturę systemów zabezpieczeń technicznych. W ostatnim miesiącu widoczna była wzmożona liczba ataków w cyberprzestrzeni. Obiekty infrastruktury krytycznej i centra danych są na nie szczególnie narażone. W związku z obowiązywaniem trzeciego stopnia alarmowego CRP (CHARLIE-CRP) na terytorium całego kraju wiele organizacji dokonało weryfikacji polityki bezpieczeństwa i procedur business continuity. Teraz poprzeczka wymagań została podniesiona bardzo wysoko.
Data centers muszą zapewniać swoim klientom bezpieczeństwo danych i aplikacji oraz ciągłość działania, zwiększać wydajność i niezawodność systemów, przy jednoczesnym minimalizowaniu kosztów operacyjnych i inwestycyjnych. Dlatego jest tak istotne, by były budowane od podstaw zgodnie z najwyższymi standardami. Już sam wybór ich lokalizacji jest ważny, są to miejsca położone z dala od terenów narażonych na powodzie, centrów miejskich (ryzyko rozprzestrzeniania się pożarów), poza ruchem lotniczym (katastrofy lotnicze). Co ważne, powinny mieć dostęp do dwóch niezależnych linii energetycznych. A to tylko fundamenty, na których budowane są kolejne systemy bezpieczeństwa.
Pomimo stosowanych środków bezpieczeństwa centra danych są szczególnie narażone nie tylko na ataki hackerskie, ale także na utratę danych (i tym samym utratę zaufania klientów). Dlatego powinny przywiązywać dużą wagę również do fizycznej ochrony swoich obiektów. Najnowsze zabezpieczenia serwerów oraz infrastruktury sieciowej zapewniają bezpieczeństwo danych, ale to infrastruktura zabezpieczeń technicznych chroni fizycznie dostęp do serwerów i tym samym do danych w miejscach, w których są one gromadzone.
Bezpieczeństwo fizyczne i najwyższy poziom jakości systemów kontroli dostępu, SSWiN oraz dozoru wizyjnego są kluczowymi elementami bezpieczeństwa centrów danych.

Infrastruktura krytyczna

w czasach turbulencji

Teza, że infrastruktura krytyczna jest miejscem mającym bezpośredni wpływ na życie całego społeczeństwa, a jednocześnie ogniskuje się w nim wiele zagrożeń, w obliczu wydarzeń z ostatnich tygodni wydaje się płaska, by nie rzec banalna. Świat zmienił się diametralnie – to także już truizm. Lecz to już jest za nami. Co więc nas czeka? Jak podejść do nowych (i czy na pewno nowych) wyzwań? To są pytania, z którymi mierzymy się codziennie.

Jacek Grzechowiak

TO, CO JEST NASZYM PRZECIWNIKIEM, A KTO LUB CO ZASOBEM KRYTYCZNYM?

Dotychczasowe spojrzenie na zagrożenia infrastruktury krytycznej koncentrowało się na incydentach i ich konsekwencjach dla obiektu lub procesów w nim zachodzących, a tym samym na skutkach zaburzenia tych procesów dla ludności. Podejście takie pomijało (bądź uwzględniało w niewielkim stopniu) oddziaływanie incydentu, jaki wydarzył się w obiekcie niebędącym infrastrukturą krytyczną, na procesy zachodzące w obiektach IK. Brzmi to trochę zawile, więc warto przedstawić na przykładach.

Kiedy w październiku 2017 r. w galerii handlowej w Stalowej Woli doszło do ataku nożownika, słowo „krytyczny" odnosiło się praktycznie wyłącznie do stanu zdrowia ofiar tego zamachu. Niewiele osób zwróciło uwagę na to, że do zabezpieczenia tego incydentu skierowano wszystkie karetki pogotowia z dwóch powiatów (sic!). Tym samym w dwóch powiatach osiągnięto krytyczny stan w elemencie infrastruktury krytycznej, jakim bez wątpienia jest system ratownictwa medycznego. Każdy zawał serca, każdy udar, każde inne schorzenie wymagające szybkiej interwencji zespołu medycznego stały się problemem poważniejszym. A przecież incydent miał miejsce w obiekcie nienależącym do IK...

Incydent jednak wcale nie musi być tak drastyczny, jak w Stalowej Woli, aby oddziaływać destrukcyjnie na „usługę krytyczną", jaką jest bezpieczeństwo publiczne. Przykładem jest bójka wielu osób w jednej z poznańskich galerii handlowych, która spowodowała konieczność skierowania tam aż 11 radiowozów, przez co znaczna część Poznania została pozbawiona patroli policji. Złodzieje z pewnością mieli łzej...

Na szczęście ani w jednym, ani w drugim przypadku nic drastycznego się nie wydarzyło.

Ale jeśli przypomnimy sobie, że *Ustawa o zarządzaniu kryzysowym* pod pojęciem infrastruktury krytycznej rozumie m.in. usługi kluczowe dla obywateli oraz służące zapewnieniu sprawnego funkcjonowania przedsiębiorców, zdamy sobie sprawę, że każdy z tych przykładów był tak naprawdę ingerencją w infrastrukturę krytyczną. To zaś prowadzi do wniosku, że incydent wcale nie musi dotyczyć obiektu IK, aby jego skutki oddziaływały negatywnie na infrastrukturę krytyczną.

Czas pandemii pokazał drugie oblicze tego problemu, przyniósł bowiem potrzebę szybkiej reakcji, w dodatku reakcji na zagrożenia praktycznie wcześniej nieznane, bo *...pojawił się wróg niewidzialny, niewyczuwalny i bardzo często niedający żadnych ostrzeżeń wstępnych. Wróg znany w wąskiej dziedzinie medycyny, ale praktycznie niemal nieznany w komercyjnej ochronie. Wróg nietolerujący bylejakości. Wymagający zmiany sposobu postrzegania rzeczywistości...*[1]. Nasze postrzeganie rzeczywistości musiało się zmienić w trybie nagłym – i to się stało. Pracownicy ochrony podjęli działania w zakresie prewencji pandemicznej niemal „z marszu". Były potknięcia i problemy, ale per saldo udało się rozwijać nie tylko konkretne działania na różnym, najczęściej wysokim poziomie efektywności. Zyskano przy tym także doświadczenie w szybkim i rozsądnym, a nade wszystko efektywnym rozwiązywaniu problemów wcześniej nieznanych, a tym samym niezdiagnozowanych.

To cenna lekcja, bo dziś ochrona musi się zmierzyć z kolejnymi zagrożeniami, które wcale nie muszą być wymierzone w obiekty IK, aby przynieść konsekwencje w postaci zaburzenia usług krytycznych. Podstawy do reagowania w skrajnych sytuacjach są, działają i wygląda na to, że jest to efektywne.

(RE)DEFINICJA IK, CZYLI NASZEGO POLA WALKI

Życie niesie niestety nowe wyzwania, które najczęściej wymagają nieszablonowego spojrzenia zarówno na spectrum zagrożeń, jak i kierunki oraz sposoby ich oddziaływania. Musimy więc kolejny raz przeanalizować, skąd, kiedy i w jaki sposób mogą się one pojawić oraz co, gdzie i jak mamy wtedy robić. Powszechnie wiadomo, że mamy w naszym kraju obiekty podlegające obowiązkowej ochronie, co nie oznacza automatycznie, że muszą stanowić część infrastruktury krytycznej. Obiekt nie musi nawet należeć do tej kategorii, aby incydent, do którego w nim dojdzie, dotyczył usług krytycznych. To zaś wymaga dużo szerszego spojrzenia na bezpieczeństwo usług krytycznych i wzięcia pod uwagę zagrożeń dla nawet niewielkich obiektów, z pozoru nienarażonych na żadne szczególne zagrożenia, które w określonych uwarunkowaniach mogą stać się ważnym celem działań organizacji przestępczych, a nawet służb obcych państw.

Siłą rzeczy – a dziś, jak nigdy wcześniej – musimy uwzględnić aktualną sytuację geopolityczną, w jakiej znaleźliśmy się wraz z rozpoczęciem agresji Rosji na Ukrainę. Groźna sytuacja powinna skłaniać nas do analizy zagrożeń wynikających z agresywnej polityki Rosji, wymagając od wszystkich bardziej wnikliwego spojrzenia na bezpieczeństwo obiektów nie tylko ponadprzeciętnie narażonych na zagrożenia wynikające ze „standardowych" uwarunkowań politycznych. Uwarunkowania polityczne mogą bowiem sprawić, że obiekt zaliczany do kategorii „zwykłych" stanie się całkiem „niezwykły" ze względu na jego profil produkcji, która obecnie jest wysyłana masowo do Ukrainy.

Czy to musi być od razu broń i amunicja? To oczywiście z pewnością będzie asortyment szczególnie ryzykowny, ale po pierwsze obiekty te już obecnie podlegają szczególnej ochronie, po drugie jest przecież cała gama wyrobów o niskim zdawałoby się profilu ryzyka.

„Standardowe" konserwy mięsne nagle stały się żywnością MRE *(Meal, Ready-to-Eat)*. Czy wcześniej nie były tą kategorią żywności? Oczywiście że były, ale... Standardowe okulary ochronne obecne w każdym zakładzie przemysłowym i z tego powodu traktowane jak coś prozaicznego, nagle stały się towarem pierwszej potrzeby walczącej armii. Jeśli mają jeszcze powłokę chroniącą przed promieniowaniem laserowym, są już zasobem wysoce pożądanym, dającym żołnierzom je posiadającym odpowiednią przewagę. A skoro tak, takie okulary z łatwością mogą stać się celem agresywnych działań, jakich dotychczas nie doświadczali ich producenci.
Kamizelki kuloodporne to oczywistość, ale już cordura (rodzaj tkanin wysoce odpornych na przetarcia), stazy (opaski) taktyczne czy baterie nie są tak traktowane, a przecież produkuje się je w obiektach niepodlegających szczególnej ochronie – jednak dziś są masowo dostarczane armii ukraińskiej. Zmiana ich przeznaczenia i gwałtowny wzrost zapotrzebowania, wreszcie potencjalne skutki braku tego asortymentu sprawiają, że zaczyna się on stawać zasobem jak najbardziej krytycznym. Jego brak może prowadzić do zaburzeń funkcjonowania całego społeczeństwa lub dużej jego części, do turbulencji w funkcjonowaniu systemu ratownictwa, czyli wchodzimy ewidentnie na pole zarządzania kryzysowego, a więc i infrastruktury krytycznej.

Przykładem incydentu, który powinien skłaniać do refleksji, jest przypadek składu amunicji w czeskiej wiosce Vrbětice. Ta mała miejscowość położona na pograniczu czesko-słowackim, zamieszkana przez 300–400 osób, w roku 2014 stała się miejscem jednego z najbardziej tajemniczych incydentów ostatnich lat. W obiekcie należącym do prywatnej firmy handlującej bronią i chronionym przez prywatną agencję ochrony doszło do sporej liczby incydentów, w tym dwu potężnych eksplozji rozrzucających odłamki w promieniu kilku kilometrów. Jak donoszą media, ślady prowadzą do rosyjskich wojskowych służb specjalnych. Podłożem tych incydentów miały być właśnie broń i środki pola walki, które z tego miejsca miały zostać przetransportowane do Ukrainy[2].
Jak więc widać, jest sporo argumentów, by spojrzeć na swój obiekt przez pryzmat jego krytycznego znaczenia. I to nie tylko w aspekcie bezpieczeństwa i obronności Polski, ale także w kontekście wsparcia obronności Ukrainy. Ten czynnik dziś może być szczególnie ważny. Bardzo

Sztywne podejście i zamknięty katalog obiektów stanowiących infrastrukturę krytyczną zdaje się właśnie odchodzić do lamusa

szybko może się okazać, że nasz obiekt, który nie należy do infrastruktury krytycznej, a nawet nie podlega obowiązkowej ochronie, ma wszelkie atrybuty do uznania go za jej część. Dlatego też celowe jest ponowne przeprowadzenie analizy zagrożeń w chronionych obiektach z wykorzystaniem narzędzi, które z pozoru nie są przeznaczone do „zwykłych" obiektów.
Przykładem takiego narzędzia jest metodyka Evil Done[3], powszechnie uważana za narzędzie dedykowane zagrożeniom terrorystycznym i obiektom szczególnie na nie podatnym. Ma ona wiele walorów pozwalających na wielowskaźnikowe zbadanie podatności obiektu i kontekstu, w jakim on funkcjonuje, a tym samym umożliwia bardziej wnikliwe spojrzenie na nasz obiekt i zagrożenia, jakim on podlega. Akty sabotażu nawet w obiektach niepowodujących zagrożeń wynikających z poważnej awarii przemysłowej (seveso) są w stanie wygenerować ryzyko innego rodzaju, jak choćby blokada drogi czy linii kolejowej, bezpośrednie czy pośrednie uszkodzenia sieci elektro-energetycznej, gazowej, wodociągowej. Konieczność odcięcia dostaw energii, gazu czy wody może mieć negatywne konsekwencje dla obiektów sąsiadujących, prowadząc do konieczności awaryjnego wstrzymania operacji (szczególnie produkcyjnych). Dlatego dotychczasowe postrzeganie bezpieczeństwa ukierunkowane na bezpieczeństwo zasobów chronionych, a zwłaszcza krytycznych w tradycyjnym rozumieniu, musi zostać zmienione. Trzeba zacząć myśleć w kategoriach obiektów i zasobów krytycznych w kontekście konkretnej sytuacji, która będzie zmieniała priorytety. Obecne sztywne podejście i nieco „zamknięty" katalog obiektów stanowiących infrastrukturę krytyczną zdaje się właśnie odchodzić do lamusa.

Wśród tych obiektów i procesów – podobnie jak w czasie pandemii – ważną rolę odgrywa logistyka. Obserwowany obecnie proces wsparcia Ukrainy przybrał wręcz niesamowite rozmiary. Liczba zaangażowanych w pomoc osób, wolumeny żywności, odzieży, środków medycznych są tak duże, że jeszcze niedawno były trudne do wyobrażenia. Bez logistyki więc ani rusz. A skoro jest to miejsce tak ważne dla nas i dla Ukrainy, to... dla przeciwników jest ważne dokładnie tak samo. W ten sposób logistyka staje się ewidentnie infrastrukturą krytyczną.

WŁĄCZMY ELASTYCZNOŚĆ MYŚLENIA

Nasze regulacje prawne opisują rodzaje obiektów IK, ale dynamicznie pojawiły się całe branże, których rola co do meritum nie zmieniła się, natomiast znaczenie – na razie jedynie dla Ukrainy – zmieniło się radykalnie. To musi skłaniać do refleksji, do poważnego rozważania, czy „sztywny" katalog ma wciąż rację bytu. Historia pokazuje, że każdy kryzys (a konflikt zbrojny jest niewątpliwie kryzysem) przynosi nowe rozwiązania oraz przewartościowuje dotychczasowe procedury i modele postępowania.
Jedną z potencjalnych tego konsekwencji wydaje się większa elastyczność w definiowaniu IK. Przyporządkowanie obiektu do tej kategorii nie powinno być sztywne, ale uzależnione od kontekstu, sytuacji, w jakiej znajduje się zarówno państwo, jak i obiekt. Unikalna produkcja może bowiem być w polu zainteresowań organizacji terrorystycznych czy służb specjalnych w kontekście dostaw tych produktów do nawet odległego państwa. I wtedy zagrożenie, mające korzenie gdzieś daleko, zmaterializuje się u nas, choć nasze wskaźniki bezpieczeństwa niczego takiego nie sygnalizowałyby. Przypadek składu amunicji we Vrbětičach jest właśnie tego przykładem. A jako że obecne wsparcie Ukrainy jest ekstremalnie szerokie, jeśli chodzi o asortyment, to zagrożenia również znacznie się rozszerzyły, obejmując dużą część naszej gospodarki.

NASZA ARMIA, CZYLI SZUKAMY UZBROJENIA

Dużą część zjawisk mogących skutkować incydentem w bezpieczeństwie mogą ujawniać pracownicy ochrony. I w praktyce tak się dzieje. Jednak dziś wchodzimy na zupełnie inny poziom – poziom infiltracji i sabotażu jako zagrożeń realnych. Co więcej, zagrożeń o rosnącym ryzyku wystąpienia. Tak jak w przypadku pandemii, niezbędna jest aktywna odpowiedź na wszystkich etapach zarządzania bezpieczeństwem i przy dużym skupieniu uwagi na zdolnościach personelu ochronnego, jego potencjale intelektualnym, wreszcie na jego świadomości. Dzisiaj np. wyciekający olej silnikowy czy jazda z niezabezpieczonym lub źle zabezpieczonym ładunkiem nie muszą świadczyć jedynie o lekceważeniu przepisów BHP. A zaobserwowany osobnik wyposażony w butle gazowe, palniki oraz inne akcesoria potrzebne do demontażu rurociągu[4] wcale nie musi być złodziejem złomu. Jeszcze kilka tygodni temu tak byśmy go postrzegali, dziś należy poszukać także innych możliwych znaczeń takiego symptomu, każdy może bowiem wskazywać na przygotowania lub dokonywanie sabotażu.
Czy wcześniej nie były ich symptomami? Oczywiście mogły być, tyle że dzisiaj zagrożenie sabotażem jest już na zupełnie innym poziomie. Podobnie jak infrastruktura krytyczna obejmująca znacznie szersze obszary, niż określa to definicja ustawowa.

Wchodzimy dziś na inny poziom incydentów bezpieczeństwa – poziom infiltracji i sabotażu jako zagrożeń realnych, o rosnącym ryzyku wystąpienia

Obecnie rozmowa z nieznajomym o naszych obowiązkach w zakresie wykonywanej usługi ochrony powinna włączać czerwone światło ostrzegawcze. Zresztą tak jak wcześniej, jednak teraz wypytywanie jest prowadzone w sposób bardziej wyrafinowany. Pracownik słabo przeszkolony nie tylko nie ochroni informacji wrażliwych, ale nawet nie zauważy, że był poddany indagacji. Być może tak właśnie było we Vrbětičach.
Przypomina mi się jedna z konferencji w Akademii Leona Koźmińskiego, podczas której trzy studentki prawa przedstawiły wyniki badań: *Ochrona pod lupą. Czego nie wiedzą klienci centrów handlowych – taśmy z wideokamer, zarys kompetencji pracownika ochrony obiektu, szefowie agencji*[5], referując uczestnikom konferencji, do jakich informacji dotarły, i to bez nadmiernego wysiłku. A były to informacje naprawdę wrażliwe. Jesteśmy 7 lat po tej konferencji. I powiem wprost: branża te siedem lat zmarnowała.

LITERATURA

1 J. Grzechowiak „IK w czasie pandemii, czyli stara atmosfera w nowym klimacie…", https://aspolska.pl/ik-w-czasie-pandemii-czyli-stara-atmosfera-w-nowym-klimacie/
2 https://cs.wikipedia.org/wiki/V%C3%BDbuchy_muni%C4%8Dn%C3%ADch_sklad%C5%AF_ve_Vrb%C4%9Btic%C3%ADch
3 A. Tomalska „Ewaluacja celów ataku terrorystycznego w przestrzeni publicznej przy zastosowaniu modelu EVIL DONE", www.abw.gov.pl [dostęp 16.08.2021].
4 https://tychy.policja.gov.pl/k27/informacje/wiadomosci/65404,Rurociag-na-zlom.html [dostęp 05.03.2021]
5 https://docplayer.pl/17796734-Sprawozdanie-z-ogolnopolskiej-konferencji-naukowej-prywatna-ochrona-bezpieczenstwa.html

JACEK GRZECHOWIAK

Menedżer ryzyka i bezpieczeństwa. Absolwent WAT, studiów podyplomowych w SGH i Akademii L. Koźmińskiego. Gościnnie wykłada na uczelniach wyższych. W przeszłości związany z grupami Securitas, Avon i Celsa, w których zarządzał bezpieczeństwem i ryzykiem. Obecnie pełni funkcję pełnomocnika Zarządu ds. Ryzyka i Bezpieczeństwa w TAURUS OCHRONA.

Bezpieczne kopalnie

w odpowiedzi na wyzwania współczesnego górnictwa

Obiekty infrastruktury krytycznej mają ogromne znaczenie dla gospodarki, wymagają zatem odpowiedniej ochrony. Zabezpieczenia powinny mieć charakter kompleksowy i obejmować zasięgiem zarówno zewnętrzne otoczenie obiektu, jak i jego wnętrze – tak, by skutecznie zapobiegać wtargnięciom na teren obiektu osób niepowołanych oraz zapewnić odpowiedni poziom bezpieczeństwa pracownikom. Aby to osiągnąć, warto postawić na zintegrowany system, składający się z kamer monitoringu, głośników i urządzeń kontroli dostępu.

Jednym ze specyficznych obiektów segmentu infrastruktury krytycznej są kopalnie wraz z całym procesem wydobywczym. Globalna produkcja górnicza osiąga właśnie najwyższe poziomy w historii – w 2018 r. wynosiła ona ponad 17,7 mld ton. Wraz z rozwojem górnictwa rośnie również zapotrzebowanie na wdrażanie rozwiązań, które pomogą w większym stopniu zadbać o bezpieczeństwo pracowników kopalni. Z pomocą przychodzi technologia, która nie tylko minimalizuje różne ryzyka, ale także pozwala podnieść efektywność operacyjną.

Jeśli chodzi o niełatwe warunki pracy, niewiele jest trudniejszych zawodów niż górnictwo. Ponadto w tak wysoce regulowanym sektorze każdy incydent, nawet mały, zawsze musi zostać dokładnie zbadany. Może to powodować częściowe wstrzymanie działalności kopalni, a co za tym idzie – mieć wpływ na jej wyniki finansowe. Aby uniknąć niepotrzebnych kosztów, coraz więcej zakładów wydobywczych decyduje się korzystać z rozwiązań dozoru wizyjnego.

PRACA W PYLE I CIEMNOŚCI

Wyobrażenie kopalni przez laika zwykle przedstawia labirynt słabo oświetlonych tuneli wydrążonych głęboko pod ziemią. Chociaż nie wszystkie kopalnie rzeczywiście funkcjonują pod powierzchnią, prawdą jest, że zła widoczność jest powszechnym wyzwaniem. Najnowsze kamery z oświetlaczami podczerwieni potrafią mu sprostać, umożliwiają bowiem przechwytywanie obrazów w całkowitej ciemności. Pomocne mogą być także kamery termowizyjne, które stanowią wsparcie, kiedy widoczność jest ograniczona. Urządzenia o wzmocnionej konstrukcji oraz te, w których zastosowano obudowy ze stali nierdzewnej, wytrzymują zarówno rygory samych operacji górniczych, jak i trudne warunki środowiska pracy.

W obiektach górniczych na widoczność wpływa nie tylko ilość światła. Nieuniknionym produktem ubocznym procesu wydobycia jest pył – to on bardzo często utrudnia pracę górników. Monitorowanie pyłu jest ważne ze względu na zdrowie i życie nie tylko pracowników kopalni, ale także społeczności lokalnej, może bowiem się przedostać poza teren zakładu. Współczesne kamery wyposażone w aplikacje analityczne oparte na głębokim uczeniu oraz termowizję mogą wykrywać i monitorować różnorodne obiekty i zagrożenia, w tym chmury pyłu, umożliwiając podjęcie działań naprawczych lub proaktywne ostrzeganie okolicznych mieszkańców i pracowników.

ZARZĄDZANIE MASZYNAMI

Zagrożenia bezpieczeństwa w górnictwie stanowią również maszyny stosowane w branży wydobywczej. Koparki górnicze – używane do wydobywania dużych ilości ziemi i skał – są ogromne. Same łyżki ważące do 10 tys. ton mogą mieć pojemność do 130 metrów sześciennych. Podobnie ciężarówki używane do transportu ziemi, skał i minerałów w ramach operacji wydobywczych po załadowaniu mogą ważyć ponad 500 ton, równocześnie poruszając się z prędkością 60 km/h. Ryzyko związane z obsługą tak ogromnych maszyn jest oczywiste. Zagrożenia te dotyczą zarówno bezpieczeństwa pracowników kopalni, jak i skutków ewentualnych awarii. W związku z tym coraz powszechniejsze jest stosowanie kamer pokładowych w celu zapewnienia operatorom i kierowcom bezpieczeństwa.

– Oprócz kamer wizyjnych często instalowane są także kamery pokładowe wyposażone w termowizję. Mogą być nieocenioną pomocą, gdy widoczność ogranicza pył. Dodatkowo można korzystać z kamer nasobnych, które pracownicy noszą na ubraniu roboczym. Często pomagają one ustalić sekwencję wydarzeń, a nagrania wykorzystuje się np. przy szkoleniach – podkreśla Marek Białek z Axis Communications.

INNOWACJE TECHNOLOGICZNE W KOPALNI

W ostatnich latach nieustannie rosną możliwości analityki wizyjnej. Oprócz klasycznego nagrywania obrazu współczesne inteligentne kamery mogą także samodzielnie rozpoznawać obiekty. W górnictwie można wykorzystać funkcje analityczne, aby np. upewnić się, że pracownicy włożyli odpowiedni sprzęt ochrony osobistej przed wejściem do kopalni lub poruszaniem się po terenie. Zaawansowane aplikacje wspomagają też m.in. liczenie osób. Pozwala to nieustannie monitorować liczbę pracowników znajdujących się na terenie obiektu, a w czasach pandemii umożliwia dodatkowo spełnianie norm związanych z koniecznym dystansem społecznym.

Innowacyjność systemów wizyjnych można wykorzystać jeszcze na jednej płaszczyźnie: wydajności operacyjnej. Wiadomo, że przerwy w pracy kopalni mogą być bardzo kosztowne. Lepiej zatem zapobiegać, niż leczyć i proaktywnie konserwować sprzęt. Przykładowo, kamery umieszczone w kluczowych punktach wzdłuż przenośników taśmowych mogą być połączone z czujnikami obciążenia, ostrzegając operatorów, gdy poziom obciążenia przekracza wyznaczone limity. Podobnie kamery do odczytu temperatury mogą być używane do monitorowania np. kabli elektrycznych i podstacji, przekazując wczesne ostrzeżenia o problemach, a nawet automatycznie wyłączając system przed wystąpieniem katastrofalnej awarii czy pożaru.

BEZPIECZEŃSTWO PRZEDE WSZYSTKIM

Nie wolno zapominać o najbardziej znanej funkcji kamer VSS, czyli o dozorze/monitoringu wizyjnym. Kopalnie, jako infrastruktura krytyczna, powinny być objęte zintegrowanym systemem kamer, które mają możliwość obracania i zbliżenia, tak by z łatwością identyfikować potencjalne zagrożenia, przy jednoczesnej minimalizacji liczby fałszywych alarmów.

Przykładowo, niedawno zamknięte szyby kopalniane są szczególnie atrakcyjne dla przestępców, ponieważ nadal może się w nich znajdować wiele cennych maszyn wykorzystywanych w poprzednich operacjach wydobywczych. Do ostrzegania operatorów o włamaniu do takich obiektów można zastosować technologie dozoru wizyjnego oraz ochrony obwodowej. Wtargnięcie intruza na chroniony obszar, zweryfikowane obrazem z kamer monitoringu, wyzwoli automatyczny alarm dźwiękowy, który pozwoli skutecznie go odstraszyć.

Kopalnie to środowiska szczególnie wymagające, realnie zagrożone wystąpieniem sytuacji narażającej ludzi na utratę życia, m.in. wzrostem temperatury i wybuchem nagromadzonych gazów. W miejscach o wysokim prawdopodobieństwie tego ryzyka można instalować tylko kamery z ochroną przeciwwybuchową (tzw. iskrobezpieczne). W połączeniu z technologią analityczną i monitoringiem temperatury urządzenia te są nie tylko klasycznymi systemami monitoringu, ale także inteligentnymi narzędziami stanowiącymi wsparcie w podejmowaniu działań związanych z bezpieczeństwem.

– Warto zauważyć, że wiele funkcji nowoczesnych kamer monitoringu wideo, w połączeniu z analizą termiczną i głębokim uczeniem, odpowiada na różnorodne wyzwania związane z sektorem wydobywczym. Korzyści zastosowania zintegrowanych systemów są dostrzegane przez coraz większą liczbę zarządzających kopalniami na całym świecie – konkluduje Marek Białek z Axis Communications.

AXIS COMMUNICATIONS POLAND

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

Zintegrowany system ochrony klasy PSIM w infrastrukturze krytycznej

Leszek Schmidt

Elektrownie konwencjonalne, gazowe, wiatrowe, wodne, farmy fotowoltaiczne – w tak strategicznych obiektach wymagane są wysokiej jakości systemy, które w sposób niezawodny podnoszą efektywność procesów produkcyjnych, zapewniają bezpieczeństwo, umożliwią natychmiastową reakcję w sytuacjach awaryjnych i dostarczą jednoznaczne dane do oceny sytuacji o zdarzeniu lub zagrożeniu. Każde wdrożenie musi być dopasowane do szczególnych warunków charakterystycznych dla tej branży.

Dobrze działająca infrastruktura techniczna ma wpływ na bezpieczeństwo i zapewnienie odpowiedniego standardu życia. Elementy infrastruktury niezbędne do minimalnego funkcjonowania gospodarki i państwa określa się mianem infrastruktury krytycznej, którą bez wątpienia jest energetyczna infrastruktura krytyczna. Aby podnieść bezpieczeństwo i niezawodność obiektów energetycznych, C&C Partners na bazie wieloletniego doświadczenia przygotowało dedykowane modułowe rozwiązanie, biorąc pod uwagę obowiązujące przepisy, specyficzne warunki oraz wymagania klientów.

TECHNIKA VS. CZŁOWIEK

Rozwój techniki sprawia, że systemy informatyczne integrujące łączność i zarządzanie danymi, połączone z procedurami zapewniają efektywniejszy nadzór nad bezpieczeństwem obiektów niż człowiek pozbawiony tych narzędzi. Potwierdzają to wdrożone na całym świecie rozwiązania WinGuard – oprogramowania klasy PSIM+ *(Physical Security Information Management).*
W swych założeniach systemy zarządzania bezpieczeństwem obiektów klasy PSIM+ nie miały wyręczać stacjonarnych pracowników ochrony, lecz ich wspierać. Jednak po latach rozwoju i poszerzania funkcjonalności systemy zintegrowane w praktyce zapewniają obiektom skuteczny monitoring i realizację założeń procesowych przez jednego operatora zdalnie, bez konieczności dozorowania wszystkich obiektów przez osobę na miejscu.
Producenci zintegrowanych systemów bezpieczeństwa klasy PSIM+ rozwijają wyjściowe założenia i wciąż udoskonalają swoje rozwiązania, wprowadzając sztuczną inteligencję (AI) do systemów zarządzania kryzysowego i wsparcia pracy operatora. Celem takiego działania jest coraz wyższy poziom bezpieczeństwa obiektów.

OBNIŻENIE KOSZTÓW ZARZĄDZANIA OBIEKTAMI

Skuteczniejszą ochronę umożliwia obecnie centralizacja zarządzania informacjami pozyskiwanymi ze wszystkich systemów zabezpieczeń technicznych zainstalowanych w chronionych obiektach. Nowoczesna technologia monitoringu wizyjnego z funkcją analizy i automatycznej detekcji niepożądanych zdarzeń podwyższa skuteczność zdalnej ochrony obiektu i zarazem umożliwia natychmiastową reakcję operatorów systemu pracujących w trybie 24/7/365.

Możliwość ograniczenia kosztów ochrony, których zdecydowaną większość pochłaniała dotychczas stała obecność w obiektach wyspecjalizowanych pracowników ochrony, jest odbierana jako duża zaleta systemu klasy PSIM+.

ELASTYCZNE NARZĘDZIE

Sam system WinGuard jest oprogramowaniem służącym do zarządzania procesem bezpieczeństwa. Dzięki technologicznej otwartości cechuje się zdolnością integrowania dotychczas użytkowanych w obiekcie technologii bezpieczeństwa, a także systemów przemysłowych, automatyki budynkowej czy komunikacji w jeden system bezpieczeństwa.

PROCES INWESTYCYJNY

WinGuard jest rozwiązaniem niepowiązanym z żadnym producentem sprzętu, co umożliwia jego szybkie wdrożenie w istniejącej infrastrukturze serwerowej. PSIM to aplikacja skalowana, co oznacza, że system może się rozwijać zgodnie z możliwościami budżetowymi jednostki.

PODSUMOWANIE

System PSIM WinGuard bez wątpienia jest rozwiązaniem przyszłościowym, z którego zarządzający obiektami rozproszonymi korzystają na całym świecie. Możliwość przeniesienia procedur obowiązujących w danym obiekcie czy kompleksie obiektów do cyfrowego świata IT jest ogromnym atutem zarówno dla inwestorów, jak i osób obsługujących system.

C&C PARTNERS
ul. 17. Stycznia 119, 121
64-100 Leszno
www.ccpartners.pl
l.schmidt@ccpartners.pl

Mobilne wieże monitoringu obwodowego chronią obiekty strategiczne

Ochrona infrastruktury krytycznej jest jednym z priorytetów stojących przed każdym państwem. Istotne jest to szczególnie w obecnej sytuacji związanej z wojną w Ukrainie. Ważne, by chronić ją przed zagrożeniami, a ewentualne uszkodzenia i zakłócenia w jej funkcjonowaniu były możliwie krótkotrwałe i łatwe do usunięcia.

Infrastrukturę krytyczną można zabezpieczać na różne sposoby, m.in. przy wykorzystaniu systemów elektronicznych, takich jak telewizja dozorowa, kontrola dostępu czy sygnalizacja włamania i napadu. Wszystkie te systemy muszą gwarantować sprawne działanie oraz jego ciągłość.

Takie niezawodne rozwiązania posiada w swoim portfolio spółka Miwi Urmet. Dowodem na to jest szereg realizacji w obiektach o znaczeniu strategicznym. Będące w naszej ofercie zintegrowane systemy: CCTV (IndigoVision, NUUO, Milesight), KD oraz SSWiN (Protege) chronią między innymi jednostki i magazyny wojskowe, dworce kolejowe oraz szpitale. Ostatnio możemy pochwalić się dostarczeniem mobilnych wież monitoringu dla jednego z dostawców energii elektrycznej. To nowoczesna i uniwersalna forma monitoringu, a jednocześnie jeszcze mało popularna.
Wieża jest kompletnym systemem telewizji dozorowej zawierającym kamery, serwer rejestracji oraz układ zasilania i transmisji. Na każdej z kilkunastu dostarczonych mobilnych wież na maszcie teleskopowym zamontowano po dwie kamery stałopozycyjne oraz głowicę PTZ. Taki dobór urządzeń wraz z samym umiejscowieniem zestawów w narożnikach chronionych obszarów zapewnia realizację funkcji monitoringu obwodowego. Kamery bullet stale obserwują dwa boki ogrodzenia, a w przypadku alarmu przecięcia linii przesyłają sygnał do centrum dozoru. Z chwilą wystąpienia alarmu głowica PTZ zostaje skierowana w miejsce, w którym nastąpiło naruszenie linii. W stanie normalnej pracy głowica PTZ wykonuje zaprogramowaną trasę, monitorując bardziej odległe miejsca. Głowica ma również zdefiniowany preset na wypadek otrzymania sygnału z czujki ruchu zabezpieczającej samą wieżę.

Transmisja obrazu jest realizowana z wykorzystaniem sieci GSM. Użycie routera z dwiema kartami SIM oraz zewnętrznymi antenami LTE zapewnia komunikację z centrum dozoru. Ze względu na wielkość strumieni, obrazy są wyświetlane na żądanie operatora lub automatycznie z chwilą wystąpienia alarmu. Gwarancją zachowania odpowiedniej jakości zapisu jest ulokowanie serwera na wieży. Rejestrowany jest zawsze główny strumień z kamer, przy czym w przypadku potrzeby obserwacji przez operatora przez dłuższy czas możliwe jest skorzystanie ze strumieni ograniczonych.
Jedynym stałym elementem instalacji są przyłącza do źródła zasilania, choć zestawy, na wypadek awarii, zostały dodatkowo wyposażone w baterie akumulatorów.
Wieże są budowane z uwzględnieniem indywidualnych potrzeb klienta. Mogą być wyposażone m.in. w panele fotowoltaiczne z modułem inteligentnego ładowania, agregat walizkowy lub zewnętrzny, urządzenia audio oraz dodatkowe doświetlenie IR lub LED. Optymalna liczba kamer to cztery stałopozycyjne oraz kamera bullet PTZ montowana na szczycie masztu.
Mobilność wież pozwala na szybkie przeniesienie kompletnego systemu w inne miejsce lub inną lokalizację. Tego typu urządzenia można również wykorzystać do monitorowania różnego rodzaju plenerowych imprez masowych, parków, placów budowy, czyli wszędzie tam, gdzie zainstalowanie tradycyjnego monitoringu może stanowić problem lub nie jest ekonomicznie uzasadnione.

MIWI-URMET
ul. Pojezierska 90A
91-341 Łódź
miwi@miwiurmet.pl
www.miwiurmet.pl

Zabezpieczenie ppoż. obiektów infrastruktury krytycznej

Infrastruktura krytyczna jest elementem strategicznym z punktu widzenia bezpieczeństwa państwa, jego rozwoju gospodarczego, stabilności, funkcjonowania społeczeństwa oraz obywateli. Dzisiaj, w XXI w. łatwo dostrzec coraz silniejsze uzależnienie funkcjonowania obiektów IK od rozwiązań technicznych. Zachodzące zmiany w tym obszarze wymagają sprostania nowym wyzwaniom związanym z podniesieniem poziomu bezpieczeństwa. Aby sprostać zadaniu, potencjalne zagrożenia, na jakie może być narażony obiekt funkcjonujący w ramach infrastruktury krytycznej, należy zdefiniować już na etapie projektowania.

Michał Białek

W odpowiedzi na możliwe scenariusze należy zaplanować systemy zabezpieczające, w tym systemy sygnalizacji pożarowej (SSP) szyte na miarę potrzeb konkretnego obiektu. Jedną z kluczowych funkcji niezawodnej centrali sygnalizacji pożarowej (CSP) jest 100-proc. redundancja komponentów sprzętowych i oprogramowania, zapewniająca utrzymanie bezpieczeństwa na najwyższym poziomie. SSP powinien odznaczać się także wysoką odpornością na zakłócenia elektromagnetyczne, a także zapewniać kompatybilność rozwiązań „w przód i wstecz", co z punktu widzenia obiektów pracujących w segmencie infrastruktury krytycznej ma olbrzymie znaczenie.
Jest to cecha gwarantująca użytkownikowi dostępność elementów zamiennych i jednocześnie eliminująca jakiekolwiek problemy przy przyszłych rozbudowach czy modernizacjach systemu.
Skupiając się na koncepcji zabezpieczenia obiektów, w tym także obiektów IK, należy mieć na uwadze, iż system sygnalizacji pożarowej, a tak naprawdę zakres związany z detekcją pożaru, to dopiero część kompletnego systemu bezpieczeństwa pożarowego obiektu.
Kolejnym obszarem, na który należy zwrócić szczególną uwagę, jest sterowanie urządzeniami przeciwpożarowymi przez jeden spójny system sygnalizacji pożarowej i sterowania urządzeniami ppoż. CSP realizująca funkcje CSUP, oprócz „standardowych" certyfikatów w zakresie sygnalizacji pożarowej, tj. dotyczących norm EN 54-2 i EN54-4, powinna być poddana dodatkowej procedurze badań i certyfikacji, które potwierdzą możliwość stosowania w zakresie sterowania i nadzorowania:

- systemu oddymiania,
- systemu ppoż. klap odcinających i kurtyn dymowych,
- systemu oddzieleń ppoż. (drzwi i bram ppoż.),
- systemu stałych urządzeń gaśniczych: gazowych, wodnych, pianowych i aerozolowych,
- instalacji wodociągowych ppoż.

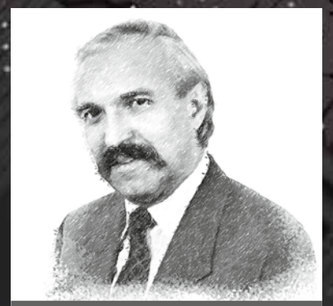
Po pomyślnym zakończeniu procedury certyfikacyjnej zintegrowana CSP/CSUP może realizować następujące funkcje w obiekcie:

- centrali sygnalizacji pożarowej zgodnie z PN-EN 54-2,
- centrali sterującej urządzeniami ppoż. w systemach kontroli rozprzestrzeniania dymu i ciepła zgodnie z KOT (prEN 12101-9),
- zasilacza do systemów kontroli rozprzestrzeniania dymu i ciepła zgodnie z PN-EN 12101-10,
- zasilacza urządzeń ppoż. zgodnie z PN-EN 54-4,
- centrali sterującej stałymi urządzeniami gaśniczymi (SUG) gazowymi zgodnie z PN-EN 12094-1,
- centrali sterującej SUG wodnymi, pianowymi, aerozolowymi zgodnie z KOT,
- centrali sterującej i nadzorującej w ramach instalacji wodociągowych i ppoż. zgodnie z KOT.

W ślad za zmieniającymi się trendami, a jednocześnie chcąc zmodernizować systemy sygnalizacji pożarowej i sterowania urządzeniami ppoż., należałoby także rozważyć wdrożenie systemu integrującego urządzenia przeciwpożarowe (SIUP).
Zintegrowany system bezpieczeństwa pożarowego realizuje funkcje wizualizacji, sterowania i zarządzania urządzeniami ppoż. oraz integruje inne systemy mające wpływ na bezpieczeństwo pożarowe obiektu. Przykładowo, wsparcie obrazem z kamer CCTV wspomaga operatora w reakcji na zagrożenia i obsłudze systemu (np. potwierdzanie lub kasowanie alarmów pożarowych).
Funkcją kluczową systemu jest możliwość aktywnego zarządzania ewakuacją osób i zmiany (gdy to wymagane) scenariusza pożarowego przez kierującego działaniami ratowniczymi. Maksymalny poziom ochrony obiektu IK osiąga się, tworząc spójny, w pełni kompatybilny i kompleksowy system zarządzania bezpieczeństwem pożarowym obiektu.

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

System perymetrycznej ochrony infrastruktury krytycznej

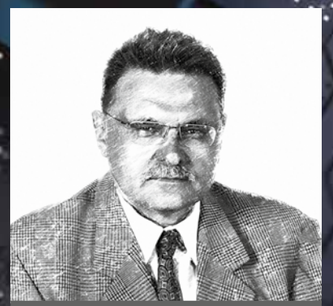


mgr inż. Stanisław Dziubak

Państwowy Instytut Badawczy

mgr inż. Paweł Gajewski

Państwowy Instytut Badawczy



dr inż. Andrzej Sobolewski

Polska Agencja Przemysłowo-Obronna

Zapewnienie bezpieczeństwa obiektom infrastruktury krytycznej wymaga oceny ryzyka wystąpienia zagrożenia oraz budowy zabezpieczeń fizycznych, które ewoluowały równolegle z postępem technicznym – od systemów ochrony obwodowej wokół zewnętrznych granic ochranianego obszaru po nowoczesne systemy dozoru perymetrycznego i powierzchniowego.

Infrastrukturę krytyczną stanowią zasoby państwa mające zasadnicze znaczenie dla funkcjonowania społeczeństwa i gospodarki. Można tu wyróżnić zasoby produkcji, transportu, dystrybucji energii i paliw, a przede wszystkim komunikacji elektronicznej stanowiącej nerw całej gospodarki i funkcjonowania państwa. Środki komunikacji elektronicznej to urządzenia teleinformatyczne wraz z magistralnymi, regionalnymi i dostępowymi sieciami światłowodowymi i radiowymi.

1. SIECI TELEINFORMATYCZNE JAKO ELEMENT INFRASTRUKTURY KRYTYCZNEJ

Sieci teleinformatyczne – telekomunikacyjne lub informatyczne (zwane dalej sieciami) – to w rzeczywistości różne elementy infrastruktury technicznej, takie jak:

- linie kablowe miedziane i światłowodowe,
- kanalizacja kablowa i studnie kablowe,
- szafy uliczne sieci dostępowych z zakończeniami kabli i urządzeniami aktywnymi,
- szafki i pomieszczenia techniczne w budynkach mieszkalnych, przemysłowych itp.,
- stacje bazowe sieci bezprzewodowych: LTE, LTE-A, 5G i inne.

Wymienione obiekty są rozmieszczone na całym obszarze pokrytym siecią. Dla linii kablowych, które są obiektami rozległymi, o długości sekcji w sieci światłowodowej do 100–120 km, a w sieci miedzianej dostępowej do ok. 10 km, wymagane jest zachowanie ciągłości torów transmisyjnych i utrzymanie ich parametrów w zakresie narzuconym przez współpracujące urządzenia aktywne. W razie uszkodzenia niezbędne jest szybkie jego wykrycie i lokalizacja. Dla pozostałych obiektów minimalny zestaw wymagań obejmuje:

- zachowanie fizycznej integralności obiektu,
- wykrywanie włamań i nieuprawnionych prac,
- wykrywanie sytuacji grożących przerwą w pracy lub uszkodzeniem, takich jak pożar, zalanie wodą, utrata zasilania i inne.

Zestaw ten może być uzupełniany o wymagania specyficzne dla danego rodzaju obiektu.
Oprócz firm telekomunikacyjnych w podobnej sytuacji są operatorzy lub właściciele infrastruktury energetycznej, kolejowej czy przemysłowej, mający obiekty bezobsługowe oraz związane z nimi sieci kablowe sygnalizacyjne, informatyczne i sterownicze.
Aktywne urządzenia sieciowe są wyposażone w funkcje nadzoru łączy. Mogą one wykryć uszkodzenie toru w linii kablowej, monitorując moc sygnału na wejściu odbiornika, lecz bez jego lokalizacji. Niestety, w przypadku wynajmowania przez właściciela infrastruktury kablowej par miedzianych i „ciemnych" włókien światłowodowych innym użytkownikom nie ma on dostępu do tych danych. W celu zachowania określonych przez umowy z klientami i regulatora parametrów jakości usług – zwykle dostępności (np. 99,99%) i czasu usunięcia uszkodzenia (np. 12 h) oraz sprawnego utrzymania infrastruktury – niezbędne jest ciągłe monitorowanie jej elementów przez dedykowany system autonomiczny.
Rozpatrując opłacalność ochrony, trzeba uwzględnić, że awarie sieci prowadzą często do zakłóceń i przerw w działaniu systemów ważnych dla gospodarki i bezpieczeństwa państwa lub firm, administracji, kolejowych, bankowych, kontroli ruchu lotniczego, policji, numerów alarmowych, przemysłu itd. Związane z tym straty pośrednie są nieporównanie wyższe od kosztów naprawy przeciętego kabla lub rozbitej szafy z aparaturą.

2. ZAGROŻENIA DLA INFRASTRUKTURY TELEKOMUNIKACYJNEJ

2.1. Uszkodzenia losowe i starzeniowe

Najczęściej spotykanymi przyczynami uszkodzeń infrastruktury kablowej są:

- roboty budowlane i drogowe, których skutkiem są przecięcia lub zgniecenia kabli oraz uszkodzenia kanalizacji i studni kablowych,
- kradzieże kabli i osprzętu, dewastacje, włamania, sabotaż,
- wypadki komunikacyjne powodujące uszkodzenia podpór linii napowietrznych i szaf ulicznych, uszkodzenia studni kablowych przez pojazdy,
- warunki zewnętrzne: wichury, szkody górnicze, osuwiska gruntu, oblodzenie, uszkodzenia linii napowietrznych przez złamane drzewa,
- błędy w trakcie prac przy utrzymaniu i eksploatacji sieci: przecięcia kabli, zwarcia przewodów, błędne przełączenia, nadmierne zginanie światłowodów,
- starzenie kabli i osprzętu pod wpływem zmian temperatury, wilgoci i wibracji,
- przegryzanie kabli przez szczury i inne zwierzęta.

Elementy sieci napowietrznych i szafy uliczne muszą sporadycznie wytrzymać temperaturę od –40°C zimą do 70°C latem, uwzględniając ich nagrzewanie wskutek nasłonecznienia. W ostatnim przypadku temperatura wewnątrz szafy z urządzeniami aktywnymi może przekroczyć 80°C, co prowadzi do niestabilności parametrów, szybkiego starzenia i awarii urządzeń. W temperaturze poniżej –25°C dochodzi natomiast do uszkodzenia akumulatorów ołowiowo-kwasowych (VRLA) używanych do zasilania rezerwowego wskutek zamarznięcia elektrolitu w rozładowanym akumulatorze.
Kable zewnętrzne i ich osprzęt pasywny lepiej znoszą działanie zmiennych temperatur i warunków atmosferycznych, ale możliwe są stopniowo postępujące uszkodzenia:

- wnikanie wilgoci i soli oraz korozja złączy wewnątrz osłon złączowych i szaf,
- uszkodzenia kabli z przewodami metalowymi przez wyładowania atmosferyczne,
- korozja i uszkodzenia mechaniczne uchwytów kabli napowietrznych,
- migracja żelu i włókien w kablach światłowodowych napowietrznych,
- kurczenie się tub w kablach światłowodowych po ekspozycji na wysoką temperaturę latem, obserwowane po spadku temperatury zimą poniżej np. –30°C; włókna ulegają silnym zgięciom wewnątrz skróconych tub lub wysuwają się z końca kabla w osłonie złączowej, a ich tłumienność wzrasta,
- luzowanie włókien wklejonych we wtykach złączy światłowodowych po degradacji kleju, połączone ze wzrostem strat i odbiciami promieniowania.

Awarie te są często wynikiem wadliwego montażu lub używania kabli i osprzętu niskiej jakości, względnie zaprojektowanych do pracy w odmiennych warunkach klimatycznych.

2.2. Uszkodzenia celowe

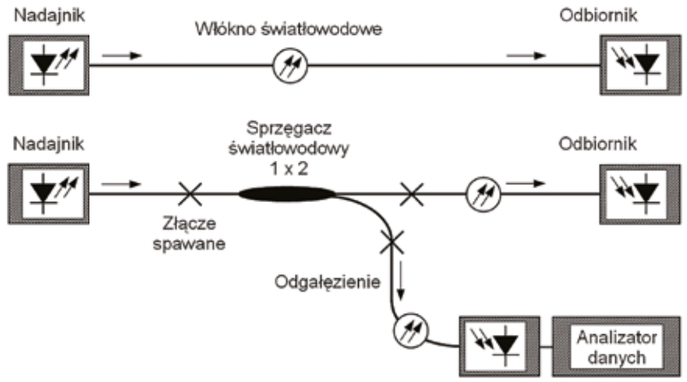
Dużym zagrożeniem dla infrastruktury sieci kablowych są celowe działania przestępcze wymienione poniżej:

- Wandalizm, dywersja i sabotaż. Przecięcie światłowodów w kilku punktach w celu zablokowania mechanizmów protekcji w sieci szkieletowej lub metropolitalnej to tani sposób na sparaliżowanie sieci obsługującej miasto, bank czy przedsiębiorstwo bez używania broni palnej lub materiałów wybuchowych. Danych o lokalizacji i funkcji kabli mogą dostarczyć byli pracownicy firm telekomunikacyjnych. W kraju notowano m.in. przecinanie kabli, by zniszczyć reputację konkurującego operatora w celu przejęcia klientów oraz w wyniku sporów o opłaty za przejście przez nieruchomości lub wynajem kanalizacji kablowej.
- Kradzieże kabli miedzianych w celu ich sprzedaży na złom, często połączone z uszkodzeniami stud-

ni kablowych oraz przecinaniem rur kanalizacji i kabli światłowodowych. Te ostatnie nie mają wartości jako surowiec wtórny, przenoszą natomiast duży ruch i są pracochłonne w naprawie.
- Nielegalne korzystanie z kanalizacji kablowej – układanie kabli przez obce firmy bez zgody właściciela i opłat; możliwe jest uszkodzenie już istniejących kabli.
- Instalowanie odgałęzienia do przechwytywania danych, także ze światłowodów.

Instalacja odgałęzienia przez rozcięcie włókna światłowodowego i wstawienie pasywnego sprzęgacza odprowadzającego 1–20% sygnału *(rys. 1)* powoduje krótkotrwałą przerwę, a następnie trwały wzrost tłumienności, zwykle o 0,5–1,5 dB, stanowiący sumę strat sprzęgacza i dwóch złączy spawanych. Odgałęzienie umożliwia też zagłuszanie lub wprowadzenie fałszywych danych. Wspólny port sprzęgacza znajduje się wtedy od strony odbiornika atakowanego łącza. Przerwa włókna podczas montażu odgałęzienia trwa 2–4 min. To może uniemożliwić wykrycie tego zdarzenia przez system monitoringu wykonujący okresowe pomiary czynnego włókna za pomocą reflektometru impulsowego (*Optical Time Domain Reflectometer* – OTDR), najczęściej co 10–30 min.

Rys. 1. Odgałęzienie sygnału ze światłowodu przez montaż sprzęgacza. Na górze – łącze w oryginalnej konfiguracji, na dole – łącze z odgałęzieniem



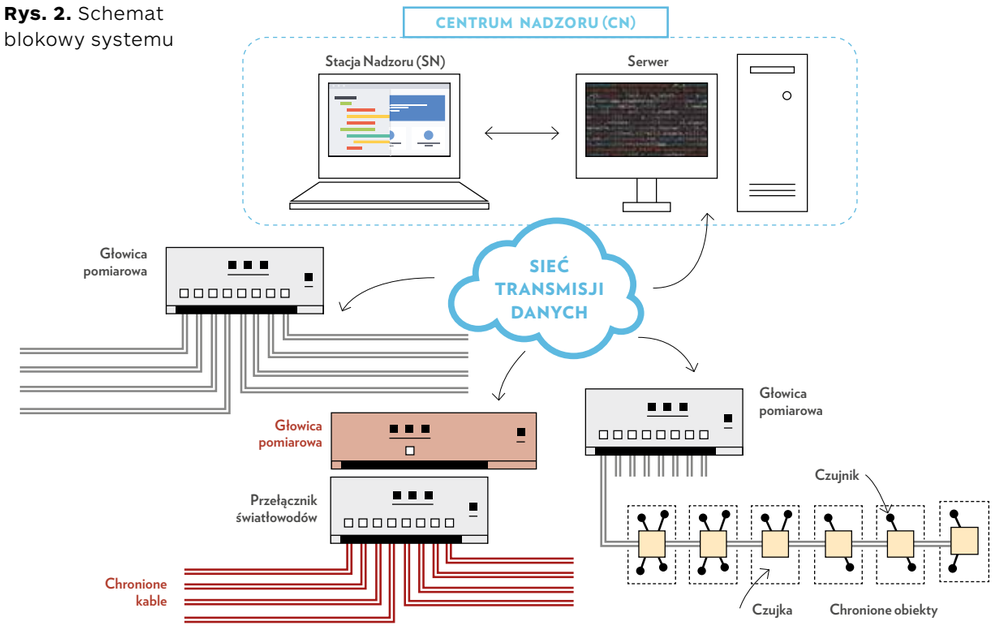
3. MONITORING INFRASTRUKTURY TELEINFORMATYCZNEJ

3.1. Monitoring infrastruktury sieciowej

Przecięcie kabla podczas robót ziemnych, sabotażu lub kradzieży powoduje natychmiast trwałą przerwę wszystkich par przewodów lub włókien światłowodowych. Podobnie jest w przypadku ponad 80% uszkodzeń losowych, stąd do wykrycia i lokalizacji uszkodzenia wystarcza nadzór wybranego włókna lub pary przewodów w linii kablowej.
Nielegalne układanie kabli wymaga wejścia do studni kablowych. Można je wykryć, monitorując włazy i drzwi w obiektach, nie ma natomiast zmian parametrów kabli. Również większość aktów sabotażu i kradzieży rozpoczyna się od włamania do studni kablowych bądź pomieszczeń lub szaf z osprzętem i aparaturą. Podstawową korzyścią z monitoringu po wykryciu i lokalizacji włamania, uszkodzenia lub sytuacji awaryjnej jest szybka reakcja przez interwencję ochrony oraz wysłanie serwisantów. Skuteczne zwalczanie wymienionych wcześniej zagrożeń wymaga scentralizowanego rozwiązania dla hermetyzacji i ochrony sieci kablowej obejmującego:
- kompletną, na bieżąco aktualizowaną ewidencję (tzw. paszportyzację) elementów sieci,
- fizyczne zabezpieczenia przed włamaniami: zamki, wzmocnione pokrywy studni itp.,
- system monitoringu wykrywający, sygnalizujący, lokalizujący i rejestrujący uszkodzenia elementów sieci, zmiany ich parametrów, włamania do studni i in.

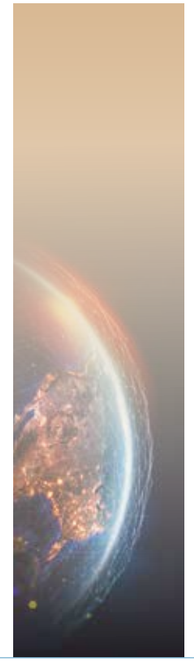
System monitoringu infrastruktury telekomunikacyjnej (zwany dalej „systemem") autorstwa Instytutu Łączności pełni tę ostatnią funkcję. Może też zapewnić integrację wszystkich związanych z eksploatacją i utrzymaniem infrastruktury systemów innych producentów, w tym wymianę danych między systemami i zintegrowane centrum nadzoru. Rozwiązania takie mogą być tworzone według indywidualnych wymagań.

Rys. 2. Schemat blokowy systemu



3.2. Funkcje systemu

Zakres funkcji systemu obejmuje:
- monitorowanie kabli z parami przewodów miedzianych,
- monitorowanie kabli światłowodowych z włóknami jednomodowymi,
- sygnalizację i lokalizację uszkodzeń kabli jw.,
- nadzór obiektów za pomocą czujników: otwarcia, pożaru, zalania wodą itp.,
- rejestrację zdarzeń w bazie danych i sygnalizowanie ich obsłudze centrum nadzoru,
- pokazywanie miejsca zdarzenia lub uszkodzenia na mapie,
- prezentację opisu obiektu lub linii kablowej oraz danych kontaktowych (serwisanci obsługujący dany obszar, agencje ochrony, posterunki policji lub innych służb),
- tworzenie raportów z danymi wybranymi według kryteriów wprowadzonych przez operatora (przedział dat, rodzaj obiektu, region, rodzaj zdarzenia),
- eksport wybranych danych.



Zakres funkcji systemu można dostosować do wymagań danego operatora lub użytkownika sieci i charakterystyki chronionej infrastruktury przez dobór lub zaprojektowanie nowych elementów sprzętowych i modułów oprogramowania.

3.3. Architektura systemu

Architekturę systemu przedstawiono na rys. 2. System składa się z komputera centrum nadzoru oraz dołączonych do niego różnego rodzaju głowic i czujek.
Miedziane linie kablowe są nadzorowane bezpośrednio przez głowice pomiarowe do kabli miedzianych, które mają 16 portów pomiarowych – jedna głowica może nadzorować do 16 kabli.

Linie światłowodowe są nadzorowane przez głowice pomiarowe do kabli światłowodowych zawierające reflektometr optyczny (OTDR). Głowica ma jeden port, do którego, za pomocą przełącznika światłowodów są sekwencyjnie dołączane pojedyncze włókna z każdego kabla światłowodowego. Mogą być nadzorowane zarówno włókna wolne, jak i wykorzystywane do transmisji (wymaga to montażu sprzęgaczy WDM na końcach linii).

System, nadzorując kable, wykonuje cyklicznie pomiary parametrów wolnej pary przewodów lub włókna w każdej linii kablowej i porównuje wyniki aktualne z wynikami wzorcowymi zapisanymi wcześniej po pomiarach sprawnego kabla. Zmiana parametrów przekraczająca ustalony zakres tolerancji powoduje alarm w centrum nadzoru i określenie miejsca uszkodzenia.
Monitorowane parametry obejmują:

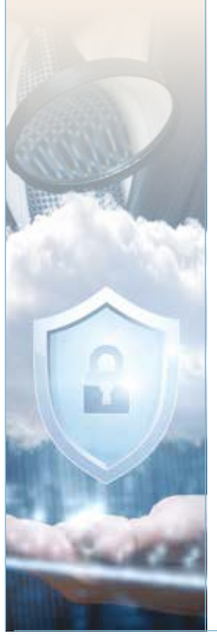
- dla par przewodów miedzianych: rezystancję pętli przewodów i pojemność między przewodami oraz planowane dodanie charakterystyk reflektometrycznych
- dla włókien światłowodowych: charakterystyki reflektometryczne (amplituda echa w funkcji odległości od głowicy pomiarowej).

Maksymalne długości monitorowanych linii kablowych wynoszą typowo dla kabli miedzianych kilka kilometrów, a dla kabli światłowodowych do 100 km.

Studnie kablowe, szafy oraz inne obiekty w terenie są nadzorowane przez montowane w nich czujki. Stany czujek są odczytywane przez komputer w centrum nadzoru za pośrednictwem odpowiednich głowic, które także zasilają czujki przez kabel transmisyjny. Jedna głowica może obsługiwać do 7 linii z czujkami, a do każdej linii o długości kilku kilometrów można dołączyć do 30 czujek. Wszystkie czujki są co kilka sekund sprawdzane przez komputer centrum, dzięki czemu można szybko wykryć ewentualne uszkodzenia w systemie, zakłócenia transmisji itp.

Centralnym elementem systemu jest jego centrum nadzoru, które stanowi komputer z oprogramowaniem użytkowym oraz opcjonalne terminale.
Głowice pomiarowe do kabli miedzianych i światłowodowych oraz przełączniki światłowodów są dołączane poprzez Ethernet i protokół TCP/IP lub opcjonalnie inny interfejs np. RS-485. Oprogramowanie centrum nadzoru realizuje funkcje związane z:

- instalacją, konfigurowaniem i nadzorem pracy elementów sprzętowych systemu,
- wprowadzaniem danych i opisów chronionych elementów sieci,
- zbieraniem i przetwarzaniem danych pomiarowych,
- wykrywaniem, sygnalizacją i lokalizacją uszkodzeń, włamań i innych zdarzeń,
- utrzymywaniem bazy danych zdarzeń,
- tworzeniem raportów z danymi zdarzeń oraz ich eksportem,
- zarządzaniem użytkownikami system.



4. BEZPIECZEŃSTWO INFRASTRUKTURY INFORMATYCZNEJ

System opracowany przez Instytut Łączności stanowi odpowiedź na potrzeby perymetrycznej ochrony sieci teleinformatycznych, systemów istotnych dla bezpieczeństwa państwa, administracji, policji, kolei, lotnictwa, banków lub przedsiębiorstw przemysłowych, handlowych i usługowych. Ochrona zapewniona przez system umożliwia przede wszystkim:

- stały nadzór nad sieciami teleinformatycznymi miedzianymi i światłowodowymi,
- natychmiastową informację o miejscu i przyczynie zdarzenia (miejsce na mapie),
- powiadamianie nadzoru o zdarzeniu i uruchomienie działań naprawczych,
- raportowanie, statystyki, analizy.

Należy zwrócić uwagę, że nawet proste uszkodzenie sieci może pośrednio wpływać na funkcjonowanie obiektów infrastruktury krytycznej i generować wielokrotnie większe koszty od inwestycji w system monitoringu infrastruktury telekomunikacyjnej.

Najpopularniejsze technologie

w ochronie perymetrycznej

William Pao

asmag.com

Wiele firm, zwłaszcza prowadzących działalność na obszarze rozległym, przykłada dużą wagę do ochrony perymetrycznej (obwodowej). Przedstawiamy najpopularniejsze technologie i zabezpieczenia elektroniczne stosowane w tego typu systemach.

Ochrona obwodowa ma na celu powstrzymanie intruza wzdłuż zewnętrznej granicy posesji przed wtargnięciem na teren chronionego obiektu. To istotna, bo wczesna technika ochronna ważnych obiektów, począwszy od infrastruktury krytycznej i obiektów wojskowych, skończywszy na obiektach komercyjnych i rezydencjach. Popyt na te rozwiązania rośnie w stałym tempie. Według MarketsandMarkets rynek ochrony perymetrycznej wzrośnie z 61,3 mld USD w 2020 r. do 96,5 mld USD do 2026 r., przy współczynniku CAGR 7,9%.

Systemy ochrony perymetrycznej wykrywają incydenty za pomocą czujników (sensorów), z których każdy, wykorzystując różne zjawiska fizyczne, oferuje unikalną metodę wykrywania. Użytkownicy mają do wyboru różne opcje. Prezentujemy najpopularniejsze technologie ochrony obwodowej.

1 RADARY I LIDARY

Radar jest urządzeniem wykrywającym za pomocą fal radiowych obiekty powietrzne, nawodne oraz lądowe, pozwalającym na określenie kierunku, odległości oraz rozmiarów wykrywanego obiektu, a w przypadku radarów dopplerowskich mierzącym także jego prędkość. Do detekcji obiektów wykorzystuje się zjawisko odbicia fal radiowych (najczęściej w paśmie mikrofal) od obiektów lub fal wysyłanych przez te obiekty.

Lidar *(Light Detection and Ranging)* to połączenie lasera z teleskopem. Czujnik lidarowy emituje wiązki laserowe do chronionego otoczenia i oblicza odległość obiektu na podstawie czasu, w jakim wiązka laserowa wraca po odbiciu od obiektu. Zaletą lidaru w porównaniu z kamerami dozorowymi jest to, że jest on niezależny od oświetlenia i trudnych warunków atmosferycznych.

– *Pod wpływem dużego zainteresowania sektora motoryzacyjnego rozwiązaniami lidarowymi są one coraz tańsze, a jednocześnie oferują lepsze możliwości w zastosowaniach zewnętrznych* – twierdzi Brad Martin, dyrektor ds. zarządzania produktami w firmie Senstar.

2 ŚWIATŁOWÓD

Działanie sensorycznych kabli światłowodowych polega na przesyłaniu wiązki światła laserowego wewnątrz światłowodu i pomiarze odbić światła pojawiających się na całej jego długości. Zakłócenia światłowodu spowodowane wibracją ogrodzenia wywołaną np. przez osobę wspinającą się lub opierającą drabinę na ogrodzeniu zmieniają ilość światła powracającego (odbitego).

– *Światłowodowe kable sensoryczne są już uznanym rozwiązaniem. Cieszą się coraz większym zainteresowaniem dzięki dostępności opłacalnych rozwiązań dla mniejszych obiektów oraz wydłużonemu, ponad 20-letniemu okresowi eksploatacji* – mówi B. Martin.

3 KOMUNIKACJA BEZPRZEWODOWA

Coraz częściej w systemach zabezpieczeń stosuje się łączność bezprzewodową.

– *Komunikacja bezprzewodowa między czujnikiem a systemem jest coraz powszechniejsza ze względu na rosnące zaufanie do technologii bezprzewodowej. Tendencja ta jest zauważalna szczególnie w przypadku ochrony rezydencji oraz małych i średnich obiektów komercyjnych* – podkreśla Ken Arimura, dyrektor generalny ds. sprzedaży w regionie Azji i Pacyfiku w firmie OPTEX.

Zainteresowaniem cieszą się także funkcje zdalnego sterowania i monitorowania.

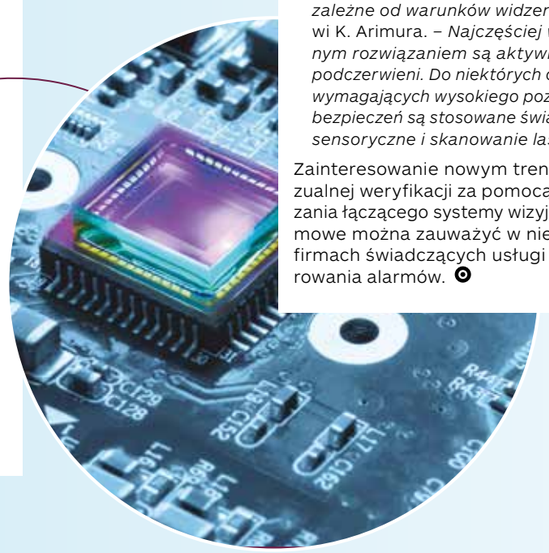
– *Możliwość zdalnego sterowania i monitorowania za pomocą smartfonów jest obecnie must have w przypadku zapytań dotyczących ochrony rezydencji. Niektóre projekty wymagają dodatkowo funkcji automatyki domowej* – dodaje K. Arimur.

4 DOZÓR WIZYJNY

Systemy telewizji dozorowej stały się popularną, wręcz niezbędną technologią ochrony obwodowej, umożliwiającą weryfikację sytuacji alarmowej.

– *Dozór wizyjny jest coraz częściej stosowany w ochronie obwodowej m.in. ze względu na rozwój zdalnego monitoringu w odpowiedzi na większe potrzeby weryfikacji wizualnej zdarzenia alarmowego i ograniczenie kosztów związanych z reagowaniem na fałszywe alarmy. Inne czujki ochrony obwodowej wykrywają, że „coś" narusza lub próbuje naruszyć ogrodzenie, natomiast telewizja dozorowa pozwala operatorom zdalnie dokładnie ustalić, „co" jest przyczyną alarmu i, najważniejsze, podjąć odpowiednią reakcję* – podkreśla Niklas Rosell, globalny menedżer produktu ds. funkcji kamer inteligentnych w Axis Communications.

– *Monitoring wizyjny ma kluczowe znaczenie dla ochrony obwodowej. Bez natychmiastowej, opartej na obrazie z kamer możliwości oceny alarmów pracownicy ochrony mogą mieć mniejsze zaufanie do informacji z systemów wykrywania włamań. Aby zmaksymalizować skuteczność dozoru wizyjnego i oceny sytuacyjnej, system zarządzania wizją musi powiązać lokalizację włamania (najlepiej z dokładnością do kilku metrów) z konkretną kamerą lub presetem PTZ. Zautomatyzowane wywoływanie kamery zapewnia wiele korzyści: szybszą reakcję operatora, mniejsze wymagania szkoleniowe, zoptymalizowaną jakość materiału wizyjnego i ustawienia retencji oraz możliwość uruchamiania środków odstraszających intruza specyficznych dla danej lokalizacji* – mówi B. Martin.



5 FUZJA SENSORÓW

Każda technologia detekcji ma zalety i wady. Połączenie różnych czujników (sensorów), czyli wykorzystanie kombinacji różnych technologii detekcji, sprawia, że ochrona perymetryczna jest bardziej skuteczna.

– Żeby móc w pełni korzystać z zalet różnych technologii, organizacje potrzebują inteligentnych, zintegrowanych rozwiązań, co pozwoli maksymalnie wykorzystać mocne strony każdej z nich. To dlatego fuzja czujników wzbudza zainteresowanie – uważa B. Martin. – *Połączenie sensorów pozwala wykorzystać dzisiejszą imponującą moc obliczeniową do analizowania danych w czasie rzeczywistym z informacjami archiwalnymi, lokalizacyjnymi, środowiskowymi i klasyfikacyjnymi przed wygenerowaniem alarmu. Dla operatorów jest to klucz do wyeliminowania uciążliwych alarmów przy zachowaniu najwyższego poziomu bezpieczeństwa.*

Przykładem jest połączenie w parę czujek systemu alarmowego i kamer dozorowych.

– *Kamery dozorowe (jako sensory) mają pewne ograniczenia – nie działają w ciemności, często na obrazie brakuje szczegółów lub kontekstu przestrzennego, które zapewnią wysoką dokładność wykrywania czy klasyfikacji incydentów. Ograniczenia te można przezwyciężyć, łącząc dane z kamer dozorowych z danymi z czujek komplementarnych (uzupełniających). Przykładowo, sensory tripwire, takie jak sensoryczne kable światłowodowe, generują alarmy z dużych ogrodzonych obszarów, podczas gdy radar i lidar dodają informacje przestrzenne i działają w złych warunkach otoczenia* – wyjaśnia Srinath Kalluri, dyrektor generalny firmy Oyla.

– *Integracja czujek z kamerami IP/VMS jest coraz powszechniejsza. Na rynku azjatyckim rozwiązania wizyjne są pierwszym wyborem użytkowników końcowych, którzy myślą o zabezpieczeniach. Jednak wielu klientów dodaje rozwiązania sensoryczne (czujki) do uruchamiania nagrywania wizyjnego i powiadamiania, uzupełniające słabe punkty rozwiązań opartych wyłącznie na telewizji dozorowej, które są zależne od warunków widzenia* – mówi K. Arimura. – *Najczęściej wybieranym rozwiązaniem są aktywne czujki podczerwieni. Do niektórych obiektów wymagających wysokiego poziomu zabezpieczeń są stosowane światłowody sensoryczne i skanowanie laserowe.*

Zainteresowanie nowym trendem wizualnej weryfikacji za pomocą rozwiązania łączącego systemy wizyjne i alarmowe można zauważyć w niektórych firmach świadczących usługi monitorowania alarmów.

Jak radzić sobie z wyzwaniami w ochronie obwodowej?

Prasanth Aby Thomas

asmag.com

W ostatnich latach systemy ochrony obwodowej znacznie rozwinęły się pod względem technologii. Obecnie ochrona obwodowa nie polega już na zakopywaniu kabli w ziemi.

Pomimo szybkiego postępu specjaliści i klienci nadal muszą stawić czoło poważnemu wyzwaniu związanemu z ochroną obwodową. Najbardziej uciążliwe są fałszywe alarmy.

– Najlepszym sposobem na ich pokonanie jest po prostu posiadanie systemu, który sygnalizuje o tym, co jest dla nas istotne – twierdzi Jammy DeSousa, starszy menedżer ds. produktów bezpieczeństwa w Johnson Controls. – Gdy system generuje zbyt wiele uciążliwych alarmów, przestaje być narzędziem skutecznym.

POPYT NA BARDZIEJ INTELIGENTNE SYSTEMY

Problem fałszywych alarmów nie jest nowy. Występują one częściej, niż się większości wydaje. Obniżają skuteczność zabezpieczenia, są też główną przyczyną dużych strat. Biorąc pod uwagę ponoszone koszty, wiele rządów nakłada kary za zbyt dużą liczbę fałszywych alarmów. Wszystkie te czynniki, a także potrzeba posiadania systemów ekonomicznie uzasadnionych spowodowały wzrost zainteresowania inteligentnymi rozwiązaniami w zakresie ochrony obwodowej.

– W przeszłości dostępne na rynku technologie nie w każdym przypadku były rozwiązaniem uzasadnionym ekonomicznie dla klientów mających rozległy teren do ochrony. Obecnie oferowane technologie są przystępne cenowo dla masowego odbiorcy. Coś, co kiedyś było poza zasięgiem budżetu klienta, dzisiaj jest łatwo dostępne – mówi J. DeSousa.

Jeśli chodzi o ograniczenie liczby fałszywych alarmów, obecnie na rynku jest wiele skutecznych rozwiązań.

NIEZBĘDNE ROZWIĄZANIA DLA OCHRONY OBWODOWEJ

W systemach ochrony perymetrycznej pojawia się wiele innowacji. Jeśli wdrożona technologia nie jest oparta na rozwiązaniach wizyjnych, weryfikacja zdarzenia alarmowego jest pierwszym krokiem w procesie ochrony. Do niezbędnych rozwiązań zabezpieczeń technicznych w ochronie obwodowej należy system zarządzania sygnałem wizyjnym dla całego terenu.

– Nie można zakładać, że ktoś monitoruje tylko obszar w jego pobliżu, może on monitorować kilka obiektów czy kampusów – podkreśla J. DeSousa. – Bardzo ważne, aby mieć obraz z kamery i mapę terenu w celu lepszego oglądu sytuacji. Jeśli chodzi o innowacje, granice nie zawsze dotyczą zewnętrznych ogrodzeń nieruchomości.

Zmiana definicji obwodu stwarza nowe wymagania i możliwości. Zależy to także od specyfiki obiektu czy przedsiębiorstwa. Czasami granica może być wyznaczona w obrębie obszaru, który ma określone strefy zabezpieczone i niezabezpieczone, np. w szpitalu.

CZYNNIKI, JAKIE NALEŻY UWZGLĘDNIAĆ W OCHRONIE OBWODOWEJ

Choć technologia ochrony staje się coraz bardziej innowacyjna, przed zainstalowaniem jakiegokolwiek rozwiązania nadal należy wziąć pod uwagę kilka czynników. Należy przede wszystkim poznać specyfikę zabezpieczanego obiektu – jego wielkość, położenie i ukształtowanie terenu.

– To pozwoli ustalić, jaki rodzaj technologii należy wybrać, np. czy zastosować technologię perymetryczną wspieraną algorytmami AI, czy starszą technologię, np. zakopywane w ziemi kable sensoryczne – kontynuuje J. DeSousa. – Ochrona obwodowa nie jest łatwym zagadnieniem, to nie jest prosty wybór bieli lub czerni. Zrozumienie wielkości i złożoności obszaru oraz przeprowadzenie z klientem analizy zagrożeń może pomóc w wyborze najskuteczniejszego rozwiązania.

Przykładowo, niektóre obszary muszą być monitorowane pod kątem określonego poziomu aktywności, a możliwość filtrowania tego, co jest dozwolone, jest bardzo ważna.

INNE WYZWANIA, KTÓRE NALEŻY ROZWAŻYĆ

Fałszywe alarmy są głównym problemem, ale skuteczność systemu ochrony obwodowej ograniczają także inne kwestie. Jammy DeSousa zauważa, że choć radar zdecydowanie zyskał na popularności, to występujące spore nierówności ochranianego terenu lub wysoka roślinność mogą stanowić problem.

– Z tego powodu, stosując tego typu rozwiązania, musimy brać pod uwagę topografię – **mówi J. DeSousa.** – Kolejnym rozwiązaniem, które cieszy się większym popytem, jest sztuczna inteligencja. Dziś możemy już efektywnie wykorzystywać kamery do obserwacji obszarów wzdłuż obwodu i na tej podstawie wykrywać dokładnie to, na czym zależy klientowi, tzn. wtargnięcie człowieka, a nie pojawienie się zwierzęcia. Możemy wykorzystać obraz z kamer CCTV do skutecznego rozróżniania obiektów znajdujących się w pobliżu granicy.

WNIOSKI

W sektorze ochrony obwodowej są wprowadzane innowacje, a do stosowanych rozwiązań wkraczają nowe technologie. Nadal jednak pozostają problemy, takie jak fałszywe alarmy, które zwiększają zapotrzebowanie na inteligentne rozwiązania mogące je weryfikować i zapewniać lepszą ochronę. W przyszłości mogą stać się priorytetem dla klientów starających się unikać strat i zbędnych kosztów.

Coraz więcej klientów preferuje analitykę wizyjną w ochronie obwodowej

Ochrona perymetryczna to ważny element polityki bezpieczeństwa przedsiębiorstwa. Do niedawna ograniczano się do takich urządzeń, jak kamery CCTV/VSS, bariery podczerwieni, rzadziej wykorzystywano radary i lidary. Obecnie analityka wideo, którą stosuje się w każdym aspekcie dozoru wizyjnego, staje się popularna również w ochronie obwodowej.

Prasanth Aby Thomas

asmag.com

Na łamach serwisu asmag.com Fabio Marti, wiceprezes ds. marketingu w firmie Azena, powiedział, że obserwuje zdecydowany wzrost zapotrzebowania na analitykę wizji w rozwiązaniach ochrony obwodowej.

– Zastosowanie analityki wideo rośnie wykładniczo ze względu na dokładność i zaawansowanie dzięki dodaniu sztucznej inteligencji – mówi Fabio Marti. – Kamery, które mogą przetwarzać sygnały wizyjne z wykorzystaniem analityki opartej na sztucznej inteligencji, mogą dokładniej wykrywać anomalie na obrazie i weryfikować je jako potencjalne zagrożenia lub fałszywe alarmy oraz pomagać operatorom w określeniu odpowiedniego poziomu reakcji.

Przykładowo kamery wyposażone w algorytmy przekraczania linii i wykrywania broni mogą ostrzegać operatorów, że człowiek nie tylko wszedł na teren strefy, ale także wykryto u niego broń. W centrum monitoringu taki alarm jest wstępnie weryfikowany pod kątem zwiększonego zagrożenia, a operatorzy są natychmiast powiadamiani o poziomie priorytetu tego zdarzenia alarmowego.

WYZWANIA DOTYCZĄCE OCHRONY OBWODOWEJ

Z ochroną perymetryczną wiąże się kilka problemów. Zagrożenia występujące na granicy terenu przedsiębiorstwa stają się coraz bardziej wyrafinowane. Wzrost popularności dronów i technologii detekcyjnych stwarza nowe rodzaje wyzwań.

– Rośnie złożoność pracy centrum monitoringu – zauważa F. Marti. – Operatorzy muszą monitorować wszystko, począwszy od systemów alarmowych i dozoru wizyjnego, poprzez systemy pogodowe i czujniki środowiskowe, media społecznościowe, skończywszy na innych funkcjach biznesowych, takich jak zarządzanie flotą czy bezpieczeństwo podróży kadry kierowniczej i personelu.

Analityka wideo z AI może rozwiązać wiele spośród tych problemów, automatyzując pewne działania i zapewniając, że osoby podejmujące decyzje mogą skupić swoją uwagę na elementach o wyższym priorytecie.

JAK ANALITYKA WIDEO POMAGA W OCHRONIE OBWODOWEJ

Fabio Marti zwrócił uwagę, że klienci wybierają analitykę wideo z kilku powodów.

Może być ona stosowana np. jako pierwsza linia obrony na granicy posesji w celu wstępnego filtrowania przychodzących alarmów.

Możliwość pełniejszej automatyzacji zweryfikowania alarmów oznacza, że operatorzy w centrum monitoringu obsługują mniejszą liczbę zdarzeń alarmowych i mogą skoncentrować swoje wysiłki na przychodzących alarmach, które zostały już wstępnie zakwalifikowane jako wymagające reakcji.
Dzięki temu operatorzy będą mieli możliwość monitorowania obrazów z dodatkowych kamer lub z większej liczby obiektów w centralnej lokalizacji albo większego obszaru geograficznego przy tej samej liczbie pracowników.

– Możliwość automatycznej korelacji sygnałów z innych systemów, np. kontroli dostępu lub wykrywania włamań, z obrazem wideo powiązanym ze zdarzeniem może również pomóc w wykryciu przyczyny fałszywego alarmu – kontynuuje F. Marti. – Może to oznaczać zdiagnozowanie różnicy między zdarzeniem związanym z bezpieczeństwem, które wymaga natychmiastowej reakcji, a usterką mechaniczną, która zamiast wysłania pracownika ochrony może wymagać wezwania technika lub złożenia zlecenia naprawy.

Integracja systemów jeszcze bardziej zwiększa korzyści. Kamery zintegrowane z systemem kontroli dostępu mogą dostarczać dane wizyjne z serii nieudanych odczytów karty przez uprawnionego użytkownika, wskazując potencjalną usterkę czytnika lub karty. Seria zwiększonych zdarzeń alarmowych przy drzwiach może również sygnalizować poluzowanie styków, jeśli kamery pokazują, że w tym czasie nie było tam żadnej osoby. Te możliwości mogą również zapewnić dodatkowe korzyści wykraczające poza prostą ochronę obwodową.

UWAGI KOŃCOWE

W miarę, jak coraz więcej klientów uświadamia sobie korzyści zapewniane przez analitykę wizyjną, również w systemach ochrony obwodowej obserwuje się wzrost popytu na nią. Problemy takie jak COVID-19 i obawy ekonomiczne zwiększyły zapotrzebowanie na lepszą, efektywniejszą ochronę zapewnianą przy mniejszej liczbie personelu w terenie. Analityka wideo jest w stanie sprostać tym wymaganiom.

> *Operatorzy muszą monitorować wszystko, począwszy od systemów alarmowych i dozoru wizyjnego, poprzez systemy pogodowe i czujniki środowiskowe, media społecznościowe, skończywszy na innych funkcjach biznesowych, takich jak zarządzanie flotą czy bezpieczeństwo podróży kadry kierowniczej i personelu.*

Rola kamer w ochronie obwodowej

Ochrona obwodowa jest jednym z kluczowych aspektów kompleksowego zabezpieczenia obiektów infrastruktury krytycznej, takich jak lotniska, elektrownie, zakłady produkcyjne, a także obiektów lub terenów zajmujących duże obszary, np. granice państw.

Michał Mielczarek

Prawdopodobnie najpopularniejszym rozwiązaniem stosowanym w ochronie obwodowej obiektów są wszelkiego rodzaju zabezpieczenia mechaniczne: ogrodzenia, druty kolczaste itp. elementy, które można w tym celu wykorzystać.
Rozwiązania te w niektórych przypadkach są wystarczające, np. tam, gdzie spodziewane zagrożenie lub straty wynikające z przedostania się intruzów do obiektu są minimalne. W ochronie obiektów infrastruktury krytycznej wręcz konieczne jest doposażenie zabezpieczeń mechanicznych w elektroniczne systemy zabezpieczeń. Mogą to być m.in. kable sensoryczne montowane na ogrodzeniu albo ukryte w ziemi, różne typy czujek zewnętrznych montowane nad ziemią, detektory wizyjne czy systemy dozoru wizyjnego. Różne systemy współdziałające ze sobą sprawiają, iż chroniony obiekt jest zabezpieczony w najwyższym stopniu.
Stosowane w ochronie obwodowej kamery dozorowe są wykorzystywane na wielu płaszczyznach. Ich zadaniem może być wykrywanie potencjalnego zagrożenia, zanim jeszcze intruz zbliży się do ogrodzenia, granicy chronionego obiektu, ale takie rozwiązanie generuje dużą liczbę fałszywych alarmów. Kolejnym celem ich stosowania jest wizyjna weryfikacja alarmów pochodzących z innych elektronicznych systemów ochrony obwodowej. Kamery mogą też śledzić intruza lub intruzów poruszających się na terenie chronionego obiektu w strefie peryferyjnej. Śledzenie może odbywać się za pomocą kamer ruchomych lub poprzez dynamiczne przełączanie kamer stacjonarnych w stacji roboczej operatora systemu monitoringu wizyjnego.
Wykorzystanych może być wiele rodzajów kamer – od standardowych kamer światła widzialnego z dodatkowym oświetlaczem podczerwieni lub bez niego, kamer ruchomych, kamer termowizyjnych stałopozycyjnych czy dualnych w wersji zarówno stałopozycyjnej, jak i ruchomej.

KAMERA MIC FUSION 9000I

Firma Bosch przy współpracy ze swoimi partnerami często stawia na kamery termowizyjne jako najskuteczniejszą metodę wykrywania zagrożeń. Kamery te występują w wielu wersjach: stałopozycyjnej z modułem termowizyjnym oraz dualnej, ruchomej z dwoma modułami kamerowymi.
Jednym z ciekawszych rozwiązań do ochrony obwodowej obiektów infrastruktury krytycznej jest sieciowa kamera Bosch MIC Fusion 9000i z dwoma modułami kamerowymi. Model ten mieści w jednej obudowie dwa przetworniki obrazu: zaawansowany przetwornik termowizyjny oraz przetwornik wizyjny w technologii Starlight o rozdzielczości 1080p. Dzięki temu kamera może przesyłać równocześnie strumienie danych wizyjnych i termowizyjnych, zwiększając do maksimum prawdopodobieństwo wykrycia odległych obiektów i odpowiedniego zareagowania na zagrożenie.

Fot. 1. Kamera Bosch MIC Fusion 9000i

Przetwornik termowizyjny jest wyposażony w najnowocześniejszy miniaturowy niechłodzony czujnik bolometryczny z tlenku wanadu. Ten bardzo czuły przetwornik termowizyjny wyposażono w atermiczny obiektyw stałoogniskowy, który zachowuje idealną równowagę między rozległością pola widzenia a maksymalnym zasięgiem wykrywania. Regulowane przez użytkownika ustawienia kontrastu i wzmocnienia umożliwiają operatorom optymalizowanie obrazu pod kątem zapewnienia sygnału wizyjnego o najwyższej jakości. Ponadto szeroki wybór trybów kolorów obrazowania termicznego umożliwia optymalizowanie obrazu termowizyjnego. Dostępne są wersje o rozdzielczości QVGA (320 pikseli) i VGA (640 pikseli) oraz o niskiej (<9 Hz) lub wysokiej (30 Hz) częstotliwości odświeżania.
W zależności od zastosowania i potrzeb można wybierać pomiędzy modułami z obiektywem o ogniskowej 50 mm, 19 mm oraz 9 mm.
Przetwornik wizyjny o rozdzielczości 1080p i częstotliwości odświeżania 60 Hz oparto na technologii Starlight. Pracuje w połączeniu z obiektywem o 30-krotnym zoomie optycznym i 12-krotnym zoomie cyfrowym, zapewniając wysoką jakość obrazu, świetnie odwzorowanie barw i niezrównaną czułość. Duży zakres dynamiki gwarantuje doskonałą wyrazistość obrazu w przypadku najbardziej wymagających scen o wysokim kontraście.

ALGORYTMY ANALIZY WIZYJNEJ

Kamera dualna MIC Fusion 9000i ma kilka wbudowanych funkcji analitycznych pozwalających na uruchomienie nawet 16 niezależnych i różnych reguł jednocześnie. Wśród standardowych reguł analitycznych znajdziemy przekroczenie linii, wejście w strefę, zmianę warunków wykrytego obiektu, wałęsanie, pozostawienie obiektu bez opieki lub jego zniknięcie itp. Ponadto wszystkie kamery Bosch, w tym MIC 9000i, mają funkcję klasyfikacji obiektów. Dzięki temu kamera jest w stanie wykrywać i klasyfikować obiekty w czterech grupach: osoby, samochody, motocykle/rowery i ciężarówki. Klasyfikacja ta wspomaga pracę operatora i doskonale uzupełnia całość systemu. Dzięki niej można ograniczyć fałszywe alarmy oraz budować zaawansowane scenariusze reakcji, biorąc pod uwagę typ zbliżającego się obiektu.
Kamera, klasyfikując zbliżający się obiekt jako osobę, może wysłać wiadomość na monitor operatora, wskazać miejsce pierwszej detekcji, wrysować w obraz trasę przemieszczania się i rozpocząć automatyczne śledzenie. Jednocześnie obiekty inne niż osoby mogą być pomijane w tym scenariuszu zadziałania lub ich detekcja może być tylko prezentowana poprzez wiadomość na monitorze operatora w oknie kamery lub panelu alarmowania.
MIC 9000i wyposażono też w algorytmy uczenia maszynowego – Camera Trainer. Ta funkcja bazująca na sieciach neuronowych pozwala na „douczenie się" nawet 16 dodatkowych reguł analitycznych. Uczenie polega na dostarczeniu pozytywnych próbek wykrywanego obiektu oraz negatywnych, będących swego rodzaju tłem obserwowanej sceny czy innymi obiektami. Reguły mogą działać jednocześnie z funkcjami podstawowymi. Dzięki temu można uruchomić nawet 32 różne reguły analityczne w jednej kamerze.

FUZJA METADANYCH

Zastosowanie dwóch modułów kamerowych na jednej głowicy ma też inną ważną zaletę – fuzję metadanych, czyli danych analitycznych. Kamera MIC Fusion 9000i pozwala na przekazywanie danych analitycznych pomiędzy dwoma modułami kamerowymi. Tam, gdzie „nie sięga" moduł wizyjny, bo obraz jest kiepskiej jakości, skutecznie może działać moduł termiczny (i analogicznie w odwrotnej sytuacji). Dzięki fuzji metadanych wszelkie wykryte obiekty, ich klasyfikacja, zachowanie czy trasy przemieszczania się są powiązywane z modułem zarówno wizyjnym, jak i termicznym.

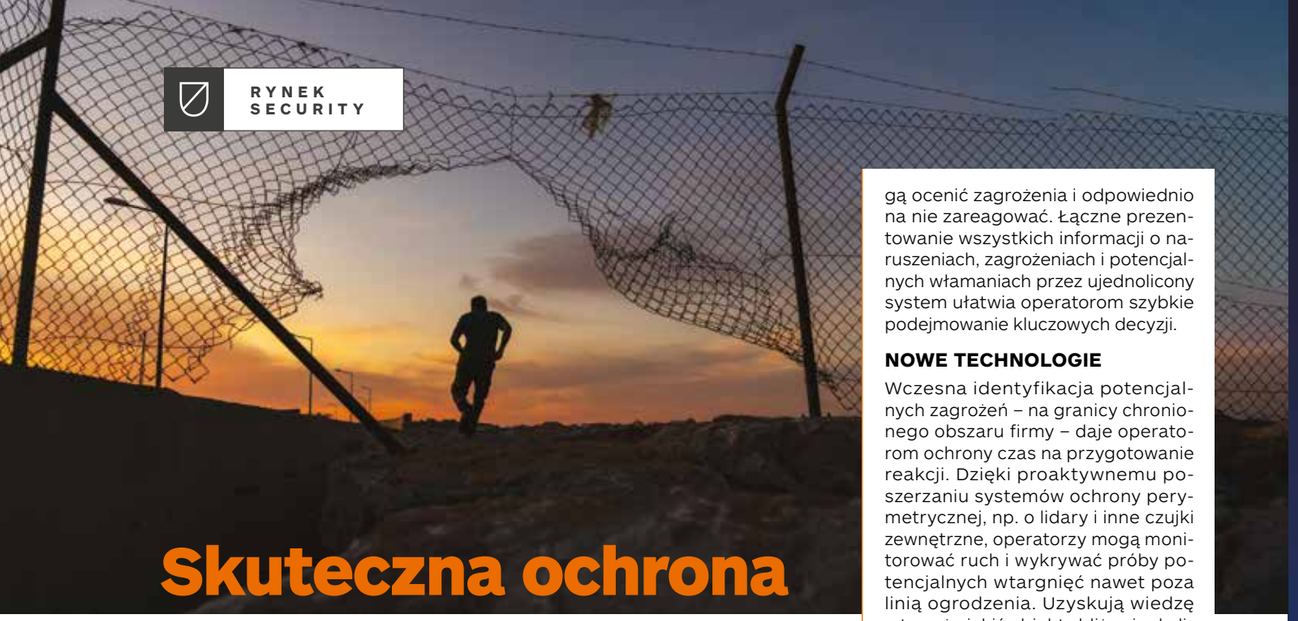
Fot. 2. Fuzja metadanych pomiędzy modułem wizyjnym a modułem termicznym

Takie rozwiązanie zdecydowanie poprawia skuteczność działania systemów monitoringu wizyjnego na dużych odległościach, a także przy niesprzyjających warunkach otoczenia.

SYSTEM ZARZĄDZANIA

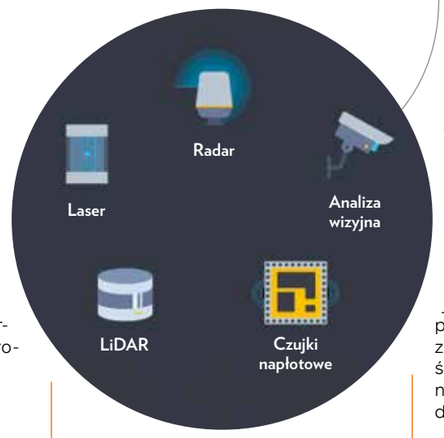
Dopełnieniem kamer MIC Fusion 9000i z funkcjami analitycznymi powinno być odpowiednie oprogramowanie wspierające oba moduły kamerowe, metadane z analityki wizji i oferujące dodatkowe funkcje, które można wykorzystać w ochronie obwodowej.
W ofercie Bosch takim rozwiązaniem jest BVMS *(Bosch Video Management System).* Oprogramowanie to pozwala na podłączenie do 2 tys. kamer w ramach jednego serwera, a do 200 tys. kamer w ramach rozproszonej infrastruktury serwer master i serwery podrzędne.
BVMS wspiera w pełni funkcje analityczne. Pozwala na obsługę zdarzeń analitycznych w czasie rzeczywistym, budowanie i wykonywanie zautomatyzowanych scenariuszy zadziałania (skrypty) oraz zarządzanie nimi z wielu poziomów stacji operatorskich. Wbudowana funkcja wyszukiwania postdowodowego umożliwia pracę z metadanymi *post factum.* Funkcja *Forensic search* działa bezpośrednio na metadanych wygenerowanych przez kamerę i zapisanych np. na macierzach ISCSI, dyskach wewnątrz rejestratorów Divar AiO lub kartach SD umieszczonych w kamerze. Umożliwia dodawanie nowych reguł analitycznych, wyszukiwanie na ich podstawie zdarzeń, klasyfikowanie obiektów. Wyszukiwanie postdowodowe obejmuje tylko metadane, dzięki czemu czas potrzebny na analizę kilku godzin zapisu jest ograniczony do minimum, co znacząco usprawnia pracę operatorów.
BVMS dostarcza także interaktywne mapy bazujące na mapach HERE, które mogą być używane w trybach online i offline. W ramach rozszerzenia funkcjonalności można je doposażyć w funkcję automatycznego śledzenia na mapach.
Połączenie kamer dualnych MIC Fusion 9000i oraz oprogramowania BVMS stanowi profesjonalne rozwiązanie do wykorzystania w ochronie obwodowej infrastruktury krytycznej, które może być rozbudowane o dodatkowe kamery czy elementy oprogramowania zarządzającego.
Elastyczność systemu, wzbogacona o szeroki wachlarz zabezpieczeń wbudowanych w kamery oraz zastosowanych w BVMS, czyni rozwiązanie Bosch skutecznym narzędziem do ochrony obwodowej obiektów infrastruktury krytycznej oraz wielu innych obiektów wymagających najwyższych standardów bezpieczeństwa.

BOSCH SECURITY AND SAFETY SYSTEMS
ul. Jutrzenki 105
02-231 Warszawa
e-mail: michal.mielczarek@pl.bosch.com



Skuteczna ochrona perymetryczna

Dla przedsiębiorstw działających na dużych obszarach, takich jak lotniska, zabezpieczenie granic terenu ma kluczowe znaczenie. Organizacja jest bardziej podatna na włamania mogące prowadzić do naruszenia bezpieczeństwa, jeśli pracownicy ochrony mają ograniczoną świadomość tego, co dzieje się w jej rozległym otoczeniu.



Wielu menedżerów ds. bezpieczeństwa zadaje sobie pytanie, jak skutecznie chronić granice firmy i zapobiegać ich naruszeniom. Naszą odpowiedzią jest wdrożenie jednolitego systemu bezpieczeństwa, a następnie włączenia nowych technologii jako części bardziej kompleksowej strategii ochrony obwodowej.

UJEDNOLICONE ROZWIĄZANIA

Brak zunifikowania swoich systemów zabezpieczeń na jednej platformie może prowadzić do powstawania luk informacyjnych lub niepełnego obrazu otoczenia. Aby te systemy działały w miejscach powiązanych ze sobą, ważne jest wprowadzenie ujednoliconego podejścia do krzyżowej kwalifikacji incydentów i alarmów o włamaniach. Zunifikowana platforma bezpieczeństwa pozwala łączyć w jednym miejscu dane zbierane przez różne systemy, zapewniając świadomość sytuacyjną niezbędną do zapewnienia bezpieczeństwa obiektów i ludzi. Przykładowo platforma Genetec™ Security Center o otwartej architekturze umożliwia połączenie systemów dozoru wizyjnego, kontroli dostępu, sygnalizacji włamania, komunikacji i automatycznego rozpoznawania tablic rejestracyjnych (ALPR) w celu lepszego zarządzania bezpieczeństwem firmy i skuteczniejszej ochrony obszaru jej działalności.

Poprzez moduł RSA *(Restricted Security Area)* platforma Security Center integruje się z coraz szerszą gamą technologii, wspierając zespoły ochrony w wykrywaniu potencjalnych zagrożeń na rozległych obszarach. Automatycznie śledzone ruchome cele są wyświetlane na mapach terenu, dzięki czemu pracownicy ochrony mogą ocenić zagrożenia i odpowiednio na nie zareagować. Łączne prezentowanie wszystkich informacji o naruszeniach, zagrożeniach i potencjalnych włamaniach przez ujednolicony system ułatwia operatorom szybkie podejmowanie kluczowych decyzji.

NOWE TECHNOLOGIE

Wczesna identyfikacja potencjalnych zagrożeń – na granicy chronionego obszaru firmy – daje operatorom ochrony czas na przygotowanie reakcji. Dzięki proaktywnemu poszerzaniu systemów ochrony perymetrycznej, np. o lidary i inne czujki zewnętrzne, operatorzy mogą monitorować ruch i wykrywać próby potencjalnych wtargnięć nawet poza linią ogrodzenia. Uzyskują wiedzę o tym, że jakiś obiekt zbliża się do linii granicznej, natomiast nie wiedzą, czy zagrożenie jest realne i jak poważne. Możliwość sprawdzenia, kto lub co zbliża się do ogrodzenia, pomaga pracownikom ochrony podejmować właściwe decyzje dotyczące koniecznych działań.

Ocena zdarzenia przy ogrodzeniu lub w innych obszarach o ograniczonym dostępie jest łatwiejsza, gdy pracownicy ochrony widzą, co dzieje się na miejscu incydentu. Klasyfikując zagrożenia wizualnie i pobierając odpowiednie dane z wielu systemów, mogą określić, czy wtargnięcie wymaga natychmiastowej reakcji. Skuteczny monitoring wizyjny wykorzystujący kamery o wysokiej rozdzielczości z oświetlaczami IR umożliwia operatorom ocenę zdarzenia i określenie działań odpowiednich do sytuacji.

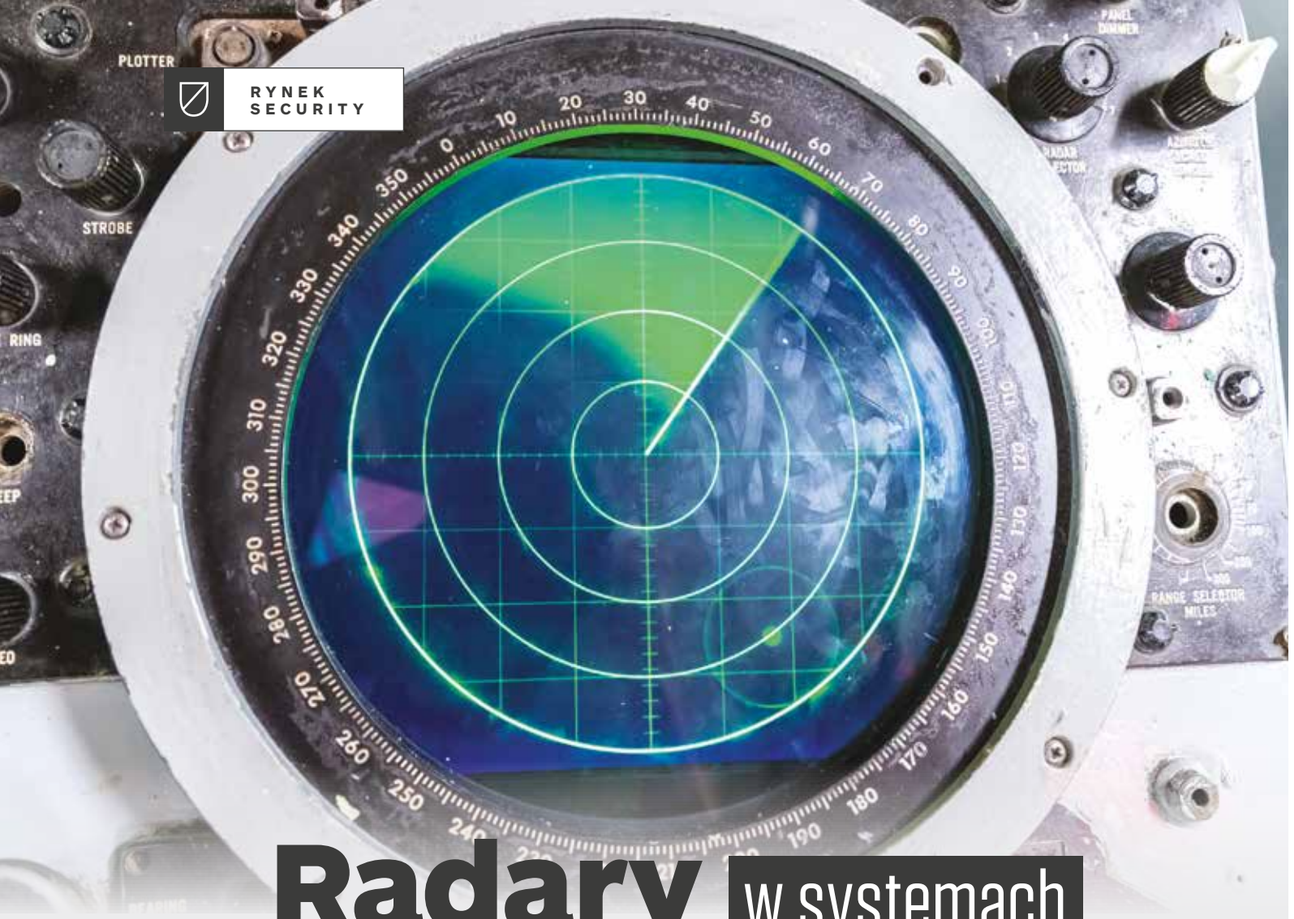
Operatorzy mogą również wykorzystywać systemy ALPR do skanowania tablic rejestracyjnych pojazdów oczekujących na wjazd, co pomaga określić poziom zagrożenia ze strony pojazdu. Przykładowo, jeśli numer rejestracyjny znajduje się na tzw. czarnej liście, operatorzy będą wiedzieli, jak zareagować.

WNIOSKI

W zapewnieniu skutecznej ochrony obwodowej najlepiej sprawdzi się podejście wielowarstwowe, które pozwoli rozszerzyć ochronę poza linię ogrodzenia. Wybierając ujednolicony system, w którym można zastosować wiele różnych nowych technologii, lepiej zabezpieczymy obiekty zarówno dziś, jak i w przyszłości.

GENETEC

2280 Alfred-Nobel Blvd.
Montreal, Canada H4S 2A4
www.genetec.com
jkozak@genetec.com



Radary i lidary w systemach zabezpieczeń

Jan T. Grusznic

Postęp w technologii niewizualnej, reprezentowanej przez radary i lidary, wywiera zauważalny wpływ na branżę bezpieczeństwa fizycznego. Oba rozwiązania zyskują na popularności jako realna alternatywa wykrywania zagrożeń wzdłuż rozległych granic terenu i na dużych obszarach.

Skuteczność systemu ochrony zależy w głównej mierze od jego zdolności do szybkiego wykrycia intruza. Jest to szczególnie ważne w przypadku zabezpieczania dużych obszarów lub terenów, gdzie incydenty związane z nieautoryzowanym wtargnięciem często są trudniej wykrywane. Radary i lidary mogą stanowić w tym względzie niebagatelne wsparcie.

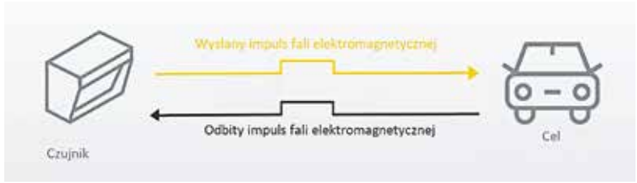
ZASADA DZIAŁANIA

Pojęcie RADAR było pierwotnie akronimem określenia ***RA****dio* ***D****etection* ***A****nd* ***R****anging* (wykrywanie i wyznaczanie odległości za pomocą fal radiowych). Technologia radarowa polega na wykorzystaniu fal radiowych do wykrywania obiektów i określania ich odległości od źródła wysłanego sygnału. Kiedy sygnał radarowy trafia na obiekt, jest zazwyczaj odbijany i rozpraszany w wielu kierunkach. Niewielka jego część jest odbijana z powrotem do urządzenia radarowego, gdzie jest wykrywana przez odbiornik. Wykryty sygnał zawiera informacje, na których podstawie można określić lokalizację, wielkość i prędkość poruszania się obiektu, od którego odbiła się fala radiowa[1].

Li*ght* ***D****etection* ***A****nd* ***R****anging* – LiDAR to technologia teledetekcji oparta na falach świetlnych: wiązka lasera podczerwonego jest emitowana w przestrzeń przez li-

1) *Radary w systemach dozoru. Aspekty techniczne i dotyczące działania*, Biała księga, Axis Communications AB, listopad 2021

Rys. 1. Zasada działania ToF (źródło: https://www.blickfeld.com)



dar, a następnie mierzony jest czas, w jakim po odbiciu od napotkanego obiektu powraca do źródła, co pozwala obliczyć odległość od emitera do obiektu. W przeciwieństwie do fal radiowych wiązki laserowe nie ulegają rozproszeniu po odbiciu i podczas powrotu do skanera (taka jest ich natura). Posiadając LiDAR o kącie widzenia 360° uzyskiwanym przy użyciu np. obracającego się lustra możliwe jest uzyskanie tzw. chmury punktów otoczenia (zestaw punktów opisujących obiekt lub powierzchnię). W oprogramowaniu z uzyskanych danych tworzony jest obraz 3D, odwzorowujący otoczenie wraz z obiektami z ich precyzyjnym położeniem w przestrzeni.

Radar działa w podobny sposób jak lidar, z tą różnicą, że zamiast światła laserowego lub LED wykorzystuje fale radiowe. Przesyła je z anteny (obrotowej lub stałej) i mierzy czas przelotu odbitego sygnału. Metoda ta, nazwana *Time-of-Flight* (ToF) jest standardem w branży, chociaż popularność zyskuje metoda fali ciągłej modulowanej częstotliwościowo – FMCW *(Frequency-Modulated Continuous-Wave)*.

Urządzenia bazujące na metodzie ToF pracują na zasadzie wysyłania w przestrzeń impulsów elektromagnetycznych i odbiorze tych impulsów po ich odbiciu od napotkanych na swojej drodze obiektów, celów *(rys. 1)*. Mierząc czas pomiędzy wysłaniem a odbiorem sygnału, można określić odległość do celu. Dla zachowania odpowiedniej rozdzielczości odległościowej stosuje się bardzo krótkie impulsy, co jednak dla uzyskania wymaganego zasięgu zmusza do zastosowania wysokiego poziomu mocy (zdolność wykrywania celów zależy od energii sygnału – im więcej energii odbije się od obiektu, tym większe prawdopodobieństwo jego wykrycia na tle szumów). Z kolei moc, z jaką można wysyłać silnie skoncentrowane impulsy, jest ściśle ograniczona przez przepisy prawa[2] i normy[3].

W metodzie FMCW odległość oblicza się nie na podstawie pomiaru czasu (jak w ToF), ale pomiaru częstotliwości odebranego sygnału *(rys. 2)*. W tym celu nadajnik urządzenia FMCW emituje falę elektromagnetyczną zmodulowaną częstotliwościowo przebiegiem piłokształtnym (w czasie jednego okresu modulacji częstotliwość nadawanego sygnału sinusoidalnego narasta liniowo, by następnie bardzo szybko powrócić do wartości początkowej). Przyjęcie takiego trybu pracy powoduje, że moc średnia nadajnika pracującego na fali ciągłej jest równa jego mocy szczytowej. Umożliwia to pracę z bardzo niskimi poziomami mocy bez pogorszenia zdolności detekcji celów. Pomiar odległości do celu odbywa się przez porównanie częstotliwości odebranego sygnału z częstotliwością początkową. Im dalej znajduje się obiekt, tym ta większa jest różnica[4].

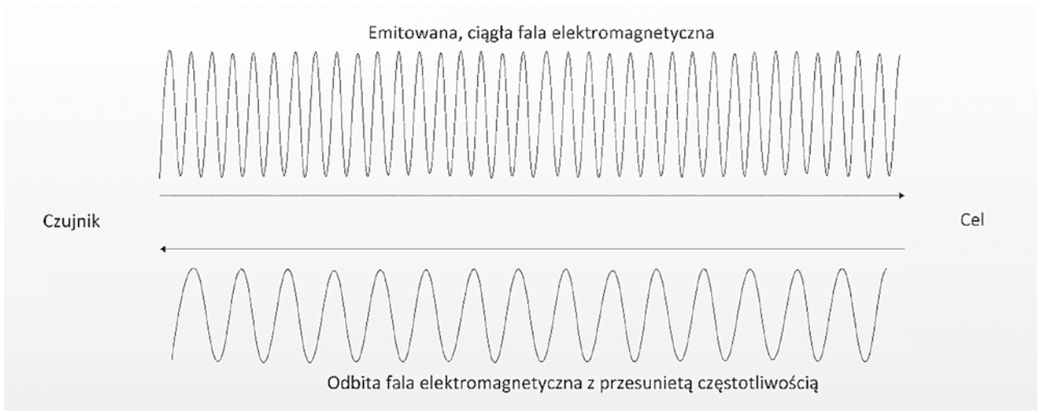
ZASTOSOWANIE

Na prawidłowe działanie lidarów i radarów natężenie światła nie ma wpływu, dzięki czemu oba rozwiązania doskonale nadają się do zastosowań zarówno z bardzo jasnym tłem, jak i w całkowitej ciemności. W takich warunkach mogą stanowić niezwykle cenne uzupełnienie systemu dozoru wizyjnego. Mimo że z reguły kamery termowizyjne z funkcją analizy również spełniają swoje zadanie, techniki niewizualne dostarczają więcej danych o obiekcie, przy niższych kosztach eksploatacji, a ich obszar detekcji jest znaczenie szerszy.

Potwierdza to Jakub Sobek z RCS Engineering: *– Technologia radarowa jest szczególnie przydatna na rozległych terenach,*

2) Rozporządzenie Ministra Cyfryzacji z 9 lutego 2022 r. w sprawie urządzeń radiowych nadawczych lub nadawczo-odbiorczych, które mogą być używane bez pozwolenia radiowego (Dz.U. 2022 poz. 567)
3) Na przykład PN-EN 60825-1:2014-11 - Bezpieczeństwo urządzeń laserowych -- Część 1
4) J. Miłosz, P. Paprocki, S. Plata: *Radary ze zmodulowaną częstotliwościowo falą nośną do wykrywania celów nawodnych*, „Nowa Technika Wojskowa" nr 9/2011

Rys. 2. Zasada działania FMCW (źródło: https://www.blickfeld.com)



gdzie chcemy wykrywać, lokalizować i śledzić obecność wielu celów jednocześnie. Jedno urządzenie pozwala zapewnić pokrycie 360 stopni nawet na bardzo dużych obszarach.
Artur Nowakowski z Linc Polska zwraca uwagę, że *w przypadku radaru mamy jeden punkt instalacji pokrywający powierzchnię nawet 300 000 m². Radary mogą być z powodzeniem stosowane zarówno na lądzie, jak i na wodzie; do ochrony dużych zbiorników wodnych w zasadzie nie ma alternatywy.*
Żadna inna technologia nie jest tak skuteczna w ochronie rozległych, otwartych, płaskich obszarów. Jak zaznacza Kazimierz Bulandra z KABE Systemy Alarmowe, *do skutecznej ochrony powierzchni lotniska zazwyczaj wystarczą 2 – 3 jednostki radarowe, co jest kosztowo równoważne perymetrii mikrofalowej czy kabla sensorycznego, a wielokrotnie bardziej skuteczne, bo chroni cały obszar.*

Jednym z zastosowań radarów jest ich wykorzystanie w systemach detekcji dronów. *Pozwala to na skuteczną ochronę infrastruktury krytycznej, ale coraz częściej wykorzystywane jest także w obiektach, których właścicielom zależy na zachowaniu prywatności* – komentuje Jakub Sobek. – *Taka informacja o lokalizacji drona jest przekazywania w przestrzeni 3D, co ułatwia jego precyzyjną lokalizację i śledzenie. W połączeniu z systemem zakłócającym, można w bardzo szybko zareagować na zbliżające się do obiektu zagrożenie.*
Z kolei Mariusz Ostapiuk z Pilz Polska zauważa, że technika radarowa może być również z sukcesem używana w aplikacjach bezpieczeństwa maszyn, gdzie często kurtyny bezpieczeństwa czy skanery laserowe się nie sprawdzają. – *Dzieje się tak wtedy, gdy warunki panujące podczas procesu produkcyjnego uniemożliwiają stosowanie urządzeń optoelektronicznych z powodu pyłu, wiórów przy obróbce drewna, wysokiej temperatury, refleksów świetlnych przy spawaniu.*
W miejscach wymagających dużej dokładności wykrycia obiektów w ustalonych granicach sprawdzają się lidary, które zapewniają dokładne pomiary odległych celów. Jacek Wójcik z Optex Security podpowiada, że technologia ta umożliwia wdrożenie zaawansowanych technik bezpieczeństwa, takich jak niestandardowe granice cyfrowe, wirtualne bariery lub wdrożenie dopracowanego systemu wykrywania włamań na obwodzie.
– *Oprogramowanie lidaru pozwala na „rysowanie" stref alarmowania, można „zasłonić" tylko okna i drzwi na konkretnej ścianie lub ustawić oddzielne strefy alarmowania np. na każdym piętrze budynku* – mówi J. Wójcik. Bardziej zaawansowane modele umożliwiają ustawienia pewnej logiki działania już w urządzeniu. – *Alarm jest wysyłany, jeżeli jedna strefa zostanie naruszona przez określony czas, a następnie zostaje naruszona kolejna strefa, co można zastosować do wykrywania tylko dużych pojazdów* – dodaje.
Lidar pozwala określić, w jakim kierunku cel jest zwrócony. Wizualizacja danych w oparciu o to rozwiązanie jest bardzo szczegółowa, umożliwiając dokładne przewidywanie, w którą stronę uda się dana osoba lub pojazd. System oparty na lidarach może również monitorować całą posiadłość i tworzyć szczegółowy model 3D otoczenia w celu śledzenia osób i obiektów. Technologia ta doskonale nadaje się do śledzenia ludzi w zatłoczonych środowiskach, nie zbierając przy tym informacji o ich tożsamości. Od budynków firmowych po sale koncertowe, lidary mogą skutecznie kontrolować i liczyć osoby przechodzące przez wejście, umożliwiając w ten sposób skuteczną kontrolę dostępu i zarządzanie tłumem[5].

OGRANICZENIA

Niewątpliwą zaletą podnoszoną przez naszych ekspertów jest wysoka odporność radarów na zakłócenia spowodowane warunkami atmosferycznymi, takimi jak mgła czy opady śniegu lub deszczu. Kazimierz Bulandra, bazując na swoim doświadczeniu w zabezpieczaniu obiektów infrastruktury krytycznej, m.in. lotnisk, za pomocą techniki radarowej ostrzega jednak, że *bardzo obfite opady deszczu lub śniegu mogą ograniczyć zasięg o ok. 30%* i radzi zastosować jednostkę radarową o takim zasięgu, żeby nawet w takich ekstremalnych warunkach była nadzorowana cała chroniona powierzchnia. Inaczej sprawa ma się z lidarami – mgła, niewielki deszcz, a nawet kurz mogą łatwo wpłynąć na działanie tego urządzenia.
Fale świetlne w lidarach mają niewielką długość (są to fale z zakresu podczerwieni), mniejszą niż jedna milionowa metra, co oznacza, że są łatwo odbijane przez krople wody w powietrzu. W efekcie intensywny deszcz znacząco zakłóci pracę tego detektora. Choć obecnie lidary są wyposażone w algorytmy znacząco podnoszące skuteczność działania w warunkach opadów, to w scenariuszach przewidujących ich wysoką intensywność zaleca się stosowanie tych rozwiązań wraz z urządzeniami wspomagającymi, takimi jak kamery lub czujki ultradźwiękowe, a nawet zmianę montażu lidaru (np. tworzenie wirtualnej ściany – montaż pionowy).
W przypadku radarów długość fal radiowych dochodzi do około 5 cm (praca w pasmie C – 5.650 ÷ 5.925 GHz), co oznacza, że po prostu przenikają przez krople wody we mgle, deszczu, śniegu, a nawet przez ziarna piasku. Rozdzielczość radarów ustępuje jednak lidarom, co widoczne jest zwłaszcza wtedy, gdy kilka obiektów znajdzie się bardzo blisko siebie. Na przykład radar może traktować dwa małe samochody w pobliżu jako jeden duży pojazd i wskazywać nieprawidłową odległość.
Jak zauważa Jarosław Sapko z Axis Communications, *rozwiązania oparte na technologii radarowej nie sprawdzą się w zatłoczonych miejscach, nie pozwolą też potwierdzić, która osoba ma prawo przebywać w tej strefie.*
Mariusz Ostapiuk podkreśla natomiast istotną rolę dobrze zaprojektowanej strefy detekcyjnej i pokrycie pełnego obszaru zagrożenia: – *Urządzenia radarowe mają swoje ograniczenia, jeśli chodzi o wielkość strefy chronionej i czas zadziałania, co należy uwzględnić projektując rozmieszczenie czujników.*

DOBRE PRAKTYKI

Radary i lidary wykorzystywane w elektronicznych systemach zabezpieczeń mogą być stosowane jako autonomiczne urządzenia wykrywające, a ich funkcjonalność można rozszerzyć, dodając do systemu kamery dostarczające obraz wizyjny. Radary są na ogół zalecane do instalacji zewnętrznych, podczas gdy lidary są w tym zakresie bardziej uniwersalne i mogą być używane zarówno w pomieszczeniach, jak i przestrzeniach zewnętrznych. Oba rozwiązania poprawiają skuteczność detekcji w wymagających warunkach, minimalizując ryzyko występowania fałszywych alarmów, pod warunkiem że stosujemy się do dobrych praktyk.
Jarosław Sapko przypomina, że *w przypadku technologii radarowej trzeba pamiętać, iż jest ona czuła na odbicia od różnych powierzchni, a zwłaszcza metalowych. Zatem efekt pracy radarów najlepiej widoczny jest podczas montażu na dużych płaskich przestrzeniach lub słupach, gdy dozorowana przestrzeń ma jak najmniej przeszkód.*
Widoczność obiektu na radarze zależy od jego skutecznej powierzchni odbicia (*Radar Cross Section*, RCS). Wartość liczbowa tego parametru, obliczana na podstawie informacji o rozmiarze, kształcie i materiale obiektu, ostatecznie determinuje jego wielkość na radarze. RCS człowieka wynosi z reguły od 0,1 do 1,0 m², ale jest to również typowa wartość RCS zgniecionej metalowej puszki po napoju, która chociaż znacznie mniejsza, jest lepiej widoczna dla radaru.
Z kolei Artur Nowakowski zwraca uwagę na lokalizację i montaż radaru: – *Podobnie jak w przypadku systemów wizyjnych, aby radar widział intruza, musi on znajdować się w jego polu widzenia. Nie może być przesłonięty przez drzewa czy krzaki, budynki, wzniesienia terenu czy schowany w zagłębieniu terenu, w takim przypadku dany obiekt nie będzie widoczny.*
Jednocześnie wymienia trzy parametry pozwalające tak ustawić system w terenie, aby detekcja była skuteczna na całym chronionym obszarze. Są to: *pole widzenia, zasięg i kąt pokrycia. Kwesta zasięgu jest sprawą oczywistą. Kąt pokrycia w poziomie i w pionie jest istotny, ponieważ ma on realny wpływ na zasięg. Mając odpowiednio duży kąt pokrycia w pionie, można zastosować radar na nierównym czy nawet górzystym terenie.*
Radar lub lidar powinny być umieszczone na wysokości gwarantującej, że wszystkie istotne cele będą „oświetlone" wiązką elektromagnetyczną. W ten sposób uzyska się optymalną wydajność. Bardzo ważnym elementem jest zapewnienie stabilnego miejsca instalacji, bez drgań lub kołysania, np. na sztywnym słupie, kratownicy lub ścianie.
Jacek Wójcik radzi, by miejsce montażu lidaru było odsunięte jak najdalej od rynien, daszków, klimatyzatorów umieszczonych na budynkach, czy krzewów, słupów, poprzecznych płotów itp. znajdujących się w linii ogrodzenia. *Zdarza się, że korona z drutu ostrzowego znajduje się w zasięgu działania lasera, po-*

5) *LiDAR in Security Applications – A Game Changer*, Florian Petit 20/01/2021, https://www.blickfeld.com/blog/lidar-in-security-applications/ [dostęp 04.04.2022]

wodując zakłócenia jego działania. Należy pamiętać, żeby linię styku lasera z podłożem czy poprzeczną ścianą „odsunąć" w oprogramowaniu od fizycznej granicy, która może powodować zwiększony „szum" i obniżyć skuteczność działania w tych miejscach.
Również na właściwą lokalizację montażu wskazuje Kazimierz Bulandra: – *Jednostki radarowe należy tak lokalizować, żeby jak największa część obszaru chronionego była dla nich widoczna, żeby nie przesłaniały jej „cienie" budynków, budowli itp. W przypadku ochrony lotnisk trzeba uwzględnić postój samolotów rzucających takie cienie. Ponieważ obszar nadzoru można dowolnie kształtować w ramach zasięgu radarów, trzeba wyciąć z nadzoru ścieżki poruszania się ochrony, dostaw itp.* Jednocześnie przestrzega, aby unikać umieszczenia radaru w pobliżu ekranów mogących silnie odbijać fale radarowe i prowadzić do zakłóceń odbioru.

PODSUMOWANIE

Jak podkreśla Kazimierz Bulandra, technologia niewizualna detekcji obecności obiektów wymaga wiedzy eksperckiej, którą dysponują nadal nieliczne firmy: – *Istnieje potrzeba przełamania pewnych schematów myślenia, co zawsze jest trudne wobec dążenia ludzi do stosowania znanych sobie technologii.* Jeszcze do niedawna większość radarów oferowała bardzo duży dystans detekcji i, jak zauważa Jakub Sobek: *Cena tych rozwiązań była bardzo wysoka. Od pewnego czasu dostępnych jest coraz więcej radarów krótkiego zasięgu w znacznie niższych cenach. Krótki zasięg sprawia, że obszar ich zastosowań znacznie się zwiększył, a koszt nie odstrasza już inwestorów.*
Na rosnącą popularność omawianych rozwiązań zwraca uwagę Jarosław Sapko, podkreślając jak ważne są szkolenia: – *Edukacja i wzrost świadomości o możliwościach wykorzystania tej technologii, przedstawione w formie przykładów udanych wdrożeń opartych na tej technologii, są sprawą kluczową.*
W podobnym tonie wypowiada się Artur Nowakowski: – *Nadal dla wielu osób z branży security rozwiązania radarowe są materią obcą, nie do końca zrozumiałą, dlatego kładziemy duży nacisk na szkolenia i prezentacje radarów w warunkach rzeczywistych. Edukacja w tym zakresie i pokazy na żywo są najlepszą demonstracją skuteczności tych rozwiązań.*

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.

LINC POLSKA

www.linc.pl

MAGOS | SR-150 – najnowszy radar

PORTFOLIO MARKI MAGOS ZOSTAŁO POSZERZONE O RADAR SR-150. JEST ON DEDYKOWANY DO ZABEZPIECZENIA NIEWIELKICH OBIEKTÓW O ZNACZENIU STRATEGICZNYM.

Duży zakres i dokładność działania oraz niskie zużycie energii (<3 W), połączone z niewielkim rozmiarem i masą sprawiają, że znajduje on zastosowanie w wielu projektach.
Inne cechy radaru SR-150:

- detekcja do 150 m,
- wykrywanie w kącie 120° (w poziomie) x 30° (w pionie),
- pokrycie działaniem szerokiego obszaru do około 23 500 m²,
- zasilanie PoE,
- skuteczność - zminimalizowanie liczby fałszywych alarmów z klasyfikacją obiektów opartą na algorytmach sztucznej inteligencji (integracja z MASS + AI),
- integracja z większością platform VMS,
- auto PTZ slew-to-cue zintegrowane z większością popularnych modeli kamer typu PTZ,
- wysoka wydajność działania i mała ilość danych dzięki przetwarzaniu brzegowemu pozwalają na bezprzewodowe przesyłanie danych oraz użycie zasilania solarnego,
- łatwa instalacja i uruchomienie dzięki automatycznemu kreatorowi MASS Wizard.

Wszystkie te cechy, w połączeniu z dużą dokładnością jego działania, praktycznie w każdych warunkach atmosferycznych (24/7) sprawiają, że radar SR-150 znajduje zastosowanie w wielu obszarach, w tym w energetyce, rafineriach paliw, w wirtualnym ogrodzeniu, w centrach danych, na lotniskach czy farmach solarnych. A to tylko przykładowe możliwości jego wykorzystania.
SR-150 doskonale uzupełnia szeroką ofertę marki MAGOS, która obejmuje radary o rożnych zakresach pracy, w tym np. znany SCEPTER-C.
Pełna oferta dostępnych modeli radarów na www.linc.pl

AXIS COMMUNICATIONS

www.axis.com/pl

AXIS D2110-VE z zaawansowaną technologią radarową

AXIS D2110-VE SECURITY RADAR TO INTELIGENTNE URZĄDZENIE SIECIOWE, KTÓRE WYKORZYSTUJE ZAAWANSOWANĄ TECHNOLOGIĘ WYKRYWANIA ZAPEWNIAJĄCĄ OCHRONĘ OBSZARU Z POKRYCIEM (KĄTEM WIDZENIA) 180° PRZEZ CAŁĄ DOBĘ PRZY NISKIM ODSETKU FAŁSZYWYCH ALARMÓW.

Dzięki wbudowanym funkcjom analitycznym idealnie nadaje się on do dozoru różnych rozległych instalacji zewnętrznych, takich jak obszary przemysłowe lub parkingi i doki załadunkowe.
Dzięki zaawansowanej technologii radarowej AXIS D2110-VE podaje dokładne położenie wykrytego obiektu w różnych warunkach atmosferycznych – przez całą dobę, 7 dni w tygodniu.
Wbudowane funkcje analizy opracowane przy wsparciu metod uczenia maszynowego i głębokiego radar umożliwiają dokładne wykrycie poruszających się obiektów, klasyfikowanie ich i śledzenie osób oraz pojazdów. Radar może również podawać prędkość poruszającego się obiektu.
AXIS D2110-VE zapewnia kompleksową ochronę dzięki polu widzenia 180° w poziomie. Może wykrywać osoby w odległości do 60 m (200 stóp) i pojazdy w odległości do 85 m (280 stóp). Funkcja inteligentnego współdziałania umożliwia zastosowanie wielu radarów blisko siebie. Dwa radary zamontowane tyłem do siebie dają pełne pokrycie 360°, co pozwala wykrywać pojazdy na powierzchni ponad 22 tys. m² (240 tys. ft²).
Urządzenie ma zaawansowane funkcje bezpieczeństwa zapobiegające nieautoryzowanemu dostępowi i zabezpieczające system. Podpisane oprogramowanie sprzętowe gwarantuje, że zainstalowano wyłącznie autoryzowane aplikacje i że pozostanie ono nienaruszone.
Radar ma również funkcję detekcji wstrząsów oraz czujnik otwarcia obudowy, które informują o próbach ingerencji w urządzenie.

Więcej na www.axis.com/pl

PILZ

www.pilz.com/pl-PL

Technologia radarowa PSENradar firmy Pilz do zabezpieczenia obszaru

W REALIZACJI ZABEZPIECZEŃ OBOWIĄZUJE ZASADA, ŻE SKANERY LUB KURTYNY ŚWIETLNE SĄ NAJLEPSZYM WYBOREM, GDY MOŻLIWE JEST ZASTOSOWANIE METOD OPTYCZNYCH I GDY URZĄDZENIE PRACUJE W CZYSTYM OTOCZENIU.

Kluczowe w podejściu do doboru zabezpieczenia jest właśnie stwierdzenie, czy możliwe jest zastosowanie metod optycznych. Jeśli odpowiedź nie jest twierdząca, to dobrym wyborem mogą być urządzenia w technologii radarowej PSENradar firmy Pilz.
Czujniki radarowe nie tylko dobrze znoszą trudne warunki pracy w miejscu zanieczyszczonym i zapylonym, ale są też doskonałym zabezpieczeniem, jeśli występują skrajne różnice temperatury i trudne warunki atmosferyczne (nawet mgła, opady śniegu i umiarkowanie intensywnego deszczu)

Technologie radarowe osiągają nieco niższą rozdzielczość i skuteczność wyznaczania krawędzi chronionego pola, a przy czasie reakcji ok. 100 ms reagują nieco wolniej niż skaner laserowy. Jednak ich sygnały mogą przenikać przez wszystkie materiały z wyjątkiem metalu i wody. Wpływ warunków otoczenia, które mogą powodować błędy w przypadku skanerów, dla systemów radarowych nie stanowią problemu. Dzieje się tak, ponieważ wykorzystują odbitą energię elektromagnetyczną i reagują na ruch.
Czujnik radarowy PSENradar swoim zasięgiem obejmuje dwa aspekty związane z bezpieczeństwem pracy: ochronę obszaru i ochronę przed przejściem za obszar chroniony.
Pierwszy gwarantuje, że po wejściu osoby w strefę zagrożenia maszyna zostanie przestawiona do stanu bezpiecznego. Natomiast ochrona przed przejściem za obszar chroniony zapobiega niezamierzonemu ponownemu uruchomieniu maszyny, gdy osoba nadal znajduje się w strefie zagrożenia.

Typowe obszary zastosowań można zatem znaleźć w przemyśle ciężkim, gdzie dominuje pył, opiłki, iskry spawalnicze lub rozbłyski jasnego światła. Technologia radarowa może być też z powodzeniem stosowana w przemyśle drzewnym, na liniach lakierniczych, w chłodniach lub odlewniach.

Więcej na https://www.pilz.com/pl-PL

Technologia LAN-RING w centralach alarmowych GALAXY DIMENSION

Tomasz Górski

Obiekty infrastruktury krytycznej w swoich wytycznych, opracowaniach technicznych, wymaganiach czy też normach „zakładowych" mają obowiązek stosowania urządzeń, elementów certyfikowanych i atestowanych pod kątem normy europejskiej EN50131 w stopniu 3. – GRADE 3. Gwarantuje to wysoką jakość dostarczanych urządzeń oraz, co cenniejsze, buduje świadomość konieczności stosowania rozwiązań zgodnych z wymaganiami inwestora. Na rynku jest duża różnorodność systemów I&HAS (SSWiN). Jednym z systemów certyfikowanych EN50131 GRADE 3 jest dystrybuowana od 25 lat przez firmę TAP Systemy Alarmowe rodzina central GALAXY, w tym GALAXY DIMENSION.

Centrale rodziny GALAXY DIMENSION mogą pracować w technologii światłowodowej. Magistrale systemowe można konwertować w standardzie *point-to-point* oraz RING z wykorzystaniem konwerterów marki MOXA lub switchy marki METEL.
Często spotykamy się z pytaniem: czy – przy założeniu, że inwestor wymaga urządzeń badanych, atestowanych i certyfikowanych dla poziomu GRADE 3 zgodnie z normą EN50131, a struktura obiektu wymaga konwersji RS485 CU (miedź) / FO *(fiber optic)* – stosowane i projektowane konwertery powinny mieć certyfikat GARDE 3 w rozumieniu EN50131? Dyskusja trwa...
Analizując sytuację, należy zauważyć, że konwerter FO bierze udział w realizacji najważniejszego toru transmisji w systemach bezpieczeństwa, a mianowicie magistrali systemowej, zapewniając stabilną komunikację pomiędzy jednostką centralną CA a podległymi rozproszonymi modułami RIO IN/OUT. Pojawiają się w tym momencie alternatywne rozwiązania:

1. Pierwsze, w którym inwestor rezygnuje z GRADE 3 dla urządzeń typu konwerter CU/FO TDW/RDW i problemu nie ma – projektujemy/dostarczamy konwertery FO sygnowane znakiem CE.
2. Drugie, w którym zamiast konwerterów FO point-to-point przechodzimy na technologię LAN-RING METEL, która ma certyfikat potwierdzony stosownymi badaniami zgodnie z GRADE 4 EN50131.

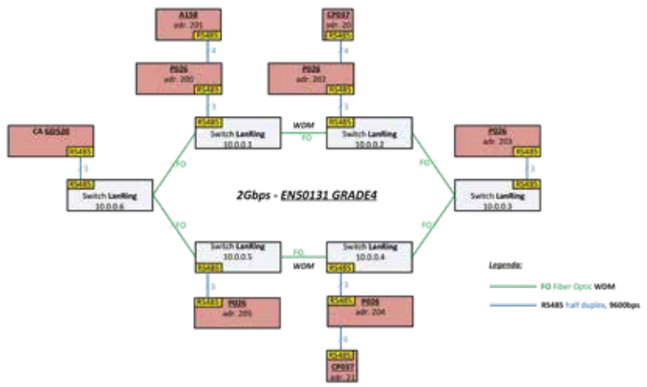
LAN-RING rozwiązuje cztery podstawowe problemy związane z projektowaniem oraz budową dużych, rozproszonych i niezawodnych systemów bezpieczeństwa. Dwa pierwsze to optoizolacja toru transmisji i technologia WDM[1], dwa kolejne to redundancja i certyfikat potwierdzony badaniami EN50131 Grade 4.

Dzięki stosowaniu LAN-RING problem utraty komunikacji pomiędzy CA a modułami rozproszonymi został całkowicie wyeliminowany. W przypadku uszkodzenia włókna pomiędzy dowolnymi switchami protokół LAN-RING automatycznie wyznacza switch „master", którego podstawowym zadaniem jest odbudowa transmisji z drugiego kierunku. Tym samym komunikacja RS4585 pozostaje ciągła i niezakłócona.

Podsumowując, LAN-RING EN50131 Grade 4 umożliwia certyfikację toru transmisji RS485-FO w stopniu 4., zapewnia pełną optoizolację toru RS485, co ma szczególne znaczenie w transmisji danych pomiędzy chronionymi budynkami zlokalizowanymi w ramach tego samego obiektu czy kompleksu. Dzięki WDM do komunikacji wykorzystujemy jedno włókno, a sama struktura ringu podnosi niezawodność działania systemu I&HAS i eliminuje całkowicie wady transmisji szeregowej RS485.

1 Technologia WDM (Wavelength Division Multiplexing) przeznaczona jest do zwielokrotniania przepustowości łącza poprzez przesyłanie, w jednym kanale fizycznym od kilku do kilkuset kanałów logicznych. Każdy z tych kanałów jest wydzielony poprzez różne długości fali.

Rys. 1. Uproszczony schemat budowy LanRing



Panel odbiorczy 2N® INDOOR VIEW

– urządzenie monitorujące i panel sterowania automatyką domową

Wewnętrzny panel odbiorczy 2N® Indoor View wzbogacono o funkcję monitorowania wizyjnego. Dzięki możliwości wysyłania poleceń za pomocą protokołu HTTP jednostka stała się sercem inteligentnego domu. Ulepszenia te są odpowiedzią na potrzeby mieszkańców luksusowych nieruchomości w trosce o ich bezpieczeństwo i wygodę.

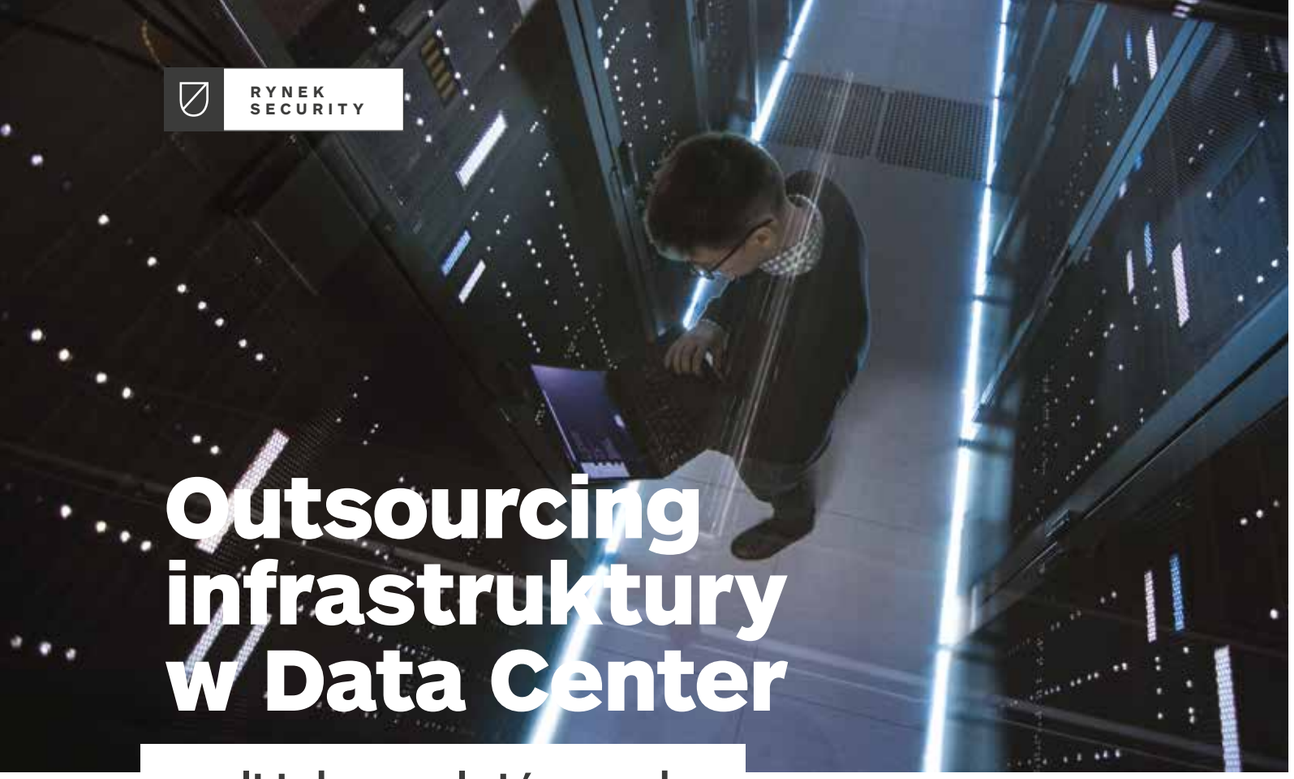
2N, lider globalnego rynku domofonów i systemów kontroli dostępu podłączonych do Internetu, zaktualizował 2N® Indoor View – jednostkę wewnętrzną dla ekskluzywnych budynków mieszkalnych – przeistaczając ją w urządzenie monitorujące oraz panel kontrolny zaawansowanych systemów automatyki domowej. Aktualizacja ma na celu sprostać wymaganiom mieszkańców luksusowych nieruchomości na całym świecie. Wygoda i bezpieczeństwo domu zawsze stanowią priorytet. Dlatego też postęp technologiczny przyczynił się do większej liczby próśb ze strony właścicieli nieruchomości o projektowanie urządzeń spełniających oba te wymagania.

NOWE OPROGRAMOWANIE 2N JEST NA NIE ODPOWIEDZIĄ. W REZULTACIE JEDNOSTKA 2N® INDOOR VIEW ZOSTAŁA ULEPSZONA NA TRZY SPOSOBY:

1. Możliwość podłączenia do czerech kamer IP. Nie ma potrzeby podłączania kamer IP do domofonu. Wystarczy, że zostaną one podłączone do tej samej sieci lokalnej co jednostka wewnętrzna. W ten sposób mieszkańcy mogą dalej używać zamontowanego w domu kolorowego siedmiocalowego dotykowego wyświetlacza 2N® Indoor View, aby monitorować korytarz, garaż i obszar za budynkiem.
2. Wykonywanie zdjęć podczas każdego wywołania domofonu. Wyobraź sobie, że w sąsiedztwie zanotowano szereg włamań. Podejrzewasz, że włamywacze mogą zadzwonić na domofon, aby sprawdzić, czy ktoś jest w domu. Domofon 2N® Indoor View automatycznie zrobi zdjęcia podczas każdego wywołania, uwzględniając nieodebrane połączenia, i doda je do rejestru połączeń.

Urządzenie wykona więcej niż jedną fotografię, jeśli osoba przy drzwiach odwróci się bokiem lub zasłoni kamerę w kluczowym momencie.

3. Funkcja sterowania automatyką domową. Urządzenie 2N® Indoor View umożliwia wysyłanie poleceń za pomocą protokołu HTTP. Pozwala to sterować urządzeniami automatyki domowej, tym samym, korzystając z jednostki wewnętrznej, można włączyć światła, odsłonić żaluzje czy wezwać windę.



Outsourcing infrastruktury w Data Center

czyli jak uwolnić zasoby firmowe i skupić się na działalności kluczowej

Jakie korzyści wiążą się z przeniesieniem infrastruktury firmowej do komercyjnego Data Center? Na to pytanie odpowiada firma Talex, posiadająca dwa ośrodki DC znajdujące się w Poznaniu i we Wrocławiu.

Ostatnie dwa lata zmieniły sposób funkcjonowania przedsiębiorstw na całym świecie. Pracownicy, których fizyczna obecność nie jest wymagana do wykonania powierzonych im obowiązków, są zachęcani do pracy z domu. Dodając do tego znaczny wzrost kosztów prowadzenia biznesu, coraz więcej polskich firm decyduje się na zredukowanie używanej infrastruktury firmowej i zajmowanej przestrzeni biurowej. Przeniesienie infrastruktury do Data Center rozwiązuje te problemy – nie tylko zwiększa poziom bezpieczeństwa i zapewnia ciągłość działania biznesu, ale też pozwala na precyzyjną predykcję kosztów utrzymania infrastruktury i większą elastyczność działań przedsiębiorstwa.

OŚRODKI DATA CENTER – CZYM CHARAKTERYZUJĄ SIĘ JAKO OBIEKTY

Data Center to ośrodki przetwarzania danych. Każdy z nas zastanawiał się nieraz, gdzie znajdują się informacje trzymane w chmurze. Zazwyczaj jest to właśnie przestrzeń wydzielona w DC. Pomieszczenia przechowujące infrastrukturę techniczną nazywamy kapsułami. W każdej z nich tworzy się optymalne warunki środowiskowe do pracy i żywotności sprzętu, wraz z systemami zapobiegającymi awariom, np. systemem gaśniczym, który wypompuje tlen z pomieszczenia, gasząc w ten sposób ewentualny pożar bez uszkodzenia infrastruktury technicznej. Oprócz tych systemów gaśniczych Talex Data Center są wyposażone w agregaty prądotwórcze ze zbiornikami paliwa zapasowego, zasilacze bezprzerwowe UPS, które w przypadku odcięcia prądu z sieci podtrzymują dostawę prądu do momentu pełnej gotowości operacyjnej agregatów, systemy klimatyzacji utrzymujące idealną temperaturę w kapsułach czy centrum nadzoru czuwające 24/7 nad stanem kapsuł i innych elementów infrastruktury.
Ośrodki DC uwzględniają bezpieczeństwo lokalizacji na etapie koncepcyjnym przed rozpoczęciem ich budowy. Idealne DC jest umiejscowione tak, by miało dostęp do dwóch niezależnych sieci energetycznych. Jest przygotowane na zalanie (odwodnienie terenu), budowane daleko od obszarów narażonych na powodzie, w lokalizacji poza ruchem powietrznym (katastrofy lotnicze) oraz z dala od centrum miejskich (rozprzestrzeniające się pożary). Takie podejście, nieco pesymistyczne, zapewnia najwyższy stopień bezpieczeństwa środowiskowego.

OCHRONA PRZED NAJWIĘKSZYM ZAGROŻENIEM

Pomimo licznych środków bezpieczeństwa, DC wciąż są narażone na wycieki danych. Dlatego dobór zabezpieczeń fizycznych i cybernetycznych o najwyższym standardzie odgrywa ogromną rolę w działalności takich firm jak Talex.
W celu uzyskania pełnej kontroli nad dostępem fizycznym należy zadbać o odpowiednią infrastrukturę bezpieczeństwa oraz odpowiedni system kontrolujący jej działanie. W Talex Data Center, oprócz systemów monitoringu CCTV, stosuje się również czytniki kart i skanery biometryczne systemu KD oraz zaawansowany system sygnalizacji włamania i napadu (SSWiN). Wszystkie te systemy są zintegrowane z platformą Nedap AEOS, zarządzającą rozbudowaną infrastrukturą fizycznych zabezpieczeń.
Producentem zarówno komponentów fizycznych, jak i oprogramowania integrującego AEOS jest Nedap Security Management. Talex zdecydował się podjąć współpracę z firmą Nedap nie tylko ze względu na możliwość pozyskania urządzeń i systemu zarządzającego od jednego zaufanego partnera, ale też mając na uwadze najwyższy standard dostarczanych usług, szerokie możliwości integracji AEOS z naszymi systemami czy udostępnianie naszym specjalistom wiedzy o systemie i jego instalacji.

– Ten ostatni punkt miał dla nas szczególne znaczenie, pozwalając naszym ekspertom na zdobycie nowych umiejętności i przeprowadzenie w 2018 r. samodzielnej implementacji systemu w naszym drugim, wrocławskim ośrodku Talex DC – wyjaśnia Maciej Puciński, architekt bezpieczeństwa fizycznego i automatyki budynkowej w Talex. I dodaje: – Tradycyjne układy bezpieczeństwa fizycznego, usiłując sprostać rosnącym oczekiwaniom użytkowników, dotarły do granicy swoich możliwości technologicznych. Nieustannie zwiększająca się ilość usług chmurowych, wirtualizacja serwerów, gwałtowny wzrost mobilności skłoniły specjalistów Talex do ponownego przemyślenia koncepcji funkcjonowania struktury ochrony fizycznej. Nedap dostarczył naszej firmie system, który umożliwia samodzielne zbudowanie na dużą skalę wymaganych struktur, co skutkuje oszczędnością czasu i sprawia, że system charakteryzuje się niższym współczynnikiem występowania błędów i wyższym współczynnikiem dostępności (Mean Time Between Maintenance – MTBM). Z kolei możliwość automatyzacji określonych obszarów pozwala obniżyć koszty operacyjne (OPEX – Operating Expenditures) ponoszone w procesach projektowania, wdrażania i uruchomienia systemu bezpieczeństwa fizycznego.

Mówiąc o ochronie danych, nie można pomijać aspektu cyberbezpieczeństwa. Ataki hakerskie stanowią duże zagrożenie bezpieczeństwa danych i wizerunku firmy (utrata zaufania klientów). Aby się przed nimi uchronić, DC podlegają ścisłej kontroli SOC *(Security Operations Center).* Przy użyciu systemów SIEM *(Security Information and Event Management)* eksperci w dziedzinie cyberbezpieczeństwa mogą na bieżąco monitorować logi aktywności w DC, zarządzając siecią i izolując podejrzane działania. W przypadku Talex Data Center, w celu dodania kolejnej warstwy zabezpieczeń, powołaliśmy zespół reagowania na incydenty bezpieczeństwa CSIRT *(Computer Security Incident Response Team),* proaktywnie analizujący możliwe incydenty i badający nowe rodzaje ataków cybernetycznych.

JAK KOMERCYJNE DC POMAGAJĄ PRZEDSIĘBIORSTWOM

Usługą najczęściej świadczoną przez komercyjne Data Center jest kolokacja sprzętu fizycznego w ośrodku przetwarzania danych. Odpowiednio zabezpieczona infrastruktura energetyczna wyklucza możliwość wystąpienia przerwy w działaniu sprzętu umieszczonego w ośrodku, a zaawansowane systemy klimatyzacji zapobiegają ich przegrzaniu i awarii. Brak przerw w działaniu, wypadków przy pracy czy konieczności konserwacji sprzętu po wystąpieniu problemu pozwala dokładnie obliczyć koszty infrastruktury i lepiej zaplanować budżet.
Przeniesienie infrastruktury do dedykowanego DC uwalnia przedsiębiorstwa od konieczności inwestowania, utrzymania i obsługi sprzętu oraz budowy własnego centrum przetwarzania danych. Kolokację można rozszerzyć o usługę hostingu, czyli budowy i utrzymania kolejnej części infrastruktury przez ekspertów DC.
Drugą najczęściej wybieraną usługą jest *cloud computing.* Data Center mają własne potężne zasoby służące do przetwarzania danych. Wspomniana kolokacja pozwala zredukować koszty związane z inwestycją w nieruchomość. Analogicznie usługi chmurowe zmniejszają nakłady poniesione na sprzęt IT i oprogramowanie. DC dostarczają infrastrukturę potrzebną do korzystania z platform i programów udostępnianych w ramach usług chmurowych, a gdy konkretny zasób nie jest już potrzebny (lub potrzebny jest dodatkowy!), użytkownik może dostosować zakres korzystania z usługi.

NOWE PODEJŚCIE BIZNESOWE

Sposób prowadzenia biznesu ewoluuje. Pandemia COVID-19 zmuszała pracowników do pracy zdalnej. Trudności logistyczne dotknęły wiele firm, szczególnie te związane z obsługą sprzętu fizycznego, dostępem do kluczowych informacji i zasobów przedsiębiorstwa. Awaria serwera była i wciąż jest w stanie sparaliżować pracę całej organizacji.
Właściciele Data Center, tacy jak Talex, oferują swoim partnerom biznesowym usługi kolokacji i *cloud computing* – chroniąc przed awariami infrastruktury i zabezpieczając dane w przypadku kolokacji oraz umożliwiając elastyczne dostosowywanie zasobów używanych przez przedsiębiorstwa na platformach wirtualizacyjnych. Dzięki temu nawet w warunkach pracy zdalnej specjaliści mogą korzystać z najnowszych technologii i potężnej mocy obliczeniowej. Firmy wspierane przez DC nie muszą martwić się o swoją infrastrukturę techniczną. Zamiast tego mogą całą uwagę poświęcić działalności kluczowej przedsiębiorstwa.

Geutebrück stawia na Polskę!

mówi Jeroen Mollé, dyrektor handlowy na Europę w firmie Geutebrück

Niewiele osób wie, że firma Geutebrück jest firmą rodzinną…
Rzeczywiście, firmą zarządzają obecnie Katharina Geutebrück i Christoph Hoffmann, którzy są już drugim pokoleniem na czele przedsiębiorstwa. Przez pół wieku ta niemiecka marka dała się poznać jako producent wysokiej jakości kamer, rejestratorów i oprogramowania do zarządzania systemami dozoru wizyjnego. Jesteśmy obecnie firmą globalną.
Działamy w atmosferze zaufania i wzajemnego zrozumienia – jak w firmie rodzinnej. Zatrudniamy pracowników na całym świecie, mamy filie i partnerów na pięciu kontynentach. Jesteśmy dumni, że ludzie wiążą z nami całą swoją karierę zawodową. W naszej firmie jest pracownik, który od niemal 45 lat jest z nami! Dzisiaj to nie zdarza się często… Wiele osób z długim stażem pracuje w dziale technicznym – ich wiedza i doświadczenie są dla nas bezcenne, są ekspertami dla pracowników wsparcia technicznego i działu sprzedaży.

Chciałbym jednocześnie podkreślić, że firma Geutebrück jest innowatorem na rynku. Nasze produkty nie są przeznaczone dla odbiorcy masowego, koncentrujemy się na ofercie dla użytkowników poszukujących rozwiązania spełniającego konkretne potrzeby, często bardzo wymagające. Trudno opracowywać innowacyjne produkty na potrzeby konkretnej niszy rynkowej. Mamy jednak bogatą ofertę rozwiązań, które możemy dopasować do indywidualnych wymagań użytkownika końcowego. Mówię tu przede wszystkim o naszym systemie VMS z sukcesem wdrażanym w nawet najbardziej wymagających projektach.
Naszą strategię można porównać do brania udziału w wyścigach samochodowych: aby wygrać, trzeba dopasować model samochodu do toru jazdy – my właśnie tak działamy: dopasowujemy rozwiązanie do specyficznych potrzeb. Proponujemy klientom dokładnie to, czego potrzebują, a rozwiązania dopracowujemy z uwzględnieniem konkretnych wymagań i oczekiwań. Dbamy także o odpowiednie szkolenie w zakresie obsługi systemu.

Na jakie rynki kierujecie swoje produkty?
Mamy bardzo dużo wdrożeń w logistyce, produkcji, obiektach infrastruktury krytycznej. Ale nasze rozwiązania można zastosować w zasadzie w każdym sektorze gospodarki – od galerii handlowych, przez banki, po zakłady karne.
Stosujemy model sprzedaży bezpośredniej, ponieważ chcemy mieć bezpośredni kontakt z klientem, proponować odpowiednie rozwiązanie do konkretnego wdrożenia. Jednocześnie chcę podkreślić, że nie koncentrujemy się tylko na sprzedaży. Zależy nam, by użytkownik końcowy rozumiał nasz produkt, umiał i lubił z niego korzystać przez wiele lat. Nie stawiamy na sprzedaż tylko dla zysku, za wszelką cenę. Zawsze szczegółowo omawiamy potrzeby klienta i dobieramy odpowiednie rozwiązanie. Na pierwszym planie stawiamy spełnienie oczekiwań i satysfakcję klienta, nie wielkość budżetu. W ten sposób działamy od wielu lat na rynku i widzimy, że dzięki takiemu podejściu klienci są wierni naszym rozwiązaniom i do nas wracają.

Jaki, oprócz Niemiec, jest wasz największy rynek?
Globalne działania firmy podzieliliśmy na trzy regiony. Pierwszym i naturalnym jest dla nas region DACHI, w którego skład wchodzą Niemcy, Austria, Szwajcaria i Włochy – tu jesteśmy najsilniejsi i najbardziej znani. Drugi region stanowi Europa, z wyłączeniem wspomnianych krajów DACHI, trzeci – nasza sprzedaż globalna poza Europę. Te trzy regiony działają podobnie: jesteśmy firmą rodzinną i tak traktujemy naszych pracowników i partnerów.
Oczywiście – jak to w rodzinie – dyskutujemy ze sobą, rywalizujemy, czasem się spieramy. Ale wszystko po to, by osiągnąć jak najlepszy efekt. Ważna jest dla nas także atmosfera pracy. Nie jesteśmy ogromną korporacją, więc wszyscy w firmie się znają, mówimy sobie po imieniu i rozmawiamy na różne tematy. W związku z pandemią zaszły oczywiście pewne zmiany, bo pracujemy częściowo zdalnie, ale nadal często spotykamy się online.

Jak budujecie sprzedaż w Polsce?
Nasza marka nie jest w Polsce powszechnie znana, ponieważ nie oferujemy produktów uniwersalnych skierowanych do masowego odbiorcy. Opracowujemy rozwiązania dopasowane do konkretnego wdrożenia. Dlatego docieramy do właściwego odbiorcy, a nie nastawiamy się na masową sprzedaż.
Obecnie z zespołem marketingu koncentrujemy się na bezpośrednich relacjach z użytkownikiem końcowym. Tu potrzebne są inne narzędzia niż w przypadku współpracy z tradycyjnymi dystrybutorami, którym wystarczą działania reklamowe, katalogi produktów czy wsparcie działu technicznego. Użytkownik końcowy oczekuje proaktywnej postawy, wsparcia eksperckiego i profesjonalnego doradztwa w zakresie konkretnego wdrożenia. W związku z tym wzmacniamy struktury naszych lokalnych przedstawicieli, którzy będą dbać o osobiste wsparcie klientów, słuchać ich potrzeb i proponować odpowiednie rozwiązania. W Polsce firmę Geutebrück reprezentuje w tym zakresie Artur Koman, który doskonale zna rynek i jego działanie.
W zależności od regionu świata stosujemy różne podejście marketingowe. Czasami decydujemy się na silną obecność w mediach społecznościowych, czasem stawiamy na udział w targach i konferencjach branżowych, innym razem organizujemy własne szkolenia i warsztaty. To, co działa w jednym kraju, nie zawsze sprawdza się w innym. Na rynek polski mamy już wiele pomysłów – na pewno o jakości i niezawodności rozwiązań Geutebrück będzie coraz głośniej…

Kamera 5 Mpix
G-Cam/
EWPC-5240
Dzięki zastosowanej technologii zapewnia doskonały obraz nawet w nocy.

Jaką strategię firma przyjęła na rynek polski?
Stawiając teraz na Polskę, nie szukamy jednak dystrybutorów, którzy głównie koncentrują się na sprzedaży. To nie wpisuje się w naszą filozofię działania. Chcemy pracować z integratorami, którzy mają już swoich klientów oraz pracowników z doświadczeniem i wiedzą techniczną, którzy znają nasze produkty i będą w stanie odpowiednio je zaprezentować i polecić użytkownikowi.
Co ważne, nie skupiamy się wyłącznie na wielkich integratorach. Mamy bardzo dobre doświadczenia także z firmami, które zatrudniają jedynie kilka osób, ale posiadają ogromną wiedzę ekspercką i wielu zadowolonych klientów. Ich sukcesy wynikają w dużej mierze z zaufania, jakim darzą ich użytkownicy – takich właśnie partnerów szukamy w Polsce. Nie ma dla nas znaczenia, czy firma zatrudnia setki pracowników, czy tylko kilku. Ważne, aby kierowała się filozofią działania podobną do naszej i oferowała najwyższą możliwą jakość.
Podstawą współpracy jest dla nas uczciwość wobec naszych partnerów i klientów, bo w ten sposób buduje się zaufanie, które procentuje. Czasami przegrywamy z konkurencją, głównie jeśli chodzi o cenę, ale niemal zawsze wygrywamy elastycznością podejścia i funkcjonalnością rozwiązania.

Gdyby miał Pan jednym zdaniem przekonać użytkownika do wyboru rozwiązania Geutebrück, co by Pan powiedział?
Jednym zdaniem będzie trudno… Ale wymienię najważniejsze atuty: oferujemy produkt na lata, dostosowany do oczekiwań użytkownika. Dbamy o to, żeby przed zaprezentowaniem klientowi rozwiązania poznać jego potrzeby, zrozumieć, przed jakimi wyzwaniami stoi, i wesprzeć go w implementacji. Oferujemy produkt przyszłościowy, który można modernizować i rozwijać w miarę potrzeb. Bazujemy na rozwiązaniach elastycznych, które można dowolnie komponować.
Jedną z zalet rozwiązań Geutebrück jest także możliwość integracji z produktami większości dostawców na rynku, a to jest dziś często sprawą kluczową. Zawsze słuchamy naszych partnerów i użytkowników końcowych, aby dostarczać im funkcjonalności, których rzeczywiście potrzebują.

Alicja automatyczny dyspozytor

Bartłomiej Dryja

W VII p.n.e. pewien Grek imieniem Hezjod w utworze *Narodziny bogów* wspomina o Talosie, mechanicznym strażniku Krety, stworzonym przez Hefajstosa. Ta sztuczna inteligencja miała strzec wyspy przed obcymi, pełniąc funkcję ruchomej „ochrony obwodowej". Musieliśmy czekać wiele stuleci, zanim marzenia o automatycznej ochronie zaczęły się powoli ziszczać. Stało się to możliwe dzięki dynamicznemu rozwojowi elektroniki i informatyki w drugiej połowie XX w.

Dziś dużo się mówi o sztucznej inteligencji, uczeniu maszynowym i automatyzacji, skupiając się na pracy z obrazem. Ma to swoje uzasadnienie. Z jednej strony mamy bowiem faktyczny problem do rozwiązania, ponieważ praca z obrazem jest pracochłonna i monotonna, czyli droga, jeżeli chcemy wykonywać ją profesjonalnie. Z drugiej zaś mamy gigantyczne budżety, jakie producenci CCTV przeznaczają na badania, walcząc o uatrakcyjnienie swoich produktów. Potrzeba klientów oraz nakłady gigantów na rozwój powodują szybki postęp w zakresie sztucznej inteligencji w tym wąskim obszarze. Pytanie, jakie sobie zadaliśmy, to czy gdzieś indziej w ochronie też jest miejsce na sztuczną inteligencję. **Czy kamery to jedyny obszar, gdzie AI może uwolnić człowieka od żmudnych czynności i zredukować koszty świadczenia usług?**

W NEXT! wierzyliśmy, że nie. Bazując na naszym ponad 20-letnim doświadczeniu, postanowiliśmy przesunąć granicę automatyzacji jeszcze dalej, oczywiście nie pomijając przy tym również zaawansowanej analityki obrazu.

Alicja to platforma do monitoringu, która ma za zadanie zautomatyzować obsługę alarmów – począwszy od odebrania sygnału z obiektu, poprzez powiadomienie właściwych osób i wysłanie patrolu, po zakończenie obsługi. Tylko w przypadku incydentów wykraczających poza standardową obsługę zdarzenie będzie kierowane do weryfikacji przez operatora człowieka. Pozwoli to jednej osobie czuwać nad wieloma tysiącami obiektów równocześnie.

PRACUJĄC NAD ALICJĄ I BUDUJĄC PODWALINY POD AUTOMATYCZNEGO OPERATORA, OPARLIŚMY SIĘ NA CZTERECH FILARACH

1. WIDEOPATROLE

Pomimo że w zakresie analityki obrazu zrobiono już wiele, a na rynku jest coraz więcej kamer i rejestratorów wyposażonych w zaawansowaną analitykę, postanowiliśmy rozwinąć Alicję także w tym obszarze. Zauważyliśmy, że m.in. operatorzy nadal spędzają całe godziny, wykonując wideopatrole. Prewencja, jaką zapewniają, jest istotnym uzupełnieniem analityki obiektowej. Pozwala wychwycić zarówno problemy techniczne, jak i próby sabotażu. Typowymi elementami poddawanymi kontroli są uszkodzenie lub celowe wyłączenie kamery, utrata ostrości, przysłonięcie lub zamalowanie obiektywu czy też obrócenie kamery.
Ponadto świadczone są usługi uzupełniające oparte na rozpoznawaniu obiektów, np. określonej liczby pojazdów parkujących na placu, samochodów o zadanych numerach rejestracyjnych, osób leżących w niedozwolonych miejscach zwanych powszechnie „śpiochami", zliczaniu klientów w sklepie o określonych godzinach. Kontrolę tych elementów przeprowadzają cyklicznie operatorzy w centrum monitoringu. Widząc to, zdecydowaliśmy się wbudować algorytmy AI w Alicję, aby zautomatyzować cały proces wideopatroli i tym samym uzupełnić analitykę obiektową. System teraz automatycznie sprawdza o określonych porach poszczególne kamery i raportuje operatorowi sytuacje odbiegające od założonych parametrów.

2. POWIADAMIANIE GŁOSOWE

Coraz większa liczba kanałów komunikacji z osobami upoważnionymi do odwoływania alarmów ciągle nie eliminuje potrzeby komunikacji głosowej z operatorem. Dlatego też obok całego wachlarza narzędzi, takich jak SMS, MMS, push, e-mail, aplikacji na smartfony czy też stron WWW, dodaliśmy wbudowany syntezator mowy i możliwość odbioru odpowiedzi. Dzięki temu Alicja zapewnia pełne spektrum dróg komunikacji. Teraz dla każdego obiektu można budować ścieżkę konwersacji, która pozwala nie tylko przekazać informację o zdarzeniu, ale także odebrać połączenie odwołujące alarm, zgłoszenie serwisu, sprawdzenie stanu obiektu oraz wywołać wiele innych reakcji, które do tej pory wymagały zaangażowania operatora.

Pracując nad Alicją oparliśmy się na **4** filarach

3. BIG DATA

Wiedzę o specyfice obsługi konkretnych obiektów operatorzy nabywają przez lata pracy w stacji monitoringu. Często korzystają z doświadczenia i kierują się intuicją, co w przypadku tego drugiego akurat nie zawsze jest pożądane. Dążąc do sytuacji, w której decyzje są podejmowane na podstawie sprawdzonych informacji i twardych danych oraz chcąc skrócić czas budowania wiedzy przez operatorów, wprowadziliśmy całą rodzinę analiz. Dostarczają one operatorowi nie tylko konkretnych informacji, takich jak dane osoby najczęściej odwołującej alarm, średni czas odwołania czy liczba fałszywych alarmów, ale także wyliczają prawdopodobieństwo prawdziwości zdarzenia na podstawie wielu informacji historycznych i bieżących.

4. OBSŁUGA ALARMÓW I KRONOS NET

Wszystkie powyższe elementy nie pozwoliłyby zbudować automatycznej stacji monitoringu, gdyby nie doświadczenie zdobyte przez lata przy rozwijaniu popularnej platformy Kronos NET. Alicja nie jest jednak nakładką na Kronos NET, ale całkowicie zmodernizowanym kodem przygotowanym w najnowszych narzędziach programowania i gotowym do instalacji w bezpiecznych środowiskach zamkniętych lub prywatnych chmurach. Wiele elementów systemu zostało przygotowanych praktycznie od zera, np. Konsola Video pełniąca funkcję oprogramowania VMS w ramach środowiska Alicja, inne przebudowano w celu zwiększenia ergonomii i możliwości, np. Konsola Monitoringu.

Wszystkich zainteresowanych pełnymi możliwościami systemu, a przede wszystkich chcących zoptymalizować koszty prowadzenia stacji monitoringu zapraszamy do kontaktu z naszą firmą.

Cyberekstraklasa – konieczny kierunek rozwoju

Dzika karta cybersecurity do wzięcia – okienko transferowe dla firm ochrony otwarte. Kto skorzysta, ten wygra!

Stosując język organizacji biznesu sportowego, można powiedzieć, że przed agencjami ochrony obecnie otwiera się opcja awansu do cyberekstraklasy. Możliwość taka pojawia się z dwóch powodów. Po pierwsze firmy ochrony poprzez swoich najwyższych rangą menedżerów informują o zmianie w modelu realizacji usług ochrony. Narracja, zgodnie z którą nie ma powrotu do usługi świadczonej głównie przez pracowników ochrony, jest niezwykle atrakcyjna, cieszy się też dużym zainteresowaniem klientów. Po drugie budżety wdrożeń technicznych w firmach ochrony przebijają kolejne, pozornie szklane sufity, a to jest bardzo dobrą wiadomością dla wszystkich.

Jacek Tyburek

Firmy technologiczne zarabiają, agencje ochrony również, klienci otrzymują usługę na nowym, zdecydowanie wyższym poziomie. Pozornie powinno być wszystko w najlepszym porządku. Gdzie więc okienko transferowe? Dlaczego ta ekstraklasa miałaby być cyberekstraklasą?

Przeprowadzona analiza usług oferowanych przez firmy ochrony pokazuje wprost, że obecna ich oferta nie zawiera elementu wsparcia swoich klientów w sferze cyberbezpieczeństwa. Gdyby przyjąć założenie, że firma ochrony w sposób świadomy rozbudowuje swoje usługi o działania ochrony przeciw cyberzagrożeniom, kolejnym krokiem powinno być zbudowanie SOC *(Security Operation Center)* dedykowanego dla swoich klientów kontraktowych lub zupełnie nowych podmiotów w portfelu. Duże firmy ochrony w Polsce, a dotyczy to z pewnością pierwszej dziesiątki o największych przychodach i zasięgach operacyjnych, liczbę klientów liczą w tysiącach. To różnej wielkości firmy komercyjne, podmioty państwowe, samorządowe i z grupy infrastruktury krytycznej kraju. Z tego względu firma posiadająca w swoich strukturach działy lub osoby zajmujące się cyberbezpieczeństwem stanowią bezcenny zasób organizacyjny umożliwiający wejście na ścieżkę rozwoju.
Etap drugi tego rozwoju to niewątpliwie plan zbudowania SOC, które będzie mogło pracować na rzecz swoich klientów, korzystając z obsługi w innych, bardziej klasycznych obszarach bezpieczeństwa. Bardzo dobrą podstawą do zbudowania efektywności operacyjnej i biznesowej takiego SOC jest oferta na konsolidowanie i monitorowanie danych z systemów przedsiębiorstwa, inicjowanie procesów reagowania na incydenty oraz zarządzanie innymi działaniami związanymi z zagrożeniami cybernetycznymi. Naturalne skorzystanie z własnej specjalizacji i przejścia z jej realizacją na inny, wyższy szczebel operacyjny zapewnia harmonijny rozwój nowego obszaru biznesowego.

Security Operation Center, jako struktura rozbudowana, zgodnie z metodologicznymi założeniami musi być strukturą drogą. Zatrudnienie minimum kilkunastu osób, które od początku będą postrzegane jako pozycja kosztowa (do pierwszego udanego dla przestępców cyberataku), często jest barierą nie do przebrnięcia. Dla firmy specjalizującej się we wszystkim, tylko nie w bezpieczeństwie, zbudowanie takiego tworu organizacyjnego będzie bardzo trudne. Z kolei dla firm utrzymujących się z tworzenia produktów bezpieczeństwa wydaje się kierunkiem rozwoju z kategorii koniecznych. Jednoczesne budowanie zadowolenia klienta z usług i pogłębiania zaufania do firmy ochrony jest czynnikiem wzmacniającym przewagę konkurencyjną.

Proces budowy SOC musi przewidywać dwie niezależne od siebie optyki. Optyka potencjalnego klienta to zazwyczaj poszukiwanie zarządzanego SOC. Zarządzany SOC, zwany również *SOC as a Service*, świadczy wszystkie usługi lub ogranicza się do monitorowania i reagowania na zdarzenia *(Managed Detection and Response)* przez dostawcę zewnętrznego. Opiera się zwykle na modelu subskrypcji – firma na podstawie zrealizowanych celów uiszcza okresową opłatę za uzgodnioną usługę SOC. Zarządzany SOC zapewnia firmie zespół zewnętrznych ekspertów ds. bezpieczeństwa cybernetycznego zajmujących się monitorowaniem, wykrywaniem i badaniem zagrożeń w całym przedsiębiorstwie. W niektórych przypadkach usuwaniem wykrytych zagrożeń (łatanie dziur, usuwanie błędów konfiguracyjnych) zajmuje się zewnętrzny zespół bezpieczeństwa, w innych zespół SOC współpracuje z wewnętrznymi zespołami IT nad ich usunięciem. Dzięki zarządzanemu SOC zagrożenia cybernetyczne są monitorowane 24x7x365 bez konieczności dużych inwestycji w oprogramowanie zabezpieczające, sprzęt i ludzi.

Zagrożenia cybernetyczne są monitorowane **24/7/365**

Należy się jednak spodziewać, że ten rodzaj SOC, monitorujący głównie incydenty w obszarze systemów bezpieczeństwa budynku (CCTV, kontrola dostępu czy system ppoż.), dla klienta może nie być rozwiązaniem atrakcyjnym. Usługą bardziej pożądaną mogłoby być monitorowanie incydentów w obszarze obiektowego BMS lub innej formule zintegrowanego panelu zarządzania funkcjonalnościami obiektu. Zdolności operacyjne, jakie powinien posiadać taki SOC w wersji podstawowej, powinny obejmować następujące elementy:

- **Przyjmowanie i rejestracja zgłoszeń**

Przyjmowanie zgłoszeń od użytkowników systemów za pośrednictwem ustalonych kanałów komunikacji. Rejestracja w systemie obsługi zgłoszeń. Wywiad, zebranie i rejestracja informacji nt. zdarzenia czy incydentu.

- **Monitoring systemów bezpieczeństwa**

Stały monitoring systemów bezpieczeństwa pod kątem alertów i wskaźników incydentów. Analiza zaobserwowanych zdarzeń w ramach procesu obsługi incydentów bezpieczeństwa. Rejestracja informacji o wystąpieniu alertu i przebiegu analizy. Informowanie i raportowanie zgodnie z ustalonymi ścieżkami eskalacji.

- **Analiza i selekcja zdarzeń**

Uzupełnienie zgromadzonych artefaktów zdarzeń o informacje kontekstowe. Weryfikacja danych w źródłach TI *(Threat Intelligence)*. Przeszukanie źródeł danych pod kątem zdarzeń powiązanych. Analiza zgromadzonych informacji i selekcja z uwzględnieniem potencjalnych incydentów bezpieczeństwa. Informowanie i raportowanie zgodnie z ustalonymi ścieżkami eskalacji.

- **Reakcja na incydent**

Analiza szczegółów technicznych i przebiegu incydentu. Określenie wpływu incydentu na zasoby i procesy organizacji. Podjęcie działań w celu powstrzymania incydentu i likwidacji zagrożenia w ustalonym zakresie zgodnie z autoryzacją.

- **Zarządzanie podatnościami**

Zarządzanie procesem skanowania podatności. Analiza wyników, określenie ryzyka każdej wykrytej podatności i ustalenie priorytetów postępowania, obsługa procesu zarządzania podatnościami (ewidencja, analiza postępów, eskalacja, raportowanie).

- **Aktywne wykrywanie zagrożeń**

Aktywna analiza zdarzeń z dostępnych źródeł informacji pod kątem wskaźników incydentów.

- **Analiza i raportowanie zagrożeń**

Analiza źródeł informacji TI pod kątem potencjalnych zagrożeń dla organizacji.

- **Wsparcie zarządzania systemami bezpieczeństwa**

Zarządzanie konfiguracją systemów bezpieczeństwa, optymalizacja polityk bez-

pieczeństwa oraz monitoring wydajności w ustalonym zakresie zgodnie z autoryzacją. Zadaniem jest wyjaśnienie i ukrócenie przypadków nieuczciwości i patologii w organizacjach.

Przez wiele lat również zarządzanie sferą bezpieczeństwa i higieny pracy, określaną z języka angielskiego jako safety, a nie security, stanowiło drugi obszar rozumienia bezpieczeństwa. Tak było do momentu rozwijania się i upowszechniania technologii IT oraz rozpowszechniania metodologii ochrony informacji. Powstawały normy różnych porządków standaryzujących, w tym najbardziej rozpowszechnione normy British Standard oraz ISO.
Sytuacja, gdy IT Security Manager lub obecnie Cybersecurity Manager awansowali w strukturach organizacyjnych, jest stosunkowo nowa. Ostatnie 20 lat to był systematyczny wzrost znaczenia specjalistów zajmujących się bezpieczeństwem biznesu, czyli jego częścią operacyjną. Niektóre firmy podniosły stanowisko kierownika ds. bezpieczeństwa do poziomu wykonawczego, tworząc stanowisko dyrektora ds. bezpieczeństwa (CSO). Chociaż typowa pozycja dyrektora ds. bezpieczeństwa istnieje w korporacyjnej rzeczywistości, są obszary bezpieczeństwa, za które odpowiedzialni będą różni CSO w różnych firmach, zależnie od branży lub sektora oraz tego, jakie rodzaje ryzyka/zagrożeń są postrzegane jako ważne do rozwiązania.

Ważne, aby CSO ściśle współpracował z innymi liderami na szczeblu kierowniczym, takimi jak HR, dział prawny, IT, finanse i poszczególne jednostki biznesowe. Skuteczne ograniczanie zagrożenia bezpieczeństwa organizacji stało się ostatnio sprawą bardziej krytyczną niż kiedykolwiek.
Wiele w tym obszarze zmieniło się od momentu wyłonienia się funkcji specjalisty ds. cybersecurity, której znaczenie w organizacji zaczęło rosnąć. Sam język i znaczenie zmieniły swoje pierwotne rozumienie. Obszar bezpieczeństwa w organizacjach zaczął być utożsamiany właśnie z bezpieczeństwem danych i IT, a nie z trudnym do jednoznacznego zdefiniowania bezpieczeństwem operacyjnym. Dynamicznie rozwijający się rynek pracy w specjalizacjach związanych z bezpieczeństwem sieci i danych spowodował, że 8 na 10 ofert pracy ze słowem „security" to obecnie oferty dla specjalistów cybersecurity lub w skrajnych przypadkach specjalistów ds. bezpieczeństwa aplikacji lub sieci.
Sukcesywne przenikanie się obszarów bezpieczeństwa tradycyjnego z bezpieczeństwem w rozumieniu prawnym, cybersecurity i operacyjnym wymaga ogromnej ilości danych zarządczych i narzędzi do efektywnego zarządzania strefą bezpieczeństwa. Jednocześnie sytuacja stałego narażenia biznesu na realne ataki cyberprzestępców wymaga skutecznego działania adekwatnego do czasu.
Tradycyjnym security menedżerom coraz trudniej nadążać kompetencyjnie za wymogami dynamicznie zmieniającego się ryzyka, czego efektem jest obniżenie rangi Security Managera w strukturze organizacyjnej. Miejsce logiki zarządzania bezpieczeństwem biznesu zajmuje perspektywa cyberbezpieczeństwa. Obszar cyberbezpieczeństwa metodologicznie nie jest jeszcze w pełni ukształtowany, więc można z pełną odpowiedzialnością mówić o stanie przejściowym w sferze zarządzania bezpieczeństwem biznesu. Dodatkowym elementem, który znacznie utrudnia realizowanie przemyślanej kompleksowej polityki bezpieczeństwa organizacji jest brak wystarczającej liczby wykwalifikowanej kadry cyberspecjalistów.

Dlatego pojawia się szansa dla firm ochrony osób i mienia, które często dysponują ogromnymi zasobami ludzkimi, wykształconymi strukturami handlowymi i siecią relacji biznesowych we wszystkich sferach gospodarki. Agencje ochrony już dzisiaj mają bazę do rozwoju usług bezpieczeństwa wykraczających poza typowe usługi ochrony fizycznej. Coraz szersze oczekiwanie klientów na monitorowanie różnego typu technologicznych systemów kontrolnych i bezpieczeństwa wzmagają apetyt na nowe rozwiązania. Zintegrowane (hybrydowe) centra mają tę zaletę, że wykonują usługi na rzecz wielu klientów, dzięki czemu są efektywne kosztowo. Z reguły nie świadczą żadnych usług, które można zakwalifikować jako związane z cyberbezpieczeństwem – nawet w odniesieniu do urządzeń i systemów pracujących w formule IoT, które monitorująca firma sama instalowała u klienta.
Liczne przykłady z dużych organizacji biznesowych, zwłaszcza firm przemysłowych (produkcyjnych), logistycznych i z obszaru infrastruktury krytycznej kraju, wskazują na tworzenie osobno przez różne służby silosowo zorganizowanych struktur interwencyjnych. Tak więc korporacyjna (zakładowa) straż pożarna posiada własne służby ratunkowe, z własnym wydzielonym centrum zarządzania operacjami oraz dyspozytornią. Podobnie zorganizowane są służby security posiadające własne pomieszczenia monitoringu wizyjnego, czasem połączone z monitoringiem GPS. Także zakładowe służby medyczne, których personel pełniący dyżury odbiera powiadomienia o zdarzeniach. Firmowe służby medyczne lub paramedyczne współpracują często ze strukturami BHP. Do tej wyliczanki służb i stanowisk zarządczych dochodzą specjaliści od utrzymania budynków oraz utrzymania technicznego obiektów. Na końcu dochodzimy do SOC, które, jeśli istnieje, jest dziełem i dumą działów IT.

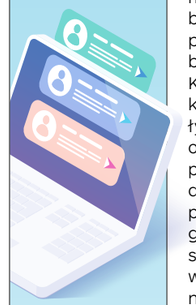
Definicja hybrydowego SOC mówi, że jest połączeniem zasobów wewnętrznych z zewnętrznymi. Wyznaczona osoba (lub kilka osób) w firmie jest odpowiedzialna za bieżące operacje SOC, a w razie potrzeby angażuje się dzielących też inne obowiązki członków zespołów, a także strony trzecie. Jeśli organizacja nie może działać w trybie 24x7x365, powstałe luki mogą być pokryte przez kilku dostawców usług bezpieczeństwa, co daje w efekcie hybrydowy model SOC. Dostawcy ci mogą świadczyć pełne usługi bezpieczeństwa MSSP *(Managed Security Services Provider)* lub ograniczać się do wykrywania zagrożeń MDR (*Managed Detection Risks)* i reagowania na nie, wykorzystując zewnętrzną platformę obsługi incydentów SIEM *(Security Information and Event Management)*. Hybrydowy model funkcjonowania SOC pozwala zredukować koszty. Jest stosowany nie tylko w małych i średnich przedsiębiorstwach współpracujących w szerokim zakresie z firmami zewnętrznymi, ale także w większych organizacjach i dojrzałych SOC, które mogą selektywnie zlecać pewne usługi bezpieczeństwa na zewnątrz.

Model hybrydowy jest również stosowany jako rozwiązanie tymczasowe przez organizacje, które chcą budować kompetencje wewnętrzne (podwykonawstwo insourcingowe), ale:

- muszą natychmiast rozwiązać problem,
- mają ograniczone kompetencje, aby od razu stać się autonomiczne,
- chcą wykorzystać dostawcę usług bezpieczeństwa do transferu wiedzy i ciągłego rozwoju.

Motorem przyjęcia takiego modelu są braki w dostępności specjalistycznej wiedzy, ogólne ograniczenia budżetowe i znaczne koszty całodobowych operacji bezpieczeństwa. Duża i rozwinięta produktowo agencja ochrony ma wszelkie zasoby, by utworzyć swoisty Hybrid SOC dla swoich klientów, którzy mogliby korzystać z istniejących zaawansowanych rozwiązań zarówno w modelu stałego abonamentu, jak i podejścia projektowego na czas zgodny z okresem życia projektu. Z powyższego opisu wyłania się realny obraz, dobrze znany w wielu dużych organizacjach. Próba znalezienia wspólnego mianownika dla wszystkich działań wspierających podstawowe działania przedsiębiorstwa prawdopodobnie początkowo napotka opór twórców pierwotnych rozwiązań. Niemniej znane są przypadki podejmowania próby integracji wymienionych służb. W takiej sytuacji problemem może być pokonanie uprzedzeń ich twórców, aby stworzyć bardziej zintegrowaną strukturę pracującą w modelu synergii sił i środków organizacyjnych i technologicznych. Drugą przeszkodą są te technologie, które zazwyczaj należałoby zastąpić nowymi przy nowym modelu działania.

To bardzo poważny koszt, który wiąże się z podróżą w nieznane. Obecnie znany jest kierunek tej podróży – jej celem jest gromadzenie jak największej ilości przydatnych danych i przekazywanie konkluzji z ich analizy do zarządów przedsiębiorstw. Dlatego same centra monitoringu, SOC czy innego rodzaju rozproszone stanowiska zarządcze służbami w coraz mniejszym stopniu odpowiadają na potrzeby biznesu. Konieczne jest tworzenie swoistych „control tower". Struktury takie, działające w reżimie odpowiedzialnego korzystania z narzędzi technologicznych w sposób bezpieczny z punktu widzenia cyberbezpieczeństwa, powstają pod hasłem hybrydowych SOC.
Konieczne jest przywołanie standardów korporacyjnych, które z reguły ubierały w ramy organizacyjne działanie w tym obszarze. W erze *big data* funkcjonujemy przy całkowicie nowych wymaganiach. Zadaniem naczelnym jest informacyjne wyprzedzanie materializacji ryzyka tak, by organizacje unikały strat. Coraz trudniej je spełnić, trzeba korzystać z wyspecjalizowanych usług lub budowy własnych, ale niezwykle kosztownych rozwiązań. Przy każdej analizie ryzyka zawsze rozważa się aspekt zarządzania odpowiedzialnością za powodzenie działań.



Przed agencjami ochrony, które swoje działania coraz odważniej opierają na technologiach teleinformatycznych, stoją dziś trudne zadania. Sprzedając klientowi produkt materialny lub usługę, muszą brać pod uwagę wszystkie aspekty jakościowe i bezpieczeństwa, posiadać pełną wiedzę na temat ich podatności. Czy zaproponowanie rozwiązania z wadami technologicznymi lub podatnościami na skuteczne ataki cyberprzestępców stanowi odpowiedzialność producenta technologii, czy dystrybutora handlowego koordynującego sprzedaż i wdrożenie? Nawet jeśli umowy są skonstruowane w sposób korzystny dla producenta rozwiązania lub jego dystrybutora, to ciągle pozostaje sfera konfliktu z klientem w sytuacji kryzysowej i utrata wizerunku.
Znacznie poważniejsze konsekwencje spotykają stronę zaatakowaną. Obecnie funkcjonujące centra monitoringu alarmów, centra monitoringu wizyjnego i monitoringi GPS znacznie rozszerzają swoje pole działania. Wolumeny przychodów ze sprzedaży systemów bezpieczeństwa (elektroniczne wraz z oprogramowaniem) rosną wykładniczo rok do roku. To oczywiście bardzo dobra wiadomość. Gorzej, że rośnie również ryzyko pośredniczenia w sprzedaży rozwiązań security z dużymi podatnościami na cyberataki.
Jednak siła, zasięg, zasoby organizacyjne i możliwości finansowe sprawiają, że firmy ochrony – przynajmniej te największe, z tzw. pierwszej piątki w Polsce – stoją w obliczu okna transferowego do ekstraklasy nowoczesnych firm posiadających zasoby organizacyjne i technologiczne, by wypełnić lukę na rynku.

Duża i rozwinięta produktowo agencja ochrony ma wszelkie zasoby, by utworzyć swoisty Hybrid SOC dla swoich klientów, którzy mogliby korzystać z istniejących zaawansowanych rozwiązań

JACEK TYBUREK

Menedżer bezpieczeństwa organizacji. Doświadczenie zdobywał w różnych obszarach bezpieczeństwa: od przemysłu i logistyki, przez BPO, po bezpieczeństwo w rzeczywistości wirtualnej. Promotor pojęcia Organisational Resilience. Obecnie związany z Black Onion Resilience Community.

System Zarządzania Ciągłością Działania (BCMS)

Cz. 3. Kolejne kroki – etap 1.

Celem etapu 1. jest zbudowanie świadomości w zakresie ciągłości działania w organizacji, wprowadzenie do projektu zaangażowanych po stronie organizacji osób, przeprowadzenie wstępnego audytu zgodności z wymaganiami normy ISO 22301, zdefiniowanie i priorytetyzacja obszarów do wdrożenia BCMS w ramach projektu oraz opracowanie polityki ciągłości działania.

Istotne, aby w procesie uczestniczyły wszystkie kluczowe osoby, w tym kluczowi pracownicy realizujący poszczególne procesy w organizacji oraz kierownik projektu, który najczęściej jest również koordynatorem BCMS, a później osobą odpowiedzialną za skuteczne utrzymanie systemu. Ponadto w grupie decydentów powinien się znaleźć przedstawiciel najwyższego kierownictwa.
Działania w ramach tego etapu mogą być realizowane jednorazowo dla głównych obszarów wdrożeniowych w ramach całej organizacji w pięciu krokach:

Tomasz Guzikowski

KROK I
BUDOWANIE ŚWIADOMOŚCI ORAZ WPROWADZENIE DO PROJEKTU

Dla skutecznej realizacji tego kroku należy przeprowadzić warsztaty mające na celu wprowadzenie do projektu i wykazanie istotności ciągłości działania w organizacji – z perspektywy nie tylko technicznej, ale także biznesowej i społecznej. Można to zrobić w formie case study opracowanego na podstawie listy incydentów wpływających na ciągłość działania, które miały miejsce w organizacji. Dobrą praktyką jest również przeprowadzenie symulacji incydentu zaburzającego ciągłość działania z wykorzystaniem istniejących procedur czy instrukcji postępowania w razie incydentów lub awarii. Nie mniej ważnym elementem tego kroku jest wprowadzenie do poszczególnych etapów prac i wyjaśnienie najważniejszych pojęć związanych z ciągłością działania i realizowanym projektem.

KROK II
WSTĘPNY AUDYT ZGODNOŚCI Z WYMAGANIAMI NORMY ISO 22301

Celem jest identyfikacja niezgodności oraz opracowanie rekomendacji pod kątem zgodności z wymaganiami normy ISO 22301. Audyt wstępny ma głównie funkcję informującą i instruktażową. Z jednej strony dostarcza informacji na temat funkcjonowania systemu bądź elementów systemu ciągłości działania, z drugiej – pozwala podpowiedzieć organizacji metodę postępowania i dobre praktyki w audytowanym obszarze.
Realizacja tego kroku polega na pozyskaniu i analizie dokumentacji odnoszącej się do zapewnienia ciągłości działania, jeżeli taka w organizacji występuje. Następnie na bazie warsztatów należy dokonać weryfikacji stosowanych praktyk i faktycznej realizacji działań związanych z ciągłością działania. Raport z przeprowadzonego audytu powinien zawierać listę zidentyfikowanych niezgodności z wymaganiami normy ISO 22301 oraz listę rekomendacji ich usunięcia.

KROK III
OPRACOWANIE KRYTERIÓW DO PRIORYTETYZACJI OBSZARÓW NA POTRZEBY WDROŻENIA

W dużych organizacjach może nie być możliwe zrealizowanie wdrożenia systemu we wszystkich kluczowych obszarach jej działalności w jednym czasie. Ważne, aby w taki sposób określić priorytety dla poszczególnych obszarów jej działalności, żeby w stosunkowo krótkim czasie wdrożenia zapewnić organizacji takie produkty, które dadzą w perspektywie największe wymierne korzyści. Poza tym wydłużający się proces wdrożeniowy może spowodować zniechęcenie pracowników i całej organizacji do dalszej realizacji projektu.
Aby osiągnąć cel niniejszego kroku, należy wspólnie z właścicielami poszczególnych obszarów i procesów uzgodnić listę kryteriów stosowanych na potrzeby priorytetyzacji obszarów umożliwiających zdefiniowanie i ustalenie kolejności wdrożenia.
Przykładowymi kryteriami mogą być:

- dojrzałość obszaru z perspektywy udokumentowania procesów w nim zachodzących,
- powtarzalność obszaru w wielu lokalizacjach (w przypadku obiektów rozproszonych),
- krytyczność obszaru dla działalności,
- wpływ na generowany przychód i koszty,
- liczba dotychczas zidentyfikowanych incydentów i awarii wpływających na ciągłość działania,
- wpływ na wizerunek organizacji.

Raport z przeprowadzonego audytu powinien zawierać listę zidentyfikowanych niezgodności z normą ISO 22301 i listę rekomendacji ich usunięcia

KROK IV
ZDEFINIOWANIE I PRIORYTETYZACJA OBSZARÓW OBJĘTYCH WDROŻENIEM

Aby zrealizować cele niniejszego kroku, dobrą praktyką jest zdefiniowanie kluczowych obszarów działalności organizacji w formie warsztatów zorganizowanych wspólnie z jej przedstawicielami. Kluczowe jest zebranie informacji o łańcuchu wartości organizacji. Podczas moderowanego warsztatu uczestnicy udzielają informacji o świadczonych usługach, dostarczanych produktach i relacjach z interesariuszami na podstawie pytań pomocniczych, m.in.

- Segment oraz struktura klientów (Komu dostarczamy nasze produkty? Co dostarczamy naszym klientom? Kto jest najważniejszym klientem?)
- Kanały dystrybucji (W jaki sposób docieramy do naszych klientów? Za pomocą jakich kanałów nasi klienci chcą nawiązywać z nami relacje? Które kanały są najbardziej opłacalne?)
- Relacje z klientami (Jakiego rodzaju relacje nasi klienci chcą z nami utrzymywać? Jakie mamy relacje z obecnymi klientami? Jakie problemy staramy się rozwiązać?)
- Struktura przychodów i kosztów (Jaki jest preferowany model rozliczeń z klientami? Jak obecnie klienci płacą za produkty/usługi? Jakie koszty ponosimy w związku z prowadzeniem działalności?)
- Kluczowe zasoby (Jakie zasoby są kluczowe, abyśmy mogli dostarczać nasze produkty/usługi?)
- Kluczowe aktywności (Jakie czynności/procesy muszą być realizowane, aby dostarczać nasze produkty/usługi i zapewniać przychód?)
- Kluczowi partnerzy/interesariusze (Kto jest naszym kluczowym partnerem, dostawcą, podwykonawcą?)

KROK V
OPRACOWANIE POLITYKI CIĄGŁOŚCI DZIAŁANIA

Kluczowym produktem prac w ramach tego kroku jest polityka ciągłości działania dla zdefiniowanych w poprzednim kroku obszarów, która powinna uwzględniać m.in.

- cel oraz zakres wdrożenia i stosowania polityki,
- kontekst organizacyjny, w tym uwarunkowania wewnętrzne i zewnętrzne odnoszące się do ciągłości działania oraz powody, dla których organizacja wdraża BCMS,
- zadania i obowiązki przypisanych ról w procesie utrzymania i ciągłego doskonalenia BCMS,
- zasady definiowania celów dla ciągłości działania,
- zobowiązanie najwyższego kierownictwa do spełniania wymagań oraz ciągłego doskonalenia

TOMASZ GUZIKOWSKI

Menedżer z wieloletnim doświadczeniem w obszarze zarządzania bezpieczeństwem i ciągłością działania, w tym bezpieczeństwa procesowego i zawodowego, ochrony infrastruktury krytycznej, ochrony informacji niejawnych w budownictwie i dużych zakładach produkcyjnych należących do grupy zakładów dużego ryzyka powstania awarii przemysłowej. Obecnie zarządza obszarem bezpieczeństwa w globalnym koncernie chemicznym CIECH.

Ocena wyrobów służących do ochrony ppoż. budynków

Cz. 2. Oznakowanie CE

W poprzednim artykule (A&S 1/2022) omówiłem ogólnie rolę i zalety oceny wyrobów dla bezpieczeństwa pożarowego budynków, wskazując jej umiejscowienie wśród wielu narzędzi budowania bezpieczeństwa pożarowego. Kontynuując tę tematykę, przybliżę dokumenty i znakowanie związane z oceną wyrobów i to, jak w praktyce skorzystać z tych dokumentów i informacji w nich zawartych.

mł. bryg. mgr inż. Grzegorz Mroczko

Przepisy rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 305/2011 z 9 marca 2011 r. ustanawiające zharmonizowane warunki wprowadzania do obrotu wyrobów budowlanych i uchylające dyrektywę Rady 89/106/EWG (Dz.U.L. 88/5 z 4.04.2011) wskazują, że potwierdzeniem przeprowadzenia oceny wyrobów jest wystawienie deklaracji właściwości użytkowych i oznakowanie wyrobu oznakowaniem CE. To z tych elementów odbiorca wyrobu powinien w łatwy i przystępny sposób uzyskać istotne informacje nt. wyrobu budowlanego. Są to zatem pierwsze elementy, z którymi odbiorcy wyrobu mają kontakt.

Najczęściej wyroby stosowane w systemach bezpieczeństwa pożarowego obiektów budowlanych są, zgodnie z przepisami budowlanymi, oceniane w systemie 1. oceny i weryfikacji stałości właściwości użytkowych (OiWSWU). Skrócony schemat postępowania zobrazowano na *rys. 1.*

Rys. 1. Skrócony schemat drogi do „oznakowania CE”

CERTYFIKAT STAŁOŚCI WŁAŚCIWOŚCI UŻYTKOWYCH

Producenci są zobowiązani do przeprowadzenia oceny i weryfikacji stałości właściwości użytkowych wyrobów budowlanych zgodnie ze wskazanym dla tego wyrobu systemem oceny. Proces oceny, na który składają się m.in.

- ocena dokumentacji wyrobu,
- badania i ocena wyników badań wyrobu,
- ocena systemu produkcji wyrobu w zakładzie produkcyjnym (ocena Zakładowej Kontroli Produkcji – ZKP),

kończy się w systemie 1 i 1+ oceny wydaniem dla wyrobu certyfikatu stałości właściwości użytkowych przez jednostkę certyfikującą posiadającą notyfikację UE w zakresie danej normy zharmonizowanej.
Baza danych jednostek notyfikowanych jest dostępna pod adresem https://ec.europa.eu/growth/tools-databases/nando/index.cfm?fuseaction=directive.notifiedbody&dir_id=33.
W obszarze wyrobów budowlanych notyfikację ma 617 jednostek certyfikujących. W zakresie wyrobów budowlanych służących do ochrony przeciwpożarowej (grupa 10 wyrobów zgodnie z załącznikiem nr IV do rozporządzenia nr 305/2011) w Europie notyfikację ma 81 jednostek notyfikowanych, a w Polsce 4 jednostki certyfikujące (CNBOP-PIB nr 1438, ITB nr 1488, Certbud nr 2310, CTO nr 2434).

Certyfikat zawiera m.in. następujące ważne informacje:

- nazwę i adres producenta wyrobu,
- nazwę i adres podmiotu wprowadzającego wyrób do obrotu,
- typ i oznaczenie wyrobu,
- właściwości użytkowe wyrobu, które zostały w procesie ocenione,
- system oceny i weryfikacji stałości właściwości użytkowych,
- numer i tytuł normy zharmonizowanej (lub Europejskiej Oceny Technicznej),
- daty ważności, które odnoszą się do momentu produkcji wyrobu (danego egzemplarza/partii),
- dane techniczne wyrobu oraz konfiguracja elementów wewnętrznych w przypadku urządzeń elektronicznych.

W tabeli 1 przedstawiono wybrane normy zharmonizowane z obszaru systemów sygnalizacji pożarowej.

Tab. 1.

LP.	WYRÓB	NUMER NORMY ZHARMONIZOWANEJ
Centrale, zasilacze, transmisja alarmów pożarowych do straży pożarnej		
1	Centrale sygnalizacji pożarowej	EN 54-2:1997 +AC:1999+A1:2006
2	Zasilacze stosowane w systemach sygnalizacji pożarowej	EN 54-4:1997 +AC:1999+A1:2002+A2:2006
3	Urządzenia transmisji alarmów pożarowych	EN 54-21:2006
CZUJKI POŻAROWE I RĘCZNE OSTRZEGACZE POŻAROWE		
4	Czujki punktowe ciepła	EN 54-5:2017+A1:2018
5	Czujki punktowe dymu	EN 54-7:2018
6	Czujki punktowe płomienia	EN 54-10:2002+A1:2005
7	Czujki liniowe dymu	EN 54-12:2015
8	Czujki dymu zasysające	EN 54-20:2006+AC:2008
9	Ręczne ostrzegacze pożarowe	EN 54-11:2001+A1:2005
URZĄDZENIA DO ALARMOWANIA O POŻARZE		
10	Sygnalizatory akustyczne	EN 54-3:2001 +A1:2002+A2:2006
11	Sygnalizatory optyczne	EN 54-23:2010
12	Centrale dźwiękowych systemów ostrzegawczych	EN 54-16:2008
13	Głośniki	EN 54-24:2008
INNE ELEMENTY LINIOWE		
14	Izolatory zwarć	EN 54-17:2005
15	Liniowe elementy wejścia/wyjścia	EN 54-18:2005+AC:2007
WYMAGANIA DLA URZĄDZEŃ WYKORZYSTUJĄCYCH ŁĄCZA RADIOWE		
16	Podzespoły SSP wykorzystujące łącza radiowe	EN 54-25:2008+AC:2012

Pełny wykaz norm zharmonizowanych z rozporządzeniem 305/2011 jest dostępny pod adresem https://ec.europa.eu/docsroom/documents/38863 (wykaz sporządzony 20.12.2019 r.). Z kolei wykaz wyrobów, dla których CNBOP-PIB prowadzi certyfikację europejską, znajduje się pod adresem https://www.cnbop.pl/uslugi/jednostka-certyfikujaca/wykazy/wykaz-pc-cpr.pdf

DEKLARACJA WŁAŚCIWOŚCI UŻYTKOWYCH (DWU)[1]

Po przeprowadzeniu wszystkich czynności z wynikiem pozytywnym producent powinien sporządzić dla wyrobu deklarację właściwości użytkowych. Powinna ona zawierać m.in.

- określenie typu wyrobu, dla którego została sporządzona,
- zamierzone zastosowanie lub zastosowania wyrobu budowlanego,
- właściwy dla wyrobu system lub systemy oceny i weryfikacji stałości właściwości użytkowych,
- numer i datę wydania normy zharmonizowanej lub europejskiej oceny technicznej, którą zastosowano do oceny wyrobu,
- deklarowane właściwości użytkowe wyrobu wyrażone w poziomach lub klasach albo w sposób opisowy, które zostały potwierdzone w procesie oceny wyrobu.

Deklaracja powinna być wystawiona w języku państwa UE, w którym wyrób jest sprzedawany, oraz dołączana do pojedynczego wyrobu lub partii wyrobów. W określonych przypadkach może być udostępniona na stronie internetowej[2] producenta i powinna pozostawać dostępna przez 10 lat. Ponieważ poziom świadomości w tym obszarze jest zróżnicowany, na rynku funkcjonują różne tego typu dokumenty, także „deklaracjopodobne", dlatego ważne, aby szczegółowo i bez pośpiechu zapoznawać się z ich treścią. Analiza deklaracji pozwala ocenić, czy:

- dotyczy wyrobu, który ma być zakupiony/dostarczony,
- jest wystawiona przez producenta wyrobu lub jego upoważnionego przedstawiciela, a nie np. firmę handlową,
- wskazuje jednostkę notyfikowaną, która przeprowadziła ocenę wyrobu,
- wskazuje właściwą normę zharmonizowaną wyrobu albo europejską ocenę techniczną,
- wyrób ma odpowiednie właściwości wymagane i niezbędne w danej sytuacji oraz czy zostały one potwierdzone, np. odporność na zimno, wytrzymałość na korozję, klasa reakcji na ogień B2ca-s1b ,d0, a1, klasa odporności ogniowej EI30, czas zachowania dostawy energii i przekazu sygnału E30-E90 itp.

OZNAKOWANIE CE

Po wystawieniu deklaracji właściwości użytkowych producent ma prawo

1 Wzór deklaracji właściwości użytkowych jest zawarty w załączniku do Rozporządzenia Delegowanego Komisji (UE) nr 574/2014 z 21 lutego 2014 r., które zmieniało załącznik III do rozporządzenia 305/2011.

2 Przy spełnieniu wymagań Rozporządzenia Delegowanego Komisji (UE) nr 157/2014 z 30 października 2013 r. w sprawie warunków udostępniania deklaracji właściwości użytkowych wyrobów budowlanych na stronie internetowej.

umieścić na wyrobie oznakowanie CE. W ten sposób producent bierze na siebie odpowiedzialność za zgodność wyrobu z deklarowanymi właściwościami użytkowymi. Oznakowanie CE należy umieścić na wyrobie budowlanym lub na jego etykiecie w sposób widoczny, czytelny i trwały. Gdy nie jest to możliwe lub nie można tego zapewnić ze względu na charakter wyrobu, nanosi się je na opakowaniu lub dokumentach towarzyszących wyrobowi.
Przykład oznakowania CE z informacją towarzyszącą przedstawiono w *tabeli 2.*

Tab. 2.

ELEMENT OZNAKOWANIA	PRZYKŁAD	
Oznakowanie CE z numerem jednostki notyfikującej, która wydała certyfikat	CE 1438	
Nazwa lub nr identyfikacyjny producenta	Spółka Sp. z o.o. ul. Nowoczesna 8a Miasto	
Dwie ostatnie cyfry roku, w którym oznakowanie CE zostało po raz pierwszy naniesione na wyrób	13	
Numer certyfikatu	1438/CPR/XXXX	
Numer i tytuł zharmonizowanej specyfikacji technicznej (hEN, ETA)	**EN 54-7:2018** *Fire detection and fire alarm systems – Part 7: Smoke detectors - Point detectors that operate using scattered light, transmitted light or ionization*	
Opis wyrobu i zamierzonego zastosowania	Napięcie pracy 16,5 V ÷ 24,6 V Maks. prąd dozorowania ≤150 µA Temperatura pracy od -10 do 55 °C (...) Punktowa czujka dymu przeznaczona do stosowania w systemach sygnalizacji pożarowej wewnątrz budynków	
Właściwości użytkowe wyrażone w poziomach, klasach lub opisowo	Reakcja na wolno rozwijające się pożary Czułość pożarowa Suche gorąco (odporność) (...)	Spełnia Spełnia Spełnia

Oznakowaniu CE powinny towarzyszyć następujące informacje:

- dwie ostatnie cyfry roku, w którym zostało ono po raz pierwszy umieszczone,
- nazwa i adres siedziby producenta lub znak identyfikujący pozwalający w łatwy i jednoznaczny sposób określić nazwę i adres producenta,
- niepowtarzalny kod identyfikacyjny typu wyrobu,
- numer referencyjny deklaracji właściwości użytkowych,
- poziom lub klasa zadeklarowanych właściwości użytkowych,
- odniesienie do zharmonizowanej specyfikacji technicznej (hEN lub ETA),
- zamierzone zastosowanie wyrobu,
- numer identyfikacyjny jednostki notyfikowanej, jeżeli brała ona udział w procesie oceny wyrobu.

WAŻNE

Oznakowanie CE naniesione zgodnie z rozporządzeniem 305/2011 na wyrobie oznacza, że wyrób został poddany ocenie i ma potwierdzone właściwości użytkowe (te właściwości powinny być wskazane w DWU oraz w informacji towarzyszącej oznakowaniu CE).
Oznakowanie CE nie oznacza jednak, że dany wyrób jest odpowiedni dla użytkownika końcowego w danym państwie członkowskim UE. W każdym przypadku należy szczegółowo weryfikować, czy wskazane w DWU właściwości użytkowe są właściwe i na właściwym poziomie/klasie wymaganej przez przepisy techniczno-budowlane danego państwa członkowskiego.

W praktyce analiza oznakowania wyrobu i deklaracji właściwości użytkowych służy ocenie, czy dany wyrób można zastosować w danej inwestycji. Pozwala na ustalenie, czy wyrób:

- został poddany właściwemu procesowi oceny,
- ma odpowiednie właściwości użytkowe dla zamierzonego miejsca instalacji (np. na zewnątrz/wewnątrz budynku), odpowiednią klasę reakcji na ogień, odpowiednią czułość detekcji pożaru itp.,

a tym samym upewnienie się, że odbiorca dokonał odpowiedniego wyboru, a wyrób/system spełni swoje zadanie w budynku. Nie ulega wątpliwości, że zagadnienie to wymaga spokojnej i szczegółowej analizy. Należy zwrócić uwagę na kilka aspektów:

1. Certyfikat stałości właściwości użytkowych to dokument, który wydaje Jednostka Notyfikowana, i jest on potrzebny przede wszystkim producentowi do wystawienia deklaracji właściwości użytkowych i oznakowania wyrobu. Certyfikat jest wydawany na podstawie wyników badań konkretnych próbek wyrobu i potwierdza, że wymagania normy zharmonizowanej w zakresie wskazanych właściwości użytkowych mają zastosowanie do wyrobu oraz że producent wdrożył system produkcji (m.in. obejmujący szczegółową dokumentację techniczną wyrobu, odpowiednie procedury postępowania, wyposażenie produkcyjne i kontrolno-pomiarowe itp.), który zapewnia, że następne egzemplarze/partie tego samego wyrobu też będą mieć odpowiednie właściwości użytkowe (zapewniona jest stałość właściwości użytkowych). System zakładowej kontroli produkcji ZKP jest cyklicznie oceniany w ramach nadzoru nad udzielonym certyfikatem w celu utrzymania jego ważności (weryfikacja stałości właściwości użytkowych). W praktyce oznacza to, że certyfikat nie jest dokumentem wystarczającym do wprowadzenia wyrobu do obrotu/dla odbiorcy wyrobu.
2. Deklaracja właściwości użytkowych jest sporządzana przez producenta i umożliwia oznakowanie wyrobu CE. Jest potrzebna odbiorcom wyrobów, ponieważ tym dokumentem producent potwierdza, że sprzedane egzemplarze partie/wyrobu mają właściwości określone w tym dokumencie. W praktyce oznacza to, że dla obiorcy wyrobu największe znaczenie ma deklaracja właściwości użytkowych (DWU) i oznakowanie wyrobu, certyfikat zaś stanowi niejako uzupełnienie dokumentacji. Zderzenie zapisów deklaracji i certyfikatu pozwala także na potwierdzenie, czy producent zawarł w deklaracji informacje nt. potwierdzonych w certyfikacji właściwościach użytkowych. Zdarza się niestety, że występują rozbieżności pomiędzy tymi dwoma dokumentami.

Oznakowanie CE naniesione zgodnie z rozporządzeniem 305/2011 na wyrobie oznacza, że wyrób został poddany ocenie i ma potwierdzone właściwości użytkowe

3. Obowiązek stosowania oznakowania CE wynika z wielu rozporządzeń i dyrektyw UE. W przypadku elektronicznych systemów zabezpieczeń ppoż. (SSP, DSO, SKRDiC) należy zwrócić uwagę na fakt, iż oznakowanie CE na te wyroby jest nanoszone także ze względu na postanowienia dyrektywy niskonapięciowej 2014/35/UE oraz dyrektywy kompatybilności elektromagnetycznej 2014/30/UE. Może zatem wystąpić sytuacja, w której na wyrobie jest oznakowanie CE wynikające tylko z jednej lub z dwóch dyrektyw, ale nie będzie ono posiadało wszystkich elementów wymaganych rozporządzeniem 305/2011 (np. brak numeru jednostki notyfikowanej, brak normy zharmonizowanej, brak informacji o deklarowanych właściwościach użytkowych itp.). W takiej sytuacji nie można stwierdzić, że wyrób spełnia także wymagania rozporządzenia 305/2011, choć ma oznakowanie CE.
4. Europejskie certyfikaty zgodności wydawane przed wejściem w życie rozporządzenia 305/2011 (CPR) na podstawie dyrektywy budowlanej 89/106/WE (CPD) pozostają nadal ważne, jeżeli w wyrobach nie wprowadzono istotnych zmian i nie zmieniła się norma zharmonizowana. Producenci mogą nadal ich używać do wystawienia DWU. W rzadkich przypadkach odbiorca wyrobu może się spotkać z następującą sytuacją:

- Certyfikat zgodności CPD + deklaracja właściwości użytkowych wyrobu + oznakowanie CE

  Certyfikaty zgodności CPD nie zawierają nistety informacji o właściwościach użytkowych. Nie jest wówczas możliwe wyłapanie ewentualnych rozbieżności pomiędzy DWU a certyfikatem. W uzasadnionych przypadkach można poprosić producenta o udostępnienie sprawozdań z badań w celu wyjaśnienia wątpliwości.

5. Warto posiłkować się także wykazami wydanych certyfikatów prowadzonymi przez Notyfikowane Jednostki Certyfikujące na stronach internetowych – wykazy takie stanowią niejako katalog sprawdzonych urządzeń, w którym każdy uczestnik rynku może sprawdzić, czy dany wyrób i jego producent zostali ocenieni z wynikiem pozytywnym.

MŁ. BRYG. MGR INŻ. GRZEGORZ MROCZKO

Absolwent SGSP, oficer PSP, pracownik Zakładu Ocen Technicznych CNBOP-PIB, koordynator ds. testowania wyrobów innowacyjnych wg procedury KG PSP, przedstawiciel Polski w TC 72 Europejskiego KT (CEN), członek KT 264 i KT 323 PKN. Od ponad 18 lat aktywny audytor jednostki certyfikującej w zakresie m.in. systemów sygnalizacji pożarowej, DSO, systemów wentylacji pożarowej, kabli i zespołów kablowych stosowanych w technicznych systemach zabezpieczeń ppoż.

Spotkanie Partnerów Schrack Seconet Polska

Nieprzerwanie od kilkudziesięciu lat firma Schrack Seconet Polska Sp. z o.o. organizuje spotkanie swoich najlepszych Partnerów w Polsce.

Spotkania Autoryzowanych Partnerów Schrack Seconet Polska mają już długoletnią tradycję. Ich celem jest przede wszystkim podsumowanie roku minionego oraz wspólne opracowanie i omówienie najważniejszych planów i strategii działania na rynku systemów zabezpieczeń w Polsce w kolejnych latach.
Tegoroczna edycja odbyła się w połowie marca, tym razem w malowniczo położonym hotelu Mikołajki Leisure *** na mazurskiej Ptasiej Wyspie.**

Rok 2021 był wyjątkowy dla Schrack Seconet pod wieloma względami. Lista referencyjna producenta powiększyła się o kolejnych kilkaset wyjątkowych, zaawansowanych technologicznie obiektów, a grono certyfikowanych specjalistów zwiększyło się o kilkuset inżynierów! Mimo ograniczeń związanych z pandemią i jej skutkami zanotowano rekordową liczbę sprzedanych systemów bezpieczeństwa i komunikacji oraz systemów integrujących urządzenia przeciwpożarowe.

W tegorocznym spotkaniu wzięło udział ponad 100 przedstawicieli firm partnerskich – głównie członków szczebla zarządzającego. Spotkanie rozpoczął Prezes Zarządu Schrack Seconet w Polsce Michał Sidor, przedstawiając wyniki sprzedaży całej grupy partnerskiej. Oprócz prezentacji przygotowanych przez zespół Schrack Seconet, które dotyczyły m.in. analizy rynku, zrealizowanych obiektów referencyjnych, nowości produktowych i działań marketingowych, niezwykle ważnymi punktami spotkania były kuluarowe dyskusje nt. możliwości rozwojowych branży bezpieczeństwa w Polsce, zmian, jakie czekają producentów poszczególnych rozwiązań w związku z dynamiczną sytuacją na świecie czy znaczenia firm partnerskich w tworzeniu nowych wartości dla całego rynku krajowego.

Firma Schrack Seconet, podsumowując ubiegłoroczne wyniki i działania, przyznała tytuł Partnera Roku firmie RS-SYSTEM Sp. z o.o. z siedzibą w Michałowicach za najlepszy wynik w sprzedaży systemów sygnalizacji pożarowej Schrack Seconet w roku 2021 oraz wysoką jakość usług.

Do grona Autoryzowanych Partnerów w Polsce przyjęto i wyróżniono kolejne, znane i cenione firmy z branży bezpieczeństwa pożarowego: DRS Sp. z o.o. z Lublina, Fire Technology s.c. z Torunia oraz TRAFO Sp. z o.o. z Warszawy.

Wręczenie nagród, a tym samym dołączenie do grona Partnerów Autoryzowanych, potwierdza wysoką etykę współpracy, profesjonalizm, indywidualne podejście do oczekiwań klientów oraz stabilną sytuację finansową wyróżnionych przedsiębiorstw.

Podczas spotkanie przyznano także kilka wyróżnień.

Za wysoką jakość usług i kompetencje wyróżniono udziałem w spotkaniu kilkudziesięciu dotychczasowych Partnerów producenta – Autoryzowanych Partnerów Wiodących, Autoryzowanych Partnerów oraz przedstawicieli firm Preautoryzowanych, którzy istotnie przyczynili się do rozwoju organizacji w Polsce. Regularne szkolenia i nieustanne podnoszenie kwalifikacji zatrudnionych przez te firmy specjalistów mają przełożenie na wysokie zadowolenie użytkowników systemów bezpieczeństwa, co stanowi najwyższą wartość dla wszystkich uczestników rynku.

Autoryzowani Partnerzy Schrack Seconet, wraz z wąską grupą Partnerów Wiodących i szerokim wsparciem Partnerów Preautoryzowanych, stanowią największą zorganizowaną grupę specjalistów – przedstawicieli konkretnego producenta w branży systemów przeciwpożarowych, których kompetencje są dokumentowane stosownymi certyfikatami, a wiedza regularnie (nie rzadziej niż co 24 mce) aktualizowana.

Więcej na www.schrack-seconet.pl

Młoda kadra dla branży

fot. Instytut Systemów Elektronicznych Wydział Elektroniki WAT

7. edycja Seminarium Branży Elektronicznych Systemów Bezpieczeństwa połączonego z konkursem o miano Mistrza Elektronicznych Systemów Bezpieczeństwa odbyła się 1 lutego 2022 r. w Instytucie Systemów Elektronicznych Wydziału Elektroniki WAT.

To cykliczne wydarzenie, organizowane głównie dla studentów specjalności Inżynieria Systemów Bezpieczeństwa w ramach kierunku Elektronika i Telekomunikacja stanowi forum wymiany doświadczeń uczestniczących w nim firm z branży ESB. W tym roku z powodów epidemicznych Seminarium i Konkurs dla studentów zorganizowano w formie zdalnej na platformie MS Teams.
Uczestniczyły w nim firmy: AAT Systemy Bezpieczeństwa, Bosch Security Systems, Hikvision Poland, ICS Polska, ID Electronics, Janex International, MR System, Polon-Alfa, Pulsar, Roger, Satel, Schrack Seconet oraz Polska Izba Systemów Alarmowych (PISA). W tym roku pojawiła się jako partner akademicki Szkoła Główna Służby Pożarniczej.
Tematem przewodnim tegorocznego Seminarium była „Współpraca Elektronicznych Systemów Bezpieczeństwa z systemami Monitoringu Wizyjnego" i większość spośród 14 prezentacji przygotowanych przez firmowych gości nawiązywała do ogólnego tematu spotkania. Zaprezentowano m.in:

- System integrujący urządzenia przeciwpożarowe – studia przypadków (Schrack Seconet);
- Wspomaganie systemów monitoringu wizyjnego poprzez algorytmy analizy wideo (Bosch Security and Safety Systems);
- Współpraca elektronicznych systemów bezpieczeństwa z systemami monitoringu wizyjnego – NMS AC (AAT Systemy Bezpieczeństwa);
- Automatyczne gaszenie – kluczowy system bezpieczeństwa i jego integracja w ramach zabezpieczeń pożarowych (Polon-Alfa);
- AI – Przyszłość systemów zabezpieczeń (Hikvision);
- Scenariusze i możliwości współpracy systemów CCTV i KD na przykładzie systemu RACS 5 firmy Roger;
- INTEGRUM, manipulatory INT-TSI (Satel);
- Zasilanie buforowe systemów PoE (Pulsar).

W konkursie o tytuł Mistrza Elektronicznych Systemów Bezpieczeństwa wyłoniono 10 laureatów. Zwycięzcą i zdobywcą statuetki MESB został Kamil Olszewski, student IV roku specjalności ISB na kierunku EiT. Tytuł pierwszego i drugiego wicemistrza wywalczyli odpowiednio Damian Boguski i Marek Ledworowski. Kolejnych siedmiu laureatów z największą liczbą punktów otrzymało wyróżnienia.
Cieszy fakt, że wśród prelegentów seminarium są absolwenci naszej instytutowej specjalności. Bliski kontakt studentów z czołowymi firmami jest dla nich okazją do zaznajomienia się z najnowszymi rozwiązaniami branży elektronicznych systemów bezpieczeństwa, zwłaszcza że jako absolwenci podejmują pracę w firmach współpracujących z Wydziałem Elektroniki.

Bezp. inf. SBESB

Więcej na https://wel.wat.edu.pl/

Konferencja Branży Ochrony

z wojennymi zagrożeniami bezpieczeństwa w tle

Na przełomie marca i kwietnia br. odbyła się 22. Konferencja Branży Ochrony zorganizowana przez Polską Izbę Ochrony. Organizator zdecydował się rozszerzyć tematykę wydarzenia o elementy dotyczące wsparcia systemu bezpieczeństwa państwa w następstwie wojny w Ukrainie i wynikających z tego zagrożeń terrorystycznych, realnych także w Polsce.

Podczas trwającej dwa dni konferencji członkowie Polskiej Izby Ochrony, zaproszeni eksperci i praktycy z wielu obszarów związanych z bezpieczeństwem mogli wymienić się doświadczeniami i poszerzyć wiedzę w zakresie zabezpieczeń obiektów niepodlegających obowiązkowej ochronie.
Wiele prelekcji stanowiło kompendium wiedzy o procedurach, możliwościach wykorzystania sektora ochrony w reagowaniu na zagrożenia w przestrzeni publicznej i wojennego państwa (dr Natalia Moch, ppłk rez. dr inż. Tomasz Białek), współdziałaniu służb ochrony z klientami korporacyjnymi (Wojciech Gradowski), przeciwdziałaniu zagrożeniom terrorystycznym i hybrydowym (dr Rafał Batkowski), zapobieganiu dywersji – infiltracji w obiektach użyteczności publicznej (Jarosław Jaźwiński) oraz zadaniach sektora ochrony w ostrzeganiu, alarmowaniu i ewakuacji podczas sytuacji kryzysowych (mjr rez. dr inż. Jarosław Stelmach).
Wymienione wystąpienia wzbogacono tematami prawidłowego podejścia do ochrony perymetrycznej (Jakub Sobek), ryzyka branży ochrony w kontekście wojny na Ukrainie (mjr rez. mgr inż. Jacek Grzechowiak) i specustawy o pomocy obywatelom Ukrainy (Rafał Wyziński).
Ciekawym akcentem wydarzenia były wystąpienia Krzysztofa Ciesielskiego na temat roli nowoczesnego marketingu w rozwoju branży ochrony w Polsce oraz radcy prawnego Sylwii Kilińskiej dotyczące najpowszechniejszych czynów nieuczciwej konkurencji.

Na fotorelację z konferencji zapraszamy na portal aspolska.pl

Integracja systemu RACS 5

z serwerowymi systemami windowymi firm KONE i SCHINDLER

Stosowanie systemów windowych do zarządzania ruchem *(Destination Dispatch System)* optymalizuje przepływ osób w obiekcie, pozwala zredukować koszty eksploatacji wind oraz zużycia energii elektrycznej, a także podnosi komfort korzystania z obiektu.

System kontroli dostępu i automatyki budynkowej RACS 5 w wersji Enterprise (Roger) oferuje możliwość integracji programowej z systemami windowymi firm KONE i Schindler. Integracja systemu RACS 5 z wymienionymi systemami windowymi pozwala na centralne zarządzanie użytkownikami obu zintegrowanych systemów z poziomu programu VISO przeznaczonego do zarządzania systemem RACS 5.
W ramach omawianej integracji można m.in.

- przypisać użytkownikowi profil definiowany po stronie systemu windowego, określający uprawnienia użytkownika w zakresie kontroli dostępu do wind i pięter;
- definiować identyfikatory dla użytkownika wind, dzięki czemu użytkownik może stosować ten sam identyfikator, co w systemie KD; funkcja ta umożliwia wykorzystanie w systemie windowym metod identyfikacji dostępnych w systemie RACS 5 (karta, odcisk palca, telefon itd.);
- definiować domyślne piętro, na które winda zawiezie użytkownika po pomyślnej identyfikacji.

Ponadto integracja z systemem windowym KONE umożliwia definiowanie trybu przywoływania windy przez użytkownika (np. dla osoby z niepełnosprawnościami, priorytet itp.).
Integracja systemu kontroli dostępu RACS 5 z systemem windowym została z powodzeniem wdrożona w trójmiejskim kompleksie biurowym 3T Office Park w Gdyni, sprawdziła się również w dwóch warszawskich wieżowcach. W fazie przygotowania są kolejne projekty, w których przewidziano zastosowanie tego rozwiązania.

Więcej na www.roger.pl

Nowości firmy Axis

Aplikacja DataFromSky

Axis Communications i czeski twórca oprogramowania DataFromSky prezentują FLOW Traffic – nową aplikację dedykowaną kamerom sieciowym Axis z procesorem *deep learning* (DLPU). Oprogramowanie jest kolejną odsłoną uniwersalnej platformy analizy ruchu FLOW, która potrafi zmienić kamerę IP w licznik rowerzystów, detektor czerwonego światła, narzędzie do monitorowania obłożenia parkingów czy adaptacyjnego zarządzania skrzyżowaniami.

FLOW Traffic jest już dostępna poprzez Axis Camera Application Platform (ACAP). – Oprogramowanie *DataFromSky*, do tej *pory dostarczane jako rozwiązanie serwerowe, chmurowe lub w ramach systemów wbudowanych, ma już ponad 5000 użytkowników w ponad 50 krajach na świecie. Cieszymy się, że możemy zaprezentować FLOW jako aplikację dla nowych kamer Axis z modułem DLPU* – podkreśla Konrad Badowski z Axis Communications.

FLOW Traffic pozwala użytkownikowi kilkoma kliknięciami zamieni kamerę Axis w czujnik ruchu. Uzyskane dane można wizualizować poprzez interaktywne widgety i udostępniać systemom innych firm przez otwarty interfejs API.
Aplikację zaprojektowano do pracy w czasie rzeczywistym. FLOW Traffic można zintegrować z platformami smart city i systemami VMS. Obsługuje także wiele urządzeń peryferyjnych i moduły I/O.

KAMERA + SZTUCZNA INTELIGENCJA = UNIWERSALNY CZUJNIK

– Budując inteligentne miasto, potrzebujemy inteligentnych czujników, które dostarczą niezbędnych danych. A gdyby istniał jeden czujnik, pozwalający określić, co mierzyć i jak komunikować się z innymi elementami infrastruktury? W DataFromSky widzimy taki czujnik w połączeniu kamery ze sztuczną inteligencją analizującą obraz w czasie rzeczywistym. Współgra to z rozwojem kamer Axis IP i ich zintegrowanym modułem głębokiego uczenia – mówi David Herman z DataFromSky.
FLOW Traffic wykorzystuje zaawansowaną technologię przetwarzania obrazu i zoptymalizowany algorytm przetwarzania trajektorii ruchu, rozpoznawania typów pojazdów, ich kolorów i tablic rejestracyjnych. Zmniejsza to koszty zakupu, eksploatacji i integracji w projektach inteligentnych parkingów, zarządzania ruchem, monitorowania pasażerów czy ochrony obiektów.

Nowa kamera nasobna

AXIS W101 Body Worn Camera to innowacyjna kamera „dla każdego", zaprojektowana w taki sposób, by zalety technologii nasobnych stały się dostępne dla użytkowników różnych branż i rynków.

Kamera AXIS W101 sprawdza się w większej liczbie zastosowań niż dotychczasowy model kamery nasobnej, ponieważ jest oferowana w dwóch kolorach: białym zapewniającym dyskrecję oraz czarnym, gdy priorytetem jej stosowania jest zwrócenie uwagi bądź odstraszenie. Oferowana z kamerą aplikacja mobilna do przeglądania materiału i dodawania etykiet jest idealnym rozwiązaniem dla każdego użytkownika, któremu zależy na szybkim i łatwym dostępie do materiału wizyjnego.
Obraz i dźwięk z kamery mają wysoką jakość, zapewniając wyjątkową ostrość każdej klatki oraz tłumienie hałasu. Obraz ma naturalne kolory z małą ilością szumu w słabo oświetlonych scenach oraz lepszy kontrast i ostrość w porównaniu z dotychczasowym modelem, a krótszy czas otwarcia migawki pozwala zredukować rozmycie obiektów w ruchu. Udoskonalone mocowanie stabilizuje rejestrowany obraz niezależnie od sytuacji. Specjalna funkcja wzmacnia głos, aby mowa była dobrze słyszalna.
W porównaniu ze swoją poprzedniczką AXIS W101 obsługuje więcej systemów GNSS, m.in. GPS, Glonass i Galileo i pozwala skuteczniej śledzić lokalizację. Nagrywanie rozpoczyna się jednym dotknięciem dużego, łatwo dostępnego przycisku, a urządzenie nagrywa do 90 s materiału jeszcze przed przyciśnięciem przycisku, umożliwiając zarejestrowanie całego zdarzenia.
Nowa kamera nasobna oparta na otwartych standardach umożliwia łatwą integrację z oprogramowaniem AXIS Camera Station i AXIS Case Insight, a także z zewnętrznymi systemami VMS i EMS działającymi lokalnie lub w chmurze.
Czas pracy kamery wynosi nawet 17 godz., a przy rozdzielczości 1080p przekracza 12 godzin. Urządzenie ładuje się przy użyciu dowolnej ładowarki USB-C. Technologia Axis Zipstream pozwala na zapisanie dowolnej ilości materiału wizyjnego bez negatywnego wpływu na jego jakość.
Dzięki kompleksowemu szyfrowaniu AXIS W101 spełnia standardy cyberbezpieczeństwa FBI. Ponadto funkcja Axis Edge Vault chroni identyfikator urządzenia Axis i upraszcza autoryzację urządzeń Axis w sieci.

Więcej na www.axis.com/pl

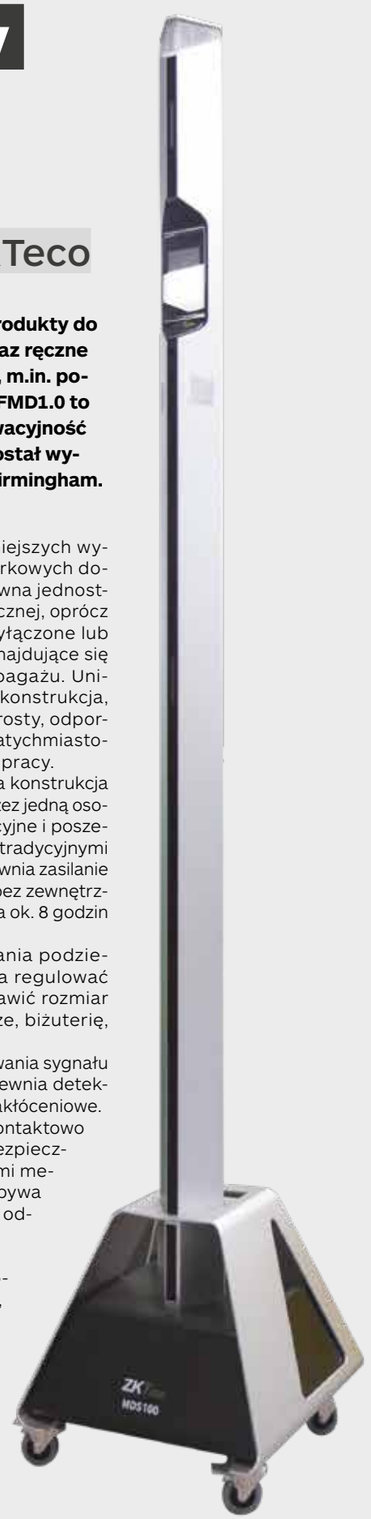
Innowacyjny wykrywacz metali

FMD 1.0. firmy ZKTeco

Firma ZKTeco ma w ofercie różne produkty do rentgenowskiej inspekcji bagaży oraz ręczne i automatyczne wykrywacze metali, m.in. popularne bramki. Wykrywacz metali FMD1.0 to nowy produkt, który za swoją innowacyjność i wyższy poziom bezpieczeństwa został wyróżniony na targach IFSEC 2021 w Birmingham.

FMD1.0 jest jednym z najskuteczniejszych wykrywaczy metali i telefonów komórkowych dostępnych na rynku. Ta całkowicie pasywna jednostka oparta na technologii ferromagnetycznej, oprócz metali potrafi wykrywać włączone, wyłączone lub zdemontowane telefony komórkowe znajdujące się przy kontrolowanej osobie lub w jej bagażu. Unikalna jednokolumnowa wolnostojąca konstrukcja, wbudowany intuicyjny wyświetlacz i prosty, odporny na uszkodzenia interfejs ułatwiają natychmiastowy montaż i wdrożenie urządzenia do pracy.
Kompaktowy rozmiar i lekka aluminiowa konstrukcja ułatwiają też przenoszenie urządzenia przez jedną osobę, co dodatkowo obniża koszty operacyjne i poszerza jego zastosowania w porównaniu z tradycyjnymi bramkami. Wbudowany akumulator zapewnia zasilanie przez ponad 28 godzin pracy w terenie bez zewnętrznego zasilania. Pełny cykl ładowania trwa ok. 8 godzin i nie zakłóca ciągłej pracy urządzenia.
Dla większej precyzji strefę wykrywania podzielono na dwie części, a czułość można regulować w zakresie 100 poziomów. Można ustawić rozmiar metalu, wyłączając np. monety, klucze, biżuterię, klamrę paska itp.
System cyfrowego przetwarzania i filtrowania sygnału oparty na technologii *Digital Pulse* zapewnia detektorowi doskonałe właściwości przeciwzakłóceniowe. Urządzenie potrafi przeskanować bezkontaktowo ponad 50 osób/minutę, jest w 100% bezpieczne dla kobiet w ciąży i osób z implantami medycznymi. Skanowanie całego ciała odbywa się podczas pojedynczego przejścia w odległości do 1 m od osi urządzenia.

Wykrywacz FMD1.0 został zaprojektowany do pracy w trudnych warunkach, m.in. w zakładach produkcyjnych, zarówno w pomieszczeniach, jak i na zewnątrz (klasa wodoszczelności IPX5). Ma szerokie zastosowanie – podczas wystaw i konferencji, imprez firmowych, w nocnych klubach, obiektach użyteczności publicznej i rządowych. Sprawdza się doskonale w magazynach, węzłach towarowych czy zakładach karnych.



Więcej na www.zkteco.eu

Interkom TID-600R

wspomaga pracę służb ochrony

Hanwha Techwin wprowadza na rynek nowy wielofunkcyjny interkom TID-600R o wysokich parametrach użytkowych. Znajdzie on wiele zastosowań, m.in. jako punkt kontaktowy w systemach informacyjnych i dyspozytorskich czy punkt przywoławczy w systemach zabezpieczających.

W interkomie TID-600R zastosowano kamerę o rozdzielczości 2 Mpix z obiektywem szerokokątnym typu „rybie oko" o kącie widzenia w poziomie 180°, w pionie 114°. Kamera ma wbudowane funkcje analizy treści obrazu, jest wyposażona w oświetlacz IR o zasięgu 5 m oraz układ rozszerzający zakres dynamiki obrazu. Pozwala to na prowadzenie obserwacji w złych warunkach oświetleniowych. Interkom jest zgodny z wymaganiami NDAA.

Interkom może być stosowany w wielu różnych obiektach, np. w placówkach opieki zdrowotnej (gdzie priorytetem jest bezdotykowa kontrola dostępu), na parkingach, w pojazdach transportu publicznego (w celu poprawy obsługi) oraz w budynkach biurowych i mieszkalnych, umożliwiając bezproblemowe przepuszczanie osób wchodzących i wychodzących.

TID-600R nie ma klasycznych przycisków, to system bezdotykowy, inicjujący połączenia interkomowe w reakcji na gesty wykonywane rękami. Rozwiązania bezdotykowe zyskały na znaczeniu w dobie pandemii COVID. Nie wymagają częstego czyszczenia i ograniczają ryzyko infekcji. Opcję bezdotykową można łatwo włączać i wyłączać za pomocą intuicyjnego interfejsu użytkownika interkomu.

Kamery użyte w interkomach TID-600R mogą przekazywać informacje o zaobserwowanych zdarzeniach do innych kamer pracujących w systemie dozorowym. Ta funkcja może być stosowana do sterowania kamerami PTZ w celu ich naprowadzania na zauważone obiekty. Na podobnej zasadzie inteligentne funkcje analizy treści obrazu mogą dostarczać informacje pracownikom służb ochrony obiektów.

Interkomy TID-600R są montowane w estetycznych metalowych obudowach w kolorze białym lub szarym, o wysokiej odporności na działanie czynników środowiskowych. Spełniają wymagania klas IP65 i IK08 oraz NEMA 4X, dzięki temu chronią urządzenia przed kurzem, wodą i innymi szkodliwymi czynnikami środowiskowymi.

Obudowy mają zabezpieczenia przeciwsabotażowe, operatorzy systemów dozorowych są ostrzegani o próbach manipulacji przy urządzeniu.

Wygląd interkomów można dostosować do specyfiki obiektów, w których są instalowane, bowiem producent oferuje dodatkowe uchwyty i inne akcesoria (zamawiane osobno).

Więcej na https://bit.ly/3wkx9eC

Kamery wieloprzetwornikowe

ze sztuczną inteligencją

Jednym z flagowych celów strategii i-PRO jest wzbogacanie oferty o rozwiązania oparte na sztucznej inteligencji, dlatego też nowe kamery są fabrycznie wyposażone w cztery wydajne aplikacje analityczne AI.

Nowe kamery wieloprzetwornikowe i-PRO są dostępne z trzema lub czterema przetwornikami obrazu o rozdzielczości 4K, 6 Mpix i 4 Mpix, co zapewnia wyjątkowo szczegółowy obraz w zakresie 180° lub 360°. Wszystkie te funkcje są wbudowane w najcieńszą i najbardziej dyskretną konstrukcję dostępną obecnie na rynku, dzięki czemu seria ta wyznacza nowe standardy w branży zabezpieczeń.

Kamery wyposażono w procesor sztucznej inteligencji umożliwiający analitykę opartą na głębokim uczeniu się, która ułatwia i przyspiesza wykrywanie osób i pojazdów. Pakiet SDK sprawia, że nowa seria jest w pełni otwarta na aplikacje innych producentów. Modele oferują szerszy zasięg i większy zakres pochylenia niż inne porównywalne modele dostępne na rynku, a także – w wybranych modelach – oświetlenie IR LED. Zdolność do autonomicznego wykrywania i rozróżniania obiektów na dużych obszarach umożliwia pracownikom ochrony skupienie się na rzeczywistych zdarzeniach, co skutecznie zwiększa ich produktywność przy jednoczesnej poprawie ogólnego poziomu bezpieczeństwa.

Zgodnie ze standardami dotyczącymi wysokiego poziomu bezpieczeństwa i integralności danych z systemów dozoru wizyjnego, nowe kamery wielosensorowe i-PRO są również wyposażone w wiodące w branży szyfrowanie FIPS 140-2 na poziomie 3, zabezpieczone przez zewnętrznego dostawcę certyfikatów. Dzięki temu kamery idealnie nadają się do szerokiej gamy zastosowań wymagających wysokiego poziomu bezpieczeństwa, np. w monitoringu miast i budynków, logistyce, przemyśle i transporcie.

Więcej na https://i-pro.com/eu/en/surveillance

Nowości firmy ZETTLER

Sygnalizatory akustyczne z lampą sygnałową

Produkty ZETTLER wykorzystują sieciową technologię MZX, która zapewnia zaawansowane możliwości wykrywania pożarów. Dzięki temu system jest jednym z najbardziej odpornych, niezawodnych i serwisowalnych systemów dostępnych na rynku, o szerokiej zgodności z normami światowymi i certyfikatami.

Eksperci firmy ZETTLER opracowali nową serię sygnalizatorów akustycznych z lampą sygnałową, wchodzących w skład urządzeń sygnalizacji optycznej *(VID – Visual Indicating Device)*.

Urządzenia przeszły rygorystyczne testy sytuacyjne, ze szczególnym uwzględnieniem wymagań normy EN54 część 23., co umożliwiło zwiększenie wydajności nowej gamy produktów. W połączeniu z ekspercką wiedzą w zakresie technologii i systemów wykrywania pożarów stanowią gamę urządzeń najwyższej klasy – zaawansowanych, spełniających wszystkie aktualne normy i wymagania produktów. Dzięki temu system jest odpowiedni do ekstremalnie trudnych, wrażliwych środowisk.

SYGNALIZATORY OPTYCZNE

Zwykle są używane jako dodatkowe wskazanie mające podnieść świadomość sytuacyjną. W przypadku wystąpienia zdarzenia nie można ich jednak stosować jako jedynego sposobu ostrzegania ludzi o potencjalnym zagrożeniu.

ADRESOWALNE ŚCIENNE SYGNALIZATORY AKUSTYCZNE Z LAMPĄ SYGNAŁOWĄ

Przed zastosowaniem jakiegokolwiek rozwiązania wskazane jest przeprowadzenie oceny ryzyka pożarowego obszaru, który ma być objęty ochroną. To określi rodzaj i specyfikację wymaganych urządzeń. Wymagane jest stosowanie sygnalizatorów akustycznych jako integralnej części systemu wykrywania i sygnalizacji pożarowej, ponieważ są one uważane za najważniejsze ze wszystkich urządzeń alarmowych.

Seria kompaktowych adresowalnych sygnalizatorów akustycznych ściennych P80AI z lampą sygnałową VID obejmuje trzy modele: P80AIW, P80AIR i P85AIR. Wszystkie charakteryzują się tą samą specyfikacją niskoprądową i wysoką mocą wyjściową: modele wewnętrzne z czerwonym i białym korpusem oraz wersja P85AIR o stopniu ochrony IP55, do użytku na zewnątrz lub do zastosowań w trudnych warunkach środowiskowych. Wszystkie modele są zgodne z wymaganiami EN54-3, 17.

ADRESOWALNE SYGNALIZATORY AKUSTYCZNE ORAZ AKUSTYCZNE Z LAMPĄ SYGNAŁOWĄ, UMIESZCZONE W PODSTAWIE CZUJKI

P80SB to adresowalny sygnalizator akustyczny w podstawie czujki, przeznaczony specjalnie do użytku z adresowalnymi czujkami ZETTLER. Umieszczony w podstawie czujki sygnalizator akustyczny alarmu pożarowego ma własny adres, dzięki czemu może być monitorowany i sterowany z centrali sygnalizacji pożarowej; pozostaje niezależny od czujki. Zarówno zasilanie, jak i komunikację dla sygnalizatora i czujki zapewnia dwuprzewodowa pętla cyfrowa. Pomaga to obniżyć koszty instalacji, ponieważ nie jest wymagane dodatkowe okablowanie.

Model P80AIB zawiera adresowalny sygnalizator akustyczny z lampą sygnałową (VID).

Więcej na https://www.zettlerfire.com/Pol_Index.asp

Czytniki kart szyfrowanych ACI42x

marki Aritech

Czytniki kart szyfrowanych to bezkompromisowy wzrost bezpieczeństwa systemu kontroli dostępu. Nowe czytniki serii ACI42x-W obsługują karty szyfrowane Mifare® DESFire®, które mogą korzystać z własnych kluczy szyfrujących, pozwalając użytkownikowi na tworzenie unikalnych identyfikatorów kompatybilnych wyłącznie z czytnikami zastosowanymi w jego obiekcie.

Czytniki wyposażono w głowice obsługujące komunikację w standardzie Bluetooth (BLE), co otwiera możliwości tworzenia systemów szyfrowanego identyfikatora mobilnego.
Seria czytników ACI42x-W obejmuje 4 różne modele, wszystkie wyposażone w kabel typu pigtail o długości 3 m. Wszystkie modele mają solidną obudowę o nowoczesnym wyglądzie. Wysoki standard wykonania pozwala na montaż wewnątrz lub na zewnątrz (pracują nawet w trudnych warunkach atmosferycznych).
Czytniki mają swobodnie programowalne 3 wielokolorowe diody LED! Uniwersalność rozwiązania zapewnia otwarta technologia zastosowanych interfejsów, która sprawia, że nowe czytniki mogą być zastosowane w systemach różnych producentów.
Do wyboru są dwa interfejsy: szyfrowany dwukierunkowy OSDP® v.2 oraz klasyczny Wiegand, który, choć nie jest szyfrowany, umożliwia wykorzystanie tych czytników do podwyższenia poziomu zabezpieczeń również starszych systemów.
Aritech jest globalną marką firmy Carrier Fire & Security tworzącą rozwiązania zabezpieczeń dla klientów prywatnych, komercyjnych i korporacyjnych. Oferuje zintegrowaną platformę bezpieczeństwa w obszarze systemów alarmowych, kontroli dostępu, dozoru wizyjnego i wykrywania pożaru.
Zainteresowane osoby mogą kontaktować się z bezpośrednio z przedstawicielami handlowymi, wykwalifikowanymi instalatorami i integratorami.

Więcej na:
pl.firesecurityproducts.com

System napłotowy BeeS

BeeS to unikatowy na rynku system dualny, który może pracować z wykorzystaniem zarówno sensorów piezoelektrycznych, jak i mikrofonowego kabla sensorycznego. Dzięki temu można go z powodzeniem stosować na różnego rodzaju ogrodzeniach, zarówno siatkowych, jak i modułowych spawanych czy palisadowych.

System BeeS, mając elastyczną konstrukcję, może chronić zarówno krótkie ogrodzenia do kilkudziesięciu metrów, jak i bardzo rozległe o długości nawet 26 km.
Wbudowany DSP (cyfrowy procesor obróbki sygnału) zapewnia wysoką skuteczność detekcji intruzów (powyżej 99%), przy współczynniku niechcianych (fałszywych) alarmów na poziomie nie większym niż 1%.
Wbudowane wyjścia przekaźnikowe pozwalają w prosty sposób podłączyć go do każdego systemu alarmowego czy dozoru wizyjnego. Ale co najważniejsze, system BeeS jest łatwy w instalacji i konfiguracji, można go zamontować bardzo szybko (nie wymaga szczegółowej wiedzy technicznej od instalatora).
System ochrony ogrodzenia BeeS jest skutecznym rozwiązaniem w atrakcyjnej cenie, które może zapewnić bezpieczeństwo różnych obiektów, zarówno prywatnych posiadłości, jak i obiektów infrastruktury krytycznej.

Więcej na: www.linc.pl

BCS MANAGER

Program do obsługi urządzeń CCTV marki BCS.

Powstał w celu obsługi urządzeń wielu linii produktowych jedną aplikacją. Dzisiaj jest już zaawansowanym programem, którego może używać zarówno indywidualny użytkownik jak i duże centra monitoringów. Aplikację cechuje łatwość i intuicyjność obsługi oraz zaimplementowanie wielu funkcji rozszerzających codzienną pracę operatora.

BCS®

dla profesjonalistów

POLSKA MARKA BCS

android iOS Windows

Google Play App Store Windows Store