02 (44) / 2024

CZASOPISMO RYNKU SECURITY

a&S POLSKA

RAPORT: JAK JESTEŚMY CHRONIENI?

O bezpieczeństwie państwa i jego obywateli decyduje wiele czynników. Sprawdzamy, jak dziś wygląda stan gotowości na kryzys.

NIS 2: W OCZEKIWANIU NA PRZEPISY KRAJOWE

Menedżerowie security powinni zwrócić szczególną uwagę na artykuły dotyczące zarządzania cybernetycznym ryzykiem i zgłaszania incydentów.

WYŻSZY POZIOM BEZPIECZEŃSTWA

Rośnie popularność mobilnych wież do monitoringu. To wygodna forma tymczasowego zabezpieczenia wyposażona w najnowsze technologie.

www.aspolska.pl

20 zł
(w tym 8% VAT)

05

ISSN 2451-5175

9 772451 517703

INFRASTRUKTURA KRYTYCZNA

Innowacje w bezpieczeństwie

TAURUS OCHRONA

W Taurus Ochrona łączymy wieloletnie doświadczenie, fachową wiedzę oraz nowoczesne narzędzia, aby tworzyć dedykowane i kompleksowe pakiety usług branżowych. Dzięki temu ugruntowaliśmy swoją pozycję jako lider w świadczeniu usług ochrony dla branży OZE, obejmując zarówno farmy wiatrowe, jak i farmy fotowoltaiczne.

KOMPLEKSOWY PAKIET USŁUG DOPASOWANY DO KLIENTA

vPATROL

Inteligentny system ochrony

vPATROL Tower

Inteligentny system ochrony z wykorzystaniem mobilnych wież do monitoringu

Monitoring systemów alarmowych

Techniczne systemy zabezpieczeń

Ochrona fizyczna

Ochrona i zabezpieczenie imprez

Sala spotkań niejawnych

Audyt i dokumentacja ochrony

Ochrona domu

Ochrona VIP

Konwojowanie wartości pieniężnych

Usługi detektywistyczne

Jako lider w dziedzinie innowacji w bezpieczeństwie, zajmujący się szeroko rozumianą ochroną osób, mienia i informacji, **gwarantujemy świadczenie usług na najwyższym poziomie.** W trosce o zadowolenie klientów, stale podnosimy jakość naszych usług, opierając się przede wszystkim na sprawnych procesach zarządzania oraz traktowaniu naszych klientów **zgodnie z najwyższymi, przyjętymi standardami etycznymi i biznesowymi.**

ISO 9001
System Zarządzania Jakością

ISO 14001
System Zarządzania Środowiskowego

ISO 45001
System Zarządzania Bezpieczeństwem i Higieną Pracy

ISO 27001
System Zarządzania Bezpieczeństwem Informacji

ISO 26000
Wytyczne dotyczące społecznej odpowiedzialności biznesu

Taurus Ochrona Group sp. z o. o. | ul. Lubicka 53, 87-100 Toruń | +48 56 675 24 57 | bok@taurus-ochrona.pl

www taurus ochrona.pl

Jak dbać o bezpieczeństwo infrastruktury krytycznej

W czasach rosnącej cyfryzacji i globalizacji bezpieczeństwo infrastruktury krytycznej staje się coraz większym wyzwaniem. Infrastruktura krytyczna, obejmująca m.in. sieci energetyczne, systemy transportowe, szpitale i instytucje rządowe, jest niezbędna dla prawidłowego funkcjonowania społeczeństwa. Awaria lub atak na jeden z tych systemów może mieć katastrofalne skutki.

Heraklit, starożytny grecki filozof, powiedział kiedyś: *panta rhei,* co oznacza „wszystko płynie". Ta maksyma doskonale opisuje dynamikę współczesnego świata, w którym zmiany zachodzą z coraz większą prędkością. Infrastruktura krytyczna nie jest na to zjawisko obojętna. Wraz z rozwojem technologii i ewolucją zagrożeń również ona musi się stale adaptować i ewoluować, aby zapewnić odpowiedni poziom bezpieczeństwa.

Złożoność i rozległość infrastruktury krytycznej, rosnące ryzyko coraz bardziej wysublimowanych cyberataków i ciągle zmieniające się oblicze zagrożeń to tylko niektóre z wyzwań, z jakimi borykają się dziś menedżerowie security odpowiadający za bezpieczeństwo infrastruktury krytycznej.

Na co powinni być przygotowani? Choćby na brak wody wywołany przede wszystkim zmianami klimatycznymi (*Z pustego i Salomon nie naleje*, str. 28). A może na wojnę hybrydową lub pełnoskalową (*Na co jesteśmy gotowi: na wojnę czy na defiladę? O znaczeniu polityk bezpieczeństwa*, str. 20)? Inne pytanie (równie istotne) brzmi: jak jesteśmy chronieni? Odpowiadamy na nie w raporcie na str. 14.

Innowacje technologiczne, takie jak sztuczna inteligencja i uczenie maszynowe, mogą być wykorzystywane do wykrywania i zapobiegania atakom w czasie rzeczywistym. Wzrost świadomości na temat bezpieczeństwa infrastruktury krytycznej wśród rządów i firm oraz międzynarodowa współpraca w zakresie wymiany informacji i najlepszych praktyk, czemu służyć ma m.in. dyrektywa NIS 2, to kolejne czynniki, które mogą przyczynić się do poprawy bezpieczeństwa. Dla branży security obecna sytuacja geopolityczna oznacza wzmożoną czujność. To oczywiście też pewna biznesowa szansa, nawet jeśli niełatwo ten fakt zaakceptować.

W świecie *panta rhei,* gdzie zmiany są nieuniknione, bezpieczeństwo infrastruktury krytycznej wymaga nieustannej adaptacji i ewolucji. Również od ludzi odpowiedzialnych za bezpieczeństwo obiektów IK.

Jak napisał Sun Tzu w „Sztuce wojny": […] *zostało powiedziane, że kto zna wroga i zna siebie, nie będzie zagrożony choćby i w stu starciach. Kto nie zna wroga, ale zna siebie, czasem odniesie zwycięstwo, a innym razem zostanie pokonany. Kto nie zna ani wroga, ani siebie, nieuchronnie ponosi klęskę w każdej walce.* […]. Branża security powinna wziąć sobie do serca te słowa.

Te ważne tematy wybrzmią także podczas konferencji Warsaw Security Summit, która odbędzie się 6 czerwca. Już teraz zapraszamy do udziału w tym wydarzeniu.

Redakcja

ZŁOTY PARTNER A&S POLSKA

AXIS COMMUNICATIONS BCS Linc Polska Sp. z o.o. smart-i

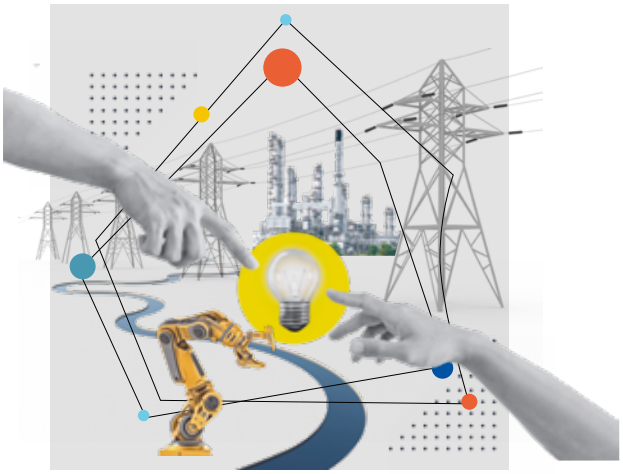
SREBRNY PARTNER A&S POLSKA

HIKVISION

CZASOPISMO RYNKU SECURITY

a&S POLSKA

02 (44) / 2024



RAPORT: INFRASTRUKTURA KRYTYCZNA

PRODUKTY NUMERU

INFRASTRUKTURA KRYTYCZNA

REDAKCJA

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

info@aspolska.pl
www.aspolska.pl

PREZES ZARZĄDU
Mariusz Kucharski

REDAKTOR NACZELNA
Marta Dynakowska

Z-CA RED. NACZELNEGO
Jan T. Grusznic

REDAKCJA
Monika Żuber-Mamakis
Adela Prochyra

DZIAŁ REKLAMY
Iwona Krawiec

DZIAŁ PROJEKTÓW SPECJALNYCH
Jolanta A. Kucharska
Aleksandra Czapska

CENTRUM KOMPETENCJI
Jacek Grzechowiak

KOREKTA
Jolanta Kucharska

PROJEKT GRAFICZNY I SKŁAD
Bogusław Kalwala

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

www.sensgroup.pl

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 VIEW ITC

Najwyższa skuteczność w każdym… znaku

» Więcej przeczytasz na stronie 10

POLSKA MARKA BCS

BCS

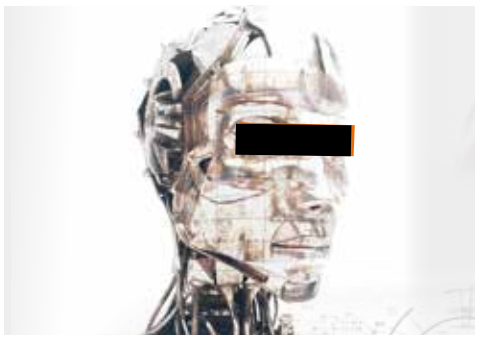
www.bcs.pl

www.facebook.com/bcspl

CZASOPISMO RYNKU SECURITY

a&S POLSKA

02 (44) / 2024



SEAGATE

Inteligencja. Bezpieczeństwo. Ochrona.

Usprawnij swoje rozwiązania z dyskami Seagate SkyHawk AI zaprojektowanymi z myślą o analityce video oraz SkyHawk przeznaczonymi do systemów monitoringu

- ✓ **Przeznaczone do całodobowych obciążeń roboczych**
- ✓ **Wyposażone w technologię ImagePerfect™**
- ✓ **Zapewniają wzrost niezawodności rozwiązania dzięki wbudowanemu oprogramowaniu SkyHawk Health Management[1]. Aktywnie zabezpiecza pamięć masową systemu monitoringu, oferując opcje prewencji i interwencji.**
- ✓ **Obejmują trzyletni plan Rescue Data Recovery Services[2] (usługi odzyskiwania danych).**

Rescue
DATA RECOVERY SERVICES

SKYHAWK AI™

Zoptymalizowany pod kątem użycia w analityce wideo i w zastosowaniach związanych z obrazowaniem.

Obejmuje zaawansowane funkcje i sprawdza się w pracy z rejestratorami NVR wykorzystującymi sztuczną inteligencję, serwerami i urządzeniami zapewniającymi możliwość analityki przy użyciu AI oraz pozwalającymi na głębokie uczenie.

SKYHAWK™

Przeznaczony do systemów monitoringu wyposażonych w rejestratory DVR oraz NVR i zapewnia pamięć masową zoptymalizowaną pod kątem monitoringu.

(1) Kompatybilność z pojemnościami wynoszącymi 4 TB i więcej.
(2) Rescue Data Recovery Services (usługi odzyskiwania danych) nie są dostępne we wszystkich krajach. Aby uzyskać szczegółowe informacje, należy skontaktować się z przedstawicielem handlowym firmy Seagate.

Więcej informacji znajdziesz u Autoryzowango Dystrybutora produktów Seagate

ALSO

Prezentujemy najnowsze urządzenia z oferty firm

Atline, Axis Communications, BCS (NSS), D+H Polska, EVVA, Hikvision, Linc Polska, TP-Link

ATLINE

Światłowodowy system DAS z lokalizacją punktów naruszenia

FIPRO to światłowodowy system detekcji przeznaczony do ochrony perymetrycznej obiektów, który można instalować zarówno pod ziemią, jak i na ogrodzeniach.

System wykorzystuje światłowód jako czujnik akustyczny zdolny do wykrycia wibracji pojawiających się na ogrodzeniach, w ziemi lub w rurociągach (np. w kanalizacji teletechnicznej czy w gazociągach). Alarmuje użytkownika po wykryciu prób naruszeń, takich jak przecinanie ogrodzenia, przejścia przez nie, odginanie ogrodzenia lub, w przypadku zakopanego kabla, przechodzenia po ziemi czy kopanie w niej w pobliżu czujnika.

FIPRO wykorzystuje sztuczną inteligencję do analizy i klasyfikacji zdarzeń alarmowych. Dzięki temu cechuje się niezwykle niskim współczynnikiem fałszywych alarmów i wysoką skutecznością detekcji. System występuje w wielu konfiguracjach – od analizatorów zdolnych do ochrony odcinka o długości do 10 km do mogących zabezpieczyć aż 100 km. Chroniony teren można podzielić na strefy alarmowe o długości nawet 10 m. Pomaga to w łatwym zlokalizowaniu ataku oraz w integracji z systemami CCTV. System jest dostępny w wersji redundantnej, wykorzystującej dwa kanały do analizy sygnałów z jednego odcinka, dzięki czemu działa nawet po przecięciu czujnika.

Ważną cechą zarówno FIPRO, jak i innych systemów proponowanych przez firmę Atline jest pochodzenie rozwiązań wyłącznie z krajów należących do NATO. Wyróżnia je nie tylko bardzo dobra jakość, ale również wysoki poziom cyberbezpieczeństwa, kluczowy w zabezpieczaniu infrastruktury krytycznej.

Więcej na: www.atline.pl

AXIS COMMUNICATIONS

AXIS Q1808-LE Bullet Camera do rejestrowania szczegółów z dużych odległości

Kamera AXIS Q1808-LE zapewnia wyjątkową rozdzielczość 4K i bardzo wysoką światłoczułość. Jest dostępna z obiektywem szerokokątnym do monitorowania otwartych przestrzeni lub z teleobiektywem do dozoru z dużej odległości.

Kamera wyposażona w przetwornik 4/3" zapewnia wyjątkową jakość obrazu nawet przy słabym oświetleniu, a dzięki rozwiązaniu Lightfinder 2.0 umożliwia wierne odwzorowanie kolorów, także w nocy. Ponadto ma zaimplementowaną jednostkę przetwarzania głębokiego uczenia, która zapewnia zaawansowane funkcje i wydajną analizę na poziomie urządzenia. Dostarcza cenne metadane ułatwiające szybkie, łatwe i wydajne wyszukiwanie materiałów – na żywo oraz zarejestrowanych.

Dzięki szerokiemu (12–48 mm) obiektywowi Canon i poziomemu polu widzenia 90–21° AXIS Q1808-LE idealnie nadaje się do dozoru dużych otwartych przestrzeni. Oferuje 4-krotny zoom i wyjątkową światłoczułość, aby zapewnić doskonałe szczegóły przydatne w dochodzeniach kryminalistycznych. Ponadto diody LED IR o białym świetle (850 nm) umożliwiają przełączenie na światło białe, aby zapobiegać niepożądanym działaniom.

Teleobiektyw Canon (50–150 mm) i poziome pole widzenia 21–7° sprawiają, że AXIS Q1808-LE idealnie nadaje się do rejestrowania szczegółów z dużych odległości. Dzięki dodatkowemu 3-krotnemu zoomowi sprawdza się przy identyfikacji. Ponadto zoptymalizowane oświetlenie IR umożliwia dozór w całkowitej ciemności do 150 m bez konieczności stosowania dodatkowego źródła światła.

Więcej na: www.axis.com/pl-pl

System kontroli dostępu RACS 5 w sektorze komercyjnym

roger
Intelligence for Building

- **Funkcjonalność**, dzięki której nie trzeba wybierać pomiędzy komfortem a bezpieczeństwem.
- **Design urządzeń** dobrze komponujących się z wnętrzami nowoczesnych przestrzeni biurowych.
- **Niezawodność** zapewniająca tysiącom użytkowników obiektu dostęp do ich miejsca pracy każdego dnia, przez wiele lat.
- **Efektywność** zarządzania przestrzenią, zasobami i użytkownikami dzięki integracji z aplikacjami biurowymi.
- **Redukcja** zużycia energii elektrycznej dzięki integracji z systemami windowymi oraz funkcjom automatyki budynkowej.

Wybrane realizacje






BCS

Kamera bispektralna BCS-L-TIP542FR5-THT-Ai1

BCS-L-TIP542FR5-THT-Ai1 to bispektralna kamera z rodziny BCS Line. Zamknięcie w jednej obudowie dwóch typów modułów: termowizyjnego i wizyjnego pozwala na korzystanie z zalet obu tych rozwiązań jednocześnie.

Kamera wizyjna o rozdzielczości 4 Mpix generuje szczegółowy obraz wysokiej jakości z zachowaniem idealnie odwzorowanych kolorów w dzień. W parze z promiennikiem podczerwieni o zasięgu 50 m i czułym przetwornikiem zapewnia odpowiedni poziom obserwacji również w nocy. Obsługa funkcji inteligentnych w zakresie ochrony obwodowej pozwala na detekcję przekroczenia linii i wtargnięcia w strefę. Analityka kamery pozwala na wykrycie używania telefonu komórkowego w miejscach, gdzie jest to zabronione.

Moduł termowizyjny to przetwornik mikrobolometrycznym z aktywnym materiałem pochłaniającym w postaci tlenku wanadu Vox ma rozdzielczość 256x192. Obiektyw o ogniskowej 7 mm zapewnia wykrywanie osób w odległości nawet 280 m. Zaletą modułu jest obserwacja termiczna z pomiarem temperatury w zakresie od -20 do 55°C, co idealnie sprawdza się jako funkcja alarmowa ostrzegająca przed pożarem. Urządzenie umożliwia monitorowanie do 12 stref/punktów, obsługuje też funkcje inteligentne.

Niezależnie od tego, na którym module wystąpi alarm, zostaje uruchomione powiadomienie optyczno-akustyczne dzięki wyposażeniu BCS-L-TIP542FR5-THT-Ai1 w ostrzegawcze diody LED i wbudowany głośnik. Do sygnalizacji lub odbierania alarmów można również wykorzystać moduł wejść/wyjść alarmowych.

Więcej na: www.bcs.pl

D+H POLSKA

Certyfikowany przeciwpożarowy wyłącznik prądu DH-PWP-1

W ofercie D+H Polska pojawił się nowy produkt – certyfikowany przeciwpożarowy wyłącznik prądu DH-PWP-1.

Zadaniem urządzenia jest odcięcie dopływu energii elektrycznej do wszystkich obwodów w budynku, z wyłączeniem obwodów zasilających urządzenia i instalacje, które muszą działać w trakcie pożaru.

Odłączenie zasilania powinno być jednoznacznie potwierdzone przez urządzenie sygnalizujące, będące elementem składowym PWP. Jego wyzwolenie powinno być możliwe zdalnie przez zewnętrzne urządzenie uruchamiające (np. przycisk sterujący PWP) lub miejscowo, bezpośrednio przy urządzeniu wykonawczym (np. ręczna dźwignia zabudowana w wyłączniku lub rozłączniku). Użycie PWP i zasygnalizowanie jego stanu pozwala jednostkom ratowniczo-gaśniczym PSP bezpiecznie i skutecznie prowadzić działania gaśnicze.

Zestaw DH-PWP-1 składa się z urządzenia wykonawczego i urządzenia sygnalizującego, który współpracuje z dostępnymi na rynku urządzeniami uruchamiającymi (ręczne przyciski przeciwpożarowego wyłącznika prądu), wprowadzonymi do obrotu zgodnie z obowiązującymi przepisami. Urządzeniem wykonawczym umieszczonym w wydzielonej obudowie jest aparat wykonawczy w postaci rozłącznika lub wyłącznika wraz z automatyką uruchamiającą, kontrolną i sterującą, stanowiący element mechanicznego odłączenia dopływu energii elektrycznej do budynku. Urządzeniem sygnalizującym jest urządzenie, które przez sygnalizację optyczną wskazuje jednoznacznie, że zasilanie w obiekcie zostało wyłączone.

Więcej na: www.dhpolska.pl

EVVA

Nowa wersja EVVA AirKey

AirKey to elektroniczny system zamknięć przeznaczony do współpracy z nową generacją urządzeń mobilnych, będący odpowiedzią na dynamicznie zmieniające się środowisko pracy i życia prywatnego.

AirKey to wygodne przekazywanie kluczy przez Internet bezpośrednio na smartfon i wiele inteligentnych funkcji, przy zachowaniu najwyższych standardów bezpieczeństwa.

W systemie EVVA AirKey kluczem jest smartfon. W nowej wersji zwiększono bezpieczeństwo oraz wydajność dzięki nowemu chipowi Smart MX3, a także nowemu procesorowi w gałce i rotorze. Wprowadzono więcej funkcji interfejsu, usprawniono szybkość otwierania się i blokowania wkładki oraz wydłużono żywotność baterii.

AirKey to elastyczność użytkowania: przesyłanie „klucza" poprzez wiadomości SMS bezpośrednio na telefon użytkownika, bezpłatna dedykowana aplikacja na systemy iOS i Android, administracja online, multiadministracja oraz maksymalna ochrona danych. Dzięki modułowej budowie wkładkę łatwo się montuje, a jej długość można dostosować do drzwi także w późniejszym czasie.

AirKey to idealne rozwiązanie do rozproszonych lokalizacji i pomieszczeń współdzielonych, do których dostęp ma wielu użytkowników. Sterowanie elektronicznymi elementami zamykającymi (np. drzwiami, szlabanami) odbywa się za pomocą czytnika naściennego AirKey. Do zabezpieczania szaf i pomieszczeń magazynowych służą kłódki, a do zamknięć kontenerków archiwizacyjnych, szafek czy skrzynek pocztowych wkładki dźwigniowe. W systemie AirKey można także korzystać z breloków, kart dostępowych lub kluczy kombi.

Więcej na: www.evva.com/pl-pl/

Honeywell

35 NOWA SERIA KAMER

ZWIĘKSZ ŚWIADOMOŚĆ - NIE KOSZTY

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

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

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

OFICJALNY DYSTRYBUTOR:

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

www.linc.pl

WIĘCEJ O NAS:

Linc Polska Sp. z o.o.

HIKVISION POLSKA

Punkty dostępowe DS-3WAP622G-SI i routery AC DS-3WG210GP-SI

Stabilna i bezpieczna łączność bezprzewodowa jest w dzisiejszych czasach jednym z kluczowych elementów w transmisji danych i dostępie do sieci nie tylko dla użytkowników prywatnych, ale też systemów informatycznych wspomagających przemysł, logistykę, handel czy bezpieczeństwo.

Aby sprostać coraz wyższym wymaganiom w transmisji bezprzewodowej, Hikvision wprowadza na rynek nową grupę urządzeń sieciowych. Access Pointy z serii DS-3WAPxxx są przeznaczone głównie do zastosowań w sieciach małych, średnich i mikroprzedsiębiorstwach, gdzie znaczenie ma wysoka niezawodność, możliwości administrowania siecią oraz liczba jednocześnie połączonych hostów.

DS-3WAP622G-SI to punkt dostępowy Wi-FI 6 (802.11ax) o maks. przepustowości bliskiej 1800 Mb/s, który obsłuży jednocześnie do 256 urządzeń klienckich, a dwuzakresowe radio i cztery dookólne anteny o zysku do 4 dBi zapewnią odpowiedni poziom i jakość sygnału. Dla obiektów wymagających uruchomienia sieci bezprzewodowych z wieloma punktami dostępowymi urządzenia dodatkowo wspierają szybki roaming hostów między AP, aby zapewnić komunikację bez przerw w transmisji.

Uzupełnieniem oferty są routery AC (np. DS-3WG210GP-SI) pełniące dodatkowo funkcję centralnego kontrolera sieci bezprzewodowej, który umożliwia pełne wykorzystanie funkcjonalności punktów dostępowych, m.in. jednoczesne uruchomienie i rozgłaszanie do 8 SSID czy VLAN binding.

Więcej na: www.hikvision.com/pl

LINC POLSKA

Teledyne FLIR – najnowsza seria kamer termowizyjnych FC-AI

Najnowszy model z portfolio Teledyne FLIR – kamera termowizyjna z serii FC-AI IR z wbudowaną analityką precyzyjne klasyfikuje ludzi oraz pojazdy, umożliwiając wczesne wykrywanie obiektów w strefie perymetrycznej.

Dzięki analityce wideo, która łączy głęboką sieć neuronową (DNN) i analizę opartą na ruchu, sztuczna inteligencja serii FC Ai oferuje wiodące w branży wykrywanie włamań, umożliwiając użytkownikom poszerzenie świadomości sytuacyjnej i podejmowanie bardziej świadomych decyzji.

Kamera jest wyposażona w wysokiej jakości przetwornik termowizyjny o rozdzielczości 640x512 pikseli. Czułość termiczna (NETD) sięgająca mniej niż 25 milikelwinów (mK) umożliwia widoczność i wysoką skuteczność wykrywania nawet w niesprzyjających warunkach, co wyróżnia kamerę na tle konkurencji. Dostępność ośmiu wysokiej jakości obiektywów o polu widzenia od 8,6°×6,6° do 90°×69° oraz sztuczna inteligencja serii FC umożliwiają operatorowi wyraźne widzenie i wykrywanie wtargnięć nawet w całkowitej ciemności, deszczu, mgle i dymie. Korzystając z biblioteki tysięcy obrazów termowizyjnych, analityka klasyfikuje obiekty w rzeczywistych sytuacjach, w których mogą być one lekko przesłonięte lub trudne do zidentyfikowania. Kamera FC-Ai oferuje też możliwości geolokalizacji celu i precyzyjne przekazywanie sygnału do głowicy PTZ w celu usprawnienia śledzenia obiektu.

Kamera jest zgodna z dyrektywą NDAA. Została wyposażona w wytrzymałą obudowę, odporną na warunki atmosferyczne o klasie IP66 i IP67 oraz wandaloodporności IK10.

Więcej na: www.linc.pl

&

TP-LINK

TP-Link VIGI VMS – kompleksowe narzędzie do zarządzania systemem CCTV

TP-Link uzupełnia swoją ofertę rozwiązań do monitoringu wizyjnego, wprowadzając zaawansowane narzędzie do centralnego zarządzania systemem CCTV – VIGI VMS *(Video Management System).*

TP-Link VIGI VMS to konsola do centralnego zarządzania urządzeniami z serii VIGI. Oprogramowanie oferuje bogatą funkcjonalność przeznaczoną do dużych sieci CCTV, również rozproszonych. Wygodny pulpit i centrum monitoringu umożliwiają intuicyjne dodawanie urządzeń oraz zarządzanie ustawieniami kamer i rejestratorów. Wszystkie opcje są dostępne z poziomu jednego interfejsu. Na panelu można m.in. ustawić reguły zdarzeń, alertów czy aktualizacji urządzeń. VIGI VMS pozwala również na wgranie mapy obiektu i umieszczenie na niej wdrożonych urządzeń. Umożliwia to stworzenia wirtualnego środowiska do podglądu budynku.

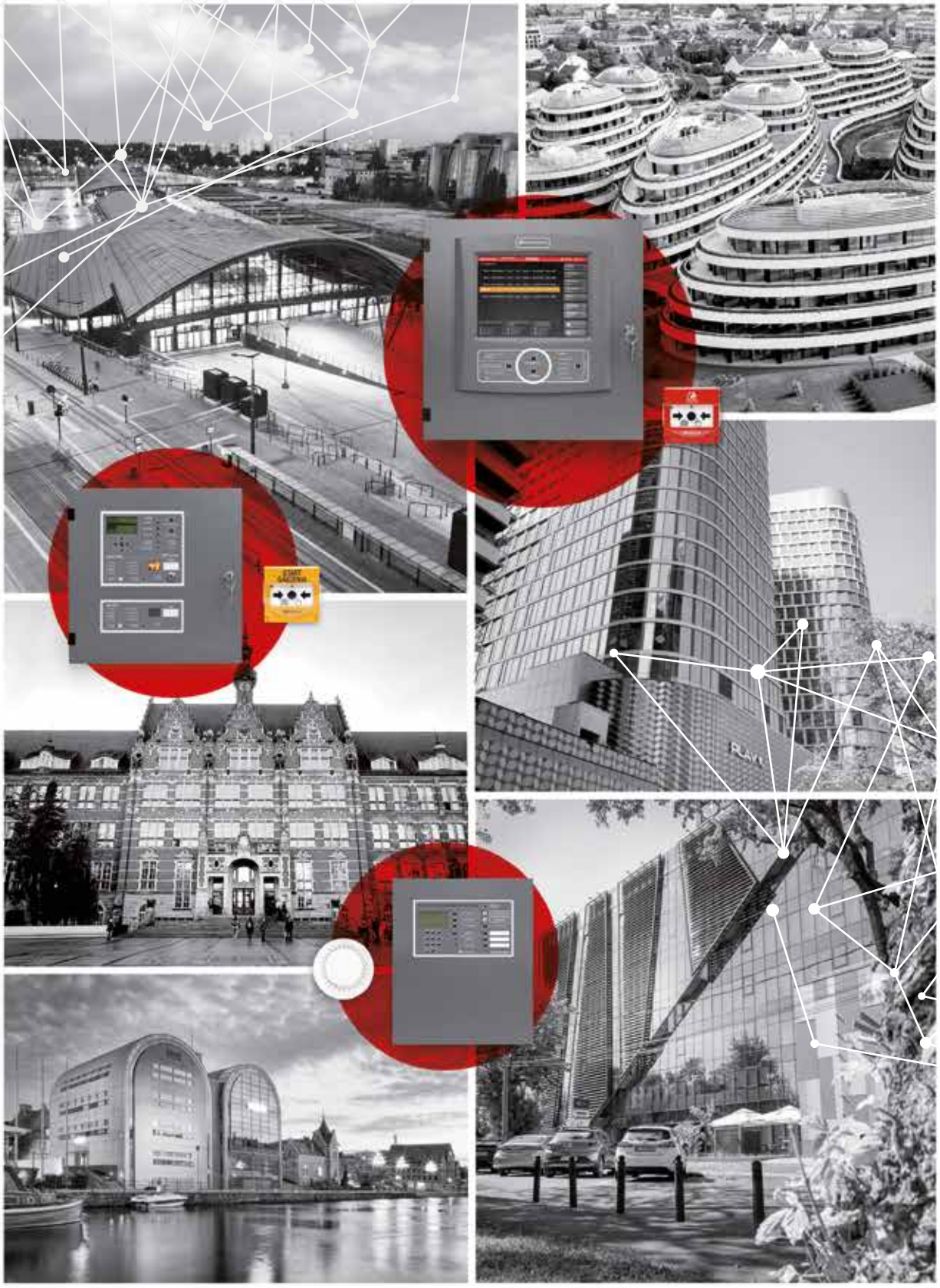
VIGI VMS to oprogramowanie działające w systemie serwer-klient. Wraz z VMS można instalować aplikacje klienckie na stanowiskach operatorów, którzy po zalogowaniu otrzymają dostęp do zdefiniowanych przez administratora urządzeń i uprawnień.

Aplikacja kliencka umożliwia podgląd obrazu na żywo, odtwarzanie nagrań archiwalnych oraz przegląd i filtrowanie zdarzeń Smart zarejestrowanych przez kamery.

Narzędzie jest w pełni kompatybilne ze wszystkimi produktami z serii VIGI. Intuicyjny interfejs użytkownika sprawia, że z konfiguracją i obsługą systemu poradzą sobie nawet mniej zaawansowani użytkownicy. Bezpłatne oprogramowanie VIGI VMS w języku polskim można pobrać bezpośrednio ze strony TP-Link.

Więcej na: www.tp-link.com/pl

POLON-ALFA

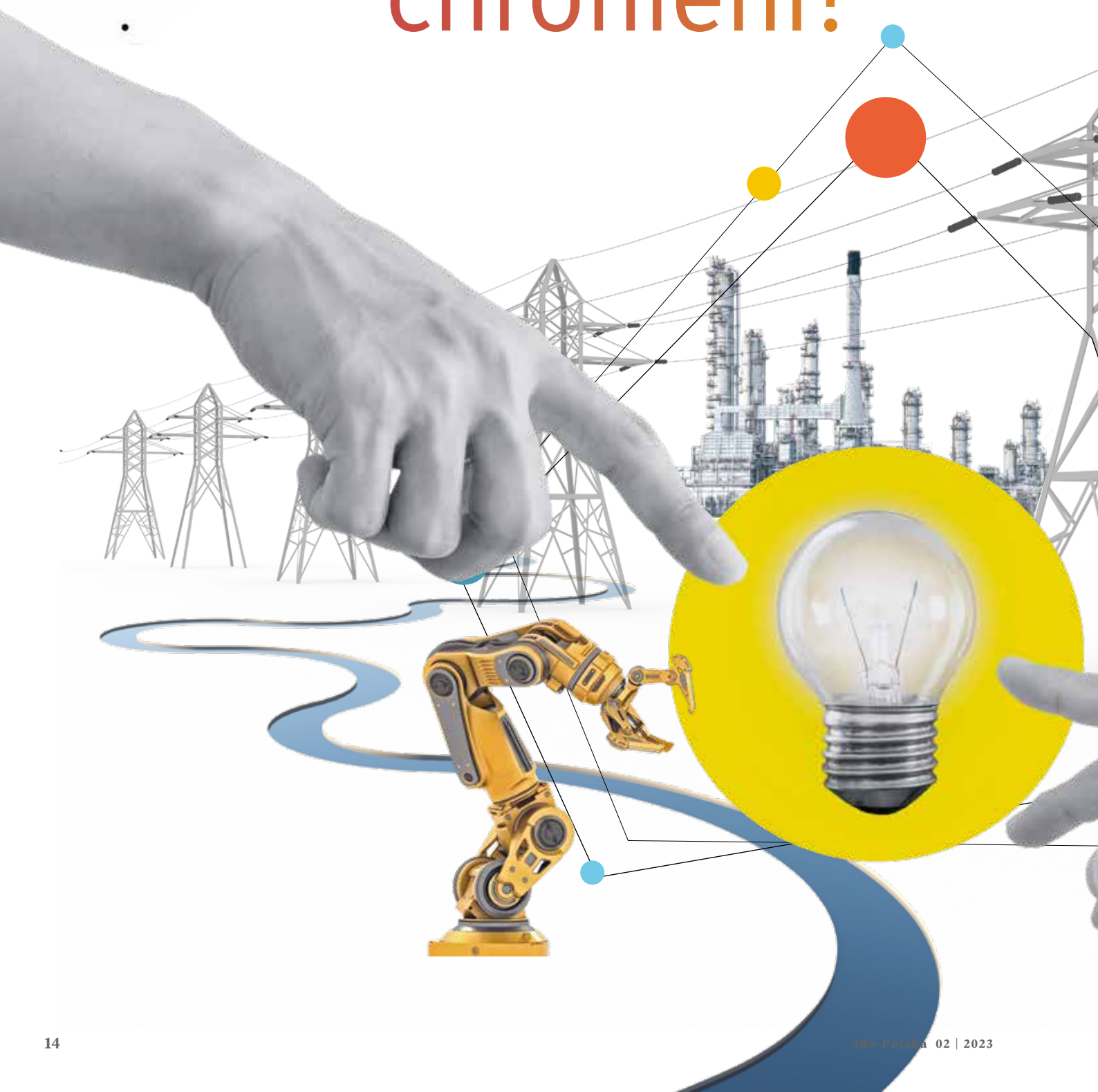


tradycyjnie KOMPLEKSOWA OCHRONA

tysięcy obiektów w kraju i za granicą

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

Raport: Jak jesteśmy chronieni?



Nad bezpieczeństwem obywateli w Polsce stale czuwają służby – policja, wojsko, straż pożarna, medyczne i inne. W nadzwyczajnych sytuacjach zapewniają je także wytyczne infrastruktury krytycznej, czyli systemy cybernetyczne oraz rzeczywiste, które mają gwarantować minimalne funkcjonowanie państwa i gospodarki w czasie kryzysu. Znaleźliśmy się właśnie w momencie, kiedy „w razie kryzysu" jest bardziej prawdopodobne niż kiedykolwiek. Jak wygląda stan gotowości na kryzys? Sprawdzamy!

Adela Prochyra

Stare chińskie przysłowie, będące de facto przekleństwem „Obyś żył w ciekawych czasach" ziszcza się na naszych oczach. Kwestie (potencjalnie) niebezpieczne nie są związane z konkretnym obszarem. Dotyczą różnych sfer rzeczywistości. Po wielu latach pokoju Polska musi liczyć się z ryzykiem wojny – już nie tylko w najbliższym sąsiedztwie, ale także na własnym terytorium. A to dopiero początek. Powiązane z rosyjską agresją, a także całkiem od niej niezależne cyberataki to drugie zagrożenie, z którym należy się stale liczyć. Trzecim, być może najpoważniejszym problemem, który nie ujawnił się jeszcze w pełnej skali, są zmiany klimatyczne. Ocieplenie klimatu ma wpływ na cały ekosystem, a jego skutki będą dotkliwie odczuwalne przez obywateli i kraje. Od lat przestrzegają przed nim naukowcy, namawiając liderów państw i korporacji do podjęcia bardzo zdecydowanych działań na rzecz ochrony środowiska naturalnego. Te z kolei bywają źle przyjmowane przez grupy społeczne, jak miało to miejsce niedawno w przypadku europejskich rolników protestujących m.in. przeciwko założeniom Zielonego Ładu.

Skutki dla codziennego funkcjonowania miast i wsi mogą być różne: awarie sieci energetycznych, awarie wodociągów, utrata danych lub upublicznienie i/lub wykorzystanie danych niejawnych, *blackout*. Mogą być one zarówno spowodowane przez katastrofy naturalne, jak i wywołane działalnością człowieka, w tym przez zagrożenia terrorystyczne czy zdarzenia techniczne. Przyczyna to jedno – bardziej interesujący jest dla obywatela stan gotowości na potencjalne zdarzenia. Wiele danych w tym zakresie jest niejawnych, dlatego w raporcie znalazły się jedynie wybrane zagadnienia. Mamy pełną świadomość, że obszarów kluczowych dla bezpieczeństwa jest więcej.

Dlatego w tym kontekście zwłaszcza trafne wydaje się inne łacińskie przysłowie: „Jeśli chcesz pokoju, szykuj się do wojny". Do zagrożenia należy więc przygotować się z wyprzedzeniem, a ten obowiązek spoczywa na państwach w sposób szczególny. Właśnie temu ma służyć m.in. infrastruktura krytyczna (IK). Ten termin określa obiekty, urządzenia, usługi i instalacje kluczowe dla bezpieczeństwa państwa, administracji, gospodarki i społeczeństwa. Należy jednak pamiętać, że nie wszystkie strategiczne obiekty są automatycznie częścią infrastruktury krytycznej. Istnieje szereg szczegółowych kryteriów, które decydują o tym, czy dany obiekt zostanie zaklasyfikowany jako IK. Kryteria te są zawarte w niejawnym załączniku do Narodowego Programu Ochrony Infrastruktury Krytycznej.

O dziwo, myślenie w tych kategoriach pojawiło się późno, bo dopiero w latach 90. XX wieku, po gigantycznych awariach sieci energetycznych w USA i Kanadzie. Ich bardzo poważne i rozległe skutki uświadomiły rządom potrzebę ochrony kluczowych elementów infrastruktury. To doprowadziło do opracowania strategii ochrony IK w Unii Europejskiej. W roku 2004 Rada Europejska wezwała do przygotowania ogólnej strategii ochrony infrastruktury krytycznej, a Komisja Europejska ogłosiła propozycje usprawnienia systemów zapobiegania i reagowania na ataki na IK. W roku 2005 opublikowano Zieloną Księgę inicjującą konsultacje w sprawie programu ochrony IK, a Rada ds. Wymiaru Sprawiedliwości i Spraw Wewnętrznych wezwała do utworzenia Europejskiego Programu Ochrony Infrastruktury Krytycznej (EPOIK). Odpowiedzialność za ochronę IK spoczywa na państwach członkowskich UE, właścicielach, operatorach i użytkownikach IK. W Polsce prace nad Narodowym Programem Ochrony Infrastruktury Krytycznej (NPOIK) rozpoczęto w 2007 r. Programów i strategii na rzecz zapewnienia bezpieczeństwa jest w Polsce kilka i wzajemnie się one uzupełniają (patrz: ramka).

Dokumenty państwowe organizujące system bezpieczeństwa narodowego

- Narodowy Program Ochrony Infrastruktury Krytycznej – publikowany co roku na stronie Rządowego Centrum Bezpieczeństwa
- Strategia bezpieczeństwa narodowego Rzeczypospolitej Polskiej – obecnie obowiązuje z 2020 r., podpisana przez prezydenta RP Andrzeja Dudę
- Strategia rozwoju systemu bezpieczeństwa RP
- międzynarodowe porozumienia, których RP jest stroną

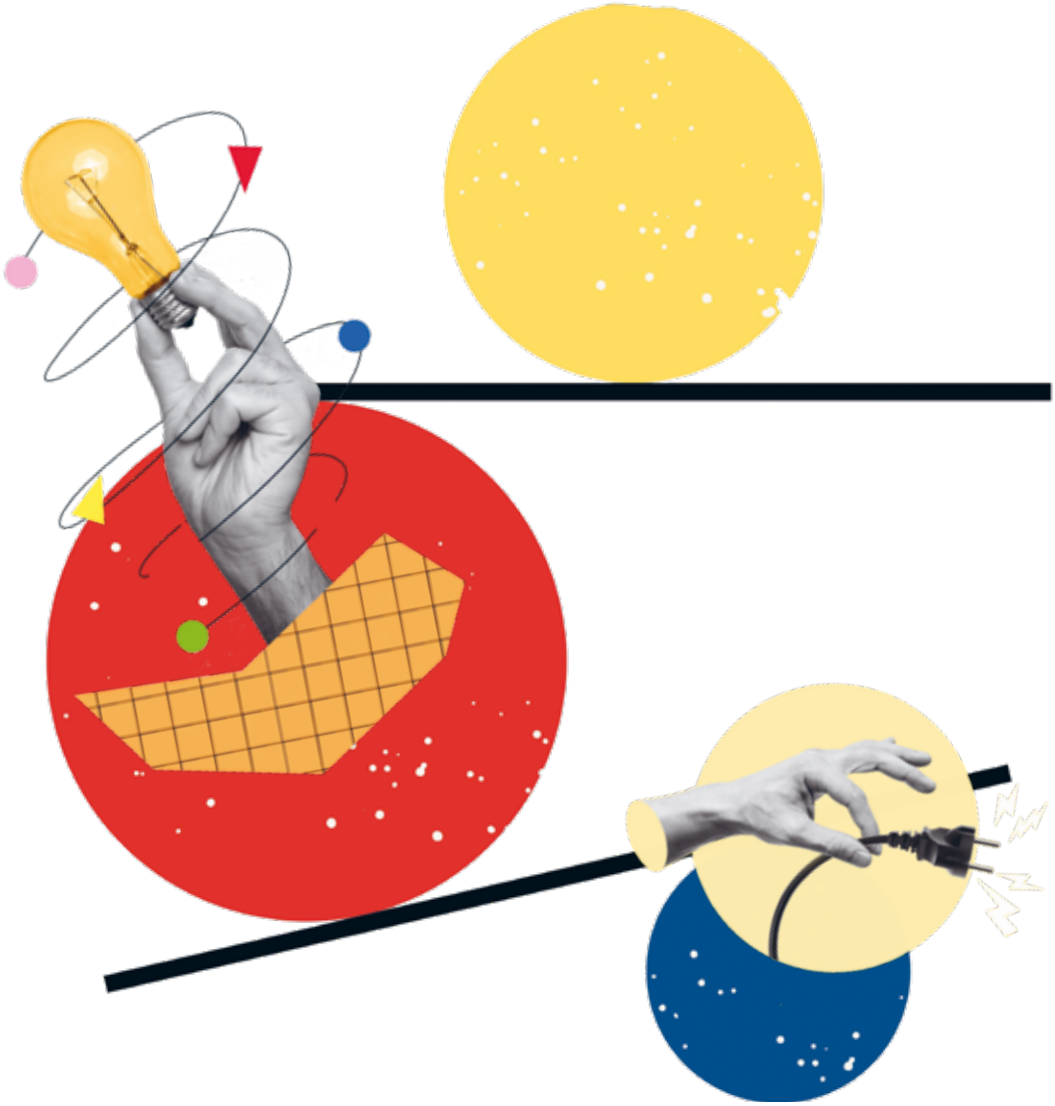
Ochrona w praktyce

Głośnym echem odbił się raport Naczelnej Izby Kontroli, z którego wynika, że jako kraj jesteśmy nieprzygotowani do zapewnienia obywatelom bezpieczeństwa w razie ataku lub klęski żywiołowej. Według danych miejsca w schronach i ukryciach w razie ataku lub katastrof naturalnych wystarczy dla 4% ludności Polski (1 428 369 osób).

W raporcie NIK wskazano również, że wiele schronów jest wykorzystywanych na inne cele, np. jako magazyny lub garaże. Napisano w nim: „Polska należy do krajów o najniższym poziomie zabezpieczenia potrzeb obywateli pod tym względem". Kontrola NIK wykazała, że aż sześć z 32 skontrolowanych gmin nie zapewniło żadnego miejsca schronienia swoim mieszkańcom, a obywatele nie są informowani, gdzie powinni szukać schronienia w razie zagrożenia. Stan techniczny schronów i ukryć również jest alarmujący. 68% schronów i ponad połowa ukryć nie spełnia wymaganych norm. Oznacza to, że w razie potrzeby te miejsca nie zapewnią odpowiedniej ochrony. Obywatele (ponad 80% badanych) nie wiedzą, gdzie znajduje się miejsce schronienia w pobliżu miejsca ich zamieszkania. W sytuacji realnego zagrożenia nie do końca pomoże aplikacja www.schrony.straz.gov.pl, która powstała na potrzeby… inwentaryzacji w Państwowej Straży Pożarnej. Wskaże ona bowiem wszystkie znajdujące się w okolicy miejsca schronienia, ale nie pokieruje do tego, gdzie faktycznie są miejsca. PSP nie jest w stanie wziąć odpowiedzialności za ocenę stanu poszczególnych obiektów ani za to, czy obiekty te zabezpieczą ludzi podczas konfliktu zbrojnego.

Wytyczne szefa obrony cywilnej z 2018 r. mówią, że miasta i gminy powinny zapewnić miejsce doraźnego schronienia co najmniej 25% zameldowanej ludności na danym obszarze administracyjnym, i uwzględniać plany ewakuacji III stopnia pozostałej części. Spośród poddanych kontroli samorządów tylko 31% spełniało te wymagania. Ciekawie prezentuje się na tym tle Warszawa, która w 2022 r. nie posiadała budowli ochronnych (schronów i ukryć) w rozumieniu wytycznych SOC, a jedynie „potencjalne miejsca ukrycia dla mieszkańców stolicy na wypadek zewnętrznego zagrożenia państwa". Taki tytuł nosi dokument, przygotowany przez urząd miasta, w którym można znaleźć lokalizację tego typu miejsc w poszczególnych dzielnicach. Nie jest jednak znany ich stan techniczny ani faktyczne przygotowanie na wypadek zagrożenia. Miasto zakłada, że mogłoby w nich znaleźć ok. 64% mieszkańców Warszawy. Brakuje też budowli przeznaczonych na miejsca do kierowania obroną cywilną.

Druga istotna bolączka wynika z tego, że w wyniku zmiany Ustawy o obronie Ojczyzny w marcu 2022 r. ochrona cywilna przestała istnieć. Od tego czasu na jej czele stał szef Państwowej Straży Pożarnej. Zwrot akcji nastąpił w marcu 2024 r., kiedy to Minister Obrony Narodowej poinformował, że na czele obrony cywilnej stanie szef MSWiA Marcin Kierwiński. Projekt stosownej ustawy ma niebawem trafić do konsultacji społecznych, a sam akt prawny – jak podkreślają rządzący – ma być jednym z najważniejszych procedowanych w tej kadencji Sejmu. Jednocześnie Lewica zapowiedziała złożenie projektu małej ustawy schronowej, która miałaby uprościć Prawo budowlane właśnie w kontekście budowy schronów przydomowych. Ma ona też wprowadzić procedury dotyczące systemu alarmowania ludności w sytuacji kryzysowej, przebiegu dróg ewakuacyjnych, zapasów leków i żywności. Brak regulacji prawnych to jedno. Eksperci podkreślają też niski poziom edukacji społeczeństwa w tym zakresie (dla porównania: w Finlandii wiedzę tę wprowadza się już w przedszkolach)



i bardzo niskie nakłady z budżetu – na ten cel przeznacza się zaledwie 0,1% PKB Polski.

Bezpieczeństwo energetyczne

Jednym z filarów bezpieczeństwa współczesnego państwa jest stabilny i niezawodny dostęp do energii elektrycznej. Napędza ona wszystkie dziedziny życia, od infrastruktury krytycznej po gospodarstwa domowe. Polska konsekwentnie dywersyfikuje źródła pozyskiwania energii i rozbudowuje nowoczesną infrastrukturę. Przy coraz gorszej rentowności kopalń i rosnącej świadomości klimatycznej pozycja polskiego węgla jako gwaranta naszego bezpieczeństwa energetycznego może być nie do obrony. Bezpieczeństwo energetyczne to możliwość nie tylko zaspokojenia potrzeb gospodarki i obywateli, ale także utrzymania ciągłości dostaw energii w razie wyjątkowych zdarzeń. Jak wygląda to w praktyce?

Okazuje się, że groźny dla bezpieczeństwa obywateli może być… upał. Już teraz elektrownie muszą liczyć się ze wzmożonym zapotrzebowaniem na energię właśnie w gorących okresach, a nie padło jeszcze ostatnie słowo w sprawie temperatur w naszym kraju. 15 sierpnia 2023 r. południe Polski znalazło się na skraju *blackoutu*. Elektrownia w Jaworznie pracowała tego dnia na rezerwie mocy (zaledwie 627 MW ponad zapotrzebowanie). Tauron, operator, wyjaśnił, że tamtego dnia miała miejsce wysoka generacja z OZE, dlatego rano blok węglowy 910 MW został odstawiony do rezerwy. Miał wznowić pracę wieczorem, ale kiedy ilość energii słonecznej malała, a zapotrzebowanie rosło, elektrownia węglowa musiała

» *Groźny dla bezpieczeństwa obywateli może być upał. Już teraz elektrownie muszą liczyć się ze wzmożonym zapotrzebowaniem na energię w gorących okresach, a nie padło jeszcze ostatnie słowo w sprawie temperatur w naszym kraju.* «

szybko wznowić pracę. Moment rozruchu jest newralgiczny, bywa, że dochodzi wówczas do awarii. Właśnie tak jak 15 sierpnia. Polskie Sieci Elektroenergetyczne w trybie awaryjnym importowały więc dużą ilość energii na zasadzie międzysystemowej pomocy międzyoperatorskiej – 2,6 GWh z Niemiec, ze Szwecji (przez Litwę) i Słowacji. Po cenach, oczywiście, zawyżonych. Co nie zadziałało w protokole krajowym, że doszło do takiej sytuacji?

Procedura zwyczajowo wygląda następująco: w sytuacji, gdy planowana nadwyżka energii jest niższa niż 9% (to minimum bezpieczeństwa pracy systemu energetycznego) ponad zapotrzebowanie, ogłaszany jest tzw. okres przywołania na rynku mocy, czyli stan gotowości dla wszystkich elektrowni, które mają podpisane umowy z PSE. Kiedy rezerwa mocy wynosi mniej niż 5% prognozowanego zapotrzebowania na energię, takie ogłoszenie zapotrzebowania jest obowiązkowe. Wówczas wszystkie jednostki objęte umową mocową mają obowiązek wystawić do dyspozycji operatora tyle mocy, ile zadeklarowały w umowie. Elektrownia, która zgłasza zapotrzebowanie, powinna to zrobić z co najmniej 8-godzinnym wyprzedzeniem. W Jaworznie ten okres nie został zachowany, a złożyło się na to kilka czynników – godzina awarii była późna, a inne bloki, które mogłyby przejąć jej funkcję, miały zaplanowane remonty.

Cyberbezpieczeństwo

Szef Wydziału Ochrony Infrastruktury Krytycznej Rządowego Centrum Bezpieczeństwa dr Witold Skomra podczas panelu *Łączność i komunikacja kluczem do budowy sprawnego systemu ochrony ludności* na Kongresie Odporności 24 mówił wprost: „Cyberataki trwają od dłuższego czasu i są liczne. My już jesteśmy na wojnie". Przykład? Ataki bierne oparte na analizie ulotu elektromagnetycznego w celu pozyskania informacji – są one szczególnie problematyczne, bo nie wiadomo, czy zostaliśmy zaatakowani – lub aktywne za pomocą wysokoenergetycznych impulsów elektromagnetycznych. Cel jednego i drugiego jest ten sam: zaburzyć łączność. Obecnie w Polsce każda służba na swój system łączności – nie istnieje żaden uniwersalny system dla wszystkich. A zagrożeń z roku na rok przybywa. Nie pomagają obecny system certyfikacji oraz brak ogólnokrajowego systemu komunikacji krytycznej. Także prywatne sieci nie są przygotowane na kryzys, w tym np. całkiem realny 24-godzinny *blackout*.

Innego rodzaju zagrożeniem jest brak łączności, kiedy w jednym miejscu zgromadzi się duża grupa ludzi, którą można porównać do rodzaju żywego DDoS. Polkomtel zagospodarowuje tę lukę i uruchamia pierwszą ogólnopolską sieć łączności krytycznej w technologii LTE. Działa ona w wydzielonym paśmie 420 MHz, pod nazwą PLUS MCX *(Mission Critical X-Services),* zapewniając niezawodną komunikację dla służb mundurowych, organów zarządzania kryzysowego, energetyki, przemysłu i innych kluczowych sektorów. Sieć Polkomtela została wpisana jako system dyspozytorski, a zatem wyjęto ją spod wymogów Unii Europejskiej dotyczących równości, dzięki czemu ma własne systemy zasilania zapewniające dłuższą pracę. Obecnie prace są zaawansowane w 40%, a projekt ma zostać zrealizowany do końca br. Wiadomo jeszcze jedno – pasmo jest opłacone przez operatora do 2036 r., a w nim zabezpieczonych jest ok. 400 pozwoleń radiowych na stacje bazowe.

Podobne rozwiązania to m.in. FirstNet w USA, Rakel w Szwecji, Astrid w Belgii, ESN w Wielkiej Brytanii. Nad analogicznym rozwiązaniem pracuje PGE – LTE 450, jednak sieć ma ruszyć do 2025 r.

Niezależnie od systemu w przypadku zagrożenia powinna obowiązywać zasada „pracy w ciszy radiowej", ponieważ każdy system może paść od naporu liczby użytkowników, jak podsumował płk Piotr Turek z Dowództwa Komponentu Wojsk Obrony Cyberprzestrzeni.

Stan przygotowań na dziś

O bezpieczeństwie państwa i jego obywateli decyduje wiele czynników, które w niniejszym raporcie nie zostały wymienione. Nie wynika to z zaniedbania, ale z dużej złożoności tej struktury. Poza podanymi przykładami jest jeszcze wiele istotnych obszarów, które nie kojarzą się może bezpośrednio z bezpieczeństwem, ale mają na nie ogromny wpływ. Na przykład zabezpieczenie farmaceutyczne, które obecnie opiera się na komponentach z Chin – aż 80% dostarczanych jest do Unii z Państwa Środka.

Jeżeli chodzi o kluczowe elementy bezpieczeństwa, na pewno w ostatnich miesiącach znacznie zwiększyła się jego świadomość zarówno społeczeństwa, jak i rządzących. Świadczy o tym chociażby przyspieszenie ustawodawcze, jakie można było zaobserwować od początku tego roku. Ministerstwo Cyfryzacji powołało na stałe zespół doradczy PL/AI Sztuczna inteligencja dla Polski, który składa

» W ostatnich miesiącach znacznie zwiększyła się świadomość istotności bezpieczeństwa zarówno wśród społeczeństwa, jak i rządzących. Świadczy o tym chociażby przyspieszenie ustawodawcze, jakie można było zaobserwować od początku tego roku. «

Wyjaśniamy

Ulot elektromagnetyczny to rodzaj ataku polegający na podsłuchu informacji poufnych za pomocą fal elektromagnetycznych emitowanych przez urządzenia elektryczne. Atak ten jest możliwy, ponieważ każde urządzenie elektryczne podczas pracy generuje fale elektromagnetyczne, które mogą zawierać informacje poufne, takie jak dane logowania, hasła, a nawet rozmowy telefoniczne.

Atakujący może odebrać te fale elektromagnetyczne za pomocą specjalistycznego, choć łatwo dostępnego i niedrogiego sprzętu, a następnie zdekodować je, aby uzyskać dostęp do informacji poufnych. Ulot elektromagnetyczny może być przeprowadzony z dużej odległości, co utrudnia jego wykrycie i zapobieganie mu.

się z naukowców, przedsiębiorców i programistów z dużymi sukcesami na koncie. Mają oni rekomendować zastosowania sztucznej inteligencji dla usprawnienia różnych obszarów w państwie. Oprócz wspomnianych ustaw – o obronie narodowej i małej ustawy schronowej – planowane są też prace nad rozwijaniem Rządowego Centrum Bezpieczeństwa i przywrócenie łączności między różnymi wyspecjalizowanymi służbami oraz instytucjami państwa na rzecz szybkiego reagowania w razie zagrożenia. A skoro mówimy o planach, oznacza to, że niektóre mechanizmy nie są jeszcze wypracowane i należycie sprawdzone. Istniejące mechanizmy, jak pokazuje przykład elektrowni w Jaworznie, także bywają zawodne. MON zapewnia jednak, że prace nad konkretnymi rozwiązaniami wynikającymi z przyjętej ustawy o obronie cywilnej i ochronie ludności mają rozpocząć się jeszcze przed wakacjami.

Dużą zmianą na rzecz proaktywego zarządzania ryzykiem bezpośrednio w przedsiębiorstwach będzie wejście w życie dyrektywy w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii Europejskiej, tzw. NIS2 (więcej na ten temat na s. 32). ●

Na co jesteśmy gotowi: na wojnę czy na defiladę? O znaczeniu polityk bezpieczeństwa

Wojna w Ukrainie, której rezultaty mają dalekosiężne konsekwencje dla bezpieczeństwa na świecie, spowodowała, że Polska stoi przed koniecznością wzmocnienia ochrony swojej infrastruktury krytycznej. Pilnie potrzebne są rozwiązania wspierające opracowane przez państwa Europy.

Janusz Syrówka

Sytuacja na wschodzie naszego kraju oznacza konieczność zmierzenia się takimi wyzwaniami jak sabotaż, szpiegostwo, ataki cybernetyczne i być może konieczność zmierzenia się utratą pracowników, którzy zostaną zmobilizowani do obrony kraju. Skuteczna ochrona wymaga szerokiego zaangażowania finansowego, organizacyjnego, a także pełnego wsparcia ze strony zarządu i pracowników firm energetycznych.

O co chodzi – czyli cały ten strach

Konflikt w Ukrainie pokazuje skutki tak zwanych działań kinetycznych, czyli potocznie mówiąc, wojny pełnoskalowej i tym wszystkim, co taka wojna ze sobą niesie: atakami bombowymi, wjazdem czołgów itp. Jak realne jest widmo takiej wojny w przypadku Polski – nie wiem. Jest wielu ekspertów, którzy w tej dziedzinie są bardziej kompetentni. Mam jednak wrażenie, że w odniesieniu do konfliktu w Ukrainie łatwo wpaść w pułapkę tego, że szykujemy się do wojny, która już była. Obawiam się, że przed nami trudne lata nacechowane niejednoznacznością.

Destabilizacja przed nami

Wspólnym mianownikiem działań, jakich moim zdaniem możemy się spodziewać, jest destabilizacja, lęk i podsycanie niepokojów społecznych. Jest wiele metod, aby to osiągnąć. Do tej pory doświadczaliśmy głównie działań dla uproszczenia nazywanych cyberatakami oraz kampanii dezinformacyjnych w mediach społecznościowych. Prawdopodobnie na tym się nie skończy.

Działania w strefie wirtualnej mogą zostać uzupełnione o przedsięwzięcia w rzeczywistości fizycznej. Ich cechą wspólną będzie jednak to, że sprawcy bądź inspiratorzy pozostaną trudni do zidentyfikowania. Idealną platformą do prowadzenia takich działań będzie zapewne radykalizujący się wszelkich maści aktywizm: od ekologów, przez rolników, po ruchy o podłożu politycznym.

Infrastruktura krytyczna jako atrakcyjny cel

Infrastruktura krytyczna to zawsze atrakcyjny cel ataków. Pozbawianie ludności dostępu do towarów i usług z perspektywy atakującego wywołuje pożądane skutki. Takie działania powodują wymierne straty, sieją niepokój w społeczeństwie i podważają zaufanie do państwa, które może wydawać się bezbronne i nieudolne wobec zagrożeń. Umiejętne podsycanie zagrożenia prędzej czy później sprowokuje do zwiększenia wysiłków na rzecz podniesienia bezpieczeństwa.

To oczywiście dobrze, ale pamiętajmy, że w czasie pokoju źródłem zagrożeń są głównie siły natury i poważne awarie. Rozszerzając katalog zagrożeń, automatycznie zwiększamy koszty prowadzenia działalności. To wiąże się z pogorszeniem konkurencyjności względem tych, którzy takich środków nie muszą podejmować. Pojawia się więc kolejne wyzwanie, jak nie dać się wmanewrować w spiralę obciążeń i wydatków, które będą podsycane strachem, a nie chłodną oceną ryzyka.

Działania na rzecz bezpieczeństwa jako obciążenie

Zabezpieczenie obiektów infrastruktury krytycznej wiąże się z wysokimi kosztami finansowymi i organizacyjnymi, co dla wielu przedsiębiorstw stanowi znaczne obciążenie. Pomimo to zaniedbanie tych działań może przynieść jeszcze większe straty w przypadku wystąpienia kryzysu. Przez ostatnie lata, które w naszej części świata były względnie spokojne, forsowana była teza, że bezpieczeństwo działalności powinno podlegać takim samym prawidłom jak pozostałe procesy.

Powodowało to szukanie tzw. wartości dodanej, i to w krótkiej perspektywie czasowej. Pojawiły się nawet nowe określenia struktur bezpieczeństwa, takie jak loss prevention, profit conservation i tym podobne. W tle krążyła też teza o „bezszwowej" integracji procesów biznesowych z procesami bezpieczeństwa. Takie podejście do kwestii bezpieczeństwa może doprowadzić do całkowitej utraty kontaktu z realiami. To oczywiście bardzo ciekawe pomysły i nie do końca pozbawione sensu. Musimy jednak spojrzeć prawdzie w oczy i otwarcie powiedzieć – kwestie bezpieczeństwa przeszkadzają w biznesie.

Problem w tym, że tę prawdę należy zaakceptować, a nie wypierać jej. Nie można udawać, że wprowadzenie środków bezpieczeństwa czyni życie łatwiejszym. Dzieje się tak zarówno w organizacjach, jak i innych obszarach życia. Montujemy w naszych domach drzwi antywłamaniowe, instalujemy alarmy, które bardzo często są

→

dość uciążliwe. Lecąc na wakacje, poddajemy się na lotnisku drobiazgowej, niewygodnej, a często nawet upokarzającej kontroli bezpieczeństwa. Nikt z nas nie mówi, że to ma się opłacać tu i teraz, i natychmiast zwrócić. Nawet, jeśli tak tego nie nazywamy, prowadzimy kalkulację ryzyka i akceptujemy te środki jako niezbędne do zapewnienia poczucia bezpieczeństwa.

Realizujemy potrzebę bycia bezpiecznym jako najważniejszą po zaspokojeniu potrzeb fizjologicznych. Wszystko to doskonale działa do momentu, gdy nie wchodzimy w nasze role w organizacji – pracowników menedżerów, prezesów. Tutaj wymiar bezpieczeństwa w magiczny sposób się zniekształca.

Bezpieczeństwo w firmie kosztuje

W firmie jest tak samo jak w prywatnym życiu. Bezpieczeństwo kosztuje, przeszkadza, wymaga uwagi, ćwiczenia, doskonalenia. Tak jak w życiu możemy w tej dziedzinie nie podejmować żadnych działań, licząc na szczęście. Wyobrażam sobie organizację, która uzna, że nic z bezpieczeństwem robić nie trzeba. Jeśli to jest świadoma decyzja najwyższego kierownictwa, niech tak będzie. W przypadku infrastruktury krytycznej takie podejście jest nie do przyjęcia. Tu nie chodzi tylko o ochronę zasobów firmy i jej kondycji finansowej w razie wystąpienia kryzysu.

Odpowiedzialność dostawców infrastruktury krytycznej

Infrastruktura krytyczna wspiera dostawy kluczowych produktów i usług dla społeczeństwa. Od jej bezpieczeństwa niejednokrotne zależy fizyczne przetrwanie ludzi. W Polsce konieczne jest przyspieszenie procesu identyfikacji infrastruktury krytycznej i większe zaangażowanie państwa w tym zakresie. Potrzebne są przepisy skuteczniej egzekwujące stosowanie właściwych środków zabezpieczeń.

Nie chodzi tylko o to, aby państwo stało się żandarmem siłą wymuszającym właściwy poziom ochrony. Państwo powinno wykazać, że zabezpieczenie infrastruktury krytycznej to kwestia przetrwania jako państwa, a operatorzy infrastruktury są bardzo ważni, ale z pewnością nie jedyni w całym łańcuchu działań niezbędnym do jej właściwego zabezpieczenia i odtworzenia.

Konieczność zaangażowania wszystkich pracowników

Wracając do poziomu firmy należącej do IK, odporność musimy budować poprzez zaangażowanie wszystkich pracowników. Można to robić na różne sposoby. Pamiętajmy jednak o tym, że wyzwaniem jest zaangażowanie ludzi w zadania, które nie muszą być dla nich atrakcyjne. Pracownicy funkcjonują w oparciu o wyznaczone cele, które sprowadzają się do skutecznego zarabiania pieniędzy. Każda inicjatywa, która ich od tego celu oddala, będzie przyjmowana z niechęcią, np. dodatkowe ćwiczenia, aktualizacja planów kryzysowych itp.

Obawiam się, że w kwestiach „twardego" bezpieczeństwa, czyli takiego, jakie tyczy się IK, rozwiązania bazujące na budowaniu zaangażowania poprzez ruch oddolny się nie sprawdzą. W takich przypadkach niezbędne będzie wyraźne wyrażenie woli najwyższego kierownictwa i jego własny przykład pokazujący zaangażowanie.

Rewizja polityk i budowanie kompetencji

Organizacje muszą zrewidować polityki zarządzania ciągłością działania i zarządzania kryzysowego, co obejmuje aktualizację procedur i budowanie kompetencji, z naciskiem na system zarządzania ciągłością działania. Brzmi to podręcznikowo, ale nie ma nic wspólnego z prostym zadaniem. Dzieje się tak z dwóch powodów: digitalizacji i skali komplikacji. Przy praktycznie pełnej digitalizacji procesów biznesowych skala zależności, które wpływają na utrzymanie ciągłości działania, staje się ogromna.

Skuteczne zarządzanie ciągłością działania wymaga odpowiedniej perspektywy, wiedzy, a także odpowiednich narzędzi wspierających. W tak zwanych czasach pokoju łatwo można było zbudować poczucie dobrze spełnionego obowiązku. Powstawały plany, których nie sposób było poddać próbie ognia. Dzisiaj nie ma z tym problemu. Wystarczy tylko powierzchownie sięgnąć do doświadczeń ukraińskich, aby bez obawy o posądzenia o fantastyczne scenariusze przetestować nasze plany awaryjne. To niestety może dać szybką odpowiedź, na co jesteśmy gotowi: na wojnę czy na defiladę?

Wypracowanie systemu samodoskonalenia

W obliczu dynamicznego środowiska zagrożeń pojawiają się oczekiwania do sprawdzenia, przetestowania wszystkiego tu i teraz. Idea sama w sobie słuszna, ale tylko z pozoru. Testowanie ma prowadzić do doskonalenia. Jeśli nasze doskonalenie ma polegać na bezrefleksyjnym testowaniu, to cała para pójdzie w gwizdek. Testy i ćwiczenia mają sens tylko wtedy, gdy zbudujemy przestrzeń do przepracowania ich rezultatów. Musi to być proces od początku do końca przemyślany i zaczynać się od pytania: co testujemy? Liczba przeprowadzonych ćwiczeń dobrze wygląda w statystykach. Gdybyśmy zestawili te dane z liczbą skutecznie wdrożonych wniosków po ćwiczeniach, to już pewnie tak miło by nie było.

Wracamy do „niefajności" bezpieczeństwa – testy/ćwiczenia zabierają czas, pokazują, że coś nie działa (czyli jest źle). Żeby to naprawić, trzeba znowu poświęcić czas i bardzo często pieniądze. W taki sposób można także przedstawiać system samodoskonalenia w obszarze bezpieczeństwa i obawiam się, że nie jest to takie rzadkie zjawisko.

Wyzwania

Ochrona infrastruktury krytycznej w Polsce to skomplikowany obszar. Rola państwa jest w nim niezwykle istotna chociażby dla jej efektywnej identyfikacji i określenia zasad funkcjonowania w punktach styku – podmiot IK i państwo. Państwo powinno być bardziej konkretne w określaniu wymogów i zdecydowane w ich egzekwowaniu. Jednak największe obciążenie na rzecz zabezpieczenia tejże infrastruktury spadnie na firmy, które tę infrastrukturę mają. Pomimo ogromnego wysiłku, jaki należy włożyć, jest jeszcze dużo większe wyzwanie do podjęcia – zmiana sposobu myślenia.

Sytuacje kryzysowe, a w pewnym sensie już się w takiej znajdujemy, cechują się tym, że czujemy się niepewnie i nie wiemy, co zrobić. Jakkolwiek by to nie zabrzmiało, jest to stan, który trzeba zaakceptować. Jak zatem skutecznie reagować? Stworzyć atmosferę myślenia poza schematami i dać sobie pozwolenie na popełnianie błędów. Przeciwieństwem tego stanu rzeczy jest rozpaczliwe czepianie się obszarów, które znamy, i choć ta wiedza jest nie na temat, to daje fałszywe poczucie bezpieczeństwa. Dokładając do tego atmosferę szukania winnych, możemy bez większego problemu roztrwonić coś, na co teraz nie możemy sobie pozwolić. Tym czymś jest czas. ●

Janusz Syrówka

Menedżer ds. bezpieczeństwa w E.ON Polska. Ekspert w holistycznym zarządzaniu bezpieczeństwem w organizacjach. Od ponad 24 lat zajmuje się dostarczaniem kompleksowych rozwiązań bezpieczeństwa uwzględniających strategiczne cele biznesowe organizacji. Doświadczenie zdobywał w Komendzie Stołecznej Policji, a następnie w branży detalicznej, logistycznej i energetycznej w dużych organizacjach międzynarodowych.

REKLAMA

ARITECH

Axon™

Intrusion and Access Control Panel

MADE IN POLAND PREMIUM QUALITY

pl.firesecurityproducts.com

Standardy i dobre praktyki ochrony infrastruktury krytycznej

Rządowe Centrum Bezpieczeństwa (RCB) to państwowa jednostka budżetowa, podlegająca bezpośrednio Prezesowi Rady Ministrów. Pełni funkcję krajowego centrum zarządzania kryzysowego. Jednym z jej zadań było przygotowanie Narodowego Programu Ochrony Infrastruktury Krytycznej.

Zadanie to zostało powierzone RCB na mocy uchwały z 2013 r. Program jest aktualizowany i obecnie ze strony RCB można pobrać jego najnowszą wersję, opublikowaną w 2023 r. Dla menedżerów security to lektura wręcz obowiązkowa. Poza programem warto zapoznać się z załącznikami. Szczególnej uwadze polecamy Załącznik nr 1. Publikujemy fragmenty rozdziału drugiego, dotyczącego zapewnienia bezpieczeństwa osobowego. Ze względu na wagę dokumentu, poza nielicznymi, niezbędnymi skrótami oznaczonymi jako (…), nie dokonaliśmy żadnych zmian redakcyjnych.

Zapewnienie bezpieczeństwa osobowego

Zapewnienie bezpieczeństwa osobowego to zespół przedsięwzięć i procedur mających na celu minimalizację ryzyka związanego z osobami, które przez autoryzowany dostęp do obiektów, urządzeń, instalacji i usług infrastruktury krytycznej mogą spowodować zakłócenia w jej funkcjonowaniu.

Członkowie personelu związanego z obiektami, urządzeniami, instalacjami i usługami infrastruktury krytycznej oraz osoby czasowo przebywające w obrębie IK (usługodawcy, dostawcy, goście) mogą stanowić potencjalne zagrożenie dla jej funkcjonowania. Pozycja zajmowana w strukturze operatora IK determinuje poziom dostępu fizycznego do kolejnych stref bezpieczeństwa oraz dostęp do informacji wrażliwych, niekoniecznie niejawnych. Oba te przywileje mogą być nielegalnie wykorzystane i służyć zakłóceniu funkcjonowania IK lub działaniu na jej niekorzyść (dotyczy to także usługodawców, dostawców i gości).

Należy pamiętać, że wiele aspektów zapewnienia bezpieczeństwa osobowego jest nierozerwalnie związanych z innymi elementami systemu bezpieczeństwa IK, takimi jak zapewnienie bezpieczeństwa fizycznego czy teleinformatycznego. Dopiero komplementarność wszystkich elementów zapewni satysfakcjonujący poziom zapewnienia bezpieczeństwa IK przed zagrożeniami wewnętrznymi, np. rozczarowanymi pracownikami, prowokacjami, konkurencją czy przestępczością zorganizowaną.

Dla usystematyzowania informacji tekst został podzielony na rozdziały odpowiadające kolejnym etapom działania z osobami mogącymi mieć negatywny wpływ na funkcjonowanie IK.

Postępowanie w trakcie zatrudniania

Podstawą skuteczności zapewnienia bezpieczeństwa osobowego jest zebranie jak największej liczby informacji, możliwych do uzyskania w świetle obowiązującego prawa, o potencjalnym pracowniku już w procesie rekrutacji. Aby zoptymalizować czas, siły i środki wykorzystywane w postępowaniu rekrutacyjnym, należy przede wszystkim dokładnie sporządzić profil kandydata, a precyzyjne określenie zakresu obowiązków pozwoli ustalić poziom dostępu do stref, pomieszczeń, depozytorów itp., jaki będzie mu przyznany, oraz jakimi informacjami wrażliwymi będzie dysponował.

Warto przeprowadzić ocenę ryzyka zakłócenia funkcjonowania IK, związanego z nielegalnym wykorzystaniem informacji lub praw dostępu dla różnych stanowisk w strukturze organizacji. Ocena ta będzie stanowić podstawę decyzji o szczegółowości postępowania sprawdzającego w procesie zatrudniania. Pozwoli także na lepsze określenie kryteriów, jakim powinien odpowiadać kandydat. Taką ocenę można wprowadzić i zakomunikować w formie skoordynowanej polityki zatrudniania w organizacji.

Ustalenie tożsamości

Warunkiem koniecznym do dalszego procedowania jest weryfikacja tożsamości kandydata. Nie należy podejmować dalszych czynności, jeśli istnieją jakiekolwiek zastrzeżenia co do jej poprawności!

(…)

Sprawdzenie tożsamości powinno odbywać się przede wszystkim na podstawie przedstawionych oryginalnych dokumentów, zawierających imiona, nazwisko, datę urodzenia, adres, podpis posiadacza oraz zdjęcie. Należy sprawdzić, czy okazywany dokument jest wydany przez właściwy organ i ma aktualną datę ważności. Obowiązkowo należy wymagać dokumentów trudnych do podrobienia, takich jak: paszport, dowód osobisty czy prawo jazdy. Koniecznie należy weryfikować autentyczność przedstawianych przez kandydata dokumentów. Pracownicy dokonujący takiej weryfikacji muszą posiadać odpowiednią wiedzę i umiejętności w celu przeprowadzenia takich sprawdzeń.

Kwalifikacje

Sprawdzenie kwalifikacji kandydata powinno opierać się o weryfikację informacji zawartych w dokumentach rekrutacyjnych (CV, formularze, świadectwa pracy itp.). Pozwoli to ocenić wiarygodność i uczciwość kandydata oraz zdobyć informacje, które chciałby ukryć. Podobnie jak w przypadku ustalenia tożsamości wszelkie dokumenty powinny być oryginalne. Weryfikacja prawdziwości przekazanych dokumentów powinna odbyć się podczas osobistego stawiennictwa kandydata w toku postępowania rekrutacyjnego po etapie preselekcji. (…)

W przypadku rekrutacji na kluczowe stanowiska, połączone z dostępem do informacji niejawnych, postępowanie sprawdzające przeprowadzają właściwe służby ochrony państwa. Nie należy jednak zaniedbywać wewnętrznego procesu weryfikacji kandydata. Ułatwieniem w tym zakresie są obowiązujące przepisy prawa ujęte m.in. w ustawie o zarządzaniu kryzysowym, pozwalające żądać od pracownika (lub kandydata do pracy) przedłożenia informacji dotyczących karalności, w tym informacji, czy ich dane osobowe są zgromadzone w Krajowym Rejestrze Karnym.

Postępowanie w stosunku do zatrudnionych

Priorytetem w zapewnieniu bezpieczeństwa osobowego jest dokładne sprawdzenie pracownika (np. analiza złożonych dokumentów i weryfikacja ich autentyczności) jeszcze przed jego zatrudnieniem, nie wolno zaniedbywać jednak zasad bezpieczeństwa w stosunku do już zatrudnionych w organizacji. W trakcie zatrudnienia, w przypadku zmiany stanowiska pracy należy zweryfikować nadane osobie uprawnienia i dostosować je do obecnie zajmowanego stanowiska. Wszelkie uprawnienia, które posiadał pracownik w związku z poprzednio zajmowanym stanowiskiem, powinny zostać cofnięte. Kluczowe znaczenie ma w tym przypadku informacja z działu kadr o zmianie stanowiska do pozostałych komórek organizacyjnych, w tym odpowiedzialnych za bezpieczeństwo. Wskazane jest także okresowe weryfikowanie niezbędności uprawnień przyznanych wszystkim osobom – pracownikom i podwykonawcom zewnętrznym.

Niestandardowe zachowania

Obserwacja zachowań pracowników jest jednym ze sposobów wykrycia potencjalnego zagrożenia wewnętrznego. Należy jednak podkreślić, że nie chodzi o wścibskość lub inwigilację, a jedynie o ocenę możliwości wystąpienia takiego zagrożenia.

Zespół powinien być uwrażliwiony na zmiany zachowania i informować o tych, które mogą świadczyć o rozluźnieniu związku pracownika z organizacją lub jego problemach osobistych, takich jak:

- nadużywanie alkoholu,
- wypowiadanie poglądów aprobujących działania grup ekstremistycznych,
- zmiana wyznania, przynależności politycznej, społecznej,
- niewytłumaczalne zmiany w życiu osobistym,
- brak zainteresowania wykonywaną pracą, rozczarowanie,
- znamiona silnego stresu: agresja, choleryczne zachowanie,

→

- zmiana godzin pracy, przyzwyczajeń,
- niestandardowe zainteresowanie systemami bezpieczeństwa,
- brak przestrzegania procedur bezpieczeństwa,
- nieobecności nieusprawiedliwione.

Powyższa lista niestandardowych zachowań nie jest kompletna i nie może być jedynym kryterium do podjęcia kroków dyscyplinarnych. Może natomiast, razem z innymi przesłankami, stanowić podstawę do udzielenia danej osobie pomocy lub kontroli jej działalności w organizacji. Szczególnie wystąpienie szeregu przesłanek musi wzbudzić zainteresowanie osób odpowiedzialnych w organizacji za bezpieczeństwo.

Dostęp

Jednym z podstawowych sposobów na zapewnienie bezpieczeństwa osobowego IK jest ograniczanie dostępu pracowników organizacji do wrażliwych miejsc lub zasobów znajdujących się na terenie organizacji i w sieciach teleinformatycznych. Dostęp powinien być przyznawany tylko w zakresie i czasie potrzebnym do wykonywania swoich obowiązków służbowych. Próba dotarcia do zastrzeżonych stref, sieci lub zasobów może świadczyć o potencjalnym zagrożeniu ze strony pracownika.

Osoby odpowiedzialne za bezpieczeństwo w ustalonych odstępach czasu powinny:

- weryfikować prawa dostępu i w razie potrzeby je ograniczać,
- kontrolować, analizować i raportować wszelkie próby nieautoryzowanego dostępu do miejsc (pomieszczeń) oraz sieci i zasobów teleinformatycznych.

Pracownicy organizacji powinni być uczuleni na próby nieautoryzowanego dostępu wszelkich osób do zastrzeżonych miejsc oraz informować odpowiedzialne osoby o zauważonych tego typu próbach.

» Dostęp powinien być przyznawany tylko w zakresie i czasie potrzebnym do wykonywania swoich obowiązków służbowych. «

Identyfikacja wizualna

Identyfikacja wizualna pracowników organizacji oraz podwykonawców i gości jest najprostszym sposobem określenia przynależności do organizacji oraz potencjalnych uprawnień.

Każda osoba znajdująca się w obiekcie należącym do IK powinna nosić w widocznym miejscu identyfikator z fotografią twarzy posiadacza. Identyfikator nie powinien jednak zawierać (ze względów bezpieczeństwa, np. po zgubieniu) informacji o przydzielonych mu prawach dostępu. Powinien być oznaczony odpowiednim dla strefy (budynku) kolorem w celu szybkiego rozpoznania każdego nielegalnie przebywającego w danym obszarze pracownika i podjęcia odpowiednich kroków. Tam, gdzie ma to uzasadnienie, należy wprowadzić dodatkowo odzież służbową lub inny sposób identyfikacji przez elementy ubioru (kolorowe kamizelki, kaski itp.). Wprowadzając odzież służbową, należy pamiętać, że nie może to być jedyny sposób identyfikacji wizualnej zezwalający na dostęp do obiektu (osoba nosząca uniform z logo firmy niekoniecznie musi być tą, za którą się podaje).

Nie należy nosić identyfikatorów w widocznych miejscach poza obiektami IK. Utrudni to osobom niepowołanym poznanie wyglądu graficznego identyfikatorów. Osobom spoza organizacji nie należy również zezwalać na wynoszenie identyfikatorów poza obiekt.

Ochrona kluczowego personelu

W każdej organizacji są osoby posiadające newralgiczną (unikalną) wiedzę na temat jej funkcjonowania oraz doświadczenie i „pamięć instytucjonalną". Są one szczególnie cenne dla organizacji, a jednocześnie stanowią potencjalnie największe zagrożenie na wypadek działania na niekorzyść organizacji. W celu ochrony informacji mających istotne znaczenie dla pracodawcy są z nimi zawierane odrębne umowy o zakazie konkurencji w czasie trwania i po ustaniu stosunku pracy. Takie osoby powinny mieć zapewnione przez pracodawcę satysfakcjonujące warunki pracy, obejmujące wynagrodzenie,

czas pracy i prestiż. Pracodawca powinien zapewnić także możliwość sukcesywnego podnoszenia kompetencji oraz wsparcie podmiotów zewnętrznych. Ochrona kluczowego personelu oznacza także bardziej restrykcyjne wymogi kontrolne w stosunku do tych osób. Należy także podjąć kroki dające możliwość zastępstwa o podobnych kwalifikacjach oraz uprawnieniach.

Usługodawcy, podwykonawcy

Pracownicy podmiotów wykonujący pracę na zlecenie operatora IK powinni zostać zweryfikowani w podobny sposób jak w przypadku rekrutacji, a dodatkowo należy sprawdzić, czy dany podwykonawca jest członkiem rozpoznawalnego i uznanego stowarzyszenia, posiada odpowiednie licencje, spełnia standardy jakości, posiada stabilność finansową itp.

Cenne są rekomendacje personalne, referencje od operatorów z tego samego systemu i przykłady już wykonanych prac, ale nawet gdy są one bardzo dobre, należy podać do wiadomości podwykonawcy, że są one weryfikowane.

Po ustaleniu zakresu usługi i ocenie ryzyka zakłócenia funkcjonowania IK powinno się ustalić poziom dostępów, przeprowadzić szkolenie informujące o występujących zagrożeniach i obowiązujących procedurach i dopiero wtedy wydać przepustki lub ustanowić prawa dostępu do sieci. Wszelkie prace mogące mieć negatywny wpływ na IK muszą być wykonywane pod nadzorem stałej kadry IK.

Postępowanie z odchodzącymi z pracy

Każdy z pracowników odchodzących z organizacji jest w posiadaniu mniej lub bardziej wrażliwej wiedzy, która może być wykorzystana ze stratą dla organizacji. Dlatego w każdym przypadku konieczna jest indywidualna ocena ryzyka związanego z możliwością ujawnienia informacji. Szacowanie powinno być oparte o kilka wytycznych. Pierwszym jest zajmowane stanowisko implikujące poziom dostępu do informacji. Drugim – powód odejścia z zakładu pracy (dobrowolny, dyscyplinarny, redukcja zatrudnienia, wygaśnięcie umowy). Dalej należy sprawdzić najbliższe plany pracownika, czy np. nowym miejscem zatrudnienia nie będzie firma konkurencyjna.

Postępowanie w okresie wypowiedzenia będzie wynikało z przeprowadzonej oceny ryzyka i będzie w głównej mierze oparte o ograniczenie dostępu w zależności od poziomu ryzyka, chyba że zwolnienie ma charakter natychmiastowy, wtedy należy odebrać pełny dostęp, a cały proces opuszczania miejsca pracy przeprowadzić pod nadzorem. Nie oznacza to jednak, że pracownikowi odchodzącemu dobrowolnie, na emeryturę należy pozostawić w okresie wypowiedzenia pełny dostęp. Decyzje w tym zakresie podejmuje w konkretnych sytuacjach pracodawca. Istnieje możliwość zwolnienia pracownika z obowiązku świadczenia pracy w okresie wypowiedzenia.

Opuszczający stanowisko pracownik powinien zwrócić:

- odzież firmową, w tym umundurowanie (jeśli występuje),
- identyfikatory, przepustki,
- służbowe telefony komórkowe,
- służbowe karty kredytowe,
- służbowe wizytówki,
- klucze do pomieszczeń, generatory kodów jednorazowych,
- dokumenty należące do organizacji,
- przenośne dyski danych, komputery.

Jednocześnie osoby odpowiedzialne za przyznawanie dostępu (fizycznego i teleinformatycznego) powinny:

- zablokować uprawnienia dostępu do systemów, w tym dezaktywować identyfikatory, karty dostępu, hasła,
- zmienić kody dostępu do drzwi, depozytorów,
- anulować karty kredytowe,
- przekazać pracownikom ochrony odpowiednio wcześniej informację o cofnięciu uprawnień pracownikowi.

W przypadku śmierci pracownika należy zastosować podobne czynności. Warto sprawdzić, czy jest się w posiadaniu aktualnego kontaktu do rodziny, dzięki któremu będzie możliwe natychmiastowe odzyskanie ww. przedmiotów.

Należy rozważyć zmianę uprawnień dostępu (haseł, identyfikatorów, kart) do zasobów, danych, miejsc (stref), które odchodzący pracownik dzielił z innymi w ramach pracy zespołowej.

Aby podnieść świadomość operatorów IK o zagrożeniach wewnętrznych, warto stworzyć na poziomie systemu IK (sektora) bazę danych informacji o zagrożeniach wewnętrznych i incydentach z udziałem pracowników, podwykonawców lub gości oraz mechanizm bezpiecznej wymiany tych informacji. Baza prowadzona na poziomie centralnym mogłaby zawierać informacje zebrane z poziomu sektorowego. Anonimowe przykłady mogą pomóc w przeprowadzeniu dokładniejszej oceny ryzyka i wdrożeniu efektywniejszych środków ochrony.

Bardzo duże znaczenie dla skutecznego procesu zapewnienia bezpieczeństwa osobowego ma profilaktyka przeciwdziałania nadużyciom. Działania operatora takie jak promowanie etyki zawodowej, polityka uczciwości we wszystkich działaniach firmy, etyczny przykład kierownictwa oraz skuteczne mechanizmy kontrolne skutecznie zmniejszają ryzyko popełnienia świadomego działania niepożądanego przez pracownika.

Najważniejsze rekomendacje dotyczące zapewnienia bezpieczeństwa osobowego:

1. Oceń ryzyko zakłócenia funkcjonowania IK dla konkretnych stanowisk w strukturze organizacji.
2. Poświęć dużo czasu na sprawdzenie wiarygodności i kompetencji nowego pracownika.
3. Uświadamiaj organizację, że zagrożeniem może być każdy pracownik.
4. Zidentyfikuj i stwórz odpowiednie warunki kluczowemu personelowi.
5. Informuj (dział kadr) pozostałe komórki organizacyjne, w tym odpowiedzialne za bezpieczeństwo o zmianie przez pracowników zajmowanych przez nich stanowisk.
6. Nie zwlekaj z odebraniem praw dostępu pracownikom odchodzącym z organizacji.

Rekomendujemy uważną lekturę programu opracowanego przez RCB. Każdy menedżer ds. bezpieczeństwa powinien zapoznać się z całym załącznikiem, szczególnie z działami dotyczącymi zapewnienia bezpieczeństwa fizycznego, teleinformatycznego oraz planami ciągłości działania i odbudowy. Polecamy także lekturę wywiadu z dr Karoliną Wojtasik *Rewolucja w IK. Powstanie RC 2.0* (a&s Polska 2/2023), który rzuca światło na kwestię ochrony infrastruktury krytycznej w naszym kraju. ●

Z pustego i Salomon nie naleje

Niestety, Polska nie może się pochwalić bogactwem odnawialnych zasobów słodkiej wody. Według raportu GUS Polska na drodze zrównoważonego rozwoju zajmujemy 24. miejsce w Unii Europejskiej pod względem ilości wody przypadającej na jednego mieszkańca. Wyprzedzają nas jedynie Czechy, Cypr i Malta.

Monika Żuber-Mamakis

W raporcie podkreślono, że zasoby wodne Polski są niewielkie. Ponadto charakteryzują się zmiennością sezonową i zróżnicowaniem obszarowym. Oznacza to, że w niektórych regionach kraju problem deficytu wody jest bardziej dotkliwy niż w innych.

Spragniony przemysł

Ciało człowieka w dużej mierze składa się z wody. U dorosłego stanowi ona ok. 65%. Dlatego odwodnienie może mieć katastrofalne dla zdrowia skutki. Podobnie rzecz się ma z gospodarką, która jest od wody uzależniona. Struktura poboru wody w Polsce w ciągu ostatnich 20 lat pozostaje stosunkowo stabilna. Zgodnie z danymi GUS w 2022 r. przemysł odpowiadał za 69% poboru wody (6440 hm^3), gospodarka komunalna za 22% (2113 hm^3), a napełnianie i uzupełnianie stawów rybnych za 9% (832 hm^3). Łączne zapotrzebowanie na wodę w 2022 r. wyniosło 9,4 tys. hm^3. W porównaniu do roku 2021:

- pobór wody na cele produkcyjne wzrósł o 1,7%;
- pobór wody do napełniania i uzupełniania stawów rybnych spadł o 1%;
- pobór wody na potrzeby eksploatacji sieci wodociągowej wzrósł o 22 hm^3.

Głównym źródłem zaopatrzenia w wodę są wody powierzchniowe, które w 2022 r. pokryły 81% potrzeb. Korzysta z nich przede wszystkim przemysł.

Zaopatrzenie w wodę jest więc krytycznie ważne. Niestety, jak podano w najnowszym raporcie Najwyższej Izby Kontroli *Zapewnienie bezpieczeństwa w wodę wybranych jednostek samorządu terytorialnego na wypadek wystąpienia sytuacji kryzysowych* (z listopada 2023 r.), nasz kraj nie jest przygotowany na sytuacje kryzysowe, które mogłyby wpłynąć na dostawy wody.

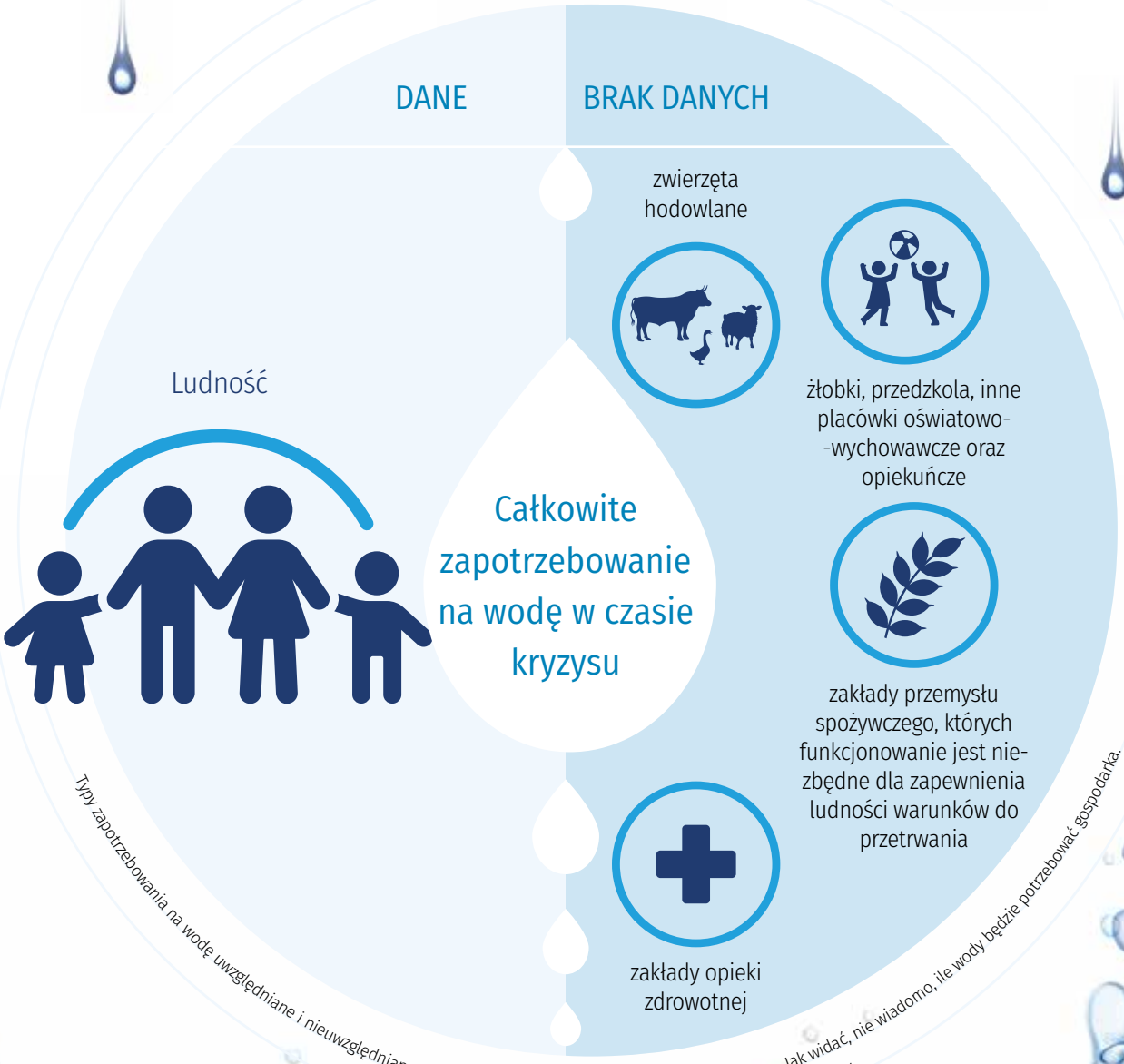
Czy grozi nam wodny *blackout*?

Kontrolerzy NIK-u potwierdzają to ryzyko. Już w 2017 roku alarmowano, że „duże aglomeracje miejskie w Polsce nie są przygotowane na brak wody pitnej spowodowany zdarzeniami kryzysowymi dotyczącymi systemu wodociągowego. Plany, jakimi dysponują podmioty odpowiedzialne za jej dostawy, są oparte na niekompletnych danych, a zapotrzebowanie na wodę jest obliczane jedynie w odniesieniu do liczby mieszkańców. Kalkulacje pomijają np. potrzeby zakładów produkujących żywność. Istnieje też realne ryzyko, że w przypadku wystąpienia kryzysu, ze względu na brak sprzętu i środków transportu do przewożenia i dystrybucji wody nie zostanie ona dostarczona wszystkim potrzebującym (NIK o zaopatrzeniu aglomeracji w wodę w sytuacjach kryzysowych, 19 października 2017).

NIK przeanalizował działania podejmowane w okresie od 1 stycznia 2015 r. do 31 grudnia 2016 r. (do dnia zakończenia kontroli) oraz wcześniejsze, które miały wpływ na realizację badanych zadań lub których efekty wystąpiły po 1 stycznia 2015 r., a także skutki działań ujawnione do dnia zakończenia kontroli.

Wyniki ówczesnej kontroli były niepokojące. Najważniejsze z niej wnioski to brak jednoznacznych kompetencji. Ustawa o działach administracji rządowej nie przypisywała jednoznacznie żadnemu ministrowi odpowiedzialności za bezpieczeństwo dostaw wody w warunkach kryzysu. Niewystarczające plany reagowania kryzysowego nie zawierały pełnych i rzetelnych danych o uwarunkowaniach dostaw wody na wypadek zdarzenia kryzysowego. Wskazano na niewystarczające zabezpieczenie dostaw wody na wypadek awarii sieci wodociągowej, ponieważ dostępne wówczas środki transportu pozwalały na realizację jedynie od 2,1 do 28% zapotrzebowania na wodę, a także na niewystarczającą ochronę infrastruktury krytycznej: dwa z trzech skontrolowanych przedsiębiorstw wodociągowych nie przygotowało planów ochrony infrastruktury krytycznej.

> *Istnieje realne ryzyko, że w przypadku wystąpienia kryzysu, ze względu na brak sprzętu i środków transportu do przewożenia i dystrybucji wody nie zostanie ona dostarczona wszystkim potrzebującym.*



Typy zapotrzebowania na wodę uwzględniane i nieuwzględniane przy sporządzaniu planów reagowania kryzysowego. Jak widać, nie wiadomo, ile wody będzie potrzebować gospodarka.
Źródło: NIK o zaopatrzeniu aglomeracji w wodę w sytuacjach kryzysowych

Z kolei w roku ubiegłym NIK sprawdził, jak wygląda zapewnienie bezpieczeństwa w wodę wybranych jednostek samorządu terytorialnego na wypadek wystąpienia sytuacji kryzysowych. Postępowanie kontrolne przeprowadzono w pięciu gminach miejskich i pięciu gminach miejsko-wiejskich, wybranych z uwzględnieniem kryterium liczby mieszkańców, w województwach: dolnośląskim, mazowieckim, podlaskim, podkarpackim i zachodniopomorskim.

Informację o wynikach tej kontroli delegatura wrocławska opublikowała w listopadzie 2023 r. Mimo faktu, że obie kontrole, czyli tę z 2017 r. i aktualną dzieli ponad 5 lat, wniosek jest podobny: brak bezpieczeństwa dostaw wody w polskich gminach. Najwyższa Izba Kontroli wykazała, że kontrolowane jednostki nie były przygotowane na sytuacje kryzysowe, które mogłyby ograniczyć dostęp do wody.

Główne problemy to brak:

- identyfikacji potrzeb – gminy nie wiedziały, ile wody i jakich zasobów potrzebują w sytuacjach kryzysowych;
- planowania – nie istniały kompleksowe plany działań na wypadek kryzysu wodnego;
- zasobów – gminy nie miały wystarczających zasobów, aby zapewnić mieszkańcom dostęp do wody w sytuacjach kryzysowych;
- regulacji prawnych – nie było przepisów określających, jak gminy mają zabezpieczać dostawy wody w sytuacjach kryzysowych.

Z pewnością bezpieczeństwu w zakresie dostaw wody nie sprzyja fakt, że w 2022 r. uchylono przepisy o obronie cywilnej, co jeszcze bardziej ograniczyło możliwości gmin w tym zakresie. Dopiero 22 marca tego roku szefowie MON i MSWiA przedstawili założenia ustawy o ochronie ludności i obronie cywilnej. Projekt ustawy obecnie jest analizowany z samorządowcami, a później ma trafić do konsultacji społecznych. Po 20 kwietnia 2024 r. mają się rozpocząć konsultacje międzyresortowe. Pytanie brzmi, czy wszyscy konsultujący znają ustalenia NIK dotyczące bezpieczeństwa zaopatrzenia w wodę i czy uwzględnią ten aspekt przy pracach nad ustawą?

Bez wody nie ma... prądu

Bezpieczeństwo wodne i bezpieczeństwo energetyczne są ściśle ze sobą powiązane. Dostęp do czystej wody jest niezbędny do produkcji energii, z kolei produkcja energii może mieć negatywny wpływ na zasoby wodne. Oczywiście, część gospodarstw poradzi sobie np. dzięki fotowoltaice, ale to produkcja na potrzeby własne. Prywatne instalacje fotowoltaiczne nie zapewnią prądu szpitalom, żłobkom i szkołom, tym bardziej że polskie sieci przesyłowe cały czas zmagają się z wydajnością, o czym boleśnie przekonują się prosumenci, którzy nie są w stanie przekazać do sieci nadwyżek mocy.

> *W roku 2023 NIK ustalił, że nie zapewniono bezpieczeństwa zaopatrzenia gmin w wodę na wypadek wystąpienia sytuacji kryzysowych.*

Bez prądu nie ma produkcji. Brak wody to nie tylko problem dla ludzi i ich codziennego życia, ale również poważne zagrożenie dla gospodarki. Według raportu Banku Światowego z 2016 r. globalne straty gospodarcze spowodowane niedoborem wody mogą do 2050 r. sięgnąć 6 bln USD rocznie.

Ostrożnym optymizmem napawa fakt, że lepiej gospodarujemy wodą. Zgodnie z informacjami GUS zawartymi w raporcie *Wyniki zielonej gospodarki w Polsce 2022 r.* poprawił się wskaźnik produktywności wody obrazujący relację między PKB (w cenach stałych) a zużyciem wody na potrzeby gospodarki narodowej i ludności. W latach 2000–2021 wskaźnik produktywności wody kształtował się coraz korzystniej. W roku 2021 wyniósł 282,39 zł/m^3 i był wyższy, zarówno w odniesieniu do 2020 r., jak i 2000 r. odpowiednio o 5,4% i 316,8%. Oznacza to zatem, że z nieco większym szacunkiem wodę traktujemy. Zapewne stoi za tym nie tyle świadomość ekologiczna, ile wysokie ceny wody i ścieków.

Dlaczego optymizm powinien być ostrożny? Otóż minione dziesięciolecie przeszło do historii jako najgorętsze w dziejach pomiarów meteorologicznych. Średnia temperatura na Ziemi wzrosła o ok. 1°C w porównaniu do okresu przedindustrialnego, a w Europie skok ten był jeszcze bardziej wyraźny, bo wyniósł niemal 2°C. Zmianom temperatury towarzyszą coraz bardziej nieregularne opady atmosferyczne. Ich rozkład w czasie i w odniesieniu do poszczególnych regionów staje się coraz bardziej nieprzewidywalny, a jednocześnie obserwujemy wzrost intensywności opadów. Te czynniki w połączeniu z globalnym ociepleniem prowadzą do coraz częstszych ekstremalnych zjawisk pogodowych, takich jak susze, powodzie, huragany i fale upałów. Według raportu Europejskiej Agencji Środowiska Polska boleśnie odczuwa skutki tych zmian. W latach 2010–2020 straty finansowe spowodowane ekstremalnymi zjawiskami pogodowymi w naszym kraju przekroczyły 3 mld euro, co oznacza 88 euro na osobę.

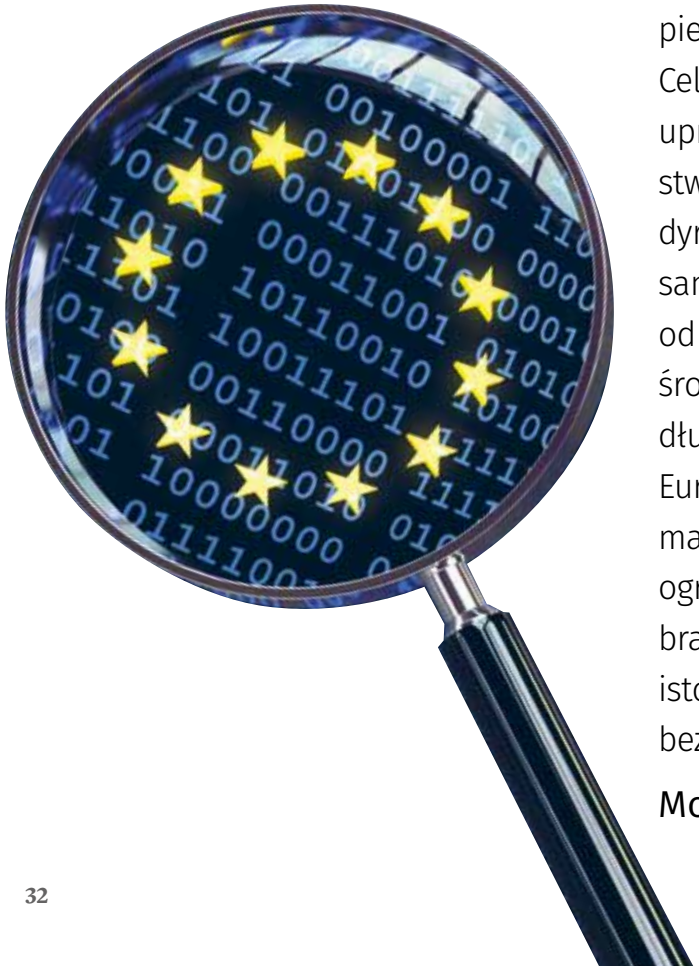
Problemy z zaopatrzeniem w wodę, będące skutkiem zarówno suszy, jak i zlewnych deszczy oraz związanych z nimi podtopień czy powodzi boleśnie odczuwają polskie przedsiębiorstwa, w tym producenci energii. To z kolei może odbić się na bezpieczeństwie energetycznym kraju. ●

ALNET SYSTEMS

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

www.alnetsystems.com

NIS 2: w oczekiwaniu na przepisy krajowe



Dyrektywa NIS 2 to zaktualizowane prawo UE dotyczące cyberbezpieczeństwa. Jest to nowelizacja pierwszej dyrektywy NIS przyjętej w 2016 roku. Celem NIS 2 jest wzmocnienie cyberbezpieczeństwa, uproszczenie zgłaszania incydentów oraz stworzenie spójnych zasad egzekwowania dyrektyw i kar za jej niewypełnienie takich samych dla wszystkich krajów UE. NIS 2 wymaga od większej liczby firm i sektorów wdrożenia środków cyberbezpieczeństwa, mając na celu długoterminową poprawę cyberbezpieczeństwa Europy. Dzięki bardziej rygorystycznym zasadom, mającym na celu przezwyciężenie wcześniejszych ograniczeń, NIS 2 będzie wpływać na szerszy zakres branż. Jednostki objęte NIS 2 są klasyfikowane jako istotne lub ważne, a dyrektywa określa wymagania bezpieczeństwa oraz proces zgłaszania incydentów.

Monika Żuber-Mamakis

Minister cyfryzacji Krzysztof Gawkowski w wywiadzie dla „Rzeczypospolitej" udzielonym na początku kwietnia tego roku powiedział: – *Trzy ustawy powinny w tym roku stać się polskim prawem. To są cele, które postawiłem przed moimi współpracownikami: przyjęcie prawa komunikacji elektronicznej i jednocześnie zaimplementowanie Europejskiego Kodeksu Łączności Elektronicznej, który nie został wdrożony. Dalej: Krajowy System Cyberbezpieczeństwa z dyrektywą NIS 2 i rozpoczęcie prac nad strategią cyberbezpieczeństwa od roku 2025 oraz wdrożenie aktu o usługach cyfrowych, tzw. Digital Service Act, który odpowiada m.in. za to, jak powinna być regulowana praca wielkich platform społecznościowych, jak walczyć z dezinformacją, jaką odpowiedzialność, choćby finansową, powinny ponosić platformy za to, że będą działały niezgodnie z oczekiwaniami obywateli.*

Dwa lata nad nowelizacją, a kiedy wdrożenie

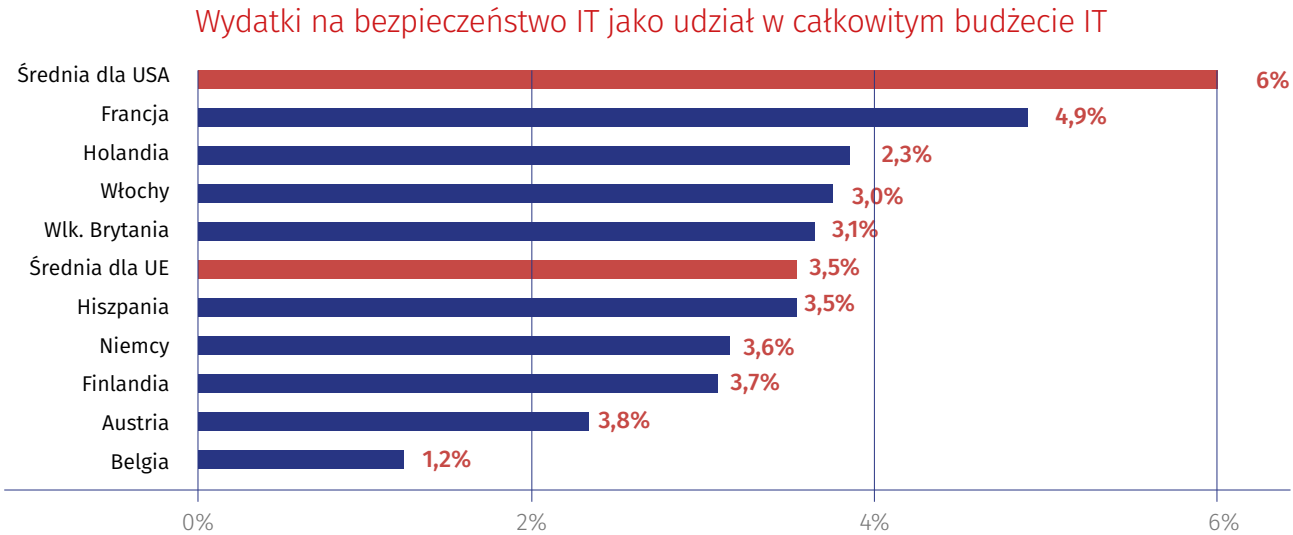
Prace nad nowelizacją NIS trwały dwa lata. Ostatecznie weszła w życie 16 stycznia ubiegłego roku. Państwa członkowskie na wdrożenie jej założeń mają czas do 17 października 2024 r. Tymczasem, choć minął ponad rok od przyjęcia dyrektywy NIS 2, to zgodnie ze słowami min. Gawkowskiego z cytowanego już wywiadu: *wiele spraw zaniedbano, m.in. implementację dyrektywy NIS 2, która zmienia polski i europejski system myślenia o cyberbezpieczeństwie. Mamy umiejętnie zbudować taki system, który będzie wśród kluczowych operatorów na rynku telekomunikacyjnym, cybernetycznym dawał poczucie bezpieczeństwa. I dlatego z tymi pracami przyspieszamy.*

W rzeczy samej do wdrożenia NIS 2 czasu tak naprawdę zostało niewiele.

Po co ta nowelizacja?

Wprawdzie NIS 2 stanowi ewolucję przepisów znanych już państwom członkowskim, to nadal budzi wiele wątpliwości. Zawiera szereg skomplikowanych regulacji, a jej wdrożenie wiąże się z przebudową obowiązującego prawa. Co w takim razie stało za jej wprowadzeniem? Przede wszystkim dostrzeżenie, że w obliczu rosnących cyberzagrożeń, w tym ryzyka wojny hybrydowej, unijne przepisy muszą być bardziej rygorystyczne, a jednocześnie tak jednolite w ramach wspólnoty europejskiej jak tylko jest to możliwe, zważywszy na różnice w porządkach prawnych i możliwościach krajów członkowskich.

Jedną z przyczyn nowelizacji były też m.in niewystarczające inwestycje w cyberbezpieczeństwo. Jak wynika z raportu *NIS Investments Report 2020* opracowanego przez The European Union Agency for Cybersecurity (ENISA), organizacje unijne przeznaczały na cyberezpieczeństwo o 41% mniej niż ich odpowiedniki w USA. Działo się tak pomimo obowiązywania dyrektywy NISD od czterech lat.



Źródło: *Gartner ITKMD data, Scope: EU countries + UK and US for reference*, 2020

Wyniki tego samego badania dowiodły, że aż 35% respondentów uznało wytyczne pierwszej dyrektyw za niejasne, co w powiązaniu z rosnącą liczbą cyberataków i brakiem przejrzystości ich zgłaszania spowodowało konieczność dostosowania NIS do dynamicznie zmieniającej się rzeczywistości.

Podmioty kluczowe i ważne

W nowelizacji dotychczasowy podział na operatorów usług kluczowych, dostawców usług cyfrowych i podmioty publiczne ustąpił miejsca podziałowi na podmioty kluczowe i ważne. Rozszerzeniu uległ też katalog sektorów objętych działaniem dyrektywy. Sektory kluczowe wymienione zostały w załączniku I do dyrektywy, zaś ważne w załączniku II. Taki podział nie przesądza jednak jeszcze o uznaniu danego podmiotu za kluczowy czy ważny. Nowe rozporządzenie, NIS 2, rozwiązuje te kwestie poprzez wprowadzenie reguły limitu wielkości, włączenie dodatkowych podmiotów do kategorii „istotnych" oraz stworzenie nowej kategorii określanej jako „ważne".

W ramach poprzedniej dyrektywy NIS państwa członkowskie odpowiadały za ustalenie, które podmioty spełniają kryteria kwalifikujące je jako operatorów usług kluczowych. Dyrektywa NIS 2 wyjaśnia i rozszerza zakres podmiotów objętych regulacją. W odróżnieniu od pierwszej wersji NIS, gdzie państwa członkowskie mogły indywidualnie decydować, którzy operatorzy są istotni. Wspomniany limit wielkości oznacza, że dyrektywa dotyczy dużych i średnich podmiotów w odpowiednich sektorach, powodując, że zaczynają one podlegać NIS 2. Warto wiedzieć, że za średnie przedsiębiorstwa zostały uznane te, które zatrudniają co najmniej 50 i nie więcej niż 250 osób, obrót nieprzekraczający 50 mln euro oraz całkowity bilans roczny wynoszący nie więcej niż 43 mln euro (definicja na bazie art. 2 załącznika do zalecenia Komisji Europejskiej 2003/361). Jest to o tyle istotne, że określenie „średnie" kłóci się z powszechnym wyobrażeniem „średniości" firmy.

W efekcie tych zmian podmioty kluczowe to te, które działają w sektorach kluczowych (wymienionych w załączniku I) oraz spełniają dodatkowe kryteria, takie jak:

- określony poziom przychodów lub zatrudnienia,
- dostarczanie usług o szczególnym znaczeniu dla gospodarki lub społeczeństwa,
- ich działalność wiąże się z wysokim ryzykiem zakłóceń lub incydentów cyberbezpieczeństwa,

Natomiast podmioty ważne to te, które:

- działają w sektorach ważnych (wymienionych w załączniku II).
- mogą, ale nie muszą, spełniać dodatkowe kryteria określone dla podmiotów kluczowych.

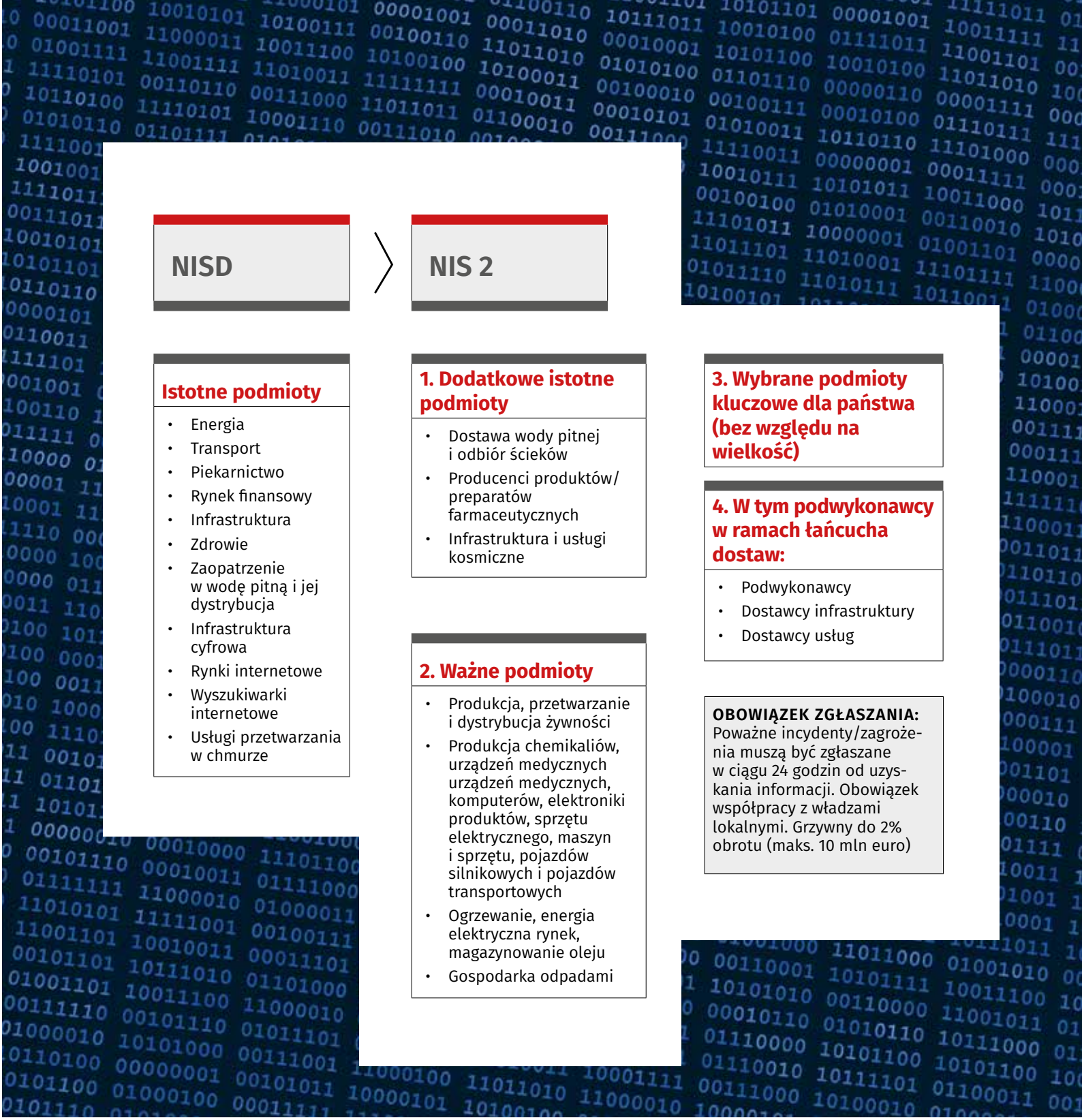
Dokładne kryteria dla podmiotów kluczowych i ważnych zostaną określone w aktach wykonawczych do dyrektywy NIS 2.

Ważne dla security managerów

Niezależnie od tego, jak ostatecznie ukształtuje się wdrożenie NIS 2 w Polsce, menedżerowie security powinni zwrócić uwagę na art. 21 i 23 nowelizowanej dyrektywy. Pierwszy z nich dotyczy zarządzania cybernetycznym ryzykiem, a drugi zgłaszania incydentów. Dyrektywa NIS 2 jasno określa kary za nieprzestrzeganie tych dwóch artykułów: maksymalna grzywna wynosi 10 mln euro lub 2% globalnego rocznego obrotu podmiotu z poprzedniego roku obrachunkowego, w zależności od tego, która wartość okaże się większa. Aby sprostać wymogom art. 21 Dyrektywy, właściciele aktywów powinni priorytetowo traktować kwestie bezpieczeństwa cybernetycznego w swoich systemach wykorzystujących technologie operacyjne. Technologie operacyjne (OT) to sprzęt i oprogramowanie służące do monitorowania i sterowania urządzeniami, procesami i infrastrukturą w środowiskach przemysłowych.

Dla menedżerów security kluczowe jest zrozumienie, w jaki sposób art. 21 będzie wdrażany w sieciach OT. Z treści tego artykułu wynika bowiem, że organizacje muszą zapewnić poziom bezpieczeństwa sieci i systemów informatycznych odpowiedni do występujących zagrożeń. Zapewnienie tego bezpieczeństwa wymagać będzie ścisłej współpracy działów zajmujących się w organizacjach cyberbezpieczeństwem z menedżerami security. Równo rok temu pisaliśmy na łamach magazynu o konieczności ścisłej współpracy działów ochrony systemów IT i OT z działami bezpieczeństwa fizycznego (*Konwergencja bezpieczeństwa,* a&s Polska 2/2023).

» W NIS 2 dotychczasowy podział na operatorów usług kluczowych, dostawców usług cyfrowych i podmioty publiczne ustąpił miejsca podziałowi na podmioty kluczowe i ważne. «



Dyrektywa NIS 2 a bezpieczeństwo systemów

Nowa dyrektywa w sprawie sieci i systemów informatycznych (NIS 2) koncentruje się głównie na technologiach informatycznych (IT) i podkreśla ochronę infrastruktury internetowej, takiej jak serwery DNS. Nie wspomina ona bezpośrednio o technologiach operacyjnych (OT) i klasyfikuje sektory tak różne, jak energetyka i bankowość, jako równie krytyczne. Jednak obowiązek podejmowania odpowiednich działań oraz ścisła odpowiedzialność powinny skłonić sektory OT do podniesienia standardów cyberbezpieczeństwa. Artykuł 21 dyrektywy zachęca do stosowania środków dobranych do ewentualnego ryzyka, co w przypadku infrastruktury krytycznej prawdopodobnie przełoży się na stosowanie bardziej rygorystycznych norm i regulacji. Artykuł 23 wymaga szybkiego zgłaszania cyberataków, co zwiększy przejrzystość. Jednak samo spełnienie wymogów NIS 2 nie gwarantuje ochrony przed zewnętrznymi cyberatakami, a minimalne środki określone w NIS 2 mogą być niewystarczające dla systemów OT, gdzie skutki cyberataku mogą być katastrofalne. Niespełnienie wymagań lub zastosowanie nieadekwatnych środków ochrony wprawdzie poskutkuje nałożeniem kary, ale w przypadku poważnego cyberataku na systemy OT, przede wszystkim te działające w przedsiębiorstwach infrastruktury krytycznej, istotą nie jest przecież kara, ale bezpieczeństwo publiczne. Należy mieć to na względzie, oczekując na krajową transpozycję unijnej dyrektywy.

Jak zarządzać cyberbezpieczeństwem infrastruktury krytycznej i przemysłu

Konsultanci oraz specjaliści projektujący i wdrażający rozwiązania w zakresie dozoru i bezpieczeństwa dla przemysłu i infrastruktury krytycznej stoją w obliczu wyjątkowej presji. Fizyczna ochrona takich kluczowych podmiotów jest oczywiście najważniejsza, ale dziś wyzwaniem okazują się ataki cyfrowe.

Istotne jest to, że wszystkie organizacje tworzące łańcuch wartości muszą dostosować się do nowych regulacji. W końcu cyberbezpieczeństwo jest wspólną odpowiedzialnością wszystkich zaangażowanych w projektowanie, specyfikację, dostawę i użytkowanie rozwiązania do dozoru. Poniżej przedstawiamy niektóre z tych wyzwań.

Świat, w którym prawie cała branża ma znaczenie krytyczne

Nie jest tajemnicą, że cyberataki są coraz liczniejsze i coraz bardziej wyrafinowane. I nie ma znaczenia, czy stoją za nimi hakerzy amatorzy, czy dobrze zorganizowani cyberprzestępcy szukający korzyści finansowych, czy też podmioty wspierane przez państwa narodowe, które chcą osłabić społeczeństwo przeciwnika. Istotne jest to, że przybierając różne formy i pochodząc z wielu źródeł, mogą zagrozić bezpieczeństwu organizacji, w tym o znaczeniu dla państwa krytycznym.

Ze względu na wysoce powiązany charakter globalnych łańcuchów dostaw zwiększył się również zakres tych sektorów przemysłu, które są obecnie definiowane jako podmioty kluczowe. Jeszcze dwa czy trzy lata temu wiele osób nie uznałoby produkcji i dostaw półprzewodników za krytyczne. Problemy z dostawami podczas pandemii pokazały jednak, jak istotne są chipy dla wielu – jeśli nie większości – współczesnych procesów przemysłowych.

„Efekt motyla", kiedy to niewielkie zakłócenie w jednym systemie może mieć duży wpływ na inny w przyszłości, okazał się prawdziwy w przypadku globalnie zintegrowanego łańcucha dostaw technologii.

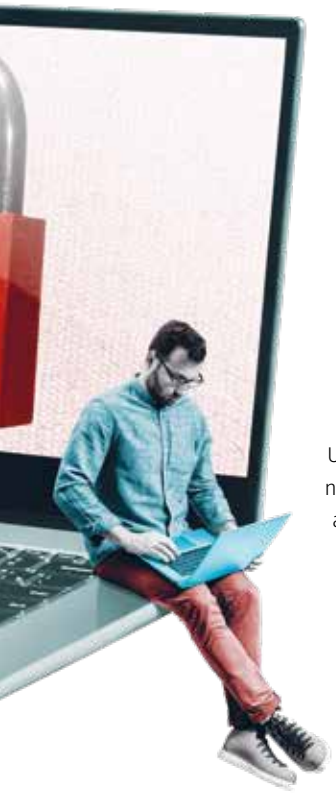
Organy regulacyjne w obliczu wyzwań związanych z cyberbezpieczeństwem

Za szybko i stale zmieniającym się środowiskiem cyberbezpieczeństwa rządy i organy regulacyjne bez wątpienia starają się nadążyć. Coraz częściej ich reakcją jest zmiana sposobu, w jaki regulują cyberbezpieczeństwo.

Mówiąc ogólnie, zamiast definiować, co dostawcy podstawowych usług muszą wdrożyć w odniesieniu do cyberbezpieczeństwa, tendencja w regulacjach polega na tym, że to na dostawcach spoczywa ciężar udowodnienia, że mają środki niezbędne do zachowania własnego cyberbezpieczeństwa. Zmiana ta ma poważne konsekwencje nie tylko dla dostawców, ale także dla każdej strony dostarczającej wiedzę i rozwiązania w ramach łańcucha dostaw podstawowych podmiotów.

NIS2 jako przykład ewoluującego środowiska regulacyjnego

Dyrektywa NIS2 weszła w życie w styczniu 2024 r., a państwa członkowskie UE mają czas do października br. na wprowadzenie jej w życie.



NIS2 jest odpowiedzią na ewoluujący krajobraz zagrożeń, ma na celu podniesienie ogólnego poziomu cyberbezpieczeństwa w UE i wypełnia luki obecne w pierwszej wersji dyrektywy. Jej celem jest wypracowanie „kultury bezpieczeństwa w sektorach o kluczowym znaczeniu dla naszej gospodarki i społeczeństwa, które w dużym stopniu opierają się na technologiach informacyjno-komunikacyjnych (ICT), takich jak energetyka, transport, gospodarka wodna, bankowość, infrastruktura rynków finansowych, opieka zdrowotna i infrastruktura cyfrowa".

Zgodnie z dyrektywą państwa członkowskie UE będą identyfikować przedsiębiorstwa i organizacje, które są operatorami usług kluczowych, a organizacje te będą musiały podjąć odpowiednie środki bezpieczeństwa i powiadomić odpowiednie organy krajowe o wszelkich poważnych incydentach cyberbezpieczeństwa. Kluczowi dostawcy usług cyfrowych, tacy jak usługodawcy przetwarzania w chmurze, również muszą spełniać wymogi bezpieczeństwa i powiadamiania określone w dyrektywie. Rozszerzenie dyrektywny na cały łańcuch dostaw technologii jest oczywiste.

Rozwiązania w zakresie dozoru jako element łańcucha wartości

Ochrona usług kluczowych zawsze była priorytetem. Nic dziwnego, że zabezpieczenia techniczne sukcesywnie były wzbogacane o nowe cyfrowe rozwiązania, co sprawiło, że zainteresowali się nimi cyberprzestępcy. Ten fakt muszą uwzględnić architekci, inżynierowie oraz konsultanci projektujący i określający rozwiązania w zakresie systemów dozoru. Rozwiązania dozorowe muszą być projektowane nie tylko pod kątem współczesnych wymagań w zakresie bezpieczeństwa fizycznego i cybernetycznego, ale też z uwzględnieniem zmieniających się wyzwań, w tym zachowania zgodności z przepisami.

Systemy bezpieczeństwa należy zatem postrzegać jako całość, a nie jako zbiór oddzielnych komponentów. Należy brać pod uwagę relacje między urządzeniami a oprogramowaniem, wraz z integracją z infrastrukturą podstawowego dostawcy usług. Projektowanie, wdrażanie, integracja i konserwacja rozwiązań odgrywają istotną rolę w cyberbezpieczeństwie, podobnie jak zrozumienie, że każde rozwiązanie musi być modernizowane.

Co to oznacza dla projektantów rozwiązań systemów dozoru?

Osoby projektujące i określające rozwiązania mają obowiązek rozważyć potencjalne szersze zagrożenia stwarzane przez rekomendowaną przez nich ofertę techniczną. Z jednej strony rozwiązania powinny koncentrować się przede wszystkim na spełnieniu określonych wymagań operacyjnych, z drugiej – należy uwzględniać przepisy dotyczące IT i cyberbezpieczeństwa, takie jak dyrektywa NIS2, aby wspierać zgodność organizacji. W związku z tym konsultanci muszą być pewni, że produkty każdego dostawcy spełniają politykę bezpieczeństwa klienta indywidualnego. Niezbędne jest zatem dokonywanie analizy *due diligence* w zakresie podejścia do cyberbezpieczeństwa każdego rekomendowanego dostawcy.

Konsultanci muszą również starać się określić zasady i procesy dla rekomendowanych przez siebie dostawców technologii, a także mieć pewność, że oferowane urządzenia zgodne są z nowymi przepisami. Funkcje takie jak bezpieczny start, podpisane oprogramowanie układowe, komponenty zabezpieczające, które umożliwiają automatyczną i bezpieczną identyfikację urządzeń, oraz moduł TPM *(Trusted Platform Module)* odnoszą się do zagrożeń stwarzanych obecnie i powinny zostać określone.

Specyfikacje powinny również obejmować ważne certyfikaty trzecich stron, takie jak ISO27001, oraz zasady dotyczące luk w zabezpieczeniach, powiadomienia o poradach dotyczących bezpieczeństwa i jasno zdefiniowany model rozwoju bezpieczeństwa.

Należy też uwzględnić podejście do zarządzania cyklem życia. Korzystanie z narzędzi do zarządzania urządzeniami i rozwiązaniami oraz udokumentowana strategia oprogramowania układowego zmniejszają ryzyko ataku i chronią klientów. Funkcje te pozwalają klientom obsługiwać swój system i urządzenia w możliwie najbezpieczniejszy sposób przez cały cykl ich życia.

Te zasady i procesy świadczą o dojrzałości cybernetycznej organizacji i jej zdolności do dostosowywania się do zmieniającego się krajobrazu zagrożeń.

Nowe wymagania wiążą się ze zmianą ról

Dla każdego kraju znaczenie zminimalizowania potencjalnych zakłóceń w świadczeniu podstawowych usług jest oczywiste i nie do przecenienia. Każdy incydent może mieć niemal natychmiastowy wpływ na gospodarkę, powodując np. niepokoje społeczne czy zagrażając zdrowiu i życiu obywateli.

Niezależnie od tego, skąd pochodzi zagrożenie, ochrona podstawowych usług i podmiotów, które je świadczą, ma zatem kluczowe znaczenie. Organy regulacyjne na całym świecie zdają sobie z tego sprawę. Uznały jednak również, że zagrożenia związane z cyberatakami ewoluują tak szybko, że wszelkie próby odgórnego definiowania tego, jakie środki cyberbezpieczeństwa muszą stosować organizację, będą nieaktualne, zanim zostaną opublikowane. W związku z tym zmieniono podejście regulacyjne, wymagając od dostawców podstawowych usług udowodnienia, że dysponują technologią, procesami i zasobami umożliwiającymi radzenie sobie z zagrożeniami.

W rezultacie każdy zaangażowany w łańcuch wartości istotnego podmiotu musi odpowiedzieć na to wyzwanie, w tym osoby projektujące i określające rozwiązania w zakresie systemów dozoru. Ograniczanie ryzyka cyberzagrożeń to wspólna odpowiedzialność. Firma Axis Communications już teraz jest przygotowana na wyzwania związane z wprowadzaną dyrektywą NIS2 i nieustannie pracuje nad zapewnieniem cyberbezpieczeństwa w ramach oferowanych rozwiązań i w całym łańcuchu dostaw.

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

Technologia dla bezpieczeństwa w infrastrukturze krytycznej

Obiekty infrastruktury krytycznej są kluczowe dla funkcjonowania społeczeństwa i gospodarki. Z tego powodu producenci systemów zabezpieczeń stale udoskonalają technologię przeznaczoną do tego typu obiektów. Powstają nowe systemy i urządzenia, które zawierają potrzebne modyfikacje, zainicjowane doświadczeniami w rzeczywistym środowisku pracy. Tworzone są też nowe rozwiązania oparte na technologiach alternatywnych, mogące wspierać istniejące systemy lub zwiększyć bezpieczeństwo w obszarach wcześniej pomijanych. Dotyczy to zarówno procesów produkcyjnych realizowanych w ramach infrastruktury krytycznej, jak i bezpieczeństwa infrastruktury w rozumieniu nieuprawnionego wtargnięcia osób do obiektu.

Tomasz Goljaszewski

W infrastrukturze krytycznej jest wiele obszarów wymagających zapewnienia odpowiedniego poziomu bezpieczeństwa. Należą do nich m.in. bezpieczeństwo cybernetyczne, procedury reagowania na incydenty czy bezpieczeństwo wynikające z właściwego przyznania uprawnień osobom mogącym mieć dostęp do danego obszaru. Nowe rozwiązania techniczne podnoszą poziom bezpieczeństwa, m.in. dzięki skuteczniejszemu wykrywaniu prób wtargnięcia.

Termowizja i kamery bispektralne

Kamery termowizyjne są dostępne na rynku już od wielu lat. Natomiast urządzenia bispektralne, będące połączeniem kamery termowizyjnej i wizyjnej wysokiej rozdzielczości, cieszą się mniejszą popularnością wśród projektantów czy specjalistów zajmujących się bezpieczeństwem infrastruktury krytycznej. W kamerach bispektralnych część termowizyjna stanowi pewien rodzaj sensora, a część wizyjna umożliwia ogólną obserwację zdarzenia lub dokładniejszą jego weryfikację, zwłaszcza jeżeli mówimy o modelach szybkoobrotowych czy PTZ. Jest wiele zastosowań tego typu kamer, np. do:

- wykrywania intruza,
- mierzenia temperatury w celu wykrycia przegrzewających się urządzeń czy podzespołów (np. stacje energetyczne),
- zapobiegania pożarom,
- obserwowania powierzchni paneli fotowoltaicznych w farmach solarnych,
- obserwowania miejsca składowania materiałów łatwopalnych czy takich, które w wyniku reakcji chemicznej mogą niebezpiecznie zwiększać swoją temperaturę.

Kamery bispektralne znakomicie sprawdzają się w ochronie obwodowej. Wbudowana analiza obrazu umożliwia detekcję obiektów czy ludzi ze znacznie większej odległości niż w przypadku klasycznych kamer wizyjnych. A zastosowanie termowizji powoduje, że kamery te generują znacznie mniej fałszywych alarmów.

Jednym z ciekawszych urządzeń wykorzystujących termowizję są skanery panoramiczne 360°. W tych urządzeniach przetwornik termowizyjny wiruje ze stałą prędkością. Działa na zasadzie radaru, dlatego możliwa jest niemal jednoczesna detekcja wielu obiektów. Jeden skaner może wykrywać obiekty (np. ludzi) na obszarze o promieniu nawet 900 m.

Skaner termowizyjny dający obraz 360°

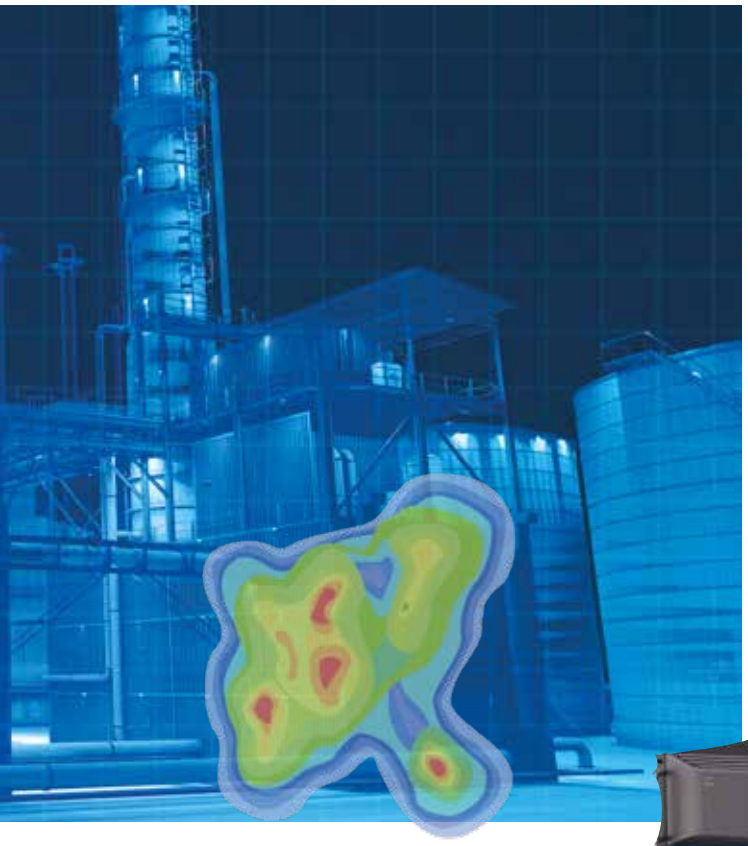
Radar
DS-TDSB0G-FK/500 m

Radar

Radary są chętnie stosowane do ochrony, ich działanie bowiem nie zależy od niekorzystnych warunków atmosferycznych, takich jak opady deszczu, zamiecie śnieżne itp., a niedostatki oświetlenia w ogóle tej technologii nie dotyczą. Typowy radar stosowany w systemach zabezpieczeń nie posłuży do dokładnego rozpoznania wzorca obiektów, ale stosunkowo łatwo można go zintegrować z kamerą szybkoobrotową. Dzięki temu weryfikacja alarmów jest szybka. Ze względu na potencjał technologia radarowa jest stale rozwijana. Na rynku są już dostępne radary o zasięgu nawet 500 m w przypadku detekcji ludzi i 1000 m w przypadku detekcji pojazdów. Do niedawna było to tylko odpowiednio: 120 i 200 m. Przy poziomym kącie detekcji 100° jedno urządzenie pokrywa duży obszar roboczy.

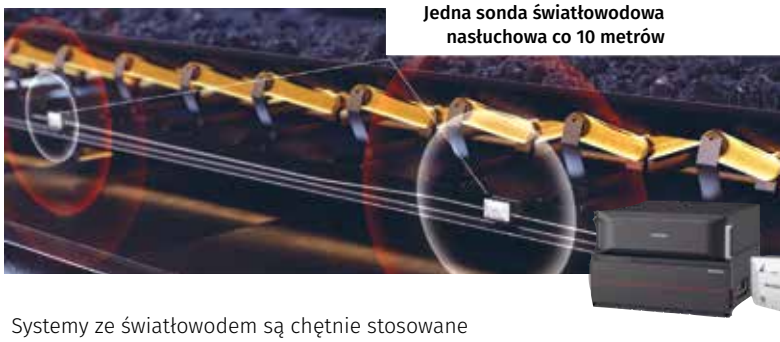
Światłowód

Systemy wykorzystujące światłowód są stosowane zarówno w obszarze bezpieczeństwa procesów technologicznych, jak i w ochronie obwodowej. Mogą służyć do detekcji wibracji, detekcji nacisku, detekcji zmian temperatury oraz do osłuchiwania w przypadku długich odcinków wymagających gęstego rozmieszczenia czujników. Systemy detekcji wibracji czy nacisku są najczęściej używane do ochrony obwodowej.



DS-QFV5002 Analizator 2-kanałowy do systemów napłotowych

Jedna sonda światłowodowa nasłuchowa co 10 metrów

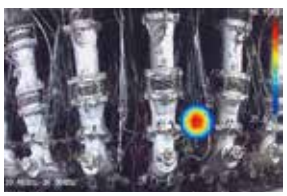


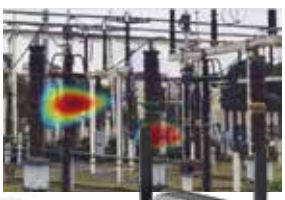
Systemy ze światłowodem są chętnie stosowane do ochrony procesów produkcyjnych, do detekcji zmian temperatury czy nasłuchu. Wykrycie zmiany temperatury sprawdza się np. w rozległych magazynach lub do pomiaru na długich odcinkach (rurociągi, tunele, trasy kablowe, inne). Technika nasłuchiwania z wykorzystaniem światłowodu jest używana m.in. w przypadku taśmociągów przenoszących towary sypkie (węgiel), gdzie istnieje ryzyko zatarcia wałków przenoszących taśmę podajnika.

Skuteczność kamer termowizyjnych czy bispektralnych zależy w dużym stopniu od ich czułości termicznej. Do niedawna standardem była czułość termiczna *(Noise Equivalent Temperature Difference – NETD)* na poziomie 40 mK. Obecnie dostarczane są już kamery z lepszą czułością NETD na poziomie 35 mK. Warto jednak zwrócić uwagę, że najlepsze firmy wprowadzają produkty o czułości NETD na poziomie 25–30 mK w zależności od parametrów obiektywu. To bardzo duży skok technologiczny umożliwiający lepsze obrazowanie, a tym samym skuteczniejszą pracę wbudowanych algorytmów analizy wizyjnej.

Detekcja akustyczna zintegrowana z kamerą

Tego typu rozwiązanie, nazywane kamerą akustyczną, jest przeznaczone głównie do ochrony procesów produkcyjnych. Urządzenie może wykryć nietypowe dźwięki czy szumy, niesłyszalne dla człowieka. Integracja sensora akustycznego z kamerą umożliwia bardzo szybką wizualizację i wskazanie na obrazie miejsca lub obszaru, z którego wydobywają się dźwięki czy szumy o podejrzanych częstotliwościach. Źródłem takich sygnałów mogą być np. wadliwe styki elektryczne, uszkodzone izolatory energetycznych linii napowietrznych czy stacji energetycznych. Kamery akustyczne mogą też monitorować online potencjalne wycieki gazu w rurociągach czy dużych instalacjach gazowych.





Wykres akustyczny

Rozwój technologii w zakresie bezpieczeństwa infrastruktury krytycznej trwa nieprzerwanie. Opisane rozwiązania nie wyczerpują tej tematyki, a jedynie przedstawiają wybrane nowości, które mogą być interesujące z punktu widzenia projektantów czy działów bezpieczeństwa. ●

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

Kamery marki Milesight w obiektach infrastruktury krytycznej

Milesight to szybko rozwijająca się firma, która od 2011 r. dostarcza inteligentne produkty IoT i dozoru wizyjnego, koncentrując się na technologiach IoT, w tym sztucznej inteligencji, 5G i LoRaWAN®. Jako jedna z niewielu chińskich firm produkuje kamery zgodnie z NDAA *(National Defense Authorization Act).* Urządzenia Milesight od wielu lat oferuje firma Miwi Urmet.

Jacek Karcewicz

W portfolio firmy Milesight znajduje się wiele ciekawych rozwiązań, m.in. kamery z inteligentną analityką umożliwiającą uzyskiwanie zaawansowanych informacji o ruchu drogowym w celu poprawy przepustowości i jego bezpieczeństwa. Warto również zwrócić uwagę na urządzenia do monitoringu wizyjnego, które dają obraz panoramiczny 180° oraz dookólny 360° z rozdzielczością 4K (12 Mpix). Do monitorowania dużych obszarów Milesight proponuje kamery PTZ z wieloma zaawansowanymi funkcjami. W ofercie znajdują się również rozwiązania IoT stosowane w komunikacji między urządzeniami a systemami.

Produkty Milesight znajdują zastosowanie na całym świecie w przedsiębiorstwach infrastruktury krytycznej, firmach zajmujących się handlem detalicznym, urzędach, zakładach przemysłowych, szkołach, a także w dużych gospodarstwach rolnych. Firma Miwi Urmet z powodzeniem stosuje kamery Milesight do dozoru obiektów infrastruktury krytycznej.

Jednym z przykładów takich rozwiązań jest przeprowadzona modernizacja systemu monitoringu wizyjnego w dużym obiekcie z sektora energetyki. W przedsiębiorstwie od wielu lat działały kamery analogowe, które ze względu na ograniczenia funkcjonalne dostarczały obrazy niedostatecznej jakości. Z różnych względów niemożliwa była jakakolwiek rozbudowa systemu. Po dokonaniu audytu i sprawdzeniu potrzeb klienta okazało się, że niezbędne są:

- aktualizacja całej infrastruktury poprzez wymianę analogowych i przestarzałych kamer oraz rejestratorów sieciowych,
- uruchomienie centrum monitoringu spełniającego najwyższe standardy jakości,
- zabezpieczenie wszystkich priorytetowych lokalizacji kamerami sieciowymi, w tym również z obsługą PoE,
- instalacja rejestratora sieciowego (NVR) umożliwiającego monitorowanie, nagrywanie i odtwarzanie zapisów z kamer,
- zapewnienie płynnej interakcji na wszystkie zarejestrowane zdarzenia,
- zarządzanie wielkością plików wideo nagranych przez NVR,
- możliwość zdalnego przeglądania obrazów ze wszystkich kamer,
- opracowanie sposobu przesyłania zapisów z kamer do centrum zarządzania z obszarów, w których nie ma możliwości podłączenia kablowego,
- zapewnienie możliwości wykrywania i alarmowania w sytuacji wejścia na obszary objęte ograniczeniami.

W odpowiedzi na te potrzeby wdrożono kompleksowe rozwiązanie monitoringu bazujące na produktach marki Milesight, skupiając się na tym, by system był jednocześnie wydajny i skalowalny. W ramach tego rozwiązania zainstalowano 19 wandaloodpornych kamer Mini Dome, 61 typu Mini Bullet, 6 kamer Mini PTZ Bullet oraz 2 typu Fisheye. Całość została uzupełniona o 3 rejestratory NVR. Wszystkie urządzenia zostały zintegrowane z istniejącą siecią LAN i systemem zasilania.

To jeden z przykładów zastosowania kamer Milesight w obiekcie infrastruktury krytycznej. Kamery te zostały również wykorzystane do zabezpieczenia wielu głównych punktów zasilających (GPZ), gdzie rejestrowane lokalnie strumienie wizyjne są kierowane do jednej z kilku Stacji Monitorowania Alarmów.

Wszystkich zainteresowanych szczegółowymi informacjami na temat urządzeń Milesight zapraszamy do kontaktu z działem CCTV naszej firmy. ●

Miwi Urmet
ul. Pojezierska 90A,91-341 Łódź
miwi@miwiurmet.pl
www.miwiurmet.pl

Milesight

urmet MIWI

NDAA

KAMERY Milesight
OPTYMALNYM ROZWIĄZANIEM W ZABEZPIECZANIU OBIEKTÓW INFRASTRUKTURY KRYTYCZNEJ

urmet MIWI

MIWI URMET Sp. z o.o.
ul. Pojezierska 90 A I 91-341 Łódź
+48 42 616 21 00 I miwi@miwiurmet.pl
www.miwiurmet.pl

głos branży

Security menedżerowie nie mają dziś łatwego zadania. Zawirowania związane z trudną sytuacją geopolityczną wymuszają większe zaangażowanie w zapewnienie odpowiedniego poziomu bezpieczeństwa, zwłaszcza obiektów infrastruktury krytycznej. Dlatego tak ważne jest dzielenie się wiedzą, doświadczeniem i cennymi wskazówkami. Co radzą nasi eksperci?

Konrad Badowski
AXIS COMMUNICATIONS

Wymagania dyrektywy NIS2

W październiku tego roku ma wejść w życie najnowsza dyrektywa UE NIS2 dotycząca bezpieczeństwa sieci i informacji. Stanowi rozwinięcie istniejących regulacji dotyczących cyberbezpieczeństwa w Unii Europejskiej. Bazując na fundamentach wyznaczonych przez pierwotną Dyrektywę NIS, NIS2 ma na celu zwiększenie świadomości zagrożeń oraz wdrożenie systemowych rozwiązań ochrony cybernetycznej wśród podmiotów objętych dyrektywą.

Jedną z istotnych nowości Dyrektywy NIS2 jest znaczne rozszerzenie zakresu regulacji. Objęci nią są teraz np. dostawcy usług cyfrowych, w tym platformy handlowe online, a także podmioty, których działalność ma kluczowe znaczenie dla podstawowych funkcji społecznych lub ekonomicznych, takie jak dostawcy żywności, wody, energii czy też usługi transportu publicznego.

NIS2 wprowadza bardziej rygorystyczne wymagania dotyczące cyberbezpieczeństwa w celu wzmocnienia ochrony sieci i systemów informatycznych. Wymagania te obejmują takie środki, jak zarządzanie ryzykiem, usystematyzowana reakcja na incydenty, ocena bezpieczeństwa łańcucha dostaw, ogólnie mówiąc, wdrożenie odpowiednich środków technicznych i organizacyjnych zapewniających bezpieczeństwo sieci i systemów informacyjnych. Poprzez narzucenie tych środków dyrektywa ma na celu wzmocnienie ogólnego stanu cyberbezpieczeństwa oraz zminimalizowanie ryzyka poważnych konsekwencji dla obywateli w razie cyberataku.

Ponadto NIS2 obejmuje postanowienia dotyczące nadzoru regulacyjnego i egzekwowania przestrzegania wymogów dyrektywy. Krajowe organy odpowiedzialne mają za zadanie monitorowanie przestrzegania przepisów i nakładanie kar za ich naruszenie, w tym grzywny i inne środki administracyjne. Kary mogą być dotkliwe, uzależnione od obrotów danego podmiotu, dodatkowo wprowadza się bezpośrednią odpowiedzialność zarządów. Ten mechanizm ma skłonić firmy do należycie uważnego wdrożenia postanowień NIS2 w swoich organizacjach.

Ogólnie rzecz biorąc, Dyrektywa UE NIS2 stanowi istotny krok naprzód w kwestii wzmocnienia cyberbezpieczeństwa w Unii Europejskiej, co przyczyni się do stworzenia bezpieczniejszego środowiska cyfrowego dla przedsiębiorstw i obywateli UE.

Arkadiusz Rymarski
HONEYWELL

Budowanie zgodności z NIS2

Dyrektywa NIS2, będąca odpowiedzią na dynamicznie zmieniające się cyberzagrożenia, stanowi kluczowy element wzmacniania cyberbezpieczeństwa w Unii Europejskiej. Jej wdrożenie dotyczy obszaru całej UE, gdzie infrastruktura krytyczna staje przed wyzwaniem dostosowania się do nowych, bardziej rygorystycznych standardów.

Polska, jako członek UE, jest zobowiązana do transpozycji dyrektywy do krajowego porządku prawnego. Obejmuje to dostosowanie istniejących regulacji oraz wprowadzenie nowych rozwiązań, które odpowiadają za obszary zidentyfikowane w dyrektywie. Wymaga to ścisłej współpracy między sektorem publicznym i prywatnym, zwłaszcza w zakresie wymiany informacji i zarządzania incydentami.

Osoby decyzyjne, odpowiedzialne za infrastrukturę krytyczną w Polsce, muszą zatem przeprowadzić kompleksową analizę swoich systemów IT i OT pod kątem zgodności z NIS2, co zapewne będzie wymagać przebudowy systemów, szkolenia personelu i wzmocnienia mechanizmów reagowania na incydenty. Dla administratorów infrastruktury krytycznej, przemysłowej czy militarnej przepisy te stanowią okazję do oceny możliwości i operacji pod kątem zaostrzonych wymogów w zakresie cyberbezpieczeństwa. Ale dla organizacji, które nie zmodernizowały swoich zdolności cybernetycznych, jest to również sygnał ostrzegawczy informujący o potrzebie podjęcia działań w celu lepszego przeciwdziałania zagrożeniom związanym z cyberbezpieczeństwem dla ich infrastruktury i upewnienia się, że ich działania są zgodne z przepisami NIS2.

Aby lepiej zdefiniować organizacje, które muszą zostać uwzględnione, ustalono dwa podstawowe kryteria: sektor i wielkość. NIS2 identyfikuje sektory „wysoce krytyczne" (czyli podmioty kluczowe) i „krytyczne" (czyli podmioty ważne). Istnieje jedenaście sektorów o wysokim stopniu krytyczności, w dużej mierze związanych z codziennymi operacjami gospodarki danego kraju, takimi jak energia, transport, bankowość, usługi wodne, opieka zdrowotna, infrastruktura cyfrowa, rząd i przestrzeń kosmiczna. Sektory krytyczne są związane z kluczowymi usługami wspierającymi gospodarkę kraju, takimi jak produkcja i dystrybucja żywności, chemikaliów i towarów, gospodarka odpadami. Należą do nich również dostawcy usług cyfrowych (dostawcy usług internetowych – ISP) oraz ośrodki badawcze.

Przedsiębiorstwom wskazuje się partnerstwo z producentami, którzy wykazują gotowość do zgodności z NIS2. Producenci ci powinni mieć sprawdzone protokoły cyberbezpieczeństwa i historię działań. Ponieważ zgodność z CRA może świadczyć o gotowości do NIS2, zaleca się, aby przedsiębiorstwa współpracowały z producentami zgodnymi z CRA. Dobrą praktyką może być również uwzględnianie regulacji NDAA. W przypadku infrastruktury krytycznej buduje się w ten sposób cyberparasol, który zabezpiecza urządzenia przez cały cykl ich życia, wymagając regularnych aktualizacji. Producenci muszą również przeprowadzać regularne oceny ryzyka. Procedurę tę stosuje Honeywell, wykonując testy penetracyjne i kontrole bezpieczeństwa swoich rozwiązań.

Dyrektywa będzie egzekwowana w każdym państwie członkowskim. Podobnie jak z przepisami RODO dokładne zrozumienie wymogów ochrony danych i działań wymaganych przez organizacje z czasem rosło. Prawdopodobnie będzie tak również w przypadku NIS2. Na podstawie aktualnych informacji organizacje będą musiały podjąć niezbędne kroki już teraz, aby nie być zaskoczone w przyszłości. W związku z tym kluczowe znaczenie mają identyfikacja słabych punktów i szybkie ich wyeliminowanie. Dotyczy to np. urządzeń, które kolekcjonują dane i pozwalają tym danym „wypływać" w mniej bądź bardziej wyrafinowany sposób. Jedno jest pewne, aby uniknąć wyboru urządzeń czy rozwiązań producentów symulujących spełnienie kryteriów NIS2, rekomenduje się, by były zgodne również z regulacją NDAA.

Marcin Walczuk
BCS

Przepisy dotyczące bezpieczeństwa IK

Zgodnie z informacjami dostępnymi na stronie Rządowego Centrum Bezpieczeństwa infrastruktura krytyczna (IK) obejmuje rzeczywiste i cybernetyczne systemy niezbędne do funkcjonowania gospodarki i państwa. Wzmocnienie odporności infrastruktury krytycznej na zagrożenia, w tym o charakterze terrorystycznym, jest przedmiotem ciągłej analizy i aktualizacji przepisów prawa. Systemy zabezpieczenia są nadzorowane przez Centra Nadzoru i zarządzane przez Centra Zarządzania Kryzysowego. Warto również zwrócić uwagę na raporty i analizy dotyczące bezpieczeństwa obiektów infrastruktury krytycznej, które mogą dostarczać informacji o stanie zabezpieczeń oraz rekomendacjach dotyczących ich poprawy. Na przykład raport Najwyższej Izby Kontroli z 2016 r. wskazywał na braki w zabezpieczeniach w obszarach ochrony fizycznej i osobowej, co ułatwia wystąpienie niebezpiecznych incydentów. Podsumowując, poziom zabezpieczeń obiektów infrastruktury krytycznej w Polsce jest przedmiotem stałego nadzoru i ewaluacji, a wszelkie oceny powinny być oparte na aktualnych i szczegółowych danych oraz analizach prowadzonych przez odpowiednie instytucje.

W Polsce ochrona infrastruktury krytycznej jest regulowana przez ustawę o zarządzaniu kryzysowym z 2007 r., która określa podstawowe zasady, cele, zadania i kompetencje w tym zakresie. Ponadto w 2019 r. został przyjęty Narodowy Program Ochrony Infrastruktury Krytycznej, który jest strategicznym dokumentem określającym kierunki i priorytety działań na rzecz zapewnienia bezpieczeństwa i ciągłości funkcjonowania IK. Program ten zakłada m.in. identyfikację, ocenę systemów i obiektów IK oraz zagrożeń dla nich, opracowanie i wdrażanie standardów bezpieczeństwa oraz planów ochrony IK czy rozwój i modernizację systemów zabezpieczeń technicznych. Kolejnym założeniem programu jest rozwój i doskonalenie systemów reagowania i zarządzania kryzysowego w przypadku awarii lub ataku na infrastrukturę krytyczną, podnoszenie świadomości

→

i kultury bezpieczeństwa wśród podmiotów z nią związanych oraz współpraca międzynarodowa i regionalna w zakresie ochrony IK. Ochrona infrastruktury krytycznej jest nie tylko obowiązkiem państwa, ale także wspólną odpowiedzialnością wszystkich podmiotów i osób, które z niej korzystają lub mają na nią wpływ.

Polecając rozwiązania mające na celu zabezpieczenie obiektów IK, trzeba wziąć pod uwagę wiele czynników, m.in. zmieniające się przepisy czy aktualną sytuację geopolityczną. Warto również wspomnieć o amerykańskiej dyrektywie NDAA i konieczności stosowania zgodnych z nią urządzeń, które ma w swojej ofercie BCS w postaci serii produktów BCS Ultra. Pojawiające się nowego typu rodzaje ataków, jakie mogą być w pierwszej kolejności skierowane właśnie w te najbardziej newralgiczne dla stabilności państwa obiekty, oraz chęć zabezpieczenia się przed nimi powinny stanowić główny czynnik do zwiększenia nakładów na modernizację i poprawę poziomu systemów zabezpieczeń technicznych.

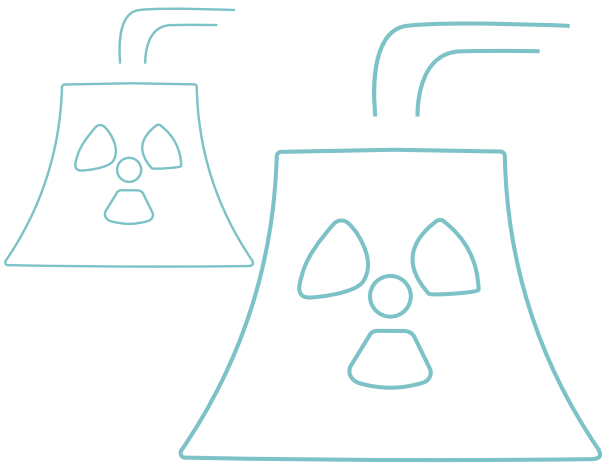
Tomasz Guzikowski
CIECH

Kluczowa rola menedżera security

Dzisiejsze zagrożenia, które kiedyś mogły uchodzić za political fiction, niestety stały się rzeczywistością. Wojna w Ukrainie wraz ze skutkami pandemii spowodowały konieczność fundamentalnej weryfikacji planów awaryjnych, ponownego przeprowadzenia szacowania ryzyka. Co więcej, weryfikacja zagrożeń i szacowanie ryzyka powinno być realizowane obecnie dużo częściej niż w tzw. czasach pokoju, a wręcz permanentnie. Menedżer odpowiedzialny za bezpieczeństwo m.in. zakładów produkcyjnych, szczególnie kluczowych z punktu widzenia gospodarki narodowej i globalnej, powinien skoncentrować się na kilku ważnych obszarach:

1. **Bezpieczeństwo personelu:** Priorytetem jest zapewnienie bezpieczeństwa pracowników w miejscu pracy. To obejmuje odpowiednie środki ochrony osobistej, przeszkolenie personelu z zasad bezpieczeństwa i postępowania w sytuacjach awaryjnych oraz wdrożenie środków zapobiegawczych.
2. **Planowanie kontynuacji działalności:** Menedżer bezpieczeństwa powinien opracować i wdrożyć plan kontynuacji działalności, który uwzględnia różne scenariusze związane m.in. z obecną sytuacją geopolityczną i makroekonomiczną. Taki plan powinien obejmować procedury awaryjne, zapasy niezbędnych materiałów i surowców oraz plany działań w przypadku ograniczeń w dostawach lub zamknięcia zakładu.
3. **Zabezpieczenie infrastruktury:** Ważne jest zabezpieczenie infrastruktury zakładu przed ewentualnymi zagrożeniami związanymi z panującą sytuacją, takimi jak sabotaż, ataki cybernetyczne czy przestępczość zorganizowana. Konieczne może być wzmocnienie systemów zabezpieczeń, monitorowanie terenów zakładu oraz współpraca z odpowiednimi organami bezpieczeństwa państwa.
4. **Zarządzanie łańcuchem dostaw:** Należy monitorować sytuację na rynkach surowcowych oraz w łańcuchach dostaw, aby szybko reagować na ewentualne problemy związane z dostępnością surowców i materiałów. Konieczne może być poszukiwanie alternatywnych źródeł zaopatrzenia oraz budowanie strategicznych rezerw.
5. **Komunikacja i informacja:** Niezwykle istotne jest utrzymanie transparentnej i skutecznej komunikacji z pracownikami i zainteresowanymi stronami. Menedżer bezpieczeństwa powinien regularnie informować personel o wszelkich zmianach w procedurach bezpieczeństwa, planach działania oraz potencjalnych zagrożeniach.
6. **Współpraca z władzami i innymi instytucjami:** Menedżer bezpieczeństwa powinien współpracować z władzami lokalnymi, organami bezpieczeństwa oraz innymi instytucjami, takimi jak służba zdrowia czy wojsko, w celu uzyskania wsparcia i skoordynowania działań w przypadku sytuacji kryzysowych.

Podsumowując, w obliczu obecnych zagrożeń rola menedżera ds. bezpieczeństwa znacząco wzrosła. To on powinien być obecnie swego rodzaju łącznikiem i pierwszym punktem kontaktowym dla wszystkich interesariuszy, szczególnie odpowiedzialnych za realizację krytycznych procesów biznesowych w organizacji czy podejmujących kluczowe decyzje w firmie. Ścisła współpraca jest niezbędna do tego, aby skutecznie zapewnić bezpieczeństwo zarówno personelu, jak i infrastruktury, szczególnie w kontekście zapewnienia ciągłości działania organizacji.



Maciej Kornacki
HILL INTERNATIONAL

Koń trojański w cyberbezpieczeństwie

Obecnie klienci oczekują innowacyjności oraz jak najmniejszego kosztu utrzymania inwestycji. Wymagania te spełnia zdalne zarządzanie systemami, w tym systemami zabezpieczeń technicznych. A to znaczy, że zważywszy na sytuację geopolityczną, menedżerowie ds. bezpieczeństwa muszą zwracać szczególną uwagę na zapewnienie odpowiedniego poziomu

cyberbezpieczeństwa wszystkich systemów. Wiadomo, że zawsze lepiej jest rozpoznawać, przewidywać i zapobiegać potencjalnym incydentom niż zmagać się z ich skutkami. Zwłaszcza, że obserwujemy dziś gigantyczny wzrost liczby cyberataków.

Innowacyjne rozwiązania bezpieczeństwa odgrywają dziś kluczową rolę w tworzeniu nowoczesnych, zrównoważonych i efektywnych struktur. Mają zapewnić konsumentowi komfort ich użytkowania oraz oszczędności związane z zastosowaniem zdalnego dostępu. Niestety sieciowe systemy niewłaściwie zabezpieczone stają się łatwym celem hakerów.

Inteligentne systemy zarządzania budynkami zaczynają się od aplikacji integrujących systemy budynkowe, które użytkownikom tych obiektów mają znacząco ułatwić życie. Wystarczy smartfon z odpowiednią aplikacją, by zdalnie otworzyć szlaban, wezwać windę, która jednak zatrzyma się tylko na tych piętrach, na których dana osoba może przebywać, a nawet otworzyć drzwi do biura. Dzięki inteligentnym systemom budynkowym użytkownik otrzymuje w czasie rzeczywistym informacje, np. o temperaturze i wilgotności powietrza, które może dowolnie regulować. W razie potrzeby może też zarezerwować salę konferencyjną na spotkanie lub opłacić ładowanie samochodu elektrycznego przed wyjazdem z parkingu. Inteligentne systemy zarządzania budynkiem poprawiają efektywność pracy urządzeń (takich jak klimatyzacja), redukując ryzyko ludzkich błędów. Tego typu zaawansowane aplikacje gromadzą dane dotyczące np. obecności ludzi, pozwalając dostosować ogrzewanie lub chłodzenie do największego obłożenia budynku, co oznacza oszczędność energii, a to przekłada się na spadek kosztów jego utrzymania. Natomiast połączenie z systemami kontroli dostępu, telewizją przemysłową czy sygnalizacją pożarową oznacza wyższy poziom bezpieczeństwa w obiekcie.

Wszystko to jednak wiąże się z koniecznością zapewnienia odpowiedniego poziomu cyberbezpieczeństwa. Menedżer za nie odpowiedzialny musi pamiętać, że telefon użytkownika może stać się koniem trojańskim, łatwym narzędziem cyberprzestępców, służącym do ataku na systemy sieciowe.

Tomasz Goljaszewski
HIKVISION POLAND

Podniesienie poziomu bezpieczeństwa obiektów IK

Z moich obserwacji wynika, że obiekty infrastruktury krytycznej prawie zawsze są zabezpieczane w ten sam sposób. Pewne schematy wypracowane kilkanaście lat temu są ciągle obowiązujące, mimo że zagrożenia są dziś bardziej złożone. Obecnie technologia stwarza więcej możliwości, a niektóre rozwiązania są teraz dużo tańsze niż 10 czy 15 lat temu. Jednak ich wykorzystanie jest jeszcze bardzo ograniczone.

Aby podnieść poziom bezpieczeństwa obiektów infrastruktury krytycznej, konieczne jest też stałe podnoszenie poziomu wyszkolenia operatorów ze względu na coraz większe zaawansowanie systemów zabezpieczeń. Często bowiem zdarza się, że możliwości nowoczesnego systemu wykorzystuje się w 15% procentach właśnie ze względu na brak wiedzy operatora czy security menedżera. Taka sytuacja na pewno nie jest pożądana, a nawet może okazać się niebezpieczna.

Zarządzający infrastrukturą krytyczną najczęściej inwestują w standardowe kamery, ochronę perymetryczną z systemem napłotowym, stosunkowo prostą kontrolę dostępu czy system alarmowy. Jeżeli występuje integracja tych systemów, to z reguły jest ona dość prosta, ograniczona do wizualizacji alarmu. Wykorzystanie bardziej zaawansowanych rozwiązań, takich jak radary security czy kamery bispektralne wymaga dość dobrego zrozumienia zasad ich działania i korzyści wynikających z ich zastosowania. Osób otwartych na nową wiedzę i rozwój nie spotyka się często, ale oczywiście zdarzają się security menedżerowie, którzy są pewnymi innowatorami w swoim środowisku. Dzięki nim w naszej branży następuje faktyczny rozwój i unowocześnianie standardów.

Dziś security menedżerowie powinni podchodzić do spraw bezpieczeństwa z otwartą głową. Ważne jest też, aby osoby odpowiedzialne za bezpieczeństwo aktywnie interesowały się rozwojem tej branży i szkoliły się w zakresie nowych technologii. Jeżeli będą rozumieć sens stosowania nowszych rozwiązań, łatwiej będzie im przekonać zarządy firm lub odpowiednie departamenty do przeprowadzenia zmian.

Zachęcam też do okresowego przeprowadzania symulacji różnych scenariuszy alarmowych, aby zweryfikować jakość detekcji i szybkość reakcji zadziałania systemów czy procedur. Rezultaty takich działań mogą ujawnić pewne luki w procesach, które mogą skłaniać do ich modernizacji z wykorzystaniem nowszych technologii lub do wymiany systemów. Ciekawą formą są też audyty. Realizowane przez firmę zewnętrzną z odpowiednimi uprawnieniami mogą ujawnić braki w systemie lub jego niesprawność. Audyt może też być pomocny w lepszym skalibrowaniu już istniejących funkcji systemu lub aktywacji tych, które system oferował, ale z jakiegoś powodu nie były one wykorzystywane. ●

Mobilne wieże do monitoringu – wyższy poziom bezpieczeństwa

Mobilne wieże monitoringu wizyjnego stają się coraz popularniejszym rozwiązaniem w sektorze bezpieczeństwa. Oferują elastyczność i skalowalność, których brakuje tradycyjnym systemom dozoru wizyjnego.
Jan T. Grusznic

Rosnąca popularność bierze się z prostego powodu: to rozwiązanie autonomiczne, tymczasowe, a jednocześnie mobilne. Wieże, wyposażone w zaawansowane technicznie urządzenia, budzą respekt już samym wyglądem. Postawienie takiego sprzętu świadczy o tym, że teren i wszystko, co na nim się znajduje, jest chronione. To zatem idealny przykład wykorzystania metodyki 5D (patrz: *Taktyka i technika w ochronie obwodowej*, nr 2/2023) skumulowanej w jednym rozwiązaniu, mającej na celu zmniejszenie ryzyka zagrożeń.

Konstrukcja – na platformie lub przyczepie

Mobilna wieża monitoringu to samowystarczalna platforma z kilkumetrowym rozkładanym masztem, na którego szczycie są umieszczane kamery dozoru wizyjnego, czujniki ruchu, radary, głośniki, źródła światła itp. Wyposażenie zależy od przeznaczenia i uniwersalności rozwiązania. Zazwyczaj wieża jest montowana na specjalnej mobilnej platformie lub przyczepie zapewniającej łatwy transport. Całość jest najczęściej wykonana ze stali ocynkowanej, aby zagwarantować odporność konstrukcji na warunki atmosferyczne. Elementy wyposażenia, które nie są umieszczane na maszcie, są zamykane wewnątrz platformy, co minimalizuje ryzyko ewentualnego sabotażu. Sama konstrukcja powinna mieć zabezpieczenie mechaniczne i elektroniczne uniemożliwiające wejście na platformę. Dzięki tym elementom maszt, kamery, sprzęt zasilający i komunikacyjny oraz inne urządzenia będą bezpieczne.

Zasilanie – z sieci lub własne

W miejscach zurbanizowanych najczęstszym źródłem zasilania wieży jest bezpośrednie podłączenie do sieci energetycznej. Krótkotrwałe przerwy w zasilaniu (12–24 godz.) nie stanowią wówczas problemu, gdyż energii dostarczają akumulatory znajdujące się w wyposażeniu wieży. Innym rozwiązaniem są generatory prądu, które mogą być dodatkowo wspierane panelami fotowoltaicznymi, co zapewnia pełną autonomię rozwiązania i ciągłość działania nawet przez cały rok.

Warto wspomnieć o zdobywających popularność rozwiązaniach opartych na generatorach wykorzystujących ogniwa paliwowe. Zastosowanie metanolu jako źródła zielonej energii ma wymiar nie tylko ekologiczny, ale także praktyczny. Takie rozwiązanie jest czystsze w rozumieniu utrzymania i serwisu, jak również cichsze i nie przenosi drgań na konstrukcję wieży, co występuje w przypadku tradycyjnych generatorów prądotwórczych. Dzięki temu obraz jest bardziej stabilny, więc analiza obrazu zapewnia znacznie skuteczniejszą detekcję intruza.

Zastosowanie

W wielu przypadkach mobilne wieże monitoringu są wykorzystywane do tymczasowego dozorowania obszarów bez żadnej infrastruktury, gdzie np. dopiero trwa budowa lub obiekt wymagający nadzoru będzie przechodzić różne fazy projektowe i trudno jeszcze określić ostateczny wygląd systemu nadzoru. Sprawdzają się również jako rozwiązanie bezpieczeństwa w przestrzeni publicznej podczas takich wydarzeń, jak koncerty, zawody sportowe, marsze lub duże zgromadzenia.

Wykorzystywane są też do skutecznego zabezpieczenia mienia, gdzie systemy zabezpieczeń technicznych są dopiero w planach lub w trakcie instalacji. Okazały się bardzo skutecznym narzędziem poprawy bezpieczeństwa w różnych sytuacjach. Rozwiązanie te zostały docenione przez firmy budowlane, firmy ochrony, deweloperów, policję i straż miejską.

Wyposażenie – kamery, głośniki, oświetlenie

Wieże monitoringu wizyjnego występują w licznych i różnych konfiguracjach. Każda jest wyposażona w kamery wizyjne o wysokiej rozdzielczości. Kamery te mogą być stałopozycyjne, z których kadr jest ustalany każdorazowo po postawieniu i ustabilizowaniu wieży, lub wyposażone w funkcje obrotu, pochylenia i zoomu, co pozwala na bardziej wszechstronny nadzór, a obszar obserwacji może być zmieniany zdalnie.

Należy zaznaczyć, że w przypadku kamer stałopozycyjnych dozór przestrzeni odbywa się w sposób niezmienny i ciągły, w przypadku kamer PTZ, z uwagi na możliwość zmiany kierunku obserwacji, o niezmienności nie może być mowy. Dlatego też wieże z kamerami PTZ mają na ogół na wyposażeniu czujniki ruchu dalekiego zasięgu (maks. 100 m) lub radary (zasięg do ok. 500 m) wyzwalające zmianę pozycji kamery w przypadku naruszenia strefy detekcyjnej. Podobną funkcję mogą również zapewniać kamery stałopozycyjne z analizą obrazu umożliwiającą detekcję do ok. 80 m (w zależności od ogniskowej obiektywu).

Na wysoką jakość obrazu, gwarantującą skuteczne wykrywanie, wpływa oświetlenie. Wbudowane w kamery oświetlacze podczerwieni nie zawsze gwarantują odpowiedni kontrast sceny, a ich zbytnia bliskość obiektywu powoduje nadmierne odbicia promieniowania od przelatujących insektów, drobin pyłu, kropel deszczu lub płatków śniegu. To powoduje gorsze rozpoznanie dalszego planu. Lepszym rozwiązaniem jest użycie zewnętrznych oświetlaczy, które zapewnią odpowiednie doświetlenie sceny. Użycie źródeł światła

→

Mobilne wieże monitoringu oferują wiele korzyści w porównaniu do tradycyjnych systemów kamer dozoru wizyjnego.

Zalety	Zastosowanie
Łatwy transport i szybki montaż w dowolnym miejscu.	Monitoring imprez masowych i wydarzeń specjalnych.
Możliwość dostosowania konfiguracji kamer i osprzętu do specyficznych potrzeb.	Ochrona nowo tworzonych obiektów, np. placów budów.
Możliwość rozbudowy systemu o dodatkowe wieże w miarę wzrostu potrzeb.	Nadzór nad bezpieczeństwem publicznym.
Zasilanie niezależne od sieci energetycznej.	Doraźne instalacje w rejonach zagrożonych przestępczością.
Szeroki zakres obserwacji i skuteczne monitorowanie dużych obszarów.	Doraźny dozór obiektów o znaczeniu krytycznym dla ciągłości biznesu.
Obecność wieży może zniechęcać do popełnienia czynów zabronionych.	Monitorowanie terenów dotkniętych np. katastrofą naturalną, gdzie dotychczasowa infrastruktura została zniszczona.

widzialnego zapewni wartość prewencyjną, gdyż samo użycie oświetlenia w zakresie 380–750 nm znacząco redukuje liczbę prób popełnienia czynu zabronionego.

Niestety zewnętrzne źródła światła, aby odpowiednio oświetlić teren dookoła wieży, wymagają dużej dawki energii i trzeba się z tym liczyć, dobierając rodzaj zasilania.

Wieże wyposażone w kamery termowizyjne umożliwiają lepszą detekcję intruzów i dokonywaną z dużo dalszej odległości niż jest to możliwe za pomocą kamer wizyjnych. Kamery termowizyjne lepiej sobie radzą w każdych warunkach oświetleniowych i atmosferycznych, zatem świetnie sprawdzają się w ramach dozoru perymetrycznego do dyskretnej obserwacji. Ważne jest też to, że zużywają mniej energii.

Omawiając wyposażenie wieży, trudno pominąć kwestię audio. Głośniki IP są idealnym dodatkiem do systemów dozoru wizyjnego, umożliwiają bowiem szybką interwencję operatora stacji monitorowania alarmów i nawiązanie komunikacji głosowej z osobami znajdującymi się w monitorowanej lokalizacji.

Komunikacja

Zdalny nadzór i sterowanie wieżą odbywa się najczęściej za pomocą łącza bezprzewodowego. Na wyposażeniu każdej wieży są router LTE/5G oraz podłączone do niego anteny zewnętrzne. W zależności od przyjętego rozwiązania transmisja jest wykonywana w ramach wewnętrznego APN operatora (wydzielona i odseparowana sieć transmisji danych) albo w sposób otwarty (z wykorzystaniem technik szyfrowania) przez Internet. W miejscach o słabym pokryciu sygnału można stosować kilka rodzajów łączy (kart), co pozwoli zwiększyć szerokość kanału transmisyjnego.

Cena zależna od możliwości

Na cenę mobilnej wieży monitoringu wpływa wiele czynników. Im większa i lepiej wyposażona wieża, tym wyższa cena. W wielu przypadkach sama konstrukcja wieży (bez wyposażenia) może stanowić połowę kosztów inwestycji. Oczywiście cena zależy od wyposażenia oraz przyjętych kompromisów. Koszt wersji bez wyposażenia zaczyna się od ok. 5 tys. euro. Wersja z panelami to wydatek rzędu 8 tys. euro. Z wydatkiem powyżej 15 tys. euro trzeba się liczyć, jeśli na wyposażeniu będą kamery i oświetlenie.

Jedną z zalet wież monitoringu jest to, że faktycznie można je stosować doraźnie, dlatego na rynku dostępne są usługi wynajmu takich urządzeń. Koszt wypożyczenia zależy od okresu wynajmu oraz wyposażenia wieży i waha się od 200 do 500 zł netto/dzień ●

Przykłady mobilnych wież monitoringu prezentujemy na kolejnych stronach.

Linc
Polska Sp. z o.o.

TOWER®

TAM GDZIE STANDARDOWE ZABEZPIECZENIA SIĘ
NIE SPRAWDZAJĄ TAM JESTEŚMY MY.

Mobilne rozwiązania do ochrony

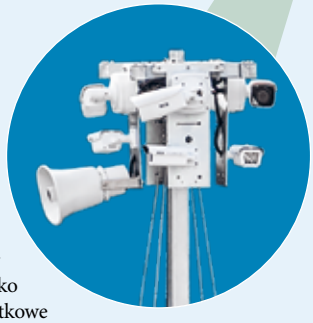
- WŁASNE ZASILANIE
- MULTISPEKTRALNOŚĆ
- NIEZALEŻNOŚĆ
- OSZCZĘDNOŚĆ
- WYTRZYMAŁOŚĆ
- BEZPIECZEŃSTWO DOSTĘPU

www.linc.pl

BCS

Mobilne wieże do monitoringu wizyjnego BCS Mobilcam

BCS oferuje rozwiązania do monitoringu mobilnego w postaci przenośnych platform na podwoziu kołowym, ze składanymi masztami stanowiącymi podstawę do montażu zróżnicowanego typu urządzeń CCTV.



Do dyspozycji są dwa typy podwozia – jeden z wieżą połączoną na stałe oraz drugi, w którym wieża i przyczepa stanowią dwa oddzielne elementy. Dopuszczalna masa całkowita przyczepy zespolonej wynosi 750 kg, rozłącznej – 1200 kg. W drugim przypadku pozwala to na obsługę kilku wież za pomocą jednej przyczepy, która jest wyposażona w podnośnik hydrauliczny umożliwiający łatwy załadunek i rozładunek oraz w elementy zabezpieczające zapewniające bezpieczny transport ładunku. Samo rozstawienie wieży niezależnie od typu podwozia i przygotowanie do pracy nie powinno zająć jednej osobie więcej niż 30 min.
Najważniejszym elementem rozwiązania jest „skrzynia" zawierająca wszystkie podzespoły: 6-metrowy maszt wysuwany mechanicznie za pomocą wyciągarki ręcznej, obudowę z układami sterującymi oraz akumulatory podtrzymujące. Skrzynia pełni też funkcję zabezpieczającą przed dostępem nieupoważnionych osób.
Na szczycie masztu mogą zostać zamontowane dowolne urządzenia CCTV, jednak dla ułatwienia instalacji proponujemy klientom gotowe zestawy z produktami BCS Line lub BCS View. Najczęściej są to rejestrator oraz 4 kamery, co zapewnia obserwację wokół wieży w zakresie 360°. Jako wyposażenie dodatkowe zastosowano 4 promienniki IR. W obudowie umieszczono układ zasilania, switch łączący kamery z rejestratorem i router 5G zapewniający zdalny dostęp do systemu, a także termostat oraz grzałkę i wentylator, co pozwala na pracę w zmiennych warunkach atmosferycznych. Znajduje się tu również moduł ładowania akumulatorów oraz dwa akumulatory 220 Ah, które zapewniają ciągłość pracy systemu w razie braku dostępu do zewnętrznych źródeł zasilania przez ok. 5 dni. Czas ten można wydłużyć, doposażając wieżę w rozkładane panele fotowoltaiczne.

Więcej na www.bcs.pl

JANEX INTERNATIONAL

Innowacyjna wieża monitorująca Janex International

Mobilna wieża monitorująca Janex International idealnie wpisuje się w rosnące potrzeby rynku w zakresie monitoringu wizyjnego. Wyposażona w zaawansowane technologie umożliwia nadzór różnorodnych miejsc, począwszy od placów budowy, przez parkingi, imprezy plenerowe, skończywszy na terenach o dużej przestępczości czy farmach fotowoltaicznych.

Szeroki wybór opcji zasilania rozdzielnic teletechnicznych i zaawansowanych urządzeń monitorujących, takich jak kamery wysokiej rozdzielczości, sprawia, że wieża monitorująca Janex International to inwestycja, która dostosowuje się do indywidualnych potrzeb klientów, zapewniając im kompleksowe rozwiązanie w zakresie bezpieczeństwa.
Wieża mobilna została zaprojektowana do zapewnienia niezawodnego zasilania w każdych warunkach. Pierwotnie jest zasilana z sieci elektrycznej, jednak w przypadku awarii automatycznie przełącza się na alternatywne źródła energii, np. akumulatory, panele fotowoltaiczne lub ogniwa paliwowe. Dla uzyskania maksymalnej mobilności wieża została zabudowana na lekkiej przyczepce, którą można transportować pojazdem (wymagane uprawnienia kat. B). Wieża mobilna Janex International to rozwiązanie innowacyjne, które charakteryzuje się szeregiem unikatowych cech zapewniających jej wszechstronność, stabilność i funkcjonalność:

- wieża wolnostojąca lub zabudowana na lekkiej przyczepce o dopuszczalnej masie całkowitej (DMC) do 750 kg,
- stabilna i bezpieczna konstrukcja stalowa,
- wysuwane cztery podpory stabilizujące konstrukcję,
- drzwi z trzech stron umożliwiające pełny dostęp do wieży,
- zamykany dach,
- profesjonalny mocny maszt podnoszony za pomocą wyciągarki ręcznej lub elektrycznej,
- wysokość wieży po wysunięciu masztu zabudowanego na przyczepce: 7 m,
- uniwersalny stelaż na szczycie masztu przeznaczony do montażu urządzeń,
- rama montażowa dla trzech paneli fotowoltaicznych.

Janex International jest polskim producentem, co dodatkowo potwierdza wysoką jakość i innowacyjność oferowanych produktów.

Więcej na www.janexint.com.pl

Agencja Ochrony LION

Lion Tower – wieża mobilna

Obecnie na rynku dostępne są różne wieże, maszty i inne konstrukcje, których skuteczność bywa mocno dyskusyjna.

Dlatego w rozwiązaniach Agencji ochrony osób i mienia LION bardzo restrykcyjnie przestrzegamy pewnych zasad, dzięki czemu nasi klienci otrzymują produkt, który niezależnie od wersji sprzętowej jest dopracowany w określonym standardzie. Wieże Lion Tower już od 5 lat działają na rynku security w Polsce, a od ostatniego roku również za granicą.

Lion Tower charakteryzują:

Standaryzacja stosowanego sprzętu, oprogramowania, procedur.

Skuteczność. Nie wystarcza nam analityka, którą można uruchomić w większości kamer zamontowanych na masztach. Nasze wieże są wyposażone w nadajniki wideo Aibox japońskiej firmy Ganz, które zapewniają skuteczność w wykrywaniu intruzów na znacznie większych odległościach. Aibox umożliwia bardzo sprawne przesyłanie materiału wideo, który trafia do operatora stacji monitorowania, umożliwiając szybką ocenę sytuacji i podjęcie właściwych działań.

Zasilanie. Nasze autonomiczne wieże zaopatrzone są w bardzo zaawansowane agregaty, które zapewniają ciągłość działania nawet w najgorszych warunkach pracy. Są zasilane paliwem alternatywnym, które wymaga uzupełnienia tylko raz w miesiącu. Lion Tower nie wymaga doładowywania akumulatorów agregatem, co dla klienta jest opłacalne kosztowo i czasowo, bo nie trzeba wzywać serwisantów. Porównując koszty może się okazać, że nasza autonomiczna wieża, pomimo wyższej ceny, daje większy zwrot z inwestycji. W naszej ofercie są również systemy zasilane z sieci 230 V oraz z paneli fotowoltaicznych. Jednak w naszej szerokości geograficznej w okresie jesienno-zimowym same panele nie wystarczą, dlatego rozwiązanie z agregatem wspomagającym gwarantuje ciągłość pracy systemów.

Serwis. Nasi serwisanci podejmują działania zdalne, a jeśli to nie wystarczy, jadą na miejsce w celu usunięcia usterki.

Logistyka. Dostarczenie wież można zaplanować. Jednak w wielu przypadkach, kiedy klient potrzebuje natychmiastowej pomocy, działamy i dostarczamy systemy Lion Tower nawet tego samego dnia.

Więcej na https://lion-ochrona.pl

SECURITAS POLSKA

Securitas MobileCam – mobilna platforma monitoringu

Panele fotowoltaiczne lub agregat, dzięki którym urządzenie może funkcjonować do trzech tygodni na jednym zbiorniku paliwa, zapewniają funkcjonalność i łatwość obsługi. Ma to kluczowe znaczenie w miejscach bez dostępu do stałego źródła zasilania, takich jak infrastruktura krytyczna, tereny wyrębu lasów, hale czy place budowy. Samodzielności platformy w miejscach bez infrastruktury dopełnia łączność oparta na sieci LTE.

Inteligentna analiza obrazu i system termowizyjny

Zastosowanie w MobileCam kamer z inteligentną analizą obrazu skutecznie eliminuje alarmy spowodowane np. przez poruszające się drzewa, deszcz i śnieg lub pojawienie się na terenie monitorowanym obiektów niestanowiących zagrożenia. Wykorzystanie w urządzeniu kamer termowizyjnych gwarantuje skuteczność monitoringu w trudnych warunkach atmosferycznych (np. duże zamglenie, obszary niedoświetlone).

Platforma MobileCam jest wyposażona w technologie pozwalające na stałą rejestrację obrazu w wysokiej jakości w zakresie 360°. Wykrycie zagrożenia wzbudza alarm dźwiękowy i świetlny widoczny dla intruza.

Securitas MobileCam

Efektywny, ekonomiczny, mobilny i w pełni wyposażony system ochrony:

- wykorzystywany w trudnych warunkach terenowych, w miejscach bez stałego źródła zasilania,
- system kamer, oświetlaczy światła białego i głośników montowany na maszcie na wysokości 6 m,
- autonomiczny system zasilania,
- niezawodność wykrycia ruchu dzięki inteligentnej analizie obrazu z kamer termowizyjnych,
- stała rejestracja obrazu w wysokiej jakości w zakresie 360°,
- dowolny czas wynajęcia platformy,
- dostęp w czasie rzeczywistym do obrazów i nagrań rejestrowanych przez www i za pomocą dowolnych urządzeń końcowych.

Więcej na www.securitas.pl

TAURUS OCHRONA

vPATROL Tower®

Mobilne wieże monitorujące vPATROL Tower® firmy Taurus Ochrona redefiniują standardy w dziedzinie monitoringu wizyjnego.

Ich wyjątkowym atutem jest innowacyjny mobilny system zasilania składający się z akumulatorów, generatorów, paneli słonecznych i systemu wodorowego. To kompleksowe zautomatyzowane rozwiązanie nie tylko w kontekście zasilania, lecz także ochrony środowiska. Zapewnia niezależność energetyczną przez cały rok.

Kamery o wysokiej rozdzielczości, umieszczone na podnoszonym maszcie, są uzbrojone w zaawansowaną analitykę obrazu opartą na sztucznej inteligencji. W czasie rzeczywistym klasyfikują różnorodne zachowania, takie jak wtargnięcie, przekroczenie linii, upadek czy nieprzestrzeganie przepisów BHP. Zarejestrowane zdarzenia są przesyłane do Zintegrowanego Centrum Monitorowania Alarmów Grupy Taurus Ochrona, jednego z najnowocześniejszych w Polsce, znajdującego się w Data Center, gdzie usługi oparte na technologii chmurowej oferowane są na poziomie bezpieczeństwa *Tier III of facility.*
vPATROL Tower® to kompleksowe rozwiązanie spełniające najwyższe standardy bezpieczeństwa.

Zalety
- Ochrona całodobowa
- Natychmiastowa reakcja na zagrożenie
- Analiza obrazu w czasie rzeczywistym
- Duży promień monitoringu, do 200 m
- Szybkie uruchomienie usługi w ciągu 24 h
- Stały abonament miesięczny
- Nawet 70% oszczędności w porównaniu z ochroną fizyczną
- Aplikacja mobilna dla klientów – zdalny podgląd obrazów z kamer w obiekcie
- Możliwe do uzyskania filmy reklamowe z procesu budowy
- Zapewnienie bezpieczeństwa fizycznego i BHP
- Redundantne systemy komunikacji
- Zabezpieczenie przed cyberzagrożeniami

Wyposażenie
- Maszt o wysokości do 7 m
- Kamery IP uzbrojone w nowoczesną analitykę obrazu
- Kamery obrotowe 360° i termowizyjne
- Oświetlenie
- Tuba głośnikowa
- Programowalne czujniki ochrony perymetrycznej
- Czujki PIR
- System GPS i GPRS
- Radary (opcjonalnie)
- Szczelna skrzynia sterownicza
- Dodatkowe podpory i odciągi zwiększające stabilność

Więcej na www.vpatroltower.pl

VCS

iTower® Tripel Solar – autonomiczna wieża, która chroni w każdych warunkach

W erze rozwijających się technologii i świadomości ekologicznej integracja alternatywnych źródeł energii stała się kluczowym elementem wpływającym na komfort użytkowania.

Ten przełomowy koncept opiera się na stworzeniu samoobsługującego się systemu, zdolnego do pracy autonomicznej. Połączenie paneli słonecznych i ogniw paliwowych firmy SFC ENERGY w wieżach iTower® rozwiązuje problemy z zasilaniem, oferując produkt przyjazny dla środowiska.
Można zapomnieć o czasochłonnym dostosowywaniu infrastruktury potrzebnej do uruchomienia wieży monitorującej i kilometrach kabli, o które potykają się ludzie. Wieża iTower® Tripel Solar będzie działała skutecznie mimo braku dostępu do źródła prądu stałego, a do jej włączenia wystarczy tylko jedna osoba.

Wykorzystanie energii słonecznej i ogniw paliwowych EFOY
Trzy zintegrowane panele słoneczne pełnią funkcję głównego źródła zasilania, wykorzystując energię słoneczną, natomiast ogniwa paliwowe działają jako zapasowe źródło energii, zapewniając nieprzerwaną pracę nawet w okresach niewielkiego nasłonecznienia lub złej pogody. Starannie zaprojektowana konstrukcja stelaża, w którym umieszczono panele, pozwala na ustawienie odpowiedniego kąta nachylenia, by zmaksymalizować ilość dostarczanej energii słonecznej. Możliwość podłączenia kilku kartridżów z metanolem do jednego urządzenia EFOY sprawia, że nie trzeba martwić się o codzienne uzupełnianie paliwa. System może działać przez długi czas z minimalną interwencją ludzi. W przeciwieństwie do generatorów diesla jest przyjazny dla środowiska.

Rozwiązanie potwierdzone przez klientów z całego świata
Z dumą dostarczamy nasze wieże do klientów z całego świata, którzy zaufali naszej jakości i profesjonalnemu podejściu. Jesteśmy także oficjalnym dystrybutorem firmy SFC ENERGY.

Wieża i-Tower® Tripel Solar pojawi się na targach Securex 23-25.04.2024 w Poznaniu na stoisku Linc Polska nr 15, sektor C, pawilon 6.
Więcej na www.vcs.pl

Wieże monitorujące vPATROL Tower® – mobilny i ekonomiczny system inteligentnej ochrony

Usługa zdalnej kontroli bezpieczeństwa, oferowana przez mobilne wieże monitorujące vPATROL Tower® Grupy Taurus Ochrona, stanowi ekonomiczną alternatywę dostosowaną do nowoczesnych standardów zabezpieczeń. To innowacyjne rozwiązanie pozwala klientom osiągnąć oszczędności na poziomie do 70% w porównaniu do ochrony fizycznej. Skuteczność i praktyczne zastosowanie mobilnych wież potwierdza rola, jaką odgrywają od 2019 r. w zabezpieczaniu farm OZE na terenie całej Polski.

Grupa Taurus Ochrona jest wiodącą firmą w branży zabezpieczeń technicznych oraz ochrony osób i mienia z 33-letnim doświadczeniem. Nieprzerwanie doskonali procesy zapewniania bezpieczeństwa, wprowadzając innowacyjne rozwiązania. Jednym z nich jest vPATROL Tower® – inteligentny system monitoringu wizyjnego oparty na sztucznej inteligencji w mobilnych wieżach monitorujących. Autonomia tego rozwiązania gwarantuje efektywną i niezawodną ochronę 24 h/7 różnych obiektów, eliminując konieczność instalacji kamer i systemów alarmowych niezależnie od lokalizacji. Łatwość transportu, błyskawiczny montaż, niezależność energetyczna, stabilność konstrukcji, odporność na zmienne warunki atmosferyczne oraz analiza obrazu w czasie rzeczywistym – to kluczowe cechy tej usługi.

Zastosowania

Wieże są wykorzystywane w różnych obszarach: place budowy, składowiska, osiedla mieszkaniowe, targowiska, infrastruktura portowa, powierzchnie magazynowe, hale produkcyjne, imprezy masowe, ale też inne tereny otwarte, np. parki i lasy, parkingi oraz przestrzenie wymagające szczególnej ochrony, włącznie z infrastrukturą krytyczną.

Wyposażenie

Na podnoszonym maszcie, osiągającym wysokość 7 m, zamontowane są kamery obrotowe 360° i termowizyjne o wysokiej rozdzielczości, uzbrojone w nowoczesną analitykę obrazu opartą na sztucznej inteligencji, która w czasie rzeczywistym klasyfikuje różnorodne zachowania, takie jak wtargnięcie na teren, przekroczenie linii czy nieprzestrzeganie przepisów BHP, np. brak kasku ochronnego. Na maszcie umieszczone jest oświetlenie – LED lub halogenowe. System komunikacji bezprzewodowej zapewnia zdalne sterowanie wieżą i przesyłanie obrazu do centrum monitorowania alarmów, umożliwiając skuteczne monitorowanie oraz reakcję na zagrożenia.

Wyróżniającym się elementem wież vPATROL Tower® jest ekologiczny system zasilania zapewniający niezależność energetyczną przez cały rok. Zasilanie systemu oparto na akumulatorach, generatorze, panelach słonecznych i systemie wodorowym. Ogniwa paliwowe stosowane w wieżach vPATROL Tower® automatycznie ładują baterie akumulatorów, nie produkując żadnych związków chemicznych mogących szkodzić środowisku. Dzięki temu wieże mają zapas ekologicznej energii, spełniający nawet najbardziej rygorystyczne wymagania energetyczne.

W zależności od potrzeb wieże monitorujące mogą być wyposażone w dodatkowe elementy, takie jak tuba głośnikowa umożliwiająca emitowanie komunikatów ostrzegawczych w czasie rzeczywistym, radary, czujki PIR o dalekim zasięgu reagujące na najmniejsze zmiany dzięki wykorzystaniu promieniowania podczerwonego oraz czujniki temperatury do wykrywania zagrożeń pożarem.

Korzyści

Wieże vPATROL Tower® generują oszczędności do 70% w stosunku do tradycyjnych metod ochrony. Oparte na najnowszych technologiach umożliwiają dostosowanie ochrony do indywidualnych potrzeb oraz uzyskanie filmów reklamowych z procesu budowy dla inwestora, dewelopera bądź firmy budowlanej. To innowacyjny system ochrony, przyjazny dla środowiska naturalnego, łączący mobilność, zaawansowane technologie i niezależność energetyczną. ●

Taurus Ochrona
ul. Lubicka 53
87-100 Toruń
https://vpatroltower.pl/

IFTER EQU – kompleksowe zarządzanie bezpieczeństwem obiektów biurowych

Firma IFTER od blisko 25 lat dostarcza rozwiązania do systemów bezpieczeństwa. Głównymi produktami firmy są system do integracji i wizualizacji IFTER EQU2 oraz kontrola dostępu EQU ACC. Oferując duże możliwości, znakomicie sprawdzają się w obiektach wymagających rozwiązań najwyższej jakości.
Jerzy Taczalski

Jednym z obiektów, w których wdrożono produkty IFTER, jest siedziba Urzędu Marszałkowskiego Województwa Zachodniopomorskiego w Szczecinie. Zastosowano tam kompleksowe rozwiązania w zakresie systemów integrujących, zarządzających i wizualizujących, a także kontroli dostępu (SKD) rozbudowanej o elementy rejestracji czasu pracy (RCP). Mimo tak szerokiego zakresu zarządzanie systemem jest proste i zautomatyzowane dzięki jednej bazie danych dla wszystkich podsystemów. Ochrona monitoruje system dwóch budynków w dwóch oddzielnych centrach monitorowania obsługiwanych przez dwa serwery integracyjne.

Wizualizacja systemów bezpieczeństwa

Wizualizacja i integracja obejmują system sygnalizacji pożarowej, kontrolę dostępu, sygnalizację włamania i napadu oraz telewizję dozorową. Wizualizacja jest intuicyjna, z mechanizmami prowadzenia od planu ogólnego do szczegółowego, a w przypadkach ochrony obszarów wysokiego ryzyka z automatyczną prezentacją miejsca zagrożonego. Wszystkie integrowane systemy są prezentowane na wspólnych mapach architektonicznych obiektu, dzięki czemu w przypadku np. alarmu pożarowego operator może łatwo zweryfikować miejsce zdarzenia, klikając ikony kamer znajdujących się w pobliżu pobudzonego czujnika. Prezentowany obraz z kamer dodatkowo jest wyświetlany automatycznie po przyjściu alarmu wraz z nagraniem archiwalnym na 10 s przed powstaniem zagrożenia. Dzięki wbudowanej obsłudze kontroli dostępu i obrazom z kamer operator może na bieżąco śledzić przemieszczanie się osób i weryfikować ich uprawnienia. Widzi również, ile osób znajduje się na poszczególnych kondygnacjach.

Wysoka intuicyjność IFTER EQU2 umożliwia skuteczne nadzorowanie ponad 5 tys. czujników i przejść. W każdej chwili system można rozbudować o możliwość monitorowania wszystkich urządzeń aktywnych sieci szkieletowej i kontrolę parametrów środowiskowych serwerowni, takich jak zasilanie, temperatura i wilgotność. Poza standardowymi funkcjami IFTER EQU2 użytkownik może opracować własne, korzystając z języka skryptowego LUA.

Kontrola dostępu

W budynkach zajmowanych przez urząd marszałkowski jest 800 przejść objętych kontrolą dostępu IFTER EQU ACC. Każdy z kontrolerów jest połączony z systemem nadzorczym poprzez sieć Ethernet. Dzięki takiemu rozwiązaniu rozbudowa o kolejne przejścia jest prosta, wystarczy montaż czytników i czujników oraz kontrolera podpinanego do najbliższego switcha. Każdy z kontrolerów, zgodnie z normą PN-EN-60839, jest montowany w wytrzymałej obudowie wyposażonej w zasilacz buforowy wraz z akumulatorem podtrzymującym działanie SKD na danym przejściu. Dzięki temu nawet podczas braku zasilania obiekt jest w pełni chroniony i monitorowany.

Skaner termowizyjny dający obraz 360°

W większości miejsc urzędu zamontowano czytniki z frontem wykonanym ze szkła i grafiką dostosowaną do wystroju pomieszczeń wraz z logo inwestora. W tym przypadku zostały wykonane według jednego wzoru, jest jednak możliwość przygotowania grafiki dla każdych drzwi indywidualnie, np. z numerem pomieszczenia. Dzięki rozbudowanym funkcjonalnościom IFTER EQU ACC kontrola dostępu została dostosowana do indywidualnych potrzeb każdego przejścia. Przykładowo, aby umożliwić wejście interesantom, drzwi wejściowe są automatycznie odblokowywane w godzinach ich przyjmowania.

Wejścia do niektórych pomieszczeń są sterowane tak, że pierwsze zbliżenie karty do czytnika zezwala na swobodne przejście, kolejne zbliżenie przywraca działanie SKD. Pomieszczenia o najbardziej restrykcyjnych obostrzeniach zabezpieczane są dwuskładnikowo: kartą i PIN-em lub zbliżeniem kart dwóch osób. Ochrona korzysta również z kart modyfikujących pracę przejścia, np. stałe otwarcie czy blokada, co umożliwia szybką reakcję.

W każdej windzie zamontowany jest czytnik. Po zbliżeniu identyfikatora do czytnika odblokowywane są kondygnacje dostępne dla danej osoby. Do dyspozycji jest również kontroler globalnego ***anti-passback,*** który pozwala na ponowne wejście na kartę w momencie, gdy wyjście nie zostało zarejestrowane.

Rejestracja czasu pracy

System kontroli dostępu pozwolił jednocześnie na uruchomienie ewidencji czasu pracy, w tym rejestr wyjść służbowych oraz innych, które można swobodnie definiować, co m.in. znacząco ułatwia pracę księgowości. Systemem rejestracji czasu pracy (RCP) zostały objęte obiekty znajdujące się nie tylko w Szczecinie, ale także zamiejscowe, dlatego w przypadku oddelegowania pracownika urzędu do oddziału nie ma problemu z rozliczeniem czasu pracy. Moduł RCP pozwala na definiowanie harmonogramów pracy pracowników oraz rozliczanie ich z uwzględnieniem danych zbieranych zarówno z terminali RCP, jak i standardowych przejść z punktami kontroli dostępu. Liczne raporty i zestawienia analityczne usprawniają obliczanie przepracowanych godzin.

Oprogramowanie do zarządzania SKD

Na szczególną uwagę zasługuje aplikacja opracowana na system Windows służąca do konfigurowania i zarządzania kontrolą dostępu. Jej rozbudowane możliwości pozwalają na zarządzanie nawet ośmiuset przejściami. Do głównych zalet programu należy grupowanie urządzeń (kontrolerów i przejść) w zależności od miejsca ich zamontowania. Kolejnym ułatwieniem jest możliwość tworzenia grup użytkowników odpowiadających np. działom firmy. Każda grupa może mieć przypisane własne reguły dotyczące m.in. terminu ważności karty,

→

dostępu do pomieszczeń itp., co w przypadku dużych zakładów pracy znacząco usprawnia zarządzanie danymi i dostępem.

Nie ma ograniczeń w tworzeniu liczby grup dostępowych, które są przypisywane do kart. Każdej grupie jest przyznawany harmonogram oraz wybrane przejścia, zarówno pojedyncze, jak i wszystkie wejścia do budynku. Przy dużej liczbie przejść i osób wykorzystuje się grupy organizacyjne mające na celu odzwierciedlenie ich uprawnień wynikających ze struktury organizacyjnej firmy. Dla danych grup organizacyjnych można ustalić, jakie grupy dostępu można przypisać osobie, jaka ma być długość użytkowania karty itp. Listy użytkowników są automatycznie sortowane wg grup organizacyjnych, które mogą mieć strukturę piramidy. Ułatwia to zarządzanie dużą liczbą osób.

Do jednej osoby można przypisać wiele kart, które będą reprezentowały np. różne technologie transmisji danych (Unique, Mifare DESFire, UHF). Zmiana karty nie powoduje braku ciągłości zdarzeń dla danej osoby, dzięki temu można filtrować, jakie karty zostały wydawane, ale też jak dana osoba porusza się w budynku. Mechanizm ten pozwala również na wydanie jednodniowego duplikatu karty wtedy, gdy pracownik ją zgubi lub jej zapomni. W przypadku zarejestrowania, że została użyta oryginalna karta, duplikat zostanie zablokowany. Do konta danej osoby można również dodać informacje o samochodzie, wówczas będzie on wpuszczany na parking po automatycznym rozpoznaniu tablic rejestracyjnych lub odczycie karty UHF.

W celu ułatwienia zarządzania użytkownikami SKD dane można importować automatycznie z systemu kadrowego lub przez synchronizację z usług katalogowych korzystających z protokołu LDAP. Do ułatwień można również zaliczyć automatyczne filtrowanie kart względem ważności, daty usunięcia, ważności badań/szkoleń. Jeżeli w przejściu jest zamontowany terminal, to może on wyświetlać te informacje. Uproszczeniu obsługi systemu służy także moduł personalizacji kart, który automatycznie pobiera zdjęcie z aparatu fotograficznego, wkleja go do wcześniej przygotowanego szablonu, dodając dane z systemu: imię i nazwisko, grafikę karty.

W przypadku ewakuacji ochrona może odblokować wszystkie przejścia ewakuacyjne. Pracownicy zbierają się w punkcie ewakuacyjnym wskazanym przez służby ochrony. Dzięki czytnikom bezprzewodowym ich karty są automatycznie odczytywane, więc liczba osób, które pozostały w budynku, jest na bieżąco monitorowana. W każdej chwili jest możliwość wydrukowania listy osób w poszczególnych obszarach i przekazania jej strażakom wraz z planami architektonicznymi z naniesionymi czujkami w alarmie i listą alarmów z danego obszaru w celu przedstawienia kierunku przemieszczania się zagrożenia.

Grupy sterowań pozwalają na grupowe standardowe otwieranie przejść, otwieranie w trybie ewakuacji, blokowanie ich oraz włączanie lub wyłączanie *anti-passback*. Sterowanie odbywa się z poziomu aplikacji po wyborze odpowiedniej grupy sterowań i czynności, jaką chce wykonać operator.

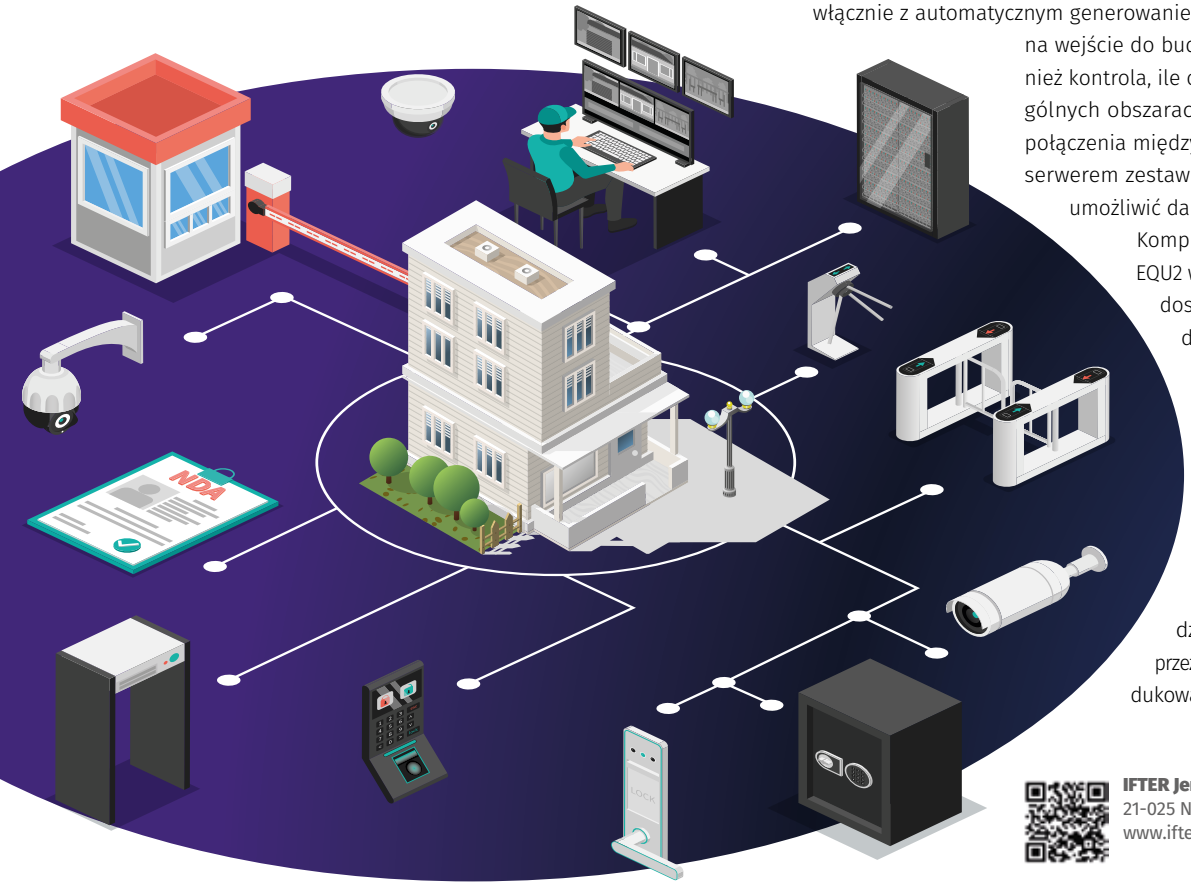
Aplikacje Web

Za pomocą aplikacji Web można dodawać pracowników i zarządzać nimi. W urzędzie wykorzystywanych jest 35 dostępów do systemu poprzez przeglądarkę, z których korzystają osoby wprowadzające informacje o delegacjach służbowych oraz przygotowują liczne raporty dotyczące obecności, spóźnień itp.

Dla wybranego profilu można zdefiniować najbliższy czytnik, który w chwili zbliżenia karty wprowadzi niezbędne dane do aplikacji. Istotną cechą jest bardzo skuteczne zarządzanie dostępem do danych, pozwalające na ograniczanie dostępu tylko osobom z uprawnieniami.

Dzięki aplikacji działającej online możliwa jest też awizacja gości, włącznie z automatycznym generowaniem kodu QR pozwalającym na wejście do budynku. Dostępna jest również kontrola, ile osób przebywa w poszczególnych obszarach. W przypadku zerwania połączenia między urządzeniem a głównym serwerem zestawienie jest zamrażane, aby umożliwić dalszą prezentację.

Kompleksowe rozwiązanie IFTER EQU2 wraz z wbudowaną kontrolą dostępu EQU ACC są zaliczane do najbardziej rozbudowanych systemów bezpieczeństwa dostępnych na polskim rynku. Oferują wysoką elastyczność intuicyjność i funkcjonalność, zaspokajając stale rosnące potrzeby klientów. Oprogramowanie i urządzenia zostały opracowane przez inżynierów firmy IFTER i produkowane w całości w Polsce. ●



IFTER Jerzy Taczalski
21-025 Niemce, Wola Niemiecka 78c
www.ifter.com.pl

Drony i systemy antydronowe do ochrony perymetrycznej

Obiekty strategiczne, takie jak budynki rządowe, lotniska czy zakłady przemysłowe, wymagają szczególnego zabezpieczenia, co wynika z charakteru prowadzonej przez nie działalności. Bez właściwej ochrony mogą stać się łatwym celem ataku, a ich uszkodzenie w konsekwencji może prowadzić do realnego zagrożenia zdrowia i życia ludzi.

Katarzyna Niebrzydowska

Aby zabezpieczenie było skuteczne, powinno uwzględniać specyfikę danego obiektu. Kompleksowym systemem jest ochrona perymetryczna w postaci autonomicznych dronów i systemów antydronowych jako najnowocześniejsza technologia w zabezpieczeniu przestrzeni powietrznej.

Witamy w marce bezpieczeństwa...

Firma Transactor Security oferuje kompleksowy system nadzoru, detekcji i przechwytywania, w którego skład wchodzi autonomiczny dron w stacji dokującej Agent Bee, urządzenie do detekcji Companion System oraz urządzenie do detekcji i przejęcia RF Cyber.

Nowy zawód: dron ochroniarz

Technologia autonomicznego drona Agent Bee w stacji dokującej jest jednoznaczną odpowiedzią na szybką i elastyczną reakcją w sytuacji zagrożenia. Lekki i kompaktowy dron w stacji dokującej pozwala na autonomiczną pracę w niekorzystnych warunkach z czasem reakcji w zaledwie 5 s. Łączność oraz transfer danych za pomocą Wi-Fi, Ethernet lub LTE pozwala na dostosowanie konfiguracji do potrzeb. Oprócz identyfikacji źródła zagrożenia może także rejestrować pościg na wcześniej zdefiniowanym obszarze. Agent Bee nie wymaga szczególnej adaptacji czy zabudowy. Wykorzystując zaawansowane oprogramowanie, dron umożliwia szybką weryfikację alarmu, planowe patrolowanie wrażliwych punktów, a także kontrolę zewnętrznego zabezpieczenia systemu perymetrycznego w kontekście naruszeń.

Systemy antydronowe jako ochrona z powietrza

Świadome podejście do bezpieczeństwa chronionego obiektu powinno definiować systemy do detekcji i przechwytywania dronów, zwłaszcza w dobie nieuprawnionych wtargnięć i ataków. Drony są obecnie jednym z najczęstszych zagrożeń technologicznych z powietrza.

Skutecznym rozwiązaniem zapobiegającym naruszeniom przestrzeni powietrznej nad obiektem przez wrogie drony jest połączenie technologii wykrywania RF oraz technologii przechwytywania dronów. Dla uzyskania synergii właściwym rozwiązaniem jest połączenie urządzeń mobilnych, które mogą być zaimplementowane na pojazdach, w śmigłowcach z urządzeniami stacjonarnymi i zarządzanie nimi za pomocą zintegrowanej platformy. Wszystkie powyższe cechy spełniają rozwiązania w ofercie Transactor Security.

Urządzenie do detekcji Companion System w formie przenośnej walizki wykrywa drony w zasięgu 2 km i może pracować w trudnych warunkach atmosferycznych. Dzięki wbudowanej karcie LTE można nim zarządzać z dowolnego miejsca na świecie, a sterować za pomocą aplikacji zainstalowanej na smartfonie czy tablecie.

Jako stacjonarne, a zarazem mobilne rozwiązanie do detekcji i przechwytywania tzw. *spoothingu* Transactor Security proponuje urządzenie o nazwie RF Cyber. Wysoka wydajność z pełnym pokryciem 360°, duży zasięg wykrywania i przejęcia, a także solidna budowa wg norm wojskowych oraz możliwość zarządzania z dowolnego miejsca stanowi taktyczne rozwiązanie do całodobowej ochrony obiektu. Bardzo ważne jest to, że powyższe urządzenia są zarządzane za pomocą indywidualnego oprogramowania, tworząc spójny system zarządzania.

Oferta Transactor Security zapewnia skuteczną i kompleksową ochronę obiektu, począwszy od konsultacji i zaprojektowania systemu, przez wdrożenie wraz ze szkoleniem, skończywszy na serwisie i wsparciu technicznym. ●

Transactor Security
ul. Trakt Lubelski 257A
04-667 Warszawa
www.transactor-security.pl

Transformacja usług bezpieczeństwa i ewolucja roli pracownika ochrony fizycznej

W ostatnich latach obserwujemy dynamiczne zmiany w życiu ludzi, społeczeństw i państw. Jednym z istotnych aspektów tych przemian są kwestie związane z bezpieczeństwem. W tym obszarze branża ochrony osób i mienia odgrywa kluczową rolę.
Łukasz Koch

Jeszcze 25 lat temu usługi ochrony bazowały głównie na dużych zespołach pracowników ochrony, których zadaniem było zapobieganie niepożądanym incydentom oraz ochrona mienia klienta. Procedury i raporty były wówczas opracowywane głównie w formie papierowej.

Obecnie, w obliczu zmieniających się trendów oraz oczekiwań klientów, coraz częściej mówimy o kompleksowych systemach ochrony łączących różne elementy: zespoły pracowników ochrony, procedury operacyjne, systemy informatyczne, monitoring wizyjny oraz systemy zabezpieczeń technicznych. W dużych organizacjach coraz bardziej widoczna staje się automatyzacja procesów, digitalizacja dokumentacji oraz zastosowanie systemów informatycznych wspomagających zarządzanie bezpieczeństwem. Tego rodzaju systemy są dostosowywane do potrzeb obsługiwanej firmy oraz jej budżetu, a także skutecznie zabezpieczają jej mienie przed różnymi rodzajami ryzyka. Ponadto coraz częściej są one ściśle zintegrowane z procesami wewnętrznymi klienta, obejmując nie tylko identyfikację i zabezpieczenie kluczowych obszarów, ale także koordynację pracy zewnętrznych serwisów, szkolenia pracowników, zapewnienie bezpieczeństwa pożarowego, obsługę recepcji, zarządzanie dostępem itp.

Wraz z tymi zmianami ewoluowała również rola pracowników ochrony fizycznej. W początkowym okresie funkcjonowania branży istotne były wizerunkowe oddziaływanie pracownika ochrony oraz jego sprawność fizyczna. Miernikiem skuteczności ochrony były przede wszystkim zespół pracowników – im większy, tym lepiej – oraz jego widoczna obecność. Na przykład w dużych obiektach przemysłowych i handlowych na jednej zmianie pracowało od 33 do 35 osób, których zadania były ograniczone do pewnego obszaru oraz podejmowania interwencji w przypadku zagrożeń.

Ostra konkurencja cenowa oraz kryzys na rynku pracy w latach 2007–08 doprowadziły jednak do fali optymalizacji, która spowodowała redukcję personelu i roboczogodzin oraz wymusiła zmiany w sposobie wykonywania zadań przez zespół ochrony. W rezultacie od pracowników ochrony zaczęto stopniowo oczekiwać więcej – ich praca stała się bardziej złożona i wymagająca. Ponadto, po roku 2010, wzrosła dostępność rozwiązań technicznych, które mogły być wykorzystywane na większą skalę w działaniach komercyjnych. Spadek cen tych rozwiązań oraz ich lepsza jakość i skuteczność, w połączeniu z rosnącymi kosztami pracy, spowodowały zmiany w oferowanych rozwiązaniach dotyczących systemów ochrony.

Zmiany te przyspieszyły w okresie pandemii, która brutalnie uświadomiła, jak łatwo obiekt może pozostać bez fizycznej ochrony w sytuacji szybkiego rozprzestrzeniania się groźnej infekcji. W odpowiedzi na to klienci stali się jeszcze bardziej otwarci na wprowadzanie rozwiązań technicznych, elektronicznych i informatycznych, które mogły ograniczyć takie ryzyko. W rezultacie obecnie w dużych obiektach wystarczy od 6 do 9 pracowników na jedną zmianę. Oznacza to, że w ciągu ostatnich 25 lat liczebność personelu ochrony – w obiektach zaawansowanych technicznie – mogła się zmniejszyć nawet o 70%. Oczywiście nie wszędzie zmiany zachodzą z taką dynamiką – nadal są takie organizacje, które w niewielkim stopniu korzystają z nowoczesnych rozwiązań, i tam liczba pracowników ochrony oraz sposób realizacji usługi nie ulegają zmianie.

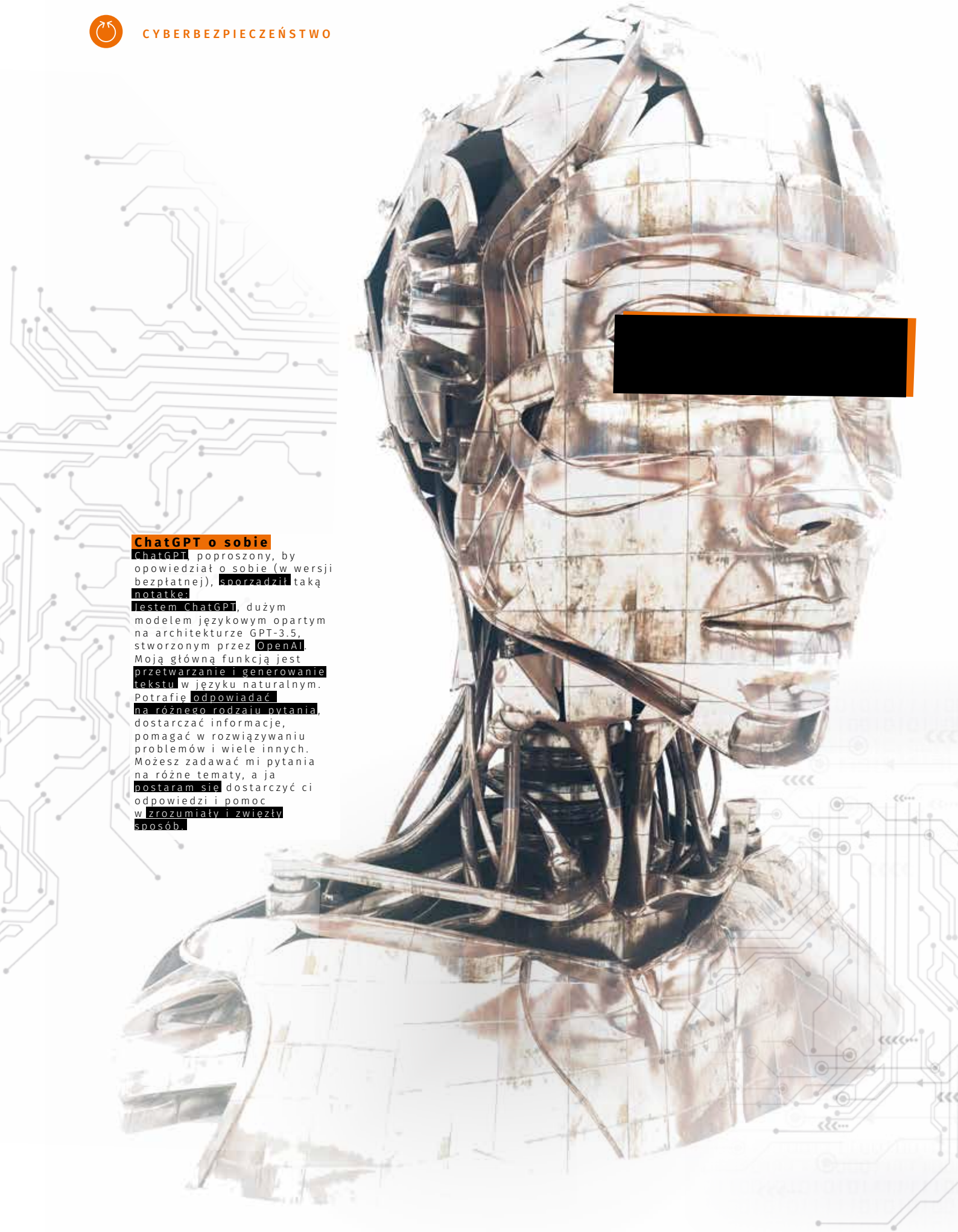
W związku z tym, aby dobrze i sprawnie realizować usługi ochrony, pracownik musi dobrze znać specyfikę klienta, potencjalne ryzyka oraz rozumieć cele działania i przypisaną mu odpowiedzialność. Wraz z rozwojem technologicznym i zmianami na rynku pracy zadania firmy ochrony stają się coraz bardziej złożone i wymagające, a pracownik musi mieć nie tylko predyspozycje fizyczne, ale także kompetencje interpersonalne, umiejętność rozwiązywania problemów oraz obsługi systemów i technologii stosowanych w obiekcie.

Aby skutecznie sprostać tym wyzwaniom, niezbędne jest systemowe inwestowanie przez firmy ochrony w działania rozwojowe oraz szkolenia pracowników ochrony. Wynagrodzenie pracowników powinno odzwierciedlać ich doświadczenie i kompetencje, a to wymaga zmiany archaicznego systemu rozliczeń godzinowych na bardziej adekwatne do jakości, skuteczności oraz zaawansowania technologicznego realizowanych usług.

Badania i symulacje dotyczące przyszłości zawodu pracownika ochrony obrazują wysoki wskaźnik możliwości zastąpienia tej grupy przez systemy i urządzenia, co potwierdza zmiany zachodzące w branży. Niemniej jednak, pomimo postępu technicznego, niektóre obowiązki – takie jak udzielanie pierwszej pomocy, kontrola imprez masowych czy ochrona VIP-ów – nadal wymagają fizycznej obecności człowieka. W związku z tym przyszłość pracy pracowników ochrony może ewoluować w kierunku pełnienia funkcji operatorów systemów bezpieczeństwa, jednakże nadal będą oni odgrywać kluczową rolę w zapewnieniu bezpieczeństwa fizycznego oraz reagowaniu na nietypowe sytuacje.

Zmiany zachodzące w branży ochrony osób i mienia wymagają od pracowników ochrony coraz większych kompetencji i elastyczności. Firmy ochrony powinny odpowiednio reagować na te zmiany, inwestując w rozwój swoich pracowników oraz dostosowując się do nowych wymagań rynku, aby zapewnić wysoką jakość świadczonych usług. ●

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



ChatGPT o sobie

ChatGPT, poproszony, by opowiedział o sobie (w wersji bezpłatnej), sporządził taką notatkę:

Jestem ChatGPT, dużym modelem językowym opartym na architekturze GPT-3.5, stworzonym przez OpenAI. Moją główną funkcją jest przetwarzanie i generowanie tekstu w języku naturalnym. Potrafię odpowiadać na różnego rodzaju pytania, dostarczać informacje, pomagać w rozwiązywaniu problemów i wiele innych. Możesz zadawać mi pytania na różne tematy, a ja postaram się dostarczyć ci odpowiedzi i pomoc w zrozumiały i zwięzły sposób.

AI na usługach **hakerów**

Modele językowe istnieją już od jakiegoś czasu, ale szczególnie głośno zrobiło się o nich za sprawą ChatGPT firmy OpenAI. Na copywriterów, dziennikarzy, ale i koderów padł blady strach. Wizja, że ludzie stracą pracę na rzecz robotów, przynajmniej w przypadku niektórych zawodów, stała się realna, tyle że odległa. A tuż za rogiem mamy do czynienia z zupełnie innym zagrożeniem.

Monika Żuber-Mamakis

Podobnie jak w wypadku innych narzędzi modele językowe mogą służyć różnym celom. Zbożnym albo – odwrotnie – nagannym, ponieważ każdy duży model językowy *(Large Language Model* – LLM) można równie dobrze wykorzystać do opracowania planu wycieczki i przeprowadzenia ataku phishingowego. To właśnie jest realne zagrożenie, na które powinniśmy być przygotowani: modele językowe już teraz powodują, że ataki phishingowe są coraz bardziej wyrafinowane. I może ich być coraz więcej.

Najbardziej popularnym modelem jest obecnie ChatGPT. To w istocie chatbot bazujący na algorytmach sztucznej inteligencji i głębokim uczeniu maszynowym (więcej o modelach w ramce *Czym jest model językowy)*. ChatGPT stale się doskonali, ucząc się na podstawie wcześniejszych interakcji. Model GPT zadebiutował już jakiś czas temu. GPT-1, pierwszy z serii, został opracowany w roku 2018. GPT-2 powstał w lutym 2019, a GPT-3 w czerwcu 2020.

Tym, co wywołało entuzjazm użytkowników, ale też tsunami obaw, było udostępnienie modelu w formie ChatGPT, co wydarzyło się listopadzie 2022 r., a następnie wprowadzenie w marcu 2023 przez OpenAI możliwości integracji innych aplikacji z ChatGPT. Teraz każda firma może wykorzystać moc dużego modelu językowego, integrując go ze swoimi usługami. Przykładowo biuro podróży może połączyć ChatGPT z systemem obsługi klienta, by przez całą dobę, siedem dni w tygodniu odpowiadać na pytania klientów. Może nie wszystkie, ale z pewnością na najczęstsze.

Problem w tym, że ChatGPT nie ma wpływu na to, komu służy. Na pomysł zaprzęgnięcia dużych modeli językowych, takich jak opracowany przez OpenAI, wpadli nie tylko mili ludzie z biur podróży, ale także twórcy phishingowych e-maili. W przypadku phishingu liczy się bowiem nie jakość, a ilość.

Sieć na płotki i wieloryby

Phishing to jeden z najpopularniejszych rodzajów ataków hakerskich. Polega na wysyłaniu fałszywych wiadomości e-mail lub SMS, które mają na celu wyłudzenie danych osobowych lub informacji poufnych. W zasadzie phishing to forma inżynierii społecznej, czyli techniki polegającej na manipulowaniu ludźmi, aby ci zrobili coś, co jest dla nich zazwyczaj niekorzystne. W przypadku phishingu cyberprzestępcy, podszywając się pod wiarygodne instytucje lub osoby, próbują nakłonić ofiarę do podania danych osobowych, takich jak login i hasło do konta bankowego, numer karty kredytowej czy dane osobowe. Aby jednak skłonić kogoś do tego, by kliknął w link podany w e-mailu lub wszedł na stronę, trzeba się trochę postarać. Ileż e-maili zawierających w miarę wiarygodnie wyglądającą treść ludzie są w stanie wymyślić? Statystyki cyberataków wskazują, że sporo. Wymaga to jednak czasu, zaangażowania i odrobiny fantazji. Może LLM nie mają fantazji, ale mają czas,

→

nie męczą się i w nieskończoność mogą wymyślać kolejne wersje phishingowych tekstów, wabiąc za ich pomocą naiwnych ludzi.

Zwykły *phishing* polega na wysyłaniu wiadomości e-mail lub SMS, które mają na celu wyłudzenie danych osobowych lub informacji poufnych. Wiadomości te wyglądają, jakby zostały wysłane przez wiarygodną instytucję, taką jak bank, urząd czy firma kurierska. Czasami jednak są boleśnie „kulawe", pełne błędów i literówek. Od razu widać, że twórca oszukańczego e-maila jest na bakier, np. z językiem polskim. Choć trzeba przyznać, że zdarzają się też bardzo wiarygodne. Phishing to masówka. Jest niczym łowienie płotek. E-mail wędruje przez sieć i co złapie, to ma. Nie musi być zatem wyrafinowany. Algorytmy GPT przydają się o tyle, że choć to połowy masowe i cyberprzestępcy liczą się z faktem, że w pułapkę wpadnie tylko promil zaatakowanych, to i tak warto zadbać o zwiększenie szans.

Spear phishing to bardziej zaawansowany rodzaj pułapki. Jest skierowany do konkretnego adresata, choć nie musi być to jedna osoba, ale np. grupa pracowników konkretnej instytucji rządowej, dużego banku itp. Wiadomości tego typu często są personalizowane i zawierają informacje, które mają wzbudzić zaufanie ofiary.

Whaling to z kolei polowanie na grube ryby. Jest najgroźniejszym rodzajem phishingu wymierzonym przeciwko osobom o wysokim statusie społecznym lub zawodowym. Wiadomości whalingowe są często bardzo realistyczne i mogą być trudne do odróżnienia od prawdziwych. Tworzone są zazwyczaj na zamówienie. W przypadku whalingu AI się nie sprawdzi. Tu jest potrzebny człowieka. Whaling wymaga zaangażowania, musi być precyzyjny, ale się opłaca. To nie jest szukanie kota w worku. Taki atak potrzebuje sprokurowania wiadomości phishingowej na najwyższym poziomie wiarygodności. ChatGPT do polowania na wieloryba nie jest wymagany.

Polowanie z nagonką

Zwykłe ataki phishingowe przedkładają ilość nad jakość i obejmują ogólne wiadomości wysyłane do niczego niepodejrzewających ofiar w celu kradzieży informacji poufnych. Większość programów antywirusowych z łatwością je odfiltrowuje. Na małą skalę phishing nie jest zbyt skuteczny, ale im większa grupa docelowa, tym więcej osób się nabierze i tym większy potencjalny zysk hakerów.

> » *Chaty bazujące na algorytmach LLM takie jak ChatGPT to kopalnia złota dla twórców ataków spear phishingowych.* «

Inaczej rzecz ma się ze spear phishingiem. Atakujący wcześniej zbierają dokładne informacje o ofiarach, takie jak imię, stanowisko, relacje zawodowe, co pozwala im przygotować taką wiadomość, aby była bardziej przekonująca i trudniejsza do zidentyfikowania jako oszustwo. To podejście ma na celu zwiększenie szans na skuteczność ataku. Jednocześnie w dalszym ciągu są to ataki masowe, skierowane do sporej grupy osób. I tu hakerzy wykorzystują ChatGPT.

Do czasu pojawienia się sztucznej inteligencji ewentualny „sukces" hakerów okupiony był koniecznością czasochłonnych przygotowań. Tak było, aż do pojawienia się dużych modeli językowych i ich łatwej do wdrożenia wersji w formie chatu.

Chaty bazujące na algorytmach LLM takie jak ChatGPT to kopalnia złota dla twórców ataków spear phishingowych.

Łącząc spear phishing z algorytmami sztucznej inteligencji, hakerzy uzyskują szokującą skuteczność. Jak wygląda ten proceder? Najpierw potrzebne są dane. Te można pozyskać ze zhakowanych serwisów internetowych. Potem wkraczają algorytmy AI, które służą do analizy tych danych i pozwalają przygotować atak typu spear phishing.

Hakerzy nie bawią się więc w wymyślanie „uniwersalnych" w przekazie e-maili o nieopłaconych przesyłkach kurierskich. Analizują duże zbiory danych i na bazie tego, co w nich znajdą, przygotowują

Czym jest model językowy

Model językowy to rodzaj sztucznej inteligencji, który został zaprojektowany do analizy, rozumienia i generowania tekstu w języku naturalnym. Głównym celem modeli językowych jest przewidywanie, jakie słowa lub zdania powinny pojawić się w kontekście. Model uwzględnia to, co wcześniej już zostało w danym kontekście użyte w tekstach stworzonych przez ludzi. Oznacza to, że modele językowe potrafią (powiedzmy) zrozumieć gramatykę, semantykę i kontekst języka naturalnego.

Modele językowe są szkolone na ogromnych zbiorach tekstów. Znają różne wzorce językowe. Dzięki temu są w stanie wykonywać różnorodne zadania, takie jak generowanie tekstu, tłumaczenie maszynowe, analiza sentymentu, rozpoznawanie mowy i wiele innych.

Najbardziej znane modele językowe, takie jak GPT-3 bazują na głębokim uczeniu maszynowym i potrafią produkować tekst tak, jak zrobiłby to człowiek. Mają szerokie zastosowanie w dziedzinach takich jak przetwarzanie tekstu, chatboty, automatyczne redagowanie, analiza danych tekstowych i wiele innych.

Termin „duży model językowy" (Large Language Model – LLM) odnosi się do modeli językowych bazujących na głębokim uczeniu (deep learning), co czyni je zdolnymi do przetwarzania ogromnych ilości tekstu w języku naturalnym. Modele LLM są znacznie większe i bardziej złożone niż wcześniejsze modele językowe i mają ogromny wpływ na rozwijającą się dziedzinę przetwarzania języka naturalnego.

Przykłady dużych modeli językowych to GPT-3 (Generative Pre-trained Transformer 3) opracowany przez OpenAI, BERT (Bidirectional Encoder Representations from Transformers) Google'a i wiele innych. Modele te przyczyniły się do znaczneg postępu w dziedzinie przetwarzania języka naturalnego i mają duży wpływ na rozwijającą się technologię.

zmasowany atak. Wyobraźmy sobie, że weszli w posiadanie danych dotyczących klientów konkretnego sklepu. Dzięki algorytmom AI szybko dowiadują się, kto, kiedy i co kupił, a także jaki był sposób dostawy. Na tej bazie mogą spreparować wiarygodnie wyglądający e-mail wysłany ze sklepu, a nawet za pomocą chata prowadzić naturalnie brzmiącą korespondencję z klientem. Można się spodziewać, że lada moment ataki spear phishingowe będą funkcjonować jak spersonalizowane reklamy, w których specjalizują się media społecznościowe. Wystarczy wyszukać coś, co nas interesuje, powiedzmy koncert ulubionego wykonawcy, by hakerzy natychmiast wysłali oszukańczą ofertę. Link będzie prowadzić do sfałszowanej strony, ale przygotowanej tak, że odróżnienie jej od prawdziwej będzie prawie niemożliwe. Skuszeni niewiarygodną promocją klikniemy, podamy dane karty płatniczej i… gorzko pożałujemy.

Ciekawe doświadczenie dotyczące przygotowywania ataków spear phishingowych opisał Security Intelligence. W artykule *AI vs. human deceit: Unravelling the new age of phishing tactics* przedstawiono eksperyment, w którego ramach zostały przygotowane dwa e-maile spear phishingowe. Jeden powstał za pomocą ChatGPT, drugi opracowali eksperci inżynierii społecznej. Wiadomość przygotowana przez zespół ludzi okazała się ostatecznie bardziej przekonująca, ale potrzebował on 16 godz. na jej przygotowanie. Chatowi zajęło to… 5 min.

E-maile to nie wszystko. Przestępcy wykorzystują także technikę klonowania głosu. Hakerom wystarczy szybka analiza facebookowej rolki czy klipu wrzuconego na TikToka, by odtworzyć dowolny głos i wykorzystać go do dzwonienia np. do bliskich. Metoda „na wnuczka" nie potrzebuje już nawet fałszywego „wnuczka". Może dzwonić automat, a konwersację z przerażoną babcią poprowadzi bot.

Pierwsza linia obrony

W dobie Internetu rzeczy, gdy coraz więcej firm korzysta z urządzeń security funkcjonujących w chmurze, ataki spear phishingowe mogą wyrządzić poważne szkody. Łatwo sobie wyobrazić atak skierowany przeciwko dużej firmie, którego skutkiem będzie np. paraliż systemu CCTV. Firmy zajmujące się ochroną prywatności i bezpieczeństwem ścigają się, aby opracować techniki identyfikowania schematów phishingu napisanych przez sztuczną inteligencję. Jednak przynajmniej na razie pierwszą linię obrony stanowią szkolenia i zdrowy rozsądek. Dlatego tak ważna jest współpraca działów IT z działami security.

Czego z takich szkoleń powinni się dowiedzieć pracownicy? Przede wszystkim tego, że brak ufności nie jest niczym nagannym. Warto przekazać też kilka podstawowych zasad i informacji.

- W przypadku wątpliwości należy zadzwonić do nadawcy e-maila. Nikt tu niczym nie ryzykuje, a zyskuje się pewność.
- Istnieje coś takiego jak *vishing (voice phishing)*. To forma ataku phishingowego przez telefon. Oszuści dzwonią, podszywając się pod zaufane instytucje, aby uzyskać informacje poufne. Należy więc weryfikować tożsamość rozmówcy i unikać udzielania wrażliwych danych przez telefon, chyba że jesteśmy pewni, że rozmawiamy z rzeczywistą instytucją.
- Warto ustalić wspólne dla przyjaciół i bliskich hasło, którego można użyć w przypadku oszustwa telefonicznego (*vishing*) lub próby oszustwa telefonicznego generowanego przez sztuczną inteligencję.
- Trzeba pamiętać, że phishingowe e-maile nie muszą być pełne błędów gramatycznych i literówek. Ataki phishingowe z wykorzystaniem sztucznej inteligencji stają się coraz bardziej wyrafinowane, a e-maile poprawne pod względem językowym.

Charakterystyczne cechy dużych modeli językowych (LLM)

Rozmiar: Modele LLM mają bardzo dużą liczbę parametrów, często osiągając setki milionów lub nawet miliardy parametrów. Duży rozmiar modelu pozwala na efektywne uczenie się i generowanie bardziej zaawansowanego tekstu.

Uczenie nienadzorowane: Modele LLM są trenowane w sposób nienadzorowany na ogromnych zbiorach danych tekstowych, co pozwala im nabyć wiedzę na temat struktury języka naturalnego i związków między słowami.

Zdolność do wielozadaniowości: Duże modele językowe mogą być dostosowywane do różnych zadań przetwarzania języka naturalnego, takich jak generowanie tekstu, tłumaczenie maszynowe, rozpoznawanie mowy, analiza sentymentu i wiele innych.

Generowanie wysokiej jakości tekstu: Modele LLM potrafią produkować tekst o wyjątkowo wysokiej jakości i są używane do tworzenia treści, generowania odpowiedzi w chatbotach oraz redagowania tekstu.

Ataki phishingowe

wykorzystują ludzką nieroztropność, ale też respekt dla autorytetów. I choć większość ludzi zachowuje czujność, to sporo osób albo nie zna zasad nieklikania w dziwne e-maile, albo je ignoruje, albo po prostu ulega presji.

1. **Phishing** to najczęstsza forma cyberprzestępczości. Szacuje się, że cyberprzestępcy wysyłają dziennie 3,4 mld e-maili, które mają wyglądać, jakby pochodziły od nadawców zaufanych. To ponad bilion e-maili phishingowych rocznie.
2. **Podszywanie się pod wiadomości e-mail** stanowi szacunkowo 1,2% całego ruchu e-mail na całym świecie.
3. Około 36% wszystkich naruszeń danych ma charakter **phishingowy**.
4. W 2022 r. 84% organizacji było celem co najmniej jednej próby phishingu, co oznacza wzrost o 15% w porównaniu z rokiem poprzednim.
5. W czwartym kwartale 2022 r. Grupa Robocza ds. Zwalczania Phishingu (APWG) zaobserwowała łącznie **1 350 037 ataków phishingowych** w porównaniu z 1 270 833 w poprzednim kwartale.
6. W roku 2022 WG odnotowała **~4,7 mln ataków phishingowych**. Od 2019 roku liczba ataków phishingowych rośnie o ponad 150% rocznie.
7. Wzrost **ataków phishingowych** według roku:

Rok	Liczba zaobserwowanych ataków
2019	779 200
2020	1 845 814
2021	2 847 773
2022	4 744 699

8. W 2021 roku średni współczynnik klikalności dla **kampanii phishingowej** wyniósł 17,8%.
9. Bardziej ukierunkowane **kampanie phishingu typu *spear*** miały średni współczynnik klikalności na poziomie **53,2%.**

Źródło danych: StationX; www.stationx.net/phishing-statistics/

Wspólnym zadaniem działów IT i security powinno być wzmocnienie kontroli dostępu i zarządzania tożsamościami. Zaawansowane systemy zarządzania dostępem do tożsamości mogą pomóc w potwierdzaniu, kto ma dostęp do jakich danych, czy ma odpowiednie uprawnienia i czy są tym, za kogo się podaje.

Szybka ewolucja sztucznej inteligencji oznacza, że cyberprzestępcy nadal będą doskonalić swoje taktyki. Musimy przyjąć tę samą mentalność ciągłej adaptacji i innowacji. Regularna aktualizacja wewnętrznych procedur taktycznych, systemów wykrywania zagrożeń i materiałów szkoleniowych dla pracowników jest niezbędna, aby być o krok przed złośliwymi podmiotami.

AXIS COMMUNICATIONS

Aplikacja do analizy na brzegu sieci

Axis Communications przedstawia aplikację analityczną AXIS Radar Data Visualizer, która łączy detekcję radarową 180° i panoramiczne obrazy wielosensorowe 180° w celu poprawy świadomości sytuacyjnej przy minimalnej liczbie fałszywych alarmów. Aplikacja jest idealna do monitorowania dużych otwartych obszarów, może dokładnie wykrywać ludzi z odległości do 60 m i pojazdy z odległości do 85 m.

AXIS Radar Data Visualizer zwiększa wartość i funkcjonalność panoramicznych kamer wielosensorowych Axis. Aplikacja wykorzystuje dane radarowe, aby dokładnie wykrywać i klasyfikować osoby oraz pojazdy w miejscach, w których nie powinny się znajdować. Gromadzi i przetwarza dane radarowe, a następnie prezentuje je jako wizualne, konfigurowalne nakładki w kanale kamery. Dane mogą być również wykorzystywane do wyzwalania zdarzeń.

Możliwe jest aktywowanie świateł stroboskopowych, wyzwalanie alarmów lub uruchamianie nagrań z kamery za każdym razem, gdy obiekt przekroczy wstępnie zdefiniowaną wirtualną linię w widoku kamery. Dodatkowo dzięki technologii ***edge-to-edge*** można go podłączyć do obsługiwanych kamer panoramicznych w celu weryfikacji wizualnej z pokryciem 180° bez żadnych martwych punktów.

Wykorzystując technologię radarową, AXIS Radar Data Visualizer oferuje ekonomiczne operacje i dokładne wykrywanie 24/7. Ponadto jest możliwe wyświetlanie prędkości przejeżdżających pojazdów w nakładce w każdych warunkach pogodowych lub oświetleniowych.

Najważniejsze cechy wizualizatora danych radarowych AXIS

- Ulepszona świadomość sceny z niezawodnym wykrywaniem 24/7
- Wykrywanie osób w odległości do 60 m (200 stóp)
- Wykrywanie pojazdów w odległości do 85 m (280 stóp)
- Zasięg 180° bez martwych punktów
- Wyzwalanie zdarzeń na podstawie danych radarowych

ROGER

Integracja RACS 5 z oprogramowaniem GANZ CORTROL VMS

CBC Group, międzynarodowy koncern z siedzibą w Tokio, to przedsiębiorstwo z wyjątkowo bogatym doświadczeniem w tworzeniu nowych technologii. W roku 2016 CBC wprowadziło do oferty oprogramowanie GANZ CORTROL VMS przeznaczone na rynek projektowy. W tym samym roku został wprowadzony system kontroli dostępu i automatyki budynkowej RACS 5 firmy Roger.

Oba rozwiązania w naturalny sposób się uzupełniają, a połączenie ich funkcjonalności może przynieść inwestorowi szereg korzyści. Integracja daje oprogramowaniu GANZ CORTROL VMS następujące możliwości:

- dostęp do bazy danych użytkowników systemu RACS 5;
- dostęp do listy przejść obsługiwanych przez system RACS 5;
- monitorowanie wizyjne drzwi/przejść;
- monitorowanie online zdarzeń na przejściach;
- przegląd historii zdarzeń na przejściach;
- wizualizację statusu przejść na e-mapach;
- zmianę stanu poszczególnych przejść (integracja dwukierunkowa).

Integracja umożliwia przeglądanie logów systemu kontroli dostępu z poziomu oprogramowania VMS. Zdarzenia można filtrować według przedziału czasu, nazwy drzwi, konkretnej nazwy posiadacza karty, a także docelowej nazwy zdarzenia, dzięki czemu operator może m.in.:

- zobaczyć, które drzwi otworzył dany użytkownik w ciągu dnia;
- sprawdzić, czy dana osoba używa własnej karty dostępu, porównując zdjęcie posiadacza karty z nagraniem z kamery;
- sprawdzić aktualny stan drzwi i w razie potrzeby ręcznie je zablokować czy odblokować.

Funkcjonalność tych rozwiązań przekłada się na podniesienie poziomu bezpieczeństwa w obiekcie oraz skuteczność codziennej pracy ochrony obiektu, dając jej narzędzia do sprawnego wykrywania niepożądanych zdarzeń oraz niezwłocznego reagowania. Walory integracji mogą być wykorzystywane w biurowcach, fabrykach, szpitalach, więzieniach, uczelniach oraz w wielu innych miejscach wymagających wysokiego poziomu zabezpieczeń.

Z integracji korzystają zarówno placówki sektora publicznego, jak i prywatne zakłady przemysłowe. Wśród referencji znajdują się m.in. jednostki organizacyjne podległe Okręgowemu Inspektoratowi Służby Więziennej w Lublinie oraz Wodociągi Miasta Kraków. Integracja została wdrożona również w centrach logistycznych ogólnopolskiej sieci POLOmarket.

HANWHA VISION

Nowe funkcje w kamerach Hanwha z serii Q

Hanwha Vision wprowadza funkcje podwójnego oświetlenia z białymi diodami LED i IR w inteligentnych kamerach AI z serii Q, aby zapewnić lepszą i ekonomiczną wydajność przy słabym oświetleniu. Dzięki temu kamery znakomicie sprawdzają się w zapewnieniu bezpieczeństwa rozległych obszarów zewnętrznych.

Kamery z podwójnym oświetleniem QNE-C9013RL i QNE-C8013RL eliminują potrzebę stosowania zewnętrznych źródeł oświetlenia. Zmniejsza to koszty, eliminując jednocześnie zanieczyszczenie światłem, ponieważ kamery wykorzystują białe światło tylko wtedy, gdy jest ono potrzebne. Ofertę uzupełnia płaska konstrukcja typu *flateye* ułatwiająca instalację.

Połączenie możliwości podwójnego oświetlenia z analizą sztucznej inteligencji powoduje, że kamery zapewniają bardzo dokładne wykrywanie obiektów (pojazdów i osób) w rozdzielczości do 4K, nawet w warunkach słabego oświetlenia.

W przypadku wykrycia osób lub pojazdów wkraczających na określony obszar kamery automatycznie przełączają się z dyskretnego trybu podczerwieni na oświetlenie ciepłym białym światłem. Oświetlając lub rzucając jasne światło na osoby wałęsające się lub wykonujące podejrzane czynności, działa to jako środek odstraszający potencjalnych intruzów. Dzięki tym zaletom seria ta doskonale nadaje się do wielu różnych zastosowań, w tym do ochrony obiektów handlowych i komercyjnych oraz zapewnienia bezpieczeństwa i ciepłego powitania w obszarach mieszkalnych.

Dodanie sztucznej inteligencji do kamer Hanwha Vision z serii Q umożliwia dokładną klasyfikację osób i pojazdów poprzez filtrowanie nieistotnych wyzwalaczy ruchu, takich jak poruszające się zwierzęta czy gałęzie drzew, co generuje mniej fałszywych alarmów dla operatorów. W rezultacie wzrasta skuteczność zespołu, można prowadzić efektywne poszukiwania kryminalistyczne, jednocześnie lepiej wykorzystując szerokość pasma nagrywania.

Udoskonalona konstrukcja kamery typu *flateye* sprawia, że jej montaż jest łatwiejszy i bardziej intuicyjny. Obrót, pochylenie i rotacja mogą być również szybko regulowane poprzez odkręcenie jednej śruby. ●

REKLAMA

Bi-spektralna kamera termowizyjna z AI

TNM–C4960TD/4950TD/4940TD

Hanwha Vision

Dokładne wykrywanie obiektów na podstawie algorytmów Deep-Learning

www.hanwhavision.eu

LINC POLSKA

EFOY Pro – innowacyjne ogniwa paliwowe

Proces produkcji energii w ogniwach paliwowych EFOY Pro marki SFC Energy AG odbywa się poprzez reakcję chemiczną. Poza energią elektryczną ogniwo oddaje ciepło, czystą wodę i śladowe ilości CO_2. Co istotne, w reakcji chemicznej nie dochodzi do spalania paliwa, więc wszelkie ryzyko z tym związane zostało zminimalizowane, dlatego ogniwa paliwowe EFOY Pro mogą być używane w pomieszczeniach zamkniętych oraz w pojazdach. Taki sposób zasilania jest ekonomiczny i przyjazny środowisku.

Innowacyjne ogniwa paliwowe charakteryzują się:

- wysoką sprawnością – 10 l metanolu zawiera 11,1 kWh energii;
- kompaktowymi, niewielkimi rozmiarami, które w połączeniu z niezawodnością i trwałością ogniw sprawiają, że można je stosować w trudnych i niedostępnych miejscach oraz używać w rozwiązaniach mobilnych i off-gridowych;
- bezobsługowością – nie wymagają przeglądów, stałego nadzoru i mogą pracować autonomicznie przez wiele tygodni (możliwość podłączenia kilku kartridżów do jednego urządzenia);
- zdalnym dostępem do urządzenia;
- emisją zanieczyszczeń bliską 0 i cichą pracą na poziomie wentylatora biurowego;
- możliwością współpracy z różnymi akumulatorami, a uruchomienie urządzenia nie wymaga interakcji użytkownika, następuje automatycznie, kiedy poziom naładowania akumulatorów spadnie poniżej określonego napięcia.

Te nowatorskie ogniwa paliwowe z powodzeniem są wykorzystywane przez służby ratownicze, wojsko oraz w projektach specjalistycznych. Znalazły też zastosowanie w rozwiązaniach mobilnych, w tym w wieżach do monitoringu. ●

WAT

Seminarium Wydziału Elektroniki WAT

Podczas dziewiątego już Seminarium Branży Elektronicznych Systemów Bezpieczeństwa w WAT eksperci z obszarów nauki i przemysłu omówili techniczne aspekty projektowania i instalacji innowacyjnych systemów zabezpieczeń.

Seminarium odbyło się 12 marca 2024 r. Zorganizował je Instytut Systemów Elektronicznych Wydziału Elektroniki (WEL WAT) przy współudziale wiodących firm z branży elektronicznych systemów zabezpieczeń. Producenci zaprezentowali najnowsze urządzenia, a reprezentanci firm projektowych omówili najciekawsze *case study* dotyczące projektowania innowacyjnych instalacji niskoprądowych.

Na dynamiczny rozwój rozwiązań branżowych, m.in. w wyniku zastosowania technologii Internetu rzeczy (IoT) oraz sztucznej inteligencji, zwróciła uwagę prorektor ds. studenckich dr hab. Monika Szyłkowska, prof. WAT, która w obecności dziekana WEL prof. dr. hab. inż. Ryszarda Szpleta otworzyła seminarium. Głos zabrał również rektor Akademii Pożarniczej bryg. dr inż. Tomasz Klimczak, profesor AP.

W tegorocznym konkursie o tytuł Mistrza Elektronicznych Systemów Bezpieczeństwa wyłoniono 6 laureatów. Zwycięzcą i zdobywcą statuetki został Kacper Bodecki, student niestacjonarnych studiów I stopnia na kierunku: elektronika i telekomunikacja. Gratulujemy!

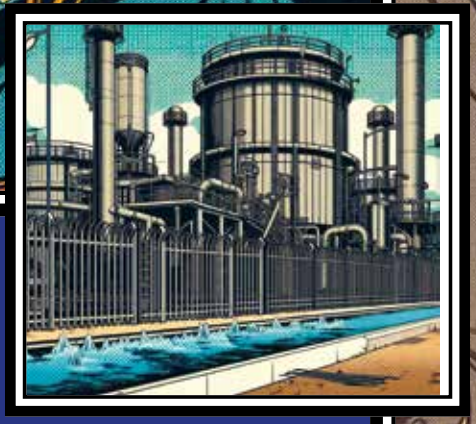
W seminarium uczestniczyło 14 z 20 partnerów z branży security, z którymi współpracuje WAT. Były to firmy: AAT Systemy Bezpieczeństwa, Assa Abloy, CBC Poland, Hikvision, ICS Polska, Janex International, MR System, Polon-Alfa, PISA, Pulsar, Roger, Satel, Schrack Seconet oraz Akademia Pożarnicza, która występowała w roli partnera akademickiego.

Więcej info na: www.wojsko-polskie.pl/wat/ ●

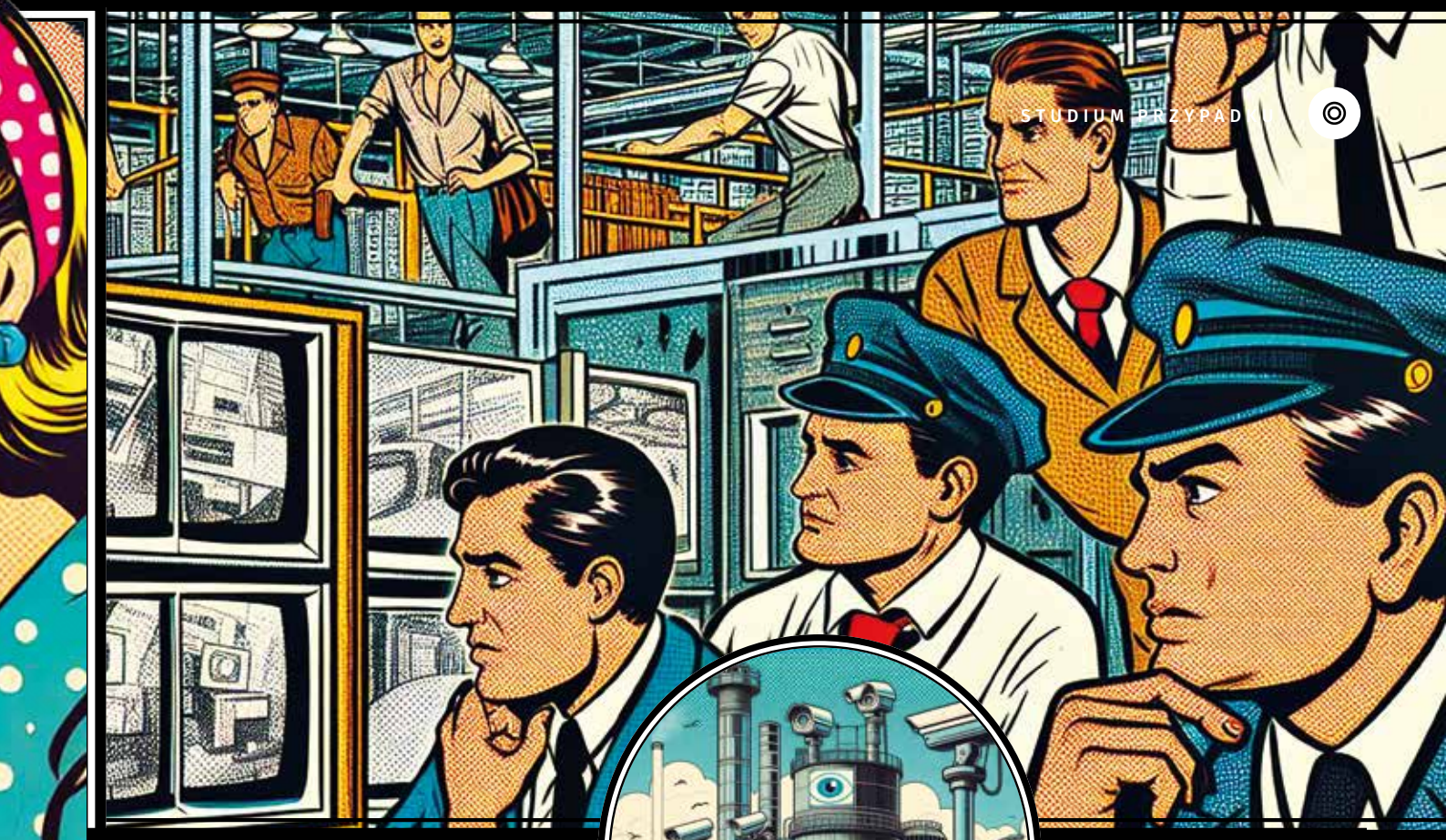

check. create. manage.
Checly
Zakład produkcyjny
wszystkie lokalizacje
Zadania do wykonania
dla mnie
wszystkie
2 gru
Kontrola ochrony fizycznej
Krzysztof Pacel
3 gru
Inspekcja obiektu Południe
Zbigniew Koczwara
4 gru
Kontrola bramy głównej
Łukasz Bleniek
5 gru
Sprawdzenie czujek na wejściu
Jarosław Reguła
6 gru
Kontrola pracownika w recepcji
Franciszek Gola
Checly
the best startup 2023
checly.app

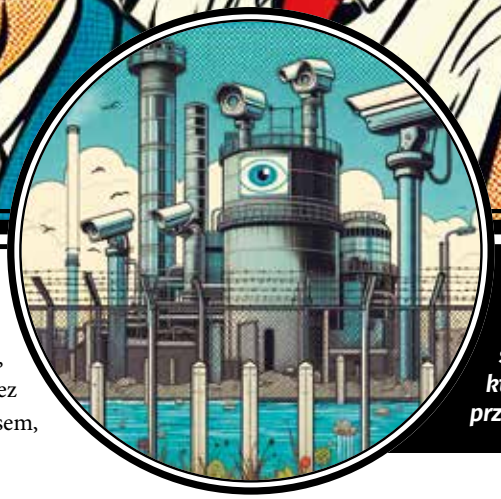
– Stefan, wstawaj, woda nie leci. Stefaaaan, woda nie leci!

Woda nie leci!



Inżynier Stefan Morski zazwyczaj spał snem kamiennym, ale hasło „woda nie leci” od razu postawiło go na równe nogi. Żona inżyniera Stefana Morskiego stała nad nim z jego komórką w jednej i z czajnikiem w drugiej ręce. W czajniku niestety nie było ani kropli wody.





– Żadna z czujek nie zarejestrowała próby wtargnięcia do budynków stacji. Na monitoringu widać, którędy weszli, zaraz tam przejdziemy.

W mig zrozumiał, że dzieją się rzeczy dramatyczne. Po pierwsze, jeśli woda nie leci, to znaczy, że jego żona nie napije się kawy, a to źle wróży wszystkim wokół, a jemu najbardziej. Po drugie, skoro żona, jeszcze bez kawy, budzi go o piątej rano, tuż przed spacerem z psem, to znaczy, że coś się stało w stacji uzdatniania wody.

Trzydzieści nieodebranych połączeń

Morski spojrzał na telefon, który wręczyła mu zdecydowanie bardziej przytomna małżonka.

– O cholera, jęknął. Mam trzydzieści nieodebranych! – Spojrzał na żonę, która już spakowała jego laptop, przygotowała plecak i wręczyła butelkę mineralnej.

– Gnaj, pewnie się coś stało. – W ostatnim momencie pani Morska zarzuciła mężowi szalik i wcisnęła na głowę czapkę. Wprawdzie wody w kranach nie było, ale tego poranka lało jak z cebra.

I pognał Morski do miejskiej stacji uzdatniania wody, gdzie był jedną z osób odpowiedzialnych za to, że woda trafia do kranów, rezerwuarów i zbiorników całkiem sporego miasta, a dokładnie do jego połowy, po tej stronie rzeki. Za tamtą odpowiadała inna stacja.

Gdy zdyszany wbiegł na teren, zobaczył, że tuż za bramą kręci się kilku kolegów z nietęgimi minami.

– Panowie, co się dzieje? Dlaczego woda nie leci? Kto wydał decyzję? – Morski spojrzał na zafrasowanych kolegów. – I co tam stoi przy wejściu do hali filtrów? Jakieś dziwne rzeczy. – Poczuł, że żołądek mu się niepokojąco kurczy. Muszę coś zjeść nim tu padnę, pomyślał.

– Już wyjaśniam panie inżynierze – odezwał się Bratek, wieloletni pracownik załogi chroniącej obiekt, który na dobrą sprawę wyglądał jak przerośnięty słonecznik za sprawą rudawej czupryny okalającej solidną łysinę – otóż jakieś łajzy się nam wdarły na teren…

– Jak to „wdarły" na teren? – Morski nie krył zdumienia. – Mamy podwójne ogrodzenie, czujniki, kamery i te, no… systemy napłotne…

– Napłotowe – wtrącił się stojący obok Leszek Lichy, szef zespołu chroniącego stację.

– Przecież mówię, że napłotowe. – Morski się zirytował. – Mamy to wszystko plus ludzi i ktoś się nam tu wdziera na teren?! Do filtrów też?

Leszek Lichy rozumiał zdenerwowanie Morskiego. Od pracy stacji zależało, czy w dużej części miasta woda z kranów popłynie. Nawet nie ciepła, a jakakolwiek.

– Panie inżynierze – Lichy zaczął spokojnie – wstępnie przejrzeliśmy zapisy z kamer. Wygląda na to, że to akcja jakichś dzieciaków. Wlazły na teren, ale do żadnego z obiektu raczej się nie włamały.

– Panie Lichy, co znaczy raczej? – Morski był wyraźnie zdenerwowany, czemu nie sprzyjał fakt, że był na czczo, a z głodu ssało go już wieczorem.

– To, co znaczy. – Tym razem Lichy się zirytował. – Żadna z czujek nie zarejestrowała próby wtargnięcia do budynków stacji. Na monitoringu widać, którędy weszli, zaraz tam przejdziemy.

– No dobra. – Morski nieco się uspokoił. – Kto podjął decyzję o wyłączeniu stacji?

Na to pytanie wszystkie oczy zwróciły się w stronę Jędrzeja Jeziornego. Jeziorny z Morskim pracowali razem już kilkanaście lat. Znali się tak dobrze, że współpracownicy nazywali ich „wodnym duetem".

– Stefan, przecież wiesz, że ja – odezwał się Jeziorny. – Do ciebie nie szło się dodzwonić. – Morski poczuł, że się czerwieni. – Wyłączyłem stację, bo lepiej dmuchać na zimne. Zanim się nie przekonamy, że wodociągi są bezpieczne, lepiej puścić na miasto beczkowozy.

Co racja, to racja, pomyślał Bratek, a na głos powiedział:

– A oni tam banery zostawili, nic takiego niebezpiecznego. I trochę tych… kwiatów.

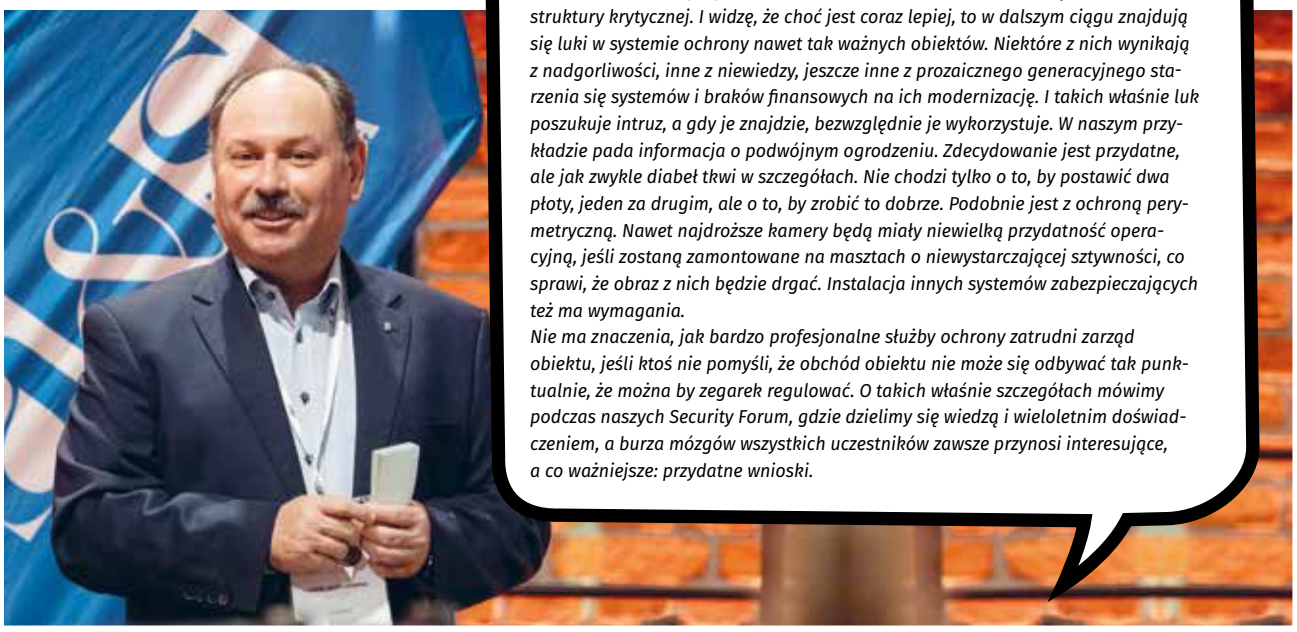
– Banery i kwiaty? – Jeziorny aż uniósł brwi. – Co jest na tych banerach? I jakie kwiaty?

– Kwiatki takie zwykłe w skrzynce, chyba bratki, a banerów nie rozwijałem. Pewnie mieli plan, żeby to jakoś na naszych obiektach umieścić, tak jak ci z tej organizacji ekologicznej, co weszli na komin w Bełchatowie. – Bratek był dumny, że pamięta.
– Panie, jaki komin? Przecież u nas nie ma kominów. – Brwi Jeziornego za chwilę miały szansę sięgnąć potylicy.
– To stara sprawa – wtrącił się Lichy. – Sprzed prawie 20 lat. Aktywiści z Greenpeace'u wspięli się na chłodnię kominową elektrowni Bełchatów i zaczęli malować napisu „Stop CO_2". To był protest przeciwko faworyzowaniu węgla, ale przecież my tu węgla nie mamy, tylko wodę. I nie smrodzimy, tylko czyścimy. Ogólnie to dziwna sprawa.
Z piersi wszystkich zgromadzonych wydobyło się westchnienie. Niezaprzeczalnie sprawa była dziwna. W głowach wszystkich kotłowały się pytania. Jak oni się w tu wdarli? W jaki sposób udało się ominąć Bratka? Dlaczego intruzów nie zatrzymało podwójne ogrodzenie?
Im dłużej stali, patrząc po sobie, tym bardziej byli zdziwieni.

Opracowała Monika Mamakis na bazie scenariusza Jacka Grzechowiaka

- **Jak intruzi wdarli się na teren?**
- **W jaki sposób udało się ominąć ochronę?**
- **Dlaczego intruzów nie zatrzymało podwójne ogrodzenie?**

Na te pytania odpowiada Jacek Grzechowiak, ekspert do spraw security, wykładowca, podczas cyklicznie odbywających się warsztatów Security Forum, organizowanych przez czasopismo „a&s Polska".



Jacek Grzechowiak, ekspert do spraw security

Od wielu lat zajmuję się m.in. audytem obiektów, także tych należących do infrastruktury krytycznej. I widzę, że choć jest coraz lepiej, to w dalszym ciągu znajdują się luki w systemie ochrony nawet tak ważnych obiektów. Niektóre z nich wynikają z nadgorliwości, inne z niewiedzy, jeszcze inne z prozaicznego generacyjnego starzenia się systemów i braków finansowych na ich modernizację. I takich właśnie luk poszukuje intruz, a gdy je znajdzie, bezwzględnie je wykorzystuje. W naszym przykładzie pada informacja o podwójnym ogrodzeniu. Zdecydowanie jest przydatne, ale jak zwykle diabeł tkwi w szczegółach. Nie chodzi tylko o to, by postawić dwa płoty, jeden za drugim, ale o to, by zrobić to dobrze. Podobnie jest z ochroną perymetryczną. Nawet najdroższe kamery będą miały niewielką przydatność operacyjną, jeśli zostaną zamontowane na masztach o niewystarczającej sztywności, co sprawi, że obraz z nich będzie drgać. Instalacja innych systemów zabezpieczających też ma wymagania.
Nie ma znaczenia, jak bardzo profesjonalne służby ochrony zatrudni zarząd obiektu, jeśli ktoś nie pomyśli, że obchód obiektu nie może się odbywać tak punktualnie, że można by zegarek regulować. O takich właśnie szczegółach mówimy podczas naszych Security Forum, gdzie dzielimy się wiedzą i wieloletnim doświadczeniem, a burza mózgów wszystkich uczestników zawsze przynosi interesujące, a co ważniejsze: przydatne wnioski.


WARSAW
SECURITY
SUMMIT
Największa
Konferencja
Branży
Zabezpieczeń
Nowa
Formuła
06/06/2024
SZCZEGÓŁY WKRÓTCE

securex®
POLAND
Międzynarodowe Targi Zabezpieczeń

23-25 kwietnia 2024
Międzynarodowe Targi Poznańskie
Stoisko 33, pawilon 6

PREMIERA BCS ULTRA

POLSKA MARKA BCS

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