02 (38) / 2023

CZASOPISMO RYNKU SECURITY

a&S POLSKA

www.aspolska.pl

Raport: Infrastruktura krytyczna

20 zł
(w tym 8% VAT)

ISSN 2451-5175

Najlepsza polityka w sieci

Nigdy nie ufaj, zawsze weryfikuj. Poznaj najlepsze praktyki dotyczące cyberbezpieczeństwa (s. 46).

Na pierwszej linii obrony

Grunt to dobra strategia i technika 5D. Jak zmniejszyć ryzyko dzięki ochronie obwodowej? (s. 56).

Odbudowa Ukrainy

Polska wobec powojennej odbudowy Ukrainy. Moralny obowiązek i... szansa dla biznesu (s. 72).

Czy jest bezpiecznie?

Od końca lat 80. XX wieku Centrum Badania Opinii Społecznej (CBOS) sprawdza, co Polacy sądzą na temat bezpieczeństwa publicznego, jak je oceniają i czy czują się w kraju bezpiecznie. Zdecydowana większość badanych, bo aż 83% nie ma dziś wątpliwości i uważa Polskę za kraj, w którym żyje się bezpiecznie. Jest tak mimo wojny toczącej się tuż za wschodnią granicą. Jednak pojawiające się coraz częściej doniesienia medialne powodują, że poczucie braku zagrożenia może zostać wystawione na próbę.

W artykule *Nieoczekiwana lekcja hiszpańskiego* (str. 22) piszemy o jednym z takich przypadków. Gdy oddajemy ten numer do druku, gorącym tematem jest sprawa zatrzymania aż 9 osób podejrzanych o współpracę z rosyjskimi służbami specjalnymi. Zgromadzone przez ABW materiały dowodzą, że grupa zatrzymanych prowadziła monitoring tras kolejowych, a ich celem było m.in. rozpoznanie, monitorowanie i dokumentowanie transportów z uzbrojeniem realizowanym na rzecz Ukrainy. W związku z tym na trasach kolejowych oraz w krajowej infrastrukturze krytycznej wprowadzony został alert bezpieczeństwa. Polecamy lekturę wywiadu z dr Karoliną Wojtasik (str. 32), ekspertką Rządowego Centrum Bezpieczeństwa, specjalizującą się w dziedzinie ochrony obiektów infrastruktury krytycznej oraz terroryzmu. Dlaczego polecamy? Bo pada w tym wywiadzie pytanie o dalsze losy RCB. Projekt ustawy o ochronie ludności oraz o stanie klęski żywiołowej przewiduje bowiem, że instytucja w obecnym kształcie przestanie istnieć. Co wówczas? Tym razem kolejne badanie CBOS, pytające Polaków o poczucie bezpieczeństwa, może wypaść nieco gorzej...

Przygotowanie tego numeru było dla nas sporym dziennikarskim i detektywistycznym wyzwaniem. Postawiliśmy sobie za cel m.in. zgromadzić informacje, w co będzie inwestowała w najbliższym czasie IK (str. 26), przygotować kompleksowy raport (str. 14) oraz mapę inwestycji w Polsce (str. 70) i dowiedzieć się, co dla firm z naszego sektora oznacza plan odbudowy wciąż walczącej Ukrainy (str. 72). O ile z pomocą niezawodnych ekspertów udało nam się trzy z czterech celów osiągnąć, o tyle pierwsze pytanie wciąż pozostaje bez odpowiedzi. Dlaczego? Bo w obiektach IK w Polsce pracują ludzie odpowiedzialni, którzy ważą słowa i znają ich moc. Zdają sobie sprawę z ciążącej na nich odpowiedzialności za bezpieczeństwo nas wszystkich. Konsekwentnie odmawiali nam dostępu do informacji lub udzielili nam odpowiedzi bardzo ogólnych, nie zdradzając tym samym żadnych szczegółów. Dzięki tym, którzy zgodzili się z nami porozmawiać, mogliśmy napisać o największych dziś wyzwaniach w IK. Zastrzegamy przy tym, że nie możemy zdradzić nic, co mogłoby narazić Polskę na niebezpieczeństwo.

Panie i Panowie, za taką postawę wielkie dzięki!

Życzymy miłej lektury

Redakcja

ZŁOTY PARTNER A&S POLSKA

AXIS COMMUNICATIONS · BCS · Linc Polska Sp. z o.o. · nedap · SCHRACK SECONET · smart-i

SREBRNY PARTNER A&S POLSKA

HIKVISION

CZASOPISMO RYNKU SECURITY

a&S POLSKA

02 (38) / 2023

SPIS TREŚCI

8 Produkty numeru

INFRASTRUKTURA KRYTYCZNA

14 Raport: Infrastruktura krytyczna
Monika Mamakis

22 Nieoczekiwana lekcja hiszpańskiego
Jacek Grzechowiak

26 Infrastruktura naprawdę krytyczna
Michalina Nowak

32 Rewolucja w IK. Powstanie RCB 2.0
Michalina Nowak

36 Zmiana podejścia do problemów bezpieczeństwa w infrastrukturze krytycznej
Tomasz Goljaszewski, Hikvision Poland

38 1200 obiektów w jednym systemie
Wywiad z Tomaszem Witosławskim, dyrektorem Biura Bezpieczeństwa PKP Energetyka

40 Głos branży – bezpieczeństwo obiektów infrastruktury krytycznej

REDAKCJA

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

info@aspolska.pl
www.aspolska.pl

PREZES ZARZĄDU
Mariusz Kucharski

REDAKTOR NACZELNA
Marta Dynakowska

Z-CA RED. NACZELNEGO
Jan T. Grusznic

REDAKCJA
Monika Mamakis
Adela Prochyra

DZIAŁ REKLAMY
Iwona Krawiec

DZIAŁ PROJEKTÓW SPECJALNYCH
Jolanta A. Kucharska
Aleksandra Czapska
Michalina Nowak

CENTRUM KOMPETENCJI
Jacek Grzechowiak

KOREKTA
Jolanta Kucharska

PROJEKT GRAFICZNY I SKŁAD
Bogusław Kalwala

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

www.sensgroup.pl

Redakcja zastrzega sobie prawo skracania i redagowania nadesłanych tekstów. Tytuły i śródtytuły pochodzą od Redakcji.

Opinie autorów nie muszą być tożsame z poglądami Redakcji.

Za treść reklam i artykułów partnerów Redakcja nie odpowiada.

Przedruki tekstów bez zgody Wydawcy są niedozwolone.

© Copyright by a&s Polska

BCS®
dla profesjonalistów

Podwójna moc na straży bezpieczeństwa

Kamera hybrydowa
BCS-P-SDIP24425SR10-AI2

Kamera obrotowa IP 4 Mpx, przetwornik 1/2.7” z obiektywem motozoom 4.8- 120 mm

Kamerą stałopozycyjna 4 Mpx z obiektywem 4 mm

Inteligentna analiza obrazu:
- ochrona perymetryczna
- rozpoznawanie obiektów
- liczenie osób

» Więcej przeczytasz na stronie 8

POLSKA MARKA BCS

www.bcs.pl
www.facebook.com/bcscctvpl

CZASOPISMO RYNKU SECURITY

a&S POLSKA

02 (38) / 2023

SPIS TREŚCI

CYBERBEZPIECZEŃSTWO

46 Najlepsza polityka: zero zaufania
Monika Mamakis

52 Inwentaryzacja urządzeń jako fundament cyberbezpieczeństwa
Axis Communications

54 Czy twój system kontroli dostępu jest odporny na cyberataki?
Nedap Security Management

RYNEK SECURITY

56 Taktyka i technika w ochronie obwodowej
Jan T. Grusznic

64 Przegląd rozwiązań do ochrony perymetrycznej:
Atline, Axis Communications, Dilectro, Hikvision, Linc Polska, Optex, PRODUS S.A.

68 Nowe wyzwania potrzebują nowych kompetencji
Jakub Sobek, Polski Związek Pracodawców Ochrona

70 Mapa inwestycji
Adela Prochyra

72 Odbudowa Ukrainy szansą dla firm polskich?
Adela Prochyra

BEZPIECZEŃSTWO POŻAROWE

76 Lepiej zapobiegać, niż gasić
Michał Zalewski

79 Bezpieczeństwo SUG-G w serwerowni a reduktory stałowypływowe
DEKK

80 Integral Remote: narzędzia zdalnego dostępu do systemu Integral EvoxX firmy Schrack Seconet w świetle wymagań normy PN-EN 50710:2022-06
Schrack Seconet Polska

SERWIS INFORMACYJNY

83 Nowości firmowe

88 Centrum Kompetencji: Trzeba umieć połączyć kropki
Monika Mamakis

AVIGILON MOTOROLA SOLUTIONS Venom PSIM PLATFORM

Nowoczesne serwerownie wymagają systemu PSIM klasy High-End

Dowiedz się więcej na www.psim.pl

MEGAVISION TECHNOLOGY Sp. z o. o., Heliotropów 1, 04-796 Warszawa, tel. +48 22 292 3 292, e-mail: psim@psim.pl

Prezentujemy najnowsze urządzenia z oferty firm:

Axis Communications, BCS (NSS), D+H Polska, Gunnebo Safe Storage, Hikvision, Nedap Security Management, Schrack Seconet Polska, TP-Link

Axis Communications

Nowa kamera PTZ Axis dostosowana do pracy w ciemności, z najszybszym zoomem optycznym

Axis Communications wprowadziła na rynek AXIS Q6318-LE, szybką kamerę PTZ z oświetleniem IR i funkcją dzień/noc do nadzoru w całkowitych ciemnościach. Kamera sprawdzi się idealnie w obiektach infrastruktury krytycznej lub w środowisku miejskim.

Nowa kamera PTZ pracująca z rozdzielczoscią 4K została wyposażona w funkcję laserowego ustawiania ostrości oraz promiennik podczerwieni, dzięki czemu możliwe jest uzyskanie obrazu nawet w całkowitej ciemności. Zastosowanie wysokiej jakości przetwornika 1/2" powoduje, że ten model wyróżnia świetna światłoczułość oraz wysoka jakość obrazu.

Zastosowane oprogramowanie AXIS Object Analytics pozwala na wykrywanie oraz klasyfikowanie ludzi i pojazdów, a następnie automatyczne podążanie *(autotracking)* za wskazanym obiektem. Natomiast funkcja Quick Zoom powoduje, że urządzenie może zmienić wartość zoomu w czasie poniżej jednej sekundy, dzięki czemu możliwa jest obserwacja bardzo dużej przestrzeni. Kamera zawiera ponadto moduł Trusted Platform Module (TPM) z certyfikatem FIPS 140-2 zapewniający najwyższy, drugi poziom cyberbezpieczeństwa.

Obrotowa kamera AXIS Q6318-LE znajdzie zastosowanie we wszystkich miejscach o istotnym znaczeniu – obiektach infrastruktury krytycznej, obiektach rządowych, lotniskach, dworcach oraz w środowisku miejskim.

Więcej na www.axis.com/pl-pl

BCS

Kompaktowe kamery szybkoobrotowe BCS Line

W ofercie BCS pojawił się nowy model kamery PTZ BCS-P-SDIP24425SR10-AI2. Jest to urządzenie hybrydowe, w którego skład wchodzą moduł kamery stałopozycyjnej o rozdzielczości 4 Mpix oraz standardowa kamera PTZ o takiej samej rozdzielczości.

W tym nietypowym modelu znalazło się miejsce na wszystkie podstawowe funkcje, które w tego typu urządzeniu powinny się znaleźć, zachowując przy tym jego niewielki rozmiar, dzięki czemu jest ono bardzo dyskretne.

Nieograniczony obrót w osi poziomej z prędkością do 80°/s można uruchomić zarówno ręcznie, jak i za pomocą wywołania presetu. Taką samą prędkość kamera oferuje dla ruchu w osi pionowej. Dodatkową zaletą charakteryzującą ruch pionowy tych modeli jest możliwość zwrócenia kamery o 15° powyżej mocowania. Urządzenia ma dwa wejścia i jedno wyjście alarmowe, wejście/wyjście audio oraz wbudowany głośnik, gniazdo kart pamięci MicroSD o pojemności maks. 256 GB oraz promiennik podczerwieni o zasięgu do 100 m, który w połączeniu z 25-krotnym zoomem optycznym zapewnia wyraźny obraz nawet bardzo oddalonych obiektów.

Prawdziwą zaletą tych kamer jest jednak inteligentna analiza obrazu, wykorzystująca wiele funkcji maksymalizujących automatyczne działanie systemu. Połączona z presetami ochrona obwodowa, w tym przekroczenie wirtualnej linii czy wkroczenie w strefę, gdzie dodatkowo można określić kierunek ruchu intruza i typ obiektu uruchomiającego alarm, pozwoli stworzyć trasę patrolową.

Więcej na www.bcs.pl

D+H POLSKA

Nowa centrala oddymiania D+H

W ofercie D+H Polska pojawiła się nowa centrala kompaktowa CPS-B1-5-01-01 do sterowania systemami oddymiania i naturalnej wentylacji. Centrala jest przeznaczona do małych obiektów, w których obsługuje 1 strefę oddymiania (1 linia, 1 grupa).

Na co dzień centrala może być wykorzystywana na rzecz naturalnej wentylacji (przewietrzania), czyli do sterowania siłownikami w oknach, co znacząco poprawia komfort wewnątrz pomieszczeń i obniża koszty, np. klimatyzacji.

Centrala jest bardzo łatwa w instalacji i wyposażona w elektroniczne zabezpieczenie przeciwzwarciowe. Sporym udogodnieniem dla instalatorów jest ponadto możliwość doprowadzenia przewodów od dołu, z góry lub z tyłu obudowy.

CPS-B1-5-0101 jest zgodna z normą EN 12101-10:2005 + AC:2007 określającą zasilanie w systemach kontroli rozprzestrzeniania się dymu i ciepła.

Ten model pozwala na zasilanie napędów o całkowitym prądzie do 5 A oraz obsługuje 8 przycisków oddymiania i 8 czujek pożarowych na linię (dozwolone są wyłącznie czujki dopuszczone przez D+H).

Na szynie DIN znajdują się miejsca na wpięcie dodatkowych modułów. Na życzenie klienta obudowa centrali może być wykonana w dowolnym kolorze.

Więcej na
www.dhpolska.pl/

GUNNEBO SAFE STORAGE

Szafy SecureIT. Zainwestuj w bezpieczeństwo informacji o znaczeniu krytycznym

Poza katastrofami naturalnymi, błędami ludzkimi i awariami technicznymi, infrastruktura krytyczna oraz obiekty wysokiego ryzyka są narażone na inne zagrożenia, w tym kradzież danych lub ataki z użyciem impulsów elektromagnetycznych (EMP).

Zaprojektowana w ścisłej współpracy z europejską agencją rządową gama szaf antywłamaniowych SecureIT marki Gunnebo zapewnia wysoki poziom ochrony serwerów i danych, zmniejszając ich podatność na zniszczenie oraz zapewniając ciągłość świadczenia usług.

W ofercie jest dostępny chroniony przed działaniem impulsu elektromagnetycznego model SecureIT Level 3 EMP, jak również inne szafy z serii zapewniające fizyczną ochronę sprzętu informatycznego przed włamaniem, manipulacją i umyślnym uszkodzeniem.

Szafy SecureIT są wykorzystywane do ochrony obiektów infrastruktury krytycznej w sektorach obejmujących instytucje rządowe, branżę telekomunikacyjną, ambasady, obiekty obronne, a nawet mobilne centra dowodzenia jednostkami bojowymi.

Więcej na
www.GunneboSafeStorage.com/pl-pl/

HIKVISION

Innowacyjny system alarmowy AX Pro

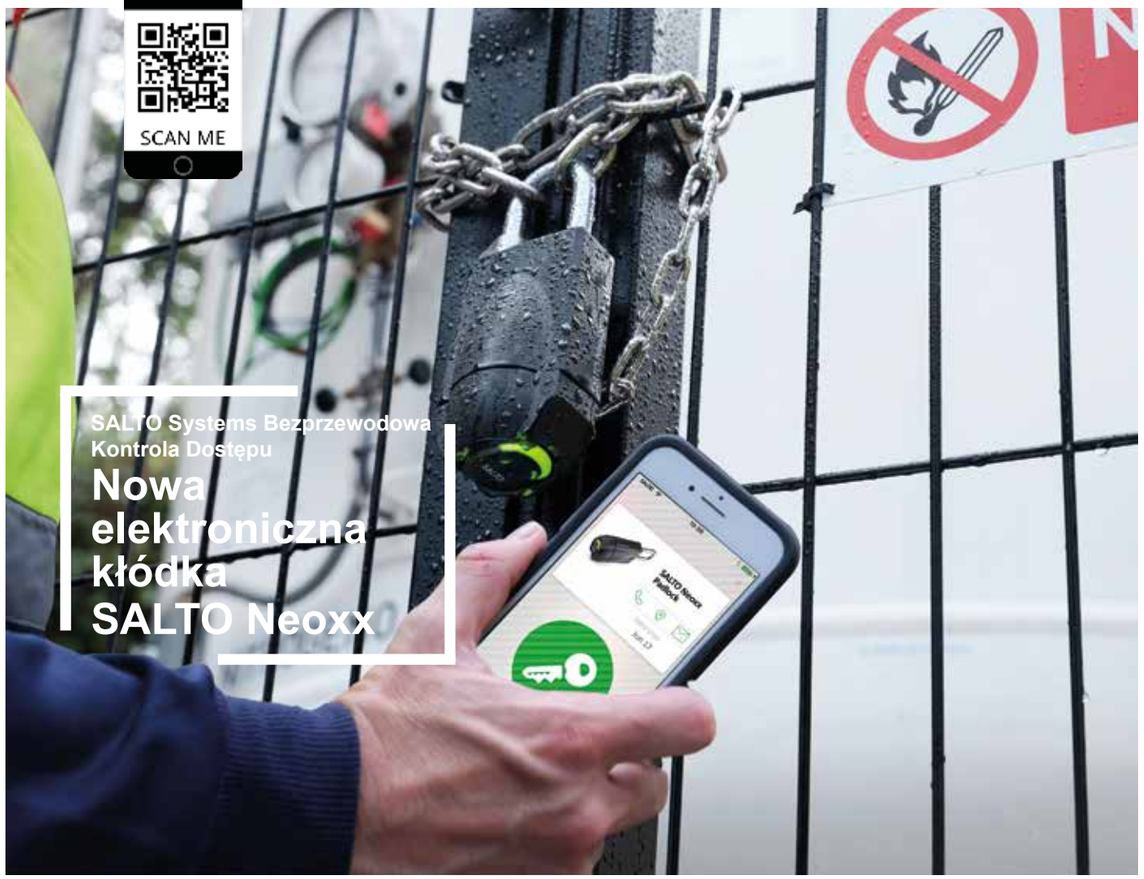
Wychodząc naprzeciw potrzebom rynku, firma Hikvision wprowadziła do swojej oferty innowacyjny system alarmowy AX Pro.

Stale rozwijane rozwiązanie, dzięki szerokiej gamie dostępnych komponentów, takich jak centrale, czujki, klawiatury, sygnalizatory, przekaźniki, elementy automatyki budynkowej, sprawdzają się zarówno w małych, i jak dużych instalacjach. Zarządzanie systemem może być realizowane w tradycyjny sposób przez klawiaturę, pilota, czytnik kart, jak również z poziomu aplikacji mobilnej.

Do wizualnej weryfikacji zdarzeń alarmowych można wykorzystać obraz z kamer powiązanych z systemem alarmowym lub z czujek PIRCAM wyposażonych w aparat. Centrale w wersji bezprzewodowej umożliwiają instalację poszczególnych komponentów bez ingerencji w konstrukcję budynku.

Zawsze stabilna innowacyjna komunikacja pozwala uzyskać połączenie między elementami systemu na odległość nawet 2000 m.

Więcej na
wwww.hikvision.com/pl/



Sprawne zarządzanie bezpieczeństwem obiektów infrastruktury krytycznej 24/7 dzięki zaawansowanej i niezawodnej technologii elektronicznej kłódki, kóra spełnia wszystkie wymogi bezpieczeństwa i nie tylko. Zapewnia ochronę, bezkluczowy i mobilny dostęp do instalacji zwiększając wydajność zarządzania rozproszoną infrastrukturą krytyczną.

+ NAJWYŻSZA OCHRONA: Innowacyjna specjalna obudowa pancerna o dwuwarstwowej konstrukcji gwarantuje maksymalną ochronę.

+ TECHNOLOGIA I DESIGN: Wyjątkowa dbałość o detale, najwyższej jakości materiały i cała technologia SALTO w jednym.

+ SMART KEY: łatwa w użyciu i bardzo bezpieczna bezkluczykowa technologia zapewnia natychmiastowy i niezawodny dostęp do dowolnych pomieszczeń.

+ PRZETESTOWANE I ZATWIERDZONE: Wodoodporność i wysoka trwałość oraz certyfikat mechatroniczny EN16864:2018.

SALTO Systems - Poland
Aeropark Business Center (Nothus), ul. 17 Stycznia 45A, 02-146 Warszawa
Tel.: +48 609 017 777 | Email: info.pl@saltosystems.com | www.saltosystems.pl

SALTO
inspiredaccess

NEDAP SECURITY MANAGEMENT

Integracja systemu AEOS z platformą PSIM Gemos

Rynek systemów zapewniających bezpieczeństwo obiektów rozwija się dynamicznie ze względu na rosnące wymagania klientów oraz coraz większą świadomość w zakresie cyberzagrożeń.

Klientom zależy również na elastyczności wyboru poszczególnych systemów, trudno bowiem znaleźć na rynku jednego producenta, który będzie miał w portfolio najlepsze w swojej klasie rozwiązania do dozoru wizyjnego, kontroli dostępu, SSWiN czy systemy ppoż. Konsekwencją wyboru najlepszych produktów jest skorzystanie z poszczególnych systemów różnych producentów, a w następnej kolejności ich integracja.

Dziś wymiana informacji i korelacja zdarzeń między CCTV, KD i SSWiN jest standardem. Realizację tych wymagań umożliwia zastosowanie platformy PSIM *(Physical Security Information Management)*, która wizualizuje system bezpieczeństwa w ramach jednej aplikacji. Pozwala to na szybsze i trafniejsze podejmowanie decyzji w trakcie zagrożenia, skraca również czas na szkolenia nowych pracowników.

Firma Nedap, ze swoją platformą AEOS, jest czołowym dostawcą sytemów kontroli dostępu intensywnie współpracującym z innymi producentami, by zapewnić kompleksowe rozwiązania swoim klientom.

Przykładem takiej współpracy jest kooperacja z firmą Ela-compil – dostawcą znanej platformy PSIM GEMOS.
Rozwiązania obu firm z powodzeniem zostały zaimplementowane w sektorze przemysłowym, publicznym czy biurowym.

Więcej na:
www.nedapsecurity.com/pl/pl

Schrack Seconet Polska

Nowa generacja głównego kontrolera systemu APS®-APROSYS - APS-9000

Schrack Seconet Polska wprowadza do oferty najnowszy produkt uznanej na świecie marki g+m elektronik ag – kontroler główny systemu APS®-APROSYS – APS-9000. Następca uznanego poprzednika, modułu APS-990, został zaprojektowany zgodnie z wymaganiami normy EN-54-16, dzięki czemu może być stosowany przede wszystkim w Dźwiękowych Systemach Ostrzegawczych (DSO) i w komercyjnych systemach nagłośnienia typu Public Address (PA), może też pracować w trybie *stand alone*.

Kompaktowa budowa kontrolera (zaledwie 1 HU) z powodzeniem zastępuje funkcjonalność wielu modułów poprzedniej generacji, np. APS-990, APS-177.2-LAN, APS-16.3, APS-56.1-NL, APS-19.2, APS-59.2 LAN, APS-01, oraz wiele innych (w tym również te z wbudowanym DSP), które występują jako osobne karty systemowe instalowane w ramach systemowych MC-03.

Nawet w wersji podstawowej kontroler APS-9000 ma wbudowane 4 niezależne odtwarzacze audio (następcy APS-19.2) umożliwiające rozsyłanie czterech komunikatów w tym samym czasie. Z kolei wbudowana karta sieciowa zapewnia połączenie dowolnej liczby systemów w sieci LAN i transmisję sygnałów audio z wykorzystaniem standardu AES67. Dodatkowo wbudowany procesor DSP zapewnia swobodny routing źródeł dźwięku oraz jego cyfrową obróbkę z zachowaniem jakości, jak to ma miejsce w przypadku profesjonalnych systemów koncertowych.

Kontroler APS-9000 uzyskał certyfikat CPR na zgodność z normą EN-PN-54-16 oraz Świadectwo Dopuszczenia zgodnie z wymaganiami Dz.U. 2010 nr 85 poz. 553 – oba dokumenty zostały wydane przez CNBOP-PIB.

Więcej na: www.schrack-seconet.pl

TP-Link

Sieciowe rejestratory wideo All-in-One TP-Link VIGI z zasilaniem PoE+

Ośmiokanałowy rejestrator VIGI NVR1008H-8MP oraz czterokanałowy VIGI NVR1004H-4P służą do rejestracji obrazu z kamer z serii TP-Link VIGI, a także przeglądania, przechowywania i odtwarzania zarejestrowanych materiałów wideo. Dzięki zasilaniu PoE+ rejestratory pełnią także funkcję przełącznika dla kamer IP.

VIGI NVR1008H-8MP jest wyposażony w 8 portów 10/100Mb/s PoE+, z których każdy oferuje do 30 W. Łączna moc rejestratora to 113 W. Z kolei VIGI NVR1004H-4P wyposażono w 4 porty 10/100Mb/s PoE+ o mocy do 30 W przy całkowitej mocy rejestratora wynoszącej 53 W.

Rejestratory zapisują materiał z kamer z rozdzielczością do 8 Mpix, w standardzie kompresji H.265+, który ogranicza nadmierne wykorzystanie przepustowości sieci. Nagrania są magazynowane na dysku SATA o pojemności do 10 TB. Dzięki pojemności dysku i zastosowanej kompresji urządzenie pozwala przechowywać nagrania nawet przez 720 dni.

NVR1008H-8MP i NVR1004H-4P umożliwiają podgląd na żywo z 8 lub 4 kamer w tym samym czasie oraz wyszukiwanie zdarzeń wg harmonogramu, co umożliwia szybkie przeglądanie materiału.

Rejestratory mają złącza zasilające oraz Audio In, Audio Out, VGA, HDMI, port Ethernet RJ45 10/100 Mb/s oraz 2 porty USB, które pozwalają na podłączenie m.in. myszki, klawiatury lub zewnętrznego dysku twardego. Dzięki mobilnej aplikacji VIGI dostępnej na urządzenia mobilne z systemem iOS i Android urządzenia można monitorować zdalnie.

Rejestratory są w pełni zgodne ze standardem ONVIF i są objęte 36-miesięczną gwarancją producenta.

Więcej na www.tp-link.com/pl/

POLON-ALFA

dobrze zaprojektowane BEZPIECZEŃSTWO

KOMPLEKSOWE
SYSTEMY SYGNALIZACJI POŻAROWEJ

• PRODUKCJA • SERWIS • SZKOLENIA
• WSPARCIE TECHNICZNE I PROJEKTOWE

AUTOMATYKA POŻAROWA

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

Raport: Infrastruktura krytyczna

Czy najbliższy szpital, most, elektrociepłownia są obiektami infrastruktury krytycznej? To informacja tajna. Lista obiektów IK jest tajemnicą i nie ma możliwości, by ustalić dokładnie, czy dana placówka na niej się znajduje. W powszechnej świadomości infrastrukturą krytyczną są wszystkie obiekty i usługi kluczowe dla bezpieczeństwa państwa i jego obywateli, choć okazuje się, że niekoniecznie od razu całego państwa i wszystkich jego obywateli. Co w takim razie wiemy o polskiej infrastrukturze krytycznej? Jaką zmianę przyniesie dyrektywa CER?

Monika Mamakis, a&s Polska

Nie każdy strategiczny obiekt należy do infrastruktury krytycznej (IK). O tym decydują szczegółowe kryteria zawarte w niejawnym załączniku do Narodowego Programu Ochrony Infrastruktury Krytycznej, opracowane przez Rządowe Centrum Bezpieczeństwa (RCB) we współpracy z ministrami i kierownikami urzędów centralnych przy wsparciu przedsiębiorców prywatnych.

Co jest, a co nie jest infrastrukturą krytyczną?

Konieczność precyzyjnego zdefiniowania, czym jest infrastruktura krytyczna, pojawiła się w roku 2002 wraz z przystąpieniem Polski do NATO. Ten temat porusza m.in. politolog Maciej Brocki w artykule *Narodowy Program Ochrony Infrastruktury Krytycznej 2018 w kształtowaniu bezpieczeństwa Rzeczypospolitej Polskiej* [„Społeczeństwo i polityka. Pismo edukacyjne" 2(59)/2019, wyd. Academica]. Jak zauważa w nim: *Przystąpienie naszego kraju do Paktu Północnoatlantyckiego wymagało dostosowania procedur oraz norm prawnych w aspekcie ochrony infrastruktury krytycznej. Mimo iż tematyka infrastruktury krytycznej w tym okresie traktowana była już jako jeden z kluczowych elementów, który może mieć wpływ na stabilność bezpieczeństwa narodowego, jak również spokój poszczególnych obywateli, brakowało zdefiniowania tego pojęcia. W wypracowaniu i sprecyzowaniu definicji, jak również określeniu kluczowych sektorów społeczno-gospodarczych, które obejmie infrastruktura krytyczna, pomogły doświadczenia innych państw.*

Definicję infrastruktury krytycznej wprowadzono ostatecznie w *Ustawie o zarządzaniu kryzysowym z 26 kwietnia 2007 roku.* Sprecyzowano w niej, że przez tego typu obiekty należy rozumieć systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców.

Infrastruktura krytyczna obejmuje systemy:
a) zaopatrzenia w energię, surowce energetyczne i paliwa,
b) łączności,
c) sieci teleinformatycznych,
d) finansowe,
e) zaopatrzenia w żywność,
f) zaopatrzenia w wodę,
g) ochrony zdrowia,
h) transportowe,
i) ratownicze,
j) zapewniające ciągłość działania administracji publicznej,
k) produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych.

→

Jak zatem widać, elementem IK może być każdego rodzaju obiekt czy usługa. Ustawowa lista jest bowiem długa, a jedynym warunkiem powodującym, że dany zakład czy usługa na taką niejawną listę zostaną wpisane, jest uzależnienie bezpieczeństwa funkcjonowania państwa od jego działania.

Jak jednak wyjaśnia ekspert ds. oceny ryzyka Piotr Kiliszek, zawodowo związany niegdyś m.in. z Jastrzębską Spółką Węglową oraz PP „Porty Lotnicze", niekoniecznie to, co laik uzna za obiekt IK, takim właśnie będzie. – *Nie każdy obiekt, który wydaje się strategiczny, takim jest. W powszechnej świadomości mosty są obiektami IK. Tymczasem tak być nie musi. Most drogowy, nawet jeśli na długim odcinku rzeki jest jedynym w okolicy, może być z powodzeniem zastąpiony mostem pontonowym. Inaczej rzecz się ma z mostem kolejowym. Ten może mieć znaczenie. Z kolei olbrzymi szpital nie musi być obiektem IK, jeśli w danym mieście, np. wojewódzkim, takich placówek jest kilka. Natomiast niewielki szpital powiatowy już obiektem IK może być, ponieważ jest np. w danym powiecie szpitalem jedynym* – ocenia.

Dyrektor Rządowego Centrum Bezpieczeństwa we współpracy z ministrami właściwymi opracowuje wykaz obiektów IK zgodnie z kryteriami zamieszczonymi w art. 3 pkt 2 *Ustawy o Ochronie Infrastruktury Krytycznej* (UZK). Wykaz ten obejmuje również europejską infrastrukturę krytyczną zlokalizowaną na terytorium Polski i innych państw członkowskich UE, która może mieć znaczący wpływ na nasz kraj.

Wykaz jest oczywiście niejawny. Na jego bazie są sporządzane wyciągi przekazywane ministrom właściwym, kierownikom urzędów centralnych odpowiedzialnym za dany system oraz wojewodom. Taki wyciąg otrzymują również właściciele, posiadacze samoistni i zależni obiektów, instalacji lub urządzeń, które trafiły na listę. Należy podkreślić, że jest to informacja, która nie może być zaskarżona przez właściciela lub posiadacza infrastruktury krytycznej. Nie można się też odwołać, bo ostatecznie to „tylko" informacja, choć można starać się o wykreślenie z takiej listy.

Rządowe Centrum Bezpieczeństwa ustawową definicję IK nieco rozszerza. Według RCB infrastruktura krytyczna to rzeczywiste i cybernetyczne systemy (obiekty, urządzenia bądź instalacje) niezbędne do minimalnego funkcjonowania gospodarki i państwa. Podkreślenie, że definicja dotyczy też systemów cybernetycznych, jest w obecnych czasach szczególnie istotne. Większość zagrożeń, jakie czyhają na obiekty IK, wynika bowiem z cyberataków.

Wraz z wprowadzeniem ustawy o zarządzaniu kryzysowym zostało zdefiniowane również pojęcie ochrony infrastruktury krytycznej. Opisano je jako zespół działań organizacyjnych, które mają na celu zapewnienie prawidłowego funkcjonowania IK lub szybkiego przywrócenia go w przypadku zagrożeń, takich jak awarie, ataki lub inne zdarzenia zakłócające jej działanie.

Co zagraża obiektom IK?

Zagrożenia są w zasadzie trzy: siły natury, awarie urządzeń i działania bądź zaniechania człowieka. W przypadku zagrożeń naturalnych sprawa jest jasna. Mowa o powodziach, silnych wiatrach, długotrwałych suszach, trzęsieniach ziemi, oblodzeniach i intensywnych opadach śniegu, a także epidemiach. Awarie urządzeń mogą mieć oczywiście różne przyczyny. Doświadczenie podpowiada, że często są one wynikiem błędu człowieka lub efektem zbiegu różnych okoliczności, tak jak to miało miejsce np. w elektrowni jądrowej Three Mile Island, gdzie 28 marca 1979 r. doszło do przegrzania rdzenia reaktora. Operator wówczas uznał, że zawór został zamknięty, choć w rzeczywistości pozostał otwarty, a w sygnalizacji nie było wskaźnika pokazującego jego prawdziwy stan. To z kolei było skutkiem błędu popełnionego na etapie projektu. Mimo stopienia jednej trzeciej rdzenia obudowa bezpieczeństwa zachowała szczelność zgodnie z projektem, a zbiornik ciśnieniowy reaktora również pozostał szczelny. Stopione paliwo zatrzymało się wewnątrz zbiornika, lecz substancje radioaktywne przedostały się przez zaprojektowane bariery elektrowni i trafiły do środowiska. Nie doszło wprawdzie do wycieku zagrażającego zdrowiu i życiu ludzi, ale społeczne zaufanie do energetyki jądrowej zostało poważnie nadszarpnięte.

Wspominamy o tym przypadku nie bez powodu. Na jego przykładzie bowiem widać wyraźnie, że ochrona infrastruktury krytycznej nie tylko oznacza zabezpieczenie zdrowia i życia obywateli, lecz także przekłada się na ich zaufanie do aparatu państwa, a to w znacznym stopniu wpływa na społeczeństwo. Ważne jest więc to, by wszelkie zagrożenia były wykrywane jak najwcześniej.

Ostatnią kategorią zagrożeń są działania człowieka, a konkretnie terroryzm będący jednym z najistotniejszych we współczesnym świecie. W zasadzie na każdy obiekt zaliczany do infrastruktury krytycznej może być przeprowadzony atak terrorystyczny. Bez wątpienia jednak celem w pierwszej kolejności będą systemy zaopatrzenia w energię, surowce energetyczne i paliwa, a także systemy łączności i sieci teleinformatycznych, systemy finansowe i systemy zaopatrzenia w wodę, choć i systemy zdrowotne czy dostaw żywności również nie mogą być bezpieczne. W obecnych czasach to systemy energetyczne i łączności stanowią najczulszy punkt, stąd wyraźna zmiana celu ewentualnego ataku.

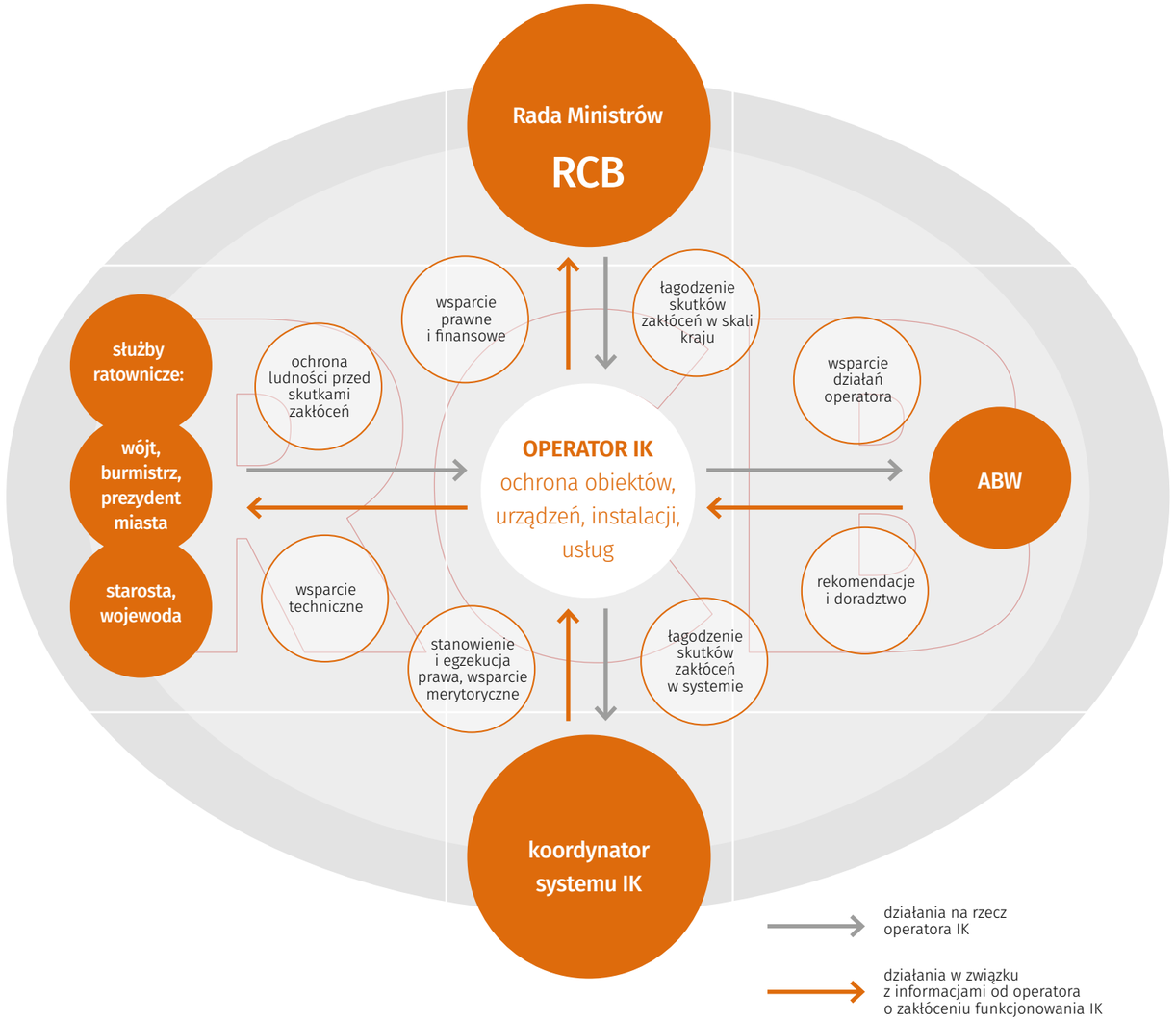
Wektor ataku się zmienia

Lista obiektów IK jest niejawna, i to nie podlega dyskusji. Nie jest zatem znana skala incydentów związanych z naruszeniem ich bezpieczeństwa. Wiemy tyle, ile przekażą nam media, a zwykle informują one opinię publiczną o spektakularnych naruszeniach. Do takich należy wypadek związany z wybuchem pocisku wystrzelonego przez ukraińską obronę przeciwlotniczą, który omyłkowo trafił na terytorium Polski w listopadzie 2022 r. (do eksplozji doszło zaledwie kilka kilometrów od linii energetycznej łączącej Polskę z Ukrainą, w odległości 150 km od jednego z największych podziemnych magazynów gazu i w podobnej odległości od magazynów paliw), czy wizyta „hiszpańskich nurków", o której analizę pokusił się Jacek Grzechowiak w artykule na str. 22.

Wiadomo jedno: wektor ataku się zmienia. Ataki fizyczne na obiekty IK zastępowane są przez ataki cybernetyczne z tej prostej przyczyny, że są łatwiejsze, choć do ich przeprowadzenia potrzebni są specjaliści. Służby powołane do takich zadań mają takich ludzi, a i w *dark webie* nie brak profesjonalistów, którzy za stosownym wynagrodzeniem podejmą się cybernetycznego ataku. To zaś oznacza nowe wyzwania związane z zapewnieniem bezpieczeństwa. Wrogie działania w cyberprzestrzeni charakteryzują się stosunkowo niskim kosztem przygotowania i potencjalnie dużymi szkodami. Dodatkowym argumentem „za" przeprowadzeniem cyberataku zamiast ataku fizycznego jest trudność wykrycia sprawcy. Cyberprzestępcy mogą więc szkodzić „na zlecenie", a ich mocodawcy mogą spać spokojnie.

Cyberataki mogą stać się najważniejszą bronią wymierzoną w obiekty IK. Według autorów raportu *The Cyber Index. International Security Trends and Realities*, przygotowanego pod auspicjami ONZ, gwałtownie rośnie liczba państw, które oficjalnie w ramach sił zbrojnych tworzą specjalne podmioty przygotowane do ochrony cyberprzestrzeni.

Doniesienia medialne coraz częściej wskazują, że masowo rośnie zjawisko cyberszpiegostwa skierowanego przeciwko obiektom IK. Owszem, w wielu przypadkach ataki hakerów, szczególnie *ransomware*, są spowodowane chęcią zarobku. Cyberprzestępcy jednak mogą się dostać do firmowych systemów IT i tkwić nich w ukryciu, do momentu otrzymania rozkazu uderzenia. Każda firma korzysta z urządzeń pochodzących z całego świata. W wielu wypadkach z krajów, co do których rozsądek nakazuje zachować ostrożność. Choć dokonanie zmasowanego cyberataku na IK, mającego wpływ na funkcjonowanie całego kraju, wydaje się mało prawdopodobne, to atak na pojedyncze obiekty jest już możliwy. A poza zagrożeniami związanymi z cyberatakiem obiekty IK trzeba chronić przed ludzkimi błędami, awariami czy siłami natury. Jak sobie z tym radzimy? Pewne światło na tę sprawę rzuca kontrola NIK. →



» *Ochrona infrastruktury krytycznej nie tylko oznacza zabezpieczenie zdrowia i życia obywateli, lecz także przekłada się na ich zaufanie do aparatu państwa.* «

Najwyższa Izba Kontroli o ochronie obiektów IK

W latach 2015-2016 Najwyższa Izba Kontroli przeprowadziła kontrolę, której celem było sprawdzenie, jak realizowana jest kwestia ochrony infrastruktury krytycznej. Raport z niej nie powstał, a szkoda, bo mogłaby to być ciekawa lektura, choć może dla wielu niezbyt przyjemna. Podsumowanie wyników zostało przedstawione na stronie NIK w październiku 2019 r. i już wówczas nie napawały one optymizmem. Można odnieść wrażenie, że jednostki odpowiedzialne za funkcjonowanie obiektów IK niespecjalnie stosują się do zapisów ustawy o zarządzaniu kryzysowym. Wnioski opublikowane przez NIK pokazują, że niektórzy zarządcy obiektów IK podchodzą do sprawy niefrasobliwie.

Kontrolerzy NIK stwierdzili szereg nieprawidłowości. Wypunktowali brak wystarczającej ochrony fizycznej obiektów powiązanych ze sobą funkcjonalnie, niezbędnych do zapewnienia bezpieczeństwa infrastruktury krytycznej. Teren nie był właściwie zabezpieczony przed wejściem osób nieuprawnionych, czasami nie korzystano z monitoringu wizyjnego, a wejścia do niektórych obiektów nie spełniały norm bezpieczeństwa. Ponadto niektóre bramy wjazdowe nie były wyposażone w zapory zabezpieczające przed wtargnięciem. W większości skontrolowanych podmiotów nie wprowadzono rozwiązań na wypadek wystąpienia zdarzeń sabotażu lub wyrządzenia szkód przez pracowników na terenie obiektów infrastruktury krytycznej.

Żaden ze skontrolowanych podmiotów nie wyodrębniał kluczowego, ze względu na przestrzeganie zasad bezpieczeństwa infrastruktury krytycznej, personelu. W większości podmioty te nie określały też procedur umożliwiających sprawdzenie wybranego oferenta wykonującego usługi na rzecz operatora infrastruktury krytycznej pod kątem jakości wykonywanych usług i zachowania poufności wykonywanych prac.

Niekiedy podmioty te nie realizowały rekomendacji dotyczących audytu sieci informatycznych działających na potrzeby obiektów infrastruktury krytycznej. Nie opracowano kompleksowych regulacji wewnętrznych dotyczących bezpieczeństwa przemysłowego systemu teleinformatycznego, a wykonawcy nie byli zobowiązani do zachowania poufności uzyskanych informacji, mimo że mieli dostęp do kluczowych systemów służących do sterowania IK.

Brak odpowiednich zabezpieczeń, m.in. w obszarach ochrony fizycznej czy osobowej, skutkował wystąpieniem groźnych incydentów w obiektach infrastruktury krytycznej i związanych z prawidłową eksploatacją instalacjach infrastruktury krytycznej. Przykładem może być kradzież z terenu jednego z obiektów infrastruktury krytycznej dwóch dużych pojemników zawierających promieniotwórczy izotop kobaltu.

Jak wspomnieliśmy, spójny raport pokontrolny nie powstał, lecz wystąpienia pokontrolne, przygotowane przez cztery delegatury NIK: w Bydgoszczy, Szczecinie, Warszawie i Łodzi, są inspirującą lekturą. Ich podsumowanie dowodzi, że jednostki samorządowe z ochroną obiektów IK w kontrolowanym okresie nie radziły sobie w dostatecznym stopniu. Zauważalna jest pewna prawidłowość – im niższy szczebel w administracyjnej hierarchii, tym gorzej wygląda kwestia IK. Na przykład, zgodnie z informacjami przygotowanymi przez delegaturę NIK w Bydgoszczy, w jednym z kontrolowanych powiatów starosta wykonywał zadania z zakresu ochrony infrastruktury krytycznej w sposób ograniczony i incydentalny, pomimo posiadanej wiedzy o lokalizacji na terenie powiatu obiektów IK. Z kolei w innym urzędzie działania wójta w zakresie bezpieczeństwa obiektów IK ograniczały się w kontrolowanym okresie do jednokrotnej korespondencji z operatorem IK. W urzędzie nie gromadzono informacji dotyczących zagrożeń obiektów IK, a także nie realizowano zadań planistycznych w obszarze rozwiązań na wypadek zniszczenia lub zakłócenia funkcjonowania IK. Opracowany w gminie Plan Zarządzania Kryzysowego nie był aktualizowany w zakresie bezpieczeństwa IK.

Jedynym obiektem IK wymienionym wprost w wystąpieniach pokontrolnych jest PKN Orlen. *Najwyższa Izba Kontroli ocenia pozytywnie realizację przez PKN ORLEN zadań w zakresie zabezpieczenia infrastruktury krytycznej. W latach objętych kontrolą PKN ORLEN przygotował i wdrożył Plan ochrony infrastruktury krytycznej, który uzgodniono z właściwymi podmiotami. W badanym zakresie przyjęte przez PKN ORLEN standardy ochrony fizycznej, technicznej, teleinformatycznej, osobowej i prawnej IK były stosowane, a powołany w Spółce pełnomocnik do spraw ochrony infrastruktury krytycznej wypełniał swoje obowiązki. (…) Analiza czterech przypadków niekorzystnych zdarzeń oraz kontrola dokumentacji wybranych budynków i urządzeń wykazała, że PKN ORLEN stosował się do przyjętych procedur ochrony i zapewnił ciągłość funkcjonowania IK w sytuacji niekorzystnych zdarzeń* – czytamy w wystąpieniu pokontrolnym.

Porównanie wyników kontroli w PKN Orlen z wynikami przeprowadzonych w jednostkach samorządowych nasuwa podejrzenie, że być może to nie niefrasobliwość odpowiada za fakt, że wnioski pokontrolne NIK dotyczące gmin i powiatów stawiają je w nie najlepszym świetle. Być może przyczyna tkwi w pieniądzach, a dokładnie w ich braku.

Owszem, gminy mogą otrzymać dotację celową na rzecz zarządzania kryzysowego. W art. 26 pkt 5 *Ustawy o zarządzaniu kryzysowym* znalazł się zapis, że na dofinansowanie zadań własnych z zakresu zarządzania kryzysowego jednostki samorządu terytorialnego mogą otrzymywać dotacje celowe z budżetu państwa. Słowem kluczem jest w tym przypadku „mogą". „Mogą" to nie znaczy, że muszą i że dostaną.

A przecież zadbanie o odpowiednią ochronę IK, niezależnie od tego, czy rzecz dotyczy firmy prywatnej, czy samorządu, kosztuje.

» Cyberatak wymierzony w obiekty IK może zdestabilizować działania państwa i stać się ważnym elementem kampanii zbrojnej. Wojna w Ukrainie pokazuje, że jest to możliwe, a przygotowanie potencjalnego ataku może mieć miejsce jeszcze w czasie pokoju. «

AWARIE ELEKTROWNI JĄDROWYCH	
1979	**Three Mile Island (USA)**. Częściowe stopienie rdzenia w drugim reaktorze.
1986	**Czarnobyl (Ukraina)**. Eksplozja reaktora spowodowała rozprzestrzenienie się radioaktywnego materiału, co miało wpływ na zdrowie i życie wielu osób.
2011	**Fukushima Daiichi (Japonia)**. Trzęsienie ziemi i tsunami w marcu spowodowały uszkodzenie elektrowni jądrowej Fukushima Daiichi w Japonii. W wyniku uszkodzeń doszło do wycieku promieniotwórczego, co miało poważne konsekwencje dla zdrowia i środowiska.

KATASTROFY NATURALNE	
1908	**Messyna (Włochy)**. Trzęsienie ziemi o sile 7,1 stopnia w skali Richtera nawiedziło miasto Messyna na Sycylii, zabijając co najmniej 70 tys. osób.
1934	**Polska**. Powódź. Jedna z największych katastrof naturalnych w historii kraju. Spowodowała ona śmierć ponad 200 osób i ogromne straty materialne.
1953	**Niderlandy**. Powódź, która spowodowała śmierć ponad 1800 osób w Holandii i Belgii, była wynikiem silnego sztormu i wysokiej fali przybrzeżnej.
1968	**Region Veneto (Włochy)**. Trzęsienie ziemi o sile 6,5 stopnia w skali Richtera. Zginęło 385 osób, setki domów ulego zniszczeniu.
1973	**Islandia**. Wybuch wulkanu Heimaey na wyspie Vestmannaeyjar zmusił tysiące ludzi do ucieczki z wyspy, a lawa i popiół zniszczyły wiele budynków i domów.
1974	**Polska (głównie Kotlina Kłodzka)**. Trzęsienie ziemi o sile 4,8 stopnia w skali Richtera spowodowało śmierć 23 osób i znaczne zniszczenia.
1985	**Bratsk (Rosja)**. Uszkodzenie elektrowni wodnej w wyniku nieprawidłowej eksploatacji zbiornika retencyjnego spowodowało poważne straty materialne i przerwy w dostawach energii elektrycznej.
1988	**Armenia**. Trzęsienie ziemi o sile 6,9 stopnia w skali Richtera zabiło ok. 25 tys. osób.
1997	**Polska**. Powódź tysiąclecia. Nawiedziła także Czechy i wschodnie Niemcy. Zginęło 114 osób, a straty zalanych regionów oszacowano na ok. 3,5 mld USD.
1998	**Adeje (Nigeria)**. Uszkodzenie rurociągu przesyłowego doprowadziło do eksplozji. W jej wyniku zginęło ponad 1000 osób, a ponad 4000 zostało rannych.
1999	**Europa (Francja, Belgia, Luksemburg, Niemcy)**. Huragan Lothar nawiedził kilka krajów europejskich, powodując śmierć 137 osób i wyrządził poważne szkody w lasach i infrastrukturze.
2009	**L'Aquila (Włochy)**. W trzęsieniu ziemi o sile 6,3 stopnia w skali Richtera zginęło 308 osób, a miasto zostało zniszczone.
2010	**Europa. (Polska, Czechy, Słowacja, Węgry, Austria, Serbia, Niemcy, Ukraina)**. Jedna z największych powodzi w tym regionie świata. Zginęło 37 osób.
2010	**Islandia**. Wybuch wulkanu Eyjafjallajökull; chmura pyłów nad Europą spowodowała zamknięcie przestrzeni powietrznej w większości krajów Europy.
2011	**Polska (Podkarpacie)**. Trzęsienie ziemi o sile 4,7 stopnia w skali Richtera nawiedziło region Podkarpacia. Spowodowało poważne zniszczenia, nie odnotowano ofiar śmiertelnych.
2012	**Polska**. Tornado, które nawiedziło miejscowość Pszczew w woj. lubuskim, spowodowało śmierć 2 osób i znaczne zniszczenia.
2014	**Bałkany (Serbia, Chorwacja, Bośnia i Hercegowina, a także Rumunia)**. Powódź, która spowodowała śmierć ponad 100 osób.
2017	**Polska (woj. pomoskie)**. W wyniku huraganu, który nawiedził Polskę w sierpniu 2017 r., zginęło 8 osób, a straty na Pomorzu oszacowano na 27 mln zł.
2018	**Kapsztad (RPA)**. Susza spowodowała przerwanie dystrybucji wody.
2021	**Grecja (Epir)**. Trzęsienie ziemi o sile 6 stopni w skali Richtera nawiedziło region Epiru w Grecji, powodując zniszczenia. Zginęła 1 osoba.
2023	**Syria i Turcja**. Trzęsienie ziemi o sile 7,8 stopnia w skali Richtera. Ostateczne straty nie są jeszcze znane, ale w lutym szacowano liczbę ofiar na ponad 50 tys.

SPEKTAKULARNE ATAKI HAKERSKIE (TE, O KTÓRYCH WIEMY)	
2007	**Estonia**. Dokonanie szeregu ataków hakerskich na serwery rządowe i komercyjne w Estonii. Ataki miały wpływ na funkcjonowanie systemów bankowych, mediów i administracji publicznej.
2014	**Niemcy**. Atak na sieć elektrowni, który miał na celu przejęcie kontroli nad nimi. Został przypisany grupie o nazwie „Dragonfly".
2015	**Ukraina**. Atak na systemy sterowania siecią energetyczną spowodował wyłączenie zasilania dla ponad 230 tys. ludzi przez ok. 6 godzin.
2015	**Ukraina**. W grudniu 2015 roku systemy przesyłowe gazu ziemnego w Ukrainie padły ofiarą cyberataku, który spowodował przerwy w dostawach gazu. Atak został przypisany do grupy hakerów o nazwie „Sandworm Ukraina. Team".
2015	**Niemcy**. Ofiarą grupy APT28 (Fancy Bear) padły serwery rządowe.
2016	**Niemcy**. Prywatna niemiecka firma energetyczna została zaatakowana przez grupę Sandworm.
2017	**Francja**. Cyberprzestępcy wzięli na celownik elektrownię jądrową. Konkretna nazwa elektrowni nie została ujawniona publicznie.
2019	**Arabia Saudyjska**. W sierpniu 2019 roku doszło do ataku na rurociąg przesyłowy ropy naftowej w Arabii Saudyjskiej. Atak spowodował uszkodzenie rurociągu i spadek produkcji ropy naftowej o ok. 5%.
2019	**Indie**. Przeprowadzenie ataku na sieć elektrowni jądrowej w Indiach, który miał na celu pozyskanie poufnych informacji dotyczących projektu budowy elektrowni.
2020	**Polska**. Duży operator sieci elektroenergetycznej padł ofiarą ataku hakerskiego, który spowodował częściowe wyłączenie systemów.

NAJBARDZIEJ ZNANE DZIAŁAJĄCE GLOBALNIE WIRUSY	
2000	**Iloveyou**. Robak, który aktywował się 4 maja 2000 roku. Wystarczyło 10 dni, by zainfekował ok. 10% pracujących w sieci komputerów. Spowodował straty wycenione na ok. 10 mld USD.
2001	**CodeRed**. Robak, który zainfekował wg różnych szacunków od 1 do 2 mln serwerów. Straty zostały wycenione na ok. 2 mld USD.
2004	**MyDoom**. Robak komputerowy wykryty 26 stycznia 2004 roku. Pozwalał na uzyskanie zdalnego dostępu do kompuerów, które były potem wykorzystywane do ataku DoS.
2004	**Sasser**. Skanował różne adresy IP i łączył się z komputerami ofiar za pomocą portów TCP 139 oraz 445. Zostały zakażone miliony urządzeń, w tym istotne urządzenia wchodzące w skład infrastruktury krytycznej. Straty oszacowano na 18 mld USD.
2007	**StormWorm**. Rozprzestrzeniał się poprzez wiadomości e-mail z zainfekowanym załącznikiem oraz fałszywe linki do newsów i filmików. W najbardziej aktywnym okresie jego działania kontrolował ok. 10 mln komputerów, z których uczynił maszyny-zombie, wykorzystywane m.in. do ataków DoS.
2010	**Stuxnet.** Robak komputerowy (*worm*). Pierwszy wirus, który powodował fizyczne zniszczenie zainfekowanych urządzeń.
2017	**WannaCry**. *Ransomware*. Duża fala ataków spowodowała zainfekowanie ponad 300 tys. komputerów w 99 krajach.
2017	**Petya/NotPetya**. Wiper. Atak sparaliżował firmy i agencje rządowe na całym świecie.

Pieniądze są ważne

Jeśli obiekt należy do infrastruktury krytycznej, to – jak mówi Piotr Kiliszek – utrzymanie jego statusu oznacza same kłopoty, zero benefitów. Firmy, których obiekty zostały wpisane na niejawną listę obiektów IK, zostają obciążone konkretnymi obowiązkami, nie mogąc jednocześnie liczyć na żadne z tego tytułu ulgi czy przywileje. Nic więc dziwnego, że zrobią wiele, by z takiej listy się „wypisać". Zresztą, faktycznie nie zawsze jest sens, by utrzymywać taki ich statut.

Zmianę w tej kwestii może przynieść dyrektywa *Critical Entities Resilience* (CER), która weszła w życie 17 stycznia 2023 r. Według ekspertów zapowiada ona rewolucję w kwestii ochrony infrastruktury krytycznej i zarządzania nią. Po pierwsze, CER wprowadza nowe narzędzia i mechanizmy, które umożliwiają państwom członkowskim Unii Europejskiej lepsze monitorowanie i ochronę infrastruktury krytycznej. Dzięki temu państwa będą szybciej reagować na zagrożenia infrastruktury krytycznej i minimalizować ich skutki.

Po drugie, dyrektywa CER wymaga od państw członkowskich, aby wyznaczały odpowiednie organy nadzorujące infrastrukturę krytyczną oraz określały ich kompetencje i obowiązki. To pozwoli na lepszą koordynację działań na poziomach krajowym i międzynarodowym, co zwiększy skuteczność działań w przypadku ataków na infrastrukturę krytyczną.

Po trzecie, dokument wprowadza nowy model współodpowiedzialności państwa za działanie wybranych sektorów gospodarki. Najważniejszym aspektem jest zapisana w art. 10 możliwość udzielania przez państwo finansowego wsparcia podmiotom zarządzającym obiektami IK. Na stronie RCB można znaleźć wyjaśnienie art. 10 pkt 1 dyrektywy CER, którego dosłowne brzmienie jest następujące: *Bez uszczerbku dla mających zastosowanie przepisów dotyczących pomocy państwa, jeżeli jest to konieczne i uzasadnione celami interesu publicznego, państwa członkowskie mogą przekazywać zasoby finansowe podmiotom krytycznym.* Według opinii RCB znaczy to dokładnie tyle, że podmioty krytyczne będą mogły liczyć na wsparcie finansowe ze strony państwa, jeśli będzie to uzasadnione bezpieczeństwem publicznym. Takie wsparcie nie będzie traktowane jako niedozwolona pomoc publiczna.

Warto zwrócić uwagę na słowa dr. Witolda Skomry, specjalisty w zakresie bezpieczeństwa narodowego, zarządzania kryzysowego, oceny ryzyka i ochrony infrastruktury krytycznej, szefa Wydziału Ochrony Infrastruktury Krytycznej w Rządowym Centrum Bezpieczeństwa, cytowane przez portal Energetyka24. *Ta dyrektywa wprowadza mechanizm, już na stałe, pomocy operatorom w sytuacjach, kiedy biznesowo nieopłacalna usługa musi być utrzymana ze względu na potrzeby państwa i obywatela.*

I to może być prawdziwe zagrożenie dla polskiej infrastruktury krytycznej – finansowanie nie tego, co trzeba. Choć dr W. Skomra w wywiadzie dla portalu WNP stwierdza także: *Kluczowym elementem jest cyberbezpieczeństwo. O wiele bardziej zagrażają nam hakerzy niż grupy dywersyjne, drony czy rakiety.* Dodajmy: hakerzy i brak pieniędzy, ale też katastrofy naturalne, ludzkie błędy i pospolite awarie. Czy w świetle tego dobrą informacją jest ta, że być może dojdzie do likwidacji RCB?

Si vis pacem, para bellum – jeśli chcesz pokoju, szykuj się do wojny. Jeśli chcemy spać spokojnie, musimy być przygotowani na najgorsze. Czy faktycznie jesteśmy? ●

Nieoczekiwana **lekcja hiszpańskiego**

W styczniu tego roku w mediach pojawiły się informacje dotyczące interwencji Morskiej Służby Poszukiwania i Ratownictwa prowadzonej u ujścia Martwej Wisły w Gdańsku. Do zdarzenia doszło w sąsiedztwie bardzo ważnych obiektów, będących zapewne obiektami infrastruktury krytycznej, czyli trzech terminali: kontenerowego, węglowego oraz paliwowego. Co się tam stało?

Jacek Grzechowiak

Według pierwszych medialnych doniesień interwencja dotyczyła udzielenia pomocy barce lub motorówce, która tonęła. Na jej pokładzie znajdowało się trzech obywateli Hiszpanii, którzy mieli nurkować co najmniej 6 godzin w rejonie, gdzie ich odnaleziono.

Potem pojawiły się szczegółowe informacje. Według nich łódź poszkodowanych nie tonęła, a jedynie uległ awarii układ sterowania. Hiszpanie (?) zostali przetransportowani na ląd, a tam przekazano ich funkcjonariuszom policji. Później mieliśmy okazję dowiedzieć się, że cudzoziemcy nurkowali podobno w bezpośrednim sąsiedztwie Naftoportu, gdzie ponoć poszukiwali bursztynu. Po przesłuchaniu zostali zwolnieni, pozostawiając swoje numery telefonów. Dwa okazały się nieaktywne, trzeci za długi. Niestety nie sprawdzono numerów telefonów, Hiszpanie zaś szybko opuścili Polskę.

Co wiemy o nocnych poszukiwaniach bursztynu?

Po tym zdarzeniu przez Polskę przetoczyła się medialna burza. Pojawiły się teorie spiskowe, utrudniając prowadzenie rzeczowej dyskusji, jaką należy podjąć po tym, co wydarzyło się na Bałtyku.

Zdarzenie to bardzo szybko zostało powiązane z wybuchem gazociągu Nord Stream, w którego przypadku szwedzka prokuratura podejrzewa zamach terrorystyczny, a także z wybuchem gazociągu łączącego Litwę i Łotwę oraz z awarią przewodu energetycznego zasilającego Bornholm i innego podobnego zdarzenia w odniesieniu do przewodu łączącego Polskę i Szwecję.

Niezależnie od tego, jakie są fakty, „hiszpański" incydent powinien skłonić do refleksji wszystkich zarządzających bezpieczeństwem, nie tylko tych sprawujących kontrolę nad obiektami stanowiącymi infrastrukturę krytyczną. Zdarzenie to po rozłożeniu na części wskazuje na kilka ciekawych elementów:

- używanie łodzi bez oświetlenia – czy po to, by uzyskać ochronę przed obserwacją, połączoną jednocześnie z możliwością wyśledzenie tego, jakimi środkami dysponują służby;
- brak środków łączności radiowej, by uniknąć namierzenia nie tylko przez służby prowadzące stały nasłuch radiowy, ale także przez radioamatorów cywilnych. Prawda jest taka, że zarówno złodzieje, jak i organizacje terrorystyczne, a także służby specjalne ostrożnie stosują środki łączności radiowej podczas realizowanych przedsięwzięć.

Hipotezy vs wątpliwości

Mając na względzie te elementy, można rozważyć kilka hipotez dotyczących tego, co „hiszpańscy nurkowie" robili u polskiego brzegu. Każda z nich może okazać się błędna, gdyż zasób posiadanych informacji jest niewielki.

Hipoteza nr 1 – działanie pozoracyjne

Prowadzone w celu odwrócenia uwagi od działania zasadniczego realizowanego w tym samym czasie w innym miejscu. Przykładem takiego działania może być lokalizacja ładunków wybuchowych na dnie morskim, by dokonać ich zdalnej eksplozji w dogodnym czasie.

Za tą hipotezą przemawia relatywnie wiele śladów, jakie zostawili sprawcy, jakby wręcz chcieli rzucać się w oczy. Do tego dochodzi →

Kontekst bezpieczeństwa obiektów IK

Obiekty infrastruktury krytycznej są przedmiotem zainteresowania obcych służb, zwłaszcza w obecnej sytuacji geopolitycznej. Na podstawie analizy różnego rodzaju incydentów można stwierdzić, że to one budują obecny kontekst bezpieczeństwa obiektów w naszym kraju. Przypomnijmy je:

- Zniszczenie składów broni w czeskiej miejscowości Vrbětice – ustalenia dziennikarzy i wolontariuszy z Belingcat wskazują, iż za zamachem stały rosyjskie służby specjalne. I choć formalnych dowodów na to nie ma, powinniśmy brać pod uwagę to, że możliwe jest dokonanie zamachu także poza strefą działań wojennych w Ukrainie. Choć w obecnej sytuacji geostrategicznej oraz w kontekście obecnych zastosowań zagrożeń informatycznych, które już oficjalnie są nazywane rodzajem wojsk, pojęcie strefy działań wojennych wydaje się już anachronizmem.
- Obecnie incydenty kinetyczne są poprzedzane incydentami informatycznymi. Patrząc z tej perspektywy, nie sposób nie wziąć pod uwagę ostrzeżenia Microsoftu, a następnie oficjalnego potwierdzenia masowego ataku na polskie firmy z branży TSL (Transport, Spedycja, Logistyka), ze wskazaniem, iż ataku dokonała powiązana z Rosją grupa Iridium. Należy przy tym podkreślić, iż atak ten został potwierdzony przez przedstawicieli Rządowego Centrum Bezpieczeństwa podczas konferencji *Normalizacja w bezpieczeństwie informacji, cyberbezpieczeństwie i bezpieczeństwie powszechnym* zorganizowanej przez Polski Komitet Normalizacyjny. Skoro doszło do tych ataków, to nie można wykluczyć przejścia Rosji do fazy kinetycznej.
- Incydenty kinetyczne w odniesieniu do infrastruktury transportowej zostały już odnotowane, np. sabotaż Deutsche Bahn. Pojawiają się komentarze, że był to odwet za atak na most Krymski. Nie jest to oczywiście niemożliwe, jednak biorąc pod uwagę niewielką różnicę czasową pomiędzy tymi incydentami, wydaje się to mało prawdopodobne. Tym niemniej Federalny Urząd Kryminalny (Bundeskriminalamt – BKA) ostrzegł przed ryzykiem ponownych ataków na infrastrukturę krytyczną.

sprzęt niskiej jakości i pogoda, które stanowią wręcz podręcznikowe alibi. Jeśli weźmiemy pod uwagę „teorię nieprzypadkowych przypadków", to mamy naturalną sytuację angażującą wiele służb, odwracając uwagę od pozostałej części akwenu i infrastruktury. A uszkodzenie napędu można bardzo łatwo upozorować.

Są również argumenty przeciw, np. nieuwzględnienie zmiany warunków pogodowych. Gdyby robili to terroryści lub służby specjalne, ten aspekt raczej zostałby uwzględniony, choć historia wojen uczy, że warunki atmosferyczne potrafiły przeszkodzić nawet w poważnych operacjach zbrojnych, mimo że ich przygotowanie uwzględniało pogodę.

Hipoteza nr 2 – penetracja przestępcza

Za tą hipotezą przemawia wykorzystanie sprzętu pozbawionego cech identyfikacyjnych, nigdzie niezarejestrowanego, z niskim echem radiolokacyjnym i elektromagnetycznym, fałszywe dane „Hiszpanów" i ponownie pogoda oraz awaria napędu. Wszystko to daje idealny pretekst do przetestowania systemu reagowania wraz z rozpoznaniem osób, miejsc, procedur, komunikatów, sygnałów, a nawet kryptonimów i oznaczeń stosowanych przez służby (jeśli „Hiszpanie" mieli kamerki czy dyktafony, mogli uzyskać o wiele więcej).

Przeciw przemawia akcja ratownicza. Penetracja przestępcza jest dokonywana albo przez specjalistów od tego działania, albo przez późniejszych sprawców. W obu przypadkach osoby te za wszelką cenę ukrywają swój pobyt w miejscu penetracji, a tutaj powiadomiły SAR, co jest dość irracjonalne, rozważając ten incydent z tej perspektywy.

Hipoteza nr 3 – realizacja działania sabotażowego

Nie mamy danych przemawiających za prawdziwością tej hipotezy, wszak nic nie eksplodowało, przynajmniej na razie. Gdybyśmy patrzyli na argumenty przeciw, z pewnością spojrzelibyśmy na amatorskie działanie sprawców, ale należy zauważyć, że i w przypadku wsi Vrbětice, i zamachu na Skripala rosyjskie służby zostawiły wiele śladów.

Niezależnie od tego, która hipoteza jest najbliższa prawdy, to każda z nich każe nieco inaczej spojrzeć na bezpieczeństwo obiektów, skłaniając do zastanowienia się, czy bezpieczeństwo obiektu powinno zaczynać się na linii ogrodzenia. I do zadania sobie pytania, czy tak mocno podkreślane w polskim prawodawstwie „granice chronionego obiektu i obszaru" faktycznie powinny stanowić koniec działań prewencyjnych.

Czy ochrona obiektów, zwłaszcza obiektów infrastruktury krytycznej, nie powinna obejmować uregulowanej formalnie prewencyjnej aktywności w strefie przyległej do tych obiektów? Czy agencje ochrony nie powinny spojrzeć nieco poza horyzont i tam poszukać wyzwań, które jeszcze niedawno byłyby ciekawym teoretycznym studium przypadku, a dziś zdecydowanie są zagrożeniami, które agencje ochrony muszą rozpatrywać w kategorii rzeczywistych wyzwań.

Zmiana krajobrazu zagrożeń

Pomocne mogą się okazać regulacje Rady Europy w sprawie odporności infrastruktury krytycznej, gdzie potrzeba wzmocnienia odporności fizycznej jest wymieniona wprost, a jednocześnie jednoznacznie stwierdzono, że *pojęcie odporności należy rozumieć jako odnoszące się do zdolności infrastruktury krytycznej do zapobiegania zdarzeniom, które w istotny sposób zakłócają lub mogą w istotny sposób zakłócić świadczenie usług kluczowych (…), a także do zdolności tej infrastruktury do ochrony przed takimi zdarzeniami, reagowania na nie, przeciwstawiania się im, łagodzenia lub amortyzowania ich skutków, przystosowywania się do nich lub przywracania poprzedniego stanu.*

W dalszej części tego dokumentu napisano, że *należy dalej rozwijać możliwości przeprowadzania na szczeblu krajowym testów warunków skrajnych dotyczących infrastruktury krytycznej, ponieważ testy takie mogłyby być przydatne do zwiększenia odporności infrastruktury krytycznej i wreszcie, że ze względu na rosnącą współzależność infrastruktury fizycznej i cyfrowej szkodliwe działania w cyberprzestrzeni ukierunkowane na obszary krytyczne mogą powodować zakłócenia lub szkody w infrastrukturze fizycznej, a sabotaż infrastruktury fizycznej może sprawić, że niedostępne staną się usługi cyfrowe.*

To wszystko zdaje się zachęcać do analizy incydentów oraz wykorzystywania ich do tworzenia scenariuszy testowych dla chronionych obiektów, aby doświadczenia z tych testów wzmacniały zdolności ochronne oraz budowały odporność organizacji na zagrożenia wydawałoby się z minionej epoki, które jednak przyszły do nas i powinny być traktowane jako zagrożenia współczesne, rzeczywiste i możliwe do wystąpienia.

Testy penetracyjne ochrony fizycznej są więc rozwiązaniem nie tylko przydatnym, ale w obecnej sytuacji wręcz niezbędnym. I nie mam tu na myśli pomysłów rodem z filmu *Mission: Impossible,* ale dobrze przemyślany projekt audytowy, zbudowany na precyzyjnym scenariuszu, aby test dawał jak najbardziej wiarygodny wynik, podobnie jak efektywne rozpoznanie najbliższego sąsiedztwa chronionych obiektów oraz jego włączenie do katalogu standardowych działań realizowanych w ramach całego systemu bezpieczeństwa, no i oczywiście zapewnienie ciągłości i wysokiej stałej efektywności tego procesu.

Pamiętajmy, że nie ma absurdalnych scenariuszy, jedynie nasza wyobraźnia jest zbyt uboga… w przeciwieństwie do wyobraźni hiszpańskich „nurków" poszukujących nocą bursztynu w Bałtyku. ●

> *Pojęcie odporności należy rozumieć jako odnoszące się do zdolności infrastruktury krytycznej do zapobiegania zdarzeniom, które w istotny sposób zakłócają lub mogą w istotny sposób zakłócić świadczenie usług kluczowych.*

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. Dyrektor Centrum Kompetencji „a&s Polska".

Infrastruktura naprawdę krytyczna

Minął ponad rok od napaści Rosji na Ukrainę. 24 lutego 2022 r. cały świat wstrzymał oddech. Walka zbrojna trwa, a w Europie toczy się debata na temat bezpieczeństwa infrastruktury krytycznej państw członkowskich Unii Europejskiej. Czy w Polsce to dziś temat numer jeden i czy w najbliższym czasie należy spodziewać się wzmocnienia zabezpieczenia IK?

Michalina Nowak, a&s Polska

Otwarcie o zagrożeniu dla obiektów infrastruktury krytycznej ze strony Rosji mówią zarówno Niemcy, jak i Norwegowie. W opublikowanym niedawno raporcie norweskie służby odpowiedzialne za bezpieczeństwo wprost wskazały, że w razie rosyjskiego konfliktu z NATO Rosja może zaatakować infrastrukturę krytyczną tego kraju. W ubiegłym roku po wstrzymaniu dostaw gazu przez Moskwę Norwegia stała się bowiem głównym dostawcą tego surowca do Europy. Niemiecka infrastruktura krytyczna ulega z kolei coraz częściej awariom i staje się ofiarą cyberataków oraz ataków terrorystycznych na tle politycznym. W październiku 2022 r. po sabotażu, który polegał na przecięciu kabli kolei niemieckiej, doszło do kilku kolejnych incydentów. Obiekty IK są obserwowane przez profesjonalne drony, których pochodzenie „nie jest oczywiste" – piszą media w Berlinie.

Stres-testy w IK

W obliczu zagrożenia ze strony Rosji Unia Europejska została zmuszona do szybszego działania na rzecz ochrony IK. Jesienią 2022 roku Ursula von der Leyen, przewodnicząca Komisji Europejskiej, przedstawiła 5-punktowy plan na rzecz odporności infrastruktury krytycznej. Jego najważniejsze elementy to:

1. wzmocnienie gotowości;
2. współpraca z państwami członkowskimi, by poddać ich infrastrukturę krytyczną testom warunków skrajnych (tzw. stres-testom znanym m.in. w świecie finansów), najpierw w sektorze energetycznym, a następnie w innych sektorach wysokiego ryzyka;
3. zwiększenie zdolności reagowania, w szczególności za pośrednictwem Unijnego Mechanizmu Ochrony Ludności;
4. efektywne wykorzystanie potencjału satelitarnego do wykrywania ewentualnych zagrożeń;
5. zacieśnienie współpracy z NATO i kluczowymi partnerami w zakresie odporności infrastruktury krytycznej.

Mając świadomość powagi problemu i wyzwań, wobec których stoją dziś menedżerowie odpowiedzialni za bezpieczeństwo w obiektach IK, zapytaliśmy kilku, jakie stoją przed nimi wyzwania i jakie działania wzmacniające zabezpieczenia zamierzają podjąć.

Pod wysokim napięciem

Bezpieczeństwo energetyczne stanowi jeden z podstawowych elementów warunkujących możliwość zapewnienia bezpiecznego funkcjonowania państwa oraz trwałego i niezakłóconego jego rozwoju. Ten sektor nabrał dodatkowego znaczenia nie tylko ze względu na skutki wojny w Ukrainie czy panujący kryzys gospodarczy. Rozwój gospodarczy łączy się bowiem z dużym wzrostem globalnego zapotrzebowania na energię, surowce energetyczne czy paliwa, a to wymusza transformację energetyczną. Według prognoz Energy Information Administration produkcja energii

elektrycznej do 2050 r. wzrośnie o 79%. Prawdopodobne jest również to, że już w 2035 r. nawet 50% energii elektrycznej będzie pochodzić ze źródeł odnawialnych.

Jak wynika z raportu Polskiego Komitetu Energii Elektrycznej, polskie spółki energetyczne intensywnie inwestują w odnawialne źródła energii (OZE). Do 2030 r. PGE planuje zmagazynowanie co najmniej 800 MWe, Tauron zakłada zwiększenie mocy OZE o ponad 500% w stosunku do 2030 r., Enea zamierza przebudować sieć pasywną na aktywną (dwukierunkową) oraz przekształcić infrastrukturę sieciową w tzw. inteligentną (*smart grid*), Energa zaś chce osiągnąć do 2030 r. aż 1,1 GWe mocy w lądowych OZE oraz udział w projektach MFW o mocy ok. 1,3 GWe.

Wszystkie obiekty elektroenergetyczne oraz sieci przesyłowe i dystrybucyjne wymagają więc szczególnej ochrony, by sprostać zmianom modelu wytwarzania energii i gospodarowania nią. O bezpieczeństwie jednego z największych dystrybutorów energii elektrycznej w Polsce mówi Ireneusz Rupik, specjalista ds. bezpieczeństwa w Grupie TAURON. – *Bezpieczeństwo jest priorytetem dla całej branży energetycznej. Wciąż pracujemy nad procesem udoskonalania rozwiązań oraz utrzymywania najwyższych standardów w zakresie fizycznego i technicznego bezpieczeństwa obiektów infrastruktury energetycznej.*

> *Oprócz najnowszych rozwiązań technicznych bardzo ważne jest podnoszenie świadomości zagrożeń wśród ludzi, gdyż to oni są najsłabszym ogniwem we wszystkich systemach bezpieczeństwa.*

Co to oznacza w praktyce? W ostatnim czasie Wsparcie Grupa TAURON stała się częścią prowadzonego przez Polski Holding Obronny projektu integracji polskiego sektora ochrony.

– *W Grupie TAURON usługi ochrony osób i mienia w zakresie ochrony fizycznej, montażu i obsługi systemów zabezpieczenia technicznego oraz monitorowania alarmów świadczy firma Wsparcie Grupa TAURON, z własną stacją monitorowania alarmów. Włączenie spółki WGT do struktur grupy PHO jest kolejnym krokiem w kierunku budowy silnego, narodowego lidera w świadczeniu kompleksowych usług ochrony. Dzięki dokonanej konsolidacji, wymianie doświadczeń, rozbudowie technologii oraz nowym obowiązkom Polski Holding Obronny wraz ze spółką Wsparcie Grupa TAURON stanie się jednym z filarów krajowego bezpieczeństwa oraz ochrony infrastruktury krytycznej państwa* – wyjaśnia specjalista.

Zapewnienie odpowiedniego poziomu bezpieczeństwa wiąże się z inwestycjami w systemy zabezpieczeń z najnowszymi technologiami. – *W roku 2023 w związku z realizacją opracowanej Koncepcji Systemu Zabezpieczenia Technicznego i Ochrony Fizycznej (SZT i OF) dla obiektu TAURON przygotowujemy postępowania przetargowe na nowe inwestycje. Wśród nich planujemy wykonanie dokumentacji projektowej dla nowych systemów zabezpieczenia technicznego obiektu, wykonanie projektu nowego DSO i modernizacji, wymiany systemu sygnalizacji pożarowej czy opracowanie projektu nowej organizacji ruchu dla obiektu wraz z przebudową ciągów komunikacyjnych* – dodaje Ireneusz Rupik.

Wodociągi nie dają się zatopić przeciwnościom

Człowiek powinien pić 2–2,5 l wody dziennie. Do tego dochodzą potrzeby związane z utrzymaniem czystości i higieny. Przyjmuje się, że jedna osoba w gospodarstwie domowym produkuje od 80 do 120 l ścieków dziennie. Odcięcie dostaw wody przez jeden dzień nie stanowi wielkiej niedogodności, lecz co się stanie, kiedy wodociągi nie będą działać przez tydzień, a woda butelkowana w sklepach zostanie wyprzedana?

Jednym z największych wyzwań w zakresie zabezpieczenia dostaw wody i odbioru ścieków jest przede wszystkim skuteczne zabezpieczenie… dostaw energii elektrycznej niezbędnej do tego, by działały przepompownie wodne i kanalizacyjne. Nie należy przy tym zapominać, że infrastruktura tych obiektów musi być odporna na zmiany temperatury w poszczególnych porach roku, gwałtowne zjawiska pogodowe, brak opadów, ale też powodzie. Sytuację utrudnia też fakt, że spółki wodociągowo-kanalizacyjne odczuwają skutki kryzysu gospodarczego. Gwałtowny wzrost kosztów energii elektrycznej oraz gazu przy równoczesnym niezmienionym poziomie taryf to duże wyzwanie.

O plany przedsiębiorstw wodociągowo-kanalizacyjnych zapytaliśmy organizację samorządu gospodarczego z tej branży Izbę Gospodarczą Wodociągi Polskie.

– *Najistotniejszym długofalowym celem branży jest oczywiście uzyskanie przez obiekty infrastruktury krytycznej samowystarczalności energetycznej, która pozwoli na uniezależnienie się od dostawców zewnętrznych. Przedsiębiorstwa wodociągowo-kanalizacyjne do tego dążą poprzez wdrażanie nowoczesnych rozwiązań technicznych i technologicznych w swoich obiektach, w myśl zarządzeń kryzysowych* – mówi główny specjalista ds. technicznych Paulina Kopeć z Izby Gospodarczej Wodociągi Polskie.

Ale to nie wszystko. W związku z dwoma nowymi dyrektywami przyjętymi w zeszłym roku (o odporności infrastruktury krytycznej i cyberbezpieczeństwie) Polska jest zobowiązana do transpozycji tych dyrektyw do polskiego prawa. – *Branża wodno-kanalizacyjna chce czynnie uczestniczyć w transpozycji i wdrażaniu tych dyrektyw. Nie jest to zadanie proste, szczególnie w kontakcie realizacji inwestycji* – dodaje.

Wojna w Ukrainie sprawiła, że wiele przedsiębiorstw weryfikuje obecnie schematy postępowania na wypadek działań wojennych. W każdej sytuacji kryzysowej niezwykle istotne są opracowane wcześniej plany, które pozwalają przedsiębiorstwom poradzić sobie z niespodziewanym zdarzeniem bez przerw w pracy. Jak zapewnia ekspert, przedsiębiorstwa wodociągowo-kanalizacyjne są przygotowane na różnego rodzaju kryzysy.

– *Przedsiębiorstwa są stale kontrolowane przez instytucje państwowe, co sprawia, że dopasowują się do nowych wyzwań i wymagań zarządzeń kryzysowych. Wprowadzają plany bezpieczeństwa wody oraz wdrażają najnowsze systemy informatyczne zarządzania w tym zakresie, znacznie poprawiając wydajność monitoringu poszczególnych etapów pobierania, uzdatniania i dostawy wody oraz odbioru i oczyszczania ścieków* – podkreśla Paulina Kopeć.

Nowe prawo transponujące dyrektywę w sprawie wody pitnej (DWD) nakłada obowiązek zarządzania ryzykiem w systemach zaopatrzenia, przez co plany bezpieczeństwa wody będą obowiązkowe – na co przedsiębiorstwa wodociągowo-kanalizacyjne są gotowe.

Infrastruktura telekomunikacyjna na fali zabezpieczeń

Infrastruktura krytyczna to także telekomunikacja. Według raportu o stanie rynku telekomunikacyjnego w Polsce za rok 2021 liczba zainstalowanych własnych węzłów sieci telekomunikacyjnych wzrosła o blisko 30 tys. w ciągu roku. Przyrost ten przekłada się na zwiększenie zasięgu sieci szerokopasmowych. W roku 2021 dostęp do Internetu stacjonarnego o przepustowości minimalnej 30 Mb/s miało ponad 80% gospodarstw domowych, a dzięki sfinalizowaniu zatwierdzonych projektów w ramach Programu Operacyjnego Polska Cyfrowa (POPC) dostęp szerokopasmowy uzyska kolejne 4% gospodarstw. Szacuje się, że w 2026 r. 81% użytkowników mobilnego dostępu do Internetu będzie korzystać z technologii 5G.

Tym perspektywom towarzyszą wyzwania. Wśród realnych zagrożeń dla infrastruktury telekomunikacyjnej najczęściej wymienia się brak dostaw prądu, błędy wywołane przez tzw. czynnik ludzki oraz

REKLAMA

> *Paleta zagrożeń i obszar cyberataków rośnie wraz z liczbą stosowanych technologii oraz coraz większym tempem tworzenia aplikacji. Niestety często oznacza to luki w zabezpieczeniach urządzeń, oprogramowaniu systemowym czy aplikacjach.*

niestabilne powiązania międzysektorowe. Polska Izba Informatyki i Telekomunikacji przekonuje, że zobowiązanie do utrzymania ciągłości sieci w Polsce traktuje bardzo poważnie. Jak zatem jest zabezpieczana infrastruktura telekomunikacyjna?

O wypowiedź poprosiliśmy jednego z największych operatorów naziemnej infrastruktury radiowo-telewizyjnej spółkę Emitel. *– Jako spółka robimy bardzo dużo, aby zbudować wysoki poziom odporności na potencjalne zagrożenia, które mogą wystąpić w przyszłości. Musimy jednak pamiętać, że budowanie bezpieczeństwa to proces długotrwały. Potrzeba czasu, cierpliwości, konsekwencji, doświadczenia i specyficznego rodzaju kompetencji. Wdrożyliśmy procedury zarządzania bezpieczeństwem informacji, przejrzeliśmy i wprowadziliśmy najlepsze praktyki rynkowe, cały czas wykorzystujemy elementy i rozwiązania z zakresu IoT. Mamy zorganizowane struktury zarządzania kryzysowego, które przetestowaliśmy skutecznie podczas pandemii, wdrożyliśmy i konsekwentnie rozwijamy oraz udoskonalamy np. ISMS (system zarządzania bezpieczeństwem informacji wg ISO 27001) czy BCMS (system zarządzania ciągłością działania wg ISO 22301)* – mówi Marcin Buzdygan, dyrektor Biura Zarządzania Bezpieczeństwem w Emitel.

Oprócz stosowania najnowszych rozwiązań technicznych bardzo ważne jest podnoszenie świadomości zagrożeń wśród ludzi, gdyż to oni są najsłabszym ogniwem we wszystkich systemach bezpieczeństwa.

– Przykładamy ogromną wagę do budowania świadomości oraz poszerzania wiedzy pracowników i współpracowników w zakresie procedur bezpieczeństwa, w tym szczególnie bezpieczeństwa informacji oraz ciągłości działania. Kompetentna i świadoma zagrożeń kadra to bardzo istotny element bezpieczeństwa – podkreśla Marcin Buzdygan.

Obiekty IK na celowniku cyberprzestępców

Infrastruktura krytyczna potrzebuje dziś nie tylko najwyższej klasy systemów zabezpieczeń technicznych, ale także stałego monitorowania zagrożeń, które pojawiają się w cyberprzestrzeni. Według prognoz Check Point w 2023 r. liczba cyberataków na obiekty użyteczności publicznej, w tym przedsiębiorstwa gazowe i energetyczne, transport publiczny, służbę zdrowia czy przedsiębiorstwa zaopatrzenia w wodę, wzrośnie. Jak podają eksperci Noventiq, Polska zajmuje szóste miejsce w Europie pod względem zagrożeń cybernetycznych. Dane wskazują również, że w 2022 r. rodzime firmy doświadczały ataków hakerskich średnio co 9 minut.

– Paleta zagrożeń i obszar cyberataków rośnie wraz z liczbą stosowanych technologii oraz coraz większym tempem tworzenia aplikacji. Niestety często oznacza to luki w zabezpieczeniach urządzeń, oprogramowaniu systemowym czy aplikacjach. Jednym z rozwiązań stosowanym w Grupie TAURON jest monitorowanie zdarzeń bezpieczeństwa w wielu warstwach, począwszy od ruchu sieciowego w urządzaniach infrastruktury, skończywszy na logowaniu zdarzeń z aplikacji użytkownika. Tak duże powiększenie obserwowanego obszaru daje lepsze spojrzenie na odporność organizacji na cyberzagrożenia – wskazuje Ireneusz Rupik.

Zapewnienie bezpieczeństwa informatycznego wiąże się z jednej strony z zatrudnianiem specjalistów umiejętnie, wręcz intuicyjnie rozpoznających niebezpieczeństwo, z drugiej – taka edukacja szeregowych pracowników, by byli odporni na manipulacje socjotechniczne, jakimi posługują się cyberprzestępcy. Wciąż bowiem najsłabszym ogniwem łańcucha zabezpieczeń obiektów infrastruktury krytycznej jest… człowiek (więcej na ten temat w artykule *Najlepsza polityka: zero zaufania*, *str. 46)*.

– Cyberzagrożenia stają się coraz większym wyzwaniem, szczególnie że ulegają dynamicznej zmianie. Pojawiają się nowe formy tego ryzyka. Staramy się je poznawać i eliminować. Współpracujemy z wieloma podmiotami, instytucjami i organizacjami, które nam w tym pomagają. Skupiamy się nie tylko na rozwiązaniach technicznych czy procesowo ograniczanych (ISMS czy też BCMS), ale także na edukacji naszej kadry. Kluczowym działaniem, jakie obecnie realizujemy, jest budowanie świadomości naszego zespołu pracowników. Uważamy, że wysoki poziom świadomości prowadzi do zmniejszenia ryzyka zagrożeń. Angażujemy zespół w ćwiczenia, regularnie organizujemy testy i prowadzimy kampanie edukacyjne, w tym spotkania online – mówi Marcin Buzdygan.

Przywoływane przez naszych rozmówców działania każą nam wierzyć, że security managerowie obiektów IK są dziś świadomi wielu zagrożeń i przygotowują swoje organizacje na realne stres-testy. Czy tak jest naprawdę? Obyśmy nie musieli się o tym przekonać.

AS
ALNET
SYSTEMS

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

NS ENTERPRISE
CMS HUB
CMS PROFESSIONAL
VCA MODULE
CMS MOBILE
NET ACCESS
NET POS
PRS ALNET

www.alnetsystems.com

Rewolucja w IK. Powstanie RCB 2.0

Powstanie narodowy audytor infrastruktury krytycznej. Przyjęta w tym roku Dyrektywa ds. odporności podmiotów krytycznych (CER) Unii Europejskiej zobowiązuje kraje członkowskie do utworzenia instytucji na kształt RCB 2.0. lub RCB PLUS. Będzie ona miała kompetencje do przeprowadzania kontroli i karania w sytuacji, gdy ochrona IK nie jest traktowana poważnie i zagraża funkcjonowaniu ciągłości działania Rzeczypospolitej Polskiej.

O zmianach, jakie czekają instytucje IK, z dr **Karoliną Wojtasik,** ekspertem RCB w dziedzinie ochrony obiektów, infrastruktury krytycznej oraz terroryzmu rozmawia Michalina Nowak.

Zacznijmy trochę przewrotnie od toczącej się dyskusji o likwidacji Rządowego Centrum Bezpieczeństwa. Co się wtedy stanie? Kto przejmie zadania RCB? Jak widzi pani kwestię ochrony IK po rozwiązaniu RCB?
To nie tyle „dyskusja o likwidacji RCB", ile wciąż zapis w aktualnym na luty 2023 r. projekcie ustawy o ochronie ludności i stanie klęski żywiołowej przygotowanym przez MSWiA. Odpowiadając kolokwialnie na pytanie, „co wtedy?", wtedy, jak w mitologii, będzie chaos. Ale zanim z chaosu wyłoni się cokolwiek, zanim powstaną rozporządzenia szczegółowe precyzujące tryb pracy i kompetencje nowego tworu czy tworów, będziemy tracić cenny czas. Tym bardziej cenny, że infrastruktura krytyczna jest dziś celem różnej formy ataków w ramach tzw. działań hybrydowych ze strony Federacji Rosyjskiej na skalę nienotowaną w naszej historii. To czas, którego absolutnie nie możemy zmarnować, zwłaszcza w aktualnej sytuacji geopolitycznej. Jak pokazują doświadczenia Ukrainy, infrastruktura krytyczna była celem wrogich działań na długo, zanim zaczęły się ataki kinetyczne (zbrojne). Dlatego dziś niezwykle ważne jest budowanie sprawnego systemu ochrony IK.

17 stycznia weszła w życie dyrektywa CER *(Critical Entities Resilience)* w sprawie odporności podmiotów krytycznych. W dokumencie zapisano m.in. obowiązek powołania „właściwej władzy", która będzie miała za zadanie dopilnować jej wdrożenia. Nie chodzi tylko o akceptację planów odpornościowych, ale też o zlecanie, prowadzenie audytów oraz karanie w przypadku naruszenia przepisów. Kto ma to robić? Rządowe Centrum Bezpieczeństwa nie ma obecnie takich uprawnień...
Dyrektywa CER daje ramy prawne na stworzenie swoistego RCB 2.0 lub – jak kto woli – RCB PLUS z kompetencjami do audytu i karania w sytuacji, gdy ochrona IK nie jest traktowana poważnie i zagraża funkcjonowaniu ciągłości działania RP. I zgadza się, na razie takich uprawnień RCB nie ma, a czas ucieka. Potrzebujemy infrastruktury krytycznej, żeby sprawnie funkcjonować jako nowoczesne społeczeństwo. A RCB potrzebuje bata na tych, którzy ochrony IK nie traktują wystarczająco poważnie. Centralnego podmiotu koordynującego ochronę IK nie zbudujemy w miesiąc, bo takie zespoły specjalistów tworzy się latami.

Zatem dyrektywa CER jest szansą na wzmocnienie RCB?
Jest szansą nie tylko na wzmocnienie RCB, lecz także na sprawny system ochrony IK, który oprze się agresorowi i będzie odpowiedzią na wyzwania przyszłości. W tej trudnej sytuacji geopolitycznej możemy stanowić wzór do naśladowania dla innych państw regionu i tym samym możemy dać impuls do zmian ich wewnętrznych procedur ochrony IK, jest jeszcze na to czas. To może być polski wkład w budowanie odporności całej Unii Europejskiej na zagrożenia hybrydowe. Widzę tego ogromną szansę.

No właśnie, budowanie odporności to jeden z kluczowych elementów przygotowywania się na kryzys bez względu na to, czego miałby on dotyczyć. Robimy to?
Staramy się, odkąd istnieje pojęcie infrastruktury krytycznej i funkcjonuje RCB. Niestety dotychczas ramy prawne nie pozwalały na wiele czynności w zakresie audytu i kontroli. Wspomniana dyrektywa CER nie bez powodu ma słowo „odporność" w tytule. Jedyny organ realizujący elementy kontroli i nadzoru w Polsce wobec obiektów, które kwalifikują się do IK systemu transportu, jest Urząd Lotnictwa Cywilnego prowadzący kontrole systemu bezpieczeństwa w lotnictwie cywilnym. Niestety nie mamy w kraju instytucji, która ma prawo robić choćby stres-testy czy testy penetracyjne ochrony fizycznej obiektów IK. Pewne ograniczone uprawnienia w tym zakresie w obszarze cyber od 2016 r. posiada ABW.

RCB prowadzi nadzór nad ochroną krajowej i europejskiej infrastruktury krytycznej. Jednocześnie przygotowuje Narodowy Plan Ochrony Infrastruktury Krytycznej, sporządza jednolity wykaz IK oraz pełni funkcję krajowego punktu kontaktowego. Operatorzy IK mają obowiązek przygotować plan ochrony IK zatwierdzany przez dyrektora RCB. Na czym w takim razie polega wspomniany nadzór?
Celem wszystkich wymienionych czynności jest doprowadzenie do takiej sytuacji, że polskie społeczeństwo będzie w stanie sprawnie funkcjonować, a administracja państwowa zachowa ciągłość działania. Chodzi o to, żeby obywatele mogli żyć, pracować, wykonywać codzienne czynności, a w sytuacjach kryzysowych odczuli ich skutki w stopniu minimalnym. To wszystko jest możliwe dzięki sprawnie działającym systemom IK.

Pod każdym z wymienionych wyżej pojęć kryją się setki czynności, które składają się na element wspomnianego nadzoru, choćby NPOIK, czyli Narodowy Plan Ochrony Infrastruktury Krytycznej, którego celem jest stworzenie warunków do poprawy bezpieczeństwa IK. NPOIK podlega aktualizacji przynajmniej raz na dwa lata, bo świat nie stoi w miejscu, a rozwój technologiczny sprawia, że pojawiają się nowe zagrożenia, które trzeba w NPOIK uwzględnić.

Na przykład?
Na przykład bezzałogowe statki powietrzne. Drony mogą nie tylko zostać użyte w różnych formach sabotażu, lecz także prowadzić rozpoznanie, filmować obiekt, zrobić zdjęcia kluczowych instalacji. Na takie zagrożenia RCB reaguje na bieżąco.

Co powinien zawierać plan ochrony IK?
To w sposób szczegółowy reguluje rozporządzenie *(Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej).* Zgodnie z tym rozporządzeniem operatorzy obiektów infrastruktury krytycznej sporządzają plan ochrony IK w terminie 9 miesięcy od daty otrzymania od Dyrektora RCB informacji o ujęciu w wykazie IK. Plan ochrony IK zawiera kilka rodzajów informacji: dane ogólne (nazwę, lokalizację, NIP, REGON, dane osoby odpowiedzialnej za utrzymywanie kontaktu z podmiotami właściwymi w zakresie ochrony IK), dane IK (charakterystykę i podstawowe parametry techniczne, szczegółową mapę, informacje o funkcjonalnych połączeniach z innymi obiektami, instalacjami, usługami) oraz ocenę ryzyka z przewidywanym scenariuszem rozwoju wydarzeń. W planie opisuje się również zależności obiektu IK od innych systemów czy też zasoby własne, które można wykorzystać w celu ochrony IK.

Kolejna grupa informacji to warianty działania: w sytuacji zagrożenia lub zakłócenia funkcjonowania IK; zapewnienia ciągłości funkcjonowania IK; odtwarzania IK oraz zasady współpracy z właściwymi miejscowo centrami zarządzania kryzysowego i organami administracji publicznej. Dokument jest więc złożony i procedury w nim zawarte są kluczowe dla zapewnienia bezpieczeństwa IK. Jeśli wcześniej istniały, plan jest dokumentem, który je spaja, jeśli ich nie było, operator jest zobligowany je wprowadzić. Ale od czasu ogłoszenia wspomnianego rozporządzenia zmieniono niektóre przepisy ustawy o zarządzaniu kryzysowym.

Co w takim razie będzie kluczowe dla przedsiębiorcy?
Dla przedsiębiorcy kluczowy będzie zapis (art. 6 pkt 5b) mówiący o tym, że jeśli operator IK jest równocześnie

> *» Dyrektywa CER daje ramy prawne na stworzenie swoistego RCB 2.0 lub – jak kto woli – RCB PLUS z kompetencjami do audytu i karania w sytuacji, gdy ochrona IK nie jest traktowana poważnie i zagraża funkcjonowaniu ciągłości działania Rzeczypospolitej Polskiej. «*

→

dostawcą usługi kluczowej, to w planie ochrony IK uwzględnia dokumentację dotyczącą cyberbezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia usług kluczowych, czyli nie uzgodni planu ochrony IK, jeśli nie dopełnił obowiązków w zakresie cyberbezpieczeństwa. Poza tym praktyka jest taka, że do planu ochrony IK dołącza się szereg innych funkcjonujących w przedsiębiorstwie planów bezpieczeństwa, np. plan ochrony fizycznej, załącznik AT do planu ochrony, plany bezpieczeństwa technicznego/procesowego. Tym sposobem plan ochrony IK pokazuje całościowo, jak operator IK wywiązuje się z obowiązku zapewnienia ochrony: fizycznej, technologicznej, osobowej, prawnej, teleinformatycznej i planów ciągłości działania, które niekiedy określa się mianem sześciopaku. Z reguły tego typu dokumenty mają kilkaset stron.

Czy w jakikolwiek sposób sprawdzane jest wdrażanie założeń w planach ochrony IK?

Plan ochrony jest konsultowany z wieloma instytucjami, które wypowiadają się wg swojej właściwości w kwestii realizacji celu nadrzędnego, jakim jest ochrona IK. Jeśli mają uwagi, plan jest korygowany. RCB nie jest więc jedyną instytucją, która sprawdza, jak jest wykonywana ochrona IK. Tymi podmiotami są właściwi terytorialnie: wojewoda, komendant wojewódzki Państwowej Straży Pożarnej, komendant wojewódzki policji, dyrektor regionalnego zarządu gospodarki wodnej, wojewódzki inspektor nadzoru budowlanego, wojewódzki lekarz weterynarii, państwowy wojewódzki inspektor sanitarny, dyrektor urzędu morskiego, minister lub kierownik urzędu centralnego, w którego właściwości znajduje się system, do którego została zaliczona dana infrastruktura krytyczna.

> *Niestety nie mamy w kraju instytucji, która ma prawo robić choćby stres-testy czy testy penetracyjne ochrony fizycznej obiektów IK.*

W NPOIK jest zapis mówiący, że zatwierdzony plan ochrony IK jest podstawowym dokumentem potwierdzającym spełnienie przez operatora obowiązku ochrony IK, a plan jest ilustracją nakładu pracy włożonej w przygotowanie i wdrożenie ochrony IK. Poprawnie przeprowadzony proces planowania podnosi zdolność organizacji do identyfikacji i zmniejszania podatności, przeciwdziałania zagrożeniom, reakcji na nie oraz minimalizacji skutków ich wystąpienia. Tak jak wspomniałam, do prowadzenia audytu, kontroli czy nadawania sankcji RCB obecnie nie ma uprawnień. Przyjęta w tym roku w Unii Europejskiej Dyrektywa ds. odporność podmiotów krytycznych zobowiązuje kraje członkowskie do utworzenia narodowego audytora IK, de facto w przypadku Polski takiego RCB 2.0./RCB PLUS.

Czy przedsiębiorcy, którzy są właścicielami obiektów IK lub nimi zarządzają, współpracują z RCB?

Obliguje ich do tego ustawa, ponadto RCB daje dostęp do unikatowej wiedzy. Coroczne Krajowe Forum Ochrony IK gromadzi specjalistów z zakresu różnych aspektów ochrony IK. Podczas zeszłorocznego forum poruszano wątek zagrożenia ze strony dronów, rozpoznania informacyjnego prowadzonego przez wrogie służby wobec obiektów IK w Europie Wschodniej, zagrożeń dla systemu transportu kolejowego w warunkach wojny hybrydowej itp. RCB oferuje standardy organizowania ochrony w różnych aspektach bezpieczeństwa IK. Jeśli operator IK poważnie traktuje ochronę i bezpieczeństwo IK, to RCB jest jego naturalnym partnerem.

A w jaki sposób do kwestii bezpieczeństwa IK podchodzą zarządzający tymi obiektami?

Bezpieczeństwo IK to zagadnienie bardzo złożone i wielowątkowe. Operatorzy IK, czyli właściciele oraz posiadacze samoistni i zależni obiektów, instalacji, urządzeń i usług IK, są różni tak, jak obiekty, którymi zarządzają, dlatego niemożliwe jest udzielenie jednoznacznej odpowiedzi na to pytanie. NPOIK zakłada, że będzie on realizowany na zasadach współodpowiedzialności, współpracy i zaufania. Jakkolwiek to, jak jest zapewniana ochrona IK w przedsiębiorstwie, zależy w dużym stopniu od podejścia i poziomu świadomości zarządzających danym operatorem IK. Nakłady na szeroko rozumiane bezpieczeństwo najczęściej nie są widoczne gołym okiem tak, jak spektakularne inwestycje, nie można się nimi pochwalić np. przed wyborami samorządowymi. W dobie kryzysu ekonomicznego, inflacji i rosnących rachunków priorytetem jest przetrwanie, ewentualnie najpilniejsze naprawy, wtedy myślenie o bezpieczeństwie schodzi na dalszy plan, bo są pilniejsze wydatki.

Kolejna kwestia to świadomość. IK jest niezbędna do funkcjonowania społeczeństwa i zapewnienia ciągłości na szczeblach zarówno centralnym, jak i lokalnym administracji państwowej – to czujemy podskórnie i nie wymaga wyjaśnienia. Jednakże praktyka w wielu przedsiębiorstwach jest taka, że status IK traktuje się jako kolejny przykry obowiązek. Wyznacza osobę odpowiedzialną za kontakt z RCB i zespół sporządzający plan bądź zleca tę czynność na zewnątrz. A ochrona IK powinna być traktowana holistycznie, czyli powinna być wpisana w DNA przedsiębiorstwa i realizowana w każdym dziale. Ochrona osobowa, ochrona prawna, ochrona teleinformatyczna (i pozostałe elementy ochrony IK) powinny być realizowane w każdym dziale. Bardzo często takie podejście nie przebija się na zarząd operatora IK bądź tam, gdzie zapadają kluczowe decyzje.

Sytuacji nie ułatwia fakt, że jedno przedsiębiorstwo może mieć jednocześnie status IK, podlegać tzw. obowiązkowej ochronie i szczególnej ochronie, a także być dostawcą usług kluczowych...

Tak, a za każdym z tych terminów idą konkretne obowiązki do spełnienia i wymogi. Trudno się nie pogubić. Kiedyś na konferencji podszedł do mnie przedstawiciel przedsiębiorstwa z miasta na prawach powiatu i zapytał, czy oni są IK, bo im się wydaje, że mogliby być, ale nie mają pewności i nie bardzo wiedzą, gdzie to sprawdzić. I to pokazuje, że często zwyczajnie brakuje wiedzy i świadomości. I najważniejsze, nie ma sankcji karnych dla przedsiębiorstw, które nie realizują NPOIK, np. w kwestii braku zatwierdzonego planu ochrony IK. Bywa też tak, że pierwsze pytanie przełożonego brzmi: ile wynosi kara za brak planu i czy to jest egzekwowane.

Niestety, podczas mojej pracy badawczej nad systemami IK oraz pracy zawodowej wielokrotnie pojawiły się niepokojące praktyki nadwerężające bezpieczeństwo tego typu obiektów. Jedną z nich jest rozpoczynanie cięć kosztów funkcjonowania IK od oszczędności na jego ochronie fizycznej. To tylko pozorna oszczędność. Przywołana przeze mnie unijna dyrektywa CER raz na zawsze te praktyki ukróci. Dlatego wszystkim nam powinno zależeć na tym, by weszła ona w życie jeszcze w tej kadencji Sejmu. W przypadku cyberbezpieczeństwa niedotrzymanie obowiązków operatora usług kluczowych oznacza spore kary finansowe, w przypadku IK dotychczas ich nie było. Jakkolwiek w razie poważnej awarii czy sytuacji kryzysowej warto pamiętać, że to będzie pierwsze pytanie prokuratury czy instytucji nadzorującej: czy spełniono wymogi i zastosowano obowiązujące procedury. A wielu przedsiębiorców o tym zapomina.

Czy jest przewidziane dofinansowanie ochrony IK ze środków publicznych? Jakie są potrzeby w tym zakresie?

Zgodnie z wymienioną już tu ustawą o zarządzaniu kryzysowym obowiązki w zakresie ochrony IK spoczywają na właścicielach oraz posiadaczach samoistnych i zależnych obiektów, instalacji lub urządzeń infrastruktury krytycznej, czyli operatorach IK. O tym, czy dany obiekt znajduje się w wykazie infrastruktury krytycznej, decyduje ostatecznie Dyrektor RCB we współpracy z właściwym ministrem, który nadzoruje dany system Operatora IK. Przedsiębiorca może też wystąpić z wnioskiem na piśmie do właściwego ministra odpowiedzialnego za system IK lub do dyrektora RCB o dokonanie oceny czy posiadane/zarządzane przez niego obiekty spełniają wymagania określone dla IK. Dyrektor RCB informuje następnie właściciela lub posiadacza IK, że jego obiekty zostały umieszczone w wykazie. Od tego momentu na właścicielu lub posiadaczu IK spoczywają szczególne obowiązki wynikające z ustawy, o których mówiłam wcześniej. Przynajmniej tak to wyglądało dotychczas.

I w tym momencie wracamy do dyrektywy CER, ponieważ zakłada ona, że podmioty krytyczne będą mogły liczyć na wsparcie finansowe od państwa, jeśli będzie to uzasadnione bezpieczeństwem publicznym. I ten rodzaj wsparcia nie będzie traktowany jako niedozwolona pomoc publiczna, co otwiera pole do przeznaczenia publicznych środków na ochronę IK i bezpośrednio angażuje państwo w zapewnienie podstawowych usług obywatelom.

> *Podczas mojej pracy badawczej nad systemami IK oraz pracy zawodowej wielokrotnie pojawiły się niepokojące praktyki nadwerężające bezpieczeństwo obiektów infrastruktury krytycznej. Jedną z nich jest rozpoczynanie cięć kosztów ich funkcjonowania od oszczędności na ochronie fizycznej. To tylko pozorna oszczędność. Przywołana przeze mnie unijna dyrektywa CER raz na zawsze te praktyki ukróci.*

Zmiana podejścia do problemów bezpieczeństwa w infrastrukturze krytycznej

Infrastruktura krytyczna to najbardziej newralgiczne obiekty dla funkcjonowania społeczeństwa i gospodarki. Zakres ochrony musi uwzględniać różne aspekty, takie jak utrzymanie ciągłości funkcjonowania obiektu, zarządzanie personelem, w niektórych wypadkach również ciągłości dostaw.

Tomasz Goljaszewski

Ostatni rok wymusił weryfikację podejścia do spraw bezpieczeństwa we wszystkich wymienionych obszarach. Z punktu widzenia dostawcy technologii chciałbym się skupić na pierwszym obszarze, czyli utrzymaniu ciągłości działania obiektu infrastruktury krytycznej. Bezpieczeństwo w tym obszarze dotyczy zarówno systemów ochrony procesów, jak i typowych systemów zabezpieczenia obiektu przed nieuprawnionym wtargnięciem, wandalizmem czy aktami sabotażu.

Jeszcze kilka lat temu prawdopodobieństwo sabotażu lub wręcz ataku terrorystycznego na obiekt infrastruktury krytycznej było oceniane jako stosunkowo niskie. Sieć informatyczna takiego obiektu co do zasady była i jest zamknięta, czyli odizolowana od Internetu. Możliwość bezpośredniego włączenia i zalogowania się do sieci obiektu uznawano za niemożliwe lub mało prawdopodobne. Systemy zabezpieczeń były nastawione głównie na wykrywanie incydentów związanych z nieuprawnionym wtargnięciem osób potencjalnie mających na celu kradzież czy wandalizm. Ostatni rok wymusił zmianę podejścia do zagrożeń, na jakie mogą być narażone tego typu obiekty. Należy wziąć pod uwagę, że osoby lub grupy, które potencjalnie mogą stanowić zagrożenie, będą zdecydowanie lepiej przygotowane, a samo zakłócenie w funkcjonowaniu obiektu może nastąpić na różne sposoby i w tym samym czasie. Atak hakerski może być skuteczny nawet w zamkniętych sieciach informatycznych, jeżeli został poprzedzony działaniami wywiadowczymi. Należy też wziąć pod uwagę ryzyko, że może on być zrealizowany przez osobę będącą wewnątrz obiektu. Wtargnięcie na obiekt może zostać niezauważone, jeżeli sprawcy wykorzystywali zaawansowane narzędzia technologiczne. Atak z zewnątrz może się powieść nawet bez wtargnięcia do obiektu, ponieważ sprawcy wykorzystują do tego celu drony, które można łatwo kupić bez wzbudzania zainteresowania odpowiednich służb. Tak definiowane zagrożenia muszą doprowadzić do zmiany podejścia do problemów bezpieczeństwa. Oczywiście, wymusza to pewne zmiany w zakresie zarówno procedur, jak i technicznych narzędzi stosowanych w systemach zabezpieczeń.

Obiekty infrastruktury krytycznej mogą mieć różną specyfikę. W zależności od rodzaju obiektu nowe podejście powinno w większym stopniu uwzględniać dublowanie systemów bezpieczeństwa oraz wykorzystanie wielu nowych technologii, również tych, które wcześniej były wykorzystywane w mniejszym zakresie lub nie były wykorzystywane wcale. Systemy odpowiadające za dostęp osób do obiektu i monitorowanie poruszania się osób na terenie obiektu, oprócz klasycznej kontroli dostępu opartej na kartach zbliżeniowych, powinny zawierać dodatkowe elementy weryfikacji, np. możliwość identyfikacji twarzy w „siatce 3D" przy jednoczesnej identyfikacji odcisków palca. Taki rodzaj zabezpieczenia utrudni „legalne" wejście i przemieszczanie się wewnątrz obiektu osób nieuprawnionych, nawet jeżeli będą posiadać kartę zbliżeniową umożliwiającą dostęp.

Do ochrony procesów wewnątrz obiektu infrastruktury krytycznej stosowane są różnego rodzaju specjalistyczne czujniki, które są na bieżąco monitorowane. Warto się zastanowić, czy oprócz typowych czujników właściwych dla danej technologii nie należy wykorzystać informacji pochodzącej z innego źródła, gdyż wiele zagrożeń może być wykrywanych dodatkowo przy użyciu specjalnych kamer termowizyjnych. Wprowadzenie tego rodzaju dodatkowego zabezpieczenia może pomóc szybciej dostrzec i zareagować na zagrożenie lub zapewnić lepszą możliwość weryfikacji, czyli oceny sytuacji i podjęcia właściwej decyzji.

Zabezpieczenie obiektu infrastruktury krytycznej w zakresie ochrony obwodowej realizowane w standardowy sposób, czyli najczęściej przy użyciu kabla sensorycznego, różnego rodzaju barier mikrofalowych lub podczerwieni ze wsparciem systemu kamer wizyjnych, może okazać się niewystarczające. Istnieją pewne sposoby sforsowania tego typu zabezpieczeń. Odpowiednie działania poprzedzające, wiedza praktyczna czy dostęp do odpowiednich narzędzi technologicznych mogą pomóc sprawcy pokonać zabezpieczenia. Osoba czy grupa po sforsowaniu takiej „przeszkody" i wejściu na teren w sposób niezauważony ma dużą swobodę działania, a skutki mogą być trudne do przewidzenia.

Z tego powodu w zabezpieczeniach infrastruktury krytycznej standardowym rozwiązaniem powinny być kamery bispektralne, które oprócz sensora wizyjnego mają również sensor termowizyjny. Takie rozwiązanie daje lepsze możliwości obserwacji ogrodzenia z zewnątrz (w strefie podejścia), co pozwala ograniczyć możliwości niepożądanych działań na terenie przyległym do obiektu infrastruktury krytycznej i jednocześnie ograniczy ilość generowanych fałszywych detekcji z kamer. Dzięki temu pracownicy ochrony zachowują większą czujność i mogą podjąć odpowiednie działania w sytuacji alarmowania o rzeczywistym zagrożeniu.

Ciekawym rozwiązaniem, które również może zwiększyć skuteczność ochrony obiektu, jest radar bezpieczeństwa połączony z kamerą PTZ. Zastosowanie radaru powoduje, że intruz, nawet po pokonaniu zabezpieczeń w pasie ogrodzenia, nie będzie mieć dostępu do zasobów na terenie obiektu. Pokrycie terenu wewnątrz obiektu detekcją przy użyciu radaru lub radarów może również skutecznie wykrywać wtargnięcie na dość dużym obszarze, a połączone z nim kamery PTZ mogą bardzo precyzyjnie śledzić intruza. Warto wspomnieć, że ten rodzaj zabezpieczenia jest odporny na złe warunki pogodowe (np. opady deszczu) oraz fałszywe alarmy wynikające z aktywności małych zwierząt.

Nowym rodzajem zagrożenia jest możliwość użycia dronów. Zakładając, że służby państwa prawidłowo wypełniają swoje zadania, pozyskanie w Polsce lub przemycenie przez granicę drona wojskowego należy uznać za mało prawdopodobne. Odpowiednie służby dość szybko trafiłyby na trop osoby lub osób, które chciałyby tego dokonać. W okresie pokoju realne zagrożenie stwarzają więc przede wszystkim drony komercyjne. Zagrożenia tego typu należy traktować bardzo poważnie. Dron komercyjny, za pomocą którego można transportować niebezpieczne materiały, również może być w sposób świadomy wykorzystany do ataku na infrastrukturę krytyczną. Taki dron można dość łatwo nabyć, nie wzbudzając podejrzeń, oraz przysposobić do celów sabotażu czy ataku terrorystycznego. Nadlatujący dron może być zaobserwowany za pomocą kamery PTZ bispektralnej (z sensorem termowizyjnym), ponieważ termowizja może być dość skutecznym narzędziem do obserwacji obiektów latających nawet niedużych rozmiarów.

Należy pamiętać, że taki punkt kamerowy musi mieć dość duży kąt obserwacji powyżej linii horyzontu. Dlatego w tym celu warto stosować kamery PTZ jako systemy pozycjonowania, ponieważ tego typu urządzenia mogą obserwować przestrzeń do 45° powyżej linii horyzontu. Wspomniana kamera PTZ może zostać użyta do zaobserwowania drona w powietrzu, ale wykrycie go taką metodą jest bardzo trudne. Z tego powodu najważniejsze obiekty infrastruktury krytycznej powinny być wyposażone w specjalne narzędzia do detekcji i unieszkodliwiania dronów.

Takimi narzędziami mogą być detektory typowych dla dronów częstotliwości, które mogą objąć detekcją obszar kilku kilometrów kwadratowych. Do unieszkodliwiania dronów, oprócz ręcznych narzędzi typu *Jammer* UAV, można zastosować stacjonarne urządzenia typu *Defender,* które są w stanie stworzyć strefę bezpieczeństwa, w której dron zostanie pozbawiony sygnału sterowania i sygnału lokalizacji. Dron do użytku komercyjnego, który straci możliwość odbierania sygnałów lokalizacyjnych i sterowania, najczęściej ląduje w trybie awaryjnym, dzięki czemu łatwo go zneutralizować. ●

DS-K1T680DF-E1 Terminal Hikvision zawierający czytnik kart zbliżeniowych, funkcję identyfikacji twarzy oraz czytnik linii papilarnych

DS-2TD3017T-3/V - Kamera Hikvision termowizyjna (bispektralna) jak czujnik technologiczny

DS-2TD6567T-50H4LX/W
Kamera PTZ Hikvision termowizyjna (bispektralna) w wykonaniu EX do obiektów przetwarzających czy magazynujących paliwa czy gaz

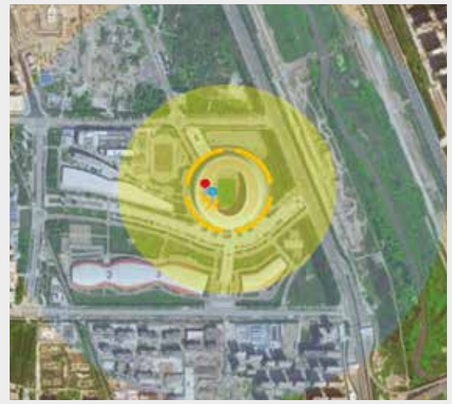
DS-2TD2667-15/PY
Kamera Hikvision termowizyjna (bispektralna) stacjonarna do ochrony obwodowej

DS-2TD4167-50/WY
DS-2TD6267-100C4L/WY Kamery PTZ Hikvision termowizyjne (bispektralne) do ochrony obwodowej (typ głowica obrotowa oraz typ system pozycjonowania)

DS-PRI120
Radar bezpieczeństwa Hikvision do linkowania z kamerami PTZ

Detektory częstotliwości sygnałów sterowania drona; zasięg do 3 km

Defender stacjonarny do blokowania sygnałów lokalizacyjnych i sterowania drona; zasięg 500 lub 1000 m



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

1200 obiektów
w jednym systemie

W celu zabezpieczenia infrastruktury zasilającej polską kolej PKP Energetyka uruchomiła Centrum Monitorowania Alarmów wyposażone w platformę integrującą PSIM *(Physical Security Information Management)*. Docelowo do 2024 r. CMA ma objąć całą Polskę, czyli prawie 1200 strategicznych obiektów, w tym także infrastruktury krytycznej. Projekt kosztował niemal 30 mln zł.

Z **Tomaszem Witosławskim**, dyrektorem Biura Bezpieczeństwa PKP Energetyka, rozmawiała Aleksandra Czapska.

System PSIM jest stosowany w wielu przedsiębiorstwach. Czy ten w obiekcie infrastruktury krytycznej różni się od monitorującego, np. zakład produkcyjny?

Kompleksowe oprogramowanie platformy integrującej PSIM dla obiektów infrastruktury krytycznej musi spełniać cechy funkcjonalne dotyczące gromadzenia i przetwarzania danych z wielu urządzeń, analizy i korelacji danych alarmowych. Musi również umożliwiać weryfikację zdarzeń, reakcję na zagrożenia powiązaną z automatycznym procesem generowania zgłoszeń przyjazdu grup interwencyjnych oraz mieć zaimplementowane moduły definiowania procedur i generowania raportów.

To wszystko jest potrzebne, aby jak najlepiej wykorzystać potencjał oprogramowania przy zminimalizowaniu ryzyka popełnienia błędu ludzkiego, na który przy obiektach IK nie możemy sobie pozwolić.

Podsumowując, należy maksymalnie wykorzystać wszystkie zalety i możliwości oprogramowania oraz ograniczyć do minimum ryzyko popełnienia błędu przez operatora obsługującego system.

Jakie korzyści wiążą się ze stosowaniem tej platformy?

System umożliwia stały dostęp do informacji z systemów podrzędnych zarządzanych przez PSIM, w tym SSWiN, KD i CCTV. Operator jest informowany o każdym alarmie niezależnie, a korelacja danych alarmowych, tj. współzależność zdarzeń w danym czasie, wyznacza lub podnosi ich priorytet. System w oparciu o zebrane dane cały czas „uczy się" analizować podobne zdarzenia i w efekcie dostarcza operatorom systemu niezbędne informacje do poprawnej ewaluacji zdarzeń. Działanie zgodnie z procedurami postępowania minimalizuje błędną analizę zdarzeń przez operatorów. Operator ma wpływ na zarządzanie zdarzeniem.

PSIM zapewnił nam jednorodną platformę do integracji różnorodnych, niezależnych systemów bezpieczeństwa i innych urządzeń, pozwalając na zarządzanie całą infrastrukturą poprzez jeden, przejrzysty interfejs komunikacyjny z uwzględnieniem naszych procedur postępowania. Monitoring pociągów sieciowych stanowi jedną z integracji obsługiwanych przez PSIM.

W PKP Energetyka głównym obszarem obsługi Zintegrowanego Systemu Monitorowania, opartym na PSIM, są bezobsługowe obiekty energetyczne. System PSIM nie jest powiązany z systemami zarządzającymi ruchem sieci. Są one autonomiczne.

Czy system działa sieciowo? Jeśli tak, w jaki sposób jest usuwany problem „białych plam" – wiadomo, że kolej dojeżdża do niemal każdego zakątka kraju.

Do komunikacji sieciowej z systemami podrzędnymi PSIM wykorzystuje zabezpieczone łącza VPN i APN. Lokalizacja pociągów sieciowych w zintegrowanej funkcjonalności z PSIM oparta na pozycjonowaniu sygnałem GSM generuje miejsca bez zasięgu i jest to problem, nad którym obecnie pracujemy. ●

brivo

ZINTEGROWANA PLATFORMA BRIVO DO KONTROLI DOSTĘPU

ŚWIATOWY LIDER I PIONIER W ZAKRESIE KONTROLI DOSTĘPU I PLATFORM OCHRONY OPARTYCH W CHMURZE

Kontrola dostępu
Zautomatyzuj kontrolę dostępu budynku oraz raportowanie

Monitoring wizyjny
Wyświetlaj obrazy w czasie rzeczywistym i przeglądaj zapisy

Zdalne zarządzanie
Zarządzaj zabezpieczeniami z dowolnego urządzenia mobilnego

Zarządzanie użytkownikami
Nadawaj uprawnienia użytkownikom w systemie

Kontrola odwiedzających
Bezpieczne warunki dla odwiedzających i pracowników

Analiza danych
Przetwarzaj informacje na temat bezpieczeństwa fizycznego

Smart-i Sp. z o.o.

www.smart-i.pl

głos branży

Kiedy kończyliśmy pracę nad tym wydaniem, w mediach pojawiła się informacja, że funkcjonariusze ABW zatrzymali grupę cudzoziemców podejrzanych o szpiegostwo. Wiele wskazuje, że zatrzymane osoby monitorowały linie kolejowe, głównie odcinki tras w województwie podkarpackim, w okolicach lotniska w Jasionce. Jest ono głównym punktem przerzutowym zachodniej broni i amunicji do Ukrainy. Tematem tego wydania jest infrastruktura krytyczna i jej ochrona. Jak widać bardzo na czasie. Głos oddajemy ekspertom.

Janusz Syrówka
EON

Lekcja z wojny w Ukrainie

Minął rok od wybuchu wojny na Ukrainie i jest to czas, kiedy zaczynają się pojawiać głębsze przemyślenia dotyczące bezpieczeństwa, zwłaszcza w odniesieniu do obszarów krytycznych. Nie są to nowe idee dla osób zajmujących się branżą szeroko rozumianego bezpieczeństwa. Nowością jest to, że idee te zaczynają przebijać się do osób zajmujących najwyższe stanowiska w firmach.

Zagrożenie wcześniej teoretycznie w ciągu kilku miesięcy się zmaterializowało. Nie da się nie odczuć skutków inwazji. Obrazy zniszczeń wylewają się z serwisów informacyjnych i mediów. Poza warstwą emocji związanych z ludzkimi tragediami widoczne są także nie mniej szokujące obrazki przedstawiające skalę strat czysto technicznych – zniszczone budynki, drogi, mosty i oczywiście infrastruktura krytyczna. Dojmujący jest heroizm służb walczących o utrzymanie dostępu do usług kluczowych, takich jak energia elektryczna, woda, ciepło i tym podobne. To, co widzimy za wschodnią granicą, to bardzo cenna lekcja dla nas. Nieskorzystanie z tych nauk oznacza brak szacunku dla wszystkich, którzy tragedię wojny odczuli na własnej skórze. Dążenie do poprawy bezpieczeństwa niesie także zagrożenia i ryzyko pójścia w złym kierunku.

Chciałbym podzielić się moimi refleksjami na temat ślepych uliczek, które czyhają na wszystkich. Pierwsza uliczka, a właściwie szeroka aleja, to cyberbezpieczeństwo. Jak jest wojna, to są ataki „cyber", z których słynie Rosja. To wszystko prawda, ale nie ma sensu porcjowanie bezpieczeństwa na kawałki i przyklejanie do tych kawałków etykietek. Albo coś jest dostatecznie bezpieczne, albo nie jest. Tutaj nie ma nic pomiędzy. Bezpieczeństwo musi być spójne i kompletne. Skupianie się na cyberochronie kosztem innych dziedzin jest błędem. Największym wyzwaniem nowych czasów jest zbudowanie systemu bezpieczeństwa pozbawionego luk. Musi on mieć możliwość dynamicznego dostosowywania się do zmian w otaczającym środowisku. Tworzenie silosów i linii demarkacyjnych to działanie wbrew dynamice świata, która jest z natury złożona. Złożoność objawia się poprzez wzajemne oddziaływanie na siebie wielu czynników zmieniających się dynamicznie w czasie.

Druga ślepa uliczka to ciągłość działania. Chodzi o to, że uliczka ta prowadzi w dobrym kierunku, ale powinniśmy udrożnić jej ślepy koniec. Zwykle definiuje go granica naszej organizacji. Tymczasem ciągłość działania musi wykraczać bardzo daleko poza granice organizacyjne. Bez uważnego przyjrzenia się dostawcom, podwykonawcom i innym istotnym partnerom – ze szczególnym uwzględnieniem dostawców rozwiązań IT i OT – nasze plany ciągłości działania pozostaną bezwartościowe.

Trzecią ślepą uliczką jest skupienie się wyłącznie na rentowności. Owszem, każda inicjatywa biznesowa musi być rentowna, ale oprócz rentowności musi być także bezpieczna na wielu płaszczyznach. Chodzi o biznesową odporność, ochronę informacji, zabezpieczenie łańcucha dostaw.

Jakub Kozak
GENETEC

Wielowarstwowa i wszechstronna ochrona obiektów IK

W przypadku ochrony obiektów infrastruktury krytycznej znaczenia nabiera wielowarstwowa i wszechstronna struktura systemu zabezpieczeń. Ochrona tych obiektów musi uwzględniać dane z wielu czujników i dostarczać zbudowanego na ich podstawie aktualnego obrazu stanu zabezpieczenia i poziomu zagrożenia.

Obecnie widzimy wyraźny trend zmierzający w kierunku integracji czy nawet unifikacji systemów zabezpieczeń, które wcześniej pracowały niezależnie. Co ważne, kiedy nie widać wyraźnych korzyści z łączenia niezależnych systemów zabezpieczeń, systemy te słusznie pozostają niezależne. Tak powinno się dziać wtedy, kiedy odizolowywanie systemów sprzyja redundancji, a nieco bardziej rozbudowana infrastruktura jest do zaakceptowania zarówno kosztowo, jak i operacyjnie. W pozostałych przypadkach unifikacja będzie lepszym rozwiązaniem.

W dzisiejszych czasach nie sposób nie wspomnieć o ochronie perymetrycznej. System zabezpieczenia obwodowego ma na celu dostarczenie spójnego i łatwego w analizie oglądu obszaru i obwodu. W tym celu musi pozwalać na wyeliminowanie nadmiernej liczby fałszywych alarmów bez utraty informacji o faktycznym zagrożeniu. Nowoczesne rozwiązania oparte na platformie zunifikowanej dają taką możliwość.

Z satysfakcją zauważamy, że klienci znacznie częściej niż jeszcze kilka lat temu jako jeden z podstawowych wymogów stawianych systemom ochrony infrastruktury krytycznej wskazują wysoki poziom cyberbezpieczeństwa. Słusznie, gdyż łańcuch jest tak silny jak jego najsłabsze ogniowo, a system bezpieczeństwa wrażliwy na ataki cybernetyczne jest bardzo słabym łańcuchem.

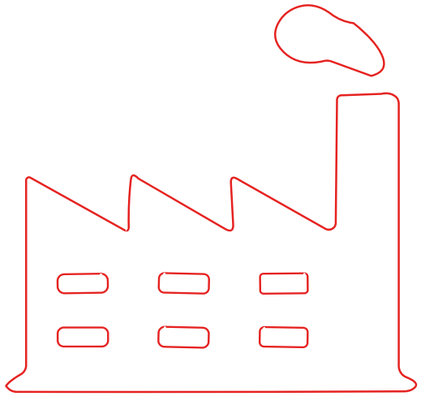
Grzegorz Kosik
NEDAP SECURITY MANAGEMENT

Dyrektywa NIS2 i jej wpływ na systemy kontroli dostępu

W obecnej sytuacji geopolitycznej większość specjalistów zajmujących się bezpieczeństwem fizycznym przed wyborem potencjalnych dostawców systemów kontroli dostępu, SSWiN czy CCTV kładzie duży nacisk na analizę zarówno urządzeń, jak i firmy. Coraz częściej brane są pod uwagę nie tylko funkcjonalności i parametry techniczne rozwiązania, ale także stabilność firmy, kraj pochodzenia i miejsce produkcji.

Kolejnym obszarem, który zaczął odgrywać bardzo dużą rolę, jest odmieniane przez wszystkie przypadki cyberbezpieczeństwo. Do niedawna wydawało się, iż wszystko związane z bezpieczeństwem sieci jest domeną departamentów IT. Dziś jednak gros komponentów systemów zabezpieczeń, tj. kamery, kontrolery drzwiowe czy centrale alarmowe, działa w sieci LAN, co oznacza, że są podatne na te same zagrożenia co infrastruktura IT. Niestety wspomniane elementy bardzo często nie są chronione odpowiednimi procedurami bezpieczeństwa, zaczynając od szyfrowania komunikacji na każdym etapie między wszystkimi urządzeniami, dwuskładnikowego logowania do aplikacji czy zastosowania znanych od lat protokołów, jakim jest chociażby 802.1x.

Z pomocą przychodzą dyrektywy UE, które standaryzują i regulują obowiązki w szeroko pojętym obszarze IT, ale nie tylko. Przykładem jest Dyrektywa NIS (*Network and Information System*) pierwotnie przedstawiona w 2016 r., a następnie przyjęta w styczniu tego roku jej aktualizacja NIS2. Wspomniana aktualizacja została rozszerzona o nowe podmioty, które podzielono na dwie kategorie: podmioty kluczowe (energetyka, transport, bankowość, opieka zdrowotna, administracja państwowa)



oraz podmioty ważne (produkcja, ze szczególnym uwzględnieniem chemikaliów i żywności, usługi pocztowe i kurierskie czy gospodarowanie odpadami).

NIS2 jasno wskazuje obowiązki związane z analizą ryzyka, obsługą incydentów, ciągłością działania systemów, ale także wykorzystanie kryptografii i mechanizmów szyfrowania.

Co to oznacza dla systemu kontroli dostępu? Należy używać przede wszystkim szyfrowanych kart, np. MIFARE DESFire. Z naszych doświadczeń wynika, że na rynku polskim jest jeszcze sporo starych rozwiązań z kartami pracującymi w technologii 125 kHz, które łatwo można skopiować. Oznacza to, iż podmioty ważne i kluczowe będą musiały migrować do technologii uznanych za bezpieczne. Jest to również jednoznaczne z zakazem stosowania tych technologii (125 kHz) w nowych postępowaniach przetargowych.

Kolejnym obszarem jest ciągle popularny i stosowany interfejs Wiegand do komunikacji między czytnikiem a kontrolerem drzwiowym, który jest nieszyfrowany i można go podsłuchać. Tutaj podejście jest analogiczne do przypadku kart. Mówiąc o NIS2, należy pamiętać, że sklasyfikowane przedsiębiorstwa mają czas na wdrożenie wymienionych regulacji do października 2024 r. Warto również wspomnieć, że regulacje NIS2 przewidują znaczące kary dla podmiotów nierealizujących zapisów dyrektywy. Kara może wynieść 10 mln euro lub 2% całkowitego rocznego światowego obrotu przedsiębiorstwa w przypadku podmiotów kluczowych oraz 7 mln euro lub 1,4% całkowitego rocznego obrotu dla podmiotów ważnych.

Piotr Rogalewski
HIKVISION

Cyberbezpieczeństwo – dobór odpowiednich rozwiązań

Sytuacja geopolityczna sprawia, że bezpieczeństwo wszelkiego rodzaju odmieniamy przez wszystkie przypadki. Oczywiście dotyczy to także systemów zabezpieczeń technicznych, szczególnie chroniących obiekty infrastruktury krytycznej.

Wbrew pozorom w tej dziedzinie jest nadal wiele do zrobienia. Wynika to po części z faktu, że systemy zabezpieczeń technicznych bardzo często traktuje się jako „z automatu" bezpieczne. Nic bardziej mylnego i nietrudno o poważny błąd w ocenie.

Jednym z takich błędów jest przyjęcie założenie, że zamknięta architektura sieciowa, bez fizycznego i logicznego dostępu z zewnątrz, jest bezpieczna. A jeśli niebezpieczeństwo czai się wewnątrz obiektu? Pomijając już nawet „klasyczny" sabotaż przemysłowy, ryzykiem dla niedokładnie zabezpieczonego okablowania może być np. niezadowolony pracownik, który w akcie zemsty postanowił „odegrać się" na pracodawcy, uszkadzając np. kable.

Jeśli do tego jest to pracownik związany z utrzymaniem sieci – tym gorzej, gdyż poważne szkody może poczynić także w warstwie logicznej, gdzie bez odpowiednich narzędzi znacznie trudniej to wykryć. Nawet fizyczne odizolowanie (np. komputer z danymi krytycznymi niepodłączony do sieci) nie daje pełnej gwarancji bezpieczeństwa. Narzędzia wykorzystujące przechwytywanie ulotu elektromagnetycznego (np. technika AirHopper) są dziś niemal powszechnie dostępne i doskonale opisane.

Zarządzanie aktualizacjami oprogramowania to kolejny czuły punkt. Brak aktualizacji wywołuje problemy wynikające ze stosowania starych wersji komponentów użytych przez twórców oprogramowania, np. rejestratora czy kamery IP. Z kolei słaba kontrola uprawnień do wykonywania aktualizacji i/lub brak szyfrowania oraz kontroli zawartości plików z taką aktualizacją to otwarcie drogi do uruchomienia na urządzeniu złośliwego oprogramowania lub nawet sparaliżowania systemu.

Jako fundament doboru właściwego zakresu środków ochrony przed przykładowymi zagrożeniami użytkownik systemu może zastosować starą, dobrą i sprawdzoną wielokrotnie zasadę *zero trust* (nie ufaj nikomu i niczemu). Jeśli do tego producent sprzętu doda od siebie filozofię *secure by design* (architektura produktu bezpieczna „od urodzenia") oraz *secure by default* (bezpieczna konfiguracja domyślna), to ryzyko wystąpienia poważnego incydentu nawet w złożonym środowisku znacznie się zmniejsza.

Jarosław Sapko
AXIS COMMUNICATIONS

Kompleksowy system ochrony

Elementem kluczowym w ochronie obiektów infrastruktury krytycznej jest zabezpieczenie obiektu, by uniemożliwić wtargnięcie osób nieupoważnionych. Z tego względu znaczenie ma ich ochrona perymetryczna. Biorąc pod uwagę, iż obiekty infrastruktury krytycznej bardzo często są dość rozległe, zabezpieczenie ich granic jest zadaniem dość skomplikowanym i wymaga znacznych nakładów finansowych.

Niezależnie od stosowanej technologii detekcji służby zabezpieczające obiekty IK muszą mieć pewność, że dany alarm nie jest fałszywy. To oznacza, że przynajmniej jedno z zastosowanych rozwiązań powinno pozwalać wizualne potwierdzić, czy incydent rzeczywiście zagraża bezpieczeństwu.

Z tego względu coraz częściej do ochrony perymetrycznej stosuje się rozwiązania integrujące różne techniki detekcji. Mogą one łączyć systemy detekcji z systemem dozoru wizyjnego lub polegać na wzbogaceniu kamer o dodatkowe detektory bądź polegać na implementacji dodatkowych protokołów komunikacyjnych umożliwiających podłączenie dodatkowych sensorów.

Przykładami takich urządzeń są kamery z wbudowanym radarem lub kamery bispektralne o znacznie większym zakresie detekcji kamery, dzięki czemu operator może potwierdzić, czy dane zagrożenie ma miejsce. Kompleksowy system ochrony często łączy się z elementami kontroli dostępu czy audio, dzięki czemu dostęp uzyskują tylko uprawnione osoby i pojazdy, a intruzi są odstraszani za pomocą zdalnych komunikatów.

Marcin Walczuk
BCS

Technologia w ochronie perymetrycznej

Funkcje analityczne w oprogramowaniu urządzeń CCTV można podzielić na kilka grup w zależności od ich zastosowania czy rodzaju. Od grupy funkcji najbardziej zaawansowanych, do których należą rozpoznawanie tablic rejestracyjnych, gromadzenie danych o obiektach widocznych na obrazie, detekcja twarzy połączona z identyfikacją na podstawie zapisanych na urządzeniach baz danych, analiza typu zachowań (bójka czy zasłabnięcie), po wykorzystywane w ochronie perymetrycznej. Podstawową zaletą tych ostatnich jest możliwość bardzo dokładnego określenia warunków, od których zależy wysłanie powiadomienia o zdarzeniu. Zastosowanie kryteriów generowania alarmu, takich jak typ czy wielkość obiektu, określenie kierunku ruchu i miejsca, w którym taki ruch jest zabroniony, w znacznym stopniu przyczynia się do zmniejszenia liczby fałszywych alarmów. Ma to szczególne znaczenie w miejscach, gdzie obecność ochrony fizycznej została zredukowana do minimum lub w ogóle jej nie ma, a zabezpieczenie obiektu opiera się jedynie na skutecznym działaniu funkcji ochrony obwodowej.

Zwiększenie skuteczności ochrony perymetrycznej można również osiągnąć, stosując synergię różnych technologii, np. przez połączenie w jednej kamerze przetwornika światła widzialnego z przetwornikiem termowizyjnym. To rozwiązanie pozwala na wykrycie intruza niezależnie od warunków oświetleniowych czy atmosferycznych i wizualne potwierdzanie sytuacji alarmowej.

Artur Nowakowski
LINC POLSKA

Holistyczne podejście do zabezpieczenia IK

Ochrona obwodowa to pierwszy stopień zabezpieczenia obiektów infrastruktury krytycznej. Takie zabezpieczenie może zostać zrealizowane za pomocą systemów wizyjnych z kamerami światła widzialnego lub termowizyjnymi wspieranymi analityką AI. Dobrym rozwiązaniem są kamery bispektralne, w których detekcja bazuje na termowizji. Dzięki temu umożliwiają one detekcję na większym dystansie i zwiększoną skuteczność w trudnych warunkach.

Innym rozwiązaniem jest wykorzystanie sensorycznego kabla światłowodowego umieszczonego na ogrodzeniu lub zakopanego, który sprawdzi się w zabezpieczeniu większości obiektów. Szczególnie polecany jest przy ogrodzeniu o nieregularnej linii lub np. do ochrony infrastruktury podziemnej (kabli transmisyjnych światłowodowych), która w wielu wypadkach też należy do IK.

Jednakże ograniczenie ochrony tylko do strefy obwodowej sprawia, że informacja o intruzie dociera do ochrony w momencie, kiedy wchodzi on w strefę, a znika po jej opuszczeniu. Dlatego równie ważne jest nadzorowanie możliwie dużej strefy na zewnętrz obiektu. Z tym zadaniem bardzo dobrze radzą sobie systemy radarowe automatycznie sterujące kamerami PTZ. Można zastosować np. małe radary o zasięgu do 150 m, a także większe jednostki, które umożliwiają ciągłą obserwację na odległość kilkuset metrów.

Coraz ważniejszym aspektem ochrony IK staje się wykrywanie dronów, które mogą być stosowane do rozpoznania terenu przed włamaniem bądź stanowić bezpośrednie zagrożenie dla obiektu

→

i bezpieczeństwa osób. W tym przypadku rozwiązaniem są radary 3D, które wykrywają małe drony z jednoczesnym określeniem ich pozycji oraz pułapu lotu. To bardzo ważny aspekt w przypadku ochrony przestrzeni powietrznej przed statkami bezzałogowymi.

Aby wielowarstwowość była skuteczna, zarządzanie musi odbywać się za pomocą jednej platformy, która ułatwi pracę służbom ochrony, zapewni większą świadomość sytuacyjną bez konieczności ciągłej obserwacji obrazu pochodzącego z wielu kamer. Podsumowując, na ochronę obiektu trzeba patrzeć całościowo, dobierając różne technologie, które wzajemnie się uzupełniają i są ze sobą kompatybilne.

Krzysztof Kunecki
SCHRACK SECONET

Zintegrowane zarządzanie bezpieczeństwem pożarowym

Dla zapewnienia najwyższego poziomu bezpieczeństwa pożarowego w obiektach coraz częściej są stosowane systemy integrujące urządzenia przeciwpożarowe (SIUP). Służą one do integracji, sterowania i zarządzania systemami ochrony przeciwpożarowej oraz współdziałania z innymi systemami w zakresie bezpieczeństwa pożarowego. Zadaniem podstawowym SIUP jest aktywne wsparcie służb ochrony obiektu w przypadku wystąpienia alarmu pożarowego lub innego zdarzenia kryzysowego.

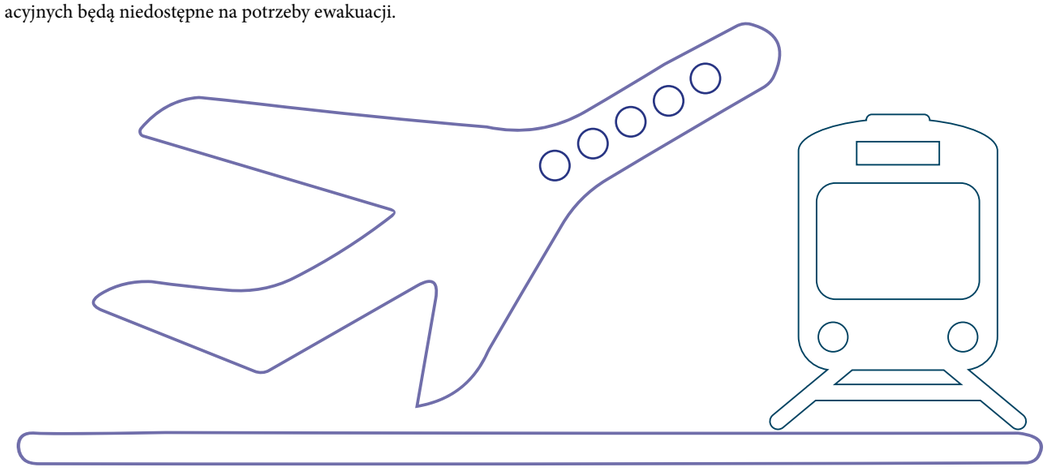
W przypadku pożaru oznacza to przede wszystkim zarządzanie ewakuacją poprzez wyświetlanie instrukcji i procedur postępowania dla służb ochrony oraz informowanie o uruchomieniu urządzeń zgodnie z założeniami scenariusza pożarowego. Co najważniejsze, kierujący działaniami ratowniczymi może z poziomu SIUP sterować urządzeniami uruchomionymi w trybie automatycznym w sytuacji, kiedy należy pokierować ewakuacją w inny sposób, np. gdy w wyniku rozwoju pożaru niektóre z dróg ewakuacyjnych będą niedostępne na potrzeby ewakuacji.

Wdrożenie SIUP w obiekcie zapewnia duże wsparcie dla służb ochrony w zakresie eksploatacji instalacji bezpieczeństwa pożarowego. SIUP może ściśle współpracować z integrowanymi systemami, pozwalając na obsługę urządzeń tak, jak z poziomu centrali danego systemu, oraz informowanie w sposób szczegółowy o stanach pracy instalacji. SIUP może prezentować szczegółowe informacje, np. wartości analogowe z czujek pożarowych dotyczące aktualnej temperatury, co pozwala na wcześniejsze powiadomienie nie tylko o zagrożeniu pożarowym. Może także powiadamiać o niebezpiecznym przekroczeniu wartości i tym samym o nieprawidłowej pracy, np. urządzeń wentylacji i klimatyzacji w serwerowniach.

Za pomocą SIUP można też obserwować wybrane urządzenia lub strefy pod kątem parametrów pracy, aby zidentyfikować np. źródło powstawania alarmów fałszywych lub nieprawidłowej pracy urządzeń. SIUP dzięki wykorzystaniu jednostek obliczeniowych o dużej mocy umożliwia analizowanie bieżącej pracy urządzeń i zdarzeń historycznych danego obiektu. Analiza zdarzeń pozwala na zidentyfikowanie miejsc wymagających szczególnej uwagi związanych z pojawiającym się alarmem fałszywym czy uszkodzeniem, co jest znacznie utrudnione, gdy analizuje się to w sposób konwencjonalny na bazie wydruków, rejestrów indywidualnych instalacji czy zapisów w papierowej książce eksploatacji.

W SIUP dostęp do danych i ich analiza mogą być wykonane od ręki z możliwością wygenerowania odpowiedniego raportu do dalszej weryfikacji przez służby ochrony czy serwis. Dla obsługi ważna jest pełna informacja o integrowanych instalacjach. Dlatego ważną funkcją SIUP jest możliwość dostępu do dokumentacji technicznej powiązanej z elementami instalacji, aby móc zapoznać się z dokładną charakterystyką urządzenia i instrukcjami w zakresie obsługi i eksploatacji. Ponadto SIUP może realizować funkcję elektronicznej książki eksploatacji poprzez opisywanie zdarzeń i stanów pracy integrowanych systemów, co jest dużym ułatwieniem w przypadku zarządzania całym cyklem życia danego projektu.

System integrujący urządzenia przeciwpożarowe umożliwia znaczne podniesienie poziomu bezpieczeństwa pożarowego obiektu dzięki aktywnemu wsparciu służb ochrony podczas stanów zagrożenia oraz istotnie ułatwia codzienną obsługę i eksploatację zintegrowanych instalacji bezpieczeństwa pożarowego. ●



roger
Intelligence for Building

VISO SMS

Platforma do zarządzania systemami bezpieczeństwa w obiekcie

- Wizualizacja i monitorowanie systemów bezpieczeństwa
- Integracja z systemami Bosch, Siemens, Honeywell, Satel, Milestone, Hikvision, Dahua i innymi
- Realizacja scenariuszy bezpieczeństwa
- Ewidencja napraw i konserwacji systemów w obiekcie
- Praca wielostanowiskowa, rejestr działań operatorów

Najlepsza polityka: zero zaufania

Liczba różnego rodzaju cyberataków z roku na rok rośnie. To konsekwencja szybko postępującej digitalizacji naszego życia i rozrastającego się Internetu rzeczy. Świat realny coraz bardziej przenika się z wirtualnym, a skutkiem tego jest większa podatność na wirusy. Jak się przed nimi bronić? Przedstawiamy najlepsze praktyki dotyczące cyberbezpieczeństwa.

Monika Mamakis, a&s Polska

Czy istnieje Święty Graal adminów, który pozwala im spać spokojnie? A może wystarczy wdrożyć jedno, ale doskonałe rozwiązanie? Na pytanie o najlepsze praktyki dotyczące ochrony firmowej infrastruktury IT i zgromadzonych w niej danych odpowiadają czterej specjaliści do spraw bezpieczeństwa pracujący na zlecenie firm różnej wielkości.

Każdy z naszych rozmówców pragnie zachować anonimowość. Jeden z nich mówi wprost: „Im o nas mniej wiedzą *(oni, czyli hakerzy – przyp. red.),* tym lepiej". Są zgodni też w dwóch innych kwestiach. Po pierwsze, każda firma, która chce zminimalizować ryzyko utraty danych, musi wdrożyć zestaw dobrych praktyk dotyczących zarówno sprzętów, jak i warstwy programistycznej infrastruktury IT. Po drugie, najczęstszym źródłem problemów jest... człowiek – jego błąd czy świadome działanie. To ludzie są najsłabszym ogniwem, jeśli chodzi o zachowanie cyberbezpieczeństwa. Padło nawet określenie „użyszkodnik" w stosunku do użytkownika. Przyznano też, że „gdyby adminom na to pozwolić, zabraliby użyszkodnikom wszystkie uprawnienia". Niestety, wówczas wrócilibyśmy w firmach do czasów kołonotatników, maszyn do pisania i liczydeł.

Człowiek – najsłabsze ogniwo

O tym, że za firmowymi cyberproblemami najczęściej stoją ludzie, napisano w ostatnim raporcie *IBM Security The Cost of a Data Breach Report* przygotowanym we współpracy z Ponemon Institute. Jego autorzy przeanalizowali m.in. dane dotyczące najpopularniejszych wektorów ataków i związany z nimi koszt naruszeń. W roku 2022 najczęstsze przypadki naruszeń dotyczyły: nie dość dobrze strzeżonych danych uwierzytelniających – 19%, phishingu – 16%, niewłaściwej konfiguracji chmury – 15% oraz luki w oprogramowaniu stron trzecich – 13%. Tymczasem błąd systemu spowodował jedynie niecałe 7% naruszeń. Autorzy raportu *Verizon 2022 Data Breach Investigations Report* podają, że 82% incydentów związanych z utratą lub wyciekiem danych wynikało z powodu działania lub zaniechania użytkowników. Podobnego zdania jest Iwona Prószyńska z CERT Polska, specjalistka ds. komunikacji, która przyznaje, że doświadczenia CERT są zbieżne z tym, co podają autorzy wspomnianych wcześniej raportów i podkreśla: „Najważniejsza jest edukacja użytkowników" (więcej w wywiadzie "Edukacja", na końcu artykułu).

Tylko edukowanie użytkowników w zakresie zagrożeń i sposobów ataków, polegających często na manipulacjach socjotechnicznych, w połączeniu z typowymi narzędziami cyberochrony, daje nadzieję na panowanie nad bezpieczeństwem firmowego IT. Słowo

→

„nadzieja" zostało użyte nie bez powodu. Nic nie zapewnia stuprocentowej ochrony, ale zawsze można ograniczyć ryzyko i zadbać o zminimalizowanie ewentualnych szkód.

Zero trust – nie ufaj nikomu

Pytani przez nas eksperci przyznają, że stosują się przede wszystkim do najnowszego paradygmatu bezpieczeństwa, jakim jest *zero trust* – nie ufaj nikomu i niczemu, przede wszystkim nie ufaj użytkownikom.

Polityka *zero trust* to strategia zabezpieczeń, wg której każdy użytkownik, urządzenie, aplikacja oraz adres IP mogą stanowić potencjalne zagrożenie. Z tego powodu polityka *zero trust* zakłada, iż należy stosować kontrolę dostępu, uwierzytelnianie i autoryzację na każdym poziomie systemu, a nie polegać na założeniu, że zaufanie można przypisać na podstawie lokalizacji użytkownika, źródła pliku lub adresu IP.

W praktyce oznacza to, że w ramach polityki *zero trust* każdy użytkownik, urządzenie lub aplikacja musi przejść przez proces uwierzytelniania, autoryzacji i weryfikacji, zanim uzyska dostęp do zasobów systemu. W przypadku, gdy te warunki nie zostaną spełnione, dostęp jest blokowany lub ograniczany.

> *» Polityka zero trust to strategia zabezpieczeń, wg której każdy użytkownik, urządzenie, aplikacja oraz adres IP mogą stanowić potencjalne zagrożenie. «*

Polityka *zero trust* wykracza poza tradycyjne podejścia do bezpieczeństwa opierające się na założeniu, że zaufane urządzenia lub sieci wewnętrzne nie stanowią zagrożenia. W erze, gdy ataki cybernetyczne stają się coraz bardziej zaawansowane i nieprzewidywalne, *zero trust* staje się jednym z najskuteczniejszych sposobów ochrony systemów i danych przed cyberzagrożeniami.

Dobre praktyki funkcjonujące w ramach polityki *zero trust* polegają zatem na wprowadzeniu:

1. Autentykacji każdej osoby, urządzenia i aplikacji, które chcą uzyskać dostęp do sieci, niezależnie od miejsca, z którego się łączą.
2. Uwierzytelnianiu każdej akcji, jaką podejmuje dana osoba, urządzenie lub aplikacja obecna w firmowej sieci.
3. Nadaniu odpowiednich uprawnień każdej osobie, urządzeniu i aplikacji w zależności od roli, którą odgrywają.
4. Ciągłej weryfikacji i oceny poziomu ryzyka dla każdego użytkownika, urządzenia i aplikacji w sieci, a następnie dostosowywaniu odpowiednich zabezpieczeń.
5. Monitorowaniu aktywności w sieci, aby wykryć nieprawidłowości i zagrożenia oraz szybko na nie reagować.
6. Izolowaniu lub ograniczaniu dostępu do zasobów sieciowych tylko do tych użytkowników, aplikacji i adresów, które faktycznie potrzebują do nich dostępu.
7. Szyfrowaniu komunikacji między urządzeniami i aplikacjami w sieci, aby uniemożliwić przechwytywanie i odczytywanie danych.
8. Korzystaniu z narzędzi do wykrywania i zapobiegania zagrożeniom, takich jak złośliwe oprogramowanie i ataki typu phishing.

Zero trust jest coraz bardziej popularnym podejściem do cyberbezpieczeństwa, promowanym m.in. przez dużych dostawców usług chmurowych, takich jak Microsoft czy AWS, ponieważ przeciwdziała zagrożeniom związanym z rosnącą liczbą połączeń między różnymi urządzeniami i sieciami. Ten model bezpieczeństwa zapewnia dostęp do prywatnych aplikacji z najniższymi uprawnieniami w oparciu na kontroli kontekstowej (użytkownik, urządzenie, aplikacje itp.). Aby to umożliwić, wiele zespołów IT wdraża nowoczesne technologie bazujące na chmurze, które mogą zastąpić tradycyjną infrastrukturę, taką jak VPN i strefy DMZ (*Demilitarized zone*, strefa zdemilitaryzowana bądź ograniczonego zaufania – to wydzielany na zaporze sieciowej obszar sieci komputerowej nienależący ani do sieci wewnętrznej, ani do sieci zewnętrznej).

Organizacja Cybersecurity Insiders opracowała *Zero Trust Adoption Report 2019*, według którego *zero trust* ułatwia firmom zachowanie bezpieczeństwa podczas przenoszenia aplikacji do chmury publicznej i sprawdza się szczególnie w tych firmach, które przeszły na pracę zdalną lub hybrydową. Według autorów raportu 78% zespołów ds. bezpieczeństwa IT zamierza w przyszłości korzystać z dostępu do sieci o zerowym zaufaniu, 19% aktywnie wdraża politykę zero trust, a 15% już ją stosuje. Jednocześnie około połowy zespołów zajmujących się bezpieczeństwem IT w przedsiębiorstwach (47%) nie ma pewności, czy ich obecna technologia zabezpieczeń jest w stanie zapewnić zerowe zaufanie. Jednocześnie najwyższym priorytetem bezpieczeństwa dostępu do aplikacji jest uprzywilejowane zarządzanie kontami użytkowników oraz uwierzytelnianie wieloskładnikowe (68%). Kolejne miejsca zajmują wykrywanie i reagowanie na nietypowe działania (61%) oraz zabezpieczanie dostępu z osobistych, niezarządzanych urządzeń (57%).

Reguły są znane

Niezależnie od tego, z jakiej wielkości firmą mamy do czynienia, reguły dotyczące skutecznej cyberochrony są podobne. Poza polityką *zero trust* nasi rozmówcy polecają stosowanie poniższych dobrych praktyk:

Firewall – to nie nowość, to solidna tradycja

Zastosowanie ochrony firewall dla sieci firmowej jest najlepszym sposobem zapobiegania cyberatakom. Zapora uniemożliwia nieautoryzowanym użytkownikom dostęp do stron internetowych, poczty elektronicznej i innych źródeł informacji, do których można uzyskać dostęp za pośrednictwem sieci. Ważne jest również, aby uzyskać oprogramowanie firewalla dla pracownika, który pracuje z firmową stroną internetową.

Aktualizacja oprogramowania bez odkładania na później

Oprogramowanie antywirusowe, serwer WWW i system operacyjny muszą być regularnie aktualizowane do najnowszych wersji. Konieczne jest instalowanie zaktualizowanego oprogramowania zabezpieczającego na wszystkich urządzeniach i w sieci, aby pomóc w ochronie przed najnowszymi cyberzagrożeniami. Niezbędne jest też aktualizowanie firmware'u sprzętu używanego w firmie.

Hasło – silne, czyli bardzo długie

Ważne, aby stosowane hasła były unikatowe, złożone i bardzo długie. Organizacje takie jak CERT zachęcają jednak do tego, by osoby odpowiedzialne za bezpieczeństwo IT odchodziły od wymuszania na użytkownikach częstej zmiany haseł.

Więcej na ten temat w wywiadzie z Iwoną Prószyńską reprezentującą CERT.

Uwierzytelnianie wieloskładnikowe

Pomaga chronić dane poprzez wprowadzenie dodatkowej warstwy bezpieczeństwa do danych. Nawet jeśli haker pozna hasło towarzyszące loginowi, to zaporę będzie stanowić drugi lub trzeci czynnik uwierzytelnienia, taki jak kod bezpieczeństwa, OTP, odcisk palca, rozpoznawanie głosu itp.

Regularne tworzenie kopii zapasowych

Tworzenie kopii zapasowych danych należy do kategorii działań podstawowych. Ważne, aby backup był robiony tak często jak tylko to możliwe ze względu na specyfikę pracy firmy, a także by był regularnie sprawdzany pod kątem możliwości odzyskania danych w razie udanego ataku. Dobrą praktyką jest wykonywanie backupu wg reguły 3-2-1. To znaczy, że powinny być tworzone co najmniej trzy kopie danych na dwóch różnych urządzeniach, a jedna z tych kopii powinna być przechowywana na zewnątrz, w innej lokalizacji.

Monitorowanie użytkowników uprzywilejowanych

Użytkownicy uprzywilejowani mogą być jednym z największych zagrożeń bezpieczeństwa danych. Szczególnie niebezpiecznym zjawiskiem, wiążącym się czasami z nadmiernymi uprawnieniami niektórych pracowników lub brakiem kontroli nad nimi, jest tzw. *shadow IT*. *Shadow IT* to termin określający nieautoryzowane i niekontrolowane przez dział IT korzystanie z aplikacji i usług przez pracowników w celu ułatwienia pracy. Może to stanowić zagrożenie bezpieczeństwa danych i utrudnić zarządzanie infrastrukturą IT. Czasami jest to wynik braku reakcji działu IT na realną potrzebę użytkowników, więc ci biorą sprawy w swoje ręce. Czasami to skutek braku koordynacji między działami. Niezależnie od powodu – zjawisko jest potencjalnie groźne.

Rozwiązaniem jest wprowadzenie do firm osoby odpowiedzialnej za kompleksowy nadzór nad infrastrukturą IT i gromadzonymi danymi, np. kierownika ds. informatyki, który będzie dbał m.in. o to, by w firmowej sieci nie pojawiły się podejrzane aplikacje czy urządzenia, liczba uprzywilejowanych użytkowników była ograniczona do niezbędnego minimum, a konta uprzywilejowane były dezaktywowane natychmiast po zakończeniu pracy.

Praca zdalna tylko przez VPN

VPN (*Virtual Private Network*) to technologia umożliwiająca bezpieczne i prywatne połączenie z Internetem poprzez szyfrowanie ruchu sieciowego. Właściwie skonfigurowany VPN pozwala na ukrycie adresu IP użytkownika oraz połączenie z Internetem

> *» Tylko edukowanie użytkowników w zakresie zagrożeń i sposobów ataków, polegających często na manipulacjach socjotechnicznych, w połączeniu z typowymi narzędziami cyberochrony, daje nadzieję na panowanie nad bezpieczeństwem firmowego IT. «*

za pośrednictwem zdalnego serwera VPN, co utrudnia monitorowanie aktywności w sieci i ataki cybernetyczne. VPN stosuje się przede wszystkim ze względu na cyberbezpieczeństwo, ponieważ zwiększa poziom prywatności, chroni dane przed przechwytywaniem i dostępem osób trzecich, a także umożliwia bezpieczne korzystanie z otwartych sieci Wi-Fi w miejscach publicznych.

A gdyby tak zamknąć dane w bunkrze?

Firmy, którym zależy na ochronie swoich danych. powinny przemyśleć inwestycję w cyfrowy bunkier (*cyber vault*), będący wieloetapową metodą zabezpieczania danych. Rozwiązanie służy do odzyskiwania danych po ataku, zwiększenia bezpieczeństwa dzięki tworzeniu dodatkowych backupów, ograniczenia do minimum dostępu z zewnątrz oraz automatyzacji zapisu przywracania danych. W Polsce jest ono oferowane m.in. przez Dell Technologies i IBM. Składa się z warstwy sprzętowej służącej do przechowywania danych i aplikacji odpowiedzialnej również za bezpieczeństwo końcowego backupu. Najważniejszą jego cechą jest całkowita izolacja od sieci zewnętrznej.

Główna idea cyfrowego bunkra polega na zabezpieczeniu danych poprzez tworzenie kopii z całej sieci pamięci masowych na urządzeniu o bardzo ograniczonym i krótkotrwałym cyklu wymiany danych. Dane ze wszystkich pamięci masowych są przesyłane do kolejnej, która zapisuje je w trybie zgodności *(compliance),* uniemożliwiając ich modyfikację czy usunięcie.

Najważniejsze jest jednak fizyczne odizolowanie kopii zapasowych od środowiska produkcyjnego. To użytkownik określa, w jakich odstępach czasu ma następować przekazywanie danych, by potem odłączyć urządzenia backupu od jakichkolwiek urządzeń zewnętrznych. Poza krótkimi momentami łączności kopie bezpieczeństwa są nie tylko niedostępne z zewnątrz, lecz także niewidoczne dla hakerów. Kolejna ważna kwestia to sprawdzenie, czy backupy nie zawierają złośliwego oprogramowania z włączonym „opóźnionym zapłonem".

Istnieją też wersje chmurowe cyfrowego bunkra, ale w ich przypadku należy się liczyć z wyciekiem danych. Za całość operacji i ich bezpieczeństwo odpowiada dostawca chmury.

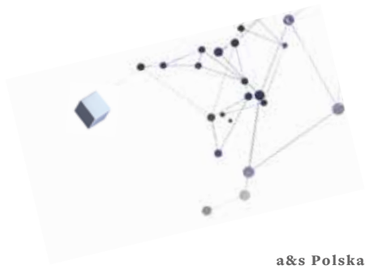
Ile kosztują cyberataki?

Skutecznie przeprowadzony atak może mieć olbrzymi wpływ na organizację. Koszty przestoju to nie wszystko. Należy doliczyć np. okup, jeśli za atak odpowiedzialny jest ransomware, koszt kary, jeśli dane wyciekną, ale także koszt ewentualnych procesów sądowych, podwyżkę stawek ubezpieczeniowych oraz utratę reputacji. Zgodnie z raportem *State of Cybersecurity Resilience 2021* firmy Accenture koszty naruszeń danych wzrosną z 3 bln USD rocznie do ponad 5 bln w 2024 r. Autorzy wspomnianego wcześniej raportu IBM sprawdzili, że choć w porównaniu z ubiegłym rokiem koszty naruszenia będących wynikiem ataku *ransomware* nieznacznie spadły, z 4,62 mln USD do 4,54 mln, to częstotliwość ataków się zwiększyła. Przyznają jednocześnie, że w badaniu nie uwzględniono kosztu okupu. Jak podała firma SlashNext w raporcie *2022 State of Phishing,* liczba ataków phishingowych w roku 2022 wzrosła o 61%. Z kolei Anti-Phishing Working Group (APWG) poinformowała, że w trzecim kwartale 2022 r. zaobserwowała łącznie 3 mln ataków phishingowych, co oznacza, że pod tym względem był to najbardziej intensywny kwartał, od kiedy APWG zaczęła gromadzić dane na ten temat.

Nie bez znaczenia jest w tym kontekście kwestia RODO. Każda firma, która gromadzi dane wrażliwe w rozumieniu RODO, niewątpliwie je też przetwarza, czyli zbiera, utrwala, organizuje, porządkuje, przechowuje, pobiera i przegląda. Niedochowanie zasad dotyczących cyberbezpieczeństwa może spowodować wyciek danych, a to bardzo kosztowne.

Gdy Rudy Giuliani został w 1993 r. burmistrzem Nowego Jorku, wprowadził politykę zero tolerancji. W ciągu kilku lat liczba przestępstw – od drobnych po włamania i pobicia – spadła o 52%, morderstw – o 68%. Niestety, cyfrowy świat rządzi się nieco innymi prawami. Wprowadzenie polityki *zero trust* nie zmniejszy liczby cyberprzestępstw, tak jak polityka zero tolerancji zmniejszyła liczbę napaści fizycznych w Nowym Jorku, ale znacząco ograniczy ich skuteczność. ●

» *Gdy ataki cybernetyczne stają się coraz bardziej zaawansowane i nieprzewidywalne, zero trust staje się jednym z najskuteczniejszych sposobów ochrony systemów i danych przed cyberzagrożeniami.* «



Edukacja!

„NIE WYMUSZAJ ZMIANY HASŁA" – MÓWI IWONA PRÓSZYŃSKA Z CERT POLSKA

Działający przy NASK polski CERT (Computer Emergency Response Team), czyli zespół specjalistów zajmujących się zarządzaniem incydentami związanymi z bezpieczeństwem informatycznym, przygotował zestaw rekomendacji dotyczących ochrony danych (informacje na ten temat na stronie cert.pl). Lista zaleceń nie jest wprawdzie długa, ale czy może pani wskazać te najważniejsze?
Zacznę od tego, że to są tylko rekomendacje. Jako CERT nie mamy wpływu na to, co robią osoby prywatne i firmy, by uchronić się przed zagrożeniami płynącymi z sieci. Możemy reagować wyłącznie na przysyłane do nas zgłoszenia. Lecz trzeba pamiętać, że obchodzenie reguł to proszenie się o kłopoty. Przechodząc do pytania, najważniejsze jest, by system kopii zapasowych był odizolowany, zaś same kopie regularnie sprawdzane. Ma to kluczowe znaczenie w wypadku coraz częstszych niestety ataków ransomware.

Kolejną ważną zasadą jest dbałość o aktualizacje systemów, zwłaszcza tych „wystawionych" do Internetu, i urządzeń będących w bezpośrednim posiadaniu pracowników. W tym kontekście bardzo ważne jest także, by dostęp zdalny do zasobów firmowych możliwy był tylko po podwójnym uwierzytelnianiu. Jednak tym, co uważam za fundament bezpieczeństwa, są edukacja pracowników i budowanie świadomości dotyczącej cyberzagrożeń oraz tego, jaki mają wpływ na bezpieczeństwo całej organizacji. W edukacji mieści się także to, by pracownicy wiedzieli, komu zgłaszać incydenty i zagrożenia, i nie bali się tego robić.

Wśród zaleceń znalazłam jedno, które nie ukrywam, bardzo mnie zaskoczyło, skierowane bezpośrednio do firm. Brzmi ono: nie wymuszaj zmiany hasła. To o tyle dziwne, że w wielu firmach polityka bezpieczeństwa wymaga od użytkowników regularnej zmiany hasła, czasami co 21 dni, czasami co trzy miesiące. Jest to kłopotliwe, ale wydaje się rozsądne, tymczasem państwo mówią: nie zmieniaj. Dlaczego?
Zanim wyjaśnię, zapytam, czy pracując, musiała pani zmieniać hasło?

Oczywiście, i to jakoś absurdalnie często.
Jak rozumiem, za każdym razem wybierała pani długie, co najmniej 12-znakowe hasło składające się z ciągu przypadkowych liter i cyfr?

Skądże. Przyznam, że hasło było stałe i zmieniała się tylko ostatnia cyfra.
Otóż to. Tak robi większość osób. Logujemy się tak często w różnych serwisach, portalach i na stronach, że najczęściej korzystamy z jednego hasła, które wydaje się nam mocne jak stal, bo ma minimum 8 znaków, w tym jeden specjalny. A jeśli administrator firmowej sieci wymusza na nas zmianę zbyt często, podmieniamy pierwszy lub ostatni znak i śpimy spokojnie. Tymczasem rzecz nie w znakach specjalnych, a w długości hasła. Im dłuższe, tym lepsze.

Długie, czyli...?
Powiedzmy 12–15 znaków. Hasła krótkie 8-znakowe można złamać w kilka minut. Hasło, które będzie mieć kilkanaście znaków, jest, przynajmniej na razie, bardzo trudne do złamania. Nie ma sensu zmuszać użytkowników do zmiany co trzy, cztery tygodnie. Zrobią dokładnie tak jak pani. Lepiej wymóc na nich to, by hasło było naprawdę długie, wówczas jego zmiana będzie konieczna dopiero wtedy, gdy mamy podejrzenie, że ktoś mógł je poznać.

Przy okazji, każdy może sprawdzić, czy jego hasło i inne dane, np. adres e-mail i numer karty kredytowej nie wyciekły do sieci. Jednym z najpopularniejszych narzędzi do tego celu jest serwis Have I Been Pwned. Wystarczy wejść na stronę https://haveibeenpwned.com/Passwords i wpisać własny adres e-mail lub telefon. Jeśli informacje o nas zostały znalezione w bazie danych naruszeń, zalecam jak najszybszą zmianę hasła na nowe i unikatowe. Używanie różnych, i raz jeszcze podkreślę, bardzo długich haseł dla różnych kont jest najlepszym sposobem ochrony przed wyciekiem hasła z jednej usługi.

Jak jednak zapamiętać takie długie i skomplikowane hasło?
Wbrew pozorom to nie jest trudne. Doprawdy nie musi być to ciąg bezsensownych znaków. Z powodzeniem może to być np. fraza *mójulubionykottozielonymisiek.* Problem pojawia się wtedy, gdy administrator danego serwisu lub strony uniemożliwia wprowadzenie tak długiego hasła, ograniczając użytkowników do tych nieszczęsnych ośmiu znaków. Na szczęście nie dzieje się to często, ale warto się wówczas zastanowić, czy naprawdę musimy z niego korzystać. Dodatkowo w „zapamiętywaniu" haseł bardzo pomocne są menedżery. Jako CERT Polska gorąco je rekomendujemy.

Bill Clinton swoją kampanię wyborczą prowadził pod hasłem „Gospodarka, głupcze". CERT Polska mówi „Edukacja, głupcze!".
Edukacja tak, choć bez „głupcze". Częścią utrzymania wysokiego poziomu bezpieczeństwa jest upewnienie się, że pracownicy niezajmujący się bezpieczeństwem IT wiedzą, w jaki sposób bezpieczeństwo wpływa na ich codzienne czynności. Przygotowanie programu szkoleniowego w zakresie świadomości bezpieczeństwa jest niezbędną częścią strategii bezpieczeństwa każdej firmy. Szczególną uwagę powinny zwracać te przedsiębiorstwa, które mają w swoim środowisku urządzenia mobilne i urządzenia IoT albo wprowadziły politykę *bring your own device,* umożliwiając pracownikom wykorzystywanie prywatnych sprzętów do pracy. To bywa wygodne dla obu stron, ale jest niebezpieczne, dlatego opracowanie planu reagowania na incydenty jest po prostu koniecznością.

Dobrą praktyką jest też zgłaszanie ich do CERT, do czego zachęcam. Nasi eksperci są do dyspozycji w trybie 24/7, bo niepokojące zjawiska w cyberprzestrzeni pojawiają się stale. ●

Inwentaryzacja urządzeń jako fundament cyberbezpieczeństwa

„Nie można chronić rzeczy, o których się nie wie” – to hasło jest często powtarzane w branży cyberbezpieczeństwa. Tym bardziej zaskakuje fakt, że kwestia inwentaryzacji urządzeń bywa często marginalizowana.

Inwentaryzacja urządzeń i zasobów pozwala organizacji monitorować typ, wiek i wydajność operacyjną urządzeń, a także zyskać pewność, że żadne informacje o lukach technologicznych i wymaganych do przeprowadzenia modernizacjach nie zostaną przeoczone.

Jednym z głównym obszarów związanych z inwentaryzacją zasobów jest zarządzanie ryzykiem, a dokładniej – cyberbezpieczeństwo. W parze z nim idzie proces wzmacniania – mający na celu ograniczenie słabych punktów do minimum – który często uważa się za czasochłonny, zwłaszcza gdy jest realizowany na poziomie urządzeń. W rezultacie podczas oddawania sprzętu do użytku obszar ten często bywa zaniedbywany.

Zbiorcze zarządzanie urządzeniami

Rozwiązanie takie jak AXIS Device Manager umożliwia szybkie i łatwe instalowanie oraz konfigurowanie urządzeń i zarządzanie nimi. To skuteczne narzędzie dla instalatorów zabezpieczeń i administratorów systemu, które służy do nadzorowania głównych zadań związanych z instalacją, ochroną i utrzymaniem. Urządzeniami można zarządzać pojedynczo lub zbiorczo, co znacząco (z godzin do minut) skraca czas potrzebny do „wzmocnienia” urządzeń, a jednocześnie gwarantuje spójne funkcjonowanie całego systemu.

AXIS Device Manager pozwala użytkownikowi utworzyć kod konfiguracyjny, który można przesłać na wszystkie urządzenia Axis. Kod powstaje zgodnie z wytycznymi Axis Hardening Guide – dokumentacji technicznej, która pomaga opracować podstawową konfigurację i podpowiada, jak sobie radzić z wciąż zmieniającym się krajobrazem zagrożeń. Axis stosuje procedury opisane w dokumentacji CIS Controls (v. 7.1; znanej wcześniej pod nazwą *SANS Top 20 Critical Security Controls*). Przygotowała ją organizacja non profit Centre for Internet Security, która słynie ze sprawdzonych praktyk w zakresie zabezpieczania systemów IT i danych.

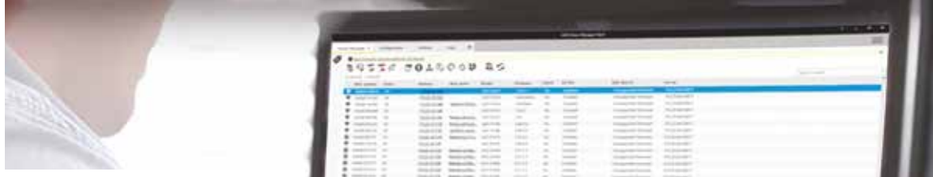
Szybka i łatwa konfiguracja nowych urządzeń jest ważna, jednak nie mniejsze znaczenie ma zarówno dostęp do aktualnych informacji o tym, co dzieje się w poszczególnych ośrodkach i systemach bezpieczeństwa, jak i monitorowanie statusu sprzętu. Ten nierzadko złożony i czasochłonny proces można uprościć, sięgając po narzędzie takie jak AXIS Device Manager Extend Base. Pozwalają na to jego funkcje, np. intuicyjne panele kontrolne ze zdalnym dostępem do ośrodków, które zapewniają natychmiastowy wgląd w informacje o wszystkich urządzeniach w połączonych ośrodkach.

Sprawne przekazywanie urządzeń do eksploatacji

Zanim przejdziemy do kwestii związanych z bezpieczeństwem urządzeń i monitorowaniem statusu sprzętu, warto zoptymalizować proces instalacji i przekazywania urządzeń do eksploatacji – może to przynieść znaczną oszczędność czasu. „Wzmacnianie” urządzeń jednego po drugim to zadanie czasochłonne. Podobnie jest w przypadku oddawania ich do użytku.

Narzędzie do zautomatyzowanego i zbiorowego przekazywania urządzeń do eksploatacji wyraźnie skraca czas zarządzania tym procesem. Oznacza to wzrost produktywności i możliwość realizacji większej liczby projektów. Inną korzyścią jest spadek kosztów towarzyszących przekazywaniu urządzeń do eksploatacji, co z kolei pomaga pozyskiwać nowych klientów dzięki bardziej konkurencyjnej ofercie.

AXIS Device Manager automatycznie wykrywa wszelkie urządzenia firmy Axis i zarządza ich konfiguracją, upraszczając w ten sposób oddanie sprzętu do użytku. Ponadto zarządza adresami IP i monitoruje status połączenia, a także instaluje aktualizacje oprogramowania sprzętowego i aplikacje do kamer. W razie potrzeby oprogramowanie może odzyskać poprzednie ustawienia, a cała komunikacja jest zabezpieczana, m.in. przy wykorzystaniu protokołów HTTPS i 802.1X. Narzędzie pozwala też swobodnie zarządzać pojedynczymi urządzeniami, gdy zajdzie taka potrzeba.



Znaczenie instalowania poprawek

Po przekazaniu urządzeń do eksploatacji kluczowego znaczenia nabiera skuteczne zarządzanie cyklem życia systemu, zwłaszcza w kontekście aktualizowania zabezpieczeń i oprogramowania sprzętowego oraz instalowania poprawek. To nieustannie trwający proces, który pozwala wykazać się integratorom systemów, ale niekiedy nakłada na nich także dodatkowe obowiązki. Przykładowo, w Wielkiej Brytanii Biuro Informacji Publicznej (Information Commissioners Office, ICO), odpowiednik instytucji ds. ochrony danych osobowych w poszczególnych krajach członkowskich UE, wskazuje wytyczne dotyczące zarządzania poprawkami. Ich nieprzestrzeganie skutkuje naruszeniem bezpieczeństwa danych konsumentów, a w efekcie – wysokimi grzywnami.

Według wytycznych „niedopełnienie powinności wyeliminowania znanych luk stanowi czynnik uwzględniany przez Biuro Informacji Publicznej przy ustalaniu, czy naruszenie siódmej zasady ustawy o ochronie danych osobowych *(odpowiednik RODO – przyp. red.)* jest wystarczająco poważne, by uzasadniało nałożenie grzywny cywilnej”.

Statystyki zaprezentowane przez CSO – serwis publikujący wiadomości, analizy i badania z dziedziny bezpieczeństwa i zarządzania ryzykiem – nie napawają optymizmem. W 60% przypadków do naruszeń dochodziło z wykorzystaniem luk, dla których poprawka była dostępna, a nie została zainstalowana. Jeżeli użytkownik końcowy zostanie ukarany za nieprzestrzeganie przepisów, ale obowiązek ich monitorowania spoczywa na zewnętrznym integratorze systemów pełniącym także funkcję podmiotu przetwarzającego dane, można przyjąć, że integrator systemów ponosi częściową odpowiedzialność za nałożoną grzywnę. Dlaczego więc przedsiębiorstwa odpowiadające za serwisowanie i utrzymanie systemów nie instalują aktualizacji na bieżąco?

Najczęstszym usprawiedliwieniem tego faktu jest brak czasu, a także skutecznych środków pozwalających na regularne aktualizowanie oprogramowania sprzętowego i poprawek. Tu również z pomocą przychodzi AXIS Device Manager, który może służyć jako szybkie i efektywne narzędzie do zapewniania zgodności z przepisami. Podobnie jak w przypadku przekazywania urządzeń do eksploatacji, oferowane oprogramowanie usprawnia utrzymanie, łącząc czasochłonne i kosztowne procesy w szybką i wydajną operację.

AXIS Device Manager monitoruje status urządzeń, aktualizuje oprogramowanie sprzętowe, odnawia certyfikaty i nimi zarządza, a w razie potrzeby przywraca ustawienia domyślne. Przedsiębiorca, który uświadomi klientom, że doskonale rozumie istniejące ryzyko, a przy tym zademonstruje skuteczny sposób zarządzania kluczowym aspektem utrzymania, może liczyć na ich zaufanie.

Monitorowanie końca okresu wsparcia

Należy wspomnieć, że równie dużą rolę odgrywa strategia wymiany rozwiązań technicznych, których okres wsparcia minął. Jego koniec przypada wtedy, gdy dostawca przestaje zapewniać wsparcie dla swojego produktu lub usługi. Strategia przedsiębiorstwa powinna przewidywać, jak długo sprzęt lub oprogramowanie będą znajdowały się w eksploatacji po wygaśnięciu okresu wsparcia, a także zakładać monitorowanie funkcjonowania rozwiązań technicznych w całej firmie.

To informacje o zasadniczym znaczeniu dla specjalistów IT odpowiedzialnych za zarządzanie politykami IT i strategią cyberbezpieczeństwa w ośrodku, ponieważ na tym etapie dostawca przestaje udostępniać aktualizacje i poprawki. W przypadku zaniechania wdrożenia alternatywnych środków wzrasta narażenie na ataki i idące za tym naruszenie zabezpieczeń danych. Nie wszystkie organizacje zdecydują się na wymianę rozwiązań technicznych, dla których okres wsparcia minął, jednak te, w których zdanie zespołów IT się liczy, z pewnością to zrobią.

Objęcie użytkowników końcowych proaktywną strategią zarządzania aktualizacjami oprogramowania sprzętowego pozwoli umocnić opartą na zaufaniu relację poprzez zwiększenie wśród użytkowników poczucia gwarancji bezpieczeństwa i zgodności z przepisami. Monitorowanie systemów i wczesne powiadamianie klientów o zbliżającym się końcu okresu wsparcia pozwala uniknąć gorączkowej paniki i sytuacji, w których klienci nie dysponują wymaganym budżetem. Takie podejście umożliwia zatem wejście na wyższy poziom relacji.

AXIS Device Manager – w połączeniu z zapewnianym użytkownikom końcowym przejrzystym doradztwem w zakresie wydajności operacyjnej zainstalowanych technologii – umożliwia dostarczanie szczegółowych informacji, np. o okresie gwarancyjnym czy końcu okresu wsparcia. Partnerom w zakresie bezpieczeństwa pozwala to dowieść swojej niezawodności.

A odpowiednio wykorzystane narzędzia, takie jak AXIS Device Manager czy AXIS Device Manager Extend Base, pomogą zadbać o wysoki poziom bezpieczeństwa klientów. ●

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

Czy twój system kontroli dostępu jest odporny na cyberataki?

Kontrola fizycznego dostępu to dzisiaj znacznie więcej niż nadawanie uprawnień dostępu do poszczególnych pomieszczeń. O cyberbezpieczeństwie rozmawiamy z **Wesleyem Keegstrą**, kierownikiem ds. integracji w firmie Nedap Security Management. Wyjaśniamy także, dlaczego cyberbezpieczeństwo stanowi istotną, choć często nieuświadamianą potrzebę ochrony systemów kontroli dostępu fizycznego.

Wiele nowoczesnych systemów kontroli dostępu fizycznego jest opartych na protokole IP i obsługiwanych przez inteligentne oprogramowanie, umożliwiając przetwarzanie ogromnych ilości danych.

Zapewnia to większą funkcjonalność, elastyczność i skalowalność oraz możliwości integracji z innymi systemami (interoperacyjność). Oznacza to również, że systemy KD stanowią część firmowej sieci IT, więc należy je chronić i aktualizować – tak jak pozostałe systemy infrastruktury IT.

Wiele przedsiębiorstw wciąż nie zadbało o cyberbezpieczeństwo swoich systemów kontroli dostępu fizycznego opartych na IP. Co pana zdaniem jest przyczyną takiego stanu?

Myślę, że dużą rolę odgrywa tu brak świadomości. Bezpieczeństwo fizycznego dostępu dotyczy czegoś, co można zobaczyć i czego można dotknąć, a więc łatwiej je zrozumieć czy uzasadnić. Cyberbezpieczeństwo jest równie ważne, a cyberataki są bardziej wyrafinowane. Brak cyberzabezpieczeń systemu KD opartego na IP jest jak pozostawienie szeroko otwartych drzwi. A jeśli zostawiamy otwarte tylne drzwi, inwestowanie czasu i pieniędzy w fizyczne zabezpieczenia obiektu nie ma sensu.

W jaki sposób cyberprzestępcy mogą naruszyć systemy kontroli dostępu fizycznego?

Cyberprzestępczość ma wiele form. Może polegać np. na nieuprawnionym pobieraniu danych lub manipulowaniu danymi przesyłanymi pomiędzy urządzeniami systemu kontroli dostępu, m.in. w celu ujawnienia, które osoby mają dostęp i w jakim miejscu. Może to być także gromadzenie danych z kart dostępu, a następnie ich kopiowanie lub klonowanie. Idąc krok dalej, cyberprzestępcy mogą ukraść czyjeś dane uwierzytelniające, aby zalogować się do oprogramowania systemu KD. Po zalogowaniu mogą udzielić nieautoryzowanego dostępu do wszelkiego rodzaju drzwi i pomieszczeń. Uzyskując dostęp do firmowej bazy danych, mogą manipulować zapisami zdarzeń lub nawet usunąć zapisy świadczące o działaniach wykonanych przez nich lub przez inne osoby.

Urządzenia systemu kontroli dostępu oparte na sieci IP współpracują z różnymi urządzeniami sieciowymi innych systemów, zatem ważne, aby każde z nich było chronione przed cyberatakami – chodzi tu zarówno o czytniki, sterowniki, kamery, jak i wiele innych urządzeń. Jakie mogą być konsekwencje cyberataku?

Skutki mogą być różne. Najbardziej oczywistym jest możliwość uzyskania fizycznego dostępu do mienia i dokonanie jego kradzieży lub nawet aktów terroryzmu. Cyberprzestępca może też – zdalnie lub uzyskując dostęp do obiektu – wykraść gromadzone i przetwarzane dane. Mogą to być informacje niejawne, takie jak dane dotyczące produktu, które w przypadku wycieku mogą zapewnić przewagę konkurentom. Cyberprzestępca może również wykraść dane osobowe lub finansowe, a to narazi administratora danych na wysokie, w zależności od branży i kraju, kary.

Naprawa skutków cyberataku i przywrócenie funkcjonalności systemów często wiąże się z kosztami. Jeśli przedsiębiorstwo nie może funkcjonować wskutek awarii systemu informatycznego, trzeba się liczyć z dodatkowymi kosztami. Cyberataki mogą również zaszkodzić reputacji firmy, a to prowadzi do strat finansowych i wpływa na rozwój i stabilność działalności. Podsumowując, w kwestii cyberbezpieczeństwa należy dmuchać na zimne.

W jaki sposób firmy mogą chronić swoje systemy kontroli dostępu fizycznego przed cyberprzestępcami?

Nikt nie może powiedzieć, że coś jest cyberbezpieczne w 100%, ale zdecydowanie lepiej zapobiegać niż leczyć. Najważniejsze kwestie to zapewnienie cyberochrony zarówno urządzeń i oprogramowania do kontroli dostępu, jak i nośników danych oraz sposobu uzyskiwania dostępu do przesyłanych informacji – nie tylko w obrębie jednego budynku, lecz także całego kraju czy na poziomie międzynarodowym.

Bardzo istotne jest wprowadzenie jasnych zasad bezpiecznego korzystania z systemów kontroli dostępu fizycznego i bezpiecznego zarządzania nimi. Powinny one obejmować elementy cyberbezpieczeństwa i wymagać korzystania z silnych haseł, zmienianych po upływie określonej liczby dni. Należy także opracować politykę bezpieczeństwa dotyczącą innych urządzeń bazujących na IP, takich jak kamery, pamiętając, że o wytrzymałości całego łańcucha decyduje jego najsłabsze ogniwo.

Pracownicy powinni zostać przeszkoleni w zakresie cyberbezpieczeństwa, aby zastosowane środki nie okazały się nieskuteczne w wyniku braku wiedzy i nieodpowiedzialnego zachowania ludzi.

Czy każda organizacja potrzebuje takiego samego poziomu cyberbezpieczeństwa?

Wymagania w zakresie cyberbezpieczeństwa mogą się różnić w zależności od branży i konkretnego przedsiębiorstwa lub organizacji. Cyberbezpieczeństwo wymaga zasobów i inwestycji, więc ważne jest to, aby odpowiednio je dopasować do sytuacji firmy.

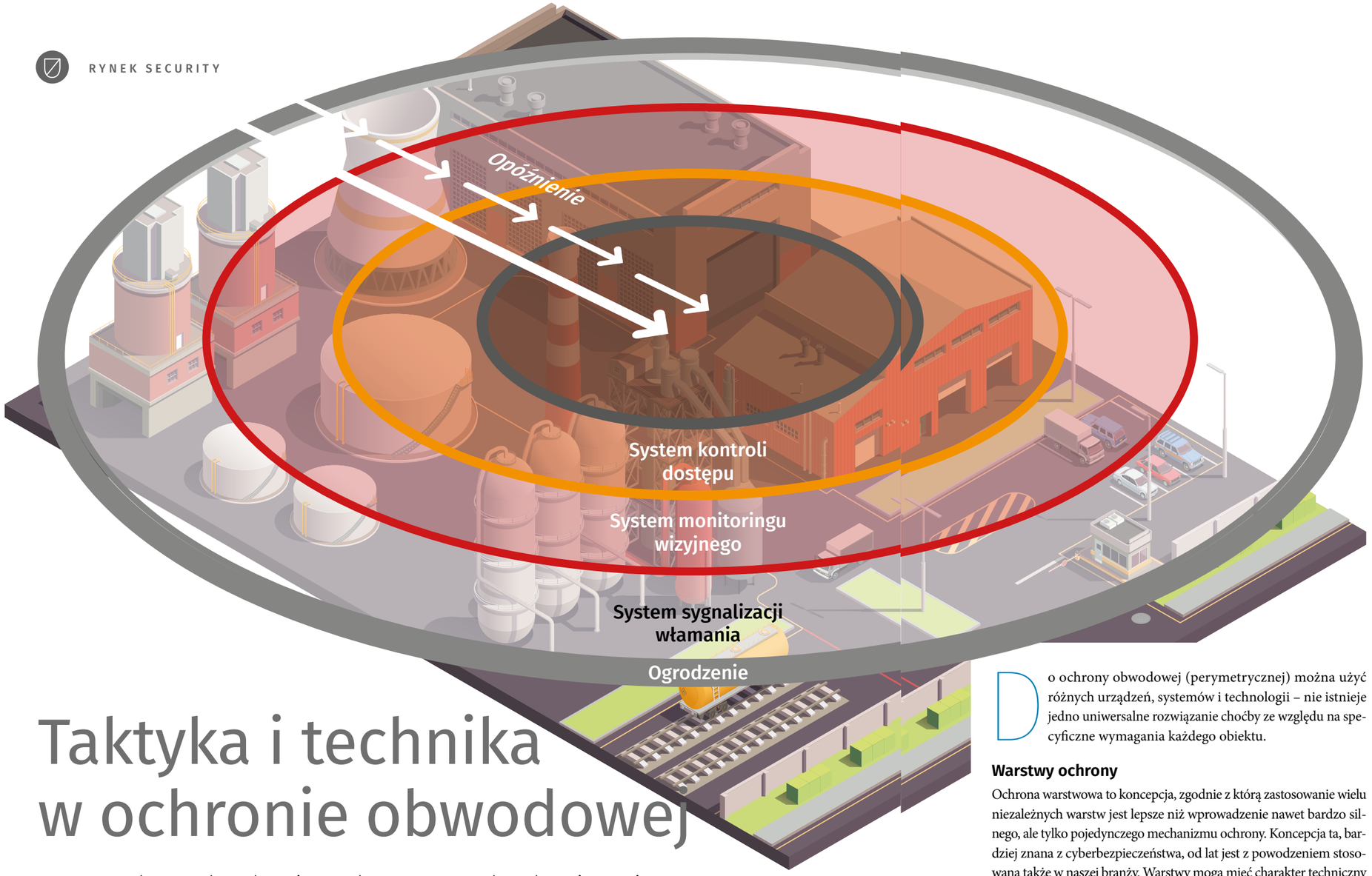
Oferowany przez firmę Nedap system kontroli dostępu AEOS zapewnia użytkownikowi kontrolę nad cyberbezpieczeństwem, umożliwiając podejmowanie decyzji, co należy zabezpieczyć i na jakim poziomie. Można zabezpieczyć np. karty, czytniki kart, kontrolery (centrale systemu KD) i bazy danych. Możliwe jest także zabezpieczenie dostępu do interfejsu użytkownika AEOS i szyfrowanie komunikacji między poszczególnymi komponentami systemu – to, co zabezpieczysz, zależy wyłącznie od ciebie. Gdy cyberbezpieczeństwo stanie się coraz ważniejsze dla organizacji, będziesz w stanie podnieść poziom ochrony w systemie AEOS. ●

Więcej o cyberbezpieczeństwie i systemie AEOS znajdziesz na www.nedapsecurity.com/pl/.

Nedap Security Management
al. Niepodległości 18
02-653 Warszawa
www.nedapsecurity.com/pl/

» Cyberbezpieczeństwo jest równie ważne co bezpieczeństwo fizyczne, a cyberataki są bardziej wyrafinowane. Brak cyberzabezpieczeń systemu KD opartego na IP jest jak pozostawienie szeroko otwartych drzwi. «

Wesley Keegstra
kierownik ds. integracji w firmie Nedap Security Management



Taktyka i technika w ochronie obwodowej

Systemy ochrony obwodowej są wykorzystywane do zabezpieczania nieruchomości, majątku i osób przebywających na terenie. Takie rozwiązania były szeroko stosowane przede wszystkim w obiektach wojskowych. Obecnie ochrona obwodowa jest równie powszechna w obiektach cywilnych.

Jan T. Grusznic, a&s Polska

Rys. 1. Graficzne ujęcie metodyki 5D

Do ochrony obwodowej (perymetrycznej) można użyć różnych urządzeń, systemów i technologii – nie istnieje jedno uniwersalne rozwiązanie choćby ze względu na specyficzne wymagania każdego obiektu.

Warstwy ochrony

Ochrona warstwowa to koncepcja, zgodnie z którą zastosowanie wielu niezależnych warstw jest lepsze niż wprowadzenie nawet bardzo silnego, ale tylko pojedynczego mechanizmu ochrony. Koncepcja ta, bardziej znana z cyberbezpieczeństwa, od lat jest z powodzeniem stosowana także w naszej branży. Warstwy mogą mieć charakter techniczny i proceduralny. Działanie ochrony obwodowej dobrze przedstawia idea „pierścieni ochrony" otaczających cel potencjalnego ataku.

Idea polega na utrzymaniu ciągłości ochrony zapewnianej przez pozostałe rozwiązania, gdy jedno z nich zostanie ominięte. Skuteczna ochrona obwodowa często jest wielowarstwowa i wielowymiarowa. Zastosowanie ochrony warstwowej pomaga w odpowiednim przygotowaniu koncepcji zabezpieczenia. Strategia ta obejmuje ludzi, procesy i technikę, mając na celu zmniejszenie ryzyka zagrożeń poprzez zastosowanie tzw. metodyki 5D *(rys. 1): Deter* (Odstraszanie), *Detect* (Wykrywanie), *Deny* (Odmawianie), *Delay* (Opóźnianie), *Defend* (Obrona).

1 ODSTRASZANIE – *Deter*

Jednym z celów ochrony obwodowej jest zniechęcenie intruza do podjęcia próby wtargnięcia na chroniony teren. Odstraszanie jest zabiegiem psychologicznym – jeśli ogrodzeniowy system ochrony jest odporny, do naruszenia może nie dojść. Odstraszanie zaczyna się w najdalszej możliwej odległości od chronionych zasobów i obejmuje kombinację różnych elementów konstrukcyjnych, takich jak utrudniające dostęp bariery fizyczne i zabezpieczenia mechaniczne. Mają one znaczny potencjał zniechęcania intruzów, a jednocześnie mogą stanowić konstrukcję do rozmieszczenia znaków/symboli bezpieczeństwa, które wzmacniają przekaz. Współpracując z widocznymi kamerami VSS, oświetleniem i nagłośnieniem, stanowią skuteczny środek odstraszający. Badania pokazują, że obecność kamer zmniejsza liczbę wtargnięć o 13% w porównaniu z obszarami ich pozbawionymi.

2 WYKRYCIE – *Detect*

Jak najwcześniejsze wykrycie nieautoryzowanego wtargnięcia na obszar chroniony jest sprawą kluczową do skutecznego zatrzymania dalszego rozwoju wypadków. Tu najważniejszą rolę odgrywają zewnętrzne elektroniczne urządzenia detekcyjne systemu ochrony obwodowej *(Perimeter Intrusion Detection System* – PIDS), które zapewnią wczesne wykrycie intruzów. Współpracujący z nim system dozoru wizyjnego umożliwia wizualną weryfikację zdarzenia i ocenę pod kątem podejmowanej reakcji.

3 ODMOWA – *Deny*

Taktyka odmowy dostępu ma na celu zatrzymanie osób nieupoważnionych na zewnątrz chronionego obiektu, przy jednoczesnym umożliwieniu wejścia osobom lub wjazdu pojazdom upoważnionym. Stosowana w tym celu technika ochronna obejmuje ogrodzenia, bariery mechaniczne oraz elektroniczne systemy kontroli dostępu, w tym urządzenia odczytujące tablice rejestracyjne pojazdów montowane przy bramach wejściowych i wjazdowych. W konwencjonalnej kontroli dostępu korzysta się z posterunków ochrony fizycznej stałej (OFS) niezbędnych, gdy jest wymagana natychmiastowa reakcja na miejscu zdarzenia.

4 OPÓŹNIENIE – *Delay*

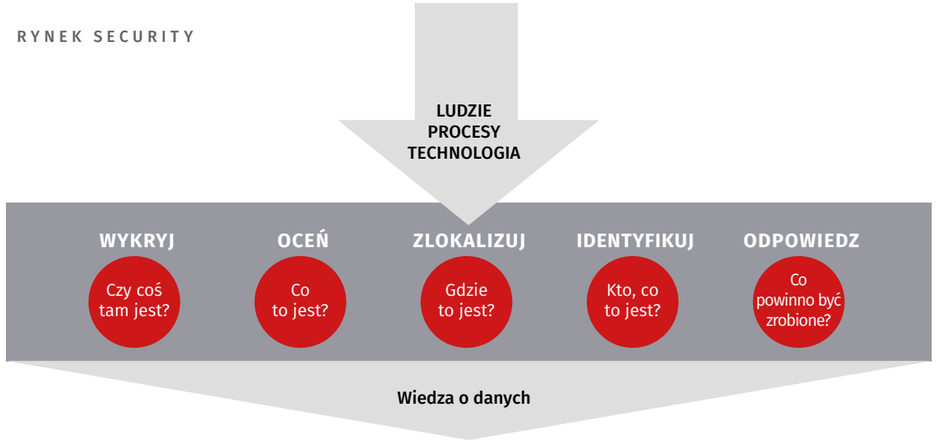
Poprawny projekt, dokładnie wykonana instalacja i właściwa struktura systemów ogrodzeniowych utrudniają wtargnięcie intruza na chroniony teren. Ochrona wielowarstwowa ma na celu opóźnienie nieautoryzowanej próby uzyskania dostępu, co pozwala na zbudowanie strategii skutecznego reagowania udaremniającej penetrację. W tym celu stosuje się różne rozwiązania zabezpieczające – mechaniczne (np. ogrodzenie) oraz elektroniczne (detektory PIDS) – które mają spowolnić działania intruza.

5 OBRONA – *Defend*

To ostatnia warstwa strategii bezpieczeństwa, kiedy zespół pracowników ochrony powstrzymuje intruza, który już wtargnął na teren. Może nim być człowiek, ale też urządzenie (np. bezzałogowy statek powietrzny) lub zwierzę. Systemy obronne i detekcyjne powinny być tak zaprojektowane, by wspierać skuteczne wykonywanie działań pracowników. Szybka reakcja na incydent naruszenia strefy perymetrycznej wymaga znajomości topografii chronionego obiektu. Zastosowane rozwiązania powinny więc zapewniać świadomość sytuacyjną (czas, lokalizacja i ogólny opis incydentu). Wsparcie systemu dozoru wizyjnego, obrazowanie radarowe czy z drona (np. na uwięzi) to najlepsze sposoby, aby poznać zakres i okoliczności naruszenia i przyspieszyć reakcję.

Koncepcja systemu ochrony obwodowej

Dostępność i złożoność elektronicznych systemów zabezpieczeń znacząco wzrosła w ostatnich latach, wpływając na sposób definiowania



Rys. 2 Koncepcja PIDS

systemu ochrony obwodowej (PIDS) przede wszystkim w aspekcie zaawansowania zastosowanych w nich rozwiązań technicznych. Branie pod uwagę głównie tego aspektu zbyt często prowadzi do wdrożenia rozwiązania droższego niż planowano, niedostosowanego do zagrożeń w obiekcie i nieefektywnego. Rodzaj i liczba zastosowanych urządzeń powinna wynikać z przeprowadzonej analizy zagrożeń (obligatoryjnej dla obiektów podlegających obowiązkowej ochronie). To niezbędny element koncepcji zabezpieczenia, pozwalający określić rzeczywiste zagrożenia oraz słabe i mocne punkty ochrony wynikające ze specyfiki obiektu, a także inne czynniki mające wpływ na jego bezpieczeństwo. Dopiero później można przystąpić do doboru urządzeń i oceny kosztów w celu określenia najlepszego rozwiązania zgodnego z szacowanym budżetem. Docelowo w pełni funkcjonujący system ochrony obwodowej powinien stale dozorować strefę perymetryczną i inne wyznaczone obszary przy użyciu techniki bez potrzeby ciągłego monitorowania ich przez człowieka. Zakres działania PIDS natomiast powinien obejmować wykrywanie, lokalizowanie, ocenę i możliwość alarmowania w czasie rzeczywistym oraz stanowić narzędzie świadomości sytuacyjnej *(rys. 2)*. W ramach PIDS można zastosować wiele rozwiązań. Każde z nich ma zalety i wady, dlatego należy je dobierać do rodzaju obiektu, sposobu ochrony, warunków środowiskowych czy ukształtowania terenu. Nie każda może wszędzie znaleźć zastosowanie, każdą natomiast można zastosować niezależnie lub w połączeniu z innymi rozwiązaniami w celu poprawy jakości i czasu detekcji.

Napłotowe systemy ochrony obwodowej

To rozwiązania oparte na kablach sensorycznych instalowanych na ogrodzeniu w celu wykrywania przypadków wspinania się po nim, przecinania, podnoszenia lub innego manipulowania przy nim. Jednym z takich rozwiązań jest światłowodowy kabel sensoryczny składający się z elementów aktywnych, przesyłających wiązkę światła przez kabel umieszczony wzdłuż ogrodzenia. Wibracje ogrodzenia wywołane przez intruza zakłócają optykę światłowodu, co jest natychmiast rozpoznawane. Inną możliwością jest zastosowanie kabla z wbudowanymi akcelerometrami zdolnymi do wykrywania wibracji wzdłuż linii ogrodzenia. Ciekawym rozwiązaniem jest mikrofonowy kabel sensoryczny wrażliwy na dźwięki.
Jednostki sterujące we wszystkich wymienionych systemach wykorzystują cyfrowe przetwarzanie sygnału i algorytmy pozwalające zminimalizować uciążliwe zakłócenia spowodowane naturalnymi zjawiskami (wiatr, deszcz czy ruch pojazdów), jednocześnie alarmując o potencjalnych naruszeniach, jeśli sygnał przekracza określone warunki i progi.
Tego typu systemy mogą być stosowane w przypadku bardzo dużych stref detekcji lub na bardzo długich odcinkach. O ile systemy światłowodowe i akcelerometryczne pozwalają zlokalizować obszar alarmu z dokładnością do 3 m od zakłócenia, o tyle systemy mikrofonowe mają zazwyczaj jedną strefę dla dużych odległości, co utrudnia ocenę konkretnego miejsca alarmu ze względu na niski poziom rozdzielczości. Wszystkie trzy wymienione rozwiązania są podatne na uciążliwe alarmy spowodowane naruszeniem ogrodzenia przez zwierzęta, silny wiatr, ulewny deszcz, śnieg czy grad. Ponadto są one skuteczne tylko wtedy, gdy intruz ma fizyczny kontakt z ogrodzeniem. System nie zareaguje, jeśli linia ogrodzenia nie zostanie fizycznie poruszona.

Bariery mikrofalowe (MV) i podczerwieni (IR)

Bariery skutecznie wykryją chodzących, biegnących lub czołgających się ludzi. Nadajnik i odbiornik bariery mikrofalowej są umieszczane

Systemy światłowodowe i akcelerometryczne

Zalety	Wady
Prosty montaż wzdłuż granicznej linii ogrodzenia	Prawidłowe działanie czujnika w dużej mierze zależy od stanu ogrodzenia
Odpowiednie dla długich ogrodzeń	Podatność na fałszywe alarmy spowodowane przez zakłócenia w ogrodzeniu (zwierzęta, wiatr, grad, duże pojazdy itp.)
Podążanie za krzywizną terenu	System jest niewolumetryczny, więc może być mostkowany lub tunelowany
Duże prawdopodobieństwo wykrycia z dokładnością do 3 m lub większą	
Odporność na EMI i RF	
Możliwość wykorzystania algorytmów adaptacyjnych w celu zminimalizowania uciążliwych fałszywych alarmów, a także do klasyfikacji zdarzeń alarmowych (wspinaczka, cięcie itp.)	

NMS ADVANCED CONTROL
POLSKI PRODUKT
INTEGRACJA • KONFIGURACJA • WIZUALIZACJA
SYSTEMÓW BEZPIECZEŃSTWA
✓ INTEGRACJA Z URZĄDZENIAMI **VSS**, **KD**, **SSWiN** ORAZ **AUTOMATYKI BUDYNKOWEJ**
✓ REJESTRACJA CZASU PRACY **RCP**
✓ KONTROLA DOSTĘPU DO **WIND I PIĘTER**
✓ **FUNKCJE GLOBALNE**
✓ **IDENTYFIKACJA BIOMETRYCZNA**
✓ PODGLĄD OBRAZU, **ODTWARZANIE ORAZ POBIERANIE NAGRAŃ**
✓ ZARZĄDZANIE **SYSTEMAMI ROZPROSZONYMI**
✓ **ROZPOZNAWANIE TABLIC REJESTRACYJNYCH**
ZINTEGROWANE ZARZĄDZANIE BEZPIECZEŃSTWEM
• Jeden interfejs dla wszystkich integrowanych systemów
• Wizualizacja systemu oraz obiektów na panelach
• Obsługa wielu monitorów
• Zaawansowane scenariusze umożliwiające definiowanie interakcji pomiędzy systemami
• Wideoweryfikacja zdarzeń
JAK TO DZIAŁA?
NMSAC.AAT.PL
NMS AC to profesjonalne polskie oprogramowanie zarządzające systemami bezpieczeństwa w obiektach.
Do nabycia u najlepszych instalatorów!
AAT SYSTEMY BEZPIECZEŃSTWA
PRODUCENT I DOSTAWCA ELEKTRONICZNYCH SYSTEMÓW ZABEZPIECZENIA MIENIA
www.aat.pl

naprzeciw siebie, często w znacznej odległości. Według niektórych producentów maksymalny użytkowy zasięg barier mikrofalowych wynosi do 250 m. Bariery MV generują pole elektromagnetyczne między nadajnikiem a odbiornikiem, tworząc niewidoczną objętościową (przestrzenną) strefę detekcji. Te rozwiązania są skuteczne w ochronie obszarów otwartych, bram lub wejść na teren oraz dachów. Dają wysokie prawdopodobieństwo wykrycia i niski poziom fałszywych alarmów. Jednocześnie są odporne na deszcz, mgłę, wiatr, kurz, padający śnieg i skrajne temperatury.

Bariery mikrofalowe nie sprawdzą się w ochronie wąskich stref (poniżej 2 m), do których poleca się bariery podczerwieni. Te są dobrym rozwiązaniem do ochrony linii ogrodzeń i bram oraz kurtynowego zabezpieczenia obiektu, okien i murów. Składają się z dwóch elementów: nadajnika transmitującego wiązkę podczerwieni oraz odbiornika, tworząc w ten sposób obwód wyzwalający. Alarm wywołuje przecięcie wiązki. Aby zapobiec fałszywym wzbudzeniom, wiązki IR mogą być programowo grupowane. Wówczas krótkie przesłonięcie pojedynczej wiązki nie wywołuje alarmu, ale wywoła go przecięcie dwóch wiązek lub przekroczenie minimalnego czasu przecięcia jednej z nich.

Systemy detekcji zakopywane w ziemi

Typowe systemy detekcji zakopywane w gruncie działają na zasadzie wykrywania wibracji lub zaburzeń objętościowych pól elektromagnetycznych. Składają się z okablowania detekcyjnego schowanego pod powierzchnią gruntu wzdłuż granicy terenu. Kabel wykrywający wibracje przenosi sygnał (elektryczny lub optyczny) o określonej częstotliwości. Jeśli obszar nad nim zostanie naruszony, częstotliwość przesyłanego sygnału zmieni się, co system przekształca w sygnał alarmu. W przypadku systemów wolumetrycznych sygnał przesyłany przez zakopany kabel tworzy niewidzialne elektromagnetyczne pole detekcji wrażliwe na zakłócenia spowodowane przez obiekt przechodzący bezpośrednio nad kablem lub w odległości 1,5 m z obu jego stron. Systemy te umożliwiają uzyskanie bardzo precyzyjnego obszaru detekcji, ale mają tę wadę, że kabel musi zostać fizycznie przeniesiony, jeśli obszar detekcji się zmieni.

Problemem jest też to, że mogą generować alarmy spowodowane przesunięciem gruntu, zalaniem wodą i innymi zmianami. Mimo że systemy te można dostroić tak, aby ignorowały obiekty poniżej określonego ciężaru, nie są one w stanie odróżnić np. człowieka od dużego zwierzęcia. Mogą być również narażone na wibracje spowodowane pobliskim ruchem ulicznym lub dużymi pojazdami i są podatne na zakłócenia EMI i RF. Rozwiązań tych zwykle nie stosuje się w przypadku długich obwodów ze względu na koszty instalacji.

Systemy radarowe

Radary zapewniają dozór obszaru w czasie rzeczywistym, wykrywają i śledzą obiekt w każdych warunkach atmosferycznych. Zastosowane jako element ochrony obwodowej PIDS mogą efektywnie dozorować znaczny teren, wykrywać i śledzić obiekt zbliżający się do granicy zabezpieczonego obszaru i dostarczać na bieżąco informacje o jego dokładnej lokalizacji. Stanowią atrakcyjną pozycję produktową ze względu na ich wysoką efektywność pokrycia (tj. wielkość dozorowanego obszaru do kosztów).

Najlepszym miejscem ich instalacji jest duży otwarty teren. Zaletą radaru w porównaniu z omówionymi wcześniej rozwiązaniami

Bariery mikrofalowe i podczerwieni

Zalety	Wady
Mikrofale rozchodzą się wolumetrycznie i mają duży zasięg detekcji	Wymagają płaskiego terenu, nie nadają się do miejsc pofałdowanych i ze wzniesieniami
Bariery IR mogą być stosowane w niewielkich strefach ze względu na bardzo wąską wiązkę	Są nieodpowiednie w miejscach, gdzie występują duże i częste opady deszczu, a drenaż nie radzi sobie z odprowadzaniem wód opadowych lub w ogóle go nie ma
Warunki atmosferyczne zazwyczaj nie stanowią problemu, ale ulewny deszcz może powodować fałszywe alarmy	Jak w przypadku każdej technologii punkt-punkt przestrzeń między czujnikami musi być wolna od roślinności, gruzu i innych obiektów, które zakłóciłyby „linię widzenia”
Bariery IR są odpowiednie dla długich, płaskich obszarów	Zasięgi barier IR w dużym stopniu zależą od warunków atmosferycznych
	Bariery MV wymagają odpowiednio dużej przestrzeni detekcyjnej z dala od potencjalnych zakłóceń

Systemy mikrofonowe

Zalety	Wady
Prosty montaż wzdłuż linii granicznej ogrodzenia	Wymaga dokładnego uziemienia wszystkich metalowych obiektów w pobliżu
Odpowiednie dla długich ogrodzeń	Ulewny deszcz może początkowo wzbudzać uciążliwe alarmy, zanim system się zaadaptuje
Podążanie za krzywizną terenu	Duże ruchome obiekty metalowe (np. pojazdy) w pobliżu czujnika mogą wzbudzać alarmy
Łatwo konfigurowalny wzorzec detekcji, który można dostosować do wielu sytuacji	System może być podatny na EMI i RF
Możliwość wykorzystania algorytmów adaptacyjnych w celu zminimalizowania fałszywych alarmów, a także klasyfikacji zdarzeń alarmowych (wspinaczka, cięcie itp.)	Nieodpowiedni w pobliżu dróg

Systemy detekcji zakopywane w ziemi

Zalety	Wady
Ukrycie systemu utrudnia potencjalnemu intruzowi jego znalezienie. Cała instalacja jest bardziej estetyczna	Możliwa podatność na uciążliwe fałszywe alarmy spowodowane przesunięciem gruntu, zalaniem wodą i wibracjami
Precyzyjne wykrywanie – większość systemów może zlokalizować miejsce naruszenia bariery z dokładnością do 3 m	Podatność na zakłócenia EMI i RF
Możliwość umieszczenia pod różnymi powierzchniami	Problemy z rozróżnianiem obiektów (zwierzę, osoba lub pojazd)
Skuteczność wykrywania pełzających intruzów	Koszt instalacji

jest możliwość wykrycia potencjalnego intruza poza chronionym obwodem, co pozwala na szybką reakcję dotyczącą ewentualnego zagrożenia.

Radar zapewnia wysoki poziom detekcji naruszeń i umożliwia ich ocenę. Zaawansowane algorytmy już teraz klasyfikują obiekt na podstawie skutecznej powierzchni odbicia *(Radar Cross Section* – RCS) i prędkości przemieszczania. Informacje o wykryciu przez radar można wykorzystać do skierowania kamery PTZ w miejsce wykrytego obiektu i w ten sposób śledzić intruza.

Kamery dozorowe

Połączenie kamer do dozoru wizyjnego oraz oprogramowania do detekcji ruchu poszerzyło zakres i możliwości rozwiązań ochrony obwodowej, umożliwiając przejście od prostej detekcji do złożonej analizy wtargnięć. Kamery termowizyjne powiązane z narzędziami do analizy wideo mogą zapewnić skuteczny dozór i monitoring w każdych warunkach oświetleniowych oraz w niemal każdych warunkach atmosferycznych. Za ich pomocą możliwe jest rozróżnienie rodzajów obiektów, przesłanie powiadomienia alarmowego na podstawie określonego zbioru warunków, takich jak kierunek i prędkość przemieszczania się osoby lub pojazdu. Kamery wizyjne również dają taką możliwość (choć nie są w stanie wykrywać obiektów z takiej odległości, z jakiej umożliwiają to kamery termowizyjne), ale potrzebują źródła światła. Kamery termowizyjne natomiast nie dorównują kamerom światła widzialnego pod względem stopnia odwzorowania szczegółów do oceny i identyfikacji. Dlatego często łączy się oba rodzaje urządzeń. Kamera termowizyjna odpowiada za detekcję i alarmy, a kamera pracująca w paśmie widzialnym zapewnia szczegółowość niezbędną podczas śledzeniu celu.

Wymienione w artykule systemy nie zamykają zbioru rozwiązań stosowanych w ochronie obwodowej – stanowią „wyciąg" najczęściej stosowanych. Coraz częściej do ochrony perymetrycznej są wykorzystywane także drony zdolne do monitorowania obszaru wokół obiektu. Bezzałogowy pojazd wyposażony w kamery wysokiej rozdzieczości może być zdalnie sterowany przez operatora kontrolującego sytuację w czasie rzeczywistym z dowolnego miejsca na świecie. Drony są również bardzo skutecznym narzędziem do szybkiego reagowania w przypadku alarmu. Mogą błyskawicznie przemieścić się do miejsca zdarzenia, przesyłając operatorowi obraz sytuacji.
Niestety, drony są stosowane nie tylko przez służby ochrony. Drugą stroną medalu jest wykorzystywanie bezzałogowych statków powietrznych przez przestępców. W odpowiedzi na to powstały… systemy antydronowe, które również mogą stanowić element ochrony perymetrycznej.
Pamiętajmy przy tym, że to służby ochrony obiektu pozostają najważniejszym elementem systemu ochrony i twórzmy nowoczesne zabezpieczenia wedle zasady: „Człowiek bez techniki jest bezbronny, technika bez człowieka jest bezużyteczna". ●

Kamery wizyjne

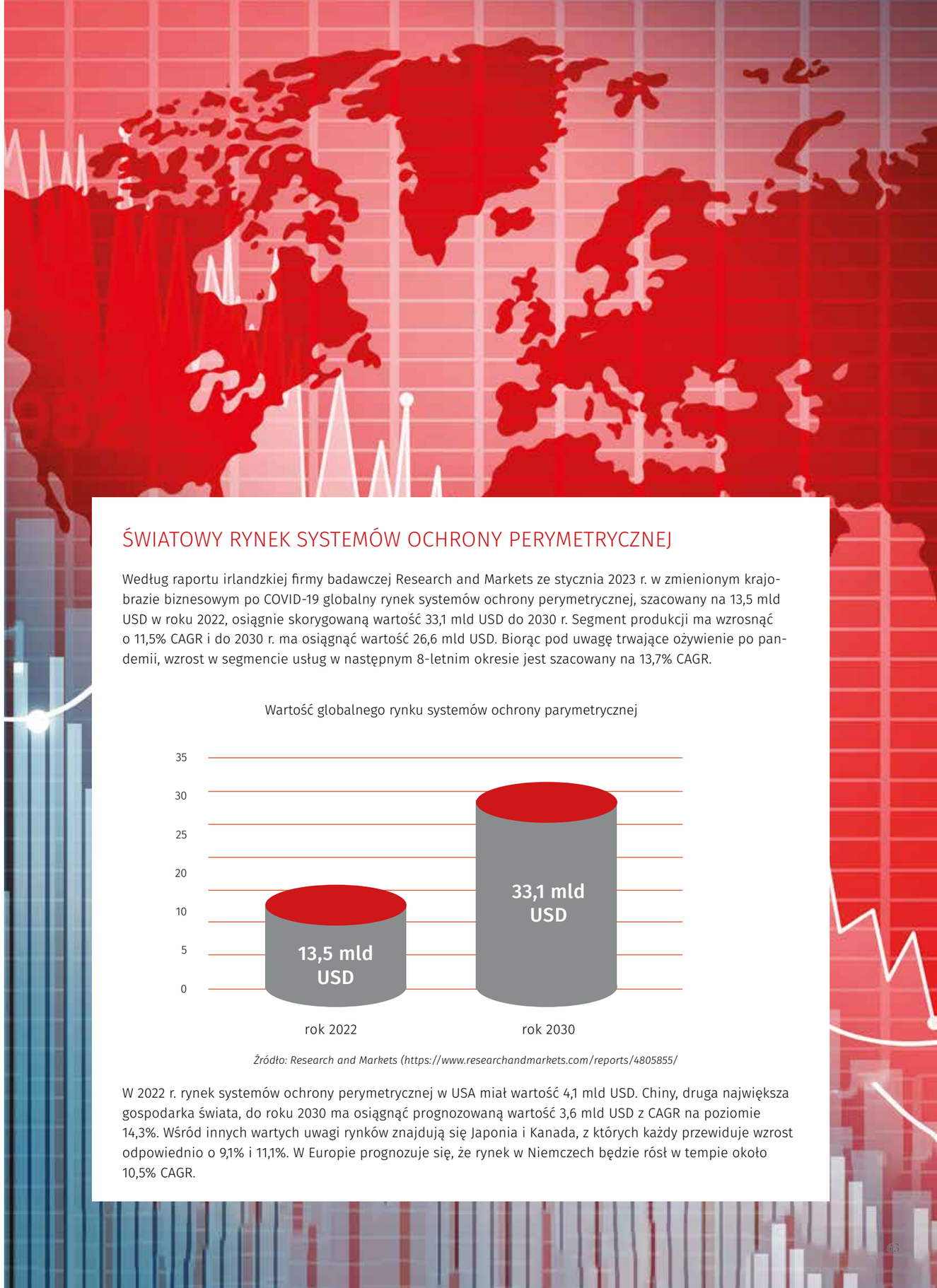
Zalety	Wady
Kamery typu dzień/noc dostarczają wysokiej jakości obrazów, o ile natężenie światła będzie wystarczające	Bez dodatkowego oświetlenia kamery typu dzień/noc stracą obraz, nawet pracując w trybie nocnym
Gdy poziom oświetlenia spada poniżej pewnego progu, kamery d/n mogą wykorzystywać bliską podczerwień, aby uzyskać wysoko kontrastowy obraz czarno-biały	Krótszy zakres detekcyjny w porównaniu z kamerami termowizyjnymi
Skuteczniejsza klasyfikacja obiektów niż w kamerach termowizyjnych	Do optymalnej pracy zaleca się zewnętrzny oświetlacz

Radary

Zalety	Wady
Skuteczne w dzień i w nocy	Wymagają płaskiego terenu, nie nadają się do miejsc o zróżnicowanej wysokości, pagórkowatych
Śledzą wykryte cele – na zewnątrz i wewnątrz obwodu	Podatność na zakłócenia w przypadku stosowania w ograniczonych obszarach – najlepiej stosować na szerokich, otwartych przestrzeniach
Działają poprawnie we mgle i przy większości warunków pogodowych	
Dokładne wykrywanie przestrzenne obiektów w czasie rzeczywistym	
Wykrywanie z oceną	

Kamery termowizyjne

Zalety	Wady
Do pracy nie potrzebują dodatkowego oświetlenia	Niska rozdzielczość
Mniejsza podatność na warunki atmosferyczne (mgła, deszcz, śnieg itp.) niż kamer pracujących w paśmie widzialnym	Mogą mieć problemy w ciepłym klimacie, gdzie temperatura gruntu jest zbliżona do temperatury ciała człowieka – może to utrudnić operatorowi dostrzeżenie intruza i wpłynąć na zdolność analizy wideo do działania zgodnie z wymaganiami
Daleki zakres detekcyjny	Przy bardzo intensywnych mgłach (klasa IIIa, IIIb wg ILS) może nastąpić redukcja zasięgów detekcyjnych – dotyczy ogniskowych 35 mm



ŚWIATOWY RYNEK SYSTEMÓW OCHRONY PERYMETRYCZNEJ

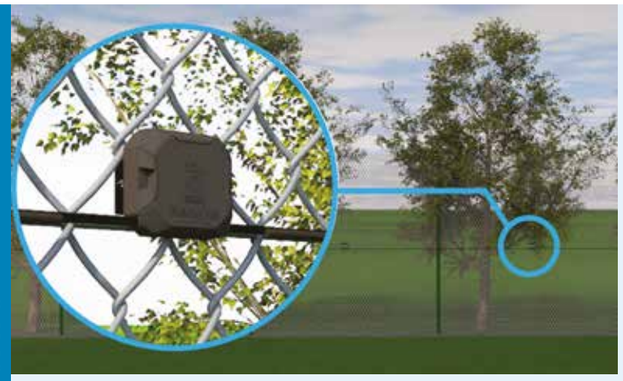
Według raportu irlandzkiej firmy badawczej Research and Markets ze stycznia 2023 r. w zmienionym krajobrazie biznesowym po COVID-19 globalny rynek systemów ochrony perymetrycznej, szacowany na 13,5 mld USD w roku 2022, osiągnie skorygowaną wartość 33,1 mld USD do 2030 r. Segment produkcji ma wzrosnąć o 11,5% CAGR i do 2030 r. ma osiągnąć wartość 26,6 mld USD. Biorąc pod uwagę trwające ożywienie po pandemii, wzrost w segmencie usług w następnym 8-letnim okresie jest szacowany na 13,7% CAGR.

Wartość globalnego rynku systemów ochrony parymetrycznej

Źródło: Research and Markets (https://www.researchandmarkets.com/reports/4805855/

W 2022 r. rynek systemów ochrony perymetrycznej w USA miał wartość 4,1 mld USD. Chiny, druga największa gospodarka świata, do roku 2030 ma osiągnąć prognozowaną wartość 3,6 mld USD z CAGR na poziomie 14,3%. Wśród innych wartych uwagi rynków znajdują się Japonia i Kanada, z których każdy przewiduje wzrost odpowiednio o 9,1% i 11,1%. W Europie prognozuje się, że rynek w Niemczech będzie rósł w tempie około 10,5% CAGR.

Atline



Fusion P2P – dualny system napłotowy

Fusion P2P jest dualnym systemem napłotowym, łączącym technologię piezoelektryczną i MEMS. Jest zbudowany ze sterownika i czujników zbierających sygnały o wibracjach pojawiających się na ogrodzeniu. Dane te są wysyłane do sterownika, który je analizuje i zgłasza alarm w razie wykrycia próby przejścia przez ogrodzenie lub jego przecięcia, odgięcia czy odkręcenia.
Podstawową zaletą, bezpośrednio wynikającą z zastosowania dwóch technologii detekcji wibracji, jest możliwość zainstalowania Fusion na prawie wszystkich rodzajach ogrodzeń metalowych i ścian. To, że sygnały z każdego czujnika są identyfikowalne, a więc analizowane oddzielnie, oznacza również, że system może być w ramach jednej instalacji montowany na różnych typach ogrodzeń.

Wyjątkową cechą systemów P2P oferowanych przez firmę Atline jest też funkcja autodiagnozy. System na bieżąco sprawdza stan każdego czujnika i magistrali, a w razie wykrycia jakichkolwiek problemów zgłasza to użytkownikom. Dzięki tej funkcji regularna konserwacja jest zbędna, co zmniejsza całkowity koszt posiadania systemu.
Fusion P2P występuje w trzech wersjach – Lite, Standard i Pro. Wszystkie wykorzystują te same czujniki i oferują te same możliwości ich konfiguracji. Wersja Light umożliwia podłączenie do 100 czujników, Standard do 300 czujników, natomiast wersja Pro pozwala łączyć wiele sterowników w konfiguracji redundantnej pętli – przy takiej instalacji przecięcie lub uszkodzenie kabla nie powoduje przerwy w działaniu systemu.
Fusion P2P jest dostarczany z połączonymi fabrycznie odcinkami czujników i okablowanym sterownikiem. Takie przygotowanie pozwala zdecydowanie zredukować błędy instalacyjne i zapewnia bezawaryjność pracy. Czujniki systemu są objęte 5-letnią gwarancją producenta.
Integracja z systemami zarządzającymi lub VSS może odbywać się z wykorzystaniem przekaźników lub protokołów komunikacyjnych w modelu TCP/IP.

Więcej na: www.atline.pl/oferta

Axis Communications

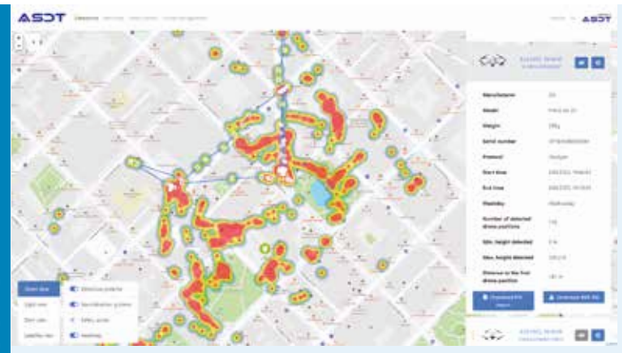
Kamera wideoradarowa AXIS Q1656-DLE

Gwarancja ochrony przed włamaniami na dużym obszarze i niezawodne wykrywanie przez całą dobę, 7 dni w tygodniu dzięki połączeniu dwóch zaawansowanych technologii: wizyjnej i radarowej. To wyjątkowe urządzenie zapewnia zaawansowaną klasyfikację obiektów opartą na głębokim uczeniu, umożliwiając wykrywanie i wizualizację na wyższym poziomie.
Innowacyjne urządzenie łączy analizę obrazowo-radarową w AXIS Object Analytics. Analiza wizyjna precyzyjnie lokalizuje i klasyfikuje obiekty dzięki funkcji głębokiego uczenia. Analiza radarowa dodaje pomiar odległości i prędkości, klasyfikację opartą na głębokim uczeniu oraz sygnaturę radaru i charakterystykę ruchu obiektów.

Inteligentny zintegrowany system obsługuje powiadomienia w najkorzystniejszy sposób, w zależności od tego, co jest najbardziej odpowiednie do okoliczności. Można wybrać minimalizację fałszywych alarmów albo dokładną analizę wszystkich zdarzeń aby niczego nie przeoczyć.
Kamera wideoradarowa AXIS Q1656-DLE łączy dwa urządzenia klasy premium – kamerę linii Q zapewniającą obraz o doskonałej użyteczności ze zintegrowanym radarem. Jest to pierwsze tego typu urządzenie w ofercie Axis. Radar wykrywa obiekty na dużych obszarach przy słabym lub zerowym oświetleniu. Wizualizuje prędkość i odległość poruszających się obiektów bezpośrednio w widoku aplikacji. Ponadto z radaru można korzystać niezależnie od sterowania kamerą PTZ, która pracuje samodzielnie.
Kamera jest wytrzymała i odporna na warunki atmosferyczne. Ma też wbudowane funkcje chroniące system przed cyberatakami. Axis Edge Vault zabezpiecza identyfikator urządzenia Axis i upraszcza uwierzytelnianie produktów Axis w sieci. Wybór AXIS Q1656-DLE wiąże się z niższymi kosztami instalacji i eksploatacji – jest jedno urządzenie do zainstalowania, jedno przyłącze kablowe, jeden adres IP i jedna licencja na oprogramowanie do zarządzania sygnałem wizyjnym (VMS).

Więcej na: www.axis.com/pl-pl

Dilectro



ASDT SENDES – system detekcji, identyfikacji, śledzenia i neutralizacji dronów

System antydronowy hiszpańskiej firmy **ASDT** to wiodące rozwiązanie C-UAS *(Counter Unmanned Aerial Systems)* na rynku. Pozwala zabezpieczyć przestrzeń powietrzną wokół infrastruktury krytycznej.
System bazuje na autorskiej technologii **SENDES** polegającej na dekodowaniu w czasie rzeczywistym częstotliwości radiowych, na których pracują drony najpopularniejszych marek (DJI, Parrot, Yuneec, WiFi, RemoteID). System składa się z czterech modułów – systemu detekcji (**SENDES DAU**), neutralizacji (**SENDES SJ**), interfejsu użytkownika (**SENDES Gate**) oraz serwerowego ekosystemu wspieranego przez AI (**SENDES Core**).
Moduł DAU pozwala na detekcję, identyfikację i śledzenie dronów na odległości do 10 km. Oprogramowanie informuje użytkownika m.in. o marce drona, numerze seryjnym, wysokości i prędkości lotu oraz pozycji startu i pilota. Opcjonalny **Moduł SJ** umożliwia neutralizację drona przez selektywne zakłócenie transmisji oraz GPS, wywołujące rozpoczęcie procedury jego powrotu do domu lub awaryjnego lądowania.
Moduły SENDES DAU i SJ wymagają do działania jedynie dostępu do zasilania i Internetu (przez złącze RJ-45 lub moduł LTE). Możliwy jest montaż wolnostojący, sufitowy lub na wieży. System jest zabezpieczony przed warunkami atmosferycznymi.
Obsługa odbywa się przez przeglądarkę z dowolnego urządzenia – komputera, tabletu czy smartfonu. Oprogramowanie oferuje intuicyjną obsługę z filtrowaniem dronów FoF (*Friend or Foe*) i generowanie raportów w formatach PDF, KML i XLSX. Pozwala też tworzyć strefy i otrzymywać automatyczne powiadomienia o ich przekroczeniu, z opcją automatycznej lub ręcznej neutralizacji.
System SENDES został z powodzeniem wdrożony m.in. w obiektach przemysłowych, rządowych, wojskowych, więzieniach czy na granicach. Był testowany na lotnisku Chopina w Warszawie, gdzie swoim zasięgiem objął ścisłe centrum miasta. System jest zgodny z Europejską Dyrektywą 2013/25/UE oraz STANAG 2345 Edition 4.

Więcej na: https://dilectro.pl/

Hikvision

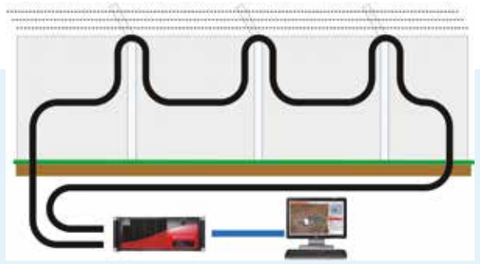
DS-2TD2667-35_PY – bi-spektralna kamera do ochrony obwodowej infrastruktury krytycznej

Kamera typu bullet jest wyposażona w dwa przetworniki: wizyjny o rozdzielczości 2688 x 1520 pikseli (4 Mpix) oraz termowizyjny o rozdzielczości 640 x 512 pikseli (model DS-2TD2667-35/PY) lub 384 x 288 (model DS-2TD2637-35/PY). Ma wbudowany promiennik IR do wsparcia detekcji wizyjnej w trybie obserwacji nocnej.
Czułość termiczna kamery (NETD – *Noise Equivalent Temperature Difference)* wynosi ≤35mk (@ 25°C, F# = 1.0) i pozwala na odczyt temperatury z dokładnością do ± 8°C w zakresie -20°C do 150°C. Oprócz pomiaru temperatury kamera wykrywa zagrożenia pożarowe, może wykryć palący się obiekt wielkości 20 x 20 cm z odległości 350 m.

Dzięki wbudowanej analizie wideo i technologii głębokiego uczenia kamera wykrywa wzorce pojazdu lub człowieka, wysyła alarm o zdarzeniu (wtargnięcie w strefę lub przekroczenie linii) zaobserwowanym z odległości 721 m (pojazd) i 257 m (człowiek).
Dla przetwornika termowizyjnego kamera ma obiektyw o ogniskowej 35 mm, co w powiązaniu z czułością termiczną pozwala na: detekcję człowieka z 1029 m, rozpoznanie człowieka z 257 m, identyfikację człowieka ze 129 m.
W tej rodzinie kamer dostępne są też modele z obiektywami o mniejszej ogniskowej: 25 lub 15 mm. W przypadku jednoczesnej obserwacji z obu przetworników można skorzystać z funkcji obraz w obrazie lub Fusion, czyli przenikanie się obrazu wizyjnego i termowizyjnego, aby uzyskać maksymalną szczegółowość w ramach jednego obrazu.
Do zasilania kamery można stosować różne źródła, np. zasilacze AC w zakresie od 18 do 30 V lub DC w zakresie od 9 do 15 V. Może też być zasilana przez POE 802.3af klasy 3. Kamera ma zabezpieczenie antykorozyjne NEMA4X, klasę szczelności obudowy IP67 i odporności mechanicznej IK10 oraz ochronę przed przepięciami i wyładowania atmosferycznymi do 6 kV. Na najdroższy element kamery, czyli przetwornik termowizyjny, Hikvision oferuje 10 lat gwarancji.

Więcej na www.hikvision.com/pl/

Linc Polska

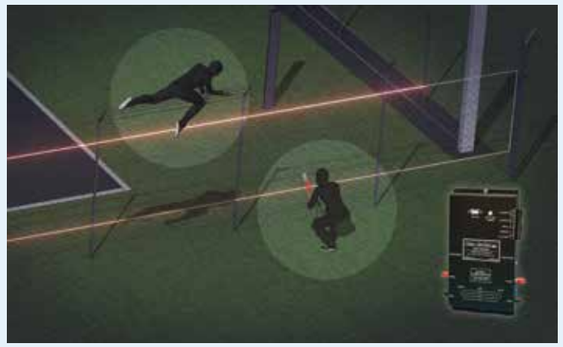


Światło lasera i sieci neuronowe na straży bezpieczeństwa

Światłowód, jako medium transmisyjne, wrósł już w codzienność dzisiejszego świata, jednak możliwości jego wykorzystania w innych celach nadal są duże. Jednym z potencjalnych zastosowań jest użycie światłowodu jako czujnika wtargnięć w ochronie obwodowej. Technologia ta jest rozwijana m.in. przez australijską firmę Future Fibre Technologies.
Rozwiązania Future Fibre Technologies pozwalają na zabezpieczenie zarówno najmniejszych obiektów komercyjnych, takich jak rezydencje czy tereny firm, obiekty małej architektury krytycznej (np. farmy solarne, punkty BTS, GPZ), jak i ważnej infrastruktury państwowej (granice, lotniska, bazy wojskowe, elektrownie, magistrale przesyłowe). Dzięki szerokiemu portfolio rozwiązań łatwo dobrać sterownik do wymagań zabezpieczanego obiektu, który zapewni dokładność wykrycia w strefie do ±12 m, a nawet ±4 m). Światłowód może być zarówno montowany na ogrodzeniu, jak i zakopany w ziemi, tworząc fizyczne i wirtualne zabezpieczenie.
Najnowszy sterownik Aura Ai-X jest oparty na technologii uczenia maszynowego bazującej na sieciach neuronowych *(deep learning)*. Łączy zalety swoich poprzedników z możliwością ciągłego doskonalenia, zmieniając sposób postrzegania wskaźników prawdopodobieństwa detekcji (POD) i niechcianych alarmów (NAR).
Wyjątkowa dokładność klasyfikacji zdarzeń, której efektem jest najwyższy wskaźnik POD, przy niemal zerowych niechcianych alarmach jest nieporównywalny z żadnym innym systemem komercyjnym. Technologia głębokiego uczenia w czasie rzeczywistym eliminuje uciążliwe fałszywe alarmy związane z warunkami atmosferycznymi, przy wskaźnikach POD powyżej 95%.
Wszystkie te cechy sprawiają, że rozwiązania Future Fibre Technologies spełniają wymagania bezpieczeństwa najbardziej wymagających obiektów. W połączeniu z systemem telewizji dozorowej tworzą skuteczną tarczę zabezpieczającą obiekt przed wtargnięciem intruza oraz zapewniającą natychmiastową reakcję służb ochrony.

Więcej na www.linc.pl

Optex



Fiber SenSys z technologią światłowodową OPTEX

OPTEX Fiber SenSys to rozwiązania oparte na aktywnym światłowodzie mocowanym do istniejącego ogrodzenia metalowego lub muru. Najbardziej zaawansowane systemy mogą być stosowane jako detektory zakopywane.
Technologia światłowodowa OPTEX skutecznie wykrywa wszelkie próby przecinania siatki, wspinanie się po ogrodzeniu, czołganie pod nim lub przewiercanie przez ścianę. Może być zastosowana na ogrodzeniach od 50 m do ponad 100 km. Systemy zostały zaprojektowane do pracy w trudnych i niebezpiecznych środowiskach zewnętrznych, mogą też zdalnie komunikować się i pobierać zasilanie.
Fiber SenSys to wytrzymałe i iskrobezpieczne rozwiązania odporne na zakłócenia elektromagnetyczne i radiowe, wilgoć, sól, promieniowanie UV, a nawet uderzenia pioruna. Gwarantują niezawodną pracę we mgle, zapyleniu czy ciemności i mogą być stosowane w strefach zagrożenia wybuchem. Zaawansowane algorytmy pozwalają określić rodzaj zakłócenia, odróżniając intruzów od fałszywych wzbudzeń generowanych np. przez wiatr.
Fiber SenSys charakteryzują się możliwością konfiguracji wielu parametrów strojenia i łatwą integracją z innymi elektronicznymi systemami zabezpieczeń.
Bardzo ważną zaletą czujników światłowodowych OPTEX jest ich zdolność do dokładnej lokalizacji intruza nawet w przypadku najdłuższych zabezpieczanych obwodów (granic terenu). Strefy alarmowe można ustawić tak, aby uruchamiały kamery, kontrolę dostępu lub systemy zarządzania budynkiem.
Oferta Fiber SenSys obejmuje systemy dedykowane do zaawansowanych aplikacji w dużych budynkach komercyjnych, obiektach wojskowych i infrastruktury krytycznej. Przewagą ekonomiczną tej technologii jest niska cena zakupu, a także niewielki koszt eksploatacji, szczególnie widoczny w przypadku rozległych instalacji (jeden punkt montażowy).

Więcej na www.optex-europe.com/pl

PRODUS S.A.

Stabilność działania i ograniczenie liczby fałszywych alarmów

Napłotowy piezoelektryczny system ochrony obwodowej PERIDECT+ znalazł szerokie zastosowanie w ochronie infrastruktury krytycznej w Polsce ze względu na jego wysoką stabilność działania oraz zdolność do ograniczenia liczby fałszywych alarmów do absolutnego minimum.
System wykrywa intruza bezpośrednio na granicy chronionego obszaru, dzięki czemu operator zyskuje czas na skuteczną reakcję. Zapewnia mniejsze ryzyko penetracji obiektu przez intruza, skuteczniej chroniąc przed zniszczeniami niż wykrywanie włamań w strefie wewnętrznej obiektu.
PERIDECT+ może być instalowany na ogrodzeniach metalowych wszystkich typów. Zastosowanie niezawodnej i bardzo czułej technologii piezoelektrycznej wykrywania, w połączeniu z cyfrową obróbką sygnałów na poziomie detektora DSP+ i zaawansowanymi algorytmami analizy danych cyfrowych przez jednostkę zarządzającą CUP+, pozwala uzyskać najwyższe prawdopodobieństwo detekcji intruza przy wyjątkowo niskiej liczbie fałszywych alarmów. System potrafi skutecznie eliminować fałszywe alarmy związane ze zjawiskami atmosferycznymi i ruchem drogowym lub kolejowym przy ogrodzeniu.
PERIDECT+ umożliwia budowę systemu w architekturze pętlowej SafeGuarded, indywidualną kalibrację detektorów DSP+ i możliwość monitorowania alarmów z bardzo dużą dokładnością. System daje, do wyboru, implementację linii detekcji w wersji standardowej, wandaloodpornej, zakopywanej lub EX. Praca systemu oparta na sieci TCP/IP umożliwia zdalny monitoring działania i natywną integrację z systemami współpracującymi (VSS/CCTV, PSIM). Pozwala to na zabezpieczenie rozległych terenów lub monitorowanie wielu obiektów rozproszonych.
System jest certyfikowany do zastosowań zarówno cywilnych, jak i militarnych. Może być używany do ochrony ogrodzonych obszarów wysokiego ryzyka, do stopnia 4. wg normy PN-EN 50131-1 i spełnia stosowne wytyczne stawiane obiektom wojskowym.

Więcej na www.produs.com.pl/

PRODUS S.A.

System barier dualnych AvantgardeDT

Bariery dualne AvantgardeDT wyróżniają się parametrami, które predestynują je do stosowania w ochronie zewnętrznej obiektów infrastruktury krytycznej, gdzie są trudne warunki pracy, a jednocześnie wymagana jest stabilna praca systemu i niski współczynnik fałszywych alarmów.
System barier dualnych AvantgardeDT działa na zasadzie korelacji technologii podczerwieni IR z technologią mikrofalową MW. Technologia wielosensorowa jest zarządzana przez pracującą w sieci procesorową jednostkę zarządzania CPU. Każdy komplet bariery dualnej składa się z zespołu (od 3 do 5) dwukierunkowych modułów podczerwieni oraz modułu mikrofalowego K-Band zainstalowanych w aluminiowych kolumnach o wysokości od 2 do 6 m. Dzięki opatentowanej technologii dwukierunkowej modułów IR oraz zastosowaniu modułu planarnej anteny mikrofalowej zapewniono eliminację fałszywych alarmów związanych z zewnętrznymi zjawiskami atmosferycznymi (gęsta mgła, opady śniegu, deszczu, gradu), opadającymi liśćmi, pojawianiem się małych zwierząt itp.
Bariera dualna zabezpiecza obszar pomiędzy jej kolumnami rozmieszczonymi w odległości do 200 m. Dualizm pracy zapewnia liniową detekcję intruza (technologia IR) oraz wolumetryczne monitorowanie terenu (technologia MW), z możliwością zaprogramowania alarmu wstępnego.
Dzięki cyfrowej analizie sygnałów system barier dualnych umożliwia analizę kierunku przekroczenia linii detekcji, tworzenie scenariuszy alarmowania oraz wykorzystanie cyfrowych algorytmów poprawiających pracę systemu w zmiennych warunkach atmosferycznych.
Bariery dualne AvantgardeDT pracujące w sieci TCP/IP zapewniają łatwe zabezpieczenie złożonych i rozległych obszarów, takich jak porty morskie, obiekty energetyczne, magazyny gazu lub paliw, obiekty penitencjarne, wojskowe czy serwerownie. Umożliwiają zdalny monitoring parametrów wraz z integracją do systemów nadrzędnych. Bariery mają certyfikację GRADE-4 (4. stopień zabezpieczenia).

Więcej na www.produs.com.pl/

Nowe wyzwania potrzebują nowych kompetencji

Ochrona obiektów infrastruktury krytycznej jest jednym z najważniejszych elementów zapewnienia bezpieczeństwa społeczeństwu. Wydarzenia w Ukrainie pokazują, że to właśnie infrastruktura krytyczna najczęściej staje się celem ataków.
Jakub Sobek, ekspert PZPO

W czasie narastających napięć geopolitycznych i oczywistego zaangażowania się Polski w wydarzenia za naszą wschodnią granicą obiekty IK są oczywistym celem np. ataków terrorystycznych lub innych działań przestępczych. Planując systemy zabezpieczeń technicznych lub działania ochronne, wiemy, że choć w wypadku operacji wojennych mogą się one okazać niewystarczające, to sprawdzą się np. do zapobiegania akcjom sabotażowym.

Choć systemy zabezpieczenia technicznego są jednym z najistotniejszych elementów ochrony obiektów, to nie możemy zapominać, że także pracownicy ochrony mają ogromne znaczenie dla zapewnienia bezpieczeństwa takim obiektom, jak elektrownie, rafinerie, wodociągi, porty lotnicze, a także sieci energetyczne i telekomunikacyjne. Współczesne systemy zabezpieczeń mają na celu ułatwienie pracy pracownikom ochrony oraz poprawę jakości i skuteczności działań podejmowanych na rzecz zapewnienia bezpieczeństwa obiektom infrastruktury krytycznej.

Współczesne systemy zabezpieczeń to kompleksowe rozwiązania, które pozwalają na kontrolę dostępu, monitorowanie obiektów, wykrywanie zagrożeń i ich sygnalizowanie. W skład tych systemów wchodzą różnego rodzaju urządzenia, takie jak kamery, czujniki ruchu, systemy ochrony perymetrycznej, czujniki dymu, systemy oświetleniowe czy zamki elektromagnetyczne. Systemy te pozwalają na uzyskanie dokładnej informacji o sytuacji na obiekcie i umożliwiają szybką reakcję w przypadku zagrożenia. Mogą skutecznie opóźnić atak na chroniony obiekt.

Rola pracownika ochrony w ciągu wielu lat zupełnie się zmieniła. W obiektach infrastruktury krytycznej pracownik jest wspomagany przez nowoczesne systemy zabezpieczenia technicznego. Najważniejsze jednak, by towarzysząc pracownikom ochrony, pomagały im w codziennych zadaniach, w minimalnym stopniu angażując uwagę pracownika, dzięki czemu będzie on mógł skupić się na zadaniach kluczowych. Wiadomo, że ze względu na rosnące koszty zatrudnienia często jeden pracownik ochrony jest odpowiedzialny za wiele zadań.

Technologia powinna zatem przekazywać pracownikowi czytelne informacje o zdarzeniach alarmowych i o tym, co dzieje się w strzeżonym przez niego obiekcie. To jest możliwe tylko dzięki integracji różnych systemów oraz prezentowaniu na monitorze wyłącznie niezbędnych informacji. Najlepiej, gdy będzie to jeden monitor, a nie pięć czy dziesięć, choć i tak niejednokrotnie bywa.

Z pomocą przychodzi oprogramowanie *Physical Security Information Management* (PSIM) integrujące wiele systemów zabezpieczeń, w tym kamery monitoringu, systemy alarmowe, kontrolę dostępu czy detektory pożarowe na jednej platformie. Dzięki temu służby ochrony mają możliwość zarządzania całością systemu z jednego miejsca, co pozwala na szybką reakcję w przypadku zagrożenia. Jedną z głównych zalet PSIM jest możliwość automatycznego wykrywania zagrożeń. Dzięki integracji wielu systemów zabezpieczeń PSIM jest w stanie dokładnie analizować dane z różnych źródeł i wykrywać nieprawidłowości.

Zaletą oprogramowania PSIM jest również możliwość przeprowadzania analizy zdarzeń. System zbiera dane na temat wszystkich zdarzeń i pozwala na ich szczegółową analizę. Dzięki temu służby ochrony mogą w przyszłości zapobiec podobnym zdarzeniom. Analiza danych pozwala również na identyfikację obszarów, w których bezpieczeństwo jest szczególnie wystawione na szwank, co umożliwia podejmowanie działań mających na celu zwiększenie jego poziomu.

Przy planowaniu systemów zabezpieczenia technicznego istotne jest, aby taki system był podzielony na wyraźne strefy: strefa perymetryczna, teren obiektu oraz wnętrze chronionych budynków. Każda z tych stref powinna być zwizualizowana i dla każdej z nich powinny zostać opracowane reguły reagowania w przypadku pojawienia się intruza.

Im wcześniej zostanie wykryta obecność osób niepożądanych, tym lepiej. Dzięki temu można zyskać na czasie i podjąć takie działania, które pozwolą zneutralizować potencjalny atak. Na konieczność szybkiego wykrycia intruza, czyli już w strefie perymetrycznej, zwraca uwagę Rządowe Centrum Bezpieczeństwa, które przygotowało rekomendacje dla infrastruktury krytycznej. To właśnie ogrodzenie zostało uznane za miejsce skutecznego wykrycia intruza. Uzupełniając system ochrony o radary i drony, zasięgiem detekcji można objąć teren poza granicami obiektu.

Integracja systemów perymetrycznych z oprogramowaniem PSIM pozwala na precyzyjną wizualizację miejsca wtargnięcia na obiekt. Dzięki temu operator systemu widzi na mapie, w którym miejscu pojawiło się zagrożenie. Dodatkowe zastosowanie systemów wizyjnych, obsługiwanych również za pomocą PSIM, pozwala na przeprowadzenie skutecznej weryfikacji.

Samojezdne roboty, algorytmy sztucznej inteligencji, lidary i systemy rozpoznawania nietypowych zdarzeń już teraz są stosowane w sektorze ochrony, a ich rozwój nabierze tempa. Pracownicy ochrony będą musieli zdobyć umiejętności w zakresie obsługi tych technologii i praktycznego ich wykorzystania. To olbrzymia szansa dla tych firm ochrony, które na czas przeszkolą swoich pracowników i postawią na ich nowe kompetencje wykorzystujące najnowsze technologie. ●

» *Integracja systemów perymetrycznych z oprogramowaniem PSIM pozwala na precyzyjną wizualizację miejsca wtargnięcia na obiekt. Dzięki temu operator systemu widzi na mapie, w którym miejscu pojawiło się zagrożenie. Dodatkowe zastosowanie systemów wizyjnych, obsługiwanych również za pomocą PSIM, pozwala na przeprowadzenie skutecznej weryfikacji.* «

Polski Związek Pracodawców Ochrona
ul. Koszykowa 61, 00-667 Warszawa
biuro@pzpochrona.pl
www.pzpochrona.pl

Mapa inwestycji

Przedstawiamy mapę dużych inwestycji, które są w trakcie realizacji lub dopiero się rozpoczną, a których termin ukończenia nie upływa przed trzecim kwartałem 2023 roku.
Adela Prochyra, a&s Polska

Aby zachować ciągłość działania przedsiębiorstwa muszą planować nowe projekty. Przedstawiona mapa inwestycji może być pomocna w zdobyciu atrakcyjnych kontraktów, które przyniosą zysk i pozwolą na kontynuowanie działalności w kolejnych latach.
Wybrane inwestycje, przydatne z punktu widzenia firm branży zabezpieczeń technicznych, będziemy prezentować cykliczne w każdym wydaniu „a&s Polska".

WARBUD

Co: MODERNIZACJA TARASÓW ORAZ ODBUDOWA SKRZYDŁA PÓŁNOCNEGO
Gdzie: Zamek Książąt Pomorskich w Szczecinie
Kiedy: 30 miesięcy od 25 sierpnia 2022 — 1

Co: PRZEBUDOWA BUDYNKÓW B I C SAMODZIELNEGO PUBLICZNEGO WOJEWÓDZKIEGO SZPITALA ZESPOLONEGO
Gdzie: Szczecin
Kiedy: II kwartał 2024 — 2

Co: CENTRUM TECHNOLOGICZNIE WSPOMAGANEJ REHABILITACJI OGÓLNOUSTROJOWEJ DLA DZIECI
Gdzie: Poznań
Kiedy: III kwartał 2024 — 3

Co: ŁÓDZKIE CENTRUM TOKSYKOLOGII DLA SAMODZIELNEGO PUBLICZNEGO ZAKŁADU OPIEKI ZDROWOTNEJ CENTRALNEGO SZPITALA KLINICZNEGO UNIWERSYTETU MEDYCZNEGO W ŁODZI
Gdzie: Łódź
Kiedy: III kwartał 2023 — 4

Co: NADBUDOWA NAD BUDYNKIEM GŁÓWNYM WOJSKOWEGO SZPITALA KLINICZNEGO Z POLIKLINIKĄ SPZOZ
Gdzie: Lublin
Kiedy: IV kwartał 2024 — 5

STRABAG

Co: UKOŃCZONY STAN SUROWY BUDYNKU AMBASADY RP W BERLINIE
Gdzie: Unter den Linden, Berlin
Kiedy: III kwartał 2023 — 6

Co: PRZEJŚCIE GRANICZNE MALHOWICE-NIŻANKOWICE – UZUPEŁNIENIE INFRASTRUKTURY DROGOWEJ DLA FUNKCJONUJĄCEGO PRZEJŚCIA W MEDYCE
Gdzie: Malhowice [woj. Podkarpackie]
Kiedy: I kwartał 2024 — 7

BUDIMEX:

Co: FARMA WIATROWA MAGNOLIA
Gdzie: Drachowo
Kiedy: pierwsze półrocze 2023 — 8

Co: FARMA FOTOWOLTAICZNA
Gdzie: Drachowo
Kiedy: do końca 2023 — 9

POLIMEX MOSTOSTAL

Co: NOWY BUDYNEK MAGAZYNOWO ADMINISTRACYJNY CENTRALNEGO MAGAZYNU ZBIORÓW MUZEALNYCH (CMZM) WRAZ Z TOWARZYSZĄCYM MU PARKIEM I NIEZBĘDNĄ INFRASTRUKTURĄ
Gdzie: Lesznowola
Kiedy: listopad 2024 — 10

Co: NOWE JEDNOSTKI WYTWÓRCZE – W TYM ŹRÓDŁO KOGENERACYJNE W ELEKTROCIEPŁOWNI BYDGOSZCZ II
Gdzie: Elektrociepłownia Bydgoszcz II
Kiedy: I kwartał 2025 — 11

Co: BLOK GAZOWO-PAROWY O MOCY 882 MW W RYBNIKU
Gdzie: Rybnik
Kiedy: grudzień 2026 — 12

MIRBUD

Co: HALA PRODUKCYJNO-MONTAŻOWA DLA PIT-RADWAR S.A. – SPÓŁKI Z POLSKIEJ GRUPY ZBROJENIOWEJ
Gdzie: Kobyłka
Kiedy: październik 2023 — 13

Co: BUDYNEK WIELOFUNKCYJNY DLA AKADEMII MARYNARKI WOJENNEJ IM. BOHATERÓW WESTERPLATT
Gdzie: Gdynia
Kiedy: 32 miesiące od 18 lipca 2022 — 14

Co: KRAKOWSKIE CENTRUM MUZYKI
Gdzie: ul. Piastowska 20, Kraków
Kiedy: czerwiec 2024 — 15

ERBUD

Co: TERMOMODERNIZACJA REKTORATU WARSZAWSKIEGO UNIWERSYTETU MEDYCZNEGO (WUM)
Gdzie: ul. Żwirki i Wigury 61, Warszawa
Kiedy: 06.09.2023 — 16

Co: BUDOWA OBOZOWISKA PRZEJŚCIOWEGO INTERMEDIATE STAGING BASE (ISB) W ŚWIĘTOSZOWIE
Gdzie: Trzebień
Kiedy: do maja 2024 — 17

UNIBEP

Co: KOTŁOWNIA GAZOWA
Gdzie: Ciepłownia Orzysz
Kiedy: IV kwartał 2023 — 18

TORPOL

Co: DWORZEC KOLEJOWY WRAZ Z INFRASTRUKTURĄ KOLEJOWĄ
Gdzie: Olsztyn Główny
Kiedy: lipiec 2023*
*Dopiero w styczniu 2023 rozpoczęły się roboty ziemne — 19

GRUPA ZUE

Co: BUDOWA TERMINALU MULTIMODALNEGO W ZDUŃSKIEJ WOLI KARSZNICACH
Gdzie: Zduńska Wola Karsznice
Kiedy: 31.10.2023 — 20

INSTAL KRAKÓW

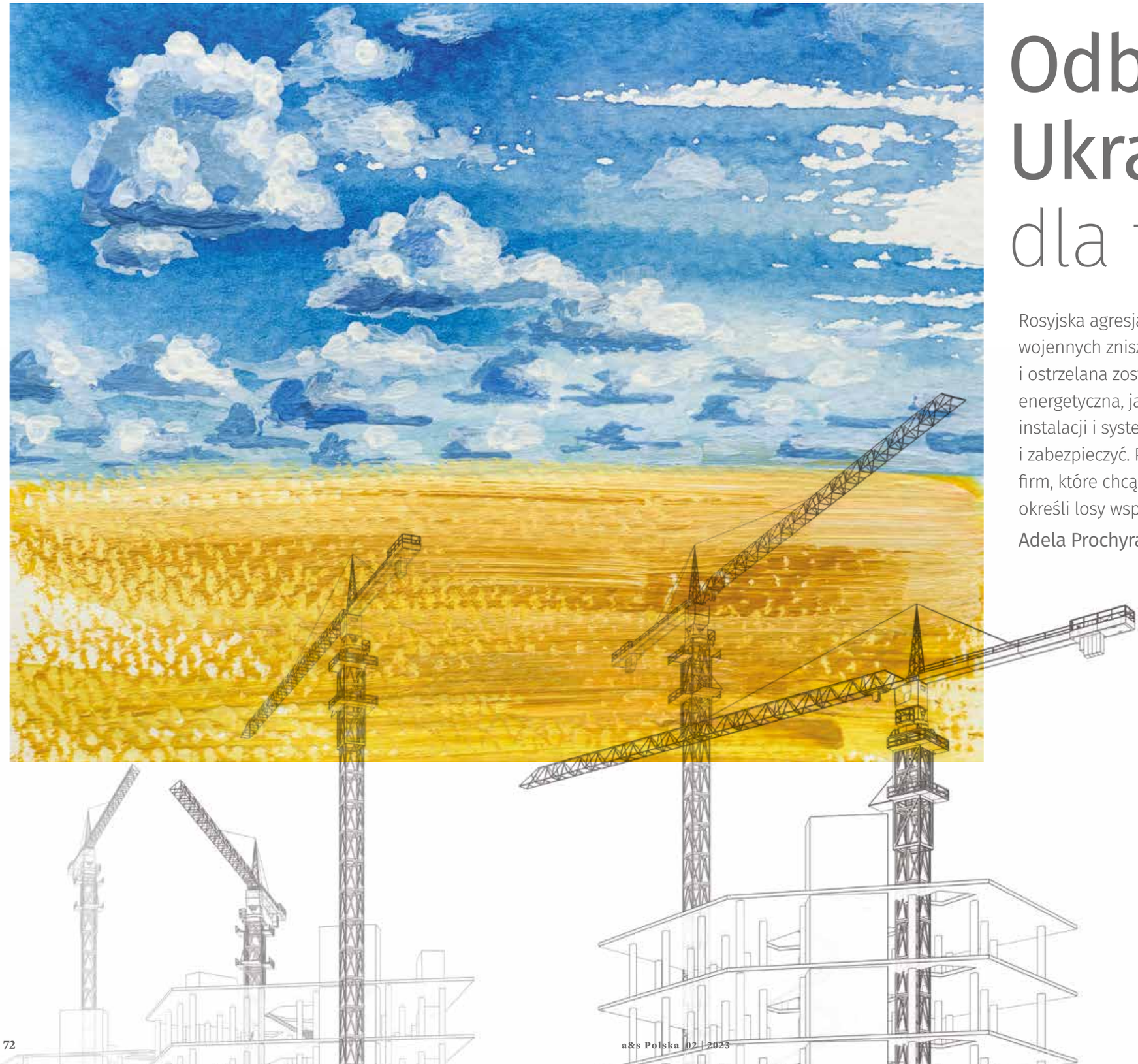
Co: MODERNIZACJA UKŁADÓW POMPOWYCH NA STACJI UZDATNIANIA WODY BIBIELA
Gdzie: Katowice
Kiedy: maj 2024 — 21

Co: MODERNIZACJA KORYT TECHNOLOGICZNYCH ZASILAJĄCYCH OSADNIKI WTÓRNE NA OCZYSZCZALNI ŚCIEKÓW PANEWNIKI W KATOWICACH
Gdzie: Katowice
Kiedy: 20.09.2023 — 22

MOSTOSTAL WARSZAWA

Co: MODERNIZACJA HOTELU KATOWICE
Gdzie: Katowice
Kiedy: 26.06.2024 — 23

Co: TERMINAL CARGO W MIĘDZYNARODOWYM PORCIE LOTNICZYM IM. JANA PAWŁA II KRAKÓW BALICE
Gdzie: Kraków Balice
Kiedy: 23 miesiące od 22 listopada 2022 — 24



Odbudowa **Ukrainy** szansą dla firm polskich?

Rosyjska agresja na Ukrainę trwa już ponad rok. W wyniku działań wojennych zniszczeniu uległa znaczna część kraju – zbombardowana i ostrzelana została infrastruktura zarówno wojskowa, transportowa, energetyczna, jak i cywilna. Oznacza to tysiące budynków, dróg, instalacji i systemów, które trzeba częściowo lub w całości odbudować i zabezpieczyć. Polska jest gotowa przystąpić do działania i zbiera zapisy firm, które chcą pomóc Ukrainie w podniesieniu się z ruin. Ten pakt określi losy współpracy obu krajów na wiele lat.

Adela Prochyra, a&s Polska

Wojna z Rosją trwa, ale równolegle z toczącymi się walkami tworzone są plany odbudowy struktur fizycznych i politycznych Ukrainy. Pomysłów, analiz i strategii wyjścia z kryzysu jest wiele. Powstają na uczelniach, w *think tankach*, a nawet w korporacjach.

Nowy „plan Marshalla" dla Ukrainy

Najważniejsza umowa to ta zawarta w lipcu 2022 r. w Lugano w Szwajcarii podczas międzynarodowej konferencji *Ukraine Recovery Conference* (URC 2022), której organizatorami były Ukraina i Szwajcaria. Wzięli w niej udział reprezentanci ponad 40 krajów i 18 organizacji międzynarodowych. Spotkanie poświęcono omówieniu kwestii planu powojennej odbudowy i dalszego rozwoju Ukrainy, roli partnerów międzynarodowych w tym procesie, priorytetów, metod, a także obszarów odbudowy państwa w zakresie gospodarczym, infrastrukturalnym, społecznym, środowiskowym oraz reform, które można wprowadzić na obecnym etapie. Zakładane działania ujęto w 15 programach sektorowych, składających się z 850 projektów, które mają być realizowane w trzech etapach. W pierwszej kolejności muszą zostać zaspokojone bieżące potrzeby związane z odtworzeniem infrastruktury krytycznej. W drugim etapie, który ma trwać od 2023 do 2025 r., zaplanowano 580 projektów opiewających na kwotę 350 mld USD, w trzecim zaś, który jest rozpisany na lata 2026–2032, 270 projektów o łącznej wartości 400 mld USD. Osią programu modernizacji Ukrainy – obok odbudowy infrastruktury – ma być stworzenie nowoczesnej, energooszczędnej gospodarki opartej w dużej mierze na odnawialnych źródłach energii. Ukraina ze względu na swoje warunki ma szansę zostać europejskim liderem w produkcji zielonej energii.

→

Ustalono także, które państwa będą odpowiedzialne za odbudowę poszczególnych części zniszczonego kraju. Polsce i Włochom przypadła odbudowa Donbasu. Polski Instytut Ekonomiczny, biorąc pod uwagę wielkość tego obszaru i skalę jego zniszczeń, oszacował, że realizowane tam projekty będą odpowiadały za 15–20% całego planu odbudowy Ukrainy i będą mieć wartość 150–200 mld USD.

– *Przedstawiony w Lugano plan jedynie częściowo dotyczy odbudowy. W istocie jest bowiem bardzo ambitnym projektem całkowitej transformacji państwa i gospodarki, szczególnie pod względem infrastruktury* – zaznacza w swojej analizie Sławomir Matuszak z Ośrodka Studiów Wschodnich.

Polska pomoc w odbudowie Ukrainy

– *Straty wywołane zniszczeniami wojennymi w Ukrainie sięgają dziś blisko 800 mld USD. To ciężar nie do udźwignięcia dla kraju, którego PKB według parytetu siły nabywczej oscyluje wokół 500 mld USD. Wsparcie Ukrainy to nasza powinność. Sąsiedztwo geograficzne i biskość kulturowa sprawiają, że Polska jest niejako moralnie zobowiązana do pomocy Ukraińcom w odbudowie ich kraju. Dlatego też rola naszego kraju, Polaków i firm polskich w tym wielkim przedsięwzięciu jest i będzie wiodąca. Zrozumienie wagi tej odpowiedzialności widać w gotowości polskich przedsiębiorców, którzy zgłaszają się do naszej bazy* – mówi Karol Kubica, kierownik biura Polskiej Agencji Inwestycji i Handlu w Kijowie.

Agencja we współpracy z Ministerstwem Rozwoju i Technologii tworzy bazę firm zainteresowanych wzięciem udziału w wielkiej odbudowie. Zgłosiło się do niej już ponad 1,8 tys. podmiotów. – *W projekt zaangażowane są przede wszystkim firmy z branży budowlanej, maszyn i urządzeń, IT/ICT, sprzętu farmaceutycznego i medycznego, spożywczej, motoryzacyjnej, rolniczej oraz rolnictwa. Liczba przedsiębiorstw z sektora security jest niewielka. Być może to się zmieni* – dodaje ekspert PAIH, który jest operatorem programu „Odbudowa Ukrainy". Nabór został uruchomiony w czerwcu 2022 r., odbyły się także konsultacje branżowe dla firm, ale zgłoszenia przyjmowane są nadal – bezterminowo. Przedsiębiorcy mogą zgłaszać się w dowolnym momencie. Formularz zgłoszeniowy dla firm polskich chętnych do współpracy przy odbudowie Ukrainy znajduje się na stronie https://odbudowaukrainy.paih.gov.pl/.

Kandydatury mogą zgłaszać firmy, które:
- są polskimi przedsiębiorstwami;
- deklarują chęć uczestnictwa we współpracy z biznesem na rzecz przygotowań do powojennej odbudowy Ukrainy;
- nie współpracują z rosyjskimi i białoruskimi podmiotami objętymi sankcjami;
- spełniają kryteria zawarte w formularzu zgłoszeniowym.

Do udziału są zachęcani przedsiębiorcy z następujących sektorów:
- budowa i wykańczanie budowli,
- farmaceutyka i sprzęt medyczny,
- rolno-spożywczy,
- motoryzacyjny,
- maszyny i urządzenia,
- IT/TCT,
- energetyczny.

Źródło: https://odbudowaukrainy.paih.gov.pl/formularz-zgloszeniowy/

– *W tym momencie trudno oszacować zapotrzebowanie na usługi oferowane przez branżę security. Jednak, biorąc pod uwagę, że wszyscy liczymy na to, iż proces odbudowy Ukrainy będzie przebiegał w oparciu o rozwiązania i narzędzia stosowane w krajach Unii Europejskiej, należy się spodziewać, że „architekci nowej Ukrainy" sięgną po usługi security, które znajdą zastosowanie w budownictwie mieszkaniowym, budynkach użyteczności publicznej czy też przy realizacji projektów infrastrukturalnych* – zapewnia Karol Kubica z PAIH.

Firmy budowlane, z którymi kontaktowaliśmy się w tej sprawie, są ostrożne w przewidywaniach i deklaracjach. Zapewne będą zapraszać do współpracy firmy zajmujące się bezpieczeństwem budynków i obiektów, o ile dojdzie do współpracy przy odbudowie i pojawi się takie zapotrzebowanie.

Finansowanie: skąd wziąć pieniądze na odbudowę Ukrainy

Chociaż nowy „plan Marshalla" został szczegółowo rozpisany na najbliższe 10 lat, zawiera kompleksowe założenia dotyczące odbudowy państwa w nowoczesnym kształcie i zintegrowania go z Unią Europejską oraz innymi strukturami światowymi, wątpliwości budzi sposób jego finansowania. Źródła, na które liczą ukraińskie władze, to granty, kredyty i inwestycje prywatne. Największy strumień pieniędzy miałby popłynąć z zamrożonych w zachodnich krajach środków należących do rosyjskich oligarchów – aktywa te są szacowane na 500 mld USD – oraz aktywów rosyjskiego Banku Centralnego i Narodowego Funduszu Dobrobytu. Założenie to jest kontrowersyjne, nie opracowano bowiem mechanizmów prawnych pozwalających na konfiskatę majątku jednego kraju i przekazanie go innemu. Przykładowo, Kanada wprowadziła stosowną ustawę, jednak bez zobowiązania do przekazania zarekwirowanych pieniędzy Ukrainie. Wielka Brytania i Komisja Europejska w osobie przewodniczącej Ursuli von der Leyen także zapowiadają opracowanie podobnych rozwiązań, lecz wciąż nie są znane nawet ramy czasowe ich przygotowania. Nie jest tajemnicą, że po wojnie Amerykanie będą chcieli zmonetyzować swoją pomoc udzieloną Ukraińcom w licznych dostawach sprzętu wojskowego.

Znaki zapytania i cała naprzód

Eksperci do spraw stosunków międzynarodowych ostrożnie wypowiadają się na temat realności założeń nowego „planu Marshalla". Kwoty podawane przez władze ukraińskie są olbrzymie, a chęci prywatnego kapitału do inwestowania w zrujnowanym, pozostającym w stanie wojny kraju mogą być przeszacowane. Ukraina jest jednocześnie rynkiem perspektywicznym. Panuje opinia, że będzie to najszybciej rozwijająca się gospodarka Europy. Słowa te padły z ust Andrew Forresta, założyciela Fortescue Metals Group, po rozmowie z Wołodymyrem Zełenskim. Po wizycie w Kijowie przedsiębiorca powołał fundusz Ukraine Green Growth Initiative, który ma inwestować w infrastrukturę i sieci telekomunikacyjne, i zasilił go 750 mln USD. Zainteresowanie tamtejszym rynkiem wykazują także inni giganci, np. fundusz inwestycyjny Black Rock czy Philip Morris International. Kolejka chętnych do odbudowy zniszczonego kraju jest długa, otwarcie mówi się też o tym, że trwa wyścig dyplomatyczny. Kto chce być obecny na tamtym rynku w najbliższych latach, powinien zacząć się na nim pojawiać już teraz.

Niektóre punkty planu wydają się nieadekwatne do sytuacji, np. konieczność uniezależnienia się energetycznego od Białorusi i Rosji (zrobione!) czy budowa obiektów sportowych (niekonieczne). Zasadne wydają się też wątpliwości co do tego, jak i przez kogo środki pieniężne miałyby być rozdzielane. Ukraina jeszcze przed wojną borykała się z ogromnymi problemami z korupcją i wymiarem sprawiedliwości. Zdaniem części jej polityków to Kijów powinien sam dysponować pieniędzmi. Przy tak złożonych i poważnych planach wymagana jest jednak pełna transparentność przy przetargach, dlatego pieniądze na konkretne projekty zapewne będą wydzielane pod nadzorem Komisji Europejskiej.

Mimo wielu niewiadomych politycy zachodni podnoszą konieczność szybkiego włączenia naszego sąsiada w globalne łańcuchy dostaw i jak najszybszą reanimację jego gospodarki. Ogromną rolę ma tu do odegrania biznes światowy i europejski, ze szczególnym wskazaniem na Polskę ze względu na liczne podobieństwa kulturowe, dobre relacje obu krajów oraz, co także bardzo istotne, tak zwaną rentę geograficzną, czyli bezpośrednie sąsiedztwo. Polska być może stanie się hubem wielkiej powojennej odbudowy, skupiającym zarówno rodzime zasoby w postaci firm gotowych wziąć udział w tym przedsięwzięciu, jak i obsługującym firmy zagraniczne, które będą korzystać ze wsparcia lub podwykonawstwa polskich przedsiębiorstw.

Skala zniszczeń – skala odbudowy

Polski Instytut Ekonomiczny podaje, że w wyniku działań wojennych zostało spustoszone ponad 100 tys. km^2 państwa. Dotychczasowe straty liczone są na ok. 136 mld USD (stan na luty 2023 r.), a łączny koszt powojennej odbudowy Ukrainy, jak podaje Europejski Bank Inwestycyjny razem z ukraińskimi władzami, ma wynieść ponad 1 bln USD. Przy czym należy pamiętać, że kwoty te zwiększają się z każdym dniem kontynuowania rosyjskiej agresji i ukraińskiej defensywy. Dodajmy, że straty związane ze śmiercią tysięcy ukraińskich obywateli oraz z emigracją kilku milionów ukraińskich kobiet z dziećmi są niepoliczalne.

Nie ma mowy, aby Ukraińcy sami poradzili sobie z przedsięwzięciem o tak dużej skali. Kraj jest obecnie zbyt osłabiony gospodarczo, a skala zniszczeń zbyt duża. Wiele firm ukraińskich zakończyło lub przerwało działalność bądź przeniosło się za granicę kraju. Wiele z nich, m.in. dzięki wydatnej pomocy naszego państwa, zakotwiczyło się w Polsce (24,1 tys. firm z kapitałem ukraińskim, z czego 13,8 tys. zarejestrowano po wybuchu wojny) i tu planuje prowadzenie działalności bez względu na dalsze losy konfliktu (deklaruje tak 66% nowo przybyłych). Jednocześnie, wedle wstępnych szacunków podanych w styczniu przez tamtejsze Ministerstwo Finansów, PKB Ukrainy zmalało o 30,4%. Bank Światowy wyliczył z kolei spadek na 35%, a pod uwagę należy także wziąć ogromną 30-procentową inflację trawiącą gospodarkę ukraińską i gigantyczny wzrost ubóstwa, będący bezpośrednim rezultatem wojny – z 18 do 60% w ciągu ostatniego roku!

Na poziomie gospodarczym ucierpiały przede wszystkim dwa kluczowe sektory: rolnictwo i przemysł, a także infrastruktura. Władze ukraińskie – siłą rzeczy, gdy trwają walki – są skupione na zapewnianiu swoim obywatelom doraźnej pomocy wojskowej i medycznej oraz łataniu niedoborów energetycznych. Bieżąca działalność jest w dużej mierze finansowana z doraźnych dotacji pomocowych z Zachodu. Spodziewana jest pomoc z Unii Europejskiej – Komisja Europejska zapowiedziała zamiar wyasygnowania 500 mln euro na odbudowę Ukrainy. Kiedy to jednak nastąpi, nie wiadomo. Ośrodek Studiów Wschodnich prognozuje, że mimo wielu znaków zapytania, przede wszystkim dotyczących sposobów finansowania odbudowy, część projektów ma szansę na realizację w najbliższym czasie. Obiecujące są zwłaszcza te inwestycje, które mają zwiększyć przepustowość granicy z Unią, gdyż jest to jedyna trasa wymiany handlowej z Ukrainą. Moralny obowiązek wsparcia zaatakowanego sąsiedniego kraju idzie tu w parze z globalnymi interesami i daje nadzieję na rozwój współpracy zarówno między krajami, jak i poszczególnych firm, np. z branży security. Swojej szansy powinny upatrywać głównie w budownictwie, źródłach odnawialnych i rolnictwie. ●

Lepiej zapobiegać niż gasić

Problematykę związaną z bezpieczeństwem pożarowym serwerowni można podzielić na dwa podstawowe aspekty. Pierwszym jest ograniczenie możliwości wybuchu pożaru oraz zabezpieczenie serwerowni przed wniknięciem pożaru z zewnątrz. Drugim – minimalizacja skutków pożaru, jeżeli już do niego dojdzie.

Michał Zalewski

Zacznijmy od rzeczy banalnej, czyli tego, że serwerownia nie może być magazynem przedmiotów niezwiązanych z jej funkcją. Bardzo często dokonując przeglądów, zwracałem uwagę, że w pomieszczeniu znajdują się rzeczy zbędne, typu łatwo palne kartony z folią i styropianami składowanymi na szafach krosowych. Czy serwerownia koniecznie musi być miejscem lokalizacji elektrycznej rozdzielnicy administracyjnej? Pamiętam kilka dyskusji na projektach na ten temat i brak zrozumienia konieczności ograniczenia takich rozwiązań. Usunięcie takiej rozdzielnicy to jedna z metod ograniczenia ryzyka wybuchu pożaru. Jednocześnie pomieszczenie o takim charakterze powinno być wydzielone ogniowo od reszty budynku, nawet jeżeli nie wymagają tego warunki ochrony ppoż. i przepisy.

A jeżeli pożar już wybuchnie?

Najprostszym rozwiązaniem jest wyposażenie serwerowni w… odpowiednią ręczną gaśnicę. Czytelnik prawdopodobnie teraz się uśmiecha, a bardziej krytyczny przerywa lekturę. Zapewniam, że taki początek rozważań ma sens. Bo przecież gaśnica odpowiednio użyta będzie skuteczna, pod warunkiem że ktoś zauważy pożar na czas, będzie umiał z gaśnicy skorzystać i najważniejsze – znajdzie się w serwerowni, gdy dojdzie do pożaru. Czyli wystarczy gaśnica? To oczywiste, że nie. Ten proces powinien być zautomatyzowany, gdyż nie zagwarantujemy obecności odpowiednich osób przez cały czas.

Na rynku są dostępne urządzenia zwane panelami gaszącymi instalowanymi w obudowach szaf i rozdzielnic, wyposażone w elementy pozwalające na automatyczne wykrycie pożaru i wypływ czynnika gaśniczego wewnątrz obudowy gaszonego urządzenia.

Najczęściej takie urządzenie to gaśnica wyposażona w specjalny przewód będący pod ciśnieniem, wzrost temperatury powoduje rozszczelnienie tego przewodu i wypływ gazu. To rozwiązanie ma pewną wadę – wprawdzie wykrywa zwiększenie temperatury (powyżej 70–100°C w zależności od producenta), jednak w serwerowniach mamy do czynienia najczęściej z pożarami urządzeń elektrycznych, w których faza tlenia się przebiega bardzo długo i w jej trakcie nie dochodzi do wydzielania dużej ilości ciepła. Samo wykrycie wzrostu temperatury to za mało. Dlatego urządzenia wyposażone w czujniki dymu to znacznie lepsze rozwiązanie, jednak również niepozbawione wad. Dla prawidłowego zdławienia pożaru wymagany jest odpowiednio długi czas działania czynnika gaszącego na źródło pożaru. A skuteczne gaszenie utrudnia wentylacja zarówno szafy, jak i całego pomieszczenia. Bez zatrzymania przepływu powietrza nie osiągniemy zamierzonego celu. Ostatnia wada takich rozwiązań: nie można ich zastosować np. do gaszenia UPS lub innych urządzeń z obudowami fabrycznymi. Efekt jest więc marny: zgasimy szafę serwerową, ale stojący obok UPS bez ochrony jest zagrożeniem.

Czy zatem dwa rozwiązania opisane wyżej są niewłaściwe? Absolutnie nie. Ich podstawową zaletą jest to, że są tanie, a pamiętajmy, że koszt rozwiązania powinien być adekwatny do wartości chronionego dobra.

> *» Dla prawidłowego zdławienia pożaru wymagany jest odpowiednio długi czas działania czynnika gaszącego na źródło pożaru. «*

Dla ochrony danych o znacznej wartości trzeba stosować rozwiązania zapewniające większą skuteczność, a przede wszystkim niezawodność. Producenci gazów gaszących oferują różnorodne rodzaje gazów gaszących wykorzystywanych w systemach gaszenia, od rozwiązań opartych na zasadzie obniżania stężenia tlenu w pomieszczeniach po oparte na molekularnym odbieraniu energii kinetycznej od cząsteczek źródeł pożaru. To obszerny temat, którego tutaj poruszać siłą rzeczy nie będziemy, a w tym artykule skoncentruję się na automatyce systemów gaszeniowych: od projektowania, przez instalację, po uruchomienie i eksploatację.

Projektowanie instalacji ppoż. dla serwerowni

System gaszenia gazem składa się z detektorów dymu, zestawu ręcznego uruchamiania gaszenia oraz powstrzymywania akcji gaśniczej, sygnalizatorów gaszenia gazem, sterowników klap odciążających (nie mylić z klapami odcinającymi wentylację bytową), trzymaczy drzwi oraz linii wyzwalającej zawory systemu gaszenia, aż po centralę sterującą gaszeniem. Podczas projektowania każdego elementu należy zwracać uwagę na specyfikę gaszenia gazem.

Detektory dymu

W planowaniu detekcji należy zwrócić uwagę na wymagany w tych systemach wyższy niż w systemach wykrywczych dymu poziom odporności na fałszywe alarmy. Aby to osiągnąć, najczęściej stosuje się podwojenie liczby czujników oraz zastosowanie koincydencji dwuczujnikowej dla gaszenia. Przypominam, by nie mylić koincydencji z potwierdzeniem alarmu przez drugą czujkę dla przyspieszenia odliczania czasu T2. To dwie różne rzeczy. W rozwiązaniach opartych nie na czujnikach adresowalnych pętlowych, ale na liniach konwencjonalnych należy zwracać uwagę na redundancję okablowania dla czujników oraz konieczność zapewnienia odporności ogniowej linii detekcyjnej.

Zestaw ręcznego uruchamiania gaszenia

Projektując dobór elementów do zestawu ręcznego uruchamiania gaszenia, należy zwrócić uwagę na… przycisk wstrzymujący wyzwalanie środka gaśniczego. To niezwykle istotne, ponieważ inaczej projektuje się algorytm pracy dla przycisków wstrzymujących gaszenie do czasu ich zwolnienia, a inaczej dla przycisków wstrzymujących gaszenie do czasu ponownego naciśnięcia przycisku uruchamiającego gaszenie. Przyjęte rozwiązanie będzie zależało od rodzaju wybranego standardu PN/EN, VDS czy NFPA.

Te różnice wpływają na sposoby oprogramowania linii sterującej klapami odciążającymi, których zadaniem jest otwarcie pomieszczenia, by umożliwić rozprężenie się gazu gaszącego, a następnie zamknięcie go w celu utrzymania przez odpowiednio dłuższy czas wymaganego stężenia czynnika gaszącego.

Sterowanie klapami odciążającymi

Ważnym aspektem projektowym jest również moment ustalania wyzwolenia akcji gaszenia. Pierwszy sposób to uruchomienie →

gaszenia po obliczonym (lub zmierzonym) czasie otwarcia klapy odciążającej. Drugi to kontrola położenia siłownika klapy oraz wyzwolenie akcji gaszenia dopiero po potwierdzeniu otwarcia klapy. Oba rozwiązania mają zwolenników i przeciwników.

W przypadku niedużych pomieszczeń, gdzie nie istnieje ryzyko zbytniego wzrostu ciśnienia w pomieszczeniu, oba rozwiązania są poprawne. Z kolei dla wielkich serwerowni, gdzie dochodzi do rozprężenia się dużej ilość gazu w krótkim czasie, a same klapy odciążające również mogą być spore, wyzwolenie akcji gaszenia przy zamkniętej klapie (lub w trakcie jej domykania) może spowodować albo zakleszczenie klapy podczas akcji, albo trwałe rozszczelnienie pomieszczenia poprzez np. uszkodzenie drzwi lub w skrajnym przypadku ściany.

Ważnym elementem koniecznym do uwzględnienia w wytycznych projektowych systemu gaszenia jest zapewnienie odpowiedniej ażurowości sufitu podwieszanego oraz podłogi podniesionej (to znacznie częstsze). Temat niezwiązany z automatyką gaszeniową, ale warto o tym pamiętać.

Jakich sygnalizatorów należy używać w systemach gaszących? Czy można używać sygnalizatorów akustycznych mimo ryzyka zakłócenia sygnałów ewakuacyjnych DSO? Moim zdaniem – tak. Można rozważać użycie sygnalizatorów akustycznych działających poniżej poziomu przyjętego w DSO jako poziom hałasu. W obiektach bez DSO nie ma przeciwskazań, jednak dla odróżnienia zagrożenia użyłbym innego rodzaju sygnalizatorów niż w SSP.

Automatyczna kontrola linii zasilających sterowanie urządzeniem

Innym ważnym aspektem projektowym jest automatyczna kontrola linii zasilających sterowanie urządzeniami wchodzącymi w skład systemu ppoż. (siłowniki klap odcinających, zawory instalacji gazowej, sygnalizatory). Kontrola ta powinna wykrywać zarówno zwarcia, jak i przerwy w okablowaniu.

Jak powinna przebiegać komunikacja z budynkowym systemem wykrywczym dymu. Spotkałem się z pomysłem ograniczenia wymiany informacji pomiędzy tymi systemami i wprowadzenia dodatkowej detekcji do chronionych pomieszczeń. Nie jest to rozwiązanie prawidłowe, a główną jego wadą jest brak pewności co do zamknięcia klap odcinających na wentylacji bytowej, które muszą być sterowane z systemu sygnalizacji pożaru (SSP), a obiektywnie wpływają na szczelność pomieszczenia serwerowni i, co za tym idzie, skuteczność akcji gaszenia. Dlatego nie wprowadzamy czujników dymu (niepotrzebne dublowanie funkcji), klapami odcinającymi sterujemy z systemu SSP i prawidłowo projektujemy interfejs: usterka, alarm I stopnia, alarm II stopnia i potwierdzenie akcji gaśniczej.

Montaż, instalacja, testy

Prawidłowość wykonania linii systemu sterowania, odpowiednio dobrane okablowanie zapewniające skuteczność działania urządzeń, kontrola prawidłowości doboru urządzeń, szczegółowy precyzyjny scenariusz zadziałania urządzeń jako wytyczne do opracowania algorytmu to elementy podobne np. do uruchamiania systemu SSP. Co jest specyficzne dla systemów gaszenia?

Bardzo ważnym elementem procesu uruchamiania systemu gaszenia jest wstępna elektromechaniczna kontrola urządzeń składających się na system: klapy odciążające z siłownikami, zawory na instalacji gazowej, trzymacze drzwiowe i samozamykacze zapewniające szczelność drzwi. Odpowiednio wyregulowane drzwi są równie ważne dla skutecznej akcji gaszenia jak dobór czynnika gaszącego.

Algorytm sterowania systemem jest bardzo skomplikowany, gdyż uwzględnia nie tylko koincydencję detekcji, sposób użycia przycisku STOP, ale też np. różne czasy otwarcia i domknięcia klap odciążających i otwarcia zaworów instalacji gazowej. Dlatego procedura testów uruchomieniowych powinna dokładnie uwzględniać każdy element tego procesu, włącznie z potwierdzonymi zmierzonymi czasami poszczególnych akcji. Dopiero wtedy można cały system uznać za skutecznie przetestowany.

Nie zapominajmy, że o bezpieczeństwie serwerowni decyduje jeszcze jeden element: szczelność gaszonego pomieszczenia. Sprawdzenie tej kwestii musi poprzedzać przekazanie obiektu do eksploatacji.

> *Instalator powinien zadbać o opracowanie instrukcji obsługi, eksploatacji i serwisowania urządzeń.*

Instalator powinien zadbać o opracowanie instrukcji obsługi, eksploatacji i serwisowania urządzeń. Taka instrukcja musi dokładnie opisywać zainstalowane urządzenia, sposoby ich obsługi (zwracam uwagę na przyciski STOP gaszenia i dwie możliwości ich użycia), ale również wytyczne eksploatacyjne (np. zakaz składowania materiałów palnych, zasłaniania klap odciążających czy otworów zapewniających ażurowość podłogi podniesionej). Nie mniej istotne jest opracowanie dla użytkownika precyzyjnych wytycznych dotyczących serwisowania urządzeń i np. wskazanie konieczności kontroli działania nadzoru nad okablowaniem do urządzeń wykonawczych.

A może podejść do tematu inaczej?

Dobranie odpowiedniego systemu gaszenia nie jest rzeczą łatwą. Zaprojektowanie skutecznej instalacji wymaga pracy projektowej wielu specjalistów, wybrania właściwych, niejednokrotne kosztownych urządzeń. Nie jest tani też ich serwis. Może więc rozważyć alternatywne rozwiązania? Może odpowiedzią jest dynamicznie rozwijający się *cloud computing*? Należy pamiętać, że koszt danego rozwiązania musi być adekwatny do wartości chronionego dobra. Zastosowanie zabezpieczeń należy zatem dopasować do wartości chronionych danych, a to, wraz z alternatywą, jaką jest chmura obliczeniowa, nakłada na inwestora, projektanta systemu informatycznego firmy, ale też projektanta systemu gaszenia obowiązek wspólnego przeanalizowania nowych wyzwań i możliwości.

Czytelnicy, którzy znają moje podejście do tematyki, wiedzą, że nieobce mi są śmiałe i kontrowersyjne tezy. Robię to celowo, by pobudzić wszystkich do dodatkowej analizy i wyrwania się z szablonowego myślenia o poruszanych kwestiach. To ważna cecha nowoczesnego projektowania, myślenia o problemach zmieniającego się świata oraz przygotowania do zupełnie nowych, jakże czasami zaskakujących wyzwań. ●

Michał Zalewski

Absolwent Politechniki Gdańskiej i studiów podyplomowych Zarządzania Projektami Politechniki Warszawskiej. W branży od 25 lat, od 13 lat niezależny konsultant, inżynier uruchomieniowy.

Bezpieczeństwo SUG-G w serwerowni a reduktory stałowypływowe

Jeden nieprawidłowo funkcjonujący element może zakłócić działanie całego systemu. Na ten aspekt powinni zwrócić uwagę m.in. projektanci instalacji ppoż., pamiętając, że czasami mniej znaczy lepiej.

Zastanawiając się nad jak najlepszą ochroną przeciwpożarową takich miejsc jak serwerownia czy data center, warto sobie odpowiedzieć na kilka pytań. Czy dodanie do stałych urządzeń gaśniczych gazowych (SUG-G) elementów, które podnosząc złożoność systemu jednocześnie obniżają jego niezawodność, nie spowoduje zmniejszenia bezpieczeństwa serwerowni? Czy reduktory stałowypływowe, instalowane na każdej butli w SUG-G na gazy obojętne, nie stanowią właśnie takich elementów obniżających niezawodność działania systemu?

Prześledźmy działanie awaryjne SUG-G spowodowane defektem jednego zespołu zaworowego. Porównajmy takie działanie w dwóch typach SUG-G, tj. wyposażonych:

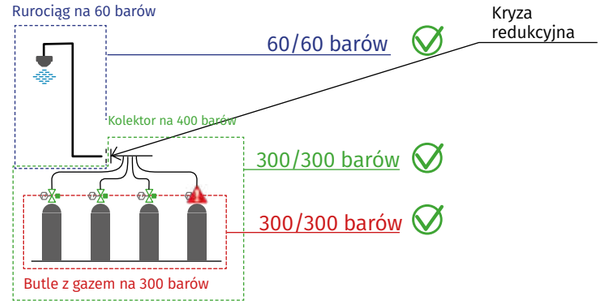
- w jeden reduktor kryzowy zainstalowany w kolektorze zbiorczym,
- w wiele reduktorów stałowypływowych zainstalowanych po jednym na każdej butli.

W tej sytuacji należy się zastanowić:

- jakie mogą być skutki „przeskoku" ciśnienia gazu z 300 barów z jednej tylko butli do kolektora zaprojektowanego na dopuszczalne ciśnienie robocze 60 barów i dalej do rurociągu też zaprojektowanego na 60 barów?
- czy reduktory stałowypływowe są tak bardzo niezawodne, że przedstawiony scenariusz awaryjny można wykluczyć?

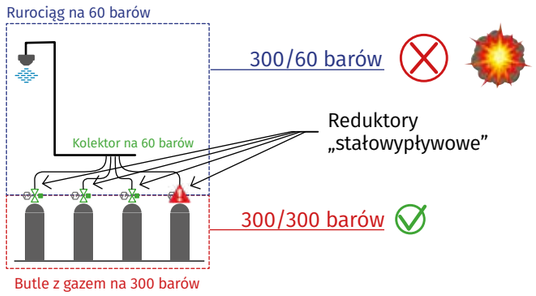
Co zatem stanowi realne zagrożenie:

- gaz o ciśnieniu 300 barów w układzie zaprojektowanym na maksymalne ciśnienie robocze 400 barów (testowe 600 barów)
- gaz o ciśnieniu 300 barów (czy nawet np. 200 barów) w układzie zaprojektowanym na maksymalne ciśnienie robocze 60 barów (testowe – 90 barów)?



W systemie SUG-G z kryzą

Redukcja ciśnienia do 60 barów odbywa się tylko na jednej kryzie zainstalowanej w kolektorze. Do kolektora zaprojektowanego na ciśnienie robocze 400 barów (testowe – 600 barów) wpływa gaz z butli pod ciśnieniem 300 barów, a wypływa pod ciśnieniem 60 barów. Następnie gaz trafia do układu zaprojektowanego na ciśnienie robocze 60 barów (testowe – 90 barów).



W systemie SUG-G stałowypływowym

Redukcja ciśnienia do 60 barów odbywa się na każdym zaworze redukcyjnym butli. Po zredukowaniu ciśnienia gaz trafia do układu zaprojektowanego na ciśnienie robocze 60 barów (testowe – 90 barów).

W rurociągach zarówno systemu kryzowego, jak i systemu stałowypływowego występują przyrosty i spadki ciśnień. W przypadku systemu stałowypływowego amplituda zmian ciśnień jest znacznie mniejsza, co pozwala na stosowanie mniejszej powierzchni odciążeń w klapach upustowych lub uzyskanie krótszego czasu wyzwolenia. Czy ten argument jest wystarczający wobec niezawodności i bezpieczeństwa, aby decydować się na system stałowypływowy? ●

DEKK Fire Solutions
ul. Dawidowska 23, 05-500 Zamienie
http://dekk.pl
info@dekk.pl

Integral Remote: narzędzia zdalnego dostępu do systemu Integral EvoxX firmy Schrack Seconet w świetle wymagań normy PN-EN 50710:2022-06

Rozwiązania do zdalnego nadzorowania, zarządzania i obsługi systemów bezpieczeństwa pożarowego oraz innych systemów bezpieczeństwa są coraz powszechniej stosowane. Wpływ na popularyzację i znaczne zwiększenie usług świadczonych zdalnie wymusiły po części pandemia COVID-19 i związane z nią ograniczenia, ale istotny był także intensywny rozwój rozwiązań do zdalnej pracy, nauki oraz generalnie komunikacji.

Wykorzystanie narzędzi do zdalnego dostępu umożliwia firmom odpowiedzialnym za wdrożenia i obsługę instalacji bezpieczeństwa pożarowego zoptymalizowanie procesów związanych ze świadczonymi usługami w zakresie całego cyklu eksploatacji instalacji z jednoczesnym optymalnym zarządzaniem zespołem specjalistów w ramach organizacji.

Wiele czynności może być wykonanych zdalnie bez potrzeby wizyty w obiekcie, a gdy jest ona niezbędna, dzięki zdalnemu dostępowi służby serwisowe mogą najpierw zdalnie przeprowadzić podstawową diagnostykę, by potem przyjechać już z wymaganymi częściami zapasowymi potrzebnymi np. w razie awarii komponentu instalacji. Zdalny dostęp daje wiele możliwości, ale i niesie wiele zagrożeń. Ważnym momentem było opublikowanie 17 czerwca 2022 normy PN-EN 50710:2022-06 zawierającej wymagania dotyczące zapewnienia bezpiecznych usług zdalnych w systemach ochrony przeciwpożarowej oraz w systemach zabezpieczeń technicznych.

Norma określa przede wszystkim wymagania w zakresie organizacji świadczenia usług z wykorzystaniem narzędzi i rozwiązań do zdalnego dostępu, wymagania techniczne, jakie powinna spełniać infrastruktura techniczna (informatyczna) w celu realizacji usług, oraz zakres czynności i ewentualne ograniczenia dotyczące operacji wykonywanych zdalnie. Od strony organizacyjnej warunki współpracy i procedury postępowania powinny być dokładnie określone w umowie podpisanej między klientem końcowym a firmą świadczącą usługi na podstawie przeprowadzonej wcześniej analizy ryzyka związanej z uruchomieniem usług wykonywanych zdalnie. Umowa powinna określać m.in.

- instalacje i urządzenia objęte zdalnym dostępem,
- zakres świadczonych usług, operacje lub testy, które mają być przeprowadzone na odległość,
- ograniczenia czasowe aktywnych sesji zdalnych w zakresie funkcji odczytu (nadzoru), sterowania (obsługi serwisowej) i zapisu (zmiany konfiguracji) zgodnie z oceną ryzyka;
- odpowiedzialność za sprawność działania infrastruktury technicznej,
- proces autoryzacji wymagany dla wykonywanych operacji oraz sposób komunikacji,
- wszelkie dodatkowe warunki wymagane przez ubezpieczyciela czy inne służby, np. straż pożarną w przypadku instalacji bezpieczeństwa pożarowego,
- granice odpowiedzialności po stronie dostawcy usług w zakresie infrastruktury informatycznej.

W normie zostały również wskazane i zdefiniowane punkty węzłowe infrastruktury informatycznej oraz wymagania dotyczące realizacji usług zdalnych. Cała infrastruktura zdalnego dostępu (IZD) służąca zapewnieniu komunikacji, od punktu końcowego po stronie klienta poprzez serwery zarządzające połączeniami a skończywszy na punktach dostępu po stronie firmy serwisowej, powinna być identyfikowalna i zarządzana przez dostawcę usług zdalnego dostępu (DUZD).

Zgodnie z normą bezpieczeństwo powinno być wspierane przez najnowocześniejsze mechanizmy, takie jak uwierzytelnianie, autoryzacja, szyfrowanie, rejestrowanie zdarzeń i identyfikowalność. Fizyczne i logiczne połączenia będące częścią IZD powinny być monitorowane pod kątem bezpieczeństwa cybernetycznego. IZD powinna być regularnie audytowana pod kątem skutecznej ochrony i stale udoskonalana w oparciu o najnowsze rozwiązania.

Rozwiązania wprowadzone już 10 lat temu przez Schrack Seconet w postaci pakietu Integral Remote idealnie wpisują się w wymagania tej normy, zapewniając kompleksowe usługi oraz najwyższy poziom bezpieczeństwa. Połączenia z instalacjami sygnalizacji pożarowej i sterowania urządzeniami przeciwpożarowymi są realizowane przez przez IZD opartej na platformie S2service z wykorzystaniem szyfrowanych połączeń VPN. Autoryzacja użytkowników jest przeprowadzana wielopoziomowo, a dostęp w przypadku najnowszego produktu pakietu Integral Remote, jakim jest Platforma Serwisowa, może być prowadzony poprzez uwierzytelnianie dwupoziomowe 2FA. IZD wymagana do połączenia między urządzeniami takimi jak routery dostępowe czy serwery zarządzające są nadzorowane przez Schrack Seconet, pełniącego funkcję DUZD.

Firma Schrack Seconet stale rozwija narzędzia pakietu Integral Remote w zakresie funkcji bezpieczeństwa oraz wprowadza nowe funkcjonalności. Jego zalety dostrzegają wszyscy interesariusze rynku systemów bezpieczeństwa pożarowego: inwestorzy, zarządcy, integratorzy oraz osoby obsługujące i serwisujące instalacje bezpieczeństwa pożarowego. W pakiecie Integral Remote zostały zaimplementowane zaawansowane rozwiązania w zakresie bezpieczeństwa pracy aplikacji, zapewniające ochronę przed nieautoryzowanym dostępem czy przypadkowym wpływem na działanie krytycznych elementów instalacji wynikających np. z błędu operatora.

Przybliżymy pokrótce komponenty wchodzące w skład pakietu i jego najważniejsze funkcje:

1. Platforma Serwisowa S2service

Platforma informatyczna pracująca w chmurze do zarządzania zdalnego całym cyklem życia projektu. Do najważniejszych funkcji należą:

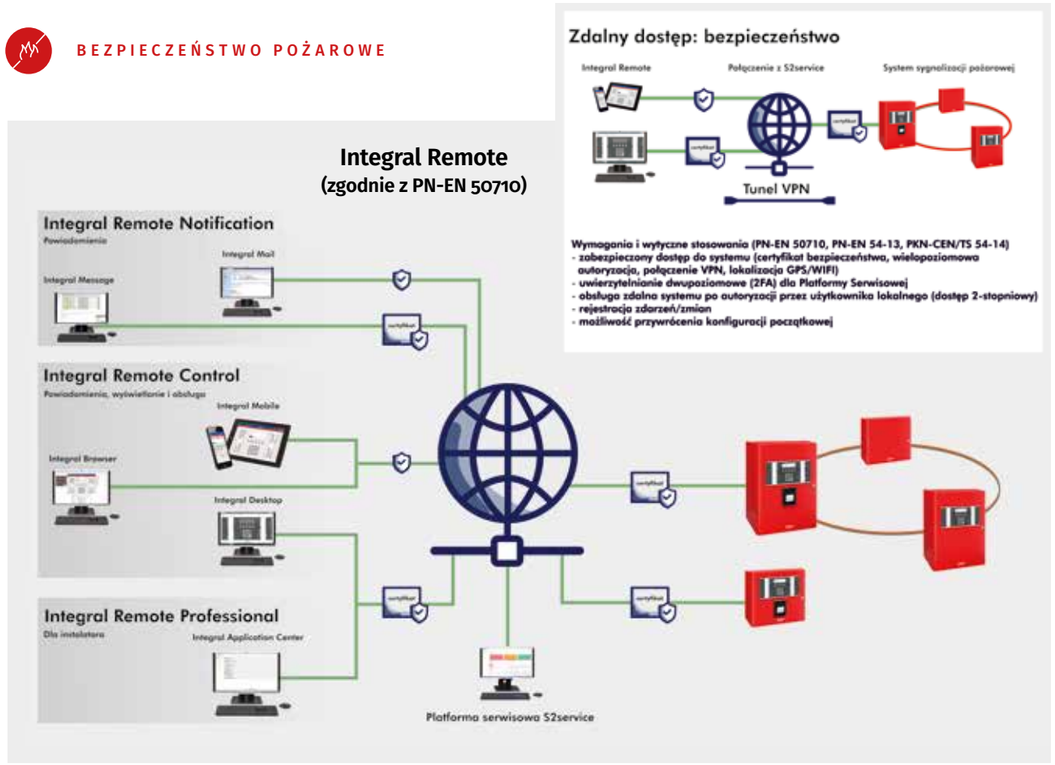
- **Dokumentacja projektowa** – pełny dostęp do aktualnej dokumentacji produktowej i projektowej oraz informacji serwisowych. Możliwość szybkiego wyszukiwania dokumentów z wykorzystaniem unikalnego kodu QR znajdującego się na urządzeniach.
- **Analiza systemu** – szczegółowa analiza pod kątem zgodności danego systemu, przyjętych rozwiązań oraz ich kompatybilności z wytycznymi producenta.
- **Rozbudowa i modernizacja** – automatyczna analiza parametrów projektowych systemu. Szczegółowa informacja o możliwościach rozbudowy, zarówno elementów wyposażenia central, jak i elementów peryferyjnych.
- **Konserwacja** – kompleksowe wsparcie dla firmy serwisującej podczas procesu konserwacji systemu. Automatyczne generowanie protokołów, list przetestowanych elementów, list nieprawidłowości itp. Możliwość szybkiego dodania dokumentacji fotograficznej i ewentualnych uwag dotyczących nieprawidłowości bezpośrednio do przygotowywanego automatycznie raportu z konserwacji.
- **Zarządzanie obiektem i zdarzeniami** – platforma serwisowa, wykorzystując bezpieczne połączenie poprzez routery S2service, ma dostęp w czasie rzeczywistym do wszystkich zdarzeń systemowych, co pozwala na szybką reakcję firmy serwisującej. Dodatkowym wsparciem w zakresie zarządzania personelem technicznym jest możliwość szybkiego przypisania zdarzenia do konkretnego użytkownika platformy w formie zgłoszenia serwisowego.

2. Integral Desktop/Integral Browser

Integral Desktop przeznaczony do obsługi serwisowej i nadzorowania instalacji z wykorzystaniem komputerów klasy PC. Program wyświetla wiernie odwzorowany panel obsługi centrali Integral EvoxX, oferując narzędzie do prostej i wygodnej obsługi w czasie rzeczywistym. Wersja językowa interfejsu może być dostosowana do operatora. W celu zapewnienia bezpiecznej pracy z oprogramowaniem Integral Desktop została wdrożona wielopoziomowa koncepcja bezpieczeństwa. Aplikacja jest chroniona kluczem sprzętowym, a użytkownik na etapie logowania się do systemu Integral EvoxX musi podać login osoby uprawnionej do zdalnego dostępu oraz hasło. Następnie po wybraniu określonego kodu dostępu operator wchodzi na odpowiedni poziom dostępu na panelu obsługi w taki sam sposób, jak w przypadku standardowego panelu obsługi MAP centrali Integral EvoxX. Rozwiązanie **Integral Browser** posiada takie same funkcjonalności co Integral Desktop, ale opiera się na przeglądarce internetowej, co pozwala na jej uruchomienie również na urządzeniach mobilnych.

3. Integral Mobile

Przeznaczony do zdalnego nadzorowania i obsługi instalacji sygnalizacji pożarowej z wykorzystaniem urządzeń mobilnych. Aplikacja odwzorowuje panel centrali Integral EvoxX, umożliwiając pełny podgląd zdarzeń oraz wykonanie operacji serwisowych przez uprawnionych użytkowników. Ponadto została wyposażona w funkcję aktywnych powiadomień



(push notification), dzięki czemu operator otrzyma informacje o wszystkich krytycznych zdarzeniach, które wystąpią w nadzorowanej instalacji sygnalizacji pożarowej. Dodatkową opcją w kwestii bezpieczeństwa jest możliwość zdefiniowania koordynat GPS do określenia dozwolonego obszaru, z którego może być wykonywana zdalna obsługa.

4. Integral Message

Przeznaczony do zdalnego nadzorowania i obsługi serwisowej wielu niezależnych instalacji sygnalizacji pożarowej Integral EvoxX. Do głównych zadań oprogramowania należy: informowanie o zdarzeniach występujących w nadzorowanych systemach, rejestracja zdarzeń w bazie danych serwera oraz wyświetlanie na stacjach klienckich. Wszystkie komunikaty są przedstawiane w formie tabelarycznej z określeniem rodzaju zdarzenia (alarm, uszkodzenie itp.), nazwy obiektu i szczegółowego opisu zdarzenia. Podczas każdego zdarzenia na ekranie komputera są wyświetlane powiadomienia typu pop-up, dzięki którym operator nie pominie kluczowych informacji pochodzących z nadzorowanych systemów. Ponadto w prosty i szybki sposób możliwe jest połączenie z daną instalacją za pomocą aplikacji Integral Desktop, która jest częścią oprogramowania Integral Message. Wszystkie operacje użytkowników są rejestrowane w systemie.

5. Integral Mail

Umożliwia wysyłanie e-maili bezpośrednio z CSP/CSUP o najważniejszych zdarzeniach w systemie Integral EvoxX (alarm, uszkodzenie itp.) na zdefiniowane adresy poczty elektronicznej użytkowników. Zakres wysyłanych komunikatów można dowolnie konfigurować w zależności od tego, kto jest ich odbiorcą i jakie informacje są dla niego kluczowe.

Pakiet oprogramowania Integral Application Center przeznaczony dla instalatorów i firm serwisujących system Integral EvoxX może być również wykorzystywany do prac zdalnych zgodnie z wymaganiami normy z wykorzystaniem infrastruktury S2service. Dzięki technologii IP, obecnej w każdej centrali z rodziny Integral EvoxX, wszystkie urządzenia mogą być zdalnie konfigurowane w pełnym zakresie funkcji. Operacje związane z wdrażaniem systemu, dotychczas wykonywane wyłącznie lokalnie w obiekcie, obecnie w coraz większym zakresie mogą być również realizowane zdalnie. W zależności od wymagań można tworzyć w oprogramowaniu dowolną liczbę użytkowników zdalnych z możliwością przypisywania im określonych funkcji i poziomów autoryzacji. Poziom autoryzacji może być indywidualnie ustawiony dla każdego użytkownika, a jego dane osobowe i hasło są zapisane w sposób zaszyfrowany w centrali – ich zmiana jest możliwa tylko poprzez przeprogramowanie systemu przez autoryzowany personel.

W celu zwiększenia poziomu bezpieczeństwa może być zastosowana dodatkowa autoryzacja dostępu przez personel obsługi obiektu do wykonywania zdalnych operacji. Funkcjonuje to w następujący sposób: po zalogowaniu się do systemu poprzez wpisanie nazwy użytkownika i hasła zdalny operator ma dostęp tylko do informacji o aktualnym stanie systemu. Aby móc obsługiwać system, musi uzyskać autoryzację od lokalnego operatora, który potwierdza połączenie z poziomu panelu obsługi centrali Integral EvoxX.

Rozwiązania w zakresie zdalnego dostępu pozwalają na znaczne usprawnienie opieki nad całym cyklem funkcjonowania instalacji bezpieczeństwa pożarowego, należy jednak stosować rozwiązania zgodne z aktualnymi wymaganiami norm i wytycznych, aby usługi realizowane zdalnie były bezpieczne.

Więcej informacji dotyczących najnowszych rozwiązań Schrack Seconet, w tym również pakietu Integral Remote, znajduje się na stronie firmy www.schrack-seconet.pl. ●

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

AAT SYSTEMY BEZPIECZEŃSTWA

Kamery Starlight Pro Duo marki NOVUS

Kamery Starlight Pro Duo wyróżniają się kolorowym i wyraźnym obrazem nawet w całkowitej ciemności. Zostały wyposażone w dwa rodzaje oświetlaczy złożonych z diod białych LED i IR.

Niezwykle wysoka czułość kamery w połączeniu z dużej mocy światłem białych diod LED umożliwia obserwację w kolorze bez względu na porę dnia (24/7) i warunki atmosferyczne. W zależności od konfiguracji kamery, białe diody LED mogą także pełnić funkcję światła ostrzegawczego po wystąpieniu zdarzenia alarmowego lub być włączane ręcznie przez użytkownika. Z kolei diody IR LED umożliwiają pracę w nocy w trybie czarno-białym, co może być przydatne w sytuacjach, w których pożądana jest obserwacja dyskretna.

Linia kamer Starlight Pro Duo wkrótce zostanie wzbogacona o modele wyposażone w funkcje analityki AI, które umożliwią zaprogramowanie reakcji po wykryciu osób lub pojazdów. To pozwoli stworzyć zaawansowane systemy wykrywania i odstraszania intruzów, spełniające w odpowiednich warunkach funkcję klasycznego systemu alarmowego. ●

GENETEC

Axis Powered by Genetec – nowość w kontroli dostępu

Axis Powered by Genetec to pierwsze rozwiązanie w branży, które umożliwia wprowadzenie zaawansowanego oprogramowania Genetec bezpośrednio do firmware'u urządzeń.

Genetec, wiodący dostawca technologii w zakresie zunifikowanych rozwiązań zabezpieczeń, bezpieczeństwa publicznego i *business intelligence,* poinformował o współpracy z Axis Communications, której efektem jest wprowadzenie Axis Powered by Genetec. To pierwsze w branży rozwiązanie kontroli dostępu łączące w jednej ofercie typu *all-in-one* oprogramowanie kontroli dostępu Genetec Synergis™ z sieciowymi kontrolerami drzwi AXIS A1210 i AXIS A1610.

Integratorzy skorzystają z łatwych do wdrożenia urządzeń fabrycznie wyposażonych w innowacyjne oprogramowanie kontroli dostępu, bez problemów związanych z tradycyjną integracją urządzenia i oprogramowania. Co więcej, urządzenia włączone do programu Axis Powered by Genetec są objęte planem stałego uzupełniania o nowe funkcje i aktualizacje oprogramowania sprzętowego oraz ochroną w zakresie cyberbezpieczeństwa świadczonym przez dwóch największych w branży innowatorów.

– *Axis i Genetec łączy zaufane partnerstwo oparte na długiej historii współpracy i pomysłowości w zakresie rozwoju* – stwierdził Michel Chalouhi, wiceprezes ds. sprzedaży globalnej w Genetec Inc. – *Jesteśmy dumni, że możemy współpracować z firmą Axis jako głównym partnerem w naszym nowym programie Powered by Genetec. Wspólne wysiłki skoncentrowane na dostarczaniu wydajnych i kreatywnych rozwiązań spełniających potrzeby klientów stanowiły podstawę rozwoju tej zaawansowanej technologii kontroli dostępu, dostarczanej w formie uproszczonej, łatwej do nabycia i wdrożenia oferty.*

– *Axis i Genetec mają za sobą długą historię wspólnych innowacji. Nowe rozwiązanie Axis Powered by Genetec jest przykładem tej współpracy w zakresie integracji najlepszych w swojej klasie urządzeń i oprogramowania, co usprawnia instalację i konserwację, a jednocześnie zwiększa cyberbezpieczeństwo* – powiedział Fredrik Nilsson, VP amerykańskiego oddziału Axis Communications.

Axis Powered by Genetec w jednym module łączy urządzenie i oprogramowanie, co upraszcza proces instalacji, zmniejsza koszty konserwacji i wprowadza wbudowane funkcje cyberbezpieczeństwa na poziomie zarówno urządzenia, jak i oprogramowania. Rozwiązanie bazujące na otwartej platformie rozszerza bazę systemów Genetec, zapewniając jednocześnie klientom większą elastyczność w zakresie modernizacji systemów w miarę ewolucji ich potrzeb.

Wybrane oferty Powered by Genetec dla wielu urządzeń brzegowych firma Genetec wprowadzi w nadchodzących kwartałach. Certyfikowani partnerzy Genetec będą mieli dostęp do rozwiązania już w kwietniu. ●

Hanwha Vision

Hanwha Techwin zmienia nazwę na Hanwha Vision

Hanwha Techwin, wiodący producent urządzeń do systemów telewizji dozorowej, 1 marca 2023 r. zmienił nazwę na Hanwha Vision.

Zmiana podyktowana została rozszerzeniem oferty firmy, będącego obecnie globalnym dostawcą rozwiązań wizyjnych. Poza produktami do dozoru wideo firma będzie dostarczać rozwiązania wizyjne nowej generacji, które integrują algorytmy sztucznej inteligencji (AI) i technologie chmurowe. W ten sposób zapewni klientom lepszy wgląd w operacje biznesowe, jednocześnie napędzając innowacje na globalnym rynku.

– *Bazujemy na innowacjach, które zapewniają nam przewagę konkurencyjną. Będziemy dostarczać rozwiązania spełniające potrzeby naszych klientów, dodając jednocześnie nową wartość dzięki zaawansowanym rozwiązaniom* – powiedział Soon-hong Ahn, prezes i dyrektor generalny Hanwha Vision.

– *W miarę, jak będziemy rozszerzać naszą działalność w sektorze monitoringu wizyjnego, dzięki analityce big data dostarczymy klientom informacji dostosowanych do ich potrzeb. Rozwiązania te umożliwią podejmowanie działań, które nie tylko zapobiegną incydentom, ale także zareagują na nie w czasie rzeczywistym. Nasze nowe rozwiązania wizyjne będą miały kluczowe znaczenie dla rozwoju strategii operacyjnych naszych klientów* – dodał prezes Ahn.

Hanwha Vision będzie stopniowo wprowadzać rebranding swoich zagranicznych filii, produktów i rozwiązań, dostosowując się do warunków rynkowych. ●

LINC POLSKA

Nowość w termowizji, czyli Teledyne FLIR Triton FH-D

Triton FH-ID to najnowszy produkt marki Teledyne FLIR (FLIR). To seria wielospektralnych stałopozycyjnych kamer, które łączą obrazowanie termowizyjne z obrazowaniem widzialnym 4K i zaawansowaną analityką.

Algorytmy analityczne opierają się na konwolucyjnej sieci neuronowej (CNN), umożliwiając dokładne wykrywanie i klasyfikację obiektów – ludzi i pojazdów, niezależnie od tego, z jaką poruszają się prędkością, co minimalizuje liczbę fałszywych alarmów.

Zastosowany przetwornik termowizyjny charakteryzuje się wysoką czułością termiczną mniejszą niż 30 mK, gwarantując jeszcze większą skuteczność działania kamer.

Seria Triton FH- ID obejmuje szeroką gamę modeli o różnym zakresie detekcji, umożliwiając wykrywanie zagrożenia praktycznie w każdych warunkach atmosferycznych i oświetleniowych. Wbudowany harmonogram zapewnia operatorom systemów zabezpieczeń taką konfigurację urządzeń, aby działały w trybie 4K w ciągu dnia, a nocą jako urządzenia termowizyjne, oferując optymalny zasięg i skuteczność w każdych warunkach. ●

AVIGILON MOTOROLA SOLUTIONS Venom PSIM PLATFORM

Dziękujemy wszystkim za ogromne zainteresowanie i zapraszamy na kolejną edycję w Arabii Saudyjskiej

MEGAVISION TECHNOLOGY Sp. z o. o., Heliotropów 1, 04-796 Warszawa, tel.: +48 22 292 3 292, e-mail: psim@psim.pl

ROGER

Integracja systemu RACS 5 z usługą katalogową Active Directory

Usługa katalogowa Active Directory (AD) firmy Microsoft to rozwiązanie powszechnie stosowane przez administratorów domenowych sieci firmowych. Pozwala zarządzać całym zbiorem użytkowników w sieci, określać ich uprawnienia do zasobów sieciowych, a także konfigurować komputery, na których pracują.

System kontroli dostępu i automatyki budynkowej RACS 5 (Roger) oferuje możliwość integracji programowej z usługą Active Directory na bazie protokołu LDAP.

Integracja umożliwia przede wszystkim centralne zarządzanie użytkownikami sieci domenowej i systemu kontroli dostępu z poziomu oprogramowania zarządzającego Active Directory. Oznacza to, że administrator usługi katalogowej może określać uprawnienia użytkowników w systemie kontroli dostępu. W ramach integracji możliwa jest:

- ręczna synchronizacja listy użytkowników RACS 5 z listą użytkowników AD,
- automatyczna synchronizacja listy użytkowników RACS 5 z listą użytkowników AD (tylko RACS 5 w wersji Enterprise).

Dodatkowo dane uwierzytelniające użytkownika Active Directory mogą być wykorzystywane przez administratora systemu RACS 5 podczas logowania się do programu zarządzającego tym systemem.
Integracja systemu RACS 5 z usługą katalogową Active Directory jest z powodzeniem stosowana przez klientów korzystających z obu rozwiązań. Pozwala ona sprawnie i profesjonalnie zarządzać uprawnieniami użytkowników na poziomie dostępu do zasobów sieciowych, jak też poruszania się po obiekcie. ●

SAFE PLACE

W poszukiwaniu dobrych praktyk na kongresie antyterrorystycznym

Czasopismo „a&s Polska” było partnerem medialnym I Ogólnopolskiego Kongresu Antyterrorystycznego „Działania antyterrorystyczne i kontrterrorystyczne. W poszukiwaniu dobrych praktyk” zorganizowanego przez firmę Safe Place.

W ciągu dwóch dni wydarzenie odwiedziło łącznie ponad 240 uczestników reprezentujących ośrodki naukowe, eksperckie, instytucje bezpieczeństwa narodowego, sektor ochrony i zabezpieczeń technicznych oraz obiekty użyteczności publicznej i infrastruktury krytycznej.

Kongres Antyterrorystyczny odbył się na przełomie lutego i marca w murach Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie. Zaplanowane sesje i panele zostały rozbudowane w celu kompleksowego omówienia poszczególnych obszarów tematycznych. Bezpieczeństwo antyterrorystyczne swym zasięgiem obejmuje szereg zagadnień, które dzięki obecności teoretyków i praktyków w znacznej części udało się omówić w trakcie obrad. Uczestnicy Kongresu mieli okazję zapoznać się z szeroką ofertą interesujących rozwiązań, urządzeń i systemów przedstawioną przez wiodących dostawców działających na rynkach polskim i zagranicznym.

Ogromną wartością kongresu było wsparcie merytoryczne i organizacyjne takich instytucji jak: Rządowe Centrum Bezpieczeństwa, NATO DEEP eAcademy, Urząd Komisji Nadzoru Finansowego, Służba Ochrony Państwa, Agencja Wywiadu, Centrum Prewencji Terrorystycznej Agencji Bezpieczeństwa Wewnętrznego, Centralny Pododdział Kontrterrorystyczny Policji „BOA”, Samodzielny Pododdział Kontrterrorystyczny Policji w Radomiu, Straż Ochrony Kolei i wiele innych.

Duże zainteresowanie pierwszą edycją kongresu spowodowało, że organizatorzy przewidują kolejne tego typu wydarzenie. Natomiast już teraz trwają przygotowania do VI Międzynarodowego Kongresu Naukowo-Technicznego Safe Place 2023, który odbędzie się 20-22 listopada w Wojskowej Akademii Technicznej w Warszawie. Tegoroczna tematyka będzie obejmowała bezpieczeństwo obiektów użyteczności publicznej i infrastruktury krytycznej wobec zagrożeń wojennych, hybrydowych i terrorystycznych. ●

SCHRACK SECONET POLSKA

Relacja ze spotkania partnerów Schrack Seconet

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 swoją wieloletnią tradycję, organizowane są niezmiennie w pierwszym kwartale roku. Ich celem jest podsumowanie roku minionego oraz wspólne opracowanie i omówienie najważniejszych planów, a także strategii działania na rynku systemów zabezpieczeń w Polsce w kolejnych latach. Tegoroczna edycja odbyła się w połowie marca, tym razem w nowo otwartym hotelu Radisson Blue***** w Ostródzie.

Rok 2022 dla Schrack Seconet w Polsce to przede wszystkim kolejna rekordowa sprzedaż systemów bezpieczeństwa, komunikacji oraz systemów integrujących urządzenia pożarowe. Lista referencyjna producenta powiększyła się o kilkaset zaawansowanych technologicznie obiektów, a grono certyfikowanych specjalistów poszerzyło się o kilkuset inżynierów!

W tegorocznym spotkaniu wzięło udział ponad 100 przedstawicieli firm partnerskich – głównie członków szczebla zarządzającego. Spotkanie rozpoczął Michał Sidor, prezes Zarządu Schrack Seconet w Polsce, przedstawiając wyniki sprzedaży całej grupy partnerskiej. Prezentacje przygotowane przez zespół Schrack Seconet dotyczyły m.in. analizy poszczególnych sektorów rynku (przemysłowego, biurowego, magazynowego, Data Center, obiektów użyteczności publicznej i medycznych), zrealizowanych obiektów referencyjnych, nowości produktowych oraz działań marketingowych. Niezwykle ważnymi punktami spotkania były kuluarowe dyskusje na temat możliwości rozwojowych branży bezpieczeństwa w Polsce, zmian, jakie czekają producentów poszczególnych rozwiązań w związku z dynamiczną sytuacją na świecie oraz znaczenia firm partnerskich w tworzeniu nowych wartości dla całego rynku krajowego.

Na spotkaniu wyróżniono kilkudziesięciu partnerów producenta – Autoryzowanych Partnerów Wiodących, Autoryzowanych Partnerów oraz przedstawicieli firm Preautoryzowanych, którzy istotnie przyczynili się do rozwoju organizacji w Polsce. Wręczenie nagród, a tym samym dołączenie do grona Partnerów Autoryzowanych potwierdza wysoką etykę współpracy, indywidualne podejście do oczekiwań klientów oraz stabilną sytuację finansową wyróżnionych przedsiębiorstw.

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

Regularne szkolenia i nieustanne podnoszenie kwalifikacji zatrudnionych przez te firmy specjalistów przejawiają się wysokim zadowoleniem użytkowników systemów bezpieczeństwa, co stanowi najwyższą wartość dla wszystkich uczestników rynku. ●

Tytuł **Partnera Roku** za najlepszy wynik w sprzedaży systemów sygnalizacji pożarowej Schrack Seconet w 2022 r. oraz wysoką jakość usług otrzymała firma **LTEC** z Piaseczna.

Do grona Autoryzowanych Partnerów Wiodących dołączyła firma **INITEL** z Opola.

Autoryzowanymi Partnerami w Polsce zostały firmy: Centrum Informatyki „ZETO” z Białegostoku, LTEC z Piaseczna, INSTAL-TECH z Gdańska.

Podczas spotkania przyznano także kilka wyróżnień:

Trzeba umieć połączyć kropki

Kiedy zabrakło istotnego surowca, a dostawca zaczął wmawiać głównemu technologowi, że przecież kierowca był, tylko nikt towaru nie odbierał, ten postanowił sam rzecz sprawdzić. Przekonał się wówczas, że nie wszystko działa w firmie tak, jak powinno. A już na pewno coś poszło nie tak, jeśli chodzi o ochronę zakładu.

Damian Maliszewski, główny technolog i jednocześnie wiceprezes, rozmawiając przez telefon, lubił spacerować. Tym razem krążył po parkingu przed budynkiem firmy niczym lew po klatce i z daleka było widać, że jest zdenerwowany. Na monitorze ochrony widać było wyraźnie, że z kimś intensywnie dyskutuje.

– Oj tam, oj tam, przecież to mógłby być mój wnuk. – Pani Maria lekceważąco machnęła ręką.

Zbyszek z dezaprobatą pokręcił głową i wyjaśnił:
– Zdenerwowany jest, bo mówią, że dostawa przyjechała, a przecież od trzech dni wypatrujemy kierowcy. Żadnego nie było. Ani na mojej zmianie, ani na Józkowej, ani nawet w nocy. Różni przyjeżdżają, nawet ostatnio jacyś pobłądzili i wypytywali o drogę, ale tych dostawców, wie pani, tych co zawsze, to nie było. Ja pilnuję. – W głosie pana Zbyszka zabrzmiała wyraźna duma.

Tymczasem główny technolog jeszcze chwilę krążył po placu, niewidzialnemu rozmówcy pokazywał to na bramę, to na kamery, a następnie zeźlony rzucił słuchawką, zakładając, że przy smartfonie jest to możliwe. I ruszył żwawym krokiem w stronę głównego wejścia do firmy.

Wszedł i przywitał się z panią Marią, którą cenił za pracowitość i zawsze dobry humor oraz za przymioty pozasłużbowe, czyli boskie pierogi z serem. Pani Maria „babciowała" większości załogi – nielicznej, ale zgranej ekipie doskonałych specjalistów – obdarowując wszystkich po trochu pierogami, dynią z własnego ogródka i dobrym słowem.

– Panie Zbyszku, pokaże mi pan te nagrania z ostatniego tygodnia? – Maliszewski zwrócił się do siedzącego za kontuarem pracownika ochrony intensywnie wpatrującego się w monitory, na których absolutnie nic się nie działo.

– Oczywiście, panie prezesie. Zbyszek prawie stanął na baczność i życzliwie zapytał: ***– A nie wolałby pan sobie na spokojnie u siebie obejrzeć, przy biurku? Bo ja mogę przynieść do pana te nagrania*** – dodał życzliwie.

– Wie pan, że to dobry pomysł. Z całego tygodnia bym chciał obejrzeć, bo czuję, że ktoś mnie tu kantuje z tym transportem. Przecież ktoś od was by zauważył, że samochód czeka przed bramą? – Ni to stwierdził, ni to zapytał Maliszewski.

Zbyszek gorliwie przytaknął, że owszem. Każdy by zauważył i albo wpuścił na plac, albo poszedł zapytać. Czujnemu oku agencyjnej ochrony nic nie umknie. Ani nikt.

– My tu, panie kierowniku – perorował Zbyszek – ***wszystko i wszystkich widzimy. Sami patrzymy i na kamerach też jest.***
Stojąca trochę z boku pani Maria odezwała się znienacka:
– A do tej skrzynki to pan zaglądał? – zwróciła się bezpośrednio do Zbyszka. ***– Bo idę do kadr, to jak coś tam jest, to mogę zanieść.***

– Eeeee tam, zawracanie gitary. Kto by tu do nas przyszedł na to zadupie, żeby życiorysa wrzucić. Jeden był ostatnio jakiś, ale tak się pokręcił, pokręcił i poszedł. Melepeta jakiś. Wyglądał, jakby do trzech nie umiał zliczyć. Zbyszek aż się uśmiechnął pod nosem, kiedy przypomniał sobie gapowaty wygląd młodego człowieka, który przyszedł pytać o pracę. Przecież on od razu widział, że nic toto nie umie. Coś mu tam wtedy burknął i spławił młodzika.

– Jak tak, to ja idę. Pani Maria sięgnęła po mop i wiadro. ***– Posprzątam u dziewczyn. To co, panie Damianku, odgrzać pierożków?*** – zapytała starsza pani głównego technologa i uśmiechnęła się filuternie.

***

Kiedy Damian Maliszewski oglądał kolejną godzinę nagrania, po pierogach od pani sprzątającej zostało tylko wspomnienie. I choć technolog przyśpieszył film tak bardzo, jak tylko się dało, czuł, że ogarnia go znużenie. Wpatrywał się w czarno-białe nagranie jak sroka w gnat i nic ciekawego nie widział. Nie było samochodu z dostawą bezcennego surowca, a bez tego lada moment stanie im produkcja. „Diabli nadali", zaklął szpetnie w myślach.

Nagle zauważył coś dziwnego. Na późnowieczornym nagraniu wykonanym 7 dni wcześniej zauważył stojący przy ogrodzeniu samochód osobowy. Było to o tyle niepokojące, że pora późna, wokół pusto, sąsiedztwo prawie żadne, pole z kapustą i stacja benzynowa. Nikt nie miał powodu, żeby zatrzymywać się przy ogrodzeniu. „Chwila, chwila…", zastanowił się Damian, „dlaczego on tu stoi?". Kolejne godziny nagrań i ten sam samochód. Dzień i dwa później. Raz rano, potem wieczorem i jeszcze popołudniu. „Co tu się dzieje?". Maliszewski się zaniepokoił. Wideo z kolejnych dni pokazało, że wokół samochodu pojawiają się ci sami ludzie i coś obserwują. W pewnym momencie jeden z nich przekroczył bramę i skierował się wprost do głównego wejścia. Tego samego miejsca, w którym przed kilkoma godzinami Damian Maliszewski rozmawiał ze służbistą Zbyszkiem i wiecznie uśmiechniętą panią Marią.

A potem zdarzyło się coś, co Maliszewskiego wyprowadziło tak bardzo z równowagi, że z trudem opanowane przez kardiologa ciśnienie skoczyło mu do niebotycznych wartości. Na jednym z ostatnich nocnych nagrań dostrzegł, jak ni z tego, ni z owego tuż przed głównym wejściem, dokładnie w tym samym miejscu, gdzie Maliszewski spacerował, rozmawiając przez telefon, pojawił się ubrany na szaro typ. Trudno o nim powiedzieć, że jakoś wyglądał. Raczej z twarzy podobny do nikogo. „Szlag by to trafił, nic nie widzę, co on tam robi?", Damian próbował dojrzeć cokolwiek na ekranie. Nagle nagrywany typ zerwał się do ucieczki, a na plac wjechał patrol interwencyjny ochrony. Damian aż usiadł wyprostowany. Ze zdumieniem patrzył, jak typ ucieka, patrol wjeżdża, któryś z pracowników

ochrony wychodzi… „Co tu się dzieje? Dlaczego nic o tym nie wiem? Dlaczego nikt mnie nie poinformował, że ktoś się kręci wokół zakładu?". Reszty tego, co pomyślał sobie Damian, zacytować się nie da. Podobnie jak tego, co powiedział, gdy zadzwonił do inspektora nadzoru. No, może poza jednym, bo to usłyszał nawet pracownik ochrony Zbyszek, a siedział przecież tuż przy wejściu do firmy.

– ***Panie!*** – wrzeszczał Damian Maliszewski. – ***Przecież my tu złoto mamy! Jak nic nas obserwowali! Dlaczego ja nic o tym nie wiem?!***
Po raz pierwszy tego dnia główny technolog ucieszył się, że dostawca nawalił.
Godzinę później pani Maria zajrzała do gabinetu Maliszewskiego i zapytała cichutko:
– ***To może ja meliski zaparzę?***

Opracowała Monika Mamakis na bazie scenariusza Jacka Grzechowiaka

- **Dlaczego Maliszewskiego tak bardzo zdenerwował fakt, że nie wiedział, co wydarzyło się pewnego wieczoru na placu firmy?**
- **Dlaczego główny technolog ucieszył się, że dostawa nie dotarła na czas?**
- **Co produkuje firma, której prezesem jest Damian Maliszewski?**

Odpowiedzi na te pytania poznali uczestnicy strategicznych warsztatów Forum Security prowadzonych przez Centrum Kompetencji a&s Polska. W warsztatach, które odbyły się 16 marca tego roku, wzięły udział osoby zaproszone przez a&s Polska.
Centrum Kompetencji a&s Polska organizuje szkolenia i warsztaty dla osób odpowiedzialnych za bezpieczeństwo fizyczne, cyfrowe i zabezpieczenia techniczne.
Przekonaj się, co o warsztatach sądzą osoby, które wzięły w nich udział:

Tomasz Ciećwierz, NIK
Jestem stałym bywalcem na wydarzeniach organizowanych przez „a&s Polska" i mogę przyznać, że to kolejne, bardzo udane szkolenie. Prowadzący to po prostu mistrz. Przytaczane przez niego przykłady i prezentacja były naprawdę odzwierciedleniem tego, co się dzieje w segmencie ochrony fizycznej. Połączenie i wskazanie odpowiednich kierunków oraz przedstawienie możliwości, jakie daje nam technika, doskonale pokazuje, na jakim poziomie może być ochrona obiektów IK. Warto też dodać, że Forum Security Centrum Kompetencji to nie suchy wykład. Tu każdy uczestnik może wziąć czynny udział w dyskusji, notabene na bardzo wysokim poziomie. To ogromny atut, że możemy wymienić się swoimi doświadczeniami z innymi specjalistami. Na Forum nie ma przypadkowych osób. To ludzie, którzy mają naprawdę wiele do powiedzenia, są bardzo aktywni na rynku i znają jego problemy.

Paweł Figlarz, ekspert IK
Doskonałe warsztaty w zupełnie nowej interaktywnej formule. Świetne miejsce, bardzo dobrze przygotowany prowadzący, duża dawka wiedzy, no i te bezcenne dyskusje z ekspertami, którzy chętnie wymieniają się swoimi doświadczeniami. Muszę przyznać, że takie spotkania są teraz szczególnie ważne i potrzebne, zwłaszcza, że świat się dynamicznie zmienia, a naszym zadaniem jest za nim nadążyć.

Jacek Zieliński, PSG
Szkolenie zostało przeprowadzone w bardzo ciekawej formie jako kompilacja teorii i praktycznych zadań. Forma prezentacji była bardzo ciekawa i autorska. Prowadzący otwarty na dyskusję, komunikatywny, kompetentny i z ogromnym doświadczeniem. Zdecydowanie warto brać udział w takich szkoleniach, zwłaszcza, że pobudzają one do myślenia i spojrzenia na sprawy znacznie szerzej i z większą otwartością, zarówno na klienta, jak i pracowników bezpieczeństwa.

a&s Polska 02 | 2023

BCS
BCS
BCS
dla profesjonalistów
Bezpieczeństwo infrastruktury krytycznej
Kamery PTZ marki BCS posiadają nawet 45-krotny zoom optyczny, oświetlacz IR do 300m, oraz funkcje inteligentnej analizy obrazu.
POLSKA MARKA
BCS
www.bcs.pl
www.facebook.com/bcscctvpl