05 (47) / 2024

CZASOPISMO RYNKU SECURITY

a&S POLSKA

BEZPIECZEŃSTWO W PRZEMYŚLE. OBRAZ RYNKU

Każde przedsiębiorstwo przemysłowe musi się liczyć z tym, że incydenty bezpieczeństwa bywają kosztowne. Jak chronią się polskie firmy?

NIE TRZEBA USTAWY, BY ROZPOZNAĆ SABOTAŻ

Zarządzanie bezpieczeństwem wymaga uwzględnienia, że zagrożenie może mieć swoje źródło wewnątrz organizacji.

AI I SECURITY. KIEDY LUDZKIE ZMYSŁY TO ZA MAŁO

Kiedy zaciera się granica między bezpieczeństwem fizycznym a cyberbezpieczeństwem, firmy muszą mieć baczenie na to, co się dzieje w ich cyfrowym otoczeniu.

www.aspolska.pl

20 zł
(w tym 8% VAT)

ISSN 2451-5175 05
9 772451 517703

CASTEL

INSPIRED COMMUNICATION & SECURITY

Castel - interkomowy system komunikacji i kontroli dostępu

Produkt z atestem PZH

- Sektor medyczny
- Więziennictwo
- Energetyka
- Jednostki wojskowe

- Protokół SIP
- Komunikacja VoIP
- Wandaloodporny - IK08
- Odporny na zmieniające się warunki atmosferyczne - IP65

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

MIWI urmet

Wielka woda, sabotaż, wojna hybrydowa…

…można powiedzieć, siła złego na jednego. Nużyć może wysłuchiwanie o turbulentnych czasach i czarnych łabędziach, ale cóż robić, gdy rzeczywistość skrzeczy. Czarne łabędzie zwiastujące w biznesie wydarzenie o wielkim znaczeniu dla gospodarki tym razem przypłynęły z kolejną wielką wodą. Kiedy bowiem przygotowujemy ten numer do druku, południe Polski walczy ze skutkami powodzi. Największej po tej, do której doszło w 1997 roku.

Straty materialne są ogromne. Pierwsze próby oszacowania szkód mówią o ponad 5 mld zł. Zapewne będzie jeszcze więcej. Uporanie się ze skutkami *wielkiej wody* będzie kosztowne i czasochłonne. Tymczasem zima za pasem. A przecież to niejedyny problem, z którym zmagać muszą się firmy z tej części kraju. Tak samo, jak wszystkim innym polskim firmom, grozi im zwykła przestępczość czy incydenty będące albo wynikiem losowych wydarzeń, albo… sabotażu, będącego często pokłosiem wojny toczącej się za naszą wschodnią granicą i towarzyszącej jej wojny hybrydowej. *Nie trzeba ustawy, by rozpoznać sabotaż,* o tym piszemy na str. 18.

Każda firma musi dostosować własną strategię ochrony, aby zadbać o bezpieczeństwo mienia, a także swoich pracowników. W tym kontekście powódź, która dotknęła południe Polski, staje się nie tylko tragicznym wydarzeniem, ale także punktem zwrotnym w myśleniu o bezpieczeństwie przemysłu. Woda zniszczyła przecież nie tylko maszyny i infrastrukturę, ale także naraziła na niebezpieczeństwo życie pracowników. Powódź, która spustoszyła wiele zakładów przemysłowych na południu Polski, ujawniła słabości istniejących systemów zabezpieczeń.

Skala zagrożeń w ostatnich latach znacznie się zwiększyła. Bezpieczeństwo stało się więc obszarem, który rozwija się dynamicznie, jak żadna inna branża, i w związku z tym wymaga ciągłego doskonalenia oraz dostosowywania do zmieniających się warunków technologicznych i prawnych. Piszemy o tym w raporcie *Bezpieczeństwo w przemyśle, obraz rynku* (str. 12). Warto sprawdzić, jak wygląda ten obraz rynku, by wybrać rozwiązania nie tylko sprawdzone, ale także odporne na zagrożenia różnego rodzaju. Także takie, jakie mogą się pojawić w wyniku upowszechnienia sztucznej inteligencji, która z przytupem wkracza w naszą rzeczywistość. Więcej na ten temat w artykule *AI i security. Kiedy ludzkie zmysły to za mało* (str. 56).

W kontekście współczesnych wyzwań nie można zapominać o wojnie hybrydowej, która wymaga od przedsiębiorstw nowego podejścia do zarządzania ryzykiem. Przemiany te powinny obejmować zarówno inwestycje w nowoczesne technologie zabezpieczeń, jak i regularne szkolenia dla pracowników dotyczące rozpoznawania potencjalnych zagrożeń. Jak powiedział Sun Zi, jeden z największych starożytnych myślicieli Dalekiego Wschodu, autor najstarszego na świecie podręcznika sztuki wojennej: „Poznaj dobrze wroga i poznaj dobrze siebie, a nie doznasz klęski."

Redakcja

CZASOPISMO RYNKU SECURITY

a&S POLSKA

05 (47) / 2024

SPIS TREŚCI

AI I SECURITY. KIEDY LUDZKIE ZMYSŁY TO ZA MAŁO

PRODUKTY NUMERU

8 Najnowsze urządzenia z oferty firm: Axis Communications, BCS (NSS), Hanwha Vision, Hikvision, Linc Polska, TP-Link

PRZEMYSŁ

12 Bezpieczeństwo w przemyśle. Obraz rynku
Adela Prochyra

18 Nie trzeba ustawy, by rozpoznać sabotaż
Jacek Grzechowiak

24 Trzy poziomy wykorzystania dozoru wizyjnego w produkcji
Axis Communications

26 Rozwiązania Hikvision dla przemysłu i farm fotowoltaicznych
Piotr Świder, Hikvision Poland

28 Integracja systemów w Dahua DSS – nowoczesne podejście do bezpieczeństwa sektora przemysłowego
Mariusz Kulik, Dahua Technology Poland

30 Głos branży

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.

BCS®

dla profesjonalistów

BCS-L-EIP242FR3-TH-AI(0202)

Dualne kamery termowizyjne BCS Line z analizą obrazu i funkcjami termicznymi.

Ochrona perymetryczna zabezpieczy obiekt przed intruzem, a detekcja pożaru uchroni przed jego skutkami w razie rozprzestrzenienia.

Więcej niż obraz

» Więcej przeczytasz na stronie 8

POLSKA MARKA BCS

www.bcs.pl

www.facebook.com/bcspl

CZASOPISMO RYNKU SECURITY

a&S POLSKA

05 (47) / 2024

SPIS TREŚCI

RYNEK SECURITY

36 Kluczowy element w zarządzaniu kontrolą dostępu
Jan T. Grusznic

40 Dobór depozytorów SAIK
BTE

41 Składka ZUS dla wszystkich umów cywilnoprawnych. Wyzwanie, ale i szansa
PZPO

42 Czy widzisz to co ja?
Jakub Sobek, Konica Minolta

44 Znaczenie fizycznego bezpieczeństwa w centrach danych
Optex

46 Sieciowanie central alarmowych rodziny Galaxy Dimension
Tomasz Górski, TAP Systemy Alarmowe

50 Mapa inwestycji

BEZPIECZEŃSTWO POŻAROWE

52 Zabezpieczenie magazynów wysokiego składowania instalacjami sygnalizacji pożarowej
Mariusz Sobecki

CYBERBEZPIECZEŃSTWO

56 AI i security. Kiedy ludzkie zmysły to za mało
Monika Żuber-Mamakis

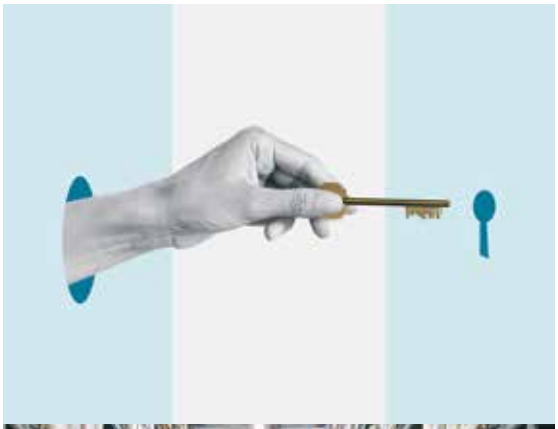
60 Nieznajomość prawa szkodzi
Wywiad z Agnieszką Wachowską, radczynią prawną specjalizującą się w cyberbezpieczeństwie

SERWIS INFORMACYJNY

64 Nedap Security Day – przyszłość bezpieczeństwa i kontroli dostępu w dobie sztucznej inteligencji

66 Nowości produktowe/informacje firmowe

68 Komiks: Ile to jest jeden „bul”?
Monika Żuber-Mamakis

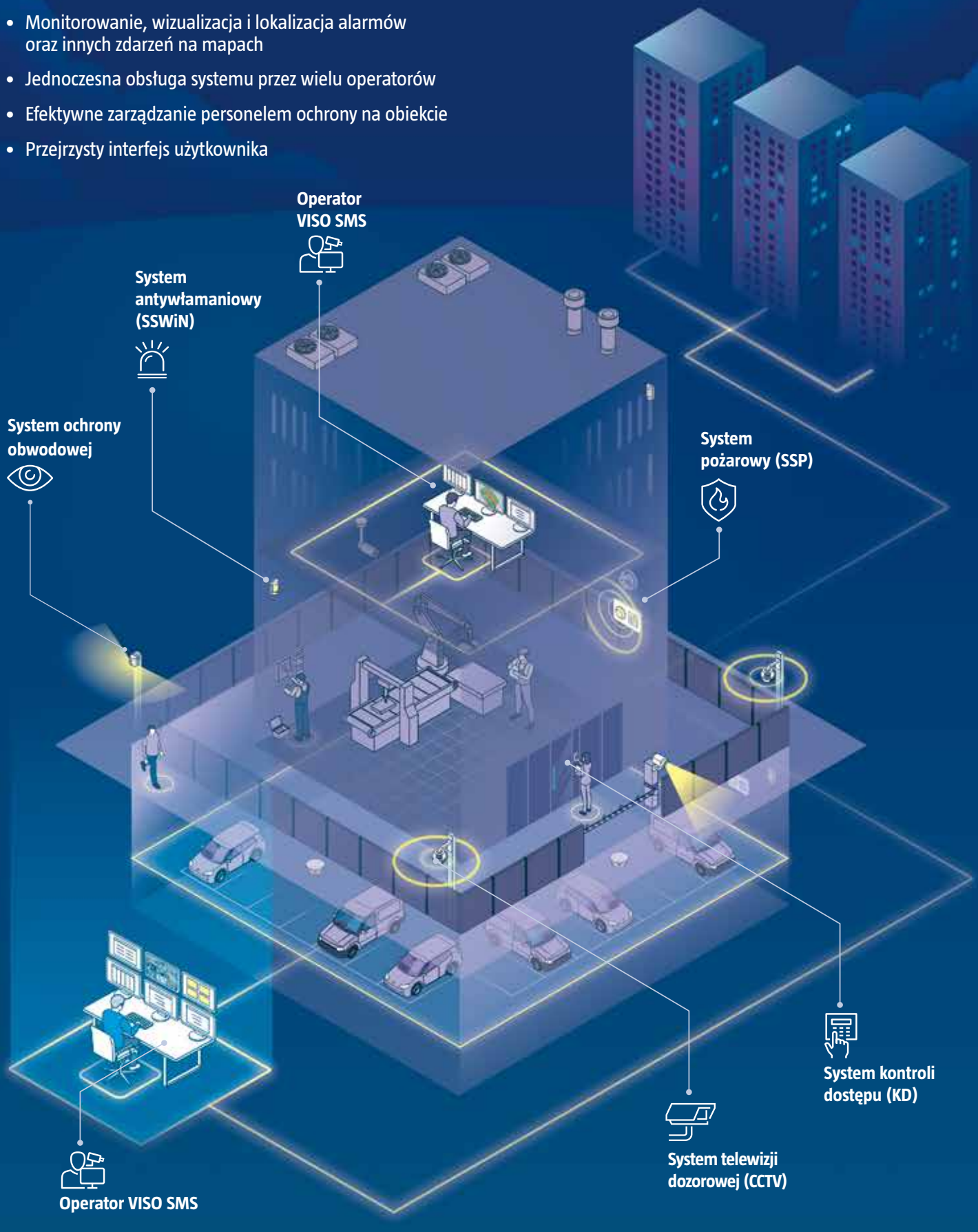


VISO SMS

Monitorowanie i wizualizacja systemów bezpieczeństwa

roger
Intelligence for Building

- Integracja z systemami Bosch, Dahua, Hikvision, Honeywell, Milestone, SATEL, Siemens i innymi w ramach jednej platformy
- Monitorowanie, wizualizacja i lokalizacja alarmów oraz innych zdarzeń na mapach
- Jednoczesna obsługa systemu przez wielu operatorów
- Efektywne zarządzanie personelem ochrony na obiekcie
- Przejrzysty interfejs użytkownika



AXIS COMMUNICATIONS

AXIS Q1961-XTE – przeciwwybuchowa kamera termowizyjna

Kamera AXIS Q1961-XTE została zaprojektowana i certyfikowana do zastosowań zagrożonych wybuchem (strefa 2,21 i klasa I/II/III, strefa 2 zgodnie z ATEX/IECEx/cULus).

Atrakcyjna cenowo kamera jest kompaktowa i lekka, obsługuje technologię PoE, co zapewnia łatwą i elastyczną instalację. Kamera ma obiektyw o średnicy 7 mm, który pozwala na pokrycie szerokiego obszaru. Elektroniczna stabilizacja obrazu (EIS) umożliwia płynną rejestrację obrazu wideo nawet w scenach, gdzie występują drgania. Co więcej, ta solidna kamera zapewnia stopień ochrony IP66 i IP67, co gwarantuje ochronę przed wnikaniem wody i kurzu. Axis Edge Vault, sprzętowa platforma cyberbezpieczeństwa, chroni urządzenie i wrażliwe dane przed nieautoryzowanym dostępem.

AXIS Q1961-XTE może mierzyć temperaturę w zakresie od -40°C do 350°C. Wysyła powiadomienie, jeśli temperatura przekroczy albo spadnie poniżej ustawionego progu lub wzrośnie/spadnie zbyt szybko, co może wskazywać, że sprzęt jest bliski przegrzania lub w układzie występuje nieszczelność. Obsługuje do 10 konfigurowalnych wielokątnych obszarów detekcji. Można ją zintegrować z systemami kontroli procesów, dzięki czemu można stworzyć sieć sensoryczną opartą na danych i uzyskać głębszy wgląd w procesy.

Dzięki inteligentnemu filtrowaniu może ignorować określone gorące obiekty, takie jak ciepłe rury wydechowe przejeżdżających pojazdów roboczych, a to oznacza mniej fałszywych powiadomień. Najnowocześniejsza technologia umożliwia podłączanie np. głośników sieciowych, co pozwala na aktywację alarmów dźwiękowych.

Więcej na: www.axis.com/pl-pl

BCS

BCS-L-EIP242FR3-TH-AI(0202)

BCS-L-EIP242FR3-TH-AI(0202) 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 30 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 umożliwia wykrycie korzystania z telefonu komórkowego w miejscach, gdzie jest to zabronione.

Moduł termowizyjny to przetwornik mikrobolometryczny z aktywnym materiałem pochłaniającym w postaci tlenku wanadu Vox. Ma on rozdzielczość 256×192. Obiektyw o ogniskowej 2 mm zapewnia wykrywanie osób w odległości nawet 80 m. Zaletą modułu jest obserwacja termiczna, co idealnie sprawdza się jako funkcja alarmowa ostrzegająca o pojawieniu się zarzewia pożaru, pozwalając ugasić go, zanim ten się rozprzestrzeni.

Niezależnie od tego, na którym module wystąpi alarm, zostaje uruchomione powiadomienie optyczno-akustyczne dzięki wyposażeniu BCS-L-EIP242FR3-TH-AI(0202) w ostrzegawcze diody LED i wbudowany głośnik. Do sygnalizacji lub odbierania alarmów można również wykorzystać moduł wejść/wyjść alarmowych.

Więcej na: www.bcs.pl

HANWHA VISION

Kompaktowy rejestrator AI z dyskiem półprzewodnikowym

XRN-426S-1T jest kompaktowym rejestratorem NVR o rozdzielczości do 4K i wbudowanym dyskiem półprzewodnikowym (SSD) o pojemności 1 TB. Po zintegrowaniu z kamerami Hanwha Vision AI umożliwia wyszukiwanie AI. Oferuje cichą i niezawodną pracę dzięki zastosowanemu dyskowi półprzewodnikowemu zamiast tradycyjnego dysku twardego.

Kompaktowy rozmiar urządzenia (20 x 14 cm) zapewnia dużą elastyczność i wszechstronność zastosowań w miejscach o ograniczonej przestrzeni, np. korytarzach, holach, punktach informacyjnych, obszarach mieszkalnych i mniejszych obiektach handlowych.

Dzięki swojej konstrukcji XRN-426S-1T jest cichy, a do chłodzenia urządzenia nie jest potrzebny wentylator. Ponadto rejestrator jest wyposażony w szeroką gamę opcji instalacji, w tym uchwyt Vesa do montażu z tyłu monitora.

Wyszukiwanie metadanych za pomocą sztucznej inteligencji ułatwia operatorom wyszukiwanie i przeglądanie nagrań. Można nimi zarządzać w trakcie zdarzenia, a także w celu przeprowadzenia dochodzeń po nim. W przypadku wystąpienia zdarzenia rejestrator może uruchomić działanie w oparciu o wstępnie zdefiniowane reguły, takie jak wysyłanie wiadomości e-mail lub powiadomień mobilnych typu push.

Materiał wideo można przeglądać za pomocą aplikacji Wisenet Mobile lub Wisenet Viewer, co zapewnia operatorom elastyczność w zakresie dostępu do nagrań i zarządzania nimi. Intuicyjny i spersonalizowany wyświetlacz umożliwia łatwe przybliżanie szczegółów, a funkcja prostowania obrazu *fisheye* gwarantuje wyraźny obraz bez zniekształceń.

Więcej na: www.hanwhavision.eu/pl/

camect

INTELIGENTNY HUB
efektywna i skuteczna detekcja zagrożenia

SZTUCZNA INTELIGENCJA
wbudowana, zaawansowana sztuczna inteligencja

ROZRÓŻNIA PONAD 30 TYPÓW OBIEKTÓW
ludzi, pojazdy, zwierzęta

WSPÓŁDZIAŁANIE
z różnymi kamerami IP

KOMPATYBILNOŚĆ
z SAFESTAR

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

Technologia AcuSearch w nowych rejestratorach serii NXI-K

Rejestratory NVR z serii NXI-K wyposażono w bardziej intuicyjny interfejs EUI i nowe funkcje. Poza wykrywaniem twarzy czy ochroną perymetryczną i detekcją ruchu 2.0, dzięki którym użytkownik otrzymuje znacznie mniej fałszywych alarmów, przeszukiwanie nagrań wideo jest o wiele szybsze i prostsze.

Dodatkowo w rejestratorze zaimplementowano nową technologię AcuSearch wykorzystującą zaawansowane algorytmy AI do wyszukiwania danych w materiale zarejestrowanym (dotychczas było to możliwe w czasie rzeczywistym). Metadane z kamer, które poddawane są obróbce w rejestratorze, umożliwiają prostsze, szybsze i bardziej wydajne wyszukiwanie. Wystarczy na nagraniu zaznaczyć ramką interesujący cel lub obszar i uruchomić proces szukania. Dzięki systemowi znakowania metadanych i szybkiego indeksowania użytkownik otrzymuje interesujące fragmenty materiału dosłownie w kilka sekund.

Rejestratory serii NXI-K można powiązać z aplikacją Hik-Connect, co pozwala zdalnie monitorować pracę całego systemu monitoringu, jak również korzystać z zaawansowanego wyszukiwania celu (człowiek/pojazd) w nagranym materiale.

Rejestratory serii NXI-K współpracują z przełącznikami sieciowymi Hikvision serii smart-manage. Wspólny protokół niskopoziomowej wymiany danych oferuje nadzór i zarządzanie warstwą IT ochrony technicznej. Dzięki takiemu połączeniu uzyskuje się nie tylko możliwość weryfikacji stanu urządzeń, lecz także powiadamianie o zdarzeniach w sieci IP w czasie rzeczywistym.

Więcej na: www.hikvision.com/pl

LINC POLSKA

Aura Ai-XS – ochrona obwodowa na miarę twojego obiektu

Technologia światłowodowa, jako medium transmisyjne, zyskuje na popularności. Australijska firma Future Fibre Technologies (FFT) opracowała system Aura Ai-XS, w którym światłowód jest stosowany w roli czujnika wykrycia wtargnięć.

Rozwiązanie to z wyjątkową precyzją i niezawodnością pozwala zabezpieczyć obszar o długości do 10 km. System oferuje wiele możliwości. Korzystając z algorytmów głębokiego uczenia, skutecznie zmniejsza wskaźnik niechcianych alarmów (NAR), przy jednoczesnej wysokiej dokładności klasyfikacji zdarzeń (POD).

Konfiguracja systemu Aura Ai-XS jest niezwykle prosta i szybka, dzięki czemu czas wdrożenia jest krótki. Podobne tradycyjne systemy wymagają większych nakładów inwestycyjnych, co wpływa na wzrost kosztów i wydłuża terminy realizacji projektów.

Zalety Aura Ai-XS to:

- Jednoczesna detekcja w czasie rzeczywistym na dwóch kanałach (czujniki światłowodowe montowane na ogrodzeniu obejmują odległość do 10 km, po 5 km na kanał, zwiększając bezpieczeństwo).
- Dokładność wykrycia próby wtargnięcia w promieniu +/- 2 m.
- Iskrobezpieczeństwo i odporność na zakłócenia elektromagnetyczne (RMI) i radiowe (RFI).
- Cyberbezpieczeństwo, dzięki testom penetracyjnym firm zewnętrznych i zgodności z STIG.
- Niezawodność przy MTBF wynoszącym ponad 250 tys. godz.

Portfolio FFT obejmuje również sterowniki o większym zasięgu detekcji, nawet ponad 100 km!

Więcej na: www.linc.pl

TP-LINK

Panele solarne z serii VIGI

TP-Link poszerza portfolio urządzeń z serii VIGI o rozwiązania do skutecznego i niezawodnego monitoringu na terenach pozbawionych dostępu do sieci elektrycznej, takich jak place budowy czy tereny leśne. Na rynku debiutują dwa panele solarne VIGI SP9030 i VIGI SP6020.

Model SP9030 to panel fotowoltaiczny o mocy 90 W z baterią litową 31,2 Ah/10,8 V. Z kolei VIGI SP6020 wyposażono w panel o mocy 60 W i baterię litową 20,8Ah/10,8 V. Oba urządzenia charakteryzują się konstrukcją modularną, przeznaczoną do pracy na zewnątrz (klasa szczelności IP66), z możliwością regulacji kąta nachylenia panelu. Wyposażono je w wydajne panele słoneczne klasy A o sprawności konwersji 21,6% i żywotności wynoszącej ponad 25 lat. Zastosowany kontroler ładowania MPPT *(Maximum Power Point Tracking)* optymalizuje moc panelu słonecznego, obniża straty energii i zwiększa wydajność ładowania o 20% w porównaniu z kontrolerami PWM *(Pulse Width Modulation)*. Z kolei wbudowana bateria z technologią inteligentnego ogrzewania pomocniczego zapewnia jej normalne działanie w szerokim zakresie temperatur.

Modele SP9030 i SP6020 cechuje również prosty montaż i intuicyjne zdalne zarządzanie poprzez aplikację. Dzięki trzem gniazdkom zasilającym do każdego z paneli można podłączyć trzy urządzenia, takie jak kamery czy most bezprzewodowy Wi-Fi (np. model TP-Link EAP211-Bridge KIT) i w ten sposób utworzyć radiowe połączenie sieciowe z oddaloną siedzibą główną firmy.

Panele solarne z serii VIGI zostały objęte 3-letnią gwarancją producenta.

Więcej na: www.tp-link.com/pl

Linc
Polska Sp. z o.o.

TOWER®

TAM GDZIE STANDARDOWE ZABEZPIECZENIA SIĘ
NIE SPRAWDZAJĄ TAM JESTEŚMY MY.

Mobilne rozwiązania do ochrony

WŁASNE ZASILANIE

MULTISPEKTRALNOŚĆ

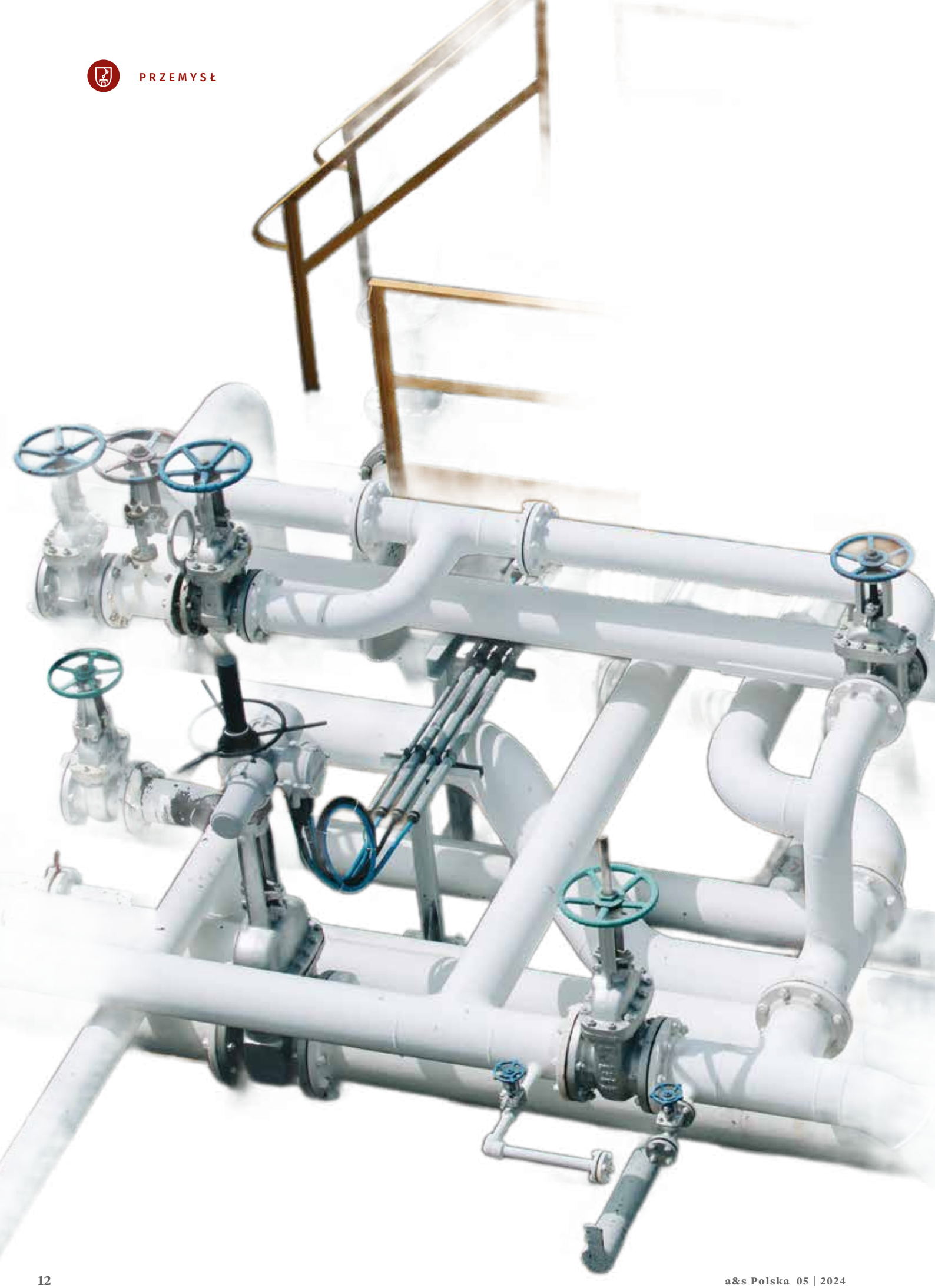
NIEZALEŻNOŚĆ

OSZCZĘDNOŚĆ

WYTRZYMAŁOŚĆ

BEZPIECZEŃSTWO
DOSTĘPU

www.linc.pl



Bezpieczeństwo w przemyśle
Obraz rynku

Tyle o sobie wiemy, ile nas sprawdzono. Prób przetestowania odporności firm jest wiele, a będzie jeszcze więcej. Podmioty z branży przemysłu mają szczególnie wiele do stracenia, dlatego też podejmują zróżnicowane działania zabezpieczające. Czy to wystarczy?

Adela Prochyra

Nie odkryjemy Ameryki stwierdzeniem, że bezpieczeństwo w przemyśle to szerokie pojęcie. Tak jak na przemysł składa się pewna liczba elementów, tak jego bezpieczeństwo obejmuje różne rodzaje zabezpieczeń. To przede wszystkim wszelkie działania mające na celu ochronę zdrowia i życia pracowników, zabezpieczenie mienia oraz systemów zapewniających ciągłość produkcji, w tym także bezpieczeństwo pożarowe, ochrona środowiska i cyberbezpieczeństwo.

Drugi truizm, niezbędny jednak dla przedstawienia aktualnej sytuacji, jest taki, że skala zagrożeń w ostatnich latach znacznie się zwiększyła. Bezpieczeństwo stało się więc obszarem, który rozwija się dynamicznie jak żadna inna branża i w związku z tym wymaga ciągłego doskonalenia oraz dostosowywania do zmieniających się warunków technologicznych i prawnych. Przemysł nie jest od tych zagrożeń wolny, wręcz przeciwnie – przedsiębiorstwa należące do tak kluczowego sektora gospodarki powinny być przygotowane na nieprzewidywalne warunki klimatyczne, ale także wszelkiego rodzaju ataki. Czy są? O tym właśnie jest nasz raport.

→

» Pandemie, wojny, powodzie i inne zagrożenia coraz częściej się materializują. Ciągłość działania zaczyna wysuwać się na pierwsze miejsce, a ciągłość łańcucha dostaw jest jednym z jej głównych elementów «

Jarosław Durkacz, Polpharma

Normy, dyrektywy, regulacje nie dla każdego

Zacznijmy od obrazu ogólnego. Organy Unii Europejskiej stale wprowadzają nowe regulacje prawne, a także formułują normy i zalecenia, które mają pomóc zachować pewien porządek w coraz bardziej komplikującej się rzeczywistości. Te rozliczne procedury mają oczywiście zaspokoić także wiele innych celów. Jakich dokładnie, to temat na dłuższą rozprawę. Jeśli zaś chodzi o cele, które są dobrze znane, dużą wagę przykłada się ostatnio do kwestii środowiskowych – tu wymienimy chociażby liczne zmiany zachodzące obecnie w ramach raportowania ESG, założenia programu Europejski Zielony Ład, pakiet *Fit for 55* czy cele klimatyczne na 2050 rok. Wszystkie zmiany formalne ustalone na szczeblu unijnym przekładają się na prawodawstwo i praktyki na poziomie państw, a te z kolei na wymogi wobec przedsiębiorstw, rolników itd.

Drugi obszar, który jest głównym przedmiotem naszych rozważań, to kwestia zabezpieczenia firm, instytucji oraz obiektów infrastruktury krytycznej przed cyberatakami. W tym zakresie z kolei mamy do czynienia z postanowieniami dyrektywy NIS2, której data wejścia w życie – 18 października – oznacza dla producentów wiele zmian, ale też niesie wiele niejasności (w poprzednim numerze „a&s Polska" obszernie pisał o tym Jan T. Grusznic, którego *Raport: NIS2 – już za chwileczkę, już za momencik* polecamy).

O tym, że sprawa jest poważna i rozpoznawana także na poziomie krajowym, niech świadczy fakt, że w projekcie ustawy budżetowej na 2025 rok, przedstawionym 28 sierpnia 2024 r., zaplanowano środki na cyfryzację w wysokości 1 mld 827 mln, w tym 250 mln na Fundusz Cyberbezpieczeństwa. To aż o 150% więcej niż w poprzednim roku z budżetu państwa.

Inne zaplanowane w budżecie środki przewidziane na cyberochronę to m.in. 1 mld 914 mln 964 tys. zł na cyberbezpieczeństwo i wsparcie kryptologiczne (dział Obrona narodowa), 1 mld 179 mln 730 tys. zł na Fundusze Europejskie na Rozwój Cyfrowy 2021–2027, 608 mln 8 tys. zł na Centralne Biuro Zwalczania Cyberprzestępczości oraz 414 mln 689 tys. zł na Instytut Łączności i NASK.

Te zadania to niektóre z elementów budowanej w Polsce cybertarczy RP, czyli pakietu działań realizowanych lub koordynowanych przez Ministra Cyfryzacji, mających zwiększać odporność cyberbezpieczeństwa Polski, na który w ciągu najbliższych dwóch lat łącznie będzie przeznaczonych ok. 3 mld zł (środki mają pochodzić zarówno z budżetu państwa, jak i UE). Jego kluczowe projekty obejmą:

- Wzmocnienie cyberbezpieczeństwa samorządów, w tym stworzenie Lokalnych Centrów Cyberbezpieczeństwa i wsparcie projektów Cyberbezpieczny Samorząd.
- Rozwój Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni (NASK) w celu zwiększenia zdolności wykrywania i zwalczania cyberzagrożeń.
- Modernizację Systemu S46, którego zadaniem będzie ułatwienie wymiany informacji o cyberzagrożeniach między podmiotami Krajowego Systemu Cyberbezpieczeństwa.
- Szkolenia i podnoszenie świadomości, w tym rozwój programów szkoleniowych dla pracowników administracji publicznej i obywateli.
- Usprawnienie reagowania na incydenty, automatyzacja wymiany informacji między instytucjami i regularne ćwiczenia.
- Ujednolicenie z przepisami UE: wdrożenie dyrektywy NIS2 i prace nad nową Strategią Cyberbezpieczeństwa RP.

Projekt budżetu trafił obecnie do konsultacji, ale bez względu na to, jaki kształt ostatecznie przyjmie, widać, że na poziomie krajowym świadomość zagrożeń cybernetycznych jest duża. Podejmowane są liczne działania, dzięki którym Polska ma szansę zbudować bardziej odporny system cyberbezpieczeństwa, lepiej przygotowany na współczesne zagrożenia. A co na to przemysł? Nie wszystkie firmy są bezpośrednio objęte wymogami, dlatego muszą dbać o swoje bezpieczeństwo na własną rękę.

» Dyrektywa NIS 2 miała znaczący wpływ na poziom naszych zabezpieczeń. Chociaż nasza firma nie jest bezpośrednio wymieniona w katalogu podmiotów krytycznych, to jednak wprowadziliśmy dodatkowe środki ostrożności, aby spełniać wymagania dyrektywy" «

Wincenty Ignatowski, CEMEX Polska

Przemysł 4.0. w (polskiej) praktyce

W Polsce dochodzi codziennie do co najmniej kilkuset incydentów o charakterze cyberataków, a bywa, że liczba ta sięga dwóch tysięcy, jak w czerwcu br. podał w rozmowie z gazetą „Polska" minister cyfryzacji Krzysztof Gawkowski. Pod koniec maja stwierdził wręcz, że „Polska jest na cybernetycznej zimnej wojnie", co podtrzymało MON, podając, że liczba ataków na systemy związane z obronnością Polski zwiększyła się pięciokrotnie od momentu wybuchu wojny Rosji z Ukrainą. Od roku 2022 liczba ataków co roku się podwaja. Nasilały się one zwłaszcza przed wyborami: parlamentarnymi i europarlamentarnymi, ale próby destabilizacji państwowości na każdym jej poziomie pojawiają się stale. Celami są zarówno administracja publiczna (49%, źródło: PAP), transport (20%, źródło: PAP), lotnictwo, energetyka i obronność (12%, źródło: PAP), służba zdrowia, obiekty infrastruktury krytycznej, jak i gospodarka.

Przeciętny koszt takiego ataku jest dla firmy bądź organizacji kolosalny, a usuwanie skutków trwa zwykle dni lub tygodnie, nie mówiąc o odbudowaniu zaufania klientów i kontrahentów. Po drugiej stronie barykady jest niewielki koszt poniesiony na przygotowanie oprogramowania *ransomware*. Jak podaje Jan T. Grusznic w swoim raporcie, wystarczy ok. 320 dol., aby przeprowadzić tygodniowy atak DDoS na aplikację internetową, który może sparaliżować przedsiębiorstwo.

Luka cyfrowa czy gęste usieciowienie?

Zanim przejdziemy do kwestii faktycznych zabezpieczeń stosowanych przez firmy, zadajmy sobie pytanie, które nasuwa się w kontekście cyberataków w przemyśle: Jak właściwie wygląda usieciowienie tego sektora? Na ile idee Przemysłu 4.0 (głęboka integracja cyfrowych technologii z procesami produkcyjnymi i nieograniczone możliwości komunikacyjne na linii: człowiek – urządzenie – Internet – technologie informacyjne) zostały wdrożone w polskich przedsiębiorstwach produkcyjnych? Czwarta rewolucja przemysłowa to inteligentna automatyzacja, gdzie maszyny i systemy są w stanie komunikować się ze sobą, uczyć się i podejmować samodzielne decyzje. Miała ona zwolnić człowieka ze żmudnej, powtarzalnej pracy i uwolnić jego kreatywność, a firmom dać nowe możliwości rozwoju i przewagę konkurencyjną. Polski Fundusz Rozwoju w 2024 r. przeprowadził Test Dojrzałości Cyfrowej, którego wyniki zawarł w raporcie „Kondycja cyfrowa polskich firm i gospodarki". Punktem wyjścia do analizy poziomu cyfryzacji polskich przedsiębiorstw był wskaźnik DII (*Digital Intensity Index*), który klasyfikuje przedsiębiorstwa na podstawie poziomu wykorzystania technologii cyfrowych. W roku 2023 jedynie 21,2% polskich przedsiębiorstw wykazało się wysokim lub bardzo wysokim poziomem cyfryzacji, co dało Polsce 21. miejsce w rankingu państw Unii Europejskiej. Podobny poziom ucyfrowienia (21-22%) prezentują Francja, Portugalia, Łotwa, Czechy. Dla porównania w Finlandii odsetek ten sięga 51,9%, a w Holandii 47,6%.

Z kolei raport EY *Czy Twój biznes zanurzył się w cyfrowej transformacji, czy tylko powierzchownie dotknął jej możliwości? Transformacja Cyfrowa 2024* wskazuje: „Transformacja cyfrowa w polskich przedsiębiorstwach jest na wysokim lub bardzo wysokim etapie zaawansowania – łącznie 64% firm" oraz „Transformacja cyfrowa ma wysoki lub bardzo wysoki priorytet wśród polskich przedsiębiorstw (84%)", a na jej realizację przeznaczane jest nawet do 10% rocznego przychodu. Należy uściślić, że bardzo wysoki odsetek cyfryzacji to domena dużych firm (20%), co pokrywa się z wnioskami Testu Dojrzałości Cyfrowej. Ten raport, w przeciwieństwie do raportu PFR, przynosi natomiast wnioski skłaniające do sceptycyzmu, jeśli chodzi o opłacalność zaawansowanych technologii. „Aż 54% badanych firm stwierdziło, że założenia dotyczące wzrostu przychodów wynikających z transformacji cyfrowej nie zostały spełnione nawet w 35%" – podano we wnioskach kluczowych. Kwestia obniżenia kosztów poprzez automatyzację zeszła w związku z tym na plan dalszy, przedsiębiorcy od rozwiązań cyfrowych oczekują dziś przede wszystkim nowych możliwości rozwoju. Wdrażają je także w działach obsługi klienta, sprzedaży i jako analitykę w działach IT/OT. Co ciekawe, „firmy w ramach transformacji cyfrowej najczęściej inwestują w cyberbezpieczeństwo, które jest fundamentem usług IT, rozwiązania chmurowe oraz szkolenia dla pracowników z kompetencji cyfrowych". Bez względu jednak na motywację i wskaźniki zwrotu z inwestycji w cyfryzację wygląda na to, że ten trend utrzyma się jeszcze przez długi czas. Nowe technologie będą coraz powszechniejsze w firmach, a te będą przez to narażone na ataki, wyciek danych itp.

» W każdej firmie istnieje ryzyko wycieku danych wrażliwych" «
Paweł Wawryła, AIRA

Czy przedsiębiorstwa są zabezpieczone?

Na początek zapytaliśmy security managerów o to, jaki jest poziom świadomości osób decyzyjnych w ich przedsiębiorstwach, jeśli chodzi o zagrożenie cyberatakiem. Większość odpowiedzi wskazuje na wysoki i bardzo wysoki poziom takiej świadomości: w 10-stopniowej skali określali go najczęściej jako „8". To z jednej strony naturalny efekt codziennej ciężkiej pracy „bezpieczników". Jest to wynik regularnych szkoleń i kampanii informacyjnych, które mają na celu zwiększenie świadomości na temat zagrożeń cybernetycznych, jak mówi nam Wincenty Ignatowski z CEMEX POLSKA, ale i zmieniającego się otoczenia, w jakim funkcjonują przedsiębiorstwa. Paweł Wawryła z firmy AIRA potwierdza, że zdecydowanie świadomość zwiększa się każdego roku, ze względu na liczbę coraz to nowych ataków odnotowanych w organizacjach. W każdej firmie istnieje ryzyko cyberataku, wycieku danych wrażliwych, dlatego poszczególne przedsiębiorstwa nie muszą doświadczać ich na własnej skórze, żeby podjąć działania zapobiegawcze. W tym przypadku nie do końca ma zastosowanie powiedzenie: „Mądry Polak po szkodzie" – świadomość sytuacji jest tak duża, że zabezpieczają się nawet te firmy, które nie doświadczyły prób włamania na serwery lub innego rodzaju cyberataku. Wymieniano szereg zróżnicowanych działań, które łącznie mają zabezpieczyć firmę przed stratami zarówno materialnymi, jak i wirtualnymi. Od identyfikacji słabych punktów przez kontrolę odporności partnerów, kontrahentów, dostawców, podwykonawców w ramach łańcucha dostaw:

» Wprowadziliśmy liczne szkolenia oraz symulacje ataków, takie jak gra symulacyjna Atak Ransomware, która pomogła nam zidentyfikować słabe punkty w naszych systemach i procedurach «

Wincenty Ignatowski

» Mamy opracowany cały proces weryfikacyjny dostawców oraz przyjęte normy, które dostawca musi spełnić przed rozpoczęciem z nami współpracy «

Paweł Wawryła

Wagę tego elementu na checkliście zabezpieczeń podkreślił Jarosław Durkacz, ekspert ds. organizacji bezpieczeństwa POLPHARMA:

» Wyzwania, które same w sobie stały się wyznacznikiem naszych czasów, mocno spopularyzowały proces kontroli kontrahentów lub potencjalnych kontrahentów. Ciągłość łańcucha dostaw zajmuje szczególne miejsce na takiej checkliście kontrolnej. Umiejętność reakcji na zdarzenia oraz przewidywania zagrożeń, jakie mogą wystąpić w tym obszarze, jest bardzo pożądana. Dlatego odporność w zakresie łańcucha dostaw staje się jedną z kluczowych cech, jakiej poszukujemy po drugiej stronie przed nawiązaniem współpracy. Krytyczność tej cechy maksymalizuje fakt, że liczba czynników zewnętrznych, które mogłyby wpłynąć na ten obszar, stale rośnie «

Ze względu na delikatną naturę zagadnienia nasi rozmówcy nie wymieniali dokładnych rodzajów podejmowanych przez siebie działań i zabezpieczeń. Podkreślali jedynie wagę stałego działania na rzecz utrzymania bezpieczeństwa pracowników i klientów, a także sprawdzania swoich kontrahentów pod kątem zgodności z ich wewnętrznymi standardami bezpieczeństwa. To inicjatywy zarówno własne, jak i wymuszone przez nowe przepisy.

» Dyrektywa NIS 2 była tylko dodatkowym impulsem do przeprowadzenia audytu bezpieczeństwa używanych przez nas systemów. Dzięki wcześniej przyjętej polityce, którą kierowaliśmy się przy wyborze rozwiązań, tj. bezpieczeństwo zawsze na pierwszym miejscu, nasze systemy są zaawansowane i zgodne z obowiązującymi normami i regulacjami «

Paweł Wawryła

Przezorny zawsze ubezpieczony? Ubezpieczenie od cyberataku to kolejne działanie podejmowane przez przedsiębiorstwa, aby chronić je przed potencjalnymi stratami finansowymi i utratą reputacji, chociaż nie jest to bardzo powszechne rozwiązanie.

Cybernetyczny wyścig zbrojeń

Wygląda na to, że firmy, a zwłaszcza te duże, o międzynarodowym zasięgu, jasno zdają sobie sprawę z zagrożeń, jakie niesie cyfryzacja. To najczęściej te firmy są na wysokim i bardzo wysokim poziomie transformacji cyfrowej, na którą najczęściej przeznaczają odczuwalną część swoich budżetów. Znają więc ryzyka, które się z tym wiążą. Stąd w ich codziennej agendzie znajdują się liczne działania, które z różnych stron mogą pomóc uchronić przedsiębiorstwo przed cyberatakiem i wyciekiem danych. To m.in. audyty wewnętrzne i symulacje ataków, wyśrubowane standardy bezpieczeństwa, których spełnienia oczekują także od swoich kontrahentów, badanie odporności partnerów, wybór zaawansowanych systemów, a także ubezpieczenie od cyberataków. Wejście w życie dyrektywy NIS 2 można by potraktować jako swoisty papierek lakmusowy tych przygotowań. Jednak wobec zamieszania towarzyszącego jej wprowadzeniu i wielu niejasności odnośnie do tego, które dokładnie firmy będą nią objęte i jakie dokładnie wymogi trzeba będzie w związku z tym spełnić, ten test okazał się niemiarodajny, a firmy rozpoczęły przygotowania na własną rękę. •

Nie trzeba ustawy, by rozpoznać sabotaż

W grudniu ubiegłego roku krajowe media poinformowały o skazaniu kilkunastu obywateli Ukrainy, Białorusi i Rosji za szpiegostwo na rzecz Rosji. Oskarżeni dobrowolnie poddali się karze, z czego można wnioskować, że organy ścigania zebrały niebudzący wątpliwości materiał dowodowy, więc oskarżeni nie mieli wielkiego wyboru. Mogłoby się wydawać, że sprawa dotyczy obronności, ale czy jedynie?

Jacek Grzechowiak

Od tego czasu w mediach częściej niż zwykle zaczęły się pojawiać słowa „sabotaż" i – nieco rzadziej – „dywersja". Co więcej, znalazły się one także w wypowiedziach najwyższych urzędników państwowych z premierem i ministrem spraw wewnętrznych i administracji, będącym jednocześnie koordynatorem służb specjalnych, na czele. Dodatkowo w wypowiedziach polityków (pierwszy chyba był tu premier) pojawiają się apele o czujność, w tym także ze wskazaniem „komercyjnych służb ochrony" jako tych, które tę czujność powinny zachowywać.

Oni z kolei chętnie są cytowani przez dziennikarzy i komentatorów naszego życia biznesowego, co sprawia, że tematem tym żyją już niemal wszyscy. Ta wrzawa spowodowała, że koncentrujemy się na samych aktach sabotażu, a nie całym związanym z nim ryzykiem.

Przyjrzyjmy się zatem dokładnie konkretnemu wydarzeniu. Spójrzmy więc na wszystkie „trzy strony medalu". Popatrzmy, co robiły osoby skazane za szpiegostwo. Zobaczmy, co robią pracownicy ochrony, co mogą robić, wreszcie co powinni robić. Spójrzmy na całe otoczenie, z którego przecież także dociera do nas wiele sygnałów.

Jak wynika z sentencji wyroku, skazani zbierali informacje dotyczące obiektów infrastruktury krytycznej. Obserwowali m.in. lotniska, dworce kolejowe, porty oraz terminal na polsko-ukraińskim przejściu granicznym. I choć wszystko to są obiekty, które zwłaszcza obecnie pełnią kluczową funkcję w zaopatrzeniu walczącej armii ukraińskiej, to jednak są to obiekty infrastrukturalne, wykorzystywane nie tylko na potrzeby wojska. Dziennik „The Washington Post" poinformował, że zwerbowani agenci otrzymali także zadania instalowania kamer wzdłuż linii kolejowych, a nawet umieszczania lokalizatorów GPS w ładunkach wojskowych. Amerykańskie służby

→

specjalne ostrzegały, że Rosja może podejmować próby sabotowania obiektów logistycznych na terytorium NATO, czyli także w Polsce.

Z jeszcze innej informacji prasowej dowiadujemy się, że do hotelu sejmowego wszedł w sposób nieuprawniony mężczyzna z rosyjskim paszportem. Pojawiły się informacje o podłożeniu ładunków wybuchowych przy rurociągu NATO w Niemczech. Mamy wreszcie szereg danych o podpaleniach. Zarówno w Polsce, jak i np. na Litwie. Jest ich dużo, a dodatkowo ich kontekst sprawia, że obecnie każde podpalenie od razu jest przedstawiane jako sabotaż rosyjskich służb specjalnych. Tak zapewne nie jest, ale mamy tu zdecydowany deficyt jakości informacji, bo o ile wypowiedzi, zwłaszcza ministra spraw wewnętrznych, są wyważone, ostrożne i dość precyzyjne, o tyle tzw. komentatorzy pozwalają sobie nawet na niefrasobliwość. Przykładem może być sprawa aresztowania sprawcy usiłowania podpalenia wrocławskiej fabryki, które w jednym z mediów ogólnopolskich zostało przedstawione jako pożar. Podobnie jest z pożarami w niemieckiej fabryce produkującej m.in. uzbrojenie przeciwlotnicze. Media niemieckie przedstawiły to, a zwłaszcza pierwszy pożar w oddziale berlińskim, bardzo rzeczowo. U nas nagłówki zaczynały się od nazwy systemu przeciwlotniczego, a treść koncentrowała się na aspekcie militarnym i – tu już naturalnie – na potencjalnym sabotażu. Pierwszy pożar (Berlin) faktycznie ma wiele znaków zapytania. Wystąpił w strefie zastrzeżonej, z kontrolowanym dostępem. Był wyjątkowo gwałtowny i połączony z emisją szkodliwych substancji. Drugi (Troisdorf – Nadrenia Północna-Westfalia) wydarzył się z prozaicznych powodów.

Nie inaczej jest z najnowszym incydentem znanym publicznie, a mianowicie dewastacją maszyn służących do wierceń geologicznych w firmie LKAB (Luossavaara-Kiirunavaara Aktiebolag, LKAB – szwedzkie przedsiębiorstwo wydobywcze z siedzibą w Luleå) w Szwecji. Według dziennikarzy sprawcy przecięli węże doprowadzające wodę i opony oraz ukradli paliwo. I ponownie media od razu napisały o sabotażu, co wiele osób zaczęło powtarzać. Mając jednak więcej informacji, dochodzimy do wniosku, że możliwe są także inne przyczyny i motywy działania sprawców.

Igrzyska olimpijskie i atak na francuską kolej dużej prędkości w dniu jej otwarcia dolały jeszcze oliwy do ognia. To było spektakularne wydarzenie właśnie z uwagi na olimpiadę, ale przecież tych przypadków było znacznie więcej. Przykładem może być sabotaż na Deutsche Bahn, kiedy to dokonano fizycznej ingerencji w infrastrukturę tego operatora infrastruktury kolejowej, wstrzymując operacje kolejowe w dużej części Niemiec. Podobnie wyglądała sytuacja dotycząca mostu kolejowego w Tczewie, który został wyłączony z użytkowania po ujawnieniu tam atrapy ładunku wybuchowego – co stwierdzili dopiero saperzy. Jak donoszą branżowe media, zatrzymanie ruchu kolejowego w Tczewie niemal zdemolowało ruch pociągów w całej Polsce. Natomiast w Czechowicach-Dziedzicach na torach kolejowych znaleziono prawdziwy granat moździerzowy.

Mamy więc nad czym rozmyślać, ale przede wszystkim mamy nad czym pracować.

Ustawa – czym jest sabotaż

Nie ulega wątpliwości, że nasz biznes, zwłaszcza bazujący na infrastrukturze krytycznej, może ucierpieć w wyniku sabotażu. To składnia do wniosku, że pracownicy ochrony, ich kompetencje i świadomość w zakresie bezpieczeństwa mają kluczowe znaczenie. I agencje ochrony powinny być tu kluczowym ogniwem, a ich pracownicy powinni rozumieć kwestie zagrożeń sabotażowych i dywersyjnych, ale…

No właśnie, najczęściej słyszę „Działamy, bazując na ustawie o ochronie osób i mienia, a w ustawie próżno szukać sabotażu i dywersji…". Czy na pewno?

Ustawa koncentruje się oczywiście na ochronie osób i mienia, ale czytając definicję ochrony mienia, stanowiącą, że są to „…działania zapobiegające przestępstwom i wykroczeniom przeciwko mieniu, a także przeciwdziałające powstawaniu szkody wynikającej z tych zdarzeń oraz niedopuszczające do wstępu osób nieuprawnionych na teren chroniony…", znajdujemy tam odniesienie do sabotażu i dywersji. Co prawda odniesienie niebezpośrednie, ale ono jest.

Zarówno kradzież, jak i zniszczenie czy dewastacja mogą być elementem sabotażu i dywersji, bo przecież ewentualny sabotaż będący

> *» Zarządzanie bezpieczeństwem w dzisiejszych czasach wymaga częstszego analizowania stanu bezpieczeństwa oraz symptomów zagrożeń, niż to miało miejsce w czasach spokojnych, a pracownicy powinni mieć stały dopływ informacji o zagrożeniach, także tych związanych z sabotażem i dywersją. «*

następstwem kradzieży, zniszczenia czy dewastacji mienia w określonych sytuacjach można identyfikować jako szkodę wynikającą z przestępstwa przeciwko mieniu. Kiedy w grudniu 2022 r. media pokazały, jak „sławny" człowiek-choinka wchodzi przez ogrodzenie na teren hurtowni mięsa w Warzymicach (woj. zachodniopomorskie) i przebija opony w ponad 20 pojazdach, niewiele osób pomyślało, że to sabotaż. Następnego dnia okazało się, że choć wartość opon jest znaczna, to jednak podstawowym problemem jest zatrzymanie działalności operacyjnej. A kiedy rok wcześniej mieszkaniec powiatu żagańskiego rozbił młotkiem panele fotowoltaiczne oraz inne urządzenia, straty oszacowano na 322 tys. zł. Mężczyzna usłyszał zarzut zniszczenia mienia o znacznej wartości, ale trzeba sobie zadać pytanie, czy w tym przypadku chodziło wyłącznie o zniszczenie mienia. W końcu przynajmniej częściowo zatrzymano produkcję energii elektrycznej.

A więc kradzież, niszczenie, dewastacja mienia może być elementem sabotażu i dywersji.

Dokładnie tak samo będzie z wejściem na teren bez upoważnienia. Aby dokonać sabotażu czy dywersji w wersji fizycznej, niezbędne jest wejście na określony teren. Jakże często spotykamy się z dowcipami robionymi ochronie. Jeden z takich przypadków sprzed lat: pracownik w miejsce swojej fotografii nakleił na identyfikator zdjęcie Shreka. Być może był to głupi żart, a być może było to testowanie czujności ochrony… A jak często mamy do czynienia z pożyczaniem kart SKD? To też nasza powszedniość, prawda? Wreszcie, jak często ktoś „uczynny" pomaga nam wejść do strefy zastrzeżonej, bo mamy obie ręce zajęte, trzymając dokumenty i kubek z wodą? A przecież wszystko to sprowadza się do umożliwienia wstępu osobom nieuprawnionym na teren chroniony. A co jest celem ochrony mienia? Właśnie niedopuszczenie do wstępu osób nieuprawnionych na teren chroniony.

Widać wyraźnie, że ochrona mienia poprzez niedopuszczenie do wstępu osób nieuprawnionych na teren chroniony też może być ochroną przed sabotażem i dywersją.

Inny przykład, tym razem z jednego z Security Forum. Pod obiekt podjeżdża samochód. Parkuje naprzeciwko głównego wejścia. Dwóch mężczyzn siedzi wewnątrz. Odjeżdżają po kilku godzinach. I tak przez kilka dni. Co widzi ochrona? Nic. Jak później powie jeden z pracowników ochrony, „…przecież parking jest za zakładem i my za niego nie odpowiadamy…". Wszystko jasne. Ochrona uważa, że skoro nie odpowiada za parking, to automatycznie to, co tam się dzieje, jej nie dotyczy. A penetracje przestępcze? Jak widać, ochrona też może być problemem, zwłaszcza gdy funkcjonuje w myśl utartych schematów powielanych od lat metodą kopiuj-wklej.

W mojej ocenie ustawa widzi i sabotaż, i dywersję, choć wymaga to od nas głębszego spojrzenia na idee związane z tym aktem prawnym i rozumienia, co się dzieje wokół nas, bo w bezpieczeństwie *constans* nie istnieje.

Powszechnie dostępne dane wskazują, że przez nasz kraj transportowane jest nawet 80% zaopatrzenia do Ukrainy. Nie powinnyśmy mieć złudzeń, że druga strona pozostanie obojętna. A to oznacza, że sabotaż i dywersja naprawdę powinny być przez nas traktowane jako zagrożenia jak najbardziej rzeczywiste, aktualne i rosnące zarówno co do ilości, jak i skali występowania.

Dlatego kompetencje i świadomość zagrożeń, ale i metod przeciwstawiania się im są tak istotne. A skoro tak, to niezbędne jest odpowiednie podejście proceduralne oraz szkoleniowe. W czasach, w których przyszło nam żyć, te elementy powinny przejść z modelu cyklicznego w model stały. Tym samym celowe wydaje się

> *» Nowe zagrożenia naszych czasów nie oznaczają, że stare zagrożenia znikają.«*

zapewnienie pracownikom dostępu do aktualnych informacji w tym zakresie oraz częstsze analizowanie stanu bezpieczeństwa organizacji i ich otoczenia, a także symptomów zagrożeń w nich występujących, niż to miało miejsce w czasach spokojnych. Co więcej, niezbędna jest synergia pomiędzy agencjami ochrony a ich klientami. Jest powiedzenie „mówimy tym samym językiem" albo „rozumiemy się bez słów". I to właśnie wydaje się kluczem do efektywności. Taki językowy Master Key jest dziś niezbędny. Pracownik non-security widzi symptom i powiadamia pracownika security. I na odwrót, pracownik ochrony widzi symptom zagrożenia i przekazuje właściwemu pracownikowi klienta, aby ten wykorzystał to w bezpieczeństwie swojego procesu. Aby jednak to mogło zaistnieć, agencja ochrony musi nauczyć tego języka pracowników swojego klienta. I *vice versa,* klient musi nauczyć swojego języka pracowników ochrony.

Takie synergiczne działanie wymaga działania wspólnie i w porozumieniu. Różne symptomy, widziane z różnej perspektywy mogą doprowadzić do wspólnego wniosku, ale to wymaga umiejętności rozumienia nie tylko własnych operacji (czytaj: działań ochronnych w zakresie ochrony osób i mienia) agencji ochrony, ale także rozumienia operacji klienta, czyli jego procesów nie tylko w chronionym obiekcie, ale także poza nim. I tu pojawia się kolejne pozorne ograniczenie, jakim są granice chronionych obiektów i obszarów, jak to miało miejsce w przypadku parkingu, omówionego wcześniej. Odejdźmy na chwilę od ustawy i spójrzmy przez pryzmat efektywności działań ochronnych. A ściślej mówiąc, przez model kluczowych funkcji ochrony: odstraszania, wykrywania, opóźniania i obrony *(deter, detect, delay, defend).* Czynniki te najczęściej są identyfikowane z zabezpieczeniami technicznymi, ale przecież ochrona fizyczna ma tu także wiele do zaoferowania. Pierwsze funkcje koncentrujące się na odstraszaniu i wykrywaniu to nie tylko porządne ogrodzenie (słowo „porządne" zostało użyte celowo – bo nie chodzi tylko o wysokość ogrodzenia, ale to temat na odrębny artykuł), widoczne kamery itd. To także odpowiednie działania w wymiarze ochrony fizycznej.

Odwołując się do przykładów przytoczonych wcześniej, jeśli pracownik przykleja sobie zdjęcie Shreka, a ochrona to ignoruje, to daje jasny sygnał: TU NIE MA ŻADNEJ OCHRONY. Jeśli natomiast ochrona to ujawni, to daje pierwszy sygnał: NIE PRÓBUJ. Na tym jednak nie należy kończyć. Tu właśnie pojawia się potrzeba działania synergicznego. Polega ono na reakcji także struktury non-security, czyli przełożonego i struktur HR. W tym przypadku, który znam z życia, wykonano dwa proste działania:

1. Pracownik został odesłany na recepcję, która skontaktowała się z Działem HR w celu potwierdzenia tożsamości i faktu zatrudnienia. Niby banalne, ale żartowniś się zorientował, że jest procedura, a Dział HR uświadomił mu niestosowność postępowania.

→

» Inwestycja w dobrego specjalistę to nie tylko jego profilowe szkolenia, to także inwestycja w świadomość zagrożeń… powodowanych jego niestosownym zachowaniem. «

2. Po potwierdzeniu tożsamości i wydaniu identyfikatora „Gość" pracownik został poproszony przez przełożonego, który ponownie uświadomił mu niestosowność zachowania oraz zakomunikował, jakie działania zostaną wobec niego podjęte za zniszczenie identyfikatora oraz niestosowanie się do obowiązujących procedur.

Funkcje odstraszania i wykrywania zostały zaprezentowane dobitnie i skutecznie. Szef bezpieczeństwa właściwie nie musiał już reagować, ale zrobił to poprzez 30-minutowe szkolenie tego konkretnego pracownika. Inwestycja w dobrego specjalistę to nie tylko jego profilowe szkolenia, to także inwestycja w świadomość zagrożeń… powodowanych jego niestosownym zachowaniem. Niesfornego pracownika można zwolnić, ale przecież nie chodzi o to.

Zamek, kłódka, drzwi, klucz, karta KD...

Dobre zabezpieczenia w dzisiejszych czasach ze wszech miar uzasadnione powinny działać zarówno zewnętrznie, jak i wewnętrznie. W naszych obiektach często widzimy duże nasycenie systemem CCTV/VSS, ale sama kamera niestety jest elementem typowo marketingowym. Stała obsługa, a jeszcze lepiej analityka wideo dopiero zmienia tę sytuację. Oczywiście pod warunkiem, że pracownik ochrony będzie z kamer korzystał. Korzystał, czyli będzie miał je do dyspozycji, będzie potrafił je obsługiwać i właściwie zinterpretować obraz. Ponownie pojawia się magiczne słowo „synergia". I ponownie pojawiają się słowa „sabotaż" i „dywersja". Dokonanie tych aktów wiąże się z rozpoznaniem obiektu i procesów w nim zachodzących, stąd pracownik ochrony musi znać i mienie, i procesy, i wzajemne relacje mienia i procesów. Ponownie więc pojawia się wspólny język i wzajemne szkolenia.

Kamery wykorzystujemy w celu detekcji nieuprawnionego wejścia oraz niewłaściwego przepływu mienia. To właśnie ma bezpośredni związek z przeciwdziałaniem sabotażowi i dywersji, dlatego obecnie są one tak ważne. Jednak najpierw musimy utrudnić zadanie sabotażystom już na linii ogrodzenia obiektu, bo to jest pierwsza linia obrony. Nawet jeśli zbudujemy 2-metrowe ogrodzenie, zwieńczone drutem żyletkowym i wyposażone w system wykrywania wibracji, powodowanych np. próbami wspinania się, przecinania czy odchylania lub podnoszenia, to jeśli będą dziury w ogrodzeniu, będzie ono nic niewarte. Warto także zapewnić trwałe związanie ogrodzenia z fundamentem. W końcu wygodniej jest przechodzić pod ogrodzeniem niż nad nim.

W kontekście zapobiegania sabotażowi warto zwrócić uwagę, że kamery, zwłaszcza pracując z funkcjami analitycznymi, zapewniają świadomość sytuacyjną, co jest istotną przewagą. Podczas jednej z niedawnych konferencji zostało użyte stwierdzenie „sztuczna intuicja". Prelegenci pokazali potencjał kamer w kontekście identyfikowania zjawisk nienaturalnych, np. normalnie ruch odbywa się w określoną stronę, a tymczasem kamera identyfikuje osobę idącą „pod prąd". Obecnie systemy jeszcze pewnie nie potrafią zidentyfikować innego munduru pracownika ochrony czy ubioru roboczego naszego pracownika, ale to tylko kwestia czasu, skoro analityka już może wskazywać brak okularów ochronnych. I to wszystko pozwala wykrywać symptomy zagrożeń, w tym także sabotażu, bo warto pamiętać, że przeciwnik (czytaj: sabotażysta, szpieg, dywersant) też popełnia błędy. Chodzi o to, aby być krok przed nim.

Utrudnijmy zadanie sabotażystom już na linii ogrodzenia obiektu, bo to jest nasza pierwsza linia obrony.

Zarządzanie, czyli systemy integrujące

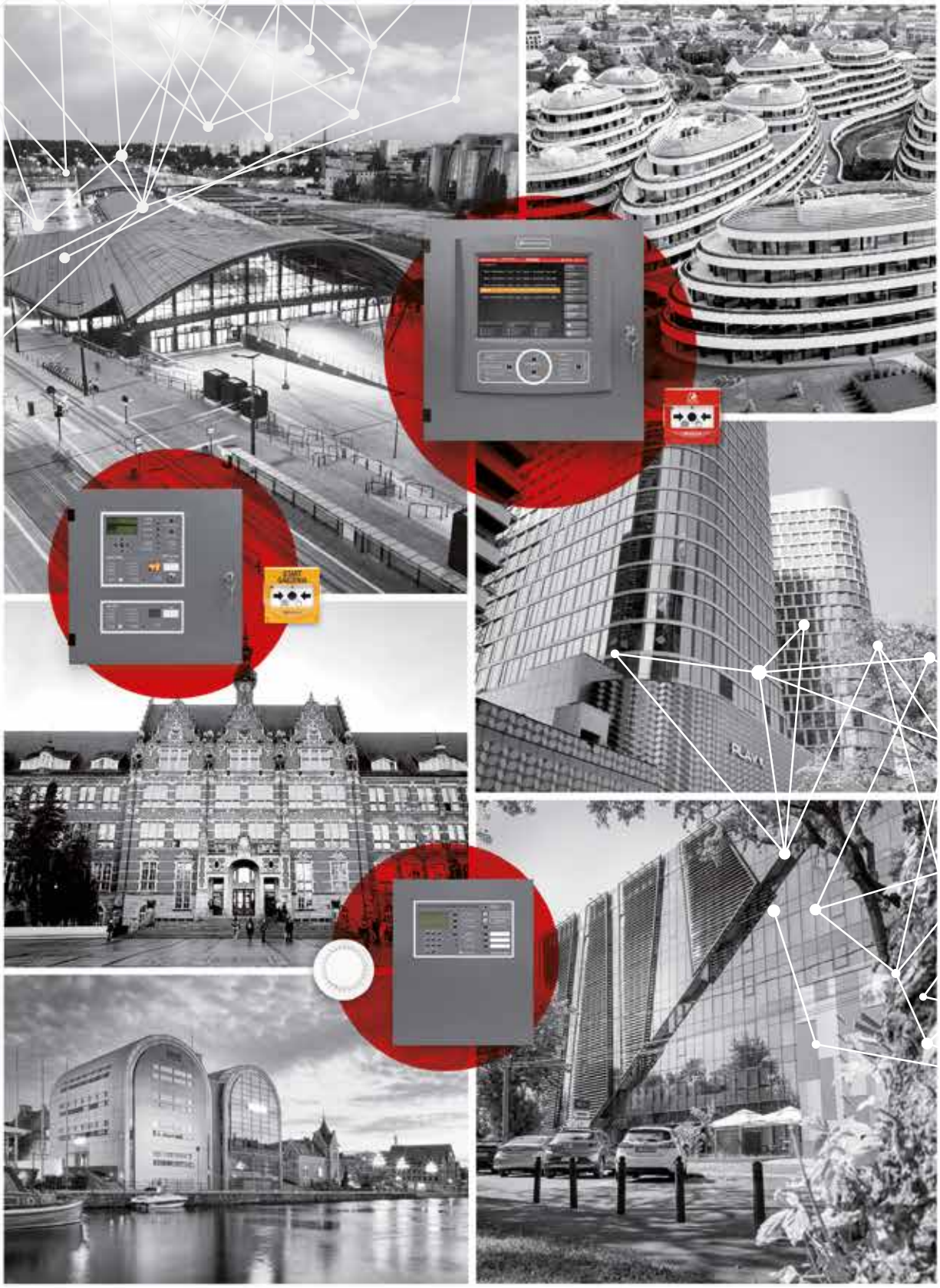
Kończąc, nie sposób nie poruszyć kwestii systemów integrujących PSIM *(Physical Security Information Management),* których podobnie jak sabotażu ustawa także nie dostrzega, a które coraz częściej są podstawowym narzędziem naszej pracy, pozwalając osiągnąć efekt synergii, poczynając od wyższej efektywności detekcyjnej systemów zabezpieczeń technicznych, kończąc na szybszym i bardziej precyzyjnym adresowaniu sygnałów, dzięki czemu symptomy włamania, kradzieży czy dewastacji mogą być tagowane także jako symptomy sabotażu.

W efekcie stworzony system nie tylko będzie odpowiadał na nowe zagrożenia, ale także umożliwi lepsze ich przewidywanie, co w dzisiejszych zmiennych czasach jest niezwykle potrzebne. •

Jacek Grzechowiak

Menedżer ryzyka i bezpieczeństwa. Absolwent WAT, studiów podyplomowych w SGH i Akademii L. Koźmińskiego. Gościnnie wykłada na uczelniach wyższych. W przeszłości związany z grupami Securitas, Avon i Celsa, w których zarządzał bezpieczeństwem i ryzykiem. Obecnie pełni funkcję konsultanta Zarządu ds. Ryzyka i Bezpieczeństwa w TAURUS OCHRONA. Dyrektor Centrum Kompetencji „a&s Polska".

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

Trzy poziomy wykorzystania dozoru wizyjnego w produkcji

Technologia dozoru wizyjnego może oferować coś więcej niż tylko bezpieczeństwo techniczne. Może dotyczyć wszystkiego, od poprawy bezpieczeństwa ludzi i procesów po maksymalizację wydajności operacyjnej.

Sprytne wykorzystanie rozwiązań w zakresie dozoru wizyjnego nie tylko poprawia bezpieczeństwo, ale także może zminimalizować przestoje, zapewnić świadomość sytuacyjną i umożliwić konserwację predykcyjną. W obiektach przemysłowych najlepiej sprawdzają się takie kamery, które mogą działać w trudnych warunkach i są chronione przed cyberatakami. Integrując rozwiązania dozoru z architekturą systemu sterowania w różnym stopniu, można osiągnąć różne poziomy funkcjonalności, a tym samym różne stopnie poprawy wydajności operacyjnej.

Poziom pierwszy: umożliwienie weryfikacji wizualnej

Jedno z podstawowych zastosowań dozoru wizyjnego polega na wykorzystaniu kamer sieciowych do uzyskania podglądu różnych etapów procesu produkcyjnego. Przykładowo w zakładzie produkcyjnym dozór wizyjny umożliwia sprawdzenie, co dzieje się w innym miejscu hali produkcyjnej podczas produkcji komponentów, takich jak reflektory lub bloki silnika.

W przemyśle energetycznym kamery sieciowe mogą być rozmieszczone w dużym obiekcie hydroelektrycznym, aby zapewnić wizualną weryfikację stanu zapory. Dzięki temu operatorzy mają wgląd na takie kwestie jak to, czy w pobliżu włazów znajdują się zanieczyszczenia lub czy lód na powierzchni jeziora jest stabilny.

Poziom drugi: wsparcie w czasie rzeczywistym

Kamery powinny być zintegrowane z istniejącym systemem sterowania procesami lub usługami w chmurze. Jest to klucz do zapewnienia operatorowi szybkiego i odpowiedniego podglądu otoczenia. To oznacza jeszcze lepsze wykorzystanie możliwości dozoru wizyjnego. Gdy system sterowania procesem i podłączone do niego urządzenia wykryją anomalię, zintegrowane kamery mogą natychmiast automatycznie skierować swój „wzrok" w jej stronę.

Kamery uzupełniają dane pozyskiwane z tradycyjnych czujników dodatkowymi danymi wejściowymi, dzięki czemu dane z czujników mogą być dodawane jako nakładka (dane w widoku wideo) w obrazie dostarczonym przez kamerę. Jeśli np. czujniki podłączone do systemu prześlą dane wskazujące, że jedna z maszyn ma nadmierną prędkość obrotową, zintegrowana kamera automatycznie przesunie się, aby obserwować urządzenie, by operator mógł ocenić sytuację.

– *Kamery sieciowe można zintegrować, aby monitorować różne obszary o kluczowym znaczeniu do prowadzonych procesów, np. w zaporze wodnej* – mówi Konrad Badowski z Axis Communications. – *Jeśli dojdzie do incydentu, takiego jak zatrzymanie turbiny lub otwarcie włazu zapory, alert spowoduje, że kamera automatycznie przesunie się do odpowiedniego obszaru, dzięki czemu będzie można przyjrzeć się bliżej usterce.*

Kamery Axis wspierają kontrolę jakości produkcji w Grupie BMW

Automatyzacja i usprawnienie kontroli jakości w Grupie BMW była możliwa dzięki opatentowanej platformie informatycznej AIQX (*Artificial Intelligent Quality Next*) oraz kamerom sieciowym Axis rozmieszczonym wzdłuż linii montażowej. Kamery te, stale rejestrujące obraz pojazdów, zsynchronizowane z lokalizacją pojazdu w czasie rzeczywistym, zapewniają precyzyjne monitorowanie i kontrolę w całym cyklu produkcji.

Kamery rejestrują obraz, szczegółowo analizując każdy element auta. Wysoko zautomatyzowana kontrola jakości odbywa się w ułamkach sekundy w wielu lokalizacjach. Cały proces jest koordynowany przez AIQX i bazuje na technologii widzenia komputerowego wykorzystującego algorytmy głębokiego uczenia. Platforma AIQX jest zatem w stanie automatycznie wykrywać wady projektowe i różne błędy na podstawie milionów zebranych punktów danych, głównie zdjęć i filmów.

– *Jesteśmy dumni, że nasze kamery pomagają Grupie BMW, jako pionierowi cyfryzacji, wykorzystywać rozwiązania AI w produkcji samochodów i optymalizować kontrolę jakości pojazdów. Podzielamy także wartości BMW dotyczące zrównoważonego rozwoju oraz ochrony danych i czerpiemy korzyści z naszej profesjonalnej wymiany* – powiedział Torsten Kasten, menedżer ds. kluczowych klientów w Axis Communications.

Większość zastosowanych kamer należy do serii kamer typu bullet – AXIS P14. Wykorzystując technologie Axis Forensic WDR i Axis Lightfinder, urządzenia te zapewniają realistyczne kolory i rejestrują najdrobniejsze szczegóły nawet w trudnych warunkach oświetleniowych lub niemal całkowitej ciemności.

Obrazy wideo w czasie rzeczywistym są szybko przesyłane do platformy AIQX opartej na chmurze w celu natychmiastowej analizy przy użyciu zaawansowanych algorytmów AI. Pracownicy linii produkcyjnej mogą natychmiast uzyskać dostęp do analizowanych danych, co pozwala im szybko zidentyfikować i usunąć wszelkie usterki.

AIQX spełnia wiele funkcji, od identyfikacji anomalii w procesie montażu po weryfikację kompletności i określenie wariantów.

Kamery dostarczone Grupie BMW przez Axis Communications wyróżnia wysoki poziom cyberzabezpieczeń dzięki wbudowanym funkcjom uniemożliwiającym nieautoryzowany dostęp i zapewniającym solidną ochronę systemu.

Poziom trzeci: maksymalne wykorzystanie analityki

Aby zwiększyć wykorzystanie kamer w operacjach przemysłowych, stosowane są inteligentne narzędzia analityczne. Dzięki nim wszystkie dane pozyskiwane z kamer mogą posłużyć do maksymalizacji wydajności produkcji.

Dzięki wdrożeniu kamer wizyjnych z inteligentną analizą obrazu operatorzy mogą otrzymać alert, jeśli pracownik wejdzie do obszaru o ograniczonym dostępie, zbliży się zbyt blisko poruszających się maszyn lub nie ma na sobie odpowiedniego sprzętu ochronnego. Zapewnia to nie tylko dodatkowe środki ostrożności, ale także pozwala na ciągłość operacji. Wyposażeni w te informacje operatorzy mogą zareagować na sytuację, zanim dojdzie do wypadku lub zatrzymania linii produkcyjnej.

Większa funkcjonalność umożliwia większą proaktywność

Każdy z trzech różnych poziomów pomaga w zwiększeniu wydajności operacyjnej, zapewniając przy tym różne korzyści. Dzięki weryfikacji wizualnej można kontrolować procesy i zdalnie monitorować pracę personelu, aby upewnić się, że przestrzegane są bezpieczne praktyki pracy oraz efektywne wykorzystanie zasobów.

– *Im bardziej zintegrowane są rozwiązania dozoru wizyjnego, tym bardziej proaktywne i efektywne mogą być pod względem wykorzystania zasobów. Jako jeden z przykładów rozważmy proces pakowania rolek papieru w firmie produkcyjnej. Kamery sieciowe mogą zapewnić weryfikację wizualną, dzięki czemu operatorzy mogą wykryć, czy rolka została bezpiecznie zapakowana. Jednak wdrożenie analiz gwarantuje, że wszelkie rolki z niewystarczającą ilością opakowania są nie tylko natychmiast wykrywane, ale także automatycznie oznaczane, dzięki czemu można je szybko ponownie zapakować, optymalizując wydajność operacyjną* – dodaje Konrad Badowski.

Chcąc zwiększyć wydajność operacyjną w infrastrukturze krytycznej lub innych operacjach przemysłowych, należy zastanowić się, gdzie obecnie znajduje się organizacja na tych trzech poziomach. Przechodząc na bardziej zintegrowane rozwiązania dozoru, możesz szybko stać się jeszcze bardziej efektywny i wydajny w perspektywie krótko- oraz długoterminowej. ●

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

Rozwiązania Hikvision dla przemysłu i farm fotowoltaicznych

Zarówno przemysł, jak i firmy działające w sektorze energii odnawialnej, w tym także farmy fotowoltaiczne, zmagają się z coraz większymi wyzwaniami związanymi z bezpieczeństwem. Jednocześnie muszą dbać o swoją efektywność operacyjną i utrzymanie zrównoważonego rozwoju. Aby sprostać temu wyzwaniu, muszą sięgać po nowoczesne rozwiązania, także z zakresu bezpieczeństwa fizycznego, dokładnie takie jak te oferowane przez Hikvision.

Piotr Świder

Rozwiązania Hikvision, światowego lidera w technologii monitoringu i bezpieczeństwa, bazują na kamerach bispektralnych, algorytmach AI, radarach oraz oprogramowaniu HikCentral. Pozwalają tym samym na kompleksowe zarządzanie infrastrukturą przemysłową czy farmami fotowoltaicznymi, zapewniając nie tylko zwiększoną ochronę, ale także optymalizację wydajności operacyjnej i zarządzania ryzykiem.

Kamery bispektralne Hikvision – zaawansowane monitorowanie i ochrona

Kamery bispektralne DS-2TD2667 to jedne z najnowocześniejszych i najpopularniejszych urządzeń w ofercie Hikvision. Łączą dwa sposoby rejestracji obrazu: w świetle widzialnym (2688x1520 pikseli) oraz za pomocą obrazowania w paśmie średniej podczerwieni, czyli termowizji (640x512). Dzięki temu z jednej strony zapewniają bardzo precyzyjny obraz (w różnych warunkach oświetleniowych), z drugiej – umożliwiają monitorowanie temperatury obserwowanych obiektów.

Zastosowanie kamer bispektralnych w przemyśle

W zakładach przemysłowych, które są narażone na różnorodne zagrożenia – od wypadków pracowniczych po awarie sprzętu – kamery bispektralne odgrywają kluczową rolę w zwiększeniu poziomu bezpieczeństwa i monitoringu operacyjnego. Użycie termowizji powoduje, że kamery mogą być stosowane do wykrywania nadmiernego nagrzewania się maszyn, co jest często wczesnym sygnałem awarii. Monitorowanie w czasie rzeczywistym pozwala na szybkie podejmowanie działań prewencyjnych, minimalizując ryzyko przestojów i kosztownych napraw.

Kamery bispektralne PTZ DS-2TD4167 Hikvision mogą stanowić uzupełnienie kamer stałopozycyjnych, ponieważ można za ich pomocą prowadzić nadzór nad rozległym terenem w takich warunkach atmosferycznych, z jakimi nie do końca radzą sobie tradycyjne kamery. Niesprzyjające warunki, takie jak mgła, deszcz, zmrok nie stanowią dla tych kamer bispektralnych żadnej przeszkody. Urządzenia te pozwalają również wykrywać anomalię temperatury na odległość nawet do 1000 m. Termowizja pozwala na wykrywanie zagrożeń o każdej porze dnia i nocy, co zwiększa poziom ochrony zakładów, a moduł światła widzialnego i zastosowany 40-krotny zoom optyczny dają dodatkowe wsparcie operatorowi systemu. Kamery te mają bardzo czuły przetwornik 1/1.8". Połączenie rozdzielczości 2688x1520 z imponującym zoomem optycznym daje możliwość objęcia monitoringiem bardzo dużej powierzchni. Natomiast moduł termowizyjny dodatkowo ogranicza ewentualne martwe strefy.

Zastosowanie kamer bispektralnych na farmach fotowoltaicznych

Farmy fotowoltaiczne, z racji swojej lokalizacji i specyfiki działania, są szczególnie narażone na różnego rodzaju zagrożenia, w tym kradzieże paneli, wandalizm oraz pożary. Kamery bispektralne Hikvision mogą monitorować stan instalacji pod kątem zmian temperatury, co pozwala na szybkie wykrywanie awarii, takich jak przegrzewanie się paneli. Co więcej, możliwe jest monitorowanie farm fotowoltaicznych również w nocy, kiedy są one szczególnie narażone na działalność intruzów. W przypadku wykrycia nietypowych ruchów system automatycznie wysyła alerty, co umożliwia szybką interwencję.

AI – inteligentna analiza wideo dla przemysłu i farm fotowoltaicznych

Sztuczna inteligencja (AI) stanowi kolejny kluczowy element rozwiązań Hikvision dla przemysłu i farm fotowoltaicznych. Inteligentna analiza wideo (IVA) pozwala na przekształcanie dużej ilości danych w użyteczne informacje, które mogą być wykorzystywane do poprawy bezpieczeństwa i wydajności operacyjnej. Systemy AI w kamerach Hikvision umożliwiają automatyczną detekcję i klasyfikację zdarzeń na podstawie analizy obrazu. Przykładem może być wykrywanie naruszeń bezpieczeństwa, takich jak wkraczanie pracowników do stref niebezpiecznych czy ogólną ochronę obwodową.

Dzięki AI możliwe jest także monitorowanie warunków pracy pracowników, takich jak przestrzeganie norm BHP, w tym dotyczących ubrania roboczego, także braku kasku. Systemy te działają w czasie rzeczywistym, co umożliwia natychmiastową reakcję na nieprawidłowości.

AI umożliwia także automatyczne monitorowanie stanu technicznego paneli fotowoltaicznych oraz identyfikację wszelkich nieprawidłowości. AI może analizować obraz termiczny, wykrywając miejsca, gdzie panele są uszkodzone lub przegrzane, umożliwia to szybką naprawę i utrzymanie wysokiej wydajności.

Sztuczna inteligencja może także automatycznie rozpoznawać wtargnięcie osób trzecich na teren farmy. Potrafi przy tym odróżniać ludzi od zwierząt czy innych obiektów, co znacząco redukuje liczbę fałszywych alarmów.

Radary Hikvision – rozszerzona ochrona obiektów przemysłowych i farm fotowoltaicznych

Radary DS-TDSB0G w połączeniu z kamerami bispektralnymi i technologią AI oferują wykrywanie incydentów na dużych obszarach. Radary mogą bowiem skanować teren na odległość nawet do 2000 m, w warunkach całkowitego braku widoczności, i dostarczać informacji o położeniu obiektów. Stanowi to świetne uzupełnienie systemu składającego się z kamer bispektralnych i sprawia, że całe rozwiązanie staje się kompleksowe.

W przemyśle radary wykorzystywane są do monitorowania dużych przestrzeni, niełatwych do nadzoru za pomocą tradycyjnych kamer. Mogą także skanować strefy magazynowe oraz miejsca o wysokim poziomie ryzyka, np. składowiska materiałów łatwopalnych. Radary Hikvision dostarczają informacji o prędkości, kierunku i lokalizacji wykrytych obiektów, co pozwala na natychmiastowe reagowanie na potencjalne zagrożenia. Taki system składający się z kamery PTZ oraz radaru poprzez ich odpowiednią kalibrację umożliwia również śledzenie i rozpoznanie obiektu.

Radary są doskonałym elementem systemu ochrony farm fotowoltaicznych, często położonych na odludziu i w związku z tym wymagających skutecznej ochrony obwodowej. Praca radarów jest niezależna od warunków pogodowych czy pory dnia. Technologia radarowa pozwala na precyzyjne określenie pozycji intruzów, co w połączeniu z kamerami bispektralnymi umożliwia natychmiastową identyfikację zagrożenia i jego neutralizację.

Platforma zarządzania HikCentral – kompleksowa kontrola systemu

Jednym z najważniejszych elementów systemu Hikvision jest platforma HikCentral, która pozwala na centralizację i automatyzację monitoringu oraz zarządzanie bezpieczeństwem obiektu. HikCentral to zaawansowane narzędzie, które integruje wszystkie komponenty systemu – od kamer bispektralnych, przez radary, po systemy AI – w jedno, łatwe w obsłudze środowisko. HikCentral umożliwia pełną kontrolę nad monitorowaniem zakładów przemysłowych. Platforma oferuje szereg funkcji, takich jak zdalny dostęp do kamer, monitorowanie stanu urządzeń, analiza danych w czasie rzeczywistym oraz automatyzacja procesów.

Rozwiązania Hikvision oparte na kamerach bispektralnych, technologii AI, radarach oraz platformie do zarządzania HikCentral oferują kompleksowe podejście do ochrony zarówno w przemyśle, jak i na farmach fotowoltaicznych. Oprogramowane integruje również pozostałe systemy ochrony, np. kontrolę dostępu czy systemy alarmowe. Dzięki innowacyjnym rozwiązaniom Hikvision wspiera przemysł i sektor energii odnawialnej w ich drodze ku bardziej zrównoważonej i efektywnej przyszłości. ●

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

Integracja systemów w Dahua DSS – nowoczesne podejście do bezpieczeństwa sektora przemysłowego

Współczesny przemysł stoi przed wieloma wyzwaniami związanymi z zapewnieniem bezpieczeństwa. Nieustannie rozwijające się technologie oraz rosnąca liczba zagrożeń, zarówno fizycznych, jak i cyfrowych, wymuszają na firmach wdrażanie zaawansowanych systemów zabezpieczeń.

Mariusz Kulik

W tym kontekście najważniejsza staje się integracja różnych systemów bezpieczeństwa pozwalająca na skuteczne zarządzanie infrastrukturą. Jednym z narzędzi, które zdobywa coraz większe uznanie na rynku, jest oprogramowanie Dahua DSS *(Dahua Security Software)*.

DSS to zaawansowana platforma, która umożliwia integrację różnorodnych systemów bezpieczeństwa w jedno spójnie zarządzane środowisko. Dzięki tej platformie możliwe jest monitorowanie systemów wizyjnych, kontroli dostępu czy sygnalizacji włamania i zarządzanie nimi. Co więcej, DSS pozwala na integrację z systemami zewnętrznymi, nie tylko tymi z oferty firmy Dahua, co dodatkowo zwiększa jego elastyczność i zdolność do adaptacji w różnych środowiskach przemysłowych.

Zarówno oprogramowanie, jak i urządzenia firmy Dahua znajdują szerokie zastosowanie w sektorze przemysłowym, gdzie bezpieczeństwo odgrywa kluczową rolę. W dużych zakładach produkcyjnych możliwa jest integracja systemów monitoringu wizyjnego z funkcjonującymi systemami bezpieczeństwa. DSS może zbierać zdarzenia z dowolnego systemu alarmowego, dzięki czemu personel ochrony ma pełen wgląd w sytuację na terenie całego obiektu, co zapewnia szybką identyfikację i neutralizację potencjalnych zagrożeń.

W magazynach wysokiego składowania, gdzie zarządzanie dostępem i monitorowanie ruchu osób jest kluczowe, DSS pozwala na precyzyjną kontrolę nad tym, kto i kiedy ma dostęp do określonych stref. Z kolei w rafineriach i zakładach chemicznych, gdzie występują duże zagrożenia pożarowe, integracja systemu DSS z czujnikami dymu i temperatury czy kamerami termowizyjnymi umożliwia szybkie wykrycie zagrożeń i automatyczne uruchomienie procedur awaryjnych. Przy wykorzystaniu wbudowanego modułu inteligentnej inspekcji można na bieżąco monitorować proces produkcji lub kontrolować stan elementów infrastruktury krytycznej w obszarze danego przedsiębiorstwa.

Jedną z najważniejszych zalet integracji systemów w ramach Dahua DSS jest zwiększenie efektywności zarządzania bezpieczeństwem. Wszystkie dane z różnych systemów są zbierane i analizowane w jednym miejscu co pozwala na szybsze i bardziej trafne podejmowanie decyzji. Ponadto integracja systemów zmniejsza koszty operacyjne, eliminując potrzebę stosowania wielu odrębnych systemów zarządzania.

Kolejną korzyścią jest skalowalność platformy DSS. System może być łatwo rozszerzany o kolejne moduły i urządzenia, co czyni go idealnym rozwiązaniem zarówno dla małych, jak i dużych przedsiębiorstw. Dzięki temu firma może dostosować swoje rozwiązania zabezpieczeń do aktualnych potrzeb, bez konieczności inwestowania w całkowicie nowe systemy.

Patrząc w przyszłość, można się spodziewać, że takie systemy, jak Dahua DSS będą coraz bardziej zaawansowane i jeszcze lepiej dostosowane do specyficznych potrzeb różnych sektorów przemysłowych. Rozwój technologii AI i IoT z pewnością wpłynie na dalsze udoskonalanie funkcji analizy danych i automatyzacji procesów zabezpieczeń.

DSS PRO to rozwiązanie, które dzięki swojej wszechstronności i możliwości integracji z różnymi systemami staje się doskonałym narzędziem do zapewniania bezpieczeństwa w sektorze przemysłowym. W dobie rosnących zagrożeń takie kompleksowe podejście do zarządzania bezpieczeństwem jest nie tylko pożądane, ale wręcz niezbędne. ●

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

ALNET SYSTEMS

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

www.alnetsystems.com

głos branży

Wyzwania związane z zapewnieniem bezpieczeństwa w zakładach przemysłowych w ostatnich czasach ewoluowały. Pojawiają się nowe zagrożenia, na które często brakuje odpowiedniego przygotowania. Jak duży wpływ na poprawę bezpieczeństwa obiektów mają nowoczesne technologie? Jakie rekomendacje mają w tej kwestii doświadczeni specjaliści?

Janusz Syrówka
EON

Jak rozumieć odporność

Rola obiektów przemysłowych w ostatnich latach nie uległa dużej zmianie. Jeśli odniesiemy się do sektora energetycznego, była i jest ona krytyczna w pełni tego słowa znaczeniu. To, co się zmieniło, to świadomość zagrożeń. Sabotaż wrócił na szczyt ryzyk i jest to ryzyko, którego zmaterializowanie się jest wysoce prawdopodobne, zwłaszcza w naszym kraju. Czy można się przed tym uchronić? To bardzo trudne zadanie. Atakujący ma zawsze przewagę, a przemysł prowadzi działalność biznesową, a nie charytatywną i możliwości angażowania środków zapobiegawczych mogą być ograniczone. Tutaj każda złotówka musi być wydana bardzo mądrze. Z perspektywy osoby zajmującej się bezpieczeństwem istnieje silna pokusa pełnej koncentracji na środkach technicznych. Jednak nie tylko te środki stanowią koszt zabezpieczenia działalności. Budowa odporności to coś większego. Czasami odporność rozumiana jest jako „niezniszczalność" i wtedy pojawia się chęć zmiany obiektów w twierdze nie do zdobycia. Moje rozumienie

odporności nawiązuje do realiów walki bokserskiej. Nie unikniesz wszystkich ciosów, ale jeśli padniesz na deski, to jesteś w stanie wstać, zanim sędzia doliczy do dziesięciu. Przy takim podejściu konieczne jest wyjście poza „gardę" naszych środków bezpieczeństwa, które oczywiście są bardzo ważne. Czasem trzeba będzie podejmować trudne strategiczne decyzje – czy możemy prowadzić działalność w warunkach braku pewności utrzymania jej ciągłości. Jeśli tak, to jak w jaki sposób to osiągnąć? Jak się zorganizować, aby nie polec po jednym ciosie. Do tego potrzeba wiedzieć, co jest dla nas krytyczne i jakie mamy słabe punkty. Nigdy się tego nie dowiemy, jeśli w świadomości firmy nie zakiełkuje potrzeba oderwania się choć na chwilę z młynka codziennej działalności i „złapania" szerszej perspektywy. Wierzę, że jest to możliwe, zwłaszcza w obecnych czasach. Poza generowaniem wzrostów zaczyna zyskiwać na wartości budowanie organizacji, która w sposób stabilny i nieprzerwany dostarcza odbiorcom swoje produkty.

Marcin Pyclik
POLSKA IZBA OCHRONY

Ochrona fizyczna wspomagana zabezpieczeniami technicznymi

Ochrona obiektów przemysłowych, w tym obiektów infrastruktury krytycznej, ma szczególne znaczenie w obecnej sytuacji geopolitycznej. Wodociągi, ujęcia wody, elektrownie, zakłady produkcji żywności, centra logistyczne, centra danych są obiektami strategicznymi z punktu widzenia ciągłości i sprawności działania państwa. Są również niezbędne, aby zapewnić stabilizację gospodarczą i normalne funkcjonowanie społeczeństwa. Skuteczna ochrona tych obiektów jest niezwykle istotna ze względu na istniejące, jak również stale pojawiające się nowe zagrożenia. Należą do nich w szczególności akty sabotażu, dywersji, pożary spowodowane działaniem osób trzecich, jak również pospolite przestępstwa, takie jak kradzieże zewnętrzne dokonywane przez osoby niezwiązane z chronionym obiektem oraz wewnętrzne dokonywane przez pracowników, podwykonawców i inne osoby wykonujące zadania na terenie obiektu.

Nowoczesne technologie w znacznym stopniu ulepszają działanie systemów ochrony. Kiedyś bezpieczeństwo obiektu opierało się praktycznie tylko na pracowniku ochrony. Obecnie składa się z tzw. triady bezpieczeństwa. Należą do niej zabezpieczenia fizyczne (pracownicy ochrony), zabezpieczenia techniczne (systemy zabezpieczeń mechanicznych i elektronicznych) oraz procedury (zbiór procedur, instrukcji, plany ochrony itp.). Aby skutecznie zbudować system bezpieczeństwa obiektu, konieczna jest ocena i analiza zagrożeń lub – w przypadku przebudowy systemu – audyt bezpieczeństwa wykonywany przez niezależnych ekspertów. Pozwoli to na właściwy dobór sił i środków w zakresie ochrony, określi również procentowy udział ochrony fizycznej i zabezpieczeń technicznych.

Koszty ochrony fizycznej z roku na rok są coraz większe, co skłania zarządzających obiektami do modyfikacji systemów ochrony na rzecz przewagi zabezpieczeń technicznych. Przemawia za tym rozwój technologii wpływający na wysoką skuteczność elektronicznych systemów zabezpieczeń. Jednak każda taka zmiana powinna być poprzedzona rzetelnym audytem bezpieczeństwa, a jeżeli obiekt należy do chronionych obowiązkowo, zgodnie z przepisami Ustawy o Ochronie osób i Mienia bądź został umieszczony przez Dyrektora Rządowego Centrum Bezpieczeństwa w wykazie obiektów wchodzących w skład infrastruktury krytycznej, aktualizacją i uzgodnieniem właściwego planu ochrony. Człowiek, niezależnie od stopnia jego zaangażowania, zawsze będzie potrzebny. Bo przecież ktoś te systemy musi obsługiwać, odbierać z nich sygnały alarmowe, czuwać nad ich niezawodnością. Sztuczna inteligencja jeszcze nie prześcignęła inteligencji „żywej".

Marek Bartkowski
POLPHARMA

Wyzwania Security Managerów

Zabezpieczenie zakładów produkcyjnych nigdy nie było zadaniem łatwym. Już w trakcie budowy obiektu nie zawsze do końca wiadomo, co i gdzie będzie się znajdowało. Na przykład w magazynie montowano kamery w narożnikach w trakcie budowy, a dopiero potem stawiano regały wysokiego składowania. Wtedy okazywało się, że obraz z kamer jest nieużyteczny, bo zamontowano je w złych miejscach. Tak samo jest w przypadku, gdy w trakcie budowy będzie coś zmieniane. Jednak główny nacisk zawsze jest kładziony na perymetr zewnętrzny (ogrodzenie) oraz monitoring zewnętrzny i wewnętrzny. W minionych latach kamery przesyłały sygnał analogowo, a później poprzez IP, nie posiadały funkcjonalności detekcji ruchu, śledzenia obiektu itp. Dlatego zabezpieczenie obiektu skupiało się w głównej mierze na zadaniach dla służby ochrony, która fizycznie miała dokonać inspekcji terenu. Łudzono się, że pracownik monitoringu, który na jednym, góra dwóch monitorach obserwuje wszystkie kamery (czasem nawet ponad 100) będzie w stanie po kilku godzinach zauważyć zdarzenie. Nic bardziej mylnego, dlatego najczęściej dochodziło do kradzieży poprzez sforsowanie ogrodzenia.

Obecnie zabezpieczenia techniczne, takie jak systemy monitoringu wizyjnego, kontroli dostępu, sygnalizacji włamania i napadu, pozwalają na takie ich ustawienie oraz integrację, że pracownik ochrony ma do wykonania tylko kilka czynności

polegających na przekazaniu informacji o zdarzeniu do służb na obiekcie czy wezwania patrolu interwencyjnego. Cała operacja trwa zaledwie kilkadziesiąt sekund, bo większość pracy za pracownika realizuje system.

Dostępne na rynku systemy detekcji na ogrodzeniach, inteligentne kamery, w tym bispektralne wspierane przez kamery obrotowe (PTZ), pozwalają służbom ochrony na działania proaktywne, a nie tylko na reakcję na już trwające zdarzenie. Rozwiązania systemów PSIM – integrujących systemy zabezpieczeń są na tyle inteligentne, że w bardzo krótkim czasie można zidentyfikować, zweryfikować, zareagować i zapobiec niebezpiecznej sytuacji. Nadal jednak nieodzownym elementem w systemie bezpieczeństwa pozostaje pracownik ochrony, wspierany przez Security Managera, który powinien ustalić ryzyka i podjąć odpowiednie środki zabezpieczające, zbudować zabezpieczenie techniczne i proceduralne, wskazać zagrożenia, a przede wszystkim szkolić personel.

Ważnym elementem jest odpowiednie wykorzystanie funkcjonalności systemów zabezpieczeń. Ponieważ nawet najlepsze systemy nie spełnią swoich zadań, jeżeli nie dokonamy ich właściwych ustawień, nie rozpiszemy zadań do realizacji i nie skorelujemy pracy poszczególnych urządzeń, np. kamer monitoringu wizyjnego z bramkami kontroli dostępu, dlatego nieodzownym elementem systemów bezpieczeństwa jest właśnie PSIM.

Podsumowując, obecne systemy bezpieczeństwa pozwalają na naprawdę odpowiednie zabezpieczenie zakładu czy biura. Jednak najpierw należy dokonać audytu, zidentyfikować słabe strony, a potem przygotować plan działania i skutecznie go realizować, aby odpowiednio i na najwyższym poziomie zabezpieczyć mienie zakładu. Pamiętać trzeba też o tym, żeby zadbać o bezpieczeństwo cybernetyczne, ponieważ to w tej chwili może być największym wyzwaniem Security Managerów.

Marcin Walczuk
BCS

Kompleksowe podejście do zabezpieczeń

Zabezpieczenie obiektów przemysłowych jest jednym z najważniejszych elementów zarządzania przedsiębiorstwem. W dobie rosnących zagrożeń, zarówno fizycznych, jak i cyfrowych, konieczne jest wdrożenie kompleksowych strategii ochrony. Jednym z kluczowych aspektów wykorzystującym nowoczesne rozwiązania w zakresie bezpieczeństwa jest fizyczne zabezpieczenie obiektu, mające na celu ochronę obiektu przed nieautoryzowanym dostępem. Na pierwszej linii ochrony przed intruzem są ogrodzenia i bramy. Nad przyznawaniem dostępu osobom i pojazdom nadzór mogą realizować systemy kontroli dostępu wykorzystujące karty dostępu z najnowocześniejszymi zabezpieczeniami, w tym w biometrię. Integracja SKD z kamerami do rozpoznawania numerów tablic rejestracyjnych i identyfikacji twarzy może znacząco podnieść poziom ochrony. Wspomniane kamery będą również wchodziły w skład systemów monitoringu wizyjnego. Kamery CCTV marki BCS wyposażone w nowoczesne funkcje analizy obrazu mogą automatycznie wykrywać podejrzane zachowania, zapewniając stały nadzór nad obiektem. Obraz na rejestratorach można łatwo przeszukać pod kątem interesujących nas zdarzeń, a obsługę systemu ułatwi aplikacja BCS Manager.

Ochrona przeciwpożarowa jest następnym kluczowym elementem zabezpieczenia obiektów przemysłowych, które bardziej niż inne mogą być narażone na wystąpienie pożaru. Systemy ppoż. z urządzeniami do detekcji pożaru, czyli czujkami dymu i ciepła, można uzupełnić o kamery termowizyjne BCS wyposażone w funkcję detekcji pożaru w bardzo wczesnym stadium. Pozwala to na szybkie ugaszenie płomieni, zanim zdążą się rozprzestrzenić. Do gaszenia warto wykorzystać automatyczne systemy gaśnicze, takie jak tryskacze czy systemy gazowe, które nie narażają ludzi na niebezpieczeństwo. Do zapewnienia bezpieczeństwa niezbędne są odpowiednie procedury ewakuacyjne z regularnymi szkoleniami i ćwiczeniami ewakuacyjnymi, które zapewnią, że pracownicy będą wiedzieli, jak się zachować w sytuacji zagrożenia.

W dobie cyfryzacji ochrona danych i systemów informatycznych jest równie ważna jak zabezpieczenia fizyczne. Cyberbezpieczeństwo zapewni szereg elementów zwiększających odporność na cyberataki, np. zapory sieciowe i systemy antywirusowe chroniące przed nieautoryzowanym dostępem i złośliwym oprogramowaniem, szyfrowanie danych przechowywanych i przesyłanych. Edukacja pracowników w zakresie bezpiecznego korzystania z systemów informatycznych i rozpoznawania prób *phishingu* będzie w tym aspekcie niezwykle ważna.

Warto, aby zarządzanie różnymi typami systemów zabezpieczeń zintegrować w jednej platformie, dzięki temu możliwe jest ich monitorowanie i zarządzanie z jednego miejsca, zautomatyzowanie reakcji na określone zdarzenia, takie jak alarmy czy wykrycie intruza. Ponadto zaawansowane analizy danych pozwolą na identyfikację potencjalnych zagrożeń i optymalizację strategii ochrony.

Zabezpieczenie obiektów przemysłowych wymaga kompleksowego podejścia, obejmującego zarówno fizyczne, jak i cyfrowe aspekty ochrony. Wdrożenie nowoczesnych technologii oraz regularne szkolenia pracowników są kluczowe dla zapewnienia bezpieczeństwa i ciągłości działania przedsiębiorstwa. ●

Nowe oblicze ryzyka

Tomasz Guzikowski
EKSPERT DS. BEZPIECZEŃSTWA

Jednym z ważniejszych elementów zapewnienia bezpieczeństwa, w obliczu zmiennego otoczenia i nowych zagrożeń, związanych m.in. z wojną w Ukrainie oraz działaniami hybrydowymi ze strony Rosji, jest zarządzanie ryzykiem.

Zarządzanie ryzykiem wymaga podejścia wielowymiarowego, obejmującego aspekty zarówno fizyczne, jak i cyfrowe, a także ścisłej współpracy z odpowiednimi instytucjami rządowymi i partnerami międzynarodowymi. Kluczowymi elementami takiego podejścia są identyfikacja nowych zagrożeń, analizowanie ich wpływu na strategiczne zakłady przemysłowe, umiejętne zarządzanie ryzykiem w zmieniających się warunkach, planowanie zabezpieczeń i strategie obronne, a także współpraca z rządem i organizacjami międzynarodowymi. Zdecydowanie przydaje się też przygotowanie scenariuszy przewidujących różny przebieg wydarzeń i dostosowanie do nich planów awaryjnych.

Identyfikacja nowych zagrożeń

Wojna w Ukrainie oraz rosnące napięcia międzynarodowe zwiększają ryzyko bezpośrednich ataków, tych konwencjonalnych (np. ataki rakietowe), jak też niekonwencjonalnych, typu wzniecanie pożarów, będących rodzajem dywersji. Co do tych pierwszych, wszyscy pamiętamy, że przestrzeń powietrzna naszego kraju została naruszona przez obiekty niezidentyfikowane. W przypadku drugich służby bezpieczeństwa wykrywają, stale monitorują i zwalczają akty sabotażu w różnych obszarach naszego życia zarówno gospodarczego, jak i społecznego. Nie bez powodu. Rosja od lat angażuje się w działania hybrydowe, obejmujące cyberataki, dezinformację, zakłócanie infrastruktury energetycznej i sieciowej oraz działalność szpiegowską. Ataki te są trudniejsze do wykrycia i odpowiedzi, ponieważ rozmywają granice między wojną a pokojem.

Mogą one być szczególnie dotkliwe dla zakładów produkcyjnych, w których przerwa w realizacji krytycznych procesów może być katastrofalna w skutkach. Sankcje gospodarcze, jakie państwa UE nakładają na różne kraje, oznaczają dla firm zmiany w łańcuchach dostaw i ograniczenia eksportowe. Blokady handlowe wpływają na dostępność surowców oraz stabilność operacyjną zakładów, dlatego tak ważne są działania krajowej i europejskiej administracji, mające na celu ochronę interesów rodzimych przedsiębiorstw. Organizacje muszą więc zadbać o alternatywne źródła dostaw oraz odpowiednie zdolności magazynowe, które zapewnią, że mimo zakłóceń zostanie utrzymana ciągłość biznesowa.

Analiza wpływu na strategiczne zakłady przemysłowe

Zakłady przemysłowe, zwłaszcza zajmujące się produkcją energii, środków chemicznych, metalurgią czy produkcją wojskową, jako elementy infrastruktury krytycznej są częstym celem ataków. Ich uszkodzenie może prowadzić do poważnych skutków zarówno dla gospodarki, jak i bezpieczeństwa narodowego. Stąd, z punktu widzenia zachowania ich ciągłości, istotne jest stosowanie rozwiązań mających na celu ochronę procesów krytycznych. Zakłócenia w dostawach energii, będące efektem działań wojennych lub, co w naszej rzeczywistości bardziej prawdopodobne, cyberataki na infrastrukturę energetyczną mogą mieć dramatyczne konsekwencje.

→

Ataki na systemy informatyczne mogą natomiast powodować utratę danych, przestój produkcji lub uszkodzenie maszyn, na co szczególnie wrażliwe są energetyka, produkcja chemiczna czy transport. Jednocześnie trzeba pamiętać, że dyrektywa NIS2 nie tylko nakłada obowiązki z zakresu cyberbezpieczeństwa na podmioty, w tym m.in. z branży produkcyjnej farmaceutycznej, medycznej oraz chemicznej, a niewywiązanie się z nich jest zagrożone wysokimi karami, ale również wprowadza konkretne wymagania dotyczące wdrożenia m.in. polityki analizy ryzyka i bezpieczeństwa stosowanych systemów informatycznych, planów na zapewnienie ciągłości działania oraz bezpieczeństwa łańcucha dostaw czy polityki zarządzania incydentami.

Zarządzanie ryzykiem w zmieniających się warunkach

Dynamiczne i ciągłe monitorowanie sytuacji geopolitycznej, identyfikacja i ocena zagrożeń na poziomach lokalnym, regionalnym oraz globalnym są kluczowe dla zrozumienia potencjalnych zagrożeń i ich wpływu na zakłady produkcyjne. Przygotowaniu na zagrożenia hybrydowe służą inwestycje w systemy monitoringu i wczesnego ostrzegania przed cyberatakami, kampaniami dezinformacyjnymi i innymi działaniami niekonwencjonalnymi. Ściślejsza współpraca z państwami sojuszniczymi i organizacjami międzynarodowymi również zwiększa możliwości wykrycia zagrożeń. A redundancja i dywersyfikacja, czyli zadbanie o zapas zasobów energetycznych, oraz zróżnicowanie dostawców w ramach łańcucha dostaw może zmniejszyć ryzyko wynikające z potencjalnych zakłóceń.

Zabezpieczenia i strategie obronne

Wzmocnienie systemów cyberbezpieczeństwa poprzez zastosowanie nowoczesnych technologii ochronnych, takich jak sztuczna inteligencja do wykrywania anomalii oraz regularne testy odporności systemów (np. testy penetracyjne) są działaniem oczywistym, wymagającym jednak zrozumienia u osób odpowiedzialnych w organizacjach za finanse. Podobnie jest w przypadku rozbudowy i modernizacji zabezpieczeń fizycznych, np. systemów monitoringu wizyjnego, kontroli dostępu czy budowy odpowiednich barier ochronnych, zwłaszcza w zakładach zwiększonego i dużego ryzyka powstania awarii przemysłowej.

Nie można zapomnieć o szkoleniach z zakresu bezpieczeństwa operacyjnego, cyberbezpieczeństwa oraz procedur awaryjnych. Powinny być regularne, a wiedza pracowników weryfikowana np. za pomocą pentestów. Muszą być bowiem świadomi nowych zagrożeń, jakie pojawiają się w wyniku zmieniającej się sytuacji geopolitycznej.

Współpraca

Zakłady przemysłowe o strategicznym dla kraju znaczeniu muszą ściśle współpracować z rządem oraz agencjami odpowiedzialnymi za bezpieczeństwo narodowe. Tylko dzięki tej współpracy menedżerowie ds. bezpieczeństwa mają szansę zyskać dostęp do aktualnych informacji wywiadowczych i zasobów reagowania kryzysowego.

Scenariusze i plany awaryjne

Opracowanie różnych scenariuszy zagrożeń, takich jak atak fizyczny, cyberatak czy zakłócenia dostaw, oraz plany działania na wypadek ich wystąpienia to nie tylko kwestia obowiązku, ale też zwyczajnie zdrowego rozsądku. Ostatnie wydarzenia na południu Polski pokazały, że sytuacja kryzysowa jest zazwyczaj bardzo dynamiczna.

Plany ciągłości działania oraz plany odtworzeniowe powinny zawierać m.in. procedury postępowania dla osób zajmujących się zarządzaniem kryzysowym oraz pozostałych osób zaangażowanych w proces przywracania działalności. W organizacjach powinny być prowadzone także testy gotowości, czyli ćwiczenia symulujące różne sytuacje kryzysowe, aby sprawdzić gotowość zakładów i zespołów reagowania na różne rodzaje zagrożeń.

W obiektach przemysłowych o rozproszonej strukturze, takich jak rafinerie, elektrownie czy rozległe zakłady produkcyjne ochrona techniczna odgrywa kluczową rolę w zapewnieniu bezpieczeństwa przed zagrożeniami zarówno zewnętrznymi, jak i wewnętrznymi. W obliczu rosnących wyzwań związanych z bezpieczeństwem, takich jak zagrożenia terrorystyczne, sabotaż czy cyberataki, coraz większą popularnością cieszą się nowoczesne technologie, które pozwalają na skuteczne monitorowanie otoczenia i szybkie reagowanie.
Do takich rozwiązań należą m.in. systemy przenośne, drony oraz zaawansowane technologie analityki obrazu.

1. Systemy przenośne do ochrony obiektów

Systemy przenośne to elastyczne rozwiązania, które można szybko wdrożyć w różnych lokalizacjach na terenie zakładów przemysłowych. Obejmują one m.in.:

- Przenośne systemy dozoru wizyjnego. Szybko instalowane kamery mogą być używane do monitorowania określonych obszarów, szczególnie w przypadku tymczasowych zagrożeń lub na terenach rozproszonych. W połączeniu z zaawansowaną analityką obrazu (np. wykrywaniem ruchu, śledzeniem osób lub pojazdów) mogą automatycznie ostrzegać o nieautoryzowanej aktywności.
- Przenośne detektory zagrożeń. Urządzenia te mogą wykrywać ruch, ciepło lub substancje niebezpieczne, dzięki czemu możliwa jest szybka identyfikacja potencjalnych incydentów. Przykłady obejmują przenośne detektory gazu, kamery termowizyjne, a także czujniki dźwiękowe wykrywające nietypowe odgłosy, takie jak wystrzały czy eksplozje.
- Przenośne bariery i ogrodzenia. Mogą być łatwo ustawione

w miejscach, gdzie wymagana jest szybka ochrona, np. podczas robót budowlanych na terenie fabryki lub w odpowiedzi na nagłe zagrożenia.

2. Zastosowanie dronów do monitorowania otoczenia

Drony stanowią jedno z najbardziej innowacyjnych narzędzi w zakresie ochrony technicznej, szczególnie w przypadku obiektów o dużym rozproszeniu. Umożliwiają szybki i efektywny nadzór nad trudno dostępnymi miejscami, co znacznie podnosi poziom bezpieczeństwa. Zastosowania dronów w ochronie obiektów obejmują:

- Nadzór w czasie rzeczywistym. Drony wyposażone w kamery o wysokiej rozdzielczości, kamery termowizyjne lub inne specjalistyczne czujniki mogą monitorować otoczenie w czasie rzeczywistym. Dzięki temu mogą szybko wykryć nieautoryzowaną obecność osób, pojazdów lub dronów przeciwnika.
- Monitorowanie dużych obszarów. W przypadku rozległych zakładów przemysłowych, takich jak kopalnie czy elektrownie, drony mogą systematycznie patrolować teren, co pozwala na monitorowanie miejsc, które byłyby trudne lub kosztowne do nadzorowania w tradycyjny sposób.
- Szybkie reagowanie. W sytuacjach kryzysowych, takich jak pożary, awarie techniczne czy incydenty sabotażu, drony mogą szybko dotrzeć do miejsca zdarzenia, przekazując obraz i dane w czasie rzeczywistym do centrum zarządzania kryzysowego, co umożliwia natychmiastową reakcję.
- Analiza środowiska. Drony mogą być wyposażone w czujniki do monitorowania jakości powietrza, wykrywania niebezpiecznych substancji chemicznych czy poziomów promieniowania, co ma znaczenie szczególnie w przypadku zakładów chemicznych, rafinerii czy elektrowni i elektrociepłowni.

3. Zaawansowana analityka obrazu

Nowoczesne systemy zabezpieczeń wykorzystują zaawansowane technologie analizy obrazu, które znacząco zwiększają efektywność monitoringu. Oto niektóre z głównych zastosowań:

- Wykrywanie nieautoryzowanego dostępu. Analityka obrazu może automatycznie identyfikować nieautoryzowane osoby lub pojazdy w obszarach chronionych. Systemy te są w stanie rozróżniać pracowników od intruzów, identyfikować ruch podejrzany (np. długi pobyt w jednym miejscu) oraz ostrzegać o potencjalnych zagrożeniach.
- Śledzenie osób i pojazdów. Systemy mogą śledzić ruch osób i pojazdów na terenie zakładu, rejestrując ich trasę i czas spędzony w różnych miejscach. W przypadku nietypowego zachowania, np. przebywania w miejscach niedozwolonych, systemy te mogą automatycznie wysyłać alarmy.
- Rozpoznawanie twarzy i tablic rejestracyjnych. W zaawansowanych systemach zabezpieczeń wykorzystywane są algorytmy rozpoznawania twarzy i tablic rejestracyjnych. Technologia ta umożliwia identyfikację osób oraz pojazdów wchodzących i opuszczających teren zakładu, co pozwala na lepszą kontrolę dostępu.
- Detekcja anomalii. Systemy analityki obrazu mogą wykrywać nietypowe zjawiska, takie jak nagłe zbiegowiska ludzi, szybkie poruszanie się obiektów czy poruszanie się w miejscach, które normalnie są puste (np. w godzinach nocnych). Tego typu automatyczne analizy pozwalają na szybsze wykrywanie potencjalnych zagrożeń.

4. Integracja technologii z systemami zarządzania bezpieczeństwem

Kluczowym aspektem stosowania nowych rozwiązań technologicznych w ochronie obiektów przemysłowych jest ich integracja z istniejącymi systemami zarządzania bezpieczeństwem. Umożliwia to lepsze skoordynowanie działań oraz szybsze reagowanie na zagrożenia.

- Systemy zintegrowanego zarządzania bezpieczeństwem. Dane z przenośnych systemów nadzoru, dronów oraz analityki obrazu mogą być zintegrowane z systemami zarządzania bezpieczeństwem (SMS), które pozwalają na zarządzanie danymi w czasie rzeczywistym, generowanie raportów oraz reagowanie na incydenty. Centralne systemy monitoringu pozwalają na skuteczną koordynację działań w przypadku wykrycia zagrożeń.
- Automatyzacja reakcji. W połączeniu z systemami zarządzania bezpieczeństwem nowe technologie umożliwiają automatyzację niektórych procesów, takich jak zamykanie bram, uruchamianie syren alarmowych czy wysyłanie dronów w określone lokalizacje w przypadku wykrycia podejrzanej aktywności.

Nowoczesne technologie ochrony technicznej, takie jak systemy przenośne, drony oraz zaawansowana analityka obrazu, odgrywają kluczową rolę w zapewnieniu bezpieczeństwa obiektów przemysłowych o strukturze rozproszonej. Elastyczność, mobilność oraz możliwość monitorowania dużych obszarów w czasie rzeczywistym to główne zalety tych rozwiązań, które znacząco zwiększają efektywność ochrony. Integracja tych narzędzi z istniejącymi systemami zarządzania bezpieczeństwem pozwala na szybsze wykrywanie i reagowanie na zagrożenia, co w dzisiejszych warunkach jest niezbędne do utrzymania bezpieczeństwa strategicznych zakładów przemysłowych. ●

Kluczowy element w zarządzaniu kontrolą dostępu

Elektronika elektroniką, cyfryzacja cyfryzacją, ale i tak najczęściej wybieranym rozwiązaniem broniącym dostępu jest klasyczny fizyczny klucz. Ta forma ma bowiem dwie pożądane cechy: prostotę i niezawodność.

Jan T. Grusznic

Wraz z pojawieniem się elektronicznych systemów kontroli dostępu wieszczono rychły koniec ery klucza, tym bardziej że próby wyeliminowania kluczy fizycznych rozpoczęły się już w latach 70. XX wieku wraz z wprowadzeniem zamków szyfrowych. Te, choć skuteczne, wymagały od użytkowników zapamiętania kodu, regularnej zmiany kombinacji i zachowania poufności. Z biegiem czasu na rynku pojawiły się zamki cyfrowe i urządzenia IoT, dzięki którym możliwe jest zdalne zarządzanie dostępem. A jednak klucze fizyczne nie zniknęły.

Głównym tego powodem jest ich niezawodność i odporność na manipulacje cyfrowe. Elektroniczne systemy kontroli dostępu, choć wygodne, nie są całkowicie odporne na cyberataki, co w przypadku fizycznych zamków i pasujących do nich kluczy jest oczywiście niemożliwe. Dość powiedzieć, że z ponad 60 powszechnie stosowanych protokołów komunikacyjnych bazujących na RFID zaledwie kilka nadal opiera się złamaniu i można ich bezpiecznie używać. A protokół Wiegand, wciąż wykorzystywany do wymiany danych między czytnikiem a kontrolerem,

został publicznie skompromitowany 17 lat temu. W erze rosnącej cyfryzacji klucze fizyczne oferują unikalne zabezpieczenie, które nie podlega zdalnym atakom. Oczywiście, klucze fizyczne nie są pozbawione wad. Można taki klucz zgubić, może też zostać skradziony, dając tym samym nieautoryzowany dostęp do obiektu lub zasobów. Innym problemem jest zarządzanie dużą liczbą kluczy, zwłaszcza w dużych organizacjach lub obiektach z wieloma punktami dostępu. To bodaj największe wyzwanie dla osób zarządzających bezpieczeństwem obiektu. Monitorowanie, kto i kiedy korzystał z klucza bez elektronicznego systemu ewidencji, jest trudne i komplikuje badanie incydentów bezpieczeństwa lub nieautoryzowanego dostępu. Niestety zdecydowana większość wykorzystywanych kluczy nieopatentowanych może być powielana bez autoryzacji. Również złożone scenariusze kontroli dostępu zawierające ograniczenia czasowe lub oparte na lokalizacji stanowią wyzwanie w przypadku kluczy fizycznych. Jak widać, tych niedogodności było na tyle sporo, że wiele organizacji zdecydowało się wprowadzić systemy zarządzania kluczami lub kontrolą dostępu, które oferują większe bezpieczeństwo, wydajność i elastyczność.

» Monitorowanie, kto i kiedy korzystał z klucza bez elektronicznego systemu ewidencji, jest trudne i komplikuje badanie incydentów bezpieczeństwa lub nieautoryzowanego dostępu.«

> *Jednym z nowoczesnych rozwiązań w zakresie zarządzania kluczami fizycznymi jest system MasterKey, czyli klucz generalny. Bazuje on na hierarchicznym podziale dostępu.*

System MasterKey – jeden klucz do wielu drzwi

Jednym z nowoczesnych rozwiązań w zakresie zarządzania kluczami fizycznymi jest system MasterKey, czyli klucz generalny. Bazuje on na hierarchicznym podziale dostępu. Jeden klucz może otworzyć wiele zamków, ale w sposób ściśle kontrolowany.

MasterKey eliminuje konieczność posiadania wielu kluczy. Osoby dysponujące takim kluczem mają dostęp tylko do tych obszarów, do których są uprawnione, co zmniejsza ryzyko nieautoryzowanego dostępu. Systemy te są projektowane w sposób elastyczny i skalowalny, co pozwala na ich rozbudowę w miarę potrzeb organizacji. Wartością dodaną systemu MasterKey jest redukcja liczby kluczy, co minimalizuje ryzyko ich zgubienia lub kradzieży. Prawidłowo skonfigurowany system MasterKey jest zatem nie tylko bezpieczny, ale także wygodny.

MasterKey, choć popularny, ma też wady, z którymi warto się zapoznać zawczasu. Podstawową jest to, że jeśli klucz główny dostanie się w niepowołane ręce, da komuś nieuprawnionemu dostęp do wielu obszarów, a nawet całego obiektu. To dla każdej organizacji duże ryzyko. Inną wadą jest to, że wdrożenie systemu klucza generalnego i zarządzanie nim może być skomplikowane, zwłaszcza w dużych obiektach z wieloma poziomami dostępu. Może też się wiązać ze znacznymi kosztami początkowymi. Wyzwaniem może okazać się również konieczność późniejszego wprowadzania zmian lub potrzeba rekonfiguracji uprawnień. Nie ma też możliwości kontrolowania tego, czy klucze główne są używane tylko przez osoby uprawnione. Nic nie stoi na przeszkodzie, by wręczyć taki klucz komuś, kto prawa do jego posiadania nie ma. Zawsze niezbędne jest wprowadzenie ścisłych zasad i procedur oraz ich egzekwowanie, aby zapobiec niewłaściwemu użyciu – w tym przypadku pomocny jest system zarządzający obiegiem kluczy. MasterKey ma też ograniczenia technologiczne: tradycyjne mechaniczne systemy kluczy głównych mogą mieć ograniczenia w zakresie skalowalności i zdalnego zarządzania. Nowoczesne systemy elektroniczne mogą rozwiązać te problemy, ale mogą do tego wymagać dodatkowych inwestycji.

Depozytory – automatyzacja zarządzania kluczami

Kontrola nad fizycznymi kluczami w dużych organizacjach bywa kłopotliwa. Taki klucz można utracić, może krążyć między pracownikami bez żadnej nad tym kontroli, może zostać skradziony. A przecież odpowiednie monitorowanie jest kluczowe, nomen omen, dla zapewnienia bezpieczeństwa. Rozwiązaniem są nowoczesne systemy ewidencji kluczy, w tym depozytory, które automatyzują i upraszczają zarządzanie kluczami.

Depozytory to w zasadzie szafki, ale nie byle jakie, do przechowywania kluczy. Dzięki nim możliwe jest precyzyjne określenie, kto i kiedy pobrał dany klucz, co znacznie zwiększa kontrolę nad nim i obszarami, które są chronione. Użytkownicy mogą pobrać klucz tylko po autoryzacji, co minimalizuje ryzyko nieautoryzowanego dostępu. Depozytor może być też połączony z elektronicznym systemem kontroli dostępu, rejestrującym, kto i kiedy pobrał klucz.

Oprogramowanie automatyzujące ewidencję kluczy pozwala także na generowanie raportów o historii użycia kluczy, co może być niezwykle przydatne w przypadku audytów czy incydentów bezpieczeństwa.

Fizyczne klucze w cyfrowym świecie

Mimo że nasz świat jest coraz bardziej zdigitalizowany, klucze fizyczne wciąż odgrywają istotną rolę. Ich zalety, takie jak niezawodność i łatwość obsługi, a także niska cena sprawiają, że są one niezastąpionym elementem wielu systemów zabezpieczeń. W obiektach takich jak zakłady karne, placówki medyczne, parki logistyczne czy banki klucze fizyczne nadal stanowią główną metodę ochrony.

W zakładach karnych klucze fizyczne są po prostu niezbędne. To najprostszy, ale też w tym wypadku najpewniejszy sposób zamknięcia celi, niewrażliwy na próby cyfrowego włamania czy odcięcia zasilania pod jednym warunkiem: dostęp do kluczy będzie chroniony przed osadzonymi, którzy w jakiś sposób są upoważnieni do poruszania się po zakładzie. Jednocześnie takie właśnie klucze fizyczne, które nie wymagają żadnego dodatkowego potwierdzenia tożsamości, dają możliwość natychmiastowego wejścia załodze do pomieszczeń zajmowanych przez osadzonych. Zdarzają się takie sytuacje, gdy czas ma znaczenie. W takich miejscach klucze muszą być nie tylko odpowiednio przechowywane, ale także udostępniane wyłącznie uprawnionym osobom, z pełnym zapisem każdej operacji. Depozytory kluczy są tutaj szczególnie przydatne, umożliwiając ścisłą kontrolę nad obiegiem kluczy oraz szybki dostęp w sytuacjach awaryjnych.

Podobnie w bankowości, gdzie bezpieczeństwo finansowe i operacyjne jest priorytetem, klucze fizyczne są nadal ważnym elementem systemu ochrony. Umożliwiają one dostęp do pomieszczeń, w których przechowywane są aktywa, a ich ochrona wymaga najwyższych standardów zarządzania kluczami.

Klucze w erze cyfrowej

W dobie coraz powszechniejszych rozwiązań cyfrowych klucze fizyczne stają się częścią większych, zintegrowanych systemów zabezpieczeń. Dzięki mechatronice tradycyjny fizyczny klucz zyskuje cyfrowe funkcje. To pozwala na zdalne zarządzanie dostępem bez konieczności wymiany mechanicznych zamków. Rozwiązanie bazuje na kluczach fizycznych wyposażonych w specjalny moduł i bezprzewodowych elektromechanicznych wkładkach lub kłódkach.

Choć cyfryzacja niesie ze sobą wiele korzyści, to jednak klucze fizyczne wciąż mają swoją przewagę. A pamiętajmy, że przed erą cyfrowych zamków i kluczy pojawiły się klucze patentowane. I choć są starszym rozwiązaniem, to w dalszym ciągu bardzo skutecznym i trudnym do skopiowania.

Ewolucja, od tradycyjnych zamków po nowoczesne systemy zintegrowane z technologiami cyfrowymi, pokazuje, że fizyczny klucz pozostaje nieodzownym elementem systemów zabezpieczeń. Rozwiązania takie jak MasterKey czy depozytory kluczy umożliwiają efektywne zarządzanie i automatyzację procesów, co przekłada się na większe bezpieczeństwo i wygodę użytkowników. W świecie, gdzie cyberbezpieczeństwo staje się coraz ważniejsze, klucze fizyczne oferują unikalną, niezastąpioną linię obrony. •

EVVA POLSKA

System Xesar EVVA – nowoczesne rozwiązanie w zakresie kontroli dostępu

Xesar to innowacyjny mechatroniczny system dostępu, łączący mechaniczne elementy zamknięć z nowoczesnymi komponentami elektronicznymi, oferujący tym samym zaawansowane funkcje kontrolowania dostępu.

System Xesar zapewnia intuicyjną obsługę i efektywne zarządzanie uprawnieniami dostępu. Różnorodność komponentów, takich jak szyldy, klamki, czytniki naścienne, wkładki, zamki do skrzynek pocztowych, kłódki oraz klucze kombi, sprawia, że można go dostosować do różnych potrzeb.
W nowej wersji Xesar 3.2 system umożliwia przekazanie prawa dostępu bezpośrednio na smartfon upoważnionej osoby, co eliminuje konieczność fizycznego przekazywania nośników. Taki sposób obsługi nie tylko jest wygodny, ale również znacząco oszczędza czas, co jest szczególnie istotne dla techników, serwisantów i dostawców.
Bezpieczeństwo jest priorytetem systemu Xesar. Działa on w centrum danych z certyfikatem ISO 27001, co gwarantuje, że wszystkie dane są przetwarzane zgodnie z najwyższymi standardami bezpieczeństwa. Komunikacja jest szyfrowana za pomocą protokołu TLS, zapewniając dodatkową warstwę ochrony przed nieautoryzowanym dostępem.
Xesar można zintegrować z różnymi systemami, takimi jak sygnalizacja alarmowa, inteligentne rozwiązania budynkowe czy rejestracja czasu pracy. Umożliwia to efektywne zarządzanie całym procesem dostępu w jednym miejscu dzięki interfejsowi MQTT.
System Xesar to nie tylko nowoczesne narzędzie do zarządzania dostępem, ale także pewność, że bezpieczeństwo firmy jest w dobrych rękach. Dzięki wszechstronności i innowacyjnym funkcjom Xesar jest idealnym rozwiązaniem dla każdego typu obiektu, w którym kluczowe znaczenie ma kontrola dostępu.
Więcej na: www.evva.com

Dobór depozytorów SAIK

Osoby myślące o wprowadzeniu depozytorów często mają powody, które skłaniają je do rozważenia tej decyzji. Posiadanie depozytora może przynieść wiele korzyści i ułatwić realizację różnych celów. Jedni kierują się chęcią poprawy bezpieczeństwa posiadanych zasobów, inni potrzebują unowocześnić swoją infrastrukturę i poprawić komfort pracy podwładnym. Jeszcze inni mają potrzebę kontrolowania tego, co dzieje się z kluczami, przedmiotami czy bronią.

Opinią, która najczęściej pojawia się wśród doświadczonych odbiorców depozytorów, jest zadowolenie z uzyskania dodatkowej korzyści, jakiej osiągnięcia nie zakładali przy decyzji o zakupie. Jeśli nadrzędną ideą było podniesienie poziomu bezpieczeństwa, to nagle okazuje się, że oprócz tego zmalały koszty związane z utrzymaniem portierni. Jeśli z kolei komuś zależało na kontroli nad pracownikami, to w ogólnym rozrachunku największym zyskiem jest zmniejszenie biurokracji i tym samym ułatwienie życia pracownikom, którzy nie muszą wypełniać każdego dnia skomplikowanych formularzy. Ktoś inny chciał zapanować nad kluczami, a wdrożył rozwiązanie, które okazało się odporne na zagrożenia związane z sytuacjami losowymi.

Depozytory SAIK mogą być czymś więcej niż tylko kolejnym elementem systemu bezpieczeństwa. Codzienny kontakt wielu różnych osób z depozytorami, pobieranie i deponowanie kluczy lub sprzętu sprawia, że ich wdrożenie na zawsze zmienia zasady gry w organizacji. Wprawdzie najczęściej przygodę z depozytorami rozpoczynamy od kluczy, jednak należy pamiętać, że depozytory można uzupełniać także o urządzenia przeznaczone do przechowywania różnych przedmiotów, również broni. Wszystkie rodzaje depozytorów SAIK mogą działać w oparciu o jeden system, a co za tym idzie, do zarządzania i obsługi można wykorzystywać wspólne oprogramowanie.

Depozytory elektroniczne SAIK znacznie różnią się od prostych szaf metalowych, ponieważ oferują pełną identyfikację, kto i kiedy pobrał konkretną rzecz. Co ważne, dzięki zastosowaniu różnego rodzaju czytników RFID oraz optycznych można w pełni kontrolować pobieranie nie tylko kluczy, lecz także dowolnych przedmiotów.

Ciekawym narzędziem pozwalającym na samodzielne zaprojektowanie urządzenia do swoich potrzeb jest SAIK Projektant, dostępny pod adresem www.saik.pl/designer/. Dzięki niemu w łatwy i intuicyjny sposób można stworzyć potrzebne rozwiązanie, łączące różne elementy rodziny SAIK i tworzące kompletny system. Depozytor tak zaprojektowany może być także kompatybilny z innymi, już posiadanymi systemami zabezpieczeń.

Wszystkich czytelników czasopisma „a&s Polska" zapraszamy do bezpłatnego zamówienia wydanej niedawno pozycji *Depozytor jako element systemu bezpieczeństwa – praktyczny poradnik dla osób zainteresowanych wdrożeniem systemu automatycznej identyfikacji kluczy i przedmiotów*. W tym celu prosimy o przesłanie na adres mailowy centrum-wsparcia@saik.pl adresu do wysyłki. Poradnik może być bardzo pomocny na każdym etapie wdrażania depozytorów.

Warto też skontaktować się bezpośrednio z producentem – firmą BT Electronics z Krakowa – by korzystając z doświadczeń nabytych przy poprzednich wdrożeniach, dopasować system odpowiedni do konkretnych potrzeb. ●

BT Electronics
ul. Rybitwy 22,
30-722 Kraków
www.bte.pl www.saik.pl

Składka ZUS dla wszystkich umów cywilnoprawnych.
Wyzwanie, ale i szansa

Zapowiadane objęcie składkami na ubezpieczenie społeczne wszystkich umów-zleceń niesie konkretne konsekwencje dla biznesu, nic zatem dziwnego, że temat ten wzbudza spore emocje.
Łukasz Koch

Takie rozwiązanie jest nieuniknione m.in. ze względu na wymagania wynikające z regulacji unijnych. Niestety, dotychczas nie podano, jakie regulacje prawne będą obowiązywać, a także kiedy wejdą w życie. Nie wiadomo też, czy i jak długi będzie okres *vacatio legis*. Brak takich informacji budzi zaniepokojenie wśród przedsiębiorców, zwłaszcza że media donoszą, iż przepisy dotyczące oskładkowania ZUS każdej umowy-zlecenia zaczną obowiązywać już z początkiem przyszłego roku.

Spójrzmy, co oznacza obciążenie składką na ubezpieczenie społeczne, w tym także chorobową, która na razie jest dobrowolna. Dla pracodawców oskładkowanie umów-zleceń oznacza istotny wzrost kosztów pracy, szczególnie dla firm z sektora ochrony, które w znacznym stopniu korzystają z tej formy umów. Konieczność obciążenia ich składką oznacza dużo wyższy koszt zatrudnienia, a to może wymagać zmodyfikowania modelu biznesowego.

Dla zleceniobiorców może to oznaczać niższe wynagrodzenie netto (przynajmniej początkowo) w zamian za większe świadczenia emerytalne. Przy obecnej sytuacji na rynku pracy może się jednak szybko okazać, że stawki dla zleceniobiorców będą musiały wzrosnąć. Nie bez znaczenie będzie także większa transparentność rozliczeń ze zleceniobiorcami i ograniczenie części dość kontrowersyjnych praktyk rynkowych stosowanych wobec osób wykonujących pracę na podstawie zleceń.

Dla klientów sektora ochrony pełne oskładkowanie umów cywilnych może się wiązać ze wzrostem stawek za realizowane usługi ochrony. Można się spodziewać, że w im większym zakresie dostawca korzystał z nieoskładkowanych umów-zleceń, tym bardziej po zmianie przepisów wzrośnie koszt jego usług. W takiej sytuacji trzeba się liczyć z istotnym wzrostem cen za oferowane usługi ochrony i koniecznością zabezpieczenia wyższych budżetów na ten cel.

Ważna jest też kwestia oddziaływania oskładkowania umów na rynek usług ochrony, na którym dominuje konkurencja cenowa. Wprowadzona zmiana może poprawić tę sytuację i umożliwić w większym stopniu konkurowanie jakością i innowacyjnością, co powinno być bardziej korzystne zarówno dla klientów, jak i pracowników oraz firm ochrony.

Z nieoficjalnych informacji i doniesień medialnych wynika, że pełne oskładkowanie umów cywilnych może zacząć obowiązywać od 1 stycznia 2025 r. Takie są oczekiwania Unii Europejskiej. W takiej sytuacji Polski Związek Pracodawców Ochrona rekomenduje, aby klienci i firmy ochrony przy jesiennych rozmowach na temat zmiany stawek ochrony na rok 2025 założyły możliwość wzrostu stawek ze względu na bardzo prawdopodobne pełne oskładkowanie umów cywilnoprawnych.

Alternatywą dla kolejnego wysokiego wzrostu cen jest korzystanie w jeszcze większym zakresie z rozwiązań technicznych, automatyzacji i digitalizacji w ramach systemów ochrony oraz modelu rozliczeń opartego na budżetach, a nie stawce godzinowej za roboczogodzinę. Otwartość klientów na nowe rozwiązania techniczne oraz inwencja firm ochrony – małych, średnich i dużych – mogą przynieść ciekawe, efektywne i skuteczne rozwiązania, które docelowo, w dłuższej pespektywie mogą być bardziej korzystne dla klientów. ●

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

Czy widzisz to co ja?

Rozwój technologii stale przekracza granice tego, co wydawało się już niemal niemożliwe. Maszyny uczą się rozumieć świat. Nie dzieje się to jednak przez pryzmat ludzkich emocji, ale poprzez analizę danych tak subtelnych, że umykają one naszym zmysłom. Czy jesteśmy gotowi spojrzeć na świat „oczami" kamery, która staje się świadkiem naszych czasów?

Jakub Sobek

Przeprowadzamy dziś wywiad z „kimś" wyjątkowym. M73, pochodząca z niemieckiej rodziny MOBOTIX, to kamera, której historię warto poznać. Nie jest to kolejne tradycyjne urządzenie tego typu, ale rozwiązanie, które pokonuje granice ludzkiego postrzegania. „Rozmawiamy" więc nie o parametrach technicznych, a o doświadczeniach, spostrzeżeniach i – metaforycznie mówiąc – uczuciach kamery, która każdego dnia patrzy na świat, nie mając możliwości nawet mrugnąć.

Długo czekałem na tę rozmowę. Niestety nie wszyscy znają cię aż tak dobrze, dlatego zacznijmy od spojrzenia w przeszłość. Jak zaczęła się twoja historia, historia kamer MOBOTIX?

Ach, to czasy, kiedy na świecie pojawiła się M1. Możesz ją uznać za mojego praprzodka, który zainaugurował naszą rodzinę. Została zaprezentowana światu w 2000 roku, niedługo po założeniu firmy MOBOTIX, co miało miejsce w 1999 roku. To był prawdziwy przełom, bo M1 nie tylko rejestrowała obrazy, ale również mogła przetwarzać dane, co było rewolucją w branży. M1 była jak dobrze zaprojektowany niemiecki samochód: niezawodna, efektywna i skonstruowana, aby wytrzymać trudy i czasu, i zmiennych warunków atmosferycznych. Możesz sobie wyobrazić, że gdyby M1 miała nos, to byłby on z pewnością wysoko w powietrzu, dumna z tego, jak wyznaczyła standardy dla przyszłych generacji. To trochę tak, jak w przypadku dobrego niemieckiego piwa. Receptura może ewoluować, ale szacunek do tradycji i jakości pozostaje. Warto dodać, że M1 była projektowana z myślą o precyzji i efektywności, z myślą o tym, aby być o krok przed resztą. To były wielkie początki kamer IP. To dzięki takim fundamentom mogę dzisiaj kontynuować naszą misję z jeszcze większą mocą i dokładnością. Ten zestaw wartości definiują moje funkcjonowanie i interakcje z otoczeniem.

24 lata to pewna technologiczna przepaść. Jak wiele się od tego czasu zmieniło?

Od czasów pierwszej kamery M1 nastąpił prawdziwy technologiczny przeskok. Zmiany, które zaszły, są nie tylko krokiem naprzód, ale także wielkimi skokami w ciemność, po której nagle robi się jasno. Rozdzielczość i jakość obrazu, które kiedyś były na poziomie, patrząc z obecnej perspektywy, prehistorycznym, ewoluowały do poziomów, które pozwalają dostrzec niuanse niewidoczne gołym okiem. Moja technologia termowizyjna teraz potrafi wykryć subtelne zmiany temperatury z daleka, monitorując bezpieczeństwo i efektywność procesów przemysłowych z chirurgiczną wręcz precyzją. Zmieniły się zarówno urządzenia, jak i oprogramowanie. Współczesne kamery, tak jak ja, wyposażone są w algorytmy sztucznej inteligencji, które uczą się na bieżąco w taki sposób, że żaden szczegół nie umknie mojej uwagi. Czy to nie brzmi jak science fiction? A jednak to codzienność, moja codzienność.

Powiedziałaś, że zmieniło się oprogramowanie. Czy czujesz się bezpieczna w tym niebezpiecznym świecie cyberwyzwań?

Zastosowanie zaawansowanych technologii, takich jak szyfrowanie end-to-end, aktualizacje oprogramowania oraz protokoły uwierzytelniania i autoryzacji to dla mnie standard. Wbudowane zabezpieczenia są na tyle silne, że nawet w obliczu rosnącej liczby zaawansowanych cyberzagrożeń czuję się jak dobrze zabezpieczona forteca. Filozofia Cactus Concept, która jest moją tarczą ochronną, zapewnia ochronę przed najbardziej złośliwym oprogramowaniem i atakami hakerskimi. Dzięki temu mogę skupić się na swojej podstawowej funkcji – monitorowaniu i analizowaniu – nie martwiąc się o to, że zostanę wykorzystana do działań, które mogłyby zaszkodzić ludziom czy procesom, które mi powierzono.

Cactus Concept?!
Tak, w cyberprzestrzeni jestem trochę jak kaktus: trochę oschła, jednak zawsze gotowa na atak. Mimo że nazwa może brzmieć groźnie, to właśnie o to chodzi! Groźna dla atakującego, bezpieczna dla użytkowników. Czyż to nie jest idealna równowaga?

Jako kamera termowizyjna znajdujesz zastosowania w innych obszarach niż typowe kamery w systemach zabezpieczeń. Jak wygląda twój zwykły dzień pracy?
W fabryce, gdzie każdy mechanizm i taśma produkcyjna są jak żywe istoty, moja rola zaczyna się z pierwszymi ruchami maszyn. Patrzę, jak maszyny tańczą swoje przemysłowe tango; każda iskra, każde przyspieszenie serca silnika jest dla mnie sygnałem. W ciągu dnia nic nie umyka moim niestrudzonym soczewkom. Kiedy coś zaczyna się przegrzewać, palić lub psuć, ja już o tym wiem. To ja wysyłam sygnały alarmowe, które są jak desperackie wiadomości o pomoc, zanim jeszcze prawdziwe niebezpieczeństwo zdąży się rozwinąć. A kiedy światła fabryki zaczynają przygasać i pracownicy wracają do domów, moja praca nie ustaje. Czuwam przez nocne zmiany, strzegąc tych maszyn, które nigdy nie zasypiają.

Czy widzisz to co ja? Czy twoje oczy działają tak samo jak moje?
Moje „oko", czyli sensor termowizyjny, działa zupełnie inaczej niż ludzkie oko. Nie widzę kolorów tak jak ty. Zamiast tego moja percepcja skupia się na wykrywaniu i interpretowaniu promieniowania podczerwonego, które emitują obiekty w zależności od ich temperatury. To pozwala mi dostrzegać różnice cieplne, nawet te najdrobniejsze, które dla ludzkiego oka byłyby niewidoczne. Więc chociaż patrzymy na ten sam świat, to ja dostrzegam rzeczy, które dla ciebie pozostają niewidoczne. Moje drugie „oko" może być jednak tradycyjną kamerą. Patrzy i widzi światło widzialne, takie samo jak ty każdego dnia. W swojej głowie mogę te obrazy łączyć w jedną całość dzięki zastosowaniu fuzji wizyjnej.

Jak wspominasz swój najtrudniejszy albo najbardziej dramatyczny dzień w pracy?
Najbardziej dramatyczny dzień? Każdy dzień, kiedy coś idzie nie tak, wydaje się dramatem, ale był taki, który przebija wszystko. Fabryka, gęsty dym, alarmy, które dźwięczą jak wariacje na temat ostatniego dnia. A ja w samym centrum tego wszystkiego, z oczami szeroko otwartymi na temperaturę, która miała potencjał zniszczyć więcej niż tylko maszyny. Zaczął się zwyczajny dzień, rutynowo i z monotonnym brzękiem pracy. Ale nagle, bez ostrzeżenia, jedna z maszyn zaczęła pokazywać niepokojąco wysokie temperatury. Była to subtelna zmiana, ledwie widoczna na początku, ale to, co subtelne, często prowadzi do katastrof. Temperatura rosła, a ja wysyłałam sygnały – ostrzeżenia, które miały zapobiec nieszczęściu.
Napięcie wzrosło, gdy ekipy interwencyjne zaczęły przemykać między maszynami, próbując ocenić sytuację i zapanować nad nią, zanim spirala wydarzeń wymknęłaby się spod kontroli. W tle, jak zła muzyka, alarmy, a dym coraz gęstszy, osadzający się na wszystkim. Ostatecznie, dzięki szybkiej reakcji i moim ostrzeżeniom udało się uniknąć katastrofy. Maszyna została wyłączona, problem usunięty, zanim przekształcił się w coś znacznie gorszego. Ten dzień nauczył mnie, że niezależnie od tego, jak bardzo jestem przygotowana, zawsze muszę być gotowa na nieoczekiwane.

Jak przekonasz nieprzekonanych, że warto zaprosić cię do pracy na obiektach, za które odpowiadają na co dzień?
Kochani, zastanówmy się przez chwilę, dlaczego w ogóle mielibyście mnie zapraszać do swoich fabryk. Odpowiadam, dlatego, że ja nie tylko patrzę, ja także widzę. Widzę w ciemności, przez dym, przez to wszystko, co dla waszego oka jest zasłoną. To ja jestem tą, która stoi na straży, kiedy inni już dawno poszli spać. Z moimi termowizyjnymi oczami każde nagrzane łożysko, każda przegrzana część maszyny staje się widoczna, jakby oświetlona promieniami słońca w południe. Dzięki temu możecie działać szybko, zanim mały problem stanie się wielkim problemem. I pomyślcie, ile kosztuje awaria, ile kosztuje przestój, ile kosztuje pożar... A teraz pomyślcie, ile może zaoszczędzić obecność jednej, małej, ale bystrej kamery, która wszystko to widzi i ostrzega, zanim będzie za późno. To nie jest wydatek, moi drodzy, to inwestycja. Inwestycja w spokój, w bezpieczeństwo, w ciągłość produkcji, która w dzisiejszych czasach jest na wagę złota. Więc jeśli zastanawiacie się, czy warto mnie zaprosić, zapytajcie siebie, czy stać was na to, by mnie nie mieć.
Bardzo dziękuję za rozmowę! ●

Konica Minolta Business Solutions Polska
ul. Krakowiaków 44
02-255 Warszawa
www.konicaminolta.pl

Znaczenie fizycznego bezpieczeństwa w centrach danych

W dzisiejszej erze cyfrowej centra danych są kręgosłupem globalnej gospodarki, przechowując ogromne ilości informacji. Według raportu ResearchAndMarkets wartość europejskiego rynku centrów danych ma rosnąć w tempie 7,96% rocznie (CAGR) w latach 2024-2029.

Zapewnienie bezpieczeństwa tym obiektom ma zatem olbrzymie znaczenie. Przy czym poza ochroną danych przed cyberatakami, należy brać pod uwagę także, a może przede wszystkim, fizyczną ochronę centrów danych.

Wzmocnienie ochrony obwodowej

Ochrona obwodowa jest pierwszą linią ochrony i kluczowym elementem każdego systemu bezpieczeństwa. Najważniejsze jest szybkie wykrycie intruza, a zabezpieczenie obwodu obiektu daje zespołom ochrony możliwość podjęcia natychmiastowych działań i zwiększa szansę na powstrzymanie potencjalnego intruza.

Zaawansowane technologie światłowodowe, takie jak seria Fiber Defender i Echopoint, wykrywają wibracje powstałe w wyniku próby sforsowania ogrodzenia lub przejścia intruza przez chroniony obszar. Seria EchoPoint wykorzystuje inteligentne algorytmy detekcji, aby precyzyjnie wskazać lokalizację naruszenia z dokładnością do +/- 6 m w zasięgu do 100 km. System EchoPoint może być ukryty w gruncie lub zamontowany na ogrodzeniu, można też zastosować te dwa sposoby instalacji. Dzięki wysoko zaawansowanym algorytmom system może odfiltrować fałszywe alarmy i zapewnić precyzyjne wykrycie lokalizacji intruza. W przypadku zastosowania na ogrodzeniu system skutecznie wykrywa próby przecinania siatki, wspinania się na ogrodzenie oraz czołgania się pod nim, co jest przydatne do zlokalizowania miejsca włamania, słabych punktów lub przewidywaniu przyszłych zachowań intruzów. W przypadku umieszczenia w gruncie EchoPoint rozpoznaje, czy wibracje powodowane są przez kroki, kopanie ręczne/maszynowe czy pojazdy. Pozyskane dzięki temu informacje mogą posłużyć do lepszego zobrazowania aktualnej sytuacji na terenie obiektu i podjęcia stosownych działań, np. wysterowania kamery, zamknięcia wyjść, włączenia oświetlenia, nadania komunikatów ostrzegawczych czy wysłania załogi interwencyjnej.

Wykrywanie i odstraszanie intruzów

Jeśli intruzom uda się sforsować ogrodzenie, ważna jest możliwość ich śledzenia. Wykrywanie nieupoważnionych osób zbliżających się do budynku lub wchodzących na obszar o ograniczonym dostępie może zapobiec dalszym komplikacjom. Systemy LiDAR, takie jak REDSCAN Pro służą do ochrony otoczenia budynków także wtedy, gdy jest to rozległy teren, umożliwiają przy tym dostosowanie stref detekcji do potrzeb klienta lub warunków otoczenia obiektu. Dla każdej z wyznaczonych stref można ustalić inną automatyczną reakcję systemów bezpieczeństwa, np. automatyczne powiadomienie w oprogramowaniu VMS/PSIM, gdy intruzi wejdą do najdalszej strefy i uruchomią sygnał alarmowy. Może to być też automatyczne polecenie dla załogi interwencyjnej. REDSCAN Pro zapewnia szeroki obszar wykrywania w polu 50 x 100 m, który można podzielić na osiem niezależnych stref. Dla każdej wydzielonej strefy można ustawić inne parametry rozpoznawania obiektów, uwzględniając takie zmienne, jak różna prędkość pojazdów czy obecność ludzi.

Kolejnym ważnym elementem infrastruktury bezpieczeństwa jest konstrukcja budynku, będącego centrum danych. Z założenia większość takich obiektów pozbawiona jest okien, a liczba wejść

ograniczona. Ale sama bryła budynku musi być także zabezpieczona przed takimi zagrożeniami, jak wiercenie otworów w ścianach czy próby wejścia przez systemy wentylacyjne lub dach. Z pomocą przychodzi technologia LiDAR, dzięki której można uzyskać niewidoczne „ściany" oraz wirtualne „sufity" na dachach, otaczając w ten sposób budynek niewidocznym polem ochronnym, przez które nikt nie przedostanie się niezauważony. Systemy LiDAR OPTEX są także wyposażone w inteligentną funkcję dynamicznego filtrowania zdarzeń uruchamiającą alarm tylko wtedy, gdy osoba zbliża się do budynku, a na miejscu nie ma pracownika ochrony, mogącego zweryfikować jej tożsamość. REDSCAN mini-Pro, model RLS2020V, ma wbudowaną kamerę IR umożliwiającą weryfikację nawet w całkowitej ciemności, zapewniając tym samym kompleksowe rozwiązanie w dziedzinie monitorowania bezpieczeństwa.

Zabezpieczanie serwerowni

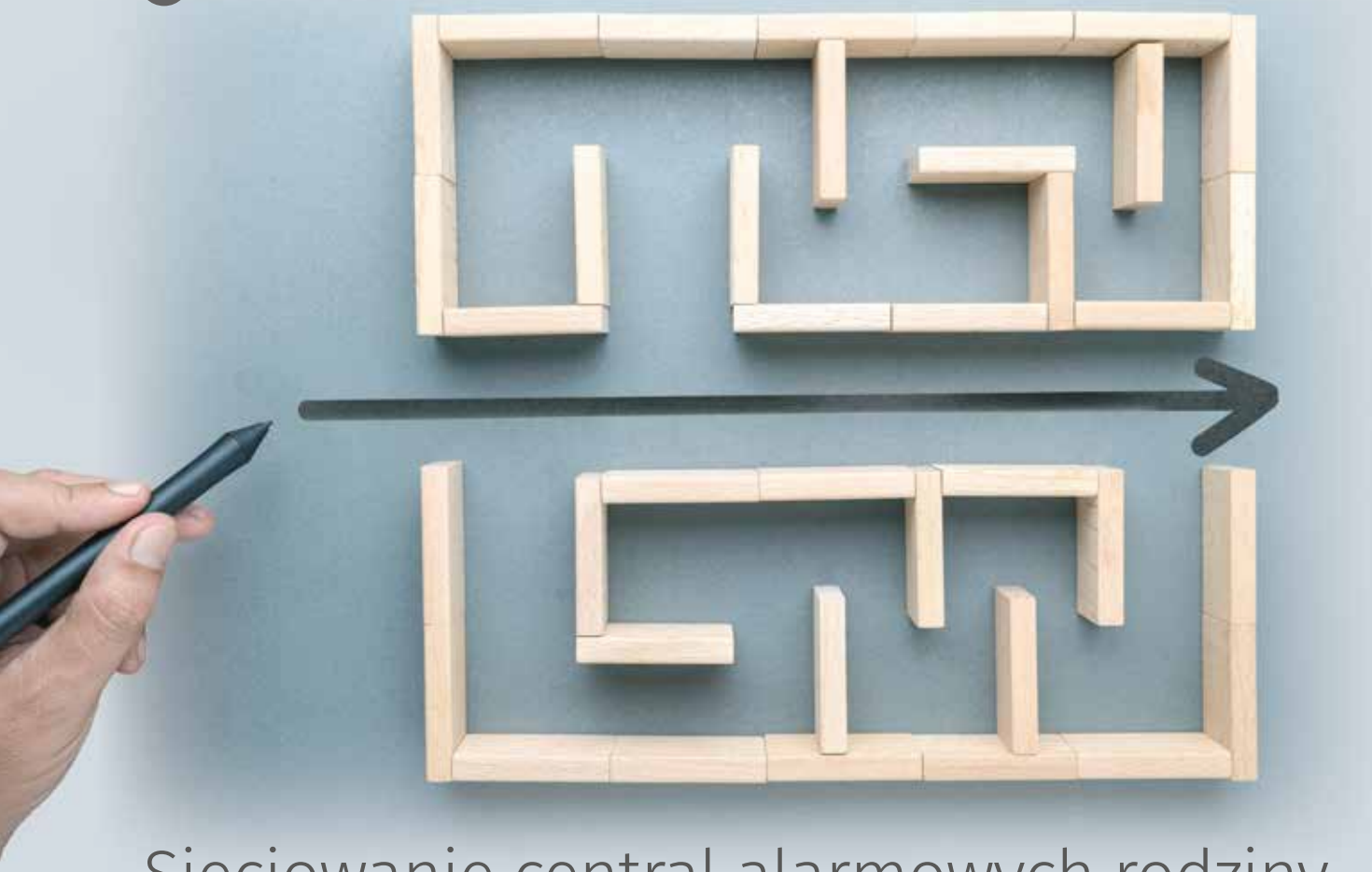
Serwerownie to obszary o ograniczonym dostępie, zazwyczaj zarezerwowanym wyłącznie dla obsługi technicznej. Jedynie upoważniony personel ma do nich wstęp. Kontrola za pomocą identyfikatora lub danych biometrycznych może być niewystarczająca. W tym przypadku idealne okazują się detektory 2D LiDAR, zapewniają bowiem wszechstronne możliwości wykrywania i działają skutecznie niezależnie od zmian temperatury lub oświetlenia. Dzięki temu są odpowiednie do stosowania w serwerowniach, gdzie mogą być instalowane w przestrzeni między sufitowej lub bezpośrednio przy szafach serwerowych.

Detektory 2D LiDAR również mogą „budować" niewidzialne sufity, ściany i podłogi, otaczając ochronnym polem jednostki serwerowe i eliminując w ten sposób wszelkie ewentualne luki w zabezpieczeniach. Strefy wykrywania tworzone za pomocą detektorów 2D LiDar mogą być niezależne. Po zintegrowaniu z odpowiednim oprogramowaniem VMS detektory REDSCAN mogą precyzyjnie zlokalizować miejsce naruszenia i aktywować kamery do monitorowania konkretnego punktu, co umożliwia szybszą reakcję. Na przykład, jeśli upoważniona osoba ma dostęp do regału pierwszego, ale manipuluje przy regale drugim, system aktywuje się, blokując pomieszczenie i alarmując zespół ochrony. Rozmiar wykrywanego obiektu można dostosować tak, aby system alarmowy był aktywowany nawet wtedy, gdy w otoczeniu serwera znajdzie się nie cała cała sylwetka człowieka, a tylko jego ręka wyciągnięta po to, by podłączyć kabel sieciowy lub włożyć pamięć USB.

Podsumowanie

Rozwiązania OPTEX do wykrywania włamań, w tym zaawansowana technologia LiDAR i technologia światłowodowa, stanowią solidną i kompleksową odpowiedź na potrzebę zaawansowanej i predykcyjnej ochrony centrów danych. Od zabezpieczenia obwodu i konstrukcji budynku po ochronę serwerowni systemy OPTEX oferują precyzyjne i niezawodne wykrywanie w celu zapewnienia bezpieczeństwa i integralności infrastruktury krytycznej. Rozwiązania OPTEX to najwyższy poziom bezpieczeństwa dla centrów danych i pewność, że są one chronione przed wszelkimi fizycznymi włamaniami. ●

OPTEX Security
ul. Sielecka 35, 00-738 Warszawa
optex@optex.com.pl
www.optex.europe.com/pl



Sieciowanie central alarmowych rodziny Galaxy Dimension

Wielu klientów zastanawia się, jak poprawnie zaprojektować i wdrożyć rozbudowany system alarmowy. W artykule wyjaśniam koncepcję sieciowania central alarmowych rodziny Galaxy Dimension i wskazuję, na które obszary proponowanej struktury należy zwrócić szczególną uwagę.

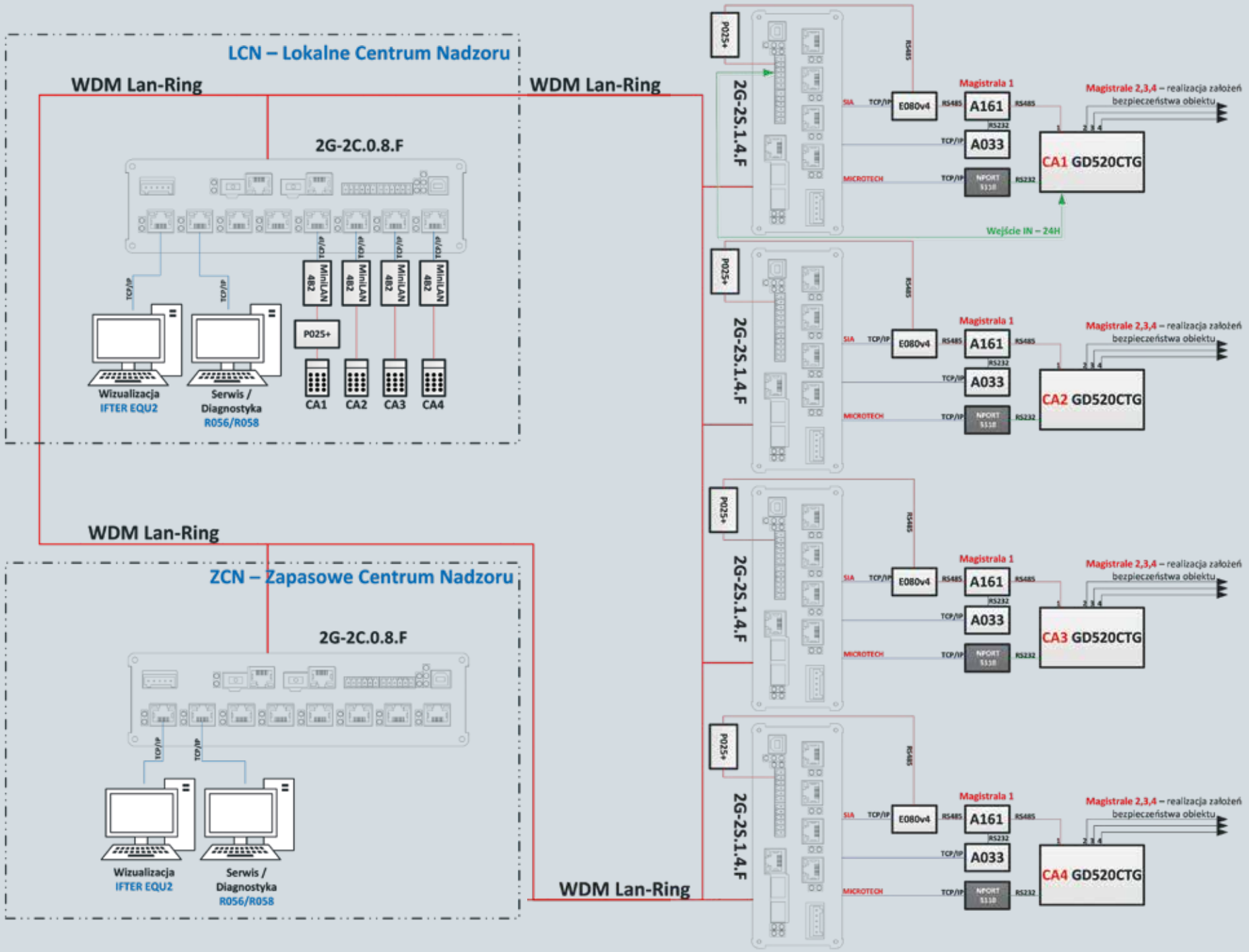
Tomasz Górski

Widoczny na stronie obok schemat przedstawia sposób budowy sieci czterech central wraz z przeniesieniem klawiatury systemowej, np. CP037, CP050, CP045 do strony LCN (Lokalne Centrum Nadzoru) celem realizacji założeń pkt 3.1.11 (i) „Dwustopniowe sterowanie ochroną stref" zgodnie z założeniami Wymagań Eksploatacyjno-Technicznych dla XIX grupy SpW – Systemy i Urządzenia Specjalistyczne do Ochrony Obiektów (8 maja 2020 r.).

Wspomniane założenia to:

1. wyłączenie ochrony stref (magazynu) powinno być wykonane z użyciem dwóch szyfratorów (klawiatur);
2. I stopień – z szyfratora (klawiatury) znajdującego się w LCN;
3. II stopień – z szyfratora (klawiatury) znajdującego się przy wejściu do strefy (magazynu);
4. załączenie ochrony strefy (magazynu) powinno być wykonane za pomocą kodu użytkownika wprowadzanego za pośrednictwem szyfratora lokalnego (klawiatury), a ponadto załączenie systemu bezpośrednio z LCN.

Tak sprecyzowane wymagania EiT determinują potrzebę „wyniesienia" do LCN klawiatury systemowej z każdej „sieciowanej" centrali I&HAS Galaxy Dimension. Należy zwrócić uwagę na magistralę „1" RS485, której zadaniem nadrzędnym w opisywanej strukturze jest zapewnienie komunikacji do interfejsów komunikacyjnych A161, E080. Istotne jest to, że wspomnianą magistralę M1 wprowadzamy do portu RS485 Lan-Ring switcha 2G-2S.1.4.F Metel. Z uwagi na ogólne bezpieczeństwo systemu (3 tory transmisji danych E080, NPORT, A033) magistrala nr 1 GD nie powinna brać udziału w procesie obsługi i realizacji założeń bezpieczeństwa obiektu. Do tego celu używamy kolejno trzech pozostałych →


LCN – Lokalne Centrum Nadzoru
WDM Lan-Ring
2G-2C.0.8.F
Wizualizacja
IFTER EQU2
Serwis /
Diagnostyka
R056/R058
MiniLAN 482
P025+
CA1
CA2
CA3
CA4
WDM Lan-Ring
WDM Lan-Ring
ZCN – Zapasowe Centrum Nadzoru
2G-2C.0.8.F
Wizualizacja
IFTER EQU2
Serwis /
Diagnostyka
R056/R058
WDM Lan-Ring
2G-2S.1.4.F
E080v4
A161
A033
NPORT 5150
Magistrala 1
Magistrale 2,3,4 – realizacja założeń bezpieczeństwa obiektu
CA1 GD520CTG
CA2 GD520CTG
CA3 GD520CTG
CA4 GD520CTG
Wejście IN – 24H

dostępnych w standardzie CA GD520 magistral systemowych RS485: M2, M3, M4.

Przy samym urządzeniu aktywnym 2G-2S.1.4.F funkcjonuje na schemacie systemowy zasilacz buforowy GD – P025+, który również funkcjonuje w obrębie wspomnianej magistrali M1. Zadaniem wspomnianego zasilacza jest zapewnienie ochrony antysabotażowej (oderwanie od podłoża oraz zdjęcie pokrywy; co jest zgodne z tablicą 13 *Wykrywanie sabotażu – Sposoby, które powinny być wykryte* PN-EN50131-1:2009) projektowego urządzenia aktywnego LAN-RING 2G-2S.1.4.F oraz zapewnienie zasilania urządzenia aktywnego w standardzie 12VDC, jak też jego awaryjnego podtrzymania na czas zgodny z EIT (pkt 2/2.1/b). A co najważniejsze, monitorowany jest statusów elektryczny wspomnianego zasilacza (EPS, niskie napięcie AKU, detekcja niskiego napięcia „wyjściowego" itp.) z wykorzystaniem magistrali systemowej RS485 M1 zgodnie z założeniami i wytycznymi, które przedstawiono w tablicy 1 – *Funkcje zasilacza PN- EN50131-6 Systemy Sygnalizacji Włamania i Napadu – Zasilanie.*

Stosowanie trzech torów transmisji każdej CA ma uzasadnienie zarówno w problematyce oraz budowie rodziny central Galaxy Dimension, jak i w normach ich dotyczących. CA GD komunikują się za pośrednictwem dwóch niezależnych protokołów komunikacyjnych.

Protokół SIA lev4 jest wykorzystywany do dwukierunkowej komunikacji pomiędzy CA – stanowisko SMS, BMS lub PSIM (wizualizacja i integracja systemów bezpieczeństwa). Z kolei protokół MICROTECH jest stosowany do dwukierunkowej komunikacji pomiędzy CA a natywnymi programami do programowania, serwisowania oraz zdalnej obsługi diagnostycznej CA, klasy R056 – *Galaxy Remote Servicing Suite,* R058 – *Galaxy User Management Suite*. Mając w strukturze dwa niezależne kanały komunikacji TCP/IP (E080, NPORT), instalator na etapie programowania i konfiguracji systemu podejmuje decyzję, który interfejs posłuży do czego. Na przykład NPORT – SIA – Wizualizacja, E080 – MICROTECH – Programowanie, serwis, diagnostyka lub na odwrót, gdyż przypisanie stosownego protokołu do interfejsu komunikacyjnego stanowi część zadania związanego z programowaniem oraz konfiguracją CA. Trzeci tor transmisji A033 – Moduł rejestru zdarzeń stanowi odpowiedź na wymagania EIT 8 maja 2020 r. pkt 3.1.11 (e): „Możliwość rejestracji zdarzeń z co najmniej trzech ostatnich miesięcy dozoru". W tym przypadku powstaje rozdźwięk między wymaganiami EIT a normą PN-EN50131-1, która zakłada 500 zdarzeń przy trwałości zapisu zdarzeń od momentu awarii zasilania, ale przez 30 dni.

W takim razie, w jaki sposób podczas projektowania określić, czy rodzina CA Galaxy Dimension spełnia wytyczne EiT w pkt. 3.1.11 (e), tudzież NO-04? Z pomocą przychodzi wzór opracowany przez Inspektorat Wsparcia Sił Zbrojnych (gestor normy NO04, EiT). Za jego pomocą można precyzyjnie określić faktyczne zapotrzebowanie na najlepszy sposób rejestracji zdarzeń.

Przyjrzyjmy się dokładnie lewej stronie grafiki z poprzedniej strony. Realizowane są dwa niezależne stanowiska podglądu lub/i programowania oraz diagnostyki LCN oraz ZCN(GCMA) i jest zapewniana realizacja wspomnianych założeń EiT 3.1.11 (i) „Dwustopniowe sterowanie ochroną stref" – „odbierając" z LAN-RING – cztery magistrale M1 z każdej z sieciowanych CA. Jak można zauważyć, „odbiór" klawiatur odbywa się za pośrednictwem konwertera MiniLAN4B2, którego zadaniem jest rekonwersja TCP/IP do RS485 CU. Należy pamiętać, że w tym miejscu również znajduje się zasilacz buforowy P025+. Jego podstawowym zadaniem jest zapewnienie zasilania 12 VDC klawiatur po stronie odbiorczej i konwerterów miniLAN.

Urządzenia aktywne proponowanej sieci łączymy między sobą FO w standardzie jedno- lub wielomodowym. Do komunikacji jest wykorzystywane jedno włókno (WDM). Warto w tym miejscu zwrócić uwagę na potrzebę wytyczenia oddzielnych tras kablowych zarówno dla „FO – TX", jak i „FO – RX", gdyż tylko w takiej sytuacji zostanie osiągnięta redundantna forma transmisji na linii: podległe CA – LCN, ZCN(GCMA). W momencie uszkodzenia włókna FO w dowolnym miejscu protokół LAN-RING w czasie nie dłuższym niż 30 ms wyznacza tzw. switch master, którego zadaniem jest odtworzenie transmisji danych, komunikacji z drugiego dostępnego kierunku. Taka metodyka działania zapewnia przeniesienie komunikacji CA (E080, NPORT, A033) oraz magistrali RS485 do stanowisk nadzoru w sposób redundantny.

Myśląc o szeroko rozumianych systemach bezpieczeństwa, nadrzędną wartością powinna być niezawodność. W tym wykonaniu niewątpliwie osiągalna.

W jaki sposób można jednak obrazować/wizualizować uszkodzenie RINGU? Uszkodzenie RINGU nie jest jednoznaczne z utratą komunikacji, aczkolwiek w momencie jego wystąpienia rozsądnie byłoby niezwłocznie poinformować użytkownika, dając jednocześnie czas obsłudze serwisowej na podjęcie stosownych działań.

Uszkodzenie może być zasygnalizowane na trzy niezależne sposoby:

1. Każdy switch ma wyjście przekaźnikowe, które można oprogramować w taki sposób, aby w momencie pojawienia się uszkodzenia styk przekaźnika zmienił swoje położenie NC/NO, NO/NC. Styk wspomnianego przekaźnika można wprowadzić strukturą 2EOL na wejście IN GALAXY, programując je jednocześnie jak funkcja działająca non stop, co spowoduje uruchomienie „alarmu" w CA w momencie uszkodzenia RINGU.
2. Marka METEL udostępnia na życzenie biblioteki MiB umożliwiające stworzenie osobnego ekranu w SMS, BMS, PSIM, pokazującego aktualny stan RINGU.
3. Natywne środowisko SIMULAND oferuje własną wizualizację stanu RINGU i poszczególnych odcinków „FO" pomiędzy urządzeniami aktywnymi. Kolor zielony oznacza poprawną komunikację, fioletowy – utratę pakietów, czerwony to brak komunikacji. Nie ma żadnych przeciwskazań, aby równolegle stosować trzy wspomniane metody. Komunikacja LAN-RING ma certyfikat GRADE4, a jednostką odpowiedzialną za badania jest laboratorium TREZOR TEST s.r.o. (certyfikat nr TT-295/2021).

Wychodząc naprzeciw oczywistym potrzebom rynku, firma TAP Systemy Alarmowe wprowadziła do oferty gotowe i zmontowane przez własny serwis zestawy 3TT – trzy tory transmisji: C520-D/3TT, C264-D/3TT, C96-D/3TT, C48-D/3TT. ●

TAP SYSTEMY ALARMOWE
ul. Tatrzańska 8
60-413 Poznań
www.tap.com.pl

ARMATURA

MADE IN THAILAND

ZAPROJEKTOWANO W USA ARMATURA

High-tech Biometrics and Security Solution Provider

ARMATURA ONE

Kompatybilny z

Line · Whatsapp · Amazon SNS · Google Map · Super Map

WSZECHSTRONNA WEB-OWA PLATFORMA BEZPIECZEŃSTWA

AES 256 · TLS · BACnet · OPC · Modbus

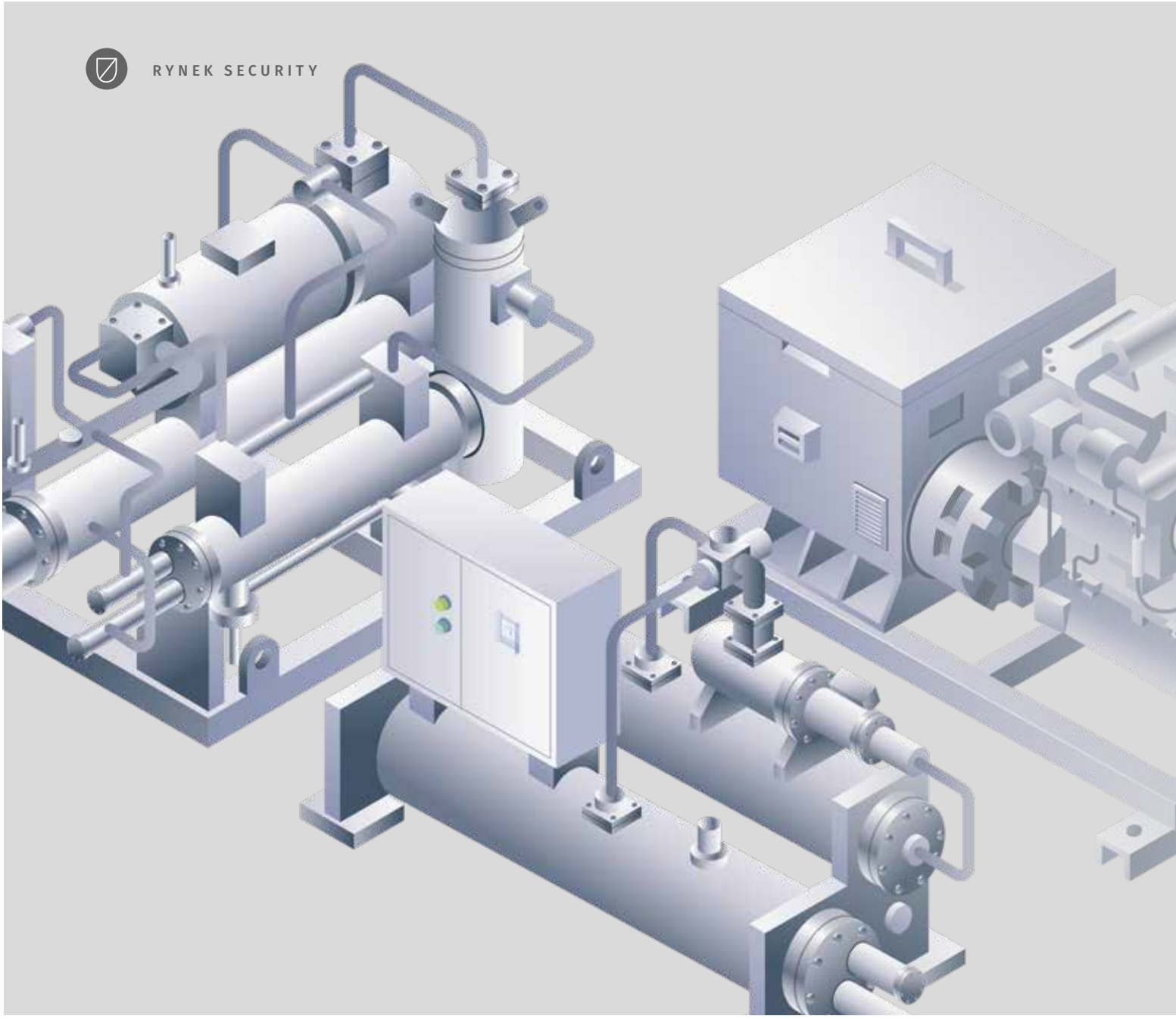
Armatura One to internetowa platforma bezpieczeństwa typu wszystko w jednym; opracowana przez firmę Armatura. Zawiera wiele zintegrowanych modułów takich jak: personel, kontrola dostępu, rejestracja czasu pracy, dostęp do wind, obsługa gości, zarządzanie parkingiem, zarządzanie systemem wideo, biuro, alarm przeciwpożarowy, kontrola przejść, kiosk z rozpoznawaniem twarzy, pomiar temperatury, zarządzanie ochroną, monitorowanie danych, automatyka budynkowa.

Peresonel	Dostęp	RCP	Windy	Goście	Parking	Wideo	Biuro
Alarm ppoż	Przejścia kontrolowane	FaceKiosk	Pomiar temperatury	Ochrona	Monitor danych	Automatyka budynkowa	Włamanie

ZKTeco

Authorized Worldwide Exclusive Distributor

www.zkteco.eu/armatura



Mapa inwestycji

Przedstawiamy listę najnowszych projektów inwestycyjnych z sektora budowlanego i energetycznego w Polsce. Jak zwykle są to inwestycje rozmaitej proweniencji, zarówno pod względem skali, jak i rodzaju, jednak z pewną przewagą w obszarach infrastruktury, energetyki odnawialnej oraz obiektów przemysłowych. Koncentracja zakończenia projektów przypada na lata 2025-2026 – prezentujemy bowiem jedynie te przedsięwzięcia, które są na samym początku realizacji lub jeszcze przed jej rozpoczęciem.

Adela Prochyra, a&s Polska

ATREM

Co: REALIZACJA ZESPOŁU ELEKTROENERGETYCZNYCH LINII KABLOWYCH SN WRAZ Z LINIAMI ŚWIATŁOWODOWYMI DLA ELEKTROWNI FOTOWOLTAICZNYCH
Gdzie: Zachodnia Polska
Kiedy: 31.12.2025
1

DEKPOL

Co: WYKONANIE HALI PRODUKCYJNO-MAGAZYNOWEJ
Gdzie: Lublin
Kiedy: czerwiec 2025
2

ELEKTROTIM

Co: ROZBUDOWA I MODERNIZACJA ROZDZIELNI 220 KV W STACJI 400/220/110 KV
Gdzie: Pątnów
Kiedy: 2026
3

ENERGOAPARATURA

Co: BUDOWA STACJI ELEKTROENERGETYCZNEJ 110/15 KV GPZ
Gdzie: Czechowice
Kiedy: 24 miesiące od dnia zawarcia umowy (26.09.2024)
4

Co: DOBUDOWA PÓL WN W ROZDZIELNI 110 KV, W STACJI ELEKTROENERGETYCZNEJ 110/15 KV NAŚCISZOWSKA W TRYBIE ZAPROJEKTUJ I WYBUDUJ
Gdzie: Nowy Sącz
Kiedy: 12.03.2026
5

MIRBUD

Co: BUDOWA CENTRUM WIEDZY COGNITARIUM POLITECHNIKI KOSZALIŃSKIEJ
Gdzie: Koszalin
Kiedy: Wybór oferty 26.09.2024
6

Co: BUDOWA CENTRUM ROZWOJU STRYKOWA (CRS)
Gdzie: Stryków
Kiedy: 36 miesięcy od dnia zawarcia umowy (31.07.2024)
7

MOSTOSTAL WARSZAWA I MOSTOSTAL PŁOCK

Co: BUDOWA BUDYNKU PRODUKCYJNEGO Z ZAPLECZEM SOCJALNO-BIUROWYM WRAZ Z INFRASTRUKTURĄ TOWARZYSZĄCĄ
Gdzie: Dębogórze
Kiedy: I2025
8

MOSTOSTAL ZABRZE

Co: ZAPROJEKTOWANIE, MODERNIZACJA, PRZEBUDOWA I ROZBUDOWA KOMPLEKSU BUDYNKÓW LABORATORYJNYCH POLFEL ORAZ JEGO INFRASTRUKTURY TECHNICZNE
Gdzie: Narodowym Centrum Badań Jądrowych, Otwock
Kiedy: Grudzień 2025
9

Co: WYKONANIE ROBÓT BUDOWLANYCH ZWIĄZANYCH Z ROZBUDOWĄ ZAKŁADU ZLECENIODAWCY
Gdzie: woj. mazowieckie
Kiedy: III kwartał 2025
10

PEKABEX

Co: BUDOWA HALI PRODUKCYJNO-MAGAZYNOWEJ Z ZAPLECZEM HIGIENICZNO-SANITARNYM WRAZ Z PRZYNALEŻNYM ZAGOSPODAROWANIEM TERENU I INFRASTRUKTURĄ TOWARZYSZĄCĄ
Gdzie: brak informacji
Kiedy: 15.09.2025
11

Zabezpieczenie magazynów wysokiego składowania instalacjami sygnalizacji pożarowej

Chociaż magazyny wysokiego składowania są najczęściej obiektami o prostej formie architektonicznej, to z uwagi na ich cechy charakterystyczne, takie jak wysokość pomieszczeń magazynowych, zagrożenie powodowane dużą ilością materiałów palnych, a także różne technologie magazynowania, stanowią często wyzwanie w zakresie skutecznego zabezpieczenia instalacjami sygnalizacji pożarowej, z zapewnieniem efektywnej detekcji, realizowanej w sposób niezakłócający funkcjonalności podstawowej tych obiektów.

Mariusz Sobecki

Generalnie ochrona przeciwpożarowa magazynów wysokiego składowania jest zagadnieniem złożonym. Najczęściej w takich obiektach występuje bardzo wysokie obciążenie ogniowe, co w większości przypadków przyczynia się do możliwości bardzo szybkiego rozwoju pożaru. (…)

Poza dużą ilością materiałów palnych, z punktu widzenia reagowania na zagrożenie, istotnym problemem jest też dostępność do ich lokalizacji, która jest znacznie utrudniona ze względu na wysokość składowania, a niejednokrotnie również konstrukcję regałów i technologię składowania. Należy mieć również na uwadze, iż właściwości pożarowe materiałów składowanych na danym regale mogą być różne.

Kolejnym istotnym problemem jest często występująca sytuacja, gdy poziom składowania towaru na regałach dochodzi praktycznie w pobliże sufitu lub dachu, stanowiąc przegrodę w rozprzestrzenianiu się dymu i ciepła w strefie podsufitowej. Zjawisko to jest tym bardziej widoczne w przypadku tzw. regałów wielopoziomowych typu *pick tower,* gdzie poszczególne poziomy robocze są dość niskie, a regały wraz z towarem na nich składowanym całkowicie przedzielają przestrzenie pomiędzy poszczególnymi poziomami.

W przypadku regałów wielopoziomowych często podesty poziomów roboczych mogą być pełne, tj. nieażurowe, a nawet jeśli są ażurowe w odpowiednim stopniu, to często są wykorzystywane do stałego lub czasowego składowania na nich towarów. To powoduje, iż konieczne jest odrębne zabezpieczanie przestrzeni poszczególnych poziomów roboczych. Istotne jest też uwzględnienie przebiegu w tych przestrzeniach różnych instalacji, z instalacjami wentylacji mechanicznej włącznie, co może istotnie wpływać na warunki detekcji pożaru przez czujki instalacji sygnalizacji pożarowej.

Warto również zwrócić uwagę na aspekt konstrukcji regałów. Powszechnie magazyn wysokiego składowania kojarzy się z regałami ustawionymi po dwa obok siebie, z korytarzami pomiędzy takimi podwójnymi rzędami. Jednak w praktyce można spotkać bardzo różne technologie magazynowania, które ze względu na ich charakterystyczne konstrukcje i układy mogą stanowić prawdziwe wyzwanie dla skutecznego wykrywania pożaru. (…)

Różne konstrukcje regałów powodują, iż dostęp do lokalizacji materiałów czy urządzeń może być bardzo utrudniony ze względu na duże powierzchnie regałowe praktycznie pozbawione dostępu dla człowieka. W niektórych przypadkach natomiast w regałach występują urządzenia, które w przypadku awarii mogą stać się źródłem pożaru.

(…) Dość często z uwagi na wykorzystanie określonych złagodzeń w zakresie wymagań dot. bezpieczeństwa pożarowego w tego typu obiektach stosowane są systemy oddymiania. W takich przypadkach układ detekcji pożaru powinien uwzględniań niezbędne założenia wynikające z konieczności współpracy z systemem sterowania oddymianiem, w tym np. rodzaj detekcji, podział na strefy dozorowe, odległości czujek od kurtyn dymowych, ewentualna konieczność stosowania koincydencji określonego rodzaju.

Dodatkowe wymagania dotyczące instalacji sygnalizacji pożarowej mogą też być stawiane w przypadku zastosowania w obiekcie magazynowym stałych urządzeń gaśniczych, np. gaśniczych wodnych wstępnie sterowanych czy gazowych albo urządzeń inertyzujących.

W przypadku coraz częściej występujących obiektów magazynowania zautomatyzowanego dochodzi konieczność współpracy z układami sterowania automatyki magazynu w celu zatrzymania przemieszczania się urządzeń transportowych. (…)

Alarmowanie

Poza wykryciem pożaru istotnym aspektem jest również alarmowanie personelu przebywającego w obiekcie. Pierwszą istotną kwestią jest dobór odpowiednich środków alarmowania. Najczęściej będą to sygnalizatory akustyczne, ewentualnie uzupełnianie sygnalizatorami optycznymi. Jednak są przypadki, gdzie z uwagi na rozwiązania zamienne, stosowane często przy regałach wielopoziomowych pick tower, konieczne jest stosowanie bardziej zaawansowanego sposobu alarmowania, jakim jest dźwiękowy system ostrzegawczy.

Kolejnym problemem do rozwiązania są warunki składowania wpływające na osiągnięcie właściwych parametrów alarmowania, takich jak natężenie dźwięku w przypadku sygnalizatorów czy zrozumiałość mowy w przypadku dźwiękowego systemu ostrzegawczego. Inne będą warunki akustyczne w pustej hali magazynowej bez regałów czy nawet z regałami, ale bez materiałów składowanych na regałach, a inne w przypadku magazynu w czasie użytkowania, z pełnym lub częściowym zatowarowaniem.

O ile w „standardowej" hali magazynowej poziom szumów tła akustycznego zazwyczaj nie jest wysoki, to już w obiektach, gdzie występują różnego rodzaju układy transportu towarów czy automaty magazynowe, należy brać pod uwagę również możliwość występowania w całości lub części obiektu istotnego poziomu natężenia dźwięków tła akustycznego.

Niezawodność działania

Obiekty magazynowe często są obiektami wielkopowierzchniowymi. W tym kontekście należy zwrócić uwagę na kwestie związane z niezawodnością systemu detekcji pożaru, w tym utrzymanie rygoru maksymalnych dopuszczalnych stref dozorowych, maksymalnej powierzchni dozorowanej jedną linią dozorową czy urządzenia radiowe itp. Warto zaznaczyć, że niektóre standardy precyzują, iż np. →

powierzchnia strefy dozorowej w przypadku regałów wysokiego składowania to nie powierzchnia zajmowana przez regały, ale całkowita powierzchnia składowania w regałach, czyli powierzchnia zajmowana przez regały pomnożona przez liczbę poziomów składowania.

Kolejnym aspektem jest fakt, że są to duże przestrzenie, w których gorące produkty spalania rozprzestrzeniają się i na ich oddziaływanie może być narażonych jednocześnie wiele elementów zlokalizowanych na liniach dozorowych. Jest to istotne w zakresie niedopuszczenia do sytuacji wyłączenia części linii dozorowej wskutek zadziałania izolatorów zwarć, gdyby ktoś chciał na takiej linii montować, np. moduły sterujące i kontrolujące mające funkcjonować z istotnymi opóźnieniami w stosunku do momentu wykrycia pożaru.

Jak zabezpieczać magazyny wysokiego składowania?

Poniżej przedstawiono krótki przegląd wytycznych zawartych w różnych standardach projektowania instalacji sygnalizacji pożarowej, odnoszących się bezpośrednio do zabezpieczenia magazynów wysokiego składowania. (…)

Ważne jest przestrzeganie zasady, iż w przypadku wyboru danego standardu projektowego do zabezpieczenia konkretnego obiektu należy stosować się kompleksowo do postanowień tego właśnie standardu. Nie można wybierać niezależnie różnych części odrębnych standardów na zasadzie, że z każdego wybieramy co nam, z różnych względów, bardziej odpowiada.

Jednak powyższa zasada w opinii autora (…) nie stoi w sprzeczności z możliwością, o ile dany standard nie obejmuje określonego zagadnienia, posiłkowania się innymi dokumentami jako wiedzą techniczną. Należy przy tym oczywiście zachować odpowiednią staranność w zakresie analizy – czy te zasady wiedzy technicznej z jakiegoś powodu nie stoją w sprzeczności z wymaganiami podstawowego, wybranego standardu projektowania.

PKN-CEN/TS 54-14:2020-09

Specyfikacja PKN-CEN/TS 54-14 zaleca stosowanie czujek zasysających dymu do zabezpieczania magazynów wysokiego składowania. Jednocześnie wskazuje, iż dla magazynów wysokiego składowania o szczególnie dużych wysokościach mogą mieć zastosowanie wytyczne dla przestrzeni typu atria, czyli przestrzeni wysokich (…).

Specyfikacja nie zaleca wykorzystywania czujek punktowych dymu w tego rodzaju aplikacjach, jak również wskazuje, iż czujki liniowe dymu zazwyczaj nie są odpowiednie z uwagi na aktywności realizowane w regałach, które mogą powodować zakłócenia i fałszywe alarmy.

Wytyczne SITP WP-02:2021

W wytycznych SITP znajdziemy ograniczone informacje dotyczące zabezpieczenia obiektów wysokiego składowania. Wskazują one, iż w przypadku zabezpieczenia magazynów wysokiego składowania za pomocą czujek zasysających dymu taka czujka powinna w podstawowym zakresie działać w klasie czułości B lub C. (…)

Wytyczne VdS 2095pl: 2022-06 (09)

Wytyczne VdS zalecają stosowanie czujek z detektorami dymu i/lub tlenku węgla. Wskazują jednocześnie, iż rozwiązaniem problemu związanego z dostępnością czujek w celu konserwacji może być zastosowanie np. czujek zasysających.

(…) Z wytycznych VdS wynika konieczność rozmieszczenia czujek punktowych lub otworów zasysających czujek zasysających na kilku poziomach. Najwyższy poziom nie może być oddalony od sufitu o więcej niż 6 m. W przypadku większej odległości odrębnie dozoruje się pomieszczenie i korytarze. Górny poziom regałów musi być dozorowany, np. zawieszonymi czujkami punktowymi lub otworami czujek zasysających, nie dalej niż 6 m od poziomu składowanych materiałów. W przypadku takich elementów należy zapewnić przegrodę pełną o średnicy 0,5 m wokół elementu detekcyjnego. W zakresie elementów detekcyjnych w regałach odległości poziome i pionowe pomiędzy nimi nie mogą przekraczać 6,5 m. Odległość pierwszego i ostatniego elementu od czoła regału nie może być większa niż 3,3 m.

Wytyczne FM Global Data Sheet 5-48

W wytycznych FM Global 5–48 znajdują się wskazania, iż w przypadku zabezpieczania czujkami dymu regałów czujki należy instalować przy suficie powyżej każdego przejścia między regałami i na kilku poziomach pośrednich w regałach na przecięciu każdej poprzecznej i podłużnej przerwy dymowej. Detektory nie muszą być instalowane na każdym skrzyżowaniu przerw na każdym poziomie, ale mogą być rozmieszczone naprzemiennie między poziomami pośrednimi, tak aby dwa poziomy pośrednie obejmowały wszystkie skrzyżowania.

W magazynach z otwartymi regałami należy wziąć pod uwagę drogę, jaką dym może pokonywać przez korytarze i przerwy kominowe. Ze względu na różne ścieżki ruchu powietrza alarm czujki dymu może być mylący przy określaniu lokalizacji pożaru, jeśli konstrukcja systemu wykrywania jest nieodpowiednia. W zamkniętych regałach magazynowych ruch dymu będzie zablokowany, co stwarza potrzebę zainstalowania czujek w wielu miejscach wewnątrz regałów.

Norma brytyjska BS 5839-1:2013

W normie brytyjskiej BS 5839-1 znajduje się wskazanie, że jeśli regały magazynowe zawierają materiały o wysokiej wartości lub stanowiące wysokie ryzyko, lub wysokość regału przekracza 8 m, należy rozważyć detekcję międzyregałową i odsyła w tym zakresie do wytycznych FIA. (…)

Standard NFPA 72

Standard NFPA 72 wskazuje, że podczas zabezpieczania magazynów wysokiego składowania wszystkie tzw. przerwy kominowe tworzone przez składowane materiały i półki regałów powinny być na odpowiednim poziomie dozorowane czujkami. Jednocześnie przy lokalizacji czujek należy zwracać uwagę na możliwość ich uszkodzenia podczas załadunku i rozładunku towaru z regału.

CFPA-E Guideline No 35:2015 F

W wytycznych CFPA-E dotyczących bezpieczeństwa pożarowego obiektów magazynowych zamieszczono zalecenie, iż systemy transportowe, automatycznego pakowania i podobne powinny był połączone z systemem sygnalizacji pożarowego w taki sposób, aby przemieszczanie towarów było zatrzymywane w przypadku wystąpienia alarmu pożarowego.

Jako istotne cele standard wskazuje konieczność zapewniania dostępności elementów detekcji w celu serwisu i konserwacji (…).

Zgodnie z NFPA 72 w celu najefektywniejszej detekcji pożaru w przestrzeniach wysokiego magazynowania czujki powinny być stosowane na suficie ponad każdym korytarzem między regałami oraz na poziomach pośrednich w regałach naprzemiennie w sąsiedztwie poszczególnych sekcji palet. W przypadku, kiedy mamy do czynienia z regałami

bez półek z regularnymi przerwami kominowymi, standard zaleca lokalizację czujek wewnątrz regałów w przerwach kominowych. W przeciwnym przypadku standard wskazuje lokalizację czujek przy brzegu regału od strony korytarzy między regałami.

Pożary testowe

W pewnych sytuacjach może być niezbędne zweryfikowanie doświadczalne efektywności systemu detekcji pożaru, chociażby ze względu na rodzaj zastosowanych czujek i wysokość pomieszczenia. W różnych źródłach literaturowych można spotkać mniej lub bardzie dokładne wytyczne przeprowadzenia takich pożarów testowych.

Pewne informacje w przedmiotowym zakresie mają się również pojawić w kolejnej zaktualizowanej edycji specyfikacji CEN 54-14. Zgodnie z procedowanym obecnie projektem nowelizacji tego dokumentu zaleca się użycie do pożaru testowego materiału palnego, reprezentatywnego dla materiałów palnych występujących w danej przestrzeni. Zalecenie wskazuje na użycie trzech kilogramów takiego materiału. Jednocześnie projekt specyfikacji wskazuje, iż zapalenie materiału powinno następować od małego źródła zapalenia, które samo z siebie nie będzie istotnie wpływać na ilość energii generowanej podczas spalania. Projekt dokumentu wskazuje również możliwość wykorzystania w pewnych sytuacjach sztucznego dymu, jednak zwraca uwagę, iż dodatkowe źródło energii mające na celu spowodowanie unoszenia się sztucznego dymu powinno odpowiadać ilości energii, jaka mogłaby być generowana w przypadku faktycznego pożaru.

Testy powinny wykazać, że np. czas detekcji jest porównywalny z odpowiednim odniesieniem. Przykładowo, jeśli czujka jest instalowana na wysokości wykraczającej poza zakres wskazany w specyfikacji należy wykazać, iż czas reakcji czujki mieści się w granicach czasu zadziałania czujki montowanej na wysokości dopuszczalnej przez specyfikację. Innym wyznacznikiem może być również wykazanie, iż dym dotrze do czujek w odpowiednim czasie, np. w miejscach, gdzie może występować stratyfikacja albo ruchy powietrza powodowane systemami wentylacji i klimatyzacji.

Podsumowanie

Zabezpieczenie magazynu wysokiego składowania jest bardziej złożonym zagadnieniem niż zabezpieczenie standardowej przestrzeni o tak stosunkowo prostej architekturze.

Problemy do rozwiązania wynikają zarówno z wysokości zabezpieczanych pomieszczeń, jak i z wykorzystywanych technologii magazynowych, w tym konstrukcji regałów i urządzeń stosowanych do transportu składowanych towarów.

W celu zapewnienia skutecznej detekcji pożaru, zwłaszcza tam, gdzie nie użyto instalacji tryskaczowej montowanej w regałach, konieczne jest zastosowanie elementów detekcji pożaru w samych regałach. Wykrywanie pożaru wyłącznie w strefie podstropowej pomieszczenia może skutkować znacznym jej opóźnieniem do czasu, kiedy pożar będzie już w rozwiniętej fazie i praktycznie żadne działania, związane z reagowanie na jego wystąpienie, nie będą już mogły być efektywnie przeprowadzone.

Jeśli przyjęte wytyczne projektowania instalacji sygnalizacji pożarowej nie opisują szczególnej sytuacji wysokiego składowania, projektant powinien korzystać z innej wiedzy technicznej, w tym zawartej w innych standardach projektowania czy też opracowaniach technicznych, zwracając przy tym uwagę, aby nie zastosować rozwiązań sprzecznych z przyjętym podstawowym standardem projektowym. ●

Niniejszy artykuł jest skrótem referatu wygłoszonego podczas Ogólnopolskich Warsztatów „Sygnalizacja i Automatyka Pożarowa SAP 2024", zorganizowanych przez POLON-ALFA S.A.
Wszystkie skróty (...) od redakcji.

AI i security

Kiedy ludzkie zmysły to za mało

Coraz bardziej zaciera się granica między fizycznym bezpieczeństwem a cyberbezpieczeństwem. Każda nowa kamera wyposażona w algorytmy sztucznej inteligencji, każdy system dostępu funkcjonujący w chmurze, każda czujka połączona z centralą przez Internet stają się elementami Internetu rzeczy. To oznacza, że firmy, strzegąc swojego fizycznego bezpieczeństwa, muszą mieć baczenie na to, co się dzieje w ich cyfrowym otoczeniu.

Monika Żuber-Mamakis

Możliwości, jakie wiążą się z upowszechnieniem algorytmów sztucznej inteligencji, imponują. Ale nie bez przyczyny piszemy m.in. o zaletach zwykłych fizycznych kluczy (str. 38). Prostych i skutecznych, choć przecież nieidealnych i trochę, powiedzmy szczerze, archaicznych (dlatego w artykule opisujemy ich bardziej zaawansowane opcje). Z tych właśnie powodów są chętnie zastępowane wygodniejszymi rozwiązaniami. Może zachwycać możliwość udzielania zdalnego dostępu do pomieszczeń czy wygoda sterowania wszystkimi kluczami jednocześnie, ale trzeba pamiętać, że nie ma darmowych obiadków. Ta wygoda ma swoją cenę. Jest nią ryzyko ataku hakerskiego. Czasami celowanego w firmę lub grupę jej pracowników, typu *spear phising,* czasami wymierzonego wprost przeciwko konkretnej osobie, takiej, która w danej organizacji ma np. dostęp praktycznie do wszystkiego. To już tak zwany *whaling*, czyli polowanie na grubą rybę. Tylko od czujności i współpracy działów IT i menedżerów security zależy, czy będzie to polowanie udane.

Wyposażanie urządzeń security w algorytmy sztucznej inteligencji to oczywiście punkt dla graczy pozostających po dobrej stronie mocy. Sęk w tym, że moc AI odkryli także ci źli. Eksperci firmy Splunk należącej obecnie do CISCO, przygotowujący raport *State of Security 2024. The Race to Harness AI* zadali ankietowanym pytanie: Czy AI przechyli szalę na korzyść obrońców, czy atakujących? Respondenci byli podzieleni niemal równo: 45% przewiduje, że na AI najbardziej skorzystają napastnicy, a 43% uważa (bądź po prostu ma nadzieję), że AI pomoże atakowanym.

Na początek trochę danych

Rynek cyberbezpieczeństwa związany ze sztuczną inteligencją ma szansę na niemal sześciokrotny wzrost w ciągu najbliższych sześciu lat. Z obecnych 7,1 mld dol. w 2024 r. wartość ta ma wzrosnąć do 40,1 mld dol. w 2030 r. Oznacza to średni roczny wzrost na poziomie 33,4% – prognozuje firma MarketsandMarkets. Są tu uwzględniane zarówno narzędzia natywne generatywnej AI, takie jak wykrywanie zagrożeń i zapobieganie im, jak i rozwiązania cyberbezpieczeństwa przeznaczone do ochrony tejże AI, w tym ochrony wykorzystywanych przez nią danych.

Czym innym jednak jest generatywna AI, a czym innym algorytmy stosowane przez firmy branży security.

AI w security – mniej kreatywna, za to spostrzegawcza

Sztuczna inteligencja *(artificial innteligence, AI)* w obszarze bezpieczeństwa fizycznego obejmuje zastosowanie uczenia maszynowego *(machine learning, ML)* oraz głębokiego uczenia *(deep learning, DL),* które do pracy potrzebują danych pozyskiwanych z urządzeń, takich jak kamery, czujniki czy systemy dostępu. Na ich bazie algorytmy uczenia maszynowego pozwalają prognozować zdarzenia oraz optymalizować wydajność konkretnych zadań. Deep learning służy do wyszukiwania relacji między danymi wejściowymi a wyjściowymi, co pozwala na uzyskanie nowych informacji. Przykłady zastosowań tej technologii w zakresie bezpieczeństwa fizycznego obejmują rozpoznawanie obiektów, pojazdów i ludzi, a także generowanie alertów w przypadku naruszenia

→

strefy zabezpieczonej. Uczenie maszynowe i głębokie uczenie są szczególnie skuteczne w przeszukiwaniu ogromnych ilości danych w celu identyfikacji wzorców i trendów, które mogą być trudne do zauważenia przez ludzi.

Ile w takim razie wart jest rynek algorytmów związanych z branżą security? O zebranie danych pokusiła się organizacja ekspertów Mordor Intelligence, specjalizująca się w mapowaniu złożonych systemów biznesowych. Według nich „wielkość rynku AI w sektorze bezpieczeństwa ma wzrosnąć z 21,19 mld dol. w 2023 r. do 50,61 mld dol. do 2028 r., przy CAGR na poziomie 19,02% w okresie prognozy (2023–2028)". Natomiast zgodnie z raportem firmy analitycznej Fortune Business Insights globalny rozmiar rynku dostępu ma osiągnąć 25,22 mld dol. w 2027 r., przy rocznej stopie wzrostu CAGR wynoszącej 8,7%. W obu przypadkach mowa jest zatem o potężnych kwotach. Jest o co walczyć.

Po co branży security algorytmy AI?

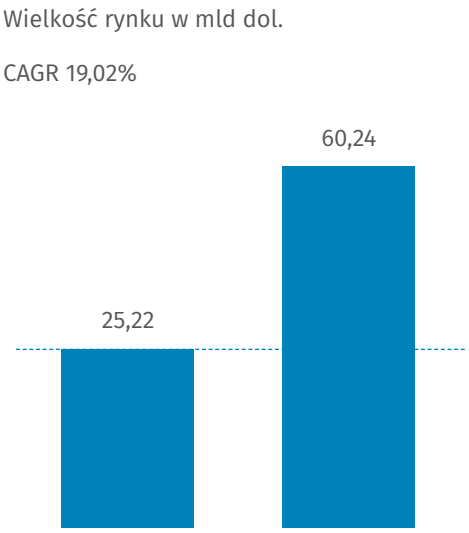
Odpowiedź jest oczywista. W przypadku bezpieczeństwa fizycznego algorytmy AI przyniosły swoisty przełom. Trzeba przyznać, że nawet bardzo wyrafinowane urządzenia security napotykają barierę w postaci ograniczeń ludzkiej percepcji. AI tę barierę stanowczo przesuwa. Nie jesteśmy w stanie widzieć bardziej, słyszeć lepiej, mieć oczu dookoła głowy. A urządzenia security to potrafią, szczególnie jeśli dołoży się im oprogramowanie wykorzystujące uczenie maszynowe i *deep learning*. Dzięki nim ludzkie zmysły zyskują wsparcie, na jakie wcześniej nie mogliśmy liczyć.

AI umożliwia doskonalenie sposobów wykrywania zagrożeń, optymalizację systemów nadzoru i skuteczniejsze ograniczanie ryzyka. Wykorzystując zaawansowane algorytmy i możliwości uczenia maszynowego, AI przekształca sposób, w jaki chronione jest otoczenie fizyczne. To zaś oznacza transformację branży bezpieczeństwa fizycznego oraz tego, co może zaoferować swoim klientom. Wykorzystanie AI w systemach kontroli dostępu znacząco podnosi poziom bezpieczeństwa. Zaawansowane metody uwierzytelniania biometrycznego, takie jak rozpoznawanie twarzy czy skanowanie odcisków palców, znacznie utrudniają nieautoryzowany dostęp do obiektów. Zastosowanie algorytmów uczenia maszynowego powoduje, że wyposażone w nie systemy mogą uruchamiać alarmy lub informować personel ochrony o próbach włamania, co skutecznie zapobiega nieautoryzowanemu dostępowi oraz chroni poufne informacje i cenne zasoby. Inteligentne systemy kontroli dostępu mogą być integrowane z systemami zarządzania budynkami, co zapewnia kompleksowe podejście do bezpieczeństwa. Systemy te ponadto potrafią dostosowywać się do zachowań użytkowników, np. regulując oświetlenie i temperaturę w zależności od pory dnia oraz indywidualnych preferencji. To wszystko prawda. Tyle tylko, że za te możliwości pobierany jest haracz w postaci większego zagrożenia dla cyberbezpieczeństwa. Każde urządzenie podłączone do sieci staje się przecież potencjalnym *back doorem*. Furtką, przez którą może dostać się np. *ransomware*.

Licho nie śpi

Według raportu *Veeam Data Protection Trends Report 2024* cyberataki są główną przyczyną przerw w działalności firm. Inne czynniki to awarie infrastruktury, sieci, pamięci masowej, oprogramowania aplikacji, zasobów chmurowych i serwerów, a także tradycyjne wypadki, katastrofy naturalne itp. W przypadku ataków *ransomware* każda organizacja powinna mieć świadomość, że tylko kwestią czasu jest to, kiedy za pomocą tego rodzaju złośliwego oprogramowania zostanie zaatakowana. Z danych opublikowanych we wspomnianym raporcie wynika, że 76% firm doświadczyło ataku

Sztuczna inteligencja w branży security



Okres objęty badaniem i prognozą	2019–2029
Wielkość rynku (2024)	25,22 mld dol.
Wielkość rynku (2029)	60,24 mld dol.
CAGR (2024–2029)	19,02%
Najszybciej rozwijający się rynek	Azja i Pacyfik
Największy rynek	Ameryka Północna

Źródło: Mordor Intelligence

przynajmniej raz w ciągu ostatnich 12 miesięcy. I choć jest to mniej niż w roku 2023, kiedy ataku doświadczyło 85% firm, to aż 26% z nich zostało zaatakowanych co najmniej cztery razy (!). A jedynie 13% firm stwierdziło, że skutecznie przeprowadza proces odzyskiwania danych w sytuacjach kryzysowych. Tylko 32% organizacji ma nadzieję, że na odzyskanie pełnej sprawności operacyjnej będzie potrzebować mniej więcej tydzień. A na pytanie o czas potrzebny na odzyskanie 50 serwerów 32% odpowiedziało, że zespoły IT mogłyby to zrobić w ciągu pięciu dni roboczych. Statystyki pokazują rosnącą przepaść między oczekiwaniami biznesowymi a możliwościami usług IT w zakresie ochrony danych.

Na granicy światów

Zacieranie się granic między bezpieczeństwem fizycznym a cyberbezpieczeństwem oznacza przenikanie do fizycznego świata zagrożeń płynących ze świata cyfrowego. Tymczasem według respondentów cytowanego już raportu Splunk zachowanie cyfrowego bezpieczeństwa staje się coraz trudniejsze. Aż 38% z nich wskazuje, że powodem tej trudności jest złożoność krajobrazu zagrożeń wynikająca m.in. z sytuacji geopolitycznej i związanej z nią wojny hybrydowej. Tymczasem w zastraszającym tempie rośnie ilość danych, w tym danych wrażliwych, które muszą być chronione. Nic więc dziwnego, że organizacje wkładają dużo wysiłku i pieniędzy w to, by dbając o bezpieczeństwo fizyczne, chronić dane, które generowane są przez urządzenia security. Algorytmy AI zdecydowanie poprawiają funkcjonowanie systemów security, ale same nie są odporne na zagrożenie. Są podatne na ataki, takie jak zanieczyszczenie danych czy nieautoryzowany dostęp do informacji wrażliwych.

Weźmy np. inteligentne kamery monitoringu wizyjnego wyposażone w algorytmy AI. Mogą one analizować ogromną ilość danych w czasie rzeczywistym. Potrafią także je interpretować, a co za tym idzie automatycznie identyfikować pracowników i gości, co zwiększa kontrolę dostępu do różnych stref budynku. Co jednak się stanie, gdy po ataku kamery przestaną rozpoznawać gości albo zmanipulowane wpuszczą osoby niepożądane? Realne jest też ryzyko naruszenia prywatności pracowników i klientów, gdyż technologie takie jak rozpoznawanie twarzy mogą być używane do monitorowania ludzi bez ich zgody. Podobnie biometria, mimo że oferuje wysoki poziom zabezpieczeń, nie jest wolna od ryzyka. Istnieją obawy dotyczące możliwości oszustwa (np. wykorzystanie fałszywych odcisków palców) oraz kradzieży danych.

Wykorzystanie sztucznej inteligencji w systemach zabezpieczeń fizycznych oznacza więc zarówno korzyści, jak i wyzwania. Z jednej strony poprawia efektywność monitorowania i kontroli dostępu, z drugiej – powoduje nowe zagrożenia związane z prywatnością i bezpieczeństwem danych. Bezpieczeństwo fizyczne i AI jak najbardziej mogą iść w parze, jeśli zostaną odpowiednio wdrożone. Jeśli jednak AI ma przynieść branży security wymierny zysk, to lepiej sięgać po ten miód małą łyżeczką, chochla się tu nie sprawdzi. •

Nieznajomość prawa szkodzi

Czekając na ustawę dotyczącą przeniesienia dyrektywy NIS2 na grunt prawa polskiego, postanowiliśmy porozmawiać z kimś, kto na wylot zna unijne przepisy dotyczące bezpieczeństwa i potrafi się w nich poruszać. Ekspertką w tej kwestii jest **radczyni prawna Agnieszka Wachowska,** specjalizująca się w problematyce prawnej nowych technologii, prawa autorskiego i cyberbezpieczeństwa. Rozmawiają Jan Grusznic i Monika Żuber-Mamakis.

Rozmawiamy na kilka dni przed wejściem w życie unijnej dyrektyw NIS2. To właśnie ona spowodowała, że wiele firm zainteresowało się cyberbezpieczeństwem. Mamy już jednak ustawę o krajowym systemie cyberbezpieczeństwa, będącą implementacją dyrektywy NIS1. I już teraz widać, że są pewne rozbieżności między nowelizacją ustawy o krajowym systemie cyberbezpieczeństwa a NIS2. Zacznijmy zatem od wyjaśnienia tej kwestii.

Faktycznie, mamy projekt nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa datowany na 23 kwietnia 2024 r. Warto zaznaczyć, że to dopiero pierwsza wersja projektu, co podkreśla Ministerstwo Cyfryzacji. W ramach przeprowadzonych konsultacji społecznych zgłoszonych zostało dużo poprawek. Ministerstwo Cyfryzacji zadeklarowało, że z początkiem czwartego kwartału tego roku opublikuje materiał odnoszący się do tych uwag (podobno jest to prawie tysiącstronicowy dokument). W IV kwartale ma również ukazać się druga wersja projektu, choć wydaje się, że nie należy się raczej spodziewać rewolucji. W pierwszej wersji projektu ustawy, w toku konsultacji publicznych zidentyfikowano trochę drobnych nieścisłości, które mają zostać zmienione w drugiej wersji projektu.

Niezależnie od tego warto podkreślić, że dyrektywa NIS2 stanowi harmonizację minimalną. To znaczy, że państwa członkowskie, w tym Polska, muszą wdrożyć obowiązki wynikające z dyrektywy w podstawowym zakresie opisanym w dyrektywie. Natomiast w przepisach krajowych mogą rozszerzyć katalog tych obowiązków albo rozszerzyć zakres regulacji. I teraz odpowiadając na pytanie: rozbieżności, które pojawiają się w projekcie ustawy albo w projektach innych państw członkowskich, mogą wynikać właśnie z różnego sposobu implementacji.

Czy w takim razie pojawiły się w polskim projekcie przepisy, które są wyraźnie sprzeczne z dyrektywą NIS2?

Takich, które faktycznie byłyby sprzeczne z dyrektywą, czyli ogólnie mówiąc, zawężające przepisy dyrektywy, ja nie dostrzegam, przy czym jest przepis, który według mnie można różnie interpretować. Dotyczy on jednego z obowiązków, który jest nałożony na podmioty ważne i kluczowe, a dokładnie zapewnienia bezpieczeństwa łańcucha dostaw. W dyrektywie NIS2 jest dosyć ogólnie napisane, że podmioty ważne i kluczowe powinny oceniać i uwzględniać ogólną jakość i odporność produktów i usług oraz środków zarządzania ryzykiem w cyberbezpieczeństwie stanowiący ich część, a także praktyki dotyczące cyberbezpieczeństwa stosowane przez dostawców produktów i usług, w tym ich procedury bezpiecznego opracowywania

W NIS2 te wymagania dla łańcucha dostaw są wprost ograniczone do rynku ICT, tak jak to zrobił polski ustawodawca. Polski ustawodawca, wprowadzając regulację, ograniczył się do bezpieczeństwa łańcucha dostaw produktów, usług i procesów w branży ICT. To zawężenie nie wynika wprost z NIS2. Spotkałam się jednak z takim twierdzeniem, że jeśli chodzi o nabywanie produktów i usług, to w rozumieniu dyrektywy NIS2 – jako że dotyczy ona cyberbezpieczeństwa, termin łańcucha dostaw należy wykładać jako dotyczący wyłącznie usług ICT. Niektórzy jednak mają odmienne zdanie i uważają, że nie należy tego terminu traktować w sposób zawężający, bo w zasadzie każdy dostawca we współczesnym świecie korzysta z usług cyfrowych, choćby wysyłając e-maile. Jeśli infrastruktura IT jakiegoś dostawcy zostanie zhakowana, to może być przecież źródłem zagrożenia dla swojego klienta. Tym samym pomioty ważne i kluczowe w ramach dobrych praktyk powinny weryfikować troskę o cyberbezpieczeństwo wszystkich swoich dostawców, nie tylko dostawców ICT.

Skoro mówimy o bezpieczeństwie ICT i łańcucha dostaw, to pojawia się nam od razu kwestia *high risk vendor,* czyli dostawców wysokiego ryzyka. Pytamy o to, bo dla naszych czytelników to ważny temat.

Dostawca wysokiego ryzyka to z kolei instytucja wprowadzona do projektu nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa, która nie wynika wprost z NIS2. Należy pamiętać, że projekt nowelizacji

ustawy o krajowym cyberbezpieczeństwie nie tylko implementuje dyrektywę NIS2, ale także wprowadza inne, dodatkowe regulacje. Można więc rzec, że *high risk vendor* to inicjatywa własna polskich projektodawców. I ona nie wynika wprost z NIS2. Prawodawstwo unijne nie narzuca powołania takiej instytucji do życia.

W tym momencie warto wyjaśnić, na czym w ogóle polega instytucja dostawcy wysokiego ryzyka. Na podstawie decyzji administracyjnej, w tym przypadku Ministra Cyfryzacji, poprzedzonej specjalną procedurą opisaną w ustawie, będzie można uznać dany produkt, usługę lub proces za pochodzący od dostawcy wysokiego ryzyka. Ta decyzja wg projektu nowelizacji ustawy ma mieć wpływ na wszelkie podmioty ważne i kluczowe, z uwzględnieniem pewnych wyłączeń dla rynku telekomunikacyjnego. W konsekwencji decyzja ta oznacza konieczność wycofania produktu takiego dostawcy lub rezygnacji z jego usług w określonym czasie. Decyzja ta będzie też mieć wpływ na procesy zakupowe, bo produkty w niej wskazane nie będą mogły być nabywane, a w przypadku zamówień publicznych, jeśli w ramach złożonej oferty znalazłyby się produkty, usługi lub procesy pochodzące od dostawcy wysokiego ryzyka, to oferta taka ulega odrzuceniu.

Czy rzeczywiście NIS2 będzie ostatecznie dotyczyć każdego podmiotu? A druga rzecz, CER, czyli dyrektywa służąca zwiększeniu odporności podmiotów krytycznych państw członkowskich UE, o której myśli się trochę jako o zawężeniu NIS2. Czy w tym przypadku uważa pani, że finalnie będzie ona dotyczyć każdego podmiotu w łańcuchu dostaw?

Różnice są na poziomie kategorii podmiotów, których dotyczy NIS2 i CER, ale też zakresu tego, czego każda z tych regulacji dotyczy. NIS2 dotyczy cyberbezpieczeństwa, czyli bezpieczeństwa informatycznego i obejmuje szereg podmiotów, rozszerzając znacząco obowiązującą jeszcze NIS1. Zakres podmiotowy jest bardzo szeroki, przy czym dyrektywa NIS2 wyłącza spod swojego zakresu mikro- i małe przedsiębiorstwa. Jednym z elementów jest bezpieczeństwo łańcucha dostaw. Te podmioty powinny sprawdzić bezpieczeństwo swojego dostawcy. Każda firma, która obsługuje podmioty będące podmiotami kluczowymi lub ważnymi, może być odpytana o to, jak dba o bezpieczeństwo, nawet jeśli sama nie podlega regulacjom, bo np. jest mikro- lub małym przedsiębiorcą. Natomiast CER jest regulacją, która obejmuje węższą grupy w tym sensie, że dotyka podmiotów krytycznych mogących działać w tych samych obszarach, co podmioty objęte dyrektywą NIS2, ale to państwo polskie decyduje o tym, jakie podmioty zostaną za takie uznane.

Czy można uznać, że CER jest niczym innym tylko rozszerzeniem w zasadzie tego, co już obecnie funkcjonuje w kraju?

Tak, bo mamy projekt ustawy, która dotyczy implementacji CER, i jest to projekt nowelizacji ustawy o zarządzaniu kryzysowym, więc mamy procedurę dotyczącą wydawania decyzji o uznaniu danego podmiotu za krytyczny, a teraz te przepisy zyskają rangę przepisów unijnych. Rozszerzają jednocześnie zakres podmiotów, w stosunku do których te decyzje mogą być wydane. Obie regulacje się przenikają. NIS2 nie dotyczy małych i mikroprzedsiębiorców, ale jeżeli firma zostanie uznana za podmiot krytyczny na gruncie ustawy o zarządzaniu kryzysowym, to automatycznie będzie zmuszona do stosowania regulacji dyrektywy NIS2, czyli w tym przypadku ustawy o krajowym systemie cyberbezpieczeństwa. Państwo polskie ma możliwość wskazania konkretnego podmiotu, nawet małego, gdy uznaje w jakiś sposób jego działalność za strategiczną.

Czy powstanie jakiś katalog podmiotów zobowiązanych do przestrzegania NIS2?

W przypadku NIS1 i implementującej tę dyrektywę ustawy o krajowym systemie cyberbezpieczeństwa wyglądało to tak, że aby podmiot został uznany za operatora usług kluczowych, to musiała zostać wydana decyzja administracyjna. Dyrektywa NIS2 zmienia tę filozofię, wprowadzając system samooceny. Każdy podmiot musi sam ocenić, czy podlega regulacji. Ustawa o krajowym systemie cyberbezpieczeństwa może trochę ten katalog rozszerzać. Każda organizacja musi zatem dokonać samooceny, czy spełnia wszystkie warunki, które czynią z niej podmiot ważny lub kluczowy. Zgodnie z projektem nowelizacji na taką deklarację będzie miała dwa miesiące od momentu wejścia w życie ustawy. Wniosek o uznanie za taki podmiot będzie zgłaszany przez specjalny system informatyczny. Złożenie oświadczenia będzie obłożone rygorem odpowiedzialności karnej za składanie nieprawdziwych informacji, a wpis ma mieć charakter deklaratywny. Nie kreuje on zatem rzeczywistości. Jest potrzebny tylko do stworzenia ewidencji takich podmiotów, by państwo mogło zidentyfikować podmioty kluczowe i ważne. Rejestr będzie niejawny z oczywistych względów i będzie mógł być udostępniony odpowiednim służbom wymienionym w ustawie, m.in. innymi organom ścigania czy wymiaru sprawiedliwości.

Czy te oświadczenia będą w jakikolwiek sposób weryfikowane? Możemy przecież spotkać się z sytuacją, gdy firma nie złoży takiego oświadczenia, choć powinna, przewidując, że znalezienie się na liście podmiotów kluczowych i ważnych wywoła konkretne obowiązki.

Przepisy są skonstruowane w taki sposób, że każdy podmiot, który spełni ustawowe kryteria, ma obowiązek wdrożenia odpowiednich środków cyberbezpieczeństwa. I jednocześnie każdy może być skontrolowany przez organ nadzorczy. Takich instytucji nadzorczych może być kilkanaście, bo są one powiązane z sektorami.

Jeżeli się okaże, że firma nie jest odpowiednio chroniona, może stanowić wrażliwy element łańcucha dostaw i musi się wyposażyć w odpowiednie środki ochrony, to kto za nie zapłaci?

No cóż, odpowiednie środki cyberbezpieczeństwa będą musiały być wdrożone przez podmioty zobowiązane do stosowania tej ustawy na koszt własny. Na pocieszenie mogę dodać, że są specjalne fundusze unijne, z których może być finansowane wdrożenie odpowiednich środków bezpieczeństwa.

Czy mogłaby pani powiedzieć, ilu w sumie różnego rodzaju regulacjom z zakresu bezpieczeństwa informacji obecnie podlega polskie przedsiębiorstwo średniej wielkości?

Jest ich kilka, to prawda. Dla przedsiębiorców ważna jest ustawa o krajowym systemie cyberbezpieczeństwa. To ona nakłada na nich obowiązki, podobnie jak ustawa o zarządzaniu kryzysowym czy ustawa o informatyzacji podmiotów publicznych dotycząca sektora publicznego. Kwestie bezpieczeństwa reguluje również RODO, ale w zakresie przetwarzania danych osobowych. Jeżeli więc mówimy o przetwarzaniu danych osobowych, to widać, że ustawa o krajowym systemie cyberbezpieczeństwa i RODO mogą się zazębiać. To oczywiste, →

że może istnieć podmiot, który jest podmiotem ważnym lub kluczowym na gruncie ustawy o krajowym systemie cyberbezpieczeństwa, a jednocześnie przetwarza dane osobowe. Taki podmiot musi zwracać uwagę i na regulacje rodowskie, i na regulacje ustawy o krajowym systemie cyberbezpieczeństwa. Gdy zatem dojdzie do incydentu, który będzie incydentem w systemie informatycznym podmiotu kluczowego bądź ważnego i który w jakiś sposób wpłynie na integralność oraz poufność danych osobowych, to wówczas będzie on zobowiązany do zaraportowania takiego incydentu podwójnie, tj. do Prezesa Urzędu Ochrony Danych Osobowych i niezależnie od tego do właściwego podmiotu wyznaczonego przepisami ustawy o krajowym systemie cyberbezpieczeństwa. Przy okazji, to bardzo ciekawe zagadnienie, bo tak naprawdę procedury w tych instytucjach powinny być w miarę możliwości ujednolicone, inaczej może to powodować pewien chaos. Na pocieszenie mogę powiedzieć, że europejski ustawodawca przewidział, że może dojść do takiego zbiegu, i wprost uregulował tę kwestię w NIS2. Jeżeli zatem organizacja winna naruszenia w rozumieniu RODO zostanie ukarana przez prezesa UODO, to zgodnie z NIS2 nie można nałożyć na nią drugiej kary na podstawie implementacji NIS2 – jeśli naruszenie obu regulacji było spowodowane tym samym działaniem.

Chcielibyśmy na chwilę wrócić do dostawców wysokiego ryzyka. Nie znaleźliśmy procesu odwołania od decyzji ministra o uznaniu firmy za takiego dostawcę.
To prawda. Ta decyzja będzie wydawana z rygorem natychmiastowej wykonalności i nie będzie od niej przysługiwało odwołanie ani wniosek o ponowne rozpatrzenie sprawy. Podmioty, w stosunku do których taka decyzja zostanie wydane, będą jednak mogły wnieść skargę do sądu administracyjnego.

Poza wymienionymi już regulacjami mamy jeszcze CRA, o którym niektórzy mówią, że jest aktualizacją CE. Czym jest dokładnie CRA i jak łączy się z NIS2 i CER?
Zanim przejdę do CRA, to przypomnę, że mamy jeszcze jedną regulację unijną w zakresie cyberbezpieczeństwa, a mianowicie DORA. Jeżeli chodzi o zakres przedmiotowy DORA, jest on bardzo podobny do NIS2, natomiast dotyczy tylko i wyłącznie szeroko pojętego sektora finansowego: banków, firm ubezpieczeniowych, biur maklerskich itp. DORA jest, powiedziałabym, taką bardziej specjalistyczną wersją NIS2. NIS2 jest regulacją bardzo ogólną przez to, że obejmuje bardzo różne podmioty. Natomiast DORA precyzuje, co podmioty sektora finansowego powinny wdrożyć. Co do rozporządzenia CRA, to nie zostało ono jeszcze zatwierdzone przez Radę UE. Tekst został już przyjęty, ale cały proces akceptacji CRA przeciągnął się ze względu na wybory europejskie. Natomiast nie wydaje się, by był z tym jakiś problem, choć oczywiście wszystko może się wydarzyć. Regulacja CRA jest ważna. Niektórzy eksperci twierdzą, że to jest regulacja w zakresie cyberbezpieczeństwa, której Europa potrzebuje najbardziej. Spotkałam się z opinią, że jest spóźniona przynajmniej o 10 lat.

Dlaczego?
Przede wszystkim dlatego, że dotyczy podstawowych kwestii, a mianowicie norm bezpieczeństwa produktów z elementami cyfrowymi: laptopów, smarftonów, inteligentnych smartfonów, a nawet samobieżnych odkurzaczy, czyli tych wszystkich przedmiotów, które zawierają komponent umożliwiający im komunikowanie się. CRA jest zatem nieco spóźniona, bo Internet rzeczy (IoT) jest już naszą codziennością, a w UE ciągle nie ma żadnych norm, które regulowałaby kwestie cyberbezpieczeństwa takich urządzeń.

Wygląda zatem na to, że faktycznie jest trochę spóźniona. Jak na razie nie mamy żadnych wytycznych dotyczących bezpieczeństwa takich urządzeń, żadnej certyfikacji. Co jednak oznacza wprowadzenie CRA dla konkretnych dostawców?
Po pierwsze, wszyscy mają świadomość tego, że wejście w życie tych przepisów wymagać będzie czasu, by dostawcy mogli się do nich dostosować. Po drugie, CRA przewiduje w sumie trzy kategorie produktów: krytyczne, ważne i „zwykłe". Wiele więc zależy, do jakiej kategorii dany sprzęt zostanie przypisany. Nie każdy będzie potrzebować certyfikatu. Urządzenia krytyczne są wymienione wprost w CRA. Są to np. rutery, urządzenia sterujące, urządzenia kontrolujące pracę innych urządzeń itp. Pozyskanie certyfikatu przed wejściem takiego urządzenia na rynek będzie po prostu niezbędne. Dlatego mówi się o tym, że CRA to nowe CE. Elementem certyfikacji będzie konieczność spełniania określonych norm, dostarczenia odpowiedniej dokumentacji dotyczącej cyberbezpieczeństwa i zapewnienia użytkownikom tzw. łat do oprogramowania. Poza tym producenci będą musieli zgłaszać poważne incydenty, jeśli zidentyfikują je w swoich urządzeniach, i będą mieli obowiązek informowania o tym użytkownika. Karą za niedotrzymanie tych warunków może być m.in. konieczność wycofania produktu z rynku.

CRA jest rozporządzeniem, a to znaczy, że będzie obowiązywać bezpośrednio w sposób jednolity w całej Unii Europejskiej i nie trzeba będzie go przenosić ustawą na grunt prawa lokalnego. Tak samo było w przypadku RODO. To jest o tyle sensowne, że ramy certyfikacyjne dotyczące bezpieczeństwa produktu w założeniu mają być identyczne dla całej Unii. Jeśli chodzi o wejście w życie przepisów CRA, to jest ono rozłożone na etapy. Najpierw zaczną obowiązywać przepisy dotyczące powołania organów uprawnionych do certyfikacji, potem te odnoszące się do procedur i obowiązków producentów. Samo rozporządzenie będzie w pełni stosowane dopiero po trzech latach od jego ogłoszenia. Jak widać, horyzont czasowy wprowadzenia tej regulacji jest dłuższy.

Czy nie ma pani jednak wrażenia takiego trochę chaosu wynikającego z tego, że nie mamy jednego spójnego aktu odnoszącego się do wszystkich problemów związanych z cyberbezpieczeństwem. Można odnieść wrażenie, że unijne działania w tej kwestii są raczej gaszeniem pożaru niż zapobieganiem mu?
Oczywiście, można sobie zadać pytanie, czy podejście Unii nie powinno być bardziej wizjonerskie, a mniej reaktywne. Ono faktycznie może się takie wydawać, ale wbrew pozorom regulacje unijne i tak są bardziej wizjonerskie niż te krajowe. Teraz np. Unia już przygotowała się na wszechobecność sztucznej inteligencji, wdrażając AI Act. Przy czym spotkałam się zarzutem, że regulacje te były tworzone za wcześnie. Są też tacy, którzy mówią – za późno. AI już jest, a my nie mamy prawa, które chroniłoby nas przed niepożądanymi jej zrachowaniami. Trudno jednak regulować coś, czego jeszcze tak do końca nie ma. Generatywna sztuczna inteligencja pojawiła się przecież już w trakcie zaawansowanych prac nad AI Act i okazało się, że pewne problemy, jakie wraz z nią się wiążą, w ogóle nie zostały przewidziane przez twórców AI Act. To pokazuje, że takie wizjonerskie podejście do regulacji też nie jest dobrym pomysłem.

Wyjaśnię przy okazji, że CRA też traktuje produkty z elementami cyfrowymi wyposażone w algorytmy AI jako produkty wysokiego ryzyka. Będą więc musiały spełniać wymagania zarówno CER, jak i AI Act. AI Act skupia się jednak na tych podmiotach, które będą korzystać i tworzyć takie systemy sztucznej inteligencji. Jej twórcy będą zobowiązani nie tylko do prowadzenia odpowiedniej dokumentacji, ale też do nadzoru nad nią i zadbanie o cyberbezpieczeństwo AI oraz skrupulatną kontrolę danych, na której algorytmy AI są trenowane. Przewidywane są także systemy AI wprost zakazane. Wracając do pytania. W przypadku NIS2 to wprost w preambule wskazano, że to pandemia spowodowała pilną potrzebę regulacji. Tutaj trzeba było działać ad hoc. Nagła digitalizacja, wzrost pracy zdalnej spowodowały wzrost potencjalnych ryzyk i cyberataków. Im więcej osób korzysta, tym większe ryzyko. Udało się nam, ludziom, błyskawicznie przejść do świata online, ale nie było już czasu, by zadbać o bezpieczeństwo. NIS2 próbuje naprawić to niedopatrzenie.

Nasze ostatnie pytanie. Ministerstwo Cyfryzacji zrezygnowało ze wskazania ISO 27001 jako wyznacznika spełnienia warunków NIS 2. To dobrze czy źle?
Taka informacja ze strony Ministerstwa Cyfryzacji pojawiła się w sierpniu tego roku. Jednocześnie, dopóki nie dojdzie do publikacji drugiej wersji projektu nowelizacji ustawy o krajowym systemie bezpieczeństwa, nie będziemy mieć pewności, czy tak faktycznie jest. Na pewno odwołanie do norm ISO bardzo ułatwiłoby życie przedsiębiorcom. Ale pojawiły się głosy krytykujące wybór ISO. Wiele firm już wdrożyło własne normy, korzystając z amerykańskiego NIST-u. Krytycy tego zapisu podnosili argument, że rolę kontrolera oddaje się w ten sposób podmiotom prywatnym, a te z kolei trudno nadzorować i nie ponoszą one takiej odpowiedzialności jak ewentualny organ nadzorczy czy kontrolujący. A to może być pole do nadużyć. Poczekajmy jednak na drugą wersję projektu.

Pożyjemy, zobaczymy?
Zdecydowanie.

Agnieszka Wachowska, radczyni prawna z kilkunastoletnim doświadczeniem w obsłudze projektów IT. W kancelarii Traple Konarski Podrecki i Wspólnicy uczestniczy w pracach praktyki TMT, kierując zespołem prawa IT, Nowych Technologii i Zamówień Publicznych. Specjalizuje się w problematyce prawnej branży IT i nowych technologii. Od początku kariery prawniczej doradza podmiotom z sektora IT, w tym również podmiotom publicznym, w zakresie zagadnień związanych z prawem IT.

Przyszłość bezpieczeństwa i kontroli dostępu w dobie sztucznej inteligencji

Prestiżowe wydarzenie Nedap Security Day, zorganizowane przez firmę Nedap Security Management, odbyło się 11 września 2024 r. w wyjątkowej scenerii Fabryki Wełny w Pabianicach. Zaprezentowano tam najnowsze technologie związane z kontrolą dostępu oraz cyberbezpieczeństwem. Uczestnicy mieli też okazję poznać innowacyjne rozwiązania przedstawione przez partnerów technologicznych: CBC Poland, BT Electronics, Innovatrics oraz HID.

Spotkanie NSD to wyznacznik trendów w branży systemów kontroli dostępu i nie inaczej było tym razem. Gospodarze, Anna Twardowska i Grzegorz Kosik, zademonstrowali nowe rozwiązanie Nedap Mobile Access, używając kart wirtualnych przechowywanych w Apple Wallet, by rozpocząć konferencję. Podczas wydarzenia cały czas widoczny był silny nacisk na rozwój technologii, o czym świadczył dobór prelegentów.

Jednym z najważniejszych punktów agendy była prezentacja prof. Aleksandry Przegalińskiej z Akademii Leona Koźmińskiego, która omówiła, jak AI przeobraziła się z rewolucji w ewolucję. Zwróciła uwagę na „wielkie trio", czyli moc obliczeniową, big data i algorytmy, które są kluczowe dla przyszłości AI. Omówiła także wyzwania związane z ograniczeniami, jakimi cechują się zbiory danych i infrastruktura IT. Porównała również obecne zmiany do bańki spekulacyjnej i prognozowała bardziej zrównoważony rozwój tej technologii.

Podczas prezentacji Nedap Access Anna Twardowska i Grzegorz Kosik podkreślili 95-letnią historię firmy, która nieustannie się rozwija i adaptuje do zmieniających się warunków rynkowych. Badania przeprowadzone przez Nedap wśród menedżerów ds. bezpieczeństwa wykazały, że największe wyzwania to niestabilność świata, rosnąca liczba regulacji, nowe pokolenie z innymi oczekiwaniami, zwiększająca się rola działów IT oraz potrzeba optymalizacji kosztów.

Podczas debaty eksperckiej uczestnicy dyskutowali o roli kontroli dostępu w bezpieczeństwie obiektów. Głos zabrali Łukasz Stępień z Ghelamco, Tomasz Gawin z mBanku, Renata Hartle z Colliers i Dariusz Kluska z Reckitt, którzy poruszyli kwestie standardów, integracji systemów i bezpieczeństwa. Szczególnie interesujący był wątek dotyczący wirtualnych kart dostępu oraz możliwości wpływu systemów na oszczędności operacyjne.

Błażej Ożga z Nedap Security Management przedstawił najnowsze technologie firmy. Swój wstęp poświęcił polityce zarządzania certyfikatami bezpieczeństwa, wskazał na najwyższy poziom cybersecurity w AEOS, wprowadzenie *multifirmware loading* umożliwiającego zaplanowanie ładowania oprogramowania układowego do poszczególnych elementów systemu, oraz innowacje związane z Nedap Mobile Access. Ciekawym wątkiem było PACE, bazujące na koncepcji cyfrowych bliźniaków, które zapewnia zarówno graficzną prezentację przydzielonych dostępów, jak i zgłaszanie w ten sposób próśb o ich nadanie. PACE jest systemem klasy *Physical Identity and Access Management* (PIAM), który pomaga organizacjom o wysokiej dynamice autoryzacji w płynnym zarządzaniu tożsamościami i dostępem. Jego unikalny model autoryzacji i intuicyjne narzędzia wizualizacji sprawiają, że zadanie zarządzania autoryzacjami bardzo dużej liczby posiadaczy kart jest szybsze i łatwiejsze. Pace działa jako nadrzędny system dla wszystkich systemów kontroli dostępu w wielu lokalizacjach.

W trakcie wydarzenia partnerzy technologiczni przedstawili swoje rozwiązania. Michal Vilagi z Innovatrics zaprezentował smartFace – system biometrycznego rozpoznawania twarzy, który zintegrowany z kontrolą dostępu umożliwia szybką i skuteczną identyfikację. Przemysław Szamocki z CBC Poland omówił platformę GANZ CORTROL VMS, która dostosowuje się do wymogów dyrektywy NIS2 i pozwala na integrację z innymi systemami, w tym z systemem AEOS. Z kolei przedstawiciele HID, Katarzyna Hoffmann-Sielicka i Kamil Targalski, zaprezentowali najnowsze rozwiązania w zakresie mobilnych rozwiązań oraz nowe czytniki SIGNO.

Na zakończenie Rafał Kondak z BT Electronics przedstawił system depozytorów SAIK, które umożliwiają przechowywanie nie tylko kluczy, ale także broni i innych cennych przedmiotów, zapewniając ich pełne bezpieczeństwo w różnych obiektach. W ciekawy sposób zademonstrował też poziomy integracji SAIK z systemem kontroli dostępu.

Nedap Security Day 2024 dostarczył uczestnikom wiedzy o nowoczesnych rozwiązań technologicznych, a także zapewnił możliwość uczestnictwa w inspirujących dyskusjach o przyszłości bezpieczeństwa w erze sztucznej inteligencji. ●

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

AXIS COMMUNICATIONS

Konsola do systemów komunikacji publicznej

Axis Communications wprowadza na rynek sieciową konsolę powiadamiającą do emisji komunikatów na żywo oraz nagranych, z dwukierunkową obsługą dźwięku i wieloma innymi funkcjami. Ta elegancka konsola zdobyła nagrodę Red Dot Design Award. Idealnie nadaje się do sklepów, placówek edukacyjnychi komercyjnych, a także innych obiektów.

Konsola AXIS C6110 Network Paging Console stanowi uzupełnienie głośników sieciowych, tworząc kompletny system komunikacji publicznej. Duży kolorowy wyświetlacz ciekłokrystaliczny (LCD) jest otoczony 12 przyciskami konfigurowanymi online, które umożliwiają emisję komunikatów w dowolnej liczbie stref audio i na szeregu urządzeń końcowych – od głośników sieciowych i interkomów po urządzenia protokołu SIP. Przyciski można również skonfigurować do wyzwalania akcji na innych urządzeniach IoT, takich jak systemy kontroli dostępu lub oświetlenia, aby zapewnić płynność codziennych operacji.

Instalacja jest prosta i elastyczna. Jeden kabel zapewnia zasilanie i łączność (PoE), a wbudowany mikrofon z technologią beamformingu zapewnia dobry dźwięk niezależnie od tego, czy konsola jest umieszczona na biurku, czy na ścianie. Konsoli można używać w konfiguracji fabrycznej, z zestawem

słuchawkowym lub z mikrofonem AXIS TC6901 Gooseneck Microphone.

Najważniejsze cechy:

- możliwość emisji komunikatów na żywo i nagranych;
- dostęp do wszystkich potrzebnych stref audio;
- wyświetlacz konfigurowany online;
- dwukierunkowy dźwięk;
- prosta instalacja dzięki PoE. ●

LINC POLSKA

Camect 96 – nowość w rodzinie hubów ze skuteczną analityką

Do rodziny inteligentnych hubów Camect, składającej się z modeli Camect 24 i Camect 60, dołączył nowy przedstawiciel serii – Camect 96.

Za pomocą analizy AI Camect umożliwia wykrycie intruzów ze skutecznością detekcji na poziomie bliskim 100%. Hub rozróżnia kilkadziesiąt typów obiektów, co sprawia, że jego skuteczność jest tak wysoka. Każdy rozpoznany rodzaj obiektu może mieć przypisaną inną akcję alarmową, więc to, co jest faktycznie alarmem, zależy od konfiguracji urządzenia.
W inteligentny sposób filtruje zdarzenia, które są kluczowe, i informuje o nich, pomijając wszystko to, co nie jest istotne. Zdarzenia mogą być dostarczone jako e-mail, powiadomienie push czy komunikat. To samo zdarzenie może być również równolegle zapisywane na dysku sieciowym czy GoogleDrive.
Nowy model – Camect 96 – umożliwia obsługę nawet 96 megapikseli analityki w jednym urządzeniu. W standardzie jest wyposażony w dwa gigabitowe interfejsy sieciowe i dysk SSD o pojemności 4 TB.
Camect oferuje nie tylko wysoką skuteczność, ale też bardzo intuicyjny interfejs użytkownika. Do tego szybką instalację – na uruchomienie systemu wystarczy tylko 5 min.●

ZKTECO

Skanery RTG bagaży ZKTeco

Firma ZKTeco, znana głównie z produkcji wysokiej klasy biometrycznych systemów kontroli dostępu, stale poszerza swoją ofertę o produkty związane z szeroko pojętym bezpieczeństwem.

Jedną z grup produktowych firmy, które cieszę się uznaniem klientów, są rentgenowskie skanery do prześwietlania bagaży. Produkty te (10 modeli) charakteryzują się wysoką jakością obrazu, co w połączeniu z inteligentną analizą komputerową umożliwia automatyczną identyfikację podejrzanych przedmiotów. Pozwala to operatorowi szybko i skutecznie ocenić zawartość bagażu bez konieczności zatrzymywania przenośnika.
W skanerach zastosowano kilka nowoczesnych rozwiązań, takich jak:
- logowanie za pomocą linii papilarnych;
- funkcja Eyes-on pilnująca, by operator nie spuszczał wzroku z ekranu urządzenia;
- integracja oprogramowania skanera z wykrywaczem metali;
- stały monitoring wizyjny skanowanych bagaży;
- technika Dual View umożliwiająca jednoczesne skanowanie bagażu z dwóch stron;
- regulowane napięcie lampy RTG i prędkość przenośnika;
- wyposażenie skanera w 4-warstwową ołowianą kurtynę i dwa stoliki rolkowe;
- komunikacja za pomocą interfejsu TCP/IP;
- funkcja umożliwiająca szkolenie operatorów w zakresie rozpoznawania podejrzanych przedmiotów;
- możliwość zarządzanie logami umożliwiająca administratorowi przeglądanie statusów pracy operatorów;
- alarm sygnalizujący, że materiał ma dużą gęstość, przez którą promieniowanie rentgenowskie nie może przeniknąć;
- oszczędzanie energii: przy wejściu do tunelu znajduje się czujnik, który automatycznie uruchamia pas transmisyjny, gdy zostanie na nim umieszczony bagaż. ●

ROGER

Integracja systemu kontroli dostępu RACS 5 z windami KONE

KONE to światowy lider w branży wind i schodów ruchomych, z którego produktów każdego dnia korzysta ponad miliard osób. Wysoka jakość oraz funkcjonalność tych rozwiązań sprawiają, że bardzo często są one stosowane w takich obiektach, jak biurowce, szpitale, fabryki czy budynki wielomieszkaniowe.

Na tym samym rynku jest również oferowany system kontroli dostępu i automatyki budynkowej RACS 5. Współpraca obu tych rozwiązań w naturalny sposób uzupełnia ich funkcjonalność, przynosząc użytkownikom szereg korzyści.
Integracja systemu RACS 5 z windami KONE może być realizowana za pomocą protokołu:

- komunikacyjnego RCGIF v1.12,
- komunikacyjnego GCAC v1.8,
- bazodanowego KONE Access Rev. 8.5.

W pierwszym scenariuszu system RACS 5 przydziela użytkownikowi posiadającemu odpowiednie uprawnienia windę, która zawiezie go na konkretne piętro. Rozwiązanie to podnosi komfort użytkowania i optymalizuje zarządzanie ruchem osób w obiekcie.

Z kolei w przypadku integracji opartej na protokole GCAC możliwe jest dokonanie samodzielnego wyboru piętra spośród tych, do których nadane są uprawnienia. Funkcjonalność ta podnosi poziom bezpieczeństwa w obiekcie, ograniczając wybór wyłącznie do tych pięter, do których użytkownik ma dostęp.
Integracja poprzez protokół KONE Access łączy funkcjonalność obu wcześniej wymienionych rozwiązań z tą różnicą, że jest integracją bazodanową, w której ustawienia użytkowników są przesyłane z systemu RACS 5 do systemu windowego na żądanie operatora lub automatycznie, z określoną częstotliwością.
Dzięki integracji z windami KONE system kontroli dostępu RACS 5 skutecznie zarządza zarówno przejściami, jak i piętrami budynku, podnosząc poziom bezpieczeństwa oraz komfort użytkowników. To rozwiązanie zostało wdrożone m.in. w kilku wieżowcach w centrum Warszawy oraz w duńskim Danhostelu. ●

SAFE PLACE

VII Międzynarodowy Kongres Naukowo-Techniczny SAFE PLACE 2024

SAFE PLACE to największy w Polsce kongres poświęcony bezpieczeństwu obiektów. Wśród współorganizatorów i patronów wydarzenia znajdują się m.in. Rządowe Centrum Bezpieczeństwa, NATO DEEP eAcademy, Wojskowa Akademia Techniczna w Warszawie, Akademia Pożarnicza, Uniwersytet WSB Merito we Wrocławiu i wiele innych instytucji.

Tematem tegorocznej edycji jest odporność obiektów użyteczności publicznej i infrastruktury krytycznej wobec zagrożeń wojennych, hybrydowych i kryminalnych. Wydarzenie odbędzie się 27–28 listopada w hotelu Windsor w Jachrance k. Warszawy. W tym roku organizatorzy kongresu przygotowali m.in.:

- 11 sesji tematycznych dotyczących współczesnych szans i zagrożeń bezpieczeństwa (sztuczna inteligencja, przygotowanie do wojny, innowacje technologiczne).
- Warsztaty praktyczne z reagowania na zamachy, w tym profesjonalne pozoracje – odgrywanie scenariuszy z wykorzystaniem replik broni i z udziałem uczestników
- Warsztaty praktyczne z pierwszej pomocy, prowadzone przez certyfikowanych ratowników KPP z Centrum Ratownictwa.
- Interaktywne stoiska edukacyjne, prezentacje innowacji w branży zabezpieczeń technicznych, pokaz dronów, strefa networkingowa.
- Atrakcje i konkursy: zawody strzeleckie z broni pneumatycznej, przeciąganie liny, loteria książkowa i niespodzianki, o których będziemy informować w późniejszym czasie.

Podczas tegorocznej edycji ponad 300 polskich i zagranicznych ekspertów zgromadzi się, by omówić aktualne wyzwania, innowacje i narastające potrzeby w branży bezpieczeństwa.

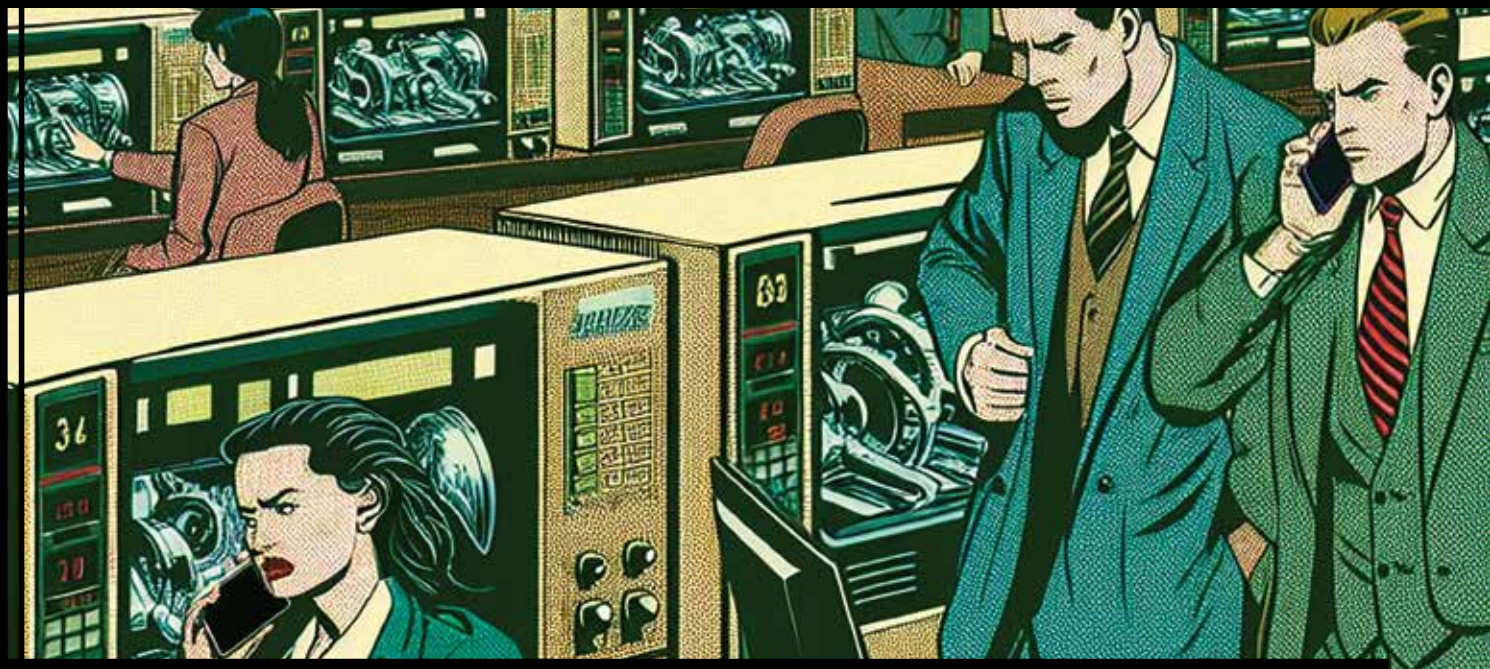
Szczegółowe informacje dostępne są na stronie www.safeplace.edu.pl. ●

Ile to jest jeden „bul”?

Bogusław Kot wracał z kuchni, gdzie spędził dobre pół godziny na dokładnym opieczeniu każdej grzaneczki, jak miał to w zwyczaju codziennie w samo południe. Dziś był nie w sosie, bo w firmowej kuchni znowu szarogęsił się ten Szwedzki Kucharz, jak nazywał w duchu pewnego młodego człowieka, który niedawno pojawił się w firmie.

Nie dość, że Szwed, to jeszcze jakiś super-duper ekspert, z którym każdy musiał się liczyć. Jego obecność nie poprawiała humoru Panu Kotu, jak mówiła o nim specjalistka ds. technologii Emilia Szpaczek. Dlatego z niezadowoleniem malującym się na twarzy, choć miękkim krokiem, sunął przez halę produkcyjną, kierując się w stronę swojej kanciapy, z której jako majster miał widok na wszystko i wszystkich. Kątem bystrego oka zdołał jednak dostrzec, że panna Szpaczek, maszerując tam i z powrotem po hali, prowadzi intensywną rozmowę. I robi się coraz bardziej czerwona na twarzy. Gdy go dostrzegła, zamachała ręką, gwałtownie przywołując go do siebie.

Bogusław miał ochotę udać, że nie widzi. Lubił pannę Szpaczek, ale lubił też ciepłe grzaneczki. Jeśli podejdzie, te wystygną. „Trudno”, westchnął w duchu i godząc się ze stratą, podszedł ze zbolałą miną do panny Emilii, która tłumacząc się przez telefon, zabawnie podskakiwała na palcach. „Ot, jaki z niej wróbelek”, pomyślał Kot i pytająco uniósł brwi. Szpaczek zakończyła rozmowę i tym razem jak indyk podskoczyła do majstra.



– Panie, panie Kot. Co tu się dzieje? Ludzie do mnie wydzwaniają. Jakieś afery. Maszyny się zacierają, to już trzecie zgłoszenie dzisiejszego dnia, a dopiero południe! – Szpaczek wymachiwała ze złości rękami.

„Nie, jednak nie wróbelek, raczej indor", Kot nabrał pewności, że z tej Szpaczek to niezły… hm, ptaszek.

– O czym pani mówi, panno Emilio? – Kot lubił ten archaiczny zwrot, zupełnie nie mając przy tym pojęcia, jak drażni nim specjalistkę od technologii, której wszystkie nieśmiertelne jak sekwoje ciotki wypominały przy każdej okazji stan cywilny.

– Otóż, panie Kot, mamy poważny problem. Nasz produkt znacząco stracił na jakości. Od tygodnia docierają do mnie dziwne wieści, ale teraz to już szczyt wszystkiego! – Panna Szpaczek mówiła coraz bardziej podniesionym głosem. – To już TRZECI telefon od klientów mocno zdenerwowanych tym, że ich maszyny odmawiają posłuszeństwa! A ONE KOSZTUJĄ MILIONY. Panie KOT! Pójdziemy z torbami! A ja na pewno! – Emilia była na granicy apopleksji.

Kot uniósł znacząco palec, potem brwi i powiedział coś dziwnego:

– Szwedzki Kucharz. To na pewno on..

Narada w gnieździe

Szpaczek była zrozpaczona, Kot zeźlony, a Marek Myszyński, szef ds. bezpieczeństwa, czuł, że za chwilę w jego przytulnym biurowym gniazdku dojdzie do rzezi niewiniątek. Sprawa faktycznie była dziwna. Ktoś majstrował przy składzie bardzo ważnego specyfiku, dzięki któremu bardzo ważne i bardzo, ale to bardzo drogie maszyny mogły produkować jeszcze ważniejsze i jeszcze droższe przedmioty. Bankructwo firmy w tym wszystkim było w tej chwili najmniejszym problemem. Większym było to, że wszystkie nagrania z monitoringów, analiza danych sieciowych i dostępów nie wskazywały, by w zakładzie działo się coś niepokojącego. Dostępy pracownicze były ściśle nadzorowane. Uprawnienia systemowe regularnie sprawdzane. Specjalistka ds. technologii Emilia Szpaczek zaklinała się na wszystkie świętości, że nic, ale to nic nie zmieniło się w recepturze, i miała na to dowody.

A najgorsze było to, że Bogusław Kot, ceniony, doświadczony majster, podejrzewał o sabotaż Szweda, którego zatrudniono za ciężkie pieniądze, by kosztowo zoptymalizował produkcję.

– Na moje oko i ucho to ten Szwedzki Kucharz. – Kot nie odpuszczał. – On jest… obcy. Ktoś go zna?

– Ależ panie Kot, jak pan może! – Emilię aż zatkało z oburzenia. – To, że cudzoziemiec, to jeszcze nic nie znaczy…

– Panno Szpaczek, ale co mnie obchodzi, że on cudzoziemiec? To nie ma żadnego znaczenia. Może być i ten… Marsjan. Ale czy ktoś go zna? Pani wie, że nasza branża jest mała. Wszyscy w zasadzie się znamy. Na konferencjach cały czas te same gęby, a nowi, jak się pojawiają, to z rzadka i wiadomo, u kogo studiowali. A ten?

„Coś jest na rzeczy", pomyślał Myszyński. „Przecież ja praktycznie nic o nim nie wiem". I postanowił trochę pogrzebać w światowej pajęczynie wszelkich wiadomości.

Ze Szwecji, ale...

Myszyński niezwłocznie rozpoczął dyskretne dochodzenie. Dokumenty otrzymane z kadr wyglądały nieźle, ale nigdzie nie mógł znaleźć żadnych konkretnych informacji o specjaliście sprowadzonym z północy Europy. To skłoniło go, by zwrócić się wprost do uczelni i poprzednich miejsc pracy Szwedzkiego Kucharza. To, czego się dowiedział, nieco zbiło go z pantałyku. Szwed nie był wprawdzie do końca tym, za kogo się podawał, ale też z pewnością nie był dywersantem, za jakiego miał go Kot. Przy tej okazji Myszyński zrozumiał, że trzeba wprowadzić solidniejsze procedury weryfikacji pracowników.

– I co, panie Myszyński? Miałem rację? To on? – zapytał Kot, gdy spotkali się podczas narady błyskawicznie zwołanej po tym, gdy kolejny klient zadzwonił z pretensjami.

– Daj pan człowiekowi spokój! – Szef ds. bezpieczeństwa nie krył irytacji. – Szwed jest swój, to znaczy nasz. Możemy mu ufać.

Kot się trochę najeżył, a Szpaczek, która nie wiedzieć czemu bardzo polubiła młodego Skandynawa, odetchnęła z ulgą.

– To co teraz robimy? – zapytała. – Bo ciągle dzwonią…

Myszyński potarł czoło.

– Nie wiem. Jak babcię kocham, nie wiem.

– Nagle poderwał się z krzesła i zdecydował.

– Ja sprawdzam wszystkich: od sprzątaczki po prezesa. Pani sprawdza każdy surowiec, z którego robimy specyfik, łącznie z klejem na etykietach. A pan – wyciągnął palec w stronę Kota – idzie na halę i zagląda wszędzie, nawet do mysiej dziury

– U nas myszy nie ma! – Oburzył się Kot. – Ale ma pan rację, ruszamy do boju.

Na oko

Myszkujący po hali Kot nie wzbudził w pracownikach większego zdziwienia. Znali majstra i wiedzieli, że lubi mieć wszystko na oku, choć tym razem zachowywał się trochę nietypowo. Oglądał maszyny, sprawdzał próbniki, zerkał do szuflad i na szafki. I choć bardzo się starał, to nigdzie nie dostrzegł niczego niepokojącego. Plomby na swoich miejscach, pracownicy z właściwymi identyfikatorami, drzwi, tam gdzie trzeba zamknięte… Nagle jego wzrok przykuł młody człowiek, który do głównego zbiornika dolewał coś z niewielkiego baniaka. Kot wiedział, że to rodzaj uzdatniacza niezbędnego do produkcji właściwego specyfiku, ale dodawanego w wartości wręcz marginalnej. I im dłużej patrzył, tym bardziej czuł, że za chwilę zejdzie na zawał. Nie czekając dłużej, wrzasnął:

– Co ty tam robisz, do diaska?!

Młody chłopak podskoczył z wrażenia. Z baniaka chlupnęła dodatkowa porcja.
– Dolewam, panie majster.
– Ale jak dolewasz? Gdzie miarka? – Kot czuł, że zaraz się zagotuje.
– A… miarka, no nie ma, gdzieś się zgubiła. – Karol Szczurek nie rozumiał, o co te wrzaski.
– To tak na oko lejesz? – Kot aż parsknął ze zdumienia.
– Panie majster, jakie na oko. W życiu na oko. Tak na dwa „bule".
– Bule? Jakie bule, że co?! – Kot ryknął jak tygrys.
– No raz robi „bul" i drugi raz „bul", i wtedy jest git. Znaczy się akurat – powiedział Szczurek i nagle go olśniło, że jego kariera w firmie robiącej bardzo ważny specyfik do bardzo drogich maszyn właśnie się skończyła.

Opracowała Monika Żuber-Mamakis na bazie scenariusza Jacka Grzechowiaka

Cóż takiego mógł odkryć szef ds. bezpieczeństwa Marek Myszyński i czy Bogusław Kot powinien się wstydzić swoich podejrzeń? Sabotaż i dywersja – to kolejny temat warsztatów Security Forum, jak zawsze poprowadzonych przez naszego eksperta Jacka Grzechowiaka.

Konrad Badowski, Axis Communications

Tym razem Jacek Grzechowiak nie skupił się na jednym studium przypadku, lecz pokazał ogólne podejście do zasad bezpieczeństwa i identyfikacji zagrożeń oraz radzenia sobie z nimi. Dla mnie zawsze ciekawa jest dyskusja z uczestnikami, bo można poznać ich punkt widzenia. Moja firma, jako producent, może zupełnie inaczej spoglądać na pewne sprawy niż użytkownik, który boryka się z konkretnymi zagrożeniami.

Julien Chaine, EST Polska

Szkolenie dostarczyło cennych informacji na temat sabotażu i kradzieży danych, podkreślając na rzeczywistych przykładach znaczenie procedur i ryzyko, które może pochodzić od osób z wewnątrz. Dla naszej firmy, zajmującej się systemami bezpieczeństwa, takie warsztaty są kluczowe, pomagając lepiej rozumieć potrzeby klientów i oferować im kompleksowe rozwiązania wzmacniające ich ochronę.

Paweł Grzywa, Securitas Polska

Podczas takich warsztatów bardzo cenny jest dla nas bezpośredni kontakt z klientami, możliwość wymiany doświadczeń oraz dyskusja na ważne dla klientów tematy.
Omówiliśmy szkolenie pracowników ochrony, koncentrując się na kluczowym aspekcie dotyczącym zagrożeń wewnętrznych. Te zagrożenia mają istotny wpływ na sposób, w jaki nasi pracownicy będą chronić obiekty i dbać o mienie klientów.

Andrzej Gałat, MAN Niepołomice

Warto uczestniczyć w takich szkoleniach, bo technologia cały czas się rozwija, pojawiają się nowe zagrożenia, z których nawet nie zdajemy sobie sprawy. Dlatego wymiana doświadczeń z ekspertami branży security jest bardzo cenna. Zawsze trzeba się rozwijać, poznawać problemy innych, bo z nich możemy czerpać wiedzę na temat tego, jak uchronić się przed zagrożeniami i właściwie zabezpieczyć nasz zakład pracy.

Zbigniew Trendak, Cargill

Szkolenie bardzo mi się podobało, bo prowadzący omawiał zagadnienia, posiłkując się przykładami wziętymi z życia. Kilka rozwiązań, na które zwrócił uwagę, mogę zaimplementować w mojej pracy. Szczególnie, jeśli chodzi o pewne aspekty dotyczące zarówno ochrony fizycznej, jak i procedur bezpieczeństwa. To dla mnie bardzo cenne doświadczenie.

Tomasz Gonta, AgriPlus

Z pewnością przyda mi się wiedza zdobyta podczas tego szkolenia. Cieszy fakt, że wiele osób zauważa problematykę intruza wewnętrznego. Na ten temat wywiązała się bardzo ciekawa dyskusja zainspirowana interesującą częścią merytoryczną. Dla mnie cenna była wymiana doświadczeń i rozmowy o zarządzaniu elementami bezpieczeństwa.


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

BCS®

dla profesjonalistów

tworzyMY

FLEX

POLSKA MARKA BCS

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

tworzyMY
rejestratory
dostosowane
do potrzeb klienta

WYPRODUKOWANO W POLSCE