



Raport: Transport i logistyka

20 zł
(w tym 8% VAT)



Security się zbroi

Rok 2023 czasem wyzwań i inwestycji.
Co się dzieje, gdy przyszłość staje się
rzeczywistością?

Od AI do osobliwości

Metawersum, superaplikacje i coraz
mniej sztuczna inteligencja – poznaj
trendy technologiczne.

Sytuacja sprzyja branży?

Jest ryzyko, jest... zabezpieczenie!
O security w czasach VUCA mówią
przedstawiciele branży.

WARSAW SECURITY SUMMIT

Największa
Konferencja
Branży
Zabezpieczeń
Nowa
Formuła

05/06/2023

SZCZEGÓŁY WKRÓTCE



EDITORIAL

Drodzy Czytelnicy

Rozwój towarzyszy nam od początku istnienia czasopisma „a&s Polska”. Kolejny rok rozpoczynamy również nastawieni na to, co nadejdzie – na inspirujące rozmowy, ciekawe opinie i fascynujące wydarzenia. Mamy ogromną nadzieję, że to wszystko znajdziecie w najnowszym wydaniu naszego magazynu.

Wiodącym tematem tego wydania jest transport i logistyka. To potężna gałąź polskiej gospodarki. Bezpośredni udział sektora transportu i magazynowania w polskim PKB wynosi 6%, ale pośrednio przyczynia się do wypracowania nawet 50% krajowego przychodu brutto. Za tymi liczbami kryje się ciężka praca ponad 125 tys. polskich firm, w wielu przypadkach niewielkich i rodzinnych (o specyfice firm rodzinnych w branży TSL przeczytacie w artykule na str. 28).

Każda z tych firm, niezależnie od wielkości, zмага się z podobnymi wyzwaniami: brakiem rąk do pracy, zmiennością otoczenia gospodarczego i prawnego, koniecznością zapewnienia dostaw – kompletnych i na czas. Dlatego postanowiliśmy przyjrzeć się temu rynkowi z bliska – pokazać jego skalę i różne oblicza. Jak polskie firmy wypadają na tle europejskich? Jak funkcjonują? Co najbardziej im dokwiera? Poznanie odpowiedzi na te pytania pozwoli lepiej zrozumieć ich potrzeby w zakresie security. Pełen raport znajdziecie na str. 14. Również „Głos branży” poświęcony jest wyzwaniom, z jakimi mierzą się firmy z branży TSL. O czym mówią eksperci, przekonacie się, zaglądając na str. 22.

Przedstawiciele branży security zapytaliśmy o kondycję rynku zabezpieczeń. Jak firmom security minął rok 2022, a jak patrzą w przyszłość? Z nadzieją czy z obawą? W niepewnych czasach, gdy w każdym momencie mogą pojawić się czarne łabędzie (Nassim Taleb, znany amerykański ekonomista, nazwał tak nieprzewidywalne i nieregularne zdarzenia o ogromnej skali i potężnych konsekwencjach), przewidywanie jest trudne. Pytani o to pracownicy firm branży security są optymistami. Może ostrożnymi, ale jednak... Szczegóły znajdziecie na str. 40, pod wymownym tytułem *Sytuacja sprzyja branży?*

Jak powiedział Niels Bohr: „Przewidywanie jest bardzo trudne, szczególnie jeśli idzie o przyszłość”. Nie zajmujemy się więc wieloletnimi przepowiedniami, przyjrzelśmy się jednak uważnie trendom technologicznym, jakie z pewnością zdominują tegoroczną gospodarkę. Jedno jest pewne – już teraz firmy powinny przygotować się na liczne wyzwania związane z etyczną stroną korzystania z AI. Sztuczna inteligencja staje się bowiem coraz mniej sztuczna (str. 56).

A przy okazji, czy zgodzicie się z nami, że w życiu jedyną pewną rzeczą jest zmiana? Gdy uważnie przyjrzyście się najnowszemu wydaniu magazynu „a&s Polska”, z pewnością zauważycie, że i my się zmieniliśmy...

Mamy nadzieję, że uznacie to za prawdziwą „dobrą zmianę”.

Życzymy miłej lektury,

Redakcja

ZŁOTY PARTNER A&S POLSKA



SREBRNY PARTNER A&S POLSKA



A&S POLSKA WYDANIE ONLINE

www.aspolska.pl/czasopismo

SPIS TREŚCI



8 Produkty Numeru

TRANSPORT I LOGISTYKA

- 14 Raport - Transport i logistyka w Polsce 2023
Adela Prochyra, a&s Polska
- 22 Głos branży
- 27 Bezpieczeństwo łańcucha dostaw w czasach VUCA
jest szczególnie ważne
DHL
- 28 Firmy rodzinne w transporcie drogowym
Jacek Tyburek
- 32 Rozwiązania do odczytu tablic rejestracyjnych
Jan Grusznic, a&s Polska
- 34 Przegląd rozwiązań ANPR
- 38 Od zarządzania personelem
po komplementarne rozwiązania logistyczne
Hikvision Poland

RYNEK SECURITY

- 40 Sytuacja sprzyja branży?
Iwona Krawiec, Monika Mamakis, a&s Polska
- 48 Security się zbroi. Przed nami rok pełen wyzwań
Michalina Nowak, a&s Polska

REDAKCJA

ADRES REDAKCJI
a&s Polska
ul. M. Rodziewiczówny 1 lok. 801
04-187 Warszawa
info@aspolska.pl
www.aspolska.pl

PREZES ZARZĄDU
Mariusz Kucharski

REDAKTOR NACZELNA
Marta Dynakowska

Z-CA RED. NACZELNEGO
Jan T. Grusznic

REDAKCJA
Monika Mamakis
Adela Prochyra

DZIAŁ REKLAMY
Iwona Krawiec

DZIAŁ PROJEKTÓW SPECJALNYCH
Jolanta A. Kucharska
Aleksandra Czapska
Michalina Nowak

CENTRUM KOMPETENCJI
Jacek Grzechowiak

KOREKTA
Jolanta Kucharska

PROJEKT GRAFICZNY I SKŁAD
Bogusław Kalwala

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

Redakcja zastrzega sobie prawo skracania i redagowania nadesłanych tekstów. Tytuły i śródtytuły pochodzą od Redakcji.
Opinie autorów nie muszą być tożsame z poglądami Redakcji.
Za treść reklam i artykułów partnerów Redakcja nie odpowiada.
Przedruki tekstów bez zgody Wydawcy są niedozwolone.

© Copyright by a&s Polska



BCS[®]

dla profesjonalistów

Podgląd na żywo Odtwarzanie Zdjęcie Aplikacja Konfiguracja **Smart Display** Otwórz platformę

admin Pomoc Wyloguj



BCS-V-TIP72VSR4-ITC

WWR 17546K

Real-time Analyze



Inf. o kameryze Camera 01

Czas przechwyty 2023-01-17 14:08:17

License Plate Type unknown

Typ pojazdu Sedan

Kolor pojazdu Czarny

Marka pojazdu Asiatar

Moving Direction Cofaj

Nazwa biblioteki list otherList

Kraj/region Poland



WWR17546K



WWR17546K



WPI14289C

**BCS VIEW Z FUNKCJĄ ANPR TO IDEALNE ROZWIĄZANIE
DLA LOGISTYKI I TRANSPORTU.
NIEZAWODNY SPOSÓB UŁATWIAJĄCY KONTROLĘ
I WERYFIKACJĘ NADJEŹDZAJĄCYCH POJAZDÓW.**



www.bcs.pl
www.facebook.com/bcspl
» Więcej przeczytasz na stronie 8



SPIS TREŚCI

TRENDY TECHNOLOGICZNE

- 54 Od sztucznej inteligencji przez metawersum do osobliwości
Monika Mamakis, a&s Polska
- 60 Sześć kluczowych trendów technologicznych,
które wpłyną na branżę security
Axis Communications

BEZPIECZEŃSTWO OBIEKTÓW

- 62 O dobrej i złej synergii dotyczącej systemów zabezpieczeń
Jacek Grzechowiak
- 66 Polski system kontroli dostępu klasy enterprise na stadionie
w Gdańsku
Roger
- 68 Inteligentny system ułatwiający szybką zmianę
reguł dostępu
Winkhaus
- 69 WaveKey. Mobilny dostęp, na którym możesz polegać!
2N
- 70 Lufthansa Technik: jak zachować równowagę pomiędzy
wolnością a wysokim poziomem bezpieczeństwa
Nedap Security Management
- 72 Bezpieczne lotnisko – obiekt i jego otoczenie
pod spójnym nadzorem
Cias

BEZPIECZEŃSTWO BIZNESU

- 74 Ochrona fizyczna i IT – zbieżność interesów i działań,
czyli jak zarządzać bezpieczeństwem
Tomasz Dacka

BEZPIECZEŃSTWO POŻAROWE

- 78 Jak otrzymać certyfikat B dla wyrobów stosowanych
w systemach bezpieczeństwa pożarowego
Grzegorz Mroczko
- 82 Nowe wyzwania, nowe pomysły, innowacyjne rozwiązania!
Nie zwalniamy tempa!
Schrack Seconet Polska

PRAWO

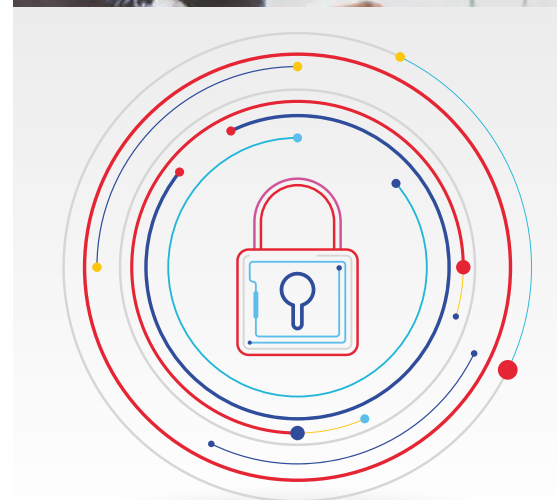
- 84 Część 1-1 normy *Systemy dozoru wizyjnego stosowane
w zabezpieczeniach* dostępna już po polsku
Waldemar Więckowski

SERWIS INFORMACYJNY

- 88 Informacje firmowe/nowości produktowe

CENTRUM KOMPETENCJI

- 92 Czym się kończy brak „bezpiecznika”
Monika Mamakis, a&s Polska



VISO SMS

Platforma do zarządzania systemami bezpieczeństwa w obiekcie

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





Prezentujemy najnowsze urządzenia z oferty firm:

**Axis Communications, BCS (NSS), Hikvision,
Nedap Security Management, Optex, smart-i,
Schrack Seconet Polska, TP-Link**



Axis Communications

AXIS Q1656-DLE Radar-Video Fusion Camera

Ochrona przed włamaniami na dużym obszarze i niezawodne wykrywanie 24/7 dzięki połączeniu dwóch potężnych technologii: wideo i radaru. To wyjątkowe urządzenie zapewnia najnowocześniejszą, opartą na głębokim uczeniu klasyfikację obiektów, co pozwala na wykrywanie i wizualizację na najwyższym poziomie.

AXIS Q1656-DLE Radar-Video Fusion Camera łączy dwa urządzenia klasy premium: najwyższej klasy kamerę z linii Q o doskonałych możliwościach wykorzystania obrazu i w pełni zintegrowany radar, który wykrywa obiekty na dużych obszarach przy słabym lub zerowym oświetleniu oraz wizualizuje prędkość i odległość poruszających się obiektów bezpośrednio w widoku aplikacji. Ponadto radaru można używać oddzielnie do prowadzenia autonomicznej kamery PTZ.

AXIS Q1656-DLE jest wytrzymała i odporna na warunki atmosferyczne, ma wbudowane funkcje cyberbezpieczeństwa, które chronią system.

Urządzenie jest łatwe do zainstalowania, wystarczy jeden przewód, jeden adres IP i jedna licencja na oprogramowanie do zarządzania wideo (VMS). Oznacza to niższe koszty instalacji i eksploatacji. Ponieważ radar „widzi” w ciemności, można ustawić wyzwalacze, które aktywują oświetlenie, lub podczerwień tylko wtedy, gdy chcemy odstraszyć intruza, zweryfikować go wizualnie lub uzyskać szczegółowe informacje. Oszczędza się również pamięć masową, ponieważ można wybrać uruchamianie nagrywania tylko w określonych sytuacjach. A niski wskaźnik fałszywych powiadomień pozwala pracownikom ochrony reagować tylko na prawdziwe zagrożenia.

Więcej na www.axis.com/pl-pl.



BCS

BCS View z funkcją ANPR - BCS-V-TIP72VSR4-ITC

Kamera BCS-V-TIP72VSR4-ITC to pierwszy model z serii BCS View wyposażony w funkcję rozpoznawania numerów tablic rejestracyjnych.

Kamera ma rozdzielczość 2 Mpix, dzięki której można łatwo zautomatyzować wjazd i wyjazd pojazdów na teren, który ma być dodatkowo chroniony. Rozdzielczość 2 Mpix może się wydawać mała, ale do prawidłowego odczytu tablic rejestracyjnych w zupełności wystarczy. Za poprawę skuteczności odpowiada też prędkość przechwytywania obrazu wynosząca 50 kl./s.

Odpowiednio skonfigurowana i prawidłowo zamontowana kamera odczyta numer tablicy rejestracyjnej i sama zadecyduje, co dalej z taką informacją zrobić. Jest wyposażona w moduł wejścia/wyjścia (1 we/ 1wy), dzięki czemu kamera może sama sterować barierą po rozpoznaniu numerów rejestracyjnych. Model zawiera obiektyw z motozoomem o ogniskowej 2,8–12 mm oraz promiennik podczerwieni o zasięgu do 40 m.

Kamera obsługuje też możliwość filtrowania numerów tablic rejestracyjnych za pomocą białej i czarnej listy, która może mieć pojemność do 10 000 wpisów. Rozpoznanie tablicy odbywa się nawet wtedy, kiedy pojazd przejeżdżający przed kamerą pozostaje w ruchu. Umożliwia to jej zastosowanie nawet w miejscach, gdzie nie ma fizycznej bariery, przed którą samochód musi się zatrzymać.

Kamera ma wbudowane systemy poprawy jakości obrazu, takie jak WDR, HLC, ręczne ustawienia promiennika IR czy migawki, aby nawet w nieprzychylnych warunkach zapewnić skuteczne rozpoznanie numeru rejestracyjnego.

Więcej na www.bcs.pl.



**Polskie profesjonalne
zintegrowane rozwiązania
VMS**

**Ponad 200 000 instalacji
na całym świecie
Jesteśmy z Wami od
2003 roku**



www.alnetsystems.com



HIKVISION

DS-K3G501SX – nowość w ofercie firmy Hikvision

Czy wdrożenie i instalacja tripoda musi być wymagająca? Tripod serii DS-K3G501SX został zaprojektowany w celu usprawnienia i zautomatyzowania procesu weryfikacji osób i ich uprawnień do nadzorowanych obszarów. Wbudowane czytniki kart Mifare (IC) pozwalają na kontrolę osób wchodzących i wychodzących.

Wbudowany kontroler dostępu z interfejsem TCP/IP jest rozpoznawany w oprogramowaniu nadzorującym jako przejście dwustronnie kontrolowane. Tripod można ustawić w jeden z trybów pracy: kontrola dwukierunkowa, kontrolowane wejście/blokada wyjścia, kontrolowane wejście/swobodne wyjście, swobodne wejście i swobodne wyjście, swobodne wejście/kontrolowane wyjście, blokada wejścia i blokada wyjścia, blokada wejścia/swobodne wyjście.

W sytuacji zagrożenia ramiona automatycznie opadają. Wykonany w klasie ochrony IP54 i ze stali nierdzewnej SUS304 pozwala na zastosowanie go w takich miejscach, jak sklepy, biura, place budowy, obiekty przemysłowe, hotele, szkoły, baseny, magazyny itd.

Więcej na www.hikvision.com/pl/.



Nedap Security Management

Integracja kontroli dostępu z systemem zarządzania gośćmi

Do aplikacji zintegrowanych z systemem kontroli dostępu Nedap AEOS dołączył Visitor Management System Click2Visit.

C2V to nowoczesne rozwiązanie zwiększające możliwości systemu KD w zakresie zaawansowanego zarządzania gośćmi w budynku. Przyspiesza ich wejście do gmachu, umożliwia wysłanie spersonalizowanych zaproszeń z kodem QR (także przy zaproszeniach grupowych), mapą

dojazdu do miejsca spotkania, informacją, kto jest gospodarzem spotkania, i logo firmy. C2V sprawdza się w obiektach biurowych i przemysłowych.

Ciekawą opcją jest możliwość wysłania zaproszenia z linkiem do regulaminu poruszania się po obiekcie, który należy podpisać, aby identyfikator gościa został aktywowany. Można też wystać link zgłoszenia do szkolenia z zakresu bezpiecznego poruszania się po obiekcie, które należy przejść przed pojawieniem się w firmie.

System umożliwia również zaproszenie gościa bezpośrednio z klienta pocztowego, np. z MS Outlook, automatyczne nadanie uprawnień do garażu, wind i publicznych przestrzeni w danym obiekcie. Użytkownik nie musi przełączać się na inne aplikacje, co znacząco skraca czas. Jest też wersja na urządzenia mobilne i obsługę Apple Wallet.

Dla obsługi recepcji nawet duża liczba wizyt w tym samym czasie jest łatwa do monitorowania. Prosty i przejrzysty interfejs umożliwia łatwy wgląd do informacji o liczbie gości w budynku oraz o zakończonych i przyszłych wizytach.

Więcej na: www.click2visit.eu.



OPTEX

FlipX Advanced – zaawansowana ochrona obiektów

OPTEX, wiodący globalny producent systemów antywłamaniowych, poinformował o kolejnej premierze. Gama czujek FlipX poszerza się o nowe czujki wewnętrzne Grade 3 z serii FlipX Advanced.

FlipX Advanced są wyposażone w specjalnie opracowany piroelement Human-catch dopasowany do rozmiarów człowieka oraz unikalną obrotową soczewkę sferyczną. Dzięki niej

czujkę można zastosować do ochrony zarówno szerokich, otwartych przestrzeni o dt. do 15 m przy kącie 85° (np. lobby hotelowe, sklep), jak i wąskich, długich obszarów do 24 m (np. korytarze, alejki magazynowe).

Inteligentna funkcja antymaskingu generuje sygnał w przypadku próby zakrycia czujki niezależnie od miejsca i sposobu maskowania. Dodatkowe algorytmy, m.in. podwójny filtr przeciwwakuceniowy (*Double Conductive Shielding*), zapewniają stabilną detekcję i redukcję fałszywych alarmów spowodowanych przez źródła światła lub zakłócenia elektromagnetyczne. Tryb „superczułości PIR” zapewnia niezawodne wykrywanie nawet w przypadku bardzo małej różnicy temperatury pomiędzy człowiekiem a otoczeniem.

Atutem jest też elegancki design z dobrze widocznym wskaźnikiem LED (sterowanym z centrali) oraz możliwość montażu na ścianie lub suficie do wysokości 3 m. Szybka i prosta instalację zapewniają wymiary listwy zaciskowa, rezystory końca linii montowane w oddzielnym gnieździe oraz pokrywa otwierana jednym ruchem ręki. Dostępne modele: FLX-A-AM (PIR), FLX-A-DAM (PIR+MW) – moduł mikrofalowy o bardzo długiej trwałości z charakterystyką detekcji dopasowaną do obszaru PIR.

Więcej na: www.optex.europe.com/pl.



POLON-ALFA


dobrze zaprojektowane BEZPIECZEŃSTWO

KOMPLEKSOWE SYSTEMY SYGNALIZACJI POŻAROWEJ

- PRODUKCJA • SERWIS • SZKOLENIA
- WSPARCIE TECHNICZNE I PROJEKTOWE

AUTOMATYKA POŻAROWA

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



Schrack Seconet Polska

ADW 535 – nowa liniowa czujka ciepła

Liniowe czujki ciepła są odpowiedzią na wymagania stawiane przed systemami wykrywania zjawisk niebezpiecznych w miejscach, gdzie konwencjonalne czujki pożarowe nie mogą być zastosowane ze względu na agresywne i krytyczne warunki atmosferyczne (np. wysoka wilgotność, ekstremalne temperatury, obszary zewnętrzne, żrące gazy, zanieczyszczenie pyłem itp.) lub tam, gdzie ze względu na wyjątkowo duże odległości i obszary do nadzorowania byłaby wymagana bardzo duża liczba czujek ciepła.

Firma Schrack Seconet wzbogaca swoją ofertę liniowych czujek ciepła o czujkę ADW 535, występującą również w wykonaniu do stref EX oznaczoną dodatkowo Hx. Czujka ADW składa się z jednostki oceniającej służącej do podłączenia jednej (ADW 535-1) lub dwóch (ADW 535-2) rurek sensorycznych z indywidualnymi, konfigurowalnymi czujnikami nadmiarowo-różnicowymi. Zasada działania jest oparta na pomiarze zwiększającego się ciśnienia powietrza w układzie zamkniętym rurki podczas jej ogrzewania. Ciśnienie jest stale monitorowane przez w pełni elektroniczny czujnik ciśnienia, porównywany i oceniany przez mikroprocesor z zaprogramowanymi poziomami alarmowymi.

W zależności od warunków środowiskowych do wykonania rurek sensorycznych są wykorzystywane różne materiały, np. miedź, stal nierdzewna lub teflon. Czujka ADW dzięki zastosowaniu modułu pętlowego XLM35 może być w pełni integrowana poprzez pętlę X-Line, co pozwala programować, obsługiwać oraz konserwować czujkę z poziomu centrali, bez konieczności udawania się bezpośrednio do czujki, która często bywa montowana w trudno dostępnych miejscach.

Więcej na: www.schrack-seconet.pl



Smart-i

Eagle Eye LPR | Automatyczne rozpoznawanie tablic rejestracyjnych w chmurze

Każdego dnia nawet kilkaset samochodów przekracza bramy centrów logistycznych. Zapanowanie nad tak dużym natężeniem ruchu jest wyzwaniem w kontekście kontroli dostępu i bezpieczeństwa. Z pomocą przychodzi nowoczesne systemy automatycznego rozpoznawania tablic rejestracyjnych – ANPR.

Jednym z takich rozwiązań jest Eagle Eye LPR – inteligentny system oparty na sieci neuronowej, który automatycznie rozpoznaje tablice rejestracyjne, a następnie umożliwia wjazd pojazdom znajdującym się na liście z przyznanym dostępem. System jest intuicyjny w obsłudze i umożliwia szybkie dodawanie nowych numerów rejestracyjnych oraz usuwanie nieaktualnych. Wszystko odbywa się w chmurze.



Wdrożenia Eagle Eye LPR przynoszą same korzyści: brak kosztów związanych z zakupem specjalnych kamer LPR (można zastosować dowolną kamerę), skalowalne rozwiązanie, które w ramach jednego systemu może być stale rozwijane (optymalizacja kosztów – płacimy za to, co w danym momencie wykorzystujemy), łatwa obsługa i zarządzanie systemem z dowolnego miejsca na świecie.

System Eagle Eye LPR wykorzystuje nowoczesną technologię, która sprawdza się w centrach logistycznych, gdzie jest duża różnorodność pojazdów i numerów rejestracyjnych. Odczytuje nawet zabrudzone tablice rejestracyjne przy szybkości do 56 km/h.

Eagle Eye to bardzo wygodne i elastyczne rozwiązanie, którego funkcjonalność łatwo dostosować do bieżących potrzeb.

Więcej na: www.smart-i.pl

Tp-Link

TP-Link VIGI C540 – 4 Mpix zewnętrzna obrotowa kamera CCTV

VIGI C540 to zewnętrzna kamera sieciowa typu PT (pan/tilt), która generuje obraz w rozdzielczości 4 Mpix. Wbudowane diody LED zapewniają kolorowy obraz także w całkowitej ciemności. Urządzenie zostało wyposażone w wodoodporną i pyłoszczelną obudowę o klasie ochrony IP66, dzięki czemu jest odporne na warunki atmosferyczne.

Kamera może być zasilana poprzez PoE w standardzie 802.3af/at lub przez klasyczny zasilacz DC 12 V. Urządzenie wykorzystuje kompresję H.265+, co zmniejsza obciążenie sieci i obniża koszty monitoringu bez utraty jakości obrazu. Nagrania z kamery mogą być rejestrowane na rejestratorze sieciowym, a także na karcie microSD.

VIGI C540 oferuje także dwukierunkową transmisję audio, czyli możliwość rozmowy przez urządzenie, np. z kurierem, którego można poprosić o zostawienie przesyłki przed drzwiami.

Kamerami z tej serii można w prosty sposób zarządzać z poziomu smartfona dzięki aplikacji VIGI na urządzenia przenośne z systemem iOS lub Android. Kamera wyśle powiadomienie *push*, gdy wykryje niepożądany ruch, zaobserwuje przekroczenie wyznaczonej granicy lub gdy ktoś zasłoni jej obiektyw. Systemem VIGI można też zarządzać z poziomu dedykowanego oprogramowania przeznaczonego dla komputerów oraz rejestratorów NVR, dostępnych w wersjach 4-, 8- i 16-kanalowych.

Wszystkie urządzenia z serii TP-Link VIGI są zgodne ze standardem ONVIF, współpracują z kamerami i rejestratorami różnych producentów i umożliwiają stworzenie kompleksowego systemu monitoringu.

Kamera VIGI C540 została objęta 3-letnią gwarancją producenta.

Więcej na: www.tp-link.com.pl



ZINTEGROWANA PLATFORMA BRIVO DO KONTROLI DOSTĘPU

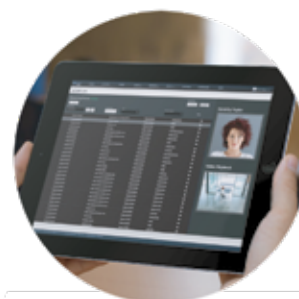
ŚWIATOWY LIDER I PIONIER W ZAKRESIE KONTROLI DOSTĘPU I PLATFORM OCHRONY OPARTYCH W CHMURZE



Kontrola dostępu
Zautomatyzuj kontrolę dostępu budynku oraz raportowanie



Monitoring wizyjny
Wyświetlaj obrazy w czasie rzeczywistym i przeglądaj zapisy



Zdalne zarządzanie
Zarządzaj zabezpieczeniami z dowolnego urządzenia mobilnego



Zarządzanie użytkownikami
Nadawaj uprawnienia użytkownikom w systemie



Kontrola odwiedzających
Bezpieczne warunki dla odwiedzających i pracowników



Analiza danych
Przetwarzaj informacje na temat bezpieczeństwa fizycznego



Raport: Transport i logistyka

Transport i logistyka to tradycyjnie temat pierwszego numeru „a&s Polska” w roku. Postanowiliśmy przyjrzeć się temu rynkowi z bliska – pokazać jego skalę i różne oblicza. Znajomość kontekstu, w jakim funkcjonują firmy tej branży, pomoże lepiej zrozumieć ich potrzeby w zakresie security.

Adela Prochyra, a&s Polska

W raporcie omawiamy polski rynek przewozów w 2023 r. – jego wielkość, największe atuty i braki, wyzwania, z jakimi się mierzy, a także perspektywy. Przedstawiamy również jego specyfikę na tle innych krajów europejskich oraz odpowiadamy na pytanie, czy Polska faktycznie jest europejską potęgą w dziedzinie transportu.

W ciągłej niepewności

Żadna branża nie działa w próżni. Wszystko, co dzieje się na świecie, znajduje odzwierciedlenie w poszczególnych sektorach gospodarki krajowych. Aktualne wydarzenia geopolityczne szczególnie mocno przenikają do transportu i logistyki. Świat nie zdążył się jeszcze otrząsnąć po pandemii koronawirusa, która zweryfikowała dotychczasowe sposoby produkcji i dystrybucji dóbr. W ostatnich dwóch latach dużo mówiło się o zerwanych łańcuchach dostaw. Chiny do końca 2022 r. prowadziły restrykcyjną politykę „zero COVID”, którą dopiero niedawno złagodziły – wciąż nie wiadomo, jakie to przyniesie skutki dla przemysłu globalnego. W Ukrainie trwa wojna z Rosją, której jednym ze skutków jest światowy kryzys energetyczny. Zmienność warunków i działanie w obszarze niepewności to naturalny element rynku.

W ciągu ostatnich trzech lat branża musiała zmierzyć się z szeregiem zmian i istotnych utrudnień:

- zamknięciem rynków i zerwaniem łańcuchów dostaw, czego negatywne skutki odczuło aż 47% przedsiębiorców (źródło: Badanie Instytutu Keralla Research na zlecenie BIG InfoMonitor);

- gwałtownym wzrostem cen energii i paliw;
- zamknięciem obszarów objętych wojną dla transportu drogowego dóbr i ludzi, co spowodowało opóźnienia i dalsze podwyżki cen dostaw;
- wzrostem inflacji – rekordowe 17,9% odnotowane w październiku 2022 r. w Polsce – i światową recesją, którą silnie odczuje zwłaszcza Europa (źródło: Raport Citibanku *Perspektywy rynkowe na 2023 r.*).

Rynek polski jest wprawdzie jednym z tych, które najłagodniej przeszły przez okres pandemii, co nie znaczy, że powyższe czynniki nie miały na niego wpływu.

Obszar TSL (transport, spedycja, logistyka) jest w Polsce duży i generuje wysokie przychody, jednak prawie żadna ze spółek transportowych nie jest notowana na Giełdzie Papierów Wartościowych w Warszawie. Oznacza to gorszy dostęp do danych firm tej branży, co z kolei przekłada się na pewne luki w źródłach, na które się tu powołujemy.

Metodologia

Wobec wielkości i złożoności zagadnienia należy przede wszystkim wyjaśnić, co rozumiemy pod pojęciami „transport” i „logistyka”. Transport można podzielić na kilka podkategorii: pasażerski, towarowy, usługi pocztowe, przeprowadzkowe, przesył rurociągowy oraz usługi związane z logistyką, magazynowaniem i przeładunkiem.

Gros danych i komentarzy w niniejszym raporcie będzie dotyczyć transportu drogowego ze względu na to, jak istotna jest jego skala. W roku 2021 przewieziono 2 253 377 tys. ton ładunków, z czego aż 2 193 845 tys. ton transportem lądowym, co stanowi ponad 97% ogółu transportu w Polsce. Zawierający się w nim transport kolejowy odbywa się na poziomie mniejszym o rząd wielkości i wynosi 237 915 tys. ton.

Transport drogowy rzeczy – usługa polegająca na przemieszczaniu ładunków pojazdami samochodowymi lub zespołami składającymi się z pojazdu samochodowego i przyczepy bądź świadczeniem usług dodatkowych związanych z tym procesem. Nie ogranicza się jedynie do samego przewozu, ale obejmuje również organizację i planowanie przepływu ładunków. Według definicji Polskiej Klasyfikacji Działalności to „działalność związana z przewozem osób lub towarów realizowana przez transport kolejowy, rurociągowy, drogowy, wodny lub powietrzny”, a także „działalność wspomagająca przewozy świadczona przez stacje, porty, dworce kolejowe, autobusowe itp. terminale w zakresie kontroli ruchu, obsługi pasażerów, bagażu i ładunków” oraz „wynajem sprzętu transportowego z kierowcą lub załogą, działalność pocztowa i kurierska”.

Transport jest bardzo ważnym elementem usług logistycznych, które zajmują się planowaniem, realizacją i kontrolowaniem efektywnego przepływu surowców, materiałów, wyrobów gotowych i informacji między punktem pochodzenia a punktem konsumpcji. Granica między transportem a innymi usługami logistycznymi jest nieostra, jednak transportem nazywamy każdą usługę logistyczną, która w trakcie realizacji zawiera przewóz towarów transportem drogowym. Może to być transport drogowy z punktu A do punktu B, transport intermodalny, czyli złożony, wykorzystujący więcej niż jedną gałąź transportu, lub kompleksowa usługa logistyczna z wieloma podzadaniami, np. analizą, dokumentacją i wykonaniem transferu, w której zawiera się transport drogami lądowymi. Transport jest usługą realizowaną przez firmy, które

w swojej podstawowej działalności mają zapisany transport drogowy towarów lub usługi towarzyszące transportowi drogowemu, a więc posługują się kodami PKD 49.41.Z lub 52 i 53.

Liczy: wielkość rynku przewozowego

Wielkość tej dziedziny i jej znaczenie dla krajowej gospodarki zasługują na uwagę branż współpracujących. W Polsce działa ok. 125 tys. firm, które zajmują się transportem drogowym towarów, co stanowi 6,6% wszystkich przedsiębiorstw zarejestrowanych w kraju, jak napisano w obszernym raporcie *Transport drogowy w Polsce 2021+*, opracowanym przez SPOTDATA na zlecenie i przy współpracy ze Związkiem Pracodawców Transport i Logistyka Polska. Jego autorzy piszą wręcz, że transport stanowi krwiobiegi gospodarki, a wartość tego rynku w Polsce szacują na 190 mld zł, przy średnim tempie wzrostu 10% w ubiegłej dekadzie (dane za 2020 r.).

Usługi przewozowe, magazynowania czy szerzej logistyczne stanowią kluczowy element łańcucha dostaw i produkcji w wielu branżach, można zatem założyć – z braku precyzyjnych danych – że transport przyczynia się do wypracowania nawet 50% polskiego PKB, a w obu dziedzinach, to jest transporcie i logistyce, zatrudnienie (na podstawie wszelkiego rodzaju umów) znajduje łącznie ok. 2 mln osób.

» W 2022 r. firmy z branży transportowej odnotowały znaczny wzrost przychodów – aż 28,8% w porównaniu do roku poprzedniego. «

Główny Urząd Statystyczny podaje bardziej szczegółowe informacje. W roku 2020 (należy wziąć poprawkę, że był to rok pandemiczny i większość branż zamroziła działalność) przychody ze sprzedaży usług w jednostkach transportu były co prawda niższe w porównaniu z rokiem poprzednim, dokładnie o 1,2%. Całkowita kwota przychodów wyniosła jednak aż 280,6 mld zł. Polska branża jest częścią większego rynku europejskiego, a ten, zgodnie z prognozą agencji badawczej Transport Intelligence, miał w 2022 r. osiągnąć wartość 390,75 mld euro. Skok ten jest wywołany postpandemicznym przebudzeniem i entuzjazmem wyrażanym zwiększoną konsumpcją. Jest to 4,9-procentowy wzrost w stosunku do roku poprzedniego i aż 6,3-procentowy w stosunku do przedpandemicznego 2019 r. Prognozy dla polskiego rynku transportowego na koniec 2022 r. były jeszcze lepsze – eksperci TI liczyli na wzrost 18,6% w stosunku do 2019 r. i zaznaczali,

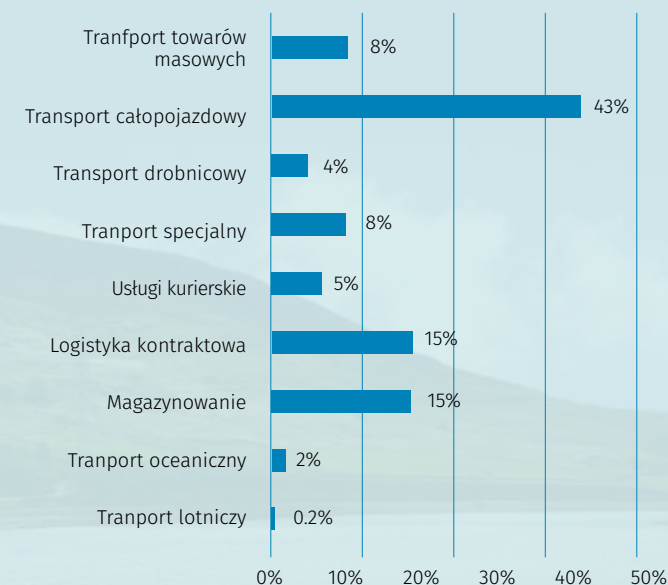
że będzie to jeden z najdynamiczniejszych wzrostów wśród krajów europejskich – lepiej miało być tylko w Norwegii, Irlandii, Estonii i na Litwie, gdzie rynki są jednak znacznie mniejsze od naszego.

Czy te prognozy się sprawdzą? Ze względu na rosnące niemal z tygodnia na tydzień koszty energii i gazu, które stanowią znaczną część wydatków, budżety wielu firm na rok 2023 zostały poddane daleko idącej korekcie. Rosnąca inflacja przekłada się z kolei na spadek konsumpcji, a ten na obniżenie wolumenów w wielu branżach, w tym transportowej.

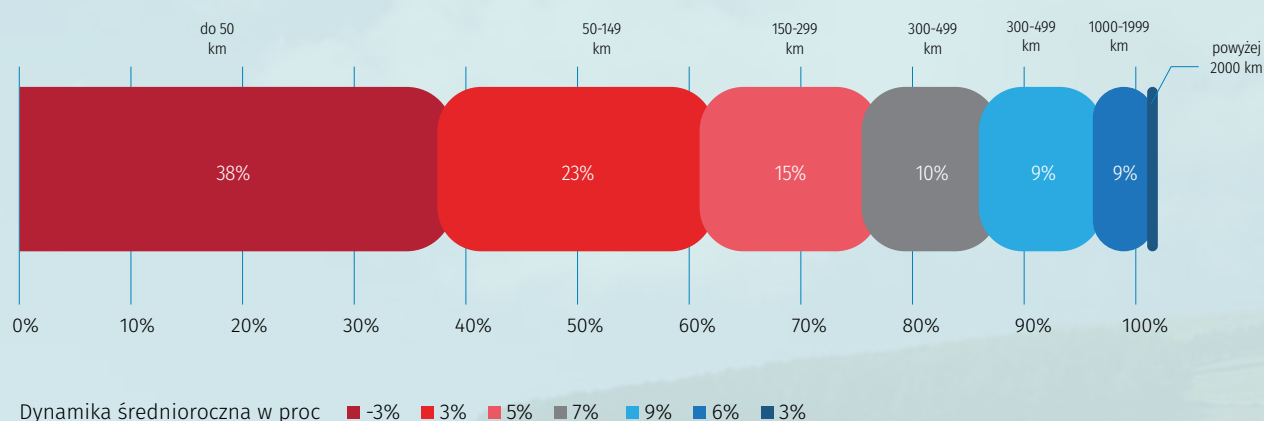
Najwięksi przewoźnicy w Polsce

„Rzeczpospolita” co roku publikuje ranking stu największych firm z branży TSL. Firmy zatrudniające 250 osób lub więcej generują 16% przychodów w Polsce (średnia UE to 21%). Liderem rankingu pod względem wysokości przychodów jest Poczta Polska,

Udział usługi w rynku logistycznym w Polsce



Struktura transportu według odległości



która dysponuje własną bazą magazynową oraz flotą 6 tys. pojazdów, zatrudnia ponad 70 tys. osób i ma 7600 punktów sprzedaży swoich usług, a te są zróżnicowane – od usług pocztowych, z których korzysta 90 proc. Polaków, przez komunikacyjne, po usługi ubezpieczeniowo-bankowe.

Kolejne miejsca zajęły:

- Amazon Fulfillment Polska
- PKP Cargo
- Grupa Raben Logistics Polska
- DPD Polska

Ten sam ranking jest źródłem informacji, że w 2022 r. firmy z branży transportowej odnotowały znaczny wzrost przychodów – 28,8% w porównaniu do roku poprzedniego. Ten wzrost był wynikiem nie tylko podniesienia cen paliw i tym samym droższych usług transportowych, ale także rosnącego rynku e-commerce. Swoją ranking pół roku wcześniej (czerwiec 2022) opublikował „Dziennik Gazeta Prawna”, który przyznał wyróżnienia w siedmiu kategoriach. Część nazw siłą rzeczy pokrywa się z rankingiem „Rzeczpospolitej”, ale ze względu na większe zróżnicowanie tematyczne wiele firm pojawia się tylko w tym drugim.

Rozdrobnienie

Lista tzw. dużych graczy, których tylko część wymieniliśmy powyżej, nadal nie oddaje obrazu całej branży TSL. Charakterystyczna dla polskiego rynku przewozowego jest przewaga mikroprzedsiębiorstw, co odróżnia go od rynków europejskich.

W branży transportowej firmy zatrudniające maksymalnie 10 osób stanowią ponad 50% wszystkich firm i odpowiadają za 37% przychodów (średnia w UE to 25%). Są to głównie jednoosobowe działalności gospodarcze, w drugiej kolejności przedsiębiorstwa rodzinne. Należy jednak pamiętać, że nie wszystkie firmy z kodem PKD sugerującym działalność transportową faktycznie ją prowadzą, dlatego dane te trzeba traktować z pewną rezerwą. Jest też wiele firm specjalizujących się w innych dziedzinach, takich jak budownictwo, które dysponują flotą i dodatkowo, poza swoją pierwotną specjalizacją, mogą świadczyć usługi przewozowe.

Dużym minusem tego rozdrobnienia jest mniejsza możliwość wprowadzania innowacji i nowoczesnych, nieraz kosztownych rozwiązań. Skutkuje to kolejnym rozziwem pomiędzy rynkami europejskimi a polskim. Rynek europejski jest bardziej wyspecjalizowany – kraje Europy Zachodniej sprawdzają się w usługach okołotransportowych, podczas gdy kraje peryferyjne oraz Europy Środkowo-Wschodniej, w tym Polska – w przewozach towarów, co jest usługą prostszą i tańszą. Należy jednak zauważyć, że struktura polskiego transportu powoli zbliża się do średniej europejskiej. Świadczy o tym m.in. fakt, który podnoszą wszystkie źródła, a mianowicie że najszybciej na rynku rośnie liczba średnich i dużych przedsiębiorstw. Ma to wiele plusów – następuje większa profesjonalizacja i lepsza organizacja rodzimych firm, a więc wyższa jakość usług.

Usługi logistyczne

Typologii usług logistycznych jest wiele. Powołujemy się na Fraunhofer Center for Applied Research on Supply Chain Services SCS, który opracował wyczerpujący raport *Top 100 in European Transport and Logistics Services*. Na tej podstawie można wyodrębnić dziewięć typów usług logistycznych:



Źródło: Ranking „Dziennika Gazeta Prawna”

- usługi transportu ładunków masowych polegające na przewozie surowców sypkich lub płynnych;
 - usługi transportu całopojazdowego, które polegają na dostarczeniu jednej partii towaru, najczęściej bez specjalistycznych wymogów dotyczących warunków transportu, z punktu A do punktu B;
 - usługi transportu drobnicowego polegające na zebraniu przesyłek od różnych nadawców i przewiezieniu ich między centrami logistycznymi, z których są następnie dystrybuowane do odbiorców pośrednich lub końcowych;
 - usługi transportu specjalnego, które polegają na spedycji i przewozie towarów wymagających specjalnych, niestandardowych warunków przewozu;
 - usługi przewozu morskiego;
 - usługi transportu lotniczego;
 - usługi magazynowe;
 - usługi logistyki kontraktowej, które polegają na organizacji w imieniu klienta całego procesu logistycznego związanego z produkcją i handlem;
 - usługi KEP, czyli przesyłek kurierskich, paczkowych i ekspresowych, polegające na kolekcjonowaniu, przewozie i dystrybucji małych przesyłek, o wadze do 50 kg, w relacjach między firmami, między firmami a konsumentami lub między konsumentami (źródło: Raport „Transport drogowy w Polsce 2021+”).
- Przeważającym na rynku ogólnoeuropejskim typem świadczonych usług jest logistyka kontraktowa, której udział jest szacowany na 40%. Pozostałe rodzaje usług logistycznych zajmują 2–11% rynku, przy zastrzeżeniu autorów *Top 100*, że zebrane dane są

niepełne. Zachowując to samo zastrzeżenie, dodajmy, że na rynku polskim – tak jak na innych rynkach Europy Środkowo-Wschodniej – dominują usługi związane z przewozem towarów.

Usługi magazynowe

Po bardzo intensywnym 2021 r., kiedy popyt netto w branży magazynowej przekroczył rekordową granicę 5,4 mln m², w 2022 r. w analogicznym okresie odnotowano niewielki spadek – 9%. Wciąż jednak utrzymuje się on na wysokim poziomie. To zapotrzebowanie wygenerowały głównie podmioty e-commerce i sektora logistyki. Zainteresowanie powierzchniami na potrzeby magazynowania było tak duże, że również odsetek pustostanów w 2021 r. był rekordowo niski (3,72), jak podano w raporcie firmy doradczej AXI IMMO. Rok później wrócił do poziomu przekraczającego 5%, za co odpowiedzialna jest branża deweloperska, która podążyła za tym perspektywnym trendem. W roku 2021 oddała ok. 2,8 mln m², w 2022 roku – poniżej 4 mln m². Do końca 2022 roku przestrzeń magazynowa na polskim rynku miała osiągnąć łącznie wielkość ok. 30 mln m². Ta powierzchnia jest rozproszona w wielu parkach w całej Polsce, co utrudnia równowagę niedoboru i nadmiaru na najbardziej popularnych rynkach. Jednocześnie zaczyna się specjalizować. Pojawiają się magazyny profilowane pod konkretny typ towarów, takie jak magazyny farmaceutyczne, dla branży motoryzacyjnej czy dla branży mody.

To ożywienie na rynku ma związek z intensywnym poszukiwaniem nowych powierzchni, które mają zabezpieczyć i nieco rozluźnić napięte łańcuchy dostaw, czyli zjawiskiem reshoringu.

» **Najbardziej optymistyczne prognozy dotyczące technologii zakładają, że do 2030 r. koszty transportu drogowego mogłyby zmniejszyć się o 47% głównie dzięki redukcji zatrudnienia.** «



Aż 45% nowego popytu wygenerowali w ubiegłym roku właśnie operatorzy logistyczni poszukujący nowych sposobów gwarancji zatowarowania. Ponadto ceny w polskim sektorze magazynowym są niższe niż w innych krajach Europy, co czyni go konkurencyjnym i pozwala mu się rozwijać. Liczba trwających na tym rynku transakcji i wolumen inwestycji, a także konsekwentny, choć już nie tak gwałtowny jak w ubiegłym roku wzrost cen wynajmowanych powierzchni potwierdzają dobrą koniunkturę. Widmo recesji i coraz wyższe koszty finansowania mogą ją oczywiście skorygować.

Wyzwania branży TSL

Obecnie w branży przewozowej toczą się równolegle procesy obejmujące różne jej obszary. Są to zmiany zarówno wprowadzane ogólnie przez ustawodawcę, jak i wypływające bezpośrednio z potrzeb środowiska. Głównym wyzwaniem nadal pozostaje nadążanie za intensywnymi i szybko zachodzącymi zmianami.

Automatyzacja. Najbardziej optymistyczne prognozy dotyczące technologii zakładają, że do 2030 r. koszty transportu drogowego mogłyby zmniejszyć się o 47% głównie dzięki redukcji zatrudnienia. Czas potrzebny na realizację zleceń skróciłby się o 40%, a samochody ciężarowe byłyby używane przez 78% czasu dostępnego w ciągu doby, podczas gdy obecnie średni wynik w branży w Europie to 29%. Rozpoczynający się okres spowolnienia gospodarczego i zmniejszenia wolumenów w transporcie w połączeniu z rosnącymi kosztami wynagrodzeń, energii i rekordową inflacją zmusi firmy do ostrej optymalizacji kosztów. Przełomową zmianą, jeśli chodzi o produktywność branży, może okazać się wdrożenie autonomicznych pojazdów, co znacząco ograniczy zapotrzebowanie na personel. „Wydłużenie możliwego czasu eksploatacji pojazdów w ciągu doby przełożyłoby się na znaczne oszczędności, ponieważ istniejące zlecenia można by zrealizować przy użyciu mniejszej liczby pojazdów. Zakres redukcji zależałby od kontekstu, ale w przypadku tras długodystansowych prawdopodobne jest ograniczenie potencjału taboru nawet do 50%” – zaznacza w raporcie *Transport drogowy w Polsce 2021+* dr Paweł Trębicki, współzałożyciel i wieloletni przewodniczący Rady TLP. Drugą odnogą tego trendu jest automatyzacja procesów magazynowania (m.in. automatyczne sortery, autonomiczne wózki widłowe, urządzenia mierzące przesyłki), która przyspieszyła w związku z dynamicznym rozwojem e-commerce, niedoborami pracowników, zwłaszcza w pandemii, i rosnącymi kosztami pracy.

Ekologia. Konieczność redukcji emisji spalin należy do poważniejszych wyzwań branży. Jedną z odpowiedzi może być promowanie transportu intermodalnego, który łączy transport drogowy np. z kolejowym. Zmiana nie dokona się jednak momentalnie, wymaga ona bowiem poważnych inwestycji w infrastrukturę, czyli decyzji na poziomach samorządowym i krajowym o budowie terminali przeładunkowych i przygotowaniu infrastruktury kolejowej. Wedle danych GUS w 2021 roku w Polsce znajdowało się 39 aktywnych terminali, z tego cztery obsługiwały przesyłki morze–kolej, morze–droga (terminale morskie), a 35 obsługiwało przesyłki kolej–droga (terminale lądowe). Dla porównania Niemcy, które co prawda są w tej dziedzinie liderem, ale też najistotniejszym kierunkiem transportu z Polski, dysponują 170 terminalami lądowymi. Według wycen PKP Cargo Connect w Polsce na 10 tys. km² znajduje się 1,41 terminali intermodalnych, podczas gdy w Szwecji jest to 2,04, w Czechach 2,79,



na Węgrzech 2,47, w Holandii 4,82, w Niemczech zaś – 5,98. Mniejsze nasycenie od naszego ma Hiszpania, która jednak znajduje się na logistycznych peryferiach.

Drugą – dążenie do budowy taboru zeroemisyjnego, czyli zastąpienie pojazdów spalinowych autami autonomicznymi oraz samochodami ciężarowymi z napędem wodorowym, co także podnosi kwestię infrastruktury do ładowania i tankowania alternatywnymi paliwami. Eksperci prognozują, że klienci coraz częściej będą zwracać uwagę na kwestie ESG, czyli realizację przez przewoźników celów środowiskowych, społecznych i związanych z ładem korporacyjnym. Ze względu na duży koszt wielu z tych rozwiązań jest prawdopodobne, że na utrzymanie wysokich standardów i realizację bardziej skomplikowanych zleceń będą sobie mogli pozwolić tylko najwięksi gracze na rynku.

Kadra. Rynek przewoźniczy zmagą się z niedoborem wykwalifikowanych kierowców, i to mimo relatywnie wysokich wynagrodzeń, które rosną szybciej niż średnie wynagrodzenia w pozostałych branżach. Ten popyt jest spowodowany nadal dobrą koniunkturą w transporcie i logistyce. Mówi się o brakujących 120–150 tys. truckerów w Polsce, ale za mało jest także magazynierów, pracowników fizycznych i specjalistów, a nawet pracowników biurowych. Konkurencja o pracownika między firmami jest silna, a duża rotacja osłabia przedsiębiorstwa i zwiększa ich koszty. Dodatkowo brak kierowców ciężarówek prawdopodobnie będzie się pogłębiał w nadchodzących latach ze względu na przechodzenie na emeryturę kierowców po 50. roku życia, którzy stanowią największą grupę wiekową w tym zawodzie. Młodzi kierowcy nie chcą pracować tak jak ich starsi koledzy, przez wiele dni i tygodni, z dala od domu. Kolejną przeszkodą są trudności w dostępie do nowoczesnego sprzętu, spowodowane ogromnymi opóźnieniami w dostawach na rynku motoryzacyjnym. Przystarzała flota nie zachęca ich do podejmowania zatrudnienia.

Pakiet Mobilności. Ta dyrektywa unijna od 2020 r. wprowadza szereg zmian w funkcjonowaniu całej europejskiej branży transportowej, a poszczególne kraje muszą dostosować ją do swojego prawa. Powstała jako próba regulacji przepisów odnoszących się m.in. do czasu jazdy i odpoczynków kierowców, sposobu delegowania kierowców, sprawiedliwej konkurencji oraz na rzecz poprawy warunków opłacania kierowców, zwłaszcza w krajach o niższej płacy minimalnej. Kolejne jej przepisy będą wdrażane stopniowo do 2026 r., ale wciąż budzi ona wiele kontrowersji wśród przewoźników ze Wschodu i z Zachodu, m.in. z powodu nielogicznych zapisów, takich jak obowiązek powrotu

pojazdów do kraju zarejestrowania co osiem tygodni, nadmierne obciążenie administracją i zbyt skomplikowane przepisy. Konsekwencje wynikające z nowych regulacji okazują się dotkliwe nie tylko dla firm. Także ustawodawca odczuje większe obciążenie chociażby związane z koniecznością zwiększenia liczby kontroli, odkąd licencję na transport muszą posiadać pojazdy od 2,5 ton, a nie – jak dotąd – od 3,5.

Reshoring. Po dekadach outsourcingu i offshoreingu przyszła pora na przekalkulowanie sposobów i miejsc pozyskiwania komponentów do produkcji. To, co było brane za pewnik, czyli niezawodność dostaw z najdalszych zakątków świata, gdzie dotychczas były produkowane materiały bądź produkty, okazało się zawodne. Portal obserwatorgospodarczy.pl podaje, że z tego powodu po pandemii aż 67% globalnych detalistów zmieniło lokalizację zaopatrzenia w komponenty i materiały niezbędne w procesie produkcji. Przeniesienie produkcji bliżej centralnych zakładów lub największych rynków zbytu oraz wynikające z tego skrócenie łańcuchów dostaw było podyktowane potrzebą zagwarantowania ich bezpieczeństwa na wypadek nieprzewidzianych wydarzeń geopolitycznych czy coraz powszechniejszych klęsk żywiołowych. Według najnowszego raportu agencji Reutersa *A Generational Shift in Sourcing* Polska (23,3% wskazań) oraz Niemcy (19,4%) mogą stać się największymi beneficjentami tego trendu. Oba kraje znalazły się na szczycie listy miejsc, do których przedsiębiorstwa planują przeniesienie produkcji komponentów. Wybór padł na nasz kraj ze względu na jego strategiczne położenie w Europie, łatwy dostęp do innych rynków strefy Schengen i UE, względną stabilność geopolityczną, coraz lepszą infrastrukturę oraz zasób siły roboczej. Na trzecim miejscu, z wynikiem 12%, znalazła się Turcja.

Podsumowanie

Polska ze względu na swoje położenie geograficzne jest bardzo istotnym punktem na mapie europejskiego transportu. Dzięki intensywnemu rozwojowi branży przez ostatnie 30 lat nasz kraj można uznać za lidera na europejskim rynku przewozów drogowych. Wszystkie dane wskazują na znaczny rozwój i wzrost przychodów w ostatnich latach, i to mimo niedoborów, m.in. kadrowych, infrastrukturalnych, technologicznych. Czy ten wznoszący trend się utrzyma, będzie zależał m.in. od tego, czy uda się wyważyć proporcje między gwałtownie rosnącym zapotrzebowaniem na nowe rynki produkcji i magazynowania, rozwojem infrastruktury do tego koniecznej i poziomem kosztów świadczenia takich usług, a także między popytem i podażą kierowców a wdrażaniem nowoczesnych technologii służących do automatyzacji procesów. ●

» Polska oraz Niemcy mogą stać się największymi beneficjentami reshoringu. Oba kraje znalazły się na szczycie listy miejsc, do których przedsiębiorstwa planują przeniesienie produkcji komponentów. «

PRZYPISY

- 1 Bank Danych Makroekonomicznych GUS; <https://bdm.stat.gov.pl/> (dostęp: 13.01.2023).
- 2 Raport *Transport drogowy w Polsce 2021+*.
- 3 <https://logistyka.rp.pl/szynowy/art37355181-nadchodzi-wysyp-terminali-intermodalnych> (dostęp: 17.01.2023).



głos branży

Polska jest jednym z największych europejskich dostawców usług transportowych i logistycznych. Ta gałąź gospodarki wnosi istotny wkład do polskiego PKB. Ale jak każda inna boryka się z wieloma trudnościami, m.in. związanymi z zapewnieniem bezpieczeństwa dostaw. O tym, jak firmy radzą sobie z tym wyzwaniem, mówią eksperci branży security.



Andrzej Żochowski

NIEZALEŻNY EKSPERT
DS. BEZPIECZEŃSTWA

Negatywne skutki wojny w Ukrainie

Ostatnie lata przyniosły wydarzenia, które w ogromnym stopniu zaczęły oddziaływać na biznes, m.in. na sektor logistyki. Jak nie trudno się domysleć, były to pandemia COVID-19 i wojna w Ukrainie. Pandemia znacząco wpłynęła na środki bezpieczeństwa i zmiany w systemie bezpieczeństwa w branży logistyki, jednak można uznać, że nie zagraża już łańcuchowi dostaw.

Natomiast konflikt zbrojny rozpoczął nową fazę zmian, które będą miały dalsze konsekwencje związane z nowymi wyzwaniami dla łańcucha dostaw. Toczące się nieprzerwanie działania wojenne spowodują jeszcze większy odpływ pracowników z Ukrainy (szczególnie mężczyzn), którzy będą wyjeżdżać do swojego kraju, aby walczyć z Rosją. Jest to o tyle bolesne, że często były to sprawdzone, zaufane osoby.

Można się także spodziewać, że skoro Polska, kraje Unii Europejskiej oraz USA są zaangażowane w dostarczanie sprzętu wojskowego dla Ukrainy, to uczestniczące w tym łańcuchu dostaw międzynarodowe firmy logistyczne i kurierskie będą atakowane przez hakerów pracujących na rzecz Federacji Rosyjskiej. Ataki hakerskie

to stały element prowadzonej przez Rosję tzw. wojny hybrydowej, której celem jest zdestabilizowanie międzynarodowego łańcucha dostaw i utrudnianie zaopatrzenia armii ukraińskiej.

Dla firm z branży TSL odczuwalnym skutkiem konfliktu zbrojnego jest „wycięcie ze światowego łańcucha dostaw” Rosji i Białorusi. Sytuacja ta negatywnie wpływa na rentowność i ma ogromny wpływ na sektor logistyki, gdyż zarówno Rosja, jak i Białoruś stanowiły tradycyjnie olbrzymi rynek zbytu, a towary dostarczane były m.in. przez polskie firmy transportowe. Już w 2022 roku spowodowało to konieczność cięcia kosztów w logistyce i szukanie oszczędności, np. za pomocą ograniczenia wydatków na systemy bezpieczeństwa. Można przypuszczać, że poskutkuje to jeszcze większą skalą rezygnacji z tzw. ochrony fizycznej na rzecz zastępowania jej elektronicznymi systemami bezpieczeństwa (systemy kontroli dostępu, CCTV oraz systemy sygnalizacji włamania i napadu).

Ochrona fizyczna będzie eliminowana jeszcze bardziej, niż miało to miejsce w ostatnich latach. Najprawdopodobniej zwiększy się także liczba podmiotów, które będą korzystać z audytów bezpieczeństwa firm zewnętrznych. Ich celem będzie głównie redukcja strat oraz optymalizacja kosztów ogólnie pojętego bezpieczeństwa w organizacjach.



Paweł Pęchorzewski

ZALANDO LOGISTICS OPERATIONS
POLSKA

Rosnąca skala przestępczości

W ostatnich latach branża logistyczna nieustannie mierzy się z poważnymi wyzwaniami. Pandemia, zakłócone łańcuchy dostaw, niedobory pracowników, zmniejszająca się podaż powierzchni ładunkowych, inflacja i związane z nią spowolnienie gospodarcze. To wszystko zagadnienia, które organizacje – nie tylko logistyczne – uwzględniają w swoich planach strategicznych, operacyjnych, a także planach ciągłości działania.

Jest jednak coś, co może w 2023 roku stanowić trudność przede wszystkim w sektorze logistyki i transportu. Mowa o rosnącej skali przestępczości wycelowanej w transport towarów.

Według danych i prognoz udostępnianych przez organizację branżową TAPA EMEA coraz większym zagrożeniem są zorganizowane grupy przestępcze trudniące się kradzieżami różnego rodzaju dóbr w trakcie ich przewozu. Ich działalność jest widoczna szczególnie w krajach zachodniej Europy, gdzie tylko pomiędzy styczniem 2021 a czerwcem 2022 odnotowano prawie 6,5 tysiąca incydentów.

Warto zwrócić uwagę, że liczby te obejmują wyłącznie zdarzenia wykryte, odpowiednio sklasyfikowane i zgłoszone TAPA EMEA, a Polska nie znajduje się na liście 10 krajów z najwyższą liczbą incydentów. Nie oznacza to jednak, że problem tutaj nie istnieje, ponieważ również polskie organy ścigania raz na jakiś czas ogłaszają rozbicie tego typu zorganizowanych grup. Trudno

przy tym oczekiwać trwałego rozwiązania, dlatego niezbędne jest położenie jeszcze większego niż wcześniej nacisku na prewencję. Jest ona bardzo ważna w firmach, których sieć logistyczna jest mocno rozproszona i których klienci codziennie otrzymują setki tysięcy zamówień w wielu krajach. Tutaj każde zakłócenie może odbić się na satysfakcji klienta, wizerunku organizacji, a w rezultacie potencjalnie skutkować dalszymi konsekwencjami.

W związku z powyższym należy spodziewać się, że w bieżącym roku działy bezpieczeństwa i zapobiegania stratom firm z branży szeroko rozumianej logistyki będą aktywnie poszukiwać dodatkowych rozwiązań pozwalających nie tylko skutecznie realizować działania zapobiegawcze, ale także umożliwiających w razie potrzeby szybką reakcję na zdarzenia niepożądane i wspomagających efektywne postępowania wyjaśniające.



Adam Sawicki

DSV INTERNATIONAL SHARED
SERVICES

Podniesienie jakości usług

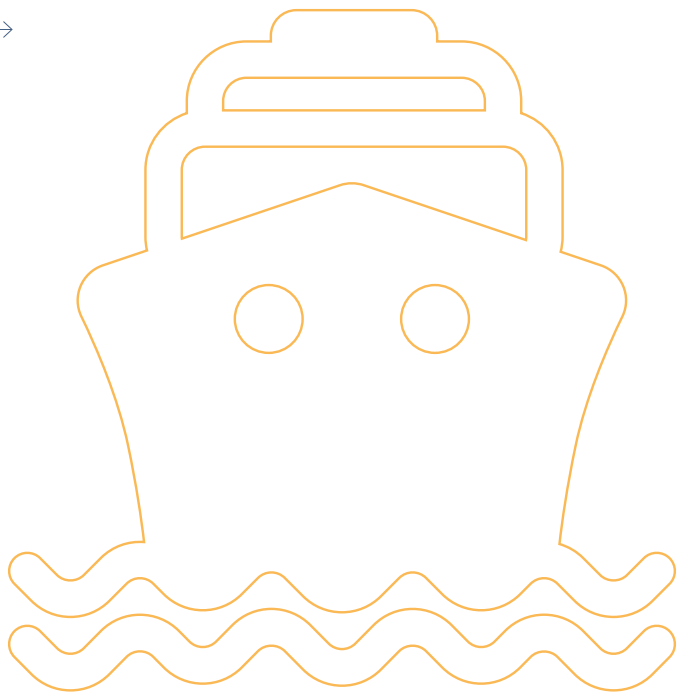
Ubiegły rok był przełomowy dla firm z branży szeroko rozumianego bezpieczeństwa. Podnoszący się po okresie pandemii rynek był rozchwiany, co wiązało się z dodatkowym ryzykiem podczas podejmowania strategicznych decyzji biznesowych. Ponadto był to rok pełen wyzwań nie tylko z uwagi na zwiększone zapotrzebowanie na produkty branży security, ale również na wciąż niestabilną sytuację geopolityczną.

Zaburzone łańcuchy dostaw przy jednocześnie krótkich terminach realizacji projektów wymusiły na globalnych firmach logistycznych zmianę podejścia. Mam tu głównie na myśli zabezpieczenie potrzeb biznesowych poprzez dostosowanie realizacji inwestycji do zmieniających się warunków na rynku zabezpieczeń.

Dojrzałość security menedżerów firm sektora TSL nabrała nowego znaczenia. Coraz częściej muszą oni podejmować większe niż dotychczas ryzyko, aby sprostać wyzwaniom rynku i postawionym przed nimi zadaniom. Większa świadomość security i logistic menedżerów oraz zacieśnienie współpracy z departamentami IT przyniosło oczekiwane rezultaty w postaci podniesienia jakości świadczonych usług przy jednoczesnej optymalizacji kosztów. Inwestycja w specjalistów IT wydaje się właściwym kierunkiem.

W nowoczesnych, w pełni zautomatyzowanych centrach logistycznych coraz częściej wprowadzane są rozwiązania chmurowe. Kluczowa jest umiejętność konfiguracji systemów w celu pełnego zaspokojenia potrzeb biznesowych. Wdrażanie odpowiednich procedur, a następnie prawidłowe działanie, reagowanie na zdarzenia zgodnie z wytycznymi z pewnością jeszcze bardziej podniesie i tak już bardzo wysoko postawioną poprzeczkę.

Podsumowując, dla branży TSL najbliższy czas będzie bardzo intensywny z punktu widzenia nowych inwestycji, co z pewnością zaowocuje projektami na szeroką skalę.



Wojciech Andziak
DHL PARCEL

Czeka nas dużo wyzwań

Dużym wyzwaniem związanym z bezpieczeństwem transportu i logistyki jest maksymalne wykorzystanie dostępnych narzędzi monitorujących nie tylko pojazd, ale także cały łańcuch dostaw. Wobec wzrostu kosztów automatyzowanie zadań dotychczas wykonywanych przez pracowników ochrony jest nie tylko jednym z rozwiązań, ale koniecznością. Innymi elementami wpływającymi na bezpieczeństwo przewożonych przesyłek są jakość i spójność danych dostarczanych przez klientów.



Daniel Kamiński
SMART-I

Rola awizacji w obsłudze parkingu buforowego

Coraz częściej widzimy sznury ciężarówek oczekujących na rozładunek w centrach dystrybucji. Czemu tak się dzieje? COVID-19 spopularyzował zakupy online. To spowodowało lawinowy wzrost

liczby centrów logistycznych, a wraz ze wzrostem liczby zakupów wzrosła liczba aut przewożących przesyłki.

Odpowiedzią na problem z samochodami blokującymi pobożę w oczekiwaniu na rozładunek może być zastosowanie parkingów buforowych. Pewnym rozwiązaniem jest skierowanie takich samochodów na plac rozładunkowy, ale to niweluje jeden problem, generuje zaś kolejne. Wśród kierowców dochodzi do nieporozumień związanych z kolejnością wjazdu, przepychanek, kolizji, a nawet kradzieży.

Lepszym pomysłem jest więc uruchomienie bezpiecznego i inteligentnego parkingu buforowego, ogrodzonego, oświetlonego i ułatwiającego zaplanowanie obsługi oczekujących na rozładunek aut. To ostatnie umożliwia system awizacji aut, który polega na tym, że przewoźnicy przez stronę internetową zgłaszają transport, podając numer rejestracyjny pojazdu oraz telefon kontaktowy kierowcy. Dzięki temu obsługa magazynu może przygotować się do dostawy i wskazać planowany czas rozładunku.

Zarejestrowany pojazd jest automatycznie wpuszczany na parking, za co odpowiada system rozpoznawania tablic rejestracyjnych, a obsługa jest powiadamiana, że dostawa dotarła i znajduje się na parkingu buforowym. Po przygotowaniu strefy rozładunkowej kierowca zostanie powiadomiony telefonicznie lub przez SMS, do której rampy ma podjechać. Szlaban wyjazdowy otworzy się wyłącznie dla kierowcy, który ma przypisany dok rozładunkowy. Kierowca chcący ominąć system trafi na koniec kolejki.

Zastosowanie kamer pozwala monitorować cały teren i w przypadku kolizji ułatwi wskazanie osoby odpowiedzialnej. Urządzenia odpowiedzialne za ochronę granic parkingu wysyłają do kierowców ostrzeżenia o próbie ich nieautoryzowanego przekroczenia. To sposób na większe bezpieczeństwo ładunku znajdującego się na pojazdach. W przypadku tak zorganizowanego parkingu buforowego jedynym wymaganiem jest doprowadzenie energii, by opisane systemy mogły działać.



Marcin Walczuk
BCS

Automatyzacja w sektorze logistycznym

Szybkość i precyzja działania w wielu obszarach gospodarki mogą stanowić kluczowy element odpowiadający za to, czy firma odniesie sukces, czy porażkę. Taki sposób działania jest niezbędny na wszystkich poziomach, począwszy od produkcji, przez pakowanie i załadunek, skończywszy na transporcie, tym bardziej że w branży transportowej nawet niewielkie opóźnienia w dostawach mogą powodować wielomilionowe straty.

Autorska aplikacja BCS Manager współpracująca z kamerami do rozpoznawania tablic rejestracyjnych BCS Line pomaga przyspieszyć transport towarów. Automatyzacja procesu wjazdu i wjazdu pojazdów, np. z parku logistycznego czy innego obiektu,

gdzie wymagana jest szczegółowa ewidencja ruchu, pozwala oszczędzić cenny czas. Wykorzystanie do tego celu aplikacji BCS Manager i kamer ITC jest proste, a co ważniejsze, znacznie ułatwia obsługę całego systemu.

Funkcje oferowane przez aplikację BCS Manager usprawniają pracę operatora systemu. Ma on wówczas możliwość edycji list tablic rejestracyjnych bezpośrednio z poziomu aplikacji, generowania raportów o zdarzeniach (wjazdach/wyjazdach) oraz ich wyszukiwania według numeru tablicy rejestracyjnej lub właściciela pojazdu.

Dzięki aplikacji BCS Manager można zapobiegać oszustwom polegającym na podmianie tablic rejestracyjnych. Jeśli numer nie będzie się zgadzał ze wzorem pojazdu, uruchomi się alarm. Ponadto połączenie kamer ITC z kamerami dozоровymi wysokiej rozdzielczości oraz BCS Managera pozwala na utworzenie stanowiska kontroli pojazdów służącego do sprawdzania uszkodzeń, do jakich dochodzi podczas załadunku i rozładunku towarów.

Wspomniane funkcje wraz z podstawowymi zaletami aplikacji BCS Manager stanowią idealne rozwiązanie do monitorowania centrów logistycznych i baz przeładunkowych.



Bogumił Szymanek
AXIS COMMUNICATIONS

Zapewnienie bezpieczeństwa w transporcie publicznym

Zapewnienie sprawności działania i ograniczenie zakłóceń w realizacji usług to najważniejsze cele systemów przeznaczonych do obiektów transportu publicznego. Dworce, lotniska czy linie metra muszą dysponować narzędziami pozwalającymi na błyskawiczną reakcję i wdrożenie procedur zapewniających ciągłość pracy. Wszyscy użytkownicy takich obiektów oczekują, że ich problemy zostaną rozwiązane sprawnie i na czas. Każde opóźnienie albo zmiana w transporcie publicznym wpływa na życie i pracę wielu osób i często odbija się na wizerunku dostawcy usług.

Z perspektywy systemów zabezpieczeń kluczowe jest więc ograniczenie incydentów związanych z naruszeniem bezpieczeństwa krytycznych elementów obiektu oraz zapewnienie wysokiego poczucia bezpieczeństwa osobom z nich korzystającym. Natychmiastowe wykrywanie zagrożeń jest niezbędne, gdyż obiekty tego typu obsługują każdego dnia rzesze ludzi chcących bezpiecznie i komfortowo podróżować. Ów komfort związany jest również z dostępem pasażerów do wielu dodatkowych usług czy sklepów. Również w tym zakresie możliwe jest wdrożenie rozwiązań optymalizujących dostęp i zwiększających efektywność działania.

Podstawowym narzędziem dozoru są niezawodne kamery, które oprócz szczegółowego obrazu pozwalają automatycznie wykrywać zagrożenia, szczególnie, jeśli są zintegrowane z innymi

systemami. Dzięki temu możliwe jest m.in. wykrycie wejścia osoby nieuprawnionej do przebywania w jakiejś przestrzeni, dostrzeżenie pozostawionego bez nadzoru bagażu, określenie poziomu zatłoczenia lub zauważenie dymu mogącego być sygnałem pożaru. System pozwala operatorowi na weryfikację zdarzenia i podjęcie odpowiednich działań. Ponadto materiał wizyjny zawierający opis obiektów (metadane) usprawnia szybkie wyszukiwanie zdarzeń.

Zastosowanie sieciowych rozwiązań audio IP daje możliwość przeciwdziałania poprzez automatyczne komunikaty czy połączenie głosowe, bez konieczności fizycznej obecności pracownika obsługi czy ochrony. Te same urządzenia mogą stanowić również elementy systemu informacji pasażerskiej. Decydując się na wybór konkretnej technologii, należy też rozważyć kwestię cyberbezpieczeństwa oraz to, czy i jak długo dostawca zapewnia wsparcie techniczne i gwarancje. Ze względu na to, że infrastruktura transportu publicznego wciąż się zmienia i rozwija, wybór musi uwzględniać przyszłe możliwości rozbudowy, integracji czy nowe potrzeby.



Jakub Dybalski
ZARZĄD DRÓG MIEJSKICH
W WARSZAWIE

Bezpieczeństwo pieszych

W warszawskim Zarządzie Dróg Miejskich przez bezpieczeństwo transportu rozumiemy przede wszystkim możliwość swobodnego i bezpiecznego korzystania z ulic przez wszystkich użytkowników. Szczególną wagę przykładamy do bezpieczeństwa niechronionych uczestników ruchu drogowego, a więc w pierwszej kolejności pieszych. Takie podejście nie wydaje się tradycyjnym zadaniem zarządcy dróg, ale dla nas jest oczywiste. Dlatego w latach 2016–2020 przeprowadziliśmy w Warszawie kompleksowy audyt przejść dla pieszych bez sygnalizacji, który był niezbędny, by doprowadzić do poprawy bezpieczeństwa osób wkraczających na jezdnię. Audyt był przedsięwzięciem unikatowym, za które Warszawa w zeszłym roku została uhonorowana przez Komisję Europejską nominacją do nagrody *Urban Road Safety Award*. Wybrani w przetargach zewnętrzni audytorzy ocenili bezpieczeństwo 4093 przejść dla pieszych, którymi administruje ZDM, biorąc pod uwagę ok. 30 kryteriów. Dla każdego przejścia z osobna wskazywali potencjalne zagrożenia i propozycje poprawy bezpieczeństwa, każdemu przyznali ocenę w skali od 0 do 5.

Audyt jest w Warszawie podstawą do sukcesywnej przebudowy kolejnych przejść. Po pierwsze, ułatwia decyzję o kolejności interwencji, wskazując, które z nich wymagają najpilniejszej zmiany, zostały bowiem najgorzej ocenione. Po drugie, jest źródłem informacji o tym, co należy poprawić. Zyskaliśmy więc wiedzę, która pozwala nam sensownie planować działania, a jednocześnie daje nam konkretne argumenty pozwalające stawić czoło grupom lobującym za takim czy innym rozwiązaniem, niekoniecznie najlepszym dla bezpieczeństwa pieszych.

Konsekwencją audytu jest zatem sukcesywne wprowadzanie zmian w przejściach, tak by były one bezpieczniejsze dla pieszych. Efekty już są widoczne. Z roku na rok maleje w stolicy liczba wypadków na zebrawkach oraz liczba śmiertelnych ofiar wypadków wśród pieszych. Odkąd ruszyliśmy z przebudowami w efekcie audytu, spadła ponaddwukrotnie.



Krzysztof Kunecki

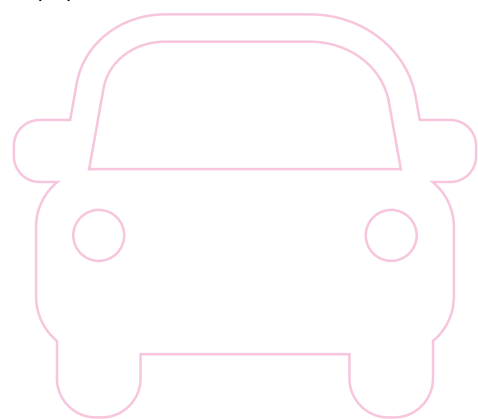
SCHRACK SECONET

Kluczowe jest wczesne wykrycie pożaru

Obiekty, takie jak dworce autobusowe, kolejowe, lotniska czy linie i stacje metra charakteryzują się tym, że może w nich przebywać jednocześnie wiele ludzi niebędących ich stałymi użytkownikami. To istotny czynnik wpływający na wdrożenie odpowiedniej koncepcji bezpieczeństwa pożarowego w celu zapewnienia bezpiecznej ewakuacji osób w przypadku alarmu pożarowego.

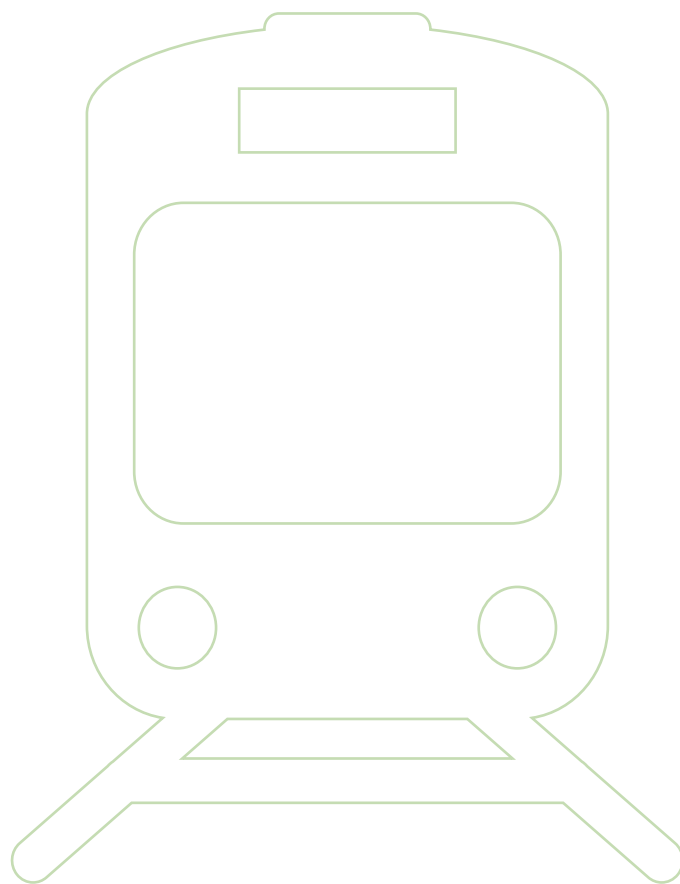
Ochrona przeciwpożarowa bardzo różnicowanych pod względem ryzyka wystąpienia pożaru obiektów, realizujących najczęściej dodatkowo również funkcje gastronomiczne, handlowe czy hotelowe jest wyzwaniem dla projektantów systemów i urządzeń ppoż. Skupiając się na aktywnych systemach bezpieczeństwa pożarowego, należy tak dobrać urządzenia, by charakteryzowały się dużą elastycznością i funkcjonalnością pozwalającą na zbudowanie zintegrowanego systemu bezpieczeństwa pożarowego.

Kluczowym zadaniem takiego systemu jest wykrycie pożaru w jego najwcześniejszym stadium. Im wcześniej zostanie wykryte zagrożenie, tym łatwiej przeprowadzić szybką i bezpieczną ewakuację. Skuteczność i elastyczność w zakresie detekcji pożaru zapewnia zastosowanie m.in. punktowych czujek wielosensorycznych dymu, ciepła oraz CO z dodatkową możliwością interaktywnego współdziałania czujników pozwalających na wykrycie przez system sygnalizacji pożarowej różnych rodzajów pożaru (np. tlewnych lub płomieniowych) i wygenerowanie sygnału pożarowego z jednoczesnym maksymalnym ograniczeniem ewentualnych fałszywych alarmów.



Ponadto we wspomnianych na początku obiektach ze względu na wymóg ochrony pomieszczeń, np. o wielkiej kubaturze czy trudnych warunkach otoczenia (tunele), powszechnie stosowane są rozwiązania specjalne detekcji pożaru, do których należą np. czujki liniowe dymu, czujki zasysające dymu, czujki liniowe ciepła czy czujki płomienia. Dostępne są również rozwiązania, w których czujki płomienia są dodatkowo wyposażone w kamerę, co pozwala na zdalną wstępną weryfikację zagrożenia.

Wsparciem dla operatorów i zarządców obiektów są systemy integrujące urządzenia przeciwpożarowe, które umożliwiają np. szybkie wyświetlenie mapy z informacją o miejscu, w którym został wykryty alarm wraz ze szczegółowymi informacjami dotyczącymi np. temperatury czy stężenia dymu. Taki system może wspomagać operatora poprzez wyświetlenie odpowiednich instrukcji postępowania oraz nadzorować skuteczność uruchomienia urządzeń automatyki pożarowej, zgodnie ze scenariuszem pożarowym. Ponadto w przypadku integracji z czujkami specjalnymi lub innymi systemami bezpieczeństwa, takimi jak system nadzoru wizyjnego, operator może korzystać z obrazów pochodzących z kamer nadzorujących obszar zagrożenia oraz drogi ewakuacyjne, co ułatwia podjęcie bez zbędnej zwłoki wymaganych działań, np. zdecydowanie o szybszym wezwaniu straży pożarnej i uruchomieniu procedury ewakuacji. Operator systemu może również ręcznie uruchomić procedurę alarmową i ewakuację w przypadku wykrytego przez niego zagrożenia pożarowego czy innych zdarzeń kryzysowych w obiekcie. ●



Bezpieczeństwo łańcucha dostaw w czasach VUCA jest szczególnie ważne



Ostatnie trzy lata były bardzo trudne dla biznesu, szczególnie w zakresie utrzymania łańcucha dostaw. COVID, blokada Kanału Sueskiego, inflacja i wojna w Ukrainie to kumulacja problemów największa od dziesięcioleci. Żyjemy w podręcznikowych warunkach VUCA. Termin ten wprowadziła amerykańska uczelnia wojskowa United States Army War College na określenie niestabilnej sytuacji. Oznacza ono: *volatility* (zmienność), *uncertainty* (niepewność), *complexity* (złożoność), *ambiguity* (niejednoznaczność).

W ostatnim raporcie TAPA za 2021 r. wskazano wzrost wartościowy i procentowy kradzieży w każdej kategorii produktowej. Już nie tylko dobra tradycyjne, takie jak elektronika, wyroby tytoniowe czy farmaceutyki są atrakcyjne dla przestępców. Lista stale się wydłuża. Zaczyna być zauważalny trend swojego „piractwa” towarów trudno dostępnych niezbędnych do produkcji.

W regionie EMEA liczba incydentów związanych z przestępstwami ładunkowymi w 2021 r. wzrosła o 29,8% w stosunku do roku poprzedniego (raport za rok 2022 nie został jeszcze opublikowany). Z pewnością dane, jakie się w nim znajdują, będą jeszcze bardziej alarmujące. Jak zabezpieczyć się przed konsekwencjami takich incydentów? Jak zapewnić lub choć zminimalizować prawdopodobieństwo strat wynikających z kradzieży przewożonych

towarów? Odpowiedź wydaje się oczywista – współpracować z partnerem logistycznym oferującym najwyższy poziom przygotowania własnych procesów i zasobów.

Takim partnerem z pewnością jest DHL Supply Chain, który działa zgodnie z rekomendacjami wykonawców certyfikowanych



w TAPA. Praktyka pokazuje, że klienci przychodzą z własnymi standardami korporacyjnymi, które należy zintegrować z globalnymi i regionalnymi standardami bezpieczeństwa. DHL, mając doświadczony multidyscyplinarny zespół projektowy, dostosowuje rozwiązania do tych potrzeb.

Wdrażanie projektu obsługi klienta DHL zaczyna od współpracy z wyselekcjonowanymi partnerami oraz technicznego dostosowania pojazdów i naczep do wymogów certyfikacji. Następnie weryfikuje i szkoli kierowców, organizuje ścisłą kontrolę przebiegu trasy, łącznie z jej śledzeniem w Centrach Monitoringu GPS i Control Tower, wprowadza ciągłe zarządzanie oraz zabezpieczenia cybersecurity. Wymienione narzędzia techniczne uzupełnione wskazaniem bezpiecznych korytarzy transportowych i sieci audytowanych na rzecz projektu parkingów powodują, że system jest kompleksowy. Tak skonstruowany proces redukuje ryzyko, a jednocześnie znacznie wzmacnia łańcuch dostaw klienta DHL.

Wdrożona przez DHL Supply Chain metodologia High Value Transportation świetnie wpisuje się w oczekiwania klientów. Bez względu na to, czy wymogiem są standardy TAPA, czy korporacyjne, technologia i realizacja projektu zapewniają bezpieczeństwo oraz pozwalają na pozyskanie wielu danych operacyjnych przydatnych klientom do prowadzenia biznesu. W zależności od potrzeb klienta dane dotyczące transportu mogą być gromadzone w czasie rzeczywistym i w odniesieniu do dowolnego okresu.

Działy transportu i bezpieczeństwa DHL dążą do stanu, w którym kierowca może się skupić na bezpiecznym przejechaniu trasy bez martwienia się o kradzież ładunku. Jednocześnie kierowca nie ma dostępu do towaru.

Za intensywny rozwój projektu High Value Transportation odpowiadają nasi pracownicy certyfikowani przez TAPA, mający szereg certyfikatów bezpieczeństwa i jakości, a co najważniejsze doświadczeni w realizacji wymagających kontraktów. ●

DHL Supply Chain
ul. Komitetu Obrony Robotników 45 D
02-146 Warszawa
www.dhl.com

PRZYPISY

1 TAPA – Stowarzyszenie Ochrony Transportowanego Mienia (Transported Asset Protection Association) to działająca od 1997 r. międzynarodowa organizacja zajmująca się szeroko pojętym bezpieczeństwem dostaw.

Firmy rodzinne w transporcie drogowym

W niewielu dziedzinach gospodarki polskie przedsiębiorstwa odniosły tak spektakularny międzynarodowy sukces, jak w przypadku transportu drogowego. Polska jest dziś liderem na europejskim rynku przewozów drogowych.

Jacek Tyburek

W minionej dekadzie branża transportowa, wyceniana na ponad 190 mld zł, rosła w rekordowym tempie 10% rocznie – wynika z raportu *Transport drogowy w Polsce 2021+* opracowanego przez SpotData na zlecenie związku pracodawców „Transport i Logistyka Polska” i przy jego merytorycznej współpracy. Na naszym rynku działa 125 tys. firm zajmujących się transportem drogowym towarów, zatrudniających około milion osób. Przedsiębiorstwa te przewożą 85% polskich towarów eksportowych i odprowadzają ponad 16 mld zł podatków do budżetu państwa i samorządów.

Transport drogowy towarów jest jedną z trzech największych branż polskiej gospodarki. Bezpośredni udział sektora transportu i magazynowania w polskim PKB wynosi 6%, jednak jego znaczenie dla gospodarki jest znacznie większe. Bez transportu inne branże nie mogłyby funkcjonować, zwłaszcza handel i przemysł. Polskie przedsiębiorstwa transportowe wnoszą ogromny wkład nie tylko w polską, ale także w europejską gospodarkę.

Polski transport jest potęgą

W 2008 r. polskie firmy przewiozły 8% wszystkich towarów transportowanych z Niemiec do Francji, w roku 2020 było to już 25%.

Obecnie więcej polskich niż francuskich kierowców dostarcza nad Sekwanę towary niemieckie.

Polski transport zdominował cały europejski rynek, będąc jednocześnie podstawą ekonomicznego krwioobiegu pomiędzy Europą a Azją. Ostatnie lata nie były łatwe dla branży, problemy przyniosły choćby Pakiet Mobilności, pandemia czy ostatnio wojna w Ukrainie i drastycznie rosnące ceny paliw. Transport, po latach prosperity, stanął w obliczu poważnego hamowania koniunktury z jednej strony, z drugiej – stał się ofiarą dynamiki własnego rozwoju. Blisko 80% firm transportowych w Polsce ma dziś trudności z prowadzeniem działalności. Właściciele firm transportowych borykają się bowiem z wieloma problemami mającymi bezpośredni wpływ na ich kondycję, przede wszystkim z niedostateczną liczbą kierowców gotowych do podjęcia pracy.

Od kilku lat w Polsce kierowcy znajdują się w pierwszej trójce najczęściej poszukiwanych pracowników. Jedną z przyczyn takiej sytuacji jest wysoki koszt zdobycia uprawnień do prowadzenia samochodów ciężarowych. Dużym utrudnieniem jest niepewność wynikająca z licznych zmian przepisów w kraju i Europie. Jako przykład mogą posłużyć uregulowania w kwestiach wynagrodzenia minimalnego wprowadzone w krajach unijnych. Stawki płacy

minimalnej dla pracowników delegowanych do Austrii, Niemiec czy Francji są naliczane w niejednakowy sposób, a także różnią się pod względem listy składników wynagrodzenia.

Polski transport rodzinny

Polskie firmy transportowe to przedsiębiorstwa dysponujące zarówno jednym lub dwoma pojazdami, jak i te mające ich 100, 500 czy nawet 1000. Przez ostatnich kilka miesięcy w zespole projektowym DHL badaliśmy potencjał różnych firm transportowych realizujących transporty towarów wysokiej wartości (*High Value Goods*; HVG). Zdecydowaną większość stanowiły klasyczne firmy rodzinne. Ich historia założycielska prawie zawsze była taka sama. W czasie przemian systemowych w Polsce „ojcowie założyciele”, nierzadko wraz z innymi członkami najbliższej rodziny, zakładali firmy transportowe, dysponując zaledwie jednym pojazdem. Biznes był stosunkowo łatwy, a zapotrzebowanie ogromne. Po 30 latach mamy na rynku firmy potężne, świetnie zorganizowane i, co ciekawe, ich pozycja bazuje na wiarygodności oraz dobrej opinii bezpiecznego i niezawodnego dostawcy usług.

Patrząc na rozwój jakościowy i ilościowy największych transportowych firm rodzinnych, można zauważyć, że każda przez

» Na naszym rynku działa 125 tys. firm zajmujących się transportem drogowym towarów, zatrudniających około miliona osób. Przedsiębiorstwa te przewożą 85% polskich towarów eksportowych i odprowadzają ponad 16 mld zł podatków do budżetu państwa i samorządów. «

lata znalazła swoją specjalność, która dała podwaliny pod strategię rozwoju. Specjalizacje poniekąd wymusiły wdrażanie szeregu certyfikowanych standardów jakości zapewniających jednocześnie określony poziom bezpieczeństwa świadczonych usług.

Jednym z takich uprawnień jest status zarejestrowanego agenta, uznanego lub znanego nadawcy. Przekłada się to na konkretne korzyści, zarówno dla klienta, który wysyła międzynarodowe przesyłki, jak i dla przedsiębiorstwa. Certyfikat zarejestrowanego agenta wspiera efektywną organizację procesu transportowego towarów na każdym jego etapie. Wszystkie ładunki lotnicze, które pochodzą od podmiotów zapewniających integralność ochrony w bezpiecznym łańcuchu dostaw – uznanego nadawcy, znanego nadawcy lub zarejestrowanego agenta – są zwolnione z kontroli bezpieczeństwa.

Wśród badanych znalazły się firmy, którym przyznano certyfikat WCA. World Cargo Alliance jest globalną organizacją zrzeszającą niezależnych spedytorów, czyli ponad 9 tys. jednostek w 193 krajach na świecie. Natomiast dysponowanie certyfikatem TAPA TSR było kluczem, wg którego sprawdzaliśmy potencjały firm. Ten najbardziej rozpoznawalny standard jest jednocześnie praktycznym narzędziem selekcji firm, którym klienci są gotowi powierzyć uczestnictwo w swoich łańcuchach dostaw.

Z kolei uzyskanie specjalistycznego certyfikatu GDP stanowi dla klientów dodatkową gwarancję niezawodności przewozu produktów farmaceutycznych. Przemysł farmaceutyczny ma specyficzne wymagania dotyczące transportu wynikające z potrzeb produktu i bezpieczeństwa jego transportu. To jedno z kluczowych produktów zaliczanych do dóbr wysokiej wartości (HVG). Obraz uzupełniają certyfikaty AEO oraz Wewnętrzny System Kontroli (WSK) – regulacje, które dotyczą zasad obrotu i transportu towarami militarnymi oraz wyrobami podwójnego zastosowania o znaczeniu strategicznym.

Największe i najlepiej rozwinięte rodzinne firmy transportowe swój poziom rozwoju i zasięg zawdzięczają właśnie inwestycjom w bezpieczeństwo. Flota pojazdów najwyższej jakości oraz standardowe procedury zatrudniania kierowców, kontroli jakości ich pracy, kontroli nad przebiegiem tras, niwelowania ryzyka – wszystkie z tych firm posiadały własne rozwinięte procesy kontroli warunków bezpieczeństwa realizowanych usług.

Inwestycja w bezpieczeństwo to nie jest koszt

Rodzinne firmy transportowe, które swój potencjał rozwinęły tak bardzo, że współpracują z największymi firmami branży TSL oraz bezpośrednio z działami transportu korporacji międzynarodowych, znalazły się na obecnym etapie rozwoju z bardzo prostej przyczyny. Rozwój zawdzięczają współpracy od początku z gigantami branży TSL, takimi jak DHL, oraz konsekwentnemu inwestowaniu w bezpieczeństwo.

Otrzymanie zlecenia na realizację transportów wysokomarżowych oznacza konieczność dostosowania się do jednego, choć

często i kilku standardów bezpieczeństwa. Zaczyna się od standardów operatora logistycznego, który jest pierwszym ogniwem po zleceniu nadawcy. DHL, i podobne mu rozmiarem firmy, opracował własne zestawy wymagań z zakresu bezpieczeństwa. Często nakładają się na nie wymagania klienta, który w zależności od towaru ma własne standardy korporacyjne. Coraz częściej strony transakcji poruszają się w ramach zasad opisanych w TAPA TSR i TAPA FSR. Wtedy wiadomo, że przewoźnik nie oferujący odpowiedniego poziomu bezpieczeństwa nie ma szans na otrzymanie zlecenia.

Rosnąca przestępczość cargo

Skąd pewność, że standardy nie będą obniżane, a wręcz przeciwnie, że będą coraz poważniej traktowane? Wskazują na to wyniki raportu *TAPA 18 months of cargo crime Europe, Middle East & Africa Region. Reporting period to 30 June 2022*.

Wzrost kradzieży w okresie objętym raportem wyniósł 29,8%. Łącznie to ponad 8300 incydentów. Co jednak ciekawe, 84% zdarzeń miało miejsce tylko w 10 krajach EMEA. Nie ma wśród nich Polski, co pokazuje, że nasz kraj cieszy się wysokim poziomem bezpieczeństwa. Krajami, w których najczęściej dochodzi do kradzieży, są Niemcy, RPA, Wlk. Brytania, Włochy i Rosja (licząc tylko w jednorazowych zdarzeniach o stracie przekraczającej 100 tys. euro). Kolejny ciekawy fakt – wzrost kradzieży nie dotyczy nie tylko dóbr wysokiej wartości takich jak elektronika, wyroby tytoniowe, farmaceutyki, alkohole. Giną też części samochodowe, rowery, żywność.

W zasadzie każda grupa produktowa jest narażona na straty.

Z tego powodu firmy transportowe o wysokim stopniu rozwoju rozwiązań z obszaru bezpieczeństwa stają się istotnym obiektem zainteresowania osób zajmujących się bezpieczeństwem w biznesie. Po pierwsze, jako odbiorcy rozwiązań technologicznych, organizacyjnych czy finansowych (ubezpieczenia) w celu podniesienia ich zdolności do realizowania zleceń transportowych. Po drugie dlatego, że firmy o odpowiednio wysokim poziomie bezpieczeństwa stanowią bezcenny zasób we własnym systemie łańcucha dostaw.

Czas na inwestycje

Przebadane przez nas firmy dysponowały nowoczesnymi pojazdami, stosowały doskonałej jakości systemy GPS i inne systemy bezpieczeństwa. Przykładowo, jedna z nich blisko 10% pojazdów z floty liczącej ich 200 zabezpieczyła je dodatkowo, umieszczając na naczepach kamery VSS. Rozwiązanie takie stosuje się wtedy, gdy klient zgłasza problemy z ilościowym i jakościowym rozliczaniem dostaw. W trasę ruszają więc pojazdy zabezpieczone w każdym niewrażliwym miejscu w kamerę VSS zintegrowaną z GPS. Wiedzą o tym tylko ci, którzy muszą wiedzieć. I nie są to ani kierowcy, ani magazynierzy, ani nikt z niższego szczebla logistycznego.

Własne centra monitoringu lub struktury o rozszerzonym zakresie nadzoru nad jakością realizacji transportów, zwane Control Tower, stają się coraz bardziej popularne, choć na razie spotykane w największych przedsiębiorstwach.

Firmy transportowe muszą zainwestować w certyfikaty bezpieczeństwa, zakupy systemów GPS czy mechanicznych systemów zamknięć. Konieczne są stała rekrutacja kierowców i ciągłe badanie jakości ich pracy i uczciwości. Tworzenie map bezpiecznych parkingów i postojów wymaga opracowania własnych baz tych miejsc lub odpłatnego korzystania z wyspecjalizowanych podmiotów.

Własne centrum monitoringu to przedsięwzięcie kosztowne. Zlecenia lub kontrakty rzadko są umowami długoterminowymi, więc inwestowanie w pełny zakres zabezpieczeń dla mniejszych firm stanowi barierę rozwoju. Co innego, gdy firma może skorzystać z bardziej elastycznego zasobu współdzielonego, jak chociażby w obszarze Control Tower.

Postępująca cyfryzacja procesów logistycznych i transportowych wprowadza kolejną kategorię zabezpieczeń – narzędzia cybersecurity, które muszą stać się elementem ochrony. Nie mniej ważny jest dobór ubezpieczenia pasującego do konkretnego kontraktu. Dobre ubezpieczenia również bywają kosztowne, ale jednocześnie stanowią poważne wsparcie dla realizacji świadomej polityki bezpieczeństwa.

Polskie rodzinne firmy transportowe, jak wszystkie tego typu, borykają się z wieloma problemami wewnętrznymi. Jednym z najważniejszych jest sukcesja. Dochodzi tu do swego rodzaju konfliktu pomiędzy modelem zarządzania założycieli firmy a koniecznością wprowadzania zmian wynikających m.in. ze skali operowania firmy.

Obecnie polska część tej branży, pomimo wielu narastających problemów, jest jednak europejskim liderem. Mimo że tak bardzo rozdrobniona, może pochwalić się swoistymi okrętami flagowymi, które znalazły się na liście TAPA TSR. To branża ludzi twardych, nawykłych do dynamicznych zmian i konieczności przystosowania swoich potencjałów do realizacji coraz bardziej ambitnych celów. ●



Jacek Tyburek

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

REKLAMA



WISENET
UCHWYĆ
SZEROKĄ
PERSPEKTYWĘ

Zachowaj najmniejsze detale

Kamera sieciowa TNB-9000 dedykowana do nadzoru wizyjnego rozległych obszarów, zapewnia odpowiednią rozdzielczość do wydobywania szczegółów z wykorzystaniem cyfrowego powiększenia przy jednoczesnej rejestracji całego obrazu



Pierwsza
profesjonalna kamera
sieciowa 8K UltraHD

Postęp w dziedzinie dozoru wizyjnego w połączeniu z nowymi technologiami opartymi na uczeniu maszynowym i sztucznej inteligencji poszerza obszar wprowadzania nowych funkcjonalności. Jednym z tego typu zastosowań jest precyzyjna identyfikacja pojazdów.

Jan T. Grusznic,
a&s Polska



Odczyt tablic rejestracyjnych – przegląd rozwiązań

Technika identyfikacji pojazdów nosi kilka nazw:

- **LPR** – LICENSE PLATE RECOGNITION,
- **ANPR** – AUTOMATIC NUMBER PLATE RECOGNITION,
- **ALPR** – AUTOMATED LICENSE PLATE READERS,
- **NPR** – NUMBER PLATE RECOGNITION.

Niezależnie od terminologii mowa o potężnym narzędziu używanym w wielu miejscach do automatyzacji procesu wjazdu/wyjazdu czy parkowania pojazdu oraz gromadzenia danych.

odnalezieniu na nagraniu pojazdu nawet w przypadkach, gdy sprawca opuścił teren, zanim dowiedział się o zdarzeniu. Rozpoznawanie numerów tablic rejestracyjnych może być bardzo przydatne również do śledzenia określonego pojazdu. Niezależnie od powodów system może powiadamiać, jeśli samochód o wskazanych numerach rejestracyjnych lub innych cechach zostanie wykryty w punkcie odczytu.

Inteligentne rozwiązania transportowe – ITS

Inteligentne rozwiązania transportowe (ITS) są istotne dla zapewnienia bezpieczniejszego korzystania z dróg w Polsce. ITS wykorzystuje podobne rozwiązania techniczne, jak te stosowane są w aplikacjach *stop-and-go*, przy czym ITS bazuje na obrazach o powtarzalnie wysokiej jakości i solidnym oprogramowaniu do odczytu tablic rejestracyjnych. Wysoka jakość obrazu jest kluczowa, głównym celem użytych w tym celu kamer jest bowiem identyfikacja pojazdów na trasach przejazdowych, a to funkcja, której nie można uzyskać za pomocą konwencjonalnych kamer dozorowych stosowanych w aplikacjach parkingowych. Kamery te muszą dostarczać wyraźnych ujęć w każdych warunkach oświetleniowych i atmosferycznych oraz przy każdej prędkości. Dzięki temu system rozpoznaje markę i model samochodu, jego typ (np. osobowy, ciężarowy), jak również kolor nadwozia czy nawet chwilową prędkość.

Rozwiązania przeznaczone dla ITS mają również możliwość jednoczesnej identyfikacji kilku pojazdów znajdujących się na sąsiednich pasach ruchu (w aplikacjach *stop-and-go* na ogół identyfikowany jest jeden pojazd w danej jednostce czasu). Dane z tych systemów wykorzystywane są również w ocenie ciągłości przepływu pojazdów z określeniem struktury rodzajowej (liczby pojazdów poszczególnych kategorii), a także struktury kierunkowej (liczba pojazdów poruszających się w określonych kierunkach), określenia pochodzenia pojazdu (np. polski, zagraniczny) czy też wskazania charakteru ruchu (lokalny, tranzytowy).

Punkty poboru opłat to kolejny obszar w ramach ITS, który wykorzystuje rozwiązania wizyjnej identyfikacji pojazdów. Obecne możliwości agregowania danych o pojazdach na podstawie obrazu wideo nie tylko zwiększa bezpieczeństwo, ale także oferuje możliwość analizy ruchu i predykcji zmian trendu. Firmy zarządzające autostradami i przedstawiciele władzy mogą również wykorzystywać tę technologię do identyfikacji naruszeń i automatyzacji procesu zarządzania ruchem. System wysyła pozyskane dane do serwera centralnego, weryfikując w ten sposób uiszczenie opłaty drogowej. Władze miast stosują to rozwiązanie do zliczania samochodów w celu przewidywania korków i kontrolowania przepływu ruchu. ●

Obecne rozwiązania wyspecjalizowane w identyfikacji pojazdów wychodzą poza optyczne rozpoznawanie znaków, czyli tradycyjny OCR (*Optical Character Recognition*), i oprócz odczytu tablic rejestracyjnych potrafią także rozpoznać markę, model samochodu, a nawet kolor jego nadwozia. A przecież już sam proces odczytu numerów rejestracyjnych jest dość skomplikowany. Wymaga od programu rozpoznania różnych elementów i w zależności od użytej czcionki, kolejności i liczby występujących po sobie znaków, przerw między nimi lub koloru tła tablicy określa nie tylko kraj pochodzenia pojazdu, ale także województwo, w jakim jest zarejestrowany, lub typ czy charakter pojazdu (np. uprzywilejowany, ekologiczny itp.).

Transport drogowy towarów jest jedną z trzech największych, obok handlu hurtowego i detalicznego, branż gospodarki polskiej. Bezpośredni udział sektora transportu i magazynowania w polskim PKB wynosi 6%, jednak jego znaczenie dla gospodarki jest znacznie większe. Bez transportu inne branże nie mogłyby funkcjonować, zwłaszcza handel i przemysł. Polskie przedsiębiorstwa transportowe wnoszą ogromny wkład nie tylko w polską, ale także w europejską gospodarkę.

Aplikacje typu *stop-and-go*

Kamery wyposażone w funkcję rozpoznawania tablic rejestracyjnych są doskonałym narzędziem do zastosowania w wielu różnych miejscach. Bardzo dobrze sprawdzają się w aplikacjach typu *stop-and-go*. Prezentowane narzędzia pozwalają dokładnie określić, które pojazdy wjechały na teren, kiedy przyjechały i kiedy z niego wyjechały. To dane, które są cenne dla osób zarządzających obiektami biurowymi czy procesami logistycznymi. Zrozumienie częstotliwości odwiedzin i czasu spędzanego przez klientów w danym miejscu stanowi też ważny element działania np. sieci sklepów i centr handlowych.

Rozwiązanie odczytujące tablice rejestracyjne może wspierać identyfikację użytkowników, nowych i nieupoważnionych osób oraz współpracować z systemami kontroli dostępu w celu usprawnienia procesu wjazdu. Parkingi są zresztą naturalnym miejscem jego użycia. Systemy identyfikujące pojazdy pomagają w egzekwowaniu przepisów parkingowych, limitów czasowych dla zarezerwowanych miejsc. Szczególnie, gdy parking ma charakter otwarty i znajduje się w pobliżu innych firm.

Tradycyjne nadzorowanie miejsc parkingowych wymaga dużych nakładów i jest nieekonomiczne. Dzięki rozwiązaniom identyfikującym pojazdy można je zautomatyzować. System natychmiast poinformuje obsługę, że np. konkretny pojazd przekroczył czas parkowania lub został postawiony na miejscu przysługującym konkretnej firmie bądź osobie.

Parkingi i garaże są miejscem ciągłego ruchu pojazdów przejeżdżających przez punkty kontrolne (szlabany lub bramy), zatem naturalna jest chęć kontrolowania, kto i kiedy wjechał oraz wyjechał. Monitorując punkty wjazdu i wyjazdu, można uzyskać większą potrzebnych informacji o tym, które samochody miały dostęp do danej lokalizacji. Uzyskane w ten sposób rejestry – zawierające czas i numery tablic – mogą posłużyć do budowania statystyk zajętości lub do szybkiego wyszukiwania informacji dotyczących powstałego incydentu. Wypadki drogowe zdarzają się nie tylko na drogach publicznych, sporo zdarzeń to kolizje parkingowe. Wykorzystanie funkcji identyfikacji pojazdów zapewnia znacznie większą przejrzystość, pomaga w łatwym i szybkim

Przykłady rozwiązań ANPR prezentujemy na kolejnej stronie →



stop
&
go



Aplikacja AXIS License Plate Verifier w zależności od kamery, na której zostanie zainstalowana, może być wykorzystywana w rozwiązaniach typu *stop&go*, a także w strefach ruchu o umiarkowanej prędkości do 70 km/h. Rozwiązanie to umożliwia łatwą integrację z innymi produktami Axis – moduły wejścia/wyjścia, sterowniki kontroli dostępu czy oprogramowanie Axis Camera Station. Dzięki czemu rozwiązanie to może być wykorzystywane do otwierania szlabanów, detekcji wjazdu nieuprawnionych pojazdów do strefy o ograniczonym ruchu czy wyszukiwania nagrań, na których pojawia się dany numer rejestracyjny. Więcej na www.axis.com/pl-pl

Parametr	Wartość
Odczyt tablic rejestracyjnych (liczba znaków min.-maks.)	3-10
Maks. prędkość pojazdu	do 70 km/h
Sterowanie automatyką szlabanu	Wbudowany przełącznik, zewnętrzny moduł we/wy, zewnętrzny sterownik kontroli dostępu, powiadomienia TCP, HTTP.
Odległość odczytu min./maks.	7 m/20 m*
Identyfikacja kierunku przemieszczania się (wjazd, wyjazd)	Tak
Funkcje MMR	Brak dla oprogramowania LPR
Praca w warunkach słabego oświetlenia	Wbudowany oświetlacz podczerwieni 850 nm o zasięgu do 45 metrów*
* Podane parametry mają zastosowanie wraz z kamerami z rodziny P14.	

stop
&
go



Kamera DHI-ITC437-PW6M-IZ-GN to połączenie doskonałej jakości obrazu w rozdzielczości 4 Mpix generowanego przez przetwornik 1/1.8" oraz zaawansowanych algorytmów AI, daje wysoką skuteczność odczytywania tablic rejestracyjnych (≥99%) w każdych warunkach. Biblioteki SDK i API pozwalają na szybką i łatwą integrację. Możliwość zasilania kamery przez PoE+ znacząco upraszcza instalację. Więcej na <https://dahuasecurity.com/ceen>

Parametr	Wartość
Odczyt tablic rejestracyjnych (liczba znaków min.-maks.)	Zależnie od kraju przeznaczenia
Maks. prędkość pojazdu	60 km/h
Sterowanie automatyką szlabanu	Wyjście przełącznikowe, 2 wyjścia transportowe, powiadomienia TCP, HTTP
Odległość odczytu min./maks.	8-30 m
Identyfikacja kierunku przemieszczania się (wjazd, wyjazd)	Tak
Funkcje MMR	Rozpoznanie typu pojazdu (osobowy, ciężarowy, motocykl, autobus itp.), modelu, marki, wersji, koloru nadwozia
Praca w warunkach słabego oświetlenia	Wbudowany oświetlacz podczerwieni 850 nm

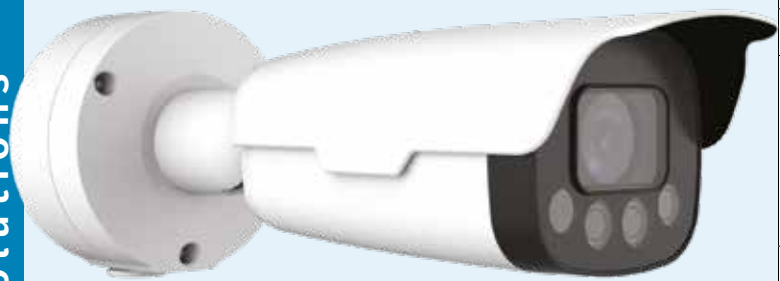
stop
&
go



Kamera BCS-TIP7401ITC-III o rozdzielczości 4 Mpix i obiektywie 10-50 mm charakteryzuje się skutecznością rozpoznawania tablic na poziomie ok. 95%. Biała/czarna lista ma pojemność do 10 000 wpisów. Więcej na www.bcs.pl

Parametr	Wartość
Odczyt tablic rejestracyjnych (liczba znaków min.-maks.)	4-10
Maks. prędkość pojazdu	60 km/h
Sterowanie automatyką szlabanu	3 wejścia, 3 wyjścia alarmowe, zewnętrzny moduł komunikacji Wiegand
Odległość odczytu min./maks.	8-30 m
Identyfikacja kierunku przemieszczania się (wjazd, wyjazd)	Tak
Funkcje MMR	Rozpoznanie typu pojazdu (osobowy, ciężarowy, dostawczy), typu nadwozia, marki, koloru nadwozia
Praca w warunkach słabego oświetlenia	Wbudowany oświetlacz IR 850 nm, 30 m

stop
&
go



Kamera Uniview HC121@TS8CR-Z umożliwia automatyczne rozpoznawanie tablic rejestracyjnych z zatrzymanych lub wolno poruszających się pojazdów. Może utworzyć samodzielny system kontroli dostępu po podłączeniu do szlabanu. Umożliwia tworzenie białych i czarnych list numerów rejestracyjnych. Może współpracować z interkomem. Dla optymalizacji przestrzeni dyskowej na zapisane tablice rejestracyjne możliwy jest zapis jedynie fragmentu obrazu z przodem auta. Więcej informacji na: www.suma.solutions

Parametr	Wartość
Odczyt tablic rejestracyjnych (liczba znaków min.-maks.)	Rozpoznaje tablice rejestracyjne z wielu krajów
Maks. prędkość pojazdu	30 km/h
Sterowanie automatyką szlabanu	Obsługa kontroli dostępu po podłączeniu do szlabanu
Odległość odczytu min./maks.	Do 7 m [zależy od wysokości montażu kamery]
Identyfikacja kierunku przemieszczania się (wjazd, wyjazd)	Nie
Funkcje MMR	Rozpoznawanie koloru nadwozia
Praca w warunkach słabego oświetlenia	Wysoka skuteczność dzięki technologii Starlight oraz użyciu oświetlacza LED IR

stop
&
go

ZKTeco



ZK-LPR Car ID. Instalacja i konfiguracja *plug&play*. Wbudowane oprogramowanie kontroli dostępu (intuicyjny interfejs w języku polskim). Zarządzanie czarną i białą listą. Rozpoznaje tablice z 84 krajów (zapis obrazów tablic). Wysyłka raportów. Samoptymalizacja. ANR. Współpraca z innymi kamerami (Master/Slave). Pamięć Flash 4 GB + karta SD 64 GB (128 GB) w komplecie.

Więcej na www.zkteco.eu

Parametr	Wartość
Odczyt tablic rejestracyjnych (liczba znaków min.-maks.)	1-12, OCR, znaki łacińskie, arabskie, tajskie, cyrylica itp.
Maks. prędkość pojazdu	20 km/h
Sterowanie automatyką szlabanu	Wbudowany przełącznik, wejścia/ wyjścia alarmowe, RS-485, TCP, HTTP
Odległość odczytu min./maks.	3 m/15 m
Identyfikacja kierunku przemieszczania się (wjazd, wyjazd)	Tak, optyczny czujnik ruchu
Funkcje MMR	[brak]
Praca w warunkach słabego oświetlenia	Wbudowany oświetlacz podczerwieni o zasięgu 50 m

ITS



Suma Solutions

Kamera VIVOTEK IP9165-LPR-v2 Kit (Street) jest samodzielnym systemem umożliwiającym rozpoznawanie tablic rejestracyjnych pojazdów poruszających się w ruchu miejskim. Dzięki najnowszemu oprogramowaniu Traffic VCA LPR+ kamera nie tylko dokładnie odczytuje numery rejestracyjne pojazdu, ale również rozpoznaje atrybuty pojazdu (w tym kolor[9] i typ[5]) oraz kierunek ruchu. Umożliwia to sprawną identyfikację pojazdów jadących pod prąd czy znalezienie pojazdów, bazując na części numeru rejestracyjnego i kolorze.

Więcej informacji na: www.suma.solutions

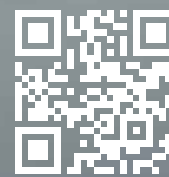
Parametr	Wartość
Odczyt tablic rejestracyjnych (liczba znaków min.-maks.)	Rozpoznaje tablice rejestracyjne z ponad 100 krajów
Maks. prędkość pojazdu	90 km/h
Odległość odczytu min./maks.	do 35 metrów
Maks. liczba jednocześnie identyfikowanych pojazdów	2
Maks. liczba jednocześnie analizowanych pasów ruchu	2
Funkcje MMR	Rozpoznanie typu pojazdu (motocykl, samochód, van, ciężarówka, autobus), koloru nadwozia, wykrywanie kierunku
Zliczanie pojazdów	Nie
Analiza tempa przepływu pojazdów	Nie
Analiza długości kolejki	Nie
Praca w warunkach słabego oświetlenia	Wysoka skuteczność dzięki użyciu oświetlacza IR, który umożliwia zdalne dostosowanie kąta padania wiązki podczerwieni

N NMS ADVANCED CONTROL**INTEGRACJA • KONFIGURACJA • WIZUALIZACJA**
SYSTEMÓW BEZPIECZEŃSTWA

- ✓ INTEGRACJA Z URZĄDZENIAMI VSS, KD, SSWiN ORAZ AUTOMATYKI BUDYNKOWEJ
- ✓ REJESTRACJA CZASU PRACY RCP
- ✓ KONTROLA DOSTĘPU DO WIND I PIĘTER
- ✓ FUNKCJE GLOBALNE
- ✓ IDENTYFIKACJA BIOMETRYCZNA
- ✓ PODGLĄD OBRAZU, ODTWARZANIE ORAZ POBIERANIE NAGRAŃ
- ✓ ZARZĄDZANIE SYSTEMAMI ROZPROSZONYMI
- ✓ ROZPOZNAWANIE TABLIC REJESTRACYJNYCH



strefy parkingowe • wizualizacja na panelach • definiowalne poziomy dostępu • zarządzanie kontrolą przejazdu • drukarki biletów wraz z kodami QR • czytniki kodów QR



JAK TO DZIAŁA?

NMSAC.AAT.PL

NMS AC to profesjonalne polskie oprogramowanie zarządzające systemami bezpieczeństwa w obiektach.

Do nabycia u najlepszych instalatorów!

AAT SYSTEMY BEZPIECZEŃSTWA

PRODUCENT I DOSTAWCA ELEKTRONICZNYCH SYSTEMÓW ZABEZPIECZENIA MIENIA
www.aat.pl



Od zarządzania personelem po komplementarne rozwiązania logistyczne

Globalizacja łańcucha dostaw, dynamicznie rozwijający się rynek e-commerce i rosnący popyt towarów są impulsem wzrostu w branży logistycznej.

Paweł Sobociński

Mamy do czynienia ze zwiększającą się liczbą nowych obiektów o różnicowanej kubaturze i coraz bardziej wyrafinowanych wymaganiach technicznych, także w sferze zabezpieczeń i ochrony. Hikvision oferuje kompleksowe rozwiązania, które nie tylko poprawiają bezpieczeństwo, ale też zwiększają efektywność operacyjną obiektów logistycznych.

Pierwszym elementem usprawniającym obiekt jest skuteczne zarządzanie personelem. Osiągnięcie tego możliwe było dzięki zaawansowanej kontroli dostępu realizowanej za pomocą terminali w połączeniu z bramkami obrotowymi lub uchylnymi. Takie rozwiązanie ma na celu szybką autoryzację wraz z rejestracją czasu pracy czy też dzięki kamerom wspartym algorytmami sztucznej inteligencji i weryfikującym wyposażenie pod kątem BHP.

Ponadto kamery mogą dostarczać informacje o efektywności pracy w monitorowanych strefach. Kolejnym elementem usprawniającym, mającym bardzo duży wpływ na oszczędności, jest analiza dóbr poprzez

monitoring wizyjny, mający na celu ochronę produktów i monitorowanie całego ruchu za pomocą analizy zajętości miejsc na regałach czy w strefach przechowywania oraz skanowania/odczytu oznakowań ładunków i wiązania danych z nagraniami archiwalnymi.

Tym sposobem integracja oprogramowania do zarządzania materiałem wizyjnym (VMS) z magazynowymi systemami informatycznymi (Warehouse Management System, WMS) sprawia, że użytkownik ma dostęp do kompleksowego wglądu w cały łańcuch realizacji zlecenia, włącznie z materiałem wideo. Optymalizacja zarządzania dokami oraz pojazdami jest możliwa za sprawą rozbudowanego systemu kamer analizujących zajętość w strefach załadunku i rozładunku. Pomiar długości czasu obsługi ciężarówek w celu jeszcze lepszego zarządzania może być komunikowany na ekranach LED/LCD w jednym systemie.

Powyższe opracowanie to opis kilku podstawowych usprawnień, które stają się standardem i wstępem do bardziej zaawansowanych działań, takich jak kompleksowe rozwiązania CCTV, KD, SSWiN zintegrowane z robotyką i *machine vision*. To sprawia, że Hikvision jako producent wspomnianych produktów staje się liderem w dostawie komplementarnych rozwiązań do logistyki.

Warto wiedzieć, że poza urządzeniami, takimi jak kamery sieciowe, kamery PTZ, sieciowe rejestratory wideo czy terminale do rozpoznawania twarzy, firma Hikvision oferuje także oprogramowanie HikCentral Professional służące do integracji i zarządzania systemami zabezpieczeń. Zostało ono tak zaprojektowane, aby sprostać różnym wyzwaniom związanym z bezpieczeństwem na jednej platformie.

Dzięki HikCentral Professional można łatwo zarządzać wieloma pojedynczymi systemami, takimi jak telewizja dozorowa, kontrola dostępu, system alarmowy i inne. Codzienne operacje stają się bardziej efektywne, a ochrona osób i mienia wszędzie się poprawia. ●



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





Sytuacja sprzyja branży?

O kondycję polskiego rynku zabezpieczeń technicznych zapytaliśmy przedstawicieli największych firm branżowych.

Iwona Krawiec, Monika Mamakis,
a&s Polska

Według danych raportu *Security 50* większość globalnych firm branży security odnotowała wzrost przychodów w porównaniu z rokiem poprzednim. Czy ta tendencja jest również zauważalna na rynku polskim? Eksperti są zgodni. Większość firm w naturalny sposób zwiększa przychody. Tendencje wzrostowe utrzymały się także w Polsce. Krzysztof Bartuszek z Securitas Polska twierdzi, że kondycję firm kształtuje nie tylko wzrost sprzedaży i rozwój nowych usług, ale także podniesienie cen. Ponadto na nowe technologie stać duże przedsiębiorstwa i to one mogą sobie pozwolić na transformację związaną z digitalizacją usług.

– W Polsce wyraźnie widać kilka trendów i pewną polaryzację. Z jednej strony są usługi, które zyskują na popularności, oparte głównie na najnowszej technologii i systemach elektronicznych, które zastępują w coraz większym stopniu proste usługi ochrony. Tutaj przychody wyraźnie rosną. Z drugiej strony są klienci, dla których ochrona jest istotna, skupiający się na jakości. Jak zwykle zyskają największe firmy oraz wyspecjalizowane firmy niszowe. Dla mniejszych podmiotów, szczególnie wykonujących proste usługi ochrony, może to stanowić istotne wyzwanie, a ograniczenia w ochronie fizycznej to dotkliwy spadek przychodów – ocenia Krzysztof Bartuszek.



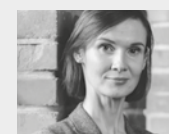
Artur Stępowski, NSS

Obserwując zmiany na rynkach w Polsce i za granicą, staramy się rozwijać własne produkty, zmniejszając negatywne wpływy zewnętrznych czynników mogących zagrozić płynności dostaw do naszych klientów lub spowodować niemożność realizacji projektów wedle nowych coraz ostrzejszych wymagań. Stawiamy na polską myśl technologiczną, wieloletnie doświadczenie, bogaty zespół specjalistów z branży elektronicznej i IT oraz własny park produkcyjny. Zainwestowaliśmy w rozwój systemów do dozoru wizyjnego połączonego z własną analityką, zbudowaliśmy rejestrator CCTV, który może być wspomagany własną sztuczną inteligencją lub analityką stron trzecich. Stworzyliśmy również od podstaw polski system alarmowy. Dzięki profesjonalnemu zespołowi konstruktorów oraz programistów udało nam się w krótkim czasie wyposażyć wszystkie systemy GPS w nadajniki LTE i umożliwić w ten sposób lokalizację rowerów, motorów i hulajnog elektrycznych. Otworzyliśmy tym samym nowy obszar działania naszej firmy.



Krzysztof Bartuszek,
Securitas Polska

Polski rynek nie jest jeszcze nasycony zintegrowanymi rozwiązaniami technicznymi i tutaj widzę perspektywę rozwoju. To naturalna transformacja. Coraz popularniejsze są m.in. usługi zdalne (w tym wideo), zdalne otwieranie obiektów, digitalizacja raportów, AI jako element, który pojawia się w procesie analizy zagrożeń, czy też już bezpośrednio wspiera systemy CCTV, kontroli dostępu i inne. Technika i technologie to jednak również ryzyko związane choćby z cyberprzestępczością. To zapewne obszar, który będzie coraz bardziej istotny. Pozostałe zagrożenia będą miały dotychczasowe podłoże lokalne i makroekonomiczne, a ich skala będzie zależna od sytuacji gospodarczej i geopolitycznej.



Anna Twardowska,
Nedap Security Management

Upatrujemy dużej szansy we wzroście świadomości klientów. Coraz częściej wybierają oni rozwiązania, które spełniają europejskie normy i mają zaimplementowane wysokiej jakości zabezpieczenia cybersecurity. Zwracają również uwagę na systemy, które są otwartą platformą, a tym samym umożliwiają rozwój i dostosowanie ich do obecnych i przyszłych wymagań organizacji. Tryb pracy hybrydowej spowodował duży wzrost zainteresowania systemem AEOS Locker Management, który umożliwia bezpieczne przechowywanie rzeczy przez pracowników, gości czy firmy serwisowe. Wyzwaniem będą w 2023 r. trwające problemy z dostępnością komponentów i związane z tym zakłócenia w dostawach sprzętu. Podjęliśmy jednak działania, by nie były one tak dokuczliwe jak w ubiegłym roku.

PERSPEKTYWY NA ROK 2023



» Na koniunkturę w branży mogą wpłynąć różne czynniki. Wśród najczęściej wymienianych znalazły się kłopoty w budownictwie, wzrost cen, a także niepewna sytuacja geopolityczna. «



W Polsce zdecydowanie podążamy za światowymi trendami. Niestety wdrażanie najnowszych rozwiązań często jest hamowane przez sytuację ekonomiczną. Artur Hejdysz z C&C Partners podkreśla, że na rozwój branży security mają wpływ uwarunkowania geopolityczne i ekonomiczne. W przypadku Polski duże projekty w zakresie bezpieczeństwa realizowane są w regionach czy branżach, które do tej pory były niedoinwestowane. Artur Hejdysz przypuszcza jednak, że w bliskiej perspektywie można spodziewać się znaczącego spowolnienia inwestycji.

– Projekty, których realizacja była planowana w trzecim i czwartym kwartale, mogą zostać wstrzymane z powodu braku środków na ich sfinansowanie lub też wzrostu kosztów przekraczających limity zakładane przez inwestorów. Terminy ich realizacji pozostaną pod znakiem zapytania. Na to wszystko duży wpływ ma niestabilność sytuacji na świecie – podkreśla.

O uwarunkowania ekonomiczne martwi się również Artur Stępowski z NSS. – Nasza branża jest bardzo podatna na wszelkie zmiany związane z kosztem pracy, inwestycjami w budownictwie czy perturbacjami w transporcie. Według GUS koniunktura w budownictwie pod koniec roku 2022 przekroczyła minus 22%. Oznacza to spadek nowych inwestycji, co niewątpliwie odbije się na gospodarce w latach 2023–2024. Dodatkowych problemów przysporzyła niestabilna sytuacja polskiego złotego, przy jednoczesnym rekordowym wzroście kursu dolara – wyjaśnia.

W podobnym tonie wypowiada się Anna Twardowska z Nedap Security Management, która zauważa, że wojna w Ukrainie i wzrost zagrożeń w zakresie cybersecurity spowodowały wzrost zainteresowania systemami zabezpieczeń technicznych. Coraz więcej firm decyduje się na inwestycje w obszarze systemu kontroli dostępu czy systemów sygnalizacji włamania i napadu.

– To, co często było traktowane jako koszt w organizacji, teraz jest traktowane jako kluczowa inwestycja w zapewnienie bezpieczeństwa

organizacji – twierdzi Anna Twardowska, zaznaczając, że wzrasta świadomość dotycząca norm, które powinny spełniać stosowane rozwiązania: – Nasze dobre referencje i coraz większe portfolio klientów powodują wzrost zainteresowania naszymi rozwiązaniami.

Kondycja firm polskich

Na rynku security daje się zauważyć wzrost aktywności firm z sektorów kontroli dostępu i telewizji dozorowej. Wiąże się to z pewnością z konsekwencjami wymagań w czasie pandemii, które zwiększyły zainteresowanie klientów, zwłaszcza rozwiązaniami bezdotykowymi. Gdy jedne czynniki wpływały na rozwój, inne go hamowały.

– Firma odnotowała duży wzrost obrotów na rynku polskim w roku 2022 mimo różnych pojawiających się problemów – wyjaśnia Marek Piotrowski z ZKTeco. – Trudno powiedzieć, na ile ten wzrost wynikał z tendencji rynkowej, a na ile z nasilonych działań promocyjnych firmy i zwiększonej aktywności handlowej. W ubiegłym roku było wiele zjawisk, które nie napawały nas optymizmem. Po wybuchu wojny w Ukrainie i odpływie sporej liczby pracowników ukraińskich z polskich budów wiele inwestycji straciło impet lub zostało wstrzymanych. Spowodowało to spadek liczby zleceń naszych klientów. Innym utrudnieniem były spore zmiany organizacyjne w naszym przedstawicielstwie na Europę, co szczególnie pod koniec roku utrudniało nam płynną obsługę zamówień klientów – podsumowuje Marek Piotrowski.

Utrzymanie tendencji wzrostowej wymagało dużego nakładu pracy, zwłaszcza przy wprowadzaniu nowych produktów, które miały pobudzić zainteresowanie klientów. Sytuację komentuje też Łukasz Kanarek z firmy Roger.

– Rok 2022 był dla nas owocny. Wzrost przychodów nie był tak spektakularny, jak w roku poprzednim, jednakże zakończyliśmy go dodatnim, dwucyfrowym wynikiem. Rozwój widzimy zwłaszcza w zakresie obsługi rynku projektowego, w którym w ostatnich

dwóch latach znacząco zwiększyliśmy udział. Na tym rynku odnotowaliśmy ponad 20-procentowy wzrost sprzedaży systemu RACS 5. Do osiągnięcia tego wyniku w znacznym stopniu przyczynił się jeden z dużych projektów sektora finansów publicznych, na którego potrzeby opracowaliśmy moduł integracji systemu RACS 5 z oprogramowaniem służącym do centralnego rozliczania czasu pracy – wyjaśnia Łukasz Kanarek.

W ubiegłym roku firmy mocno odczuwały skutki braków komponentów i zakłócenia w ciągłości łańcucha dostaw, co wpływało negatywnie na terminowość dostaw. Działające globalnie przedsiębiorstwa z branży security, takie jak Axis Communications, odnotowują wzrost dochodów, ale i one zmagają się z pandemią i zakłóceniami łańcucha dostaw, które odbijają się na dostępności produktów na rynku polskim. Dagmara Pomirska z Axis Communications zauważa, że ograniczenie dostaw zbiegło się ze wzrostem popytu, co dodatkowo wpłynęło na opóźnienia w dostawach. – Obecnie widzimy duże zainteresowanie naszą ofertą, jednak opóźnienia uniemożliwiają nam pełne wykorzystanie potencjału rynku, ponieważ część dostaw z roku 2022 została przesunięta na początek tego roku – przyznaje.

Podobne spostrzeżenia ma też Piotr Rogalewski z Hikvision Poland. – Pomimo niesprzyjających okoliczności gospodarczych udało się nam osiągnąć wyraźny wzrost przychodów, choć było to z pewnością trudniejsze niż w poprzednich latach. Mamy nadzieję, że cała branża security w Polsce może cieszyć się wzrostami, bo to przecież nasza wspólna przestrzeń biznesowa – konkluduje.

Ciekawą analizę sprzedaży produktów z poszczególnych działów zabezpieczeń przedstawił Artur Stępowski. Według niego w sektorze telewizji dozorowej wzrost opierał się głównie na nowych produktach i nowych rozwiązaniach software'owych. Firmy zajmujące się zdalnym nadzorem zaczęły dostrzegać dodatkowe możliwości wynikające z monitoringu za pośrednictwem wież mobilnych oraz korzyści płynące z analityki obrazu, która pozwala zmniejszyć liczbę fałszywych alarmów. – W obszarze monitoringu sygnałów alarmowych wzrost wiąże się z rozwojem prostych systemów alarmowych, w tym także coraz popularniejszych w naszym kraju systemów bezprzewodowych. Zmiany w systemie drogowym e-tool oraz konieczność stosowania technologii LTE spowodowała także zauważalną zwyżkę sprzedaży systemów GPS – ocenia Artur Stępowski.

Ubiegły rok był zdecydowanie dobry dla firm z branż security i IT. – Zauważyliśmy wzrost liczby zapytań dotyczących nowych projektów i inwestycji od klientów zarówno instytucjonalnych z takich branż, jak HoReCa, edukacja czy też logistyka, jak i indywidualnych, dodatkowo wyposażających swoje domy w systemy monitoringu wizyjnego czy też infrastrukturę sieciową. Większość firm z naszego sektora odnotowała wzrosty przychodów w porównaniu do poprzedniego roku – mówi Robert Gawroński z TP-Link Polska.

Pomimo problemów z dostawami i niepewną sytuacją gospodarczą również w sektorze zabezpieczeń przeciwpożarowych odnotowano wzrost zysków. Firmy, które zainwestowały wcześniej w rozbudowę swoich zakładów, odniosły sukces. Robert Pestka z POLON-ALFA zauważa, że firma osiąga stały wzrost przychodów dzięki dostarczaniu na rynek niezawodnych i technologicznie innowacyjnych rozwiązań systemów sygnalizacji i automatyki pożarowej. – Decyzje o uruchomieniu nowej hali produkcyjnej okazały się słuszne. Obecnie prowadzone działania pozwalają nam ze spokojem oceniać przyszłość, jaką przyniesie rok 2023 – twierdzi.



Jacek Karcewicz, Miwi-Urmet

Perspektywy dla branży na rok 2023 w dużym stopniu zależą od sytuacji gospodarczej. Mogą nas czekać bowiem kolejne fale kryzysu energetycznego. Inflacja utrzyma się prawdopodobnie na wysokim poziomie. Ekonomści przewidują, że gospodarka światowa mocno spowolni, część krajów wpadnie w recesję, a niektóre mogą mierzyć się z kryzysem zadłużenia. Dług publiczny będzie jednym z najważniejszych tematów, także w Polsce. Dwa główne czynniki wzrostu (konsumpcja i inwestycje) nie mają przed sobą dobrych perspektyw z uwagi na zaciśnienie polityki pieniężnej i niepewność towarzyszącą kryzysowi energetycznemu. Branża security jest jednak dosyć wysoko pozycjonowana w hierarchii potrzeb i na tym powinniśmy bazować, prognozując rozwój firm z naszej branży.



Dagmara Pomirska, Axis Communications

Przewidujemy utrzymanie wysokiego zainteresowania produktami i rozwiązaniami Axis, dlatego planujemy poszerzenie portfolio oraz wzmocnienie oferty end-to-end. Zacieśnimy współpracę z partnerami i dystrybutorami, a także wzmocnimy kanał sprzedaży oraz bezpośredni kontakt z klientami końcowymi na wybranych rynkach. W roku 2023 planujemy liczne kampanie, które będą budować większą świadomość istnienia rozwiązań dla poszczególnych segmentów rynku, m.in. infrastruktury krytycznej, przemysłu czy handlu. W tym roku liczymy na unormowanie się łańcucha dostaw i terminów realizacji. Szansą dla branży będzie rosnące zapotrzebowanie na systemy zabezpieczeń z funkcjami analitycznymi.



Piotr Rogalewski, Hikvision Poland

Rok 2023 z pewnością będzie jednym z najtrudniejszych od dawna dla światowej gospodarki. Większość ekspertów ocenia, że wojna w Ukrainie będzie konfliktem długotrwałym, a to nie jest dobry prognostyk. Wzrost stóp procentowych hamuje dostępność środków operacyjnych dla firm, a do tego dochodzą poważna inflacja i bardzo wysokie ceny energii i paliw. W ujęciu makro to wszystko oczywiście negatywnie wpływa na inwestycje i zwiększa presję na oszczędności. Niekoniecznie jednak inwestorzy będą szukać najtańszych zabezpieczeń technicznych. Ważny tu będzie stosunek jakości do ceny, a także sze-roka oferta. W Hikvision wprowadziliśmy ostatnio m.in. bogate portfolio produktów Commercial Display, co pozwoli nam na penetrację zupełnie nowych obszarów rynku.

PERSPEKTYWY NA ROK 2023



» Firmy mocno odczuły skutki zakłóceń w ciągłości łańcucha dostaw, co wpływało negatywnie na terminowość realizacji zleceń. «

Wzrost zainteresowania rozwiązaniami ppoż. potwierdza też Michał Sidor z firmy Schrack Seconet Polska. – Rok 2022 był dla nas rekordowy pod kątem przychodów, mimo że borykaliśmy się z problemami wydłużonych terminów dostaw urządzeń do naszych klientów.

Nasilone problemy z komponentami i łańcuchem dostaw

Według światowych ekspertów największym wyzwaniem ubiegłego roku były braki komponentów potrzebnych do produkcji urządzeń i zakłócenia w utrzymaniu płynności łańcuchów dostaw. Te problemy dotknęły także polski rynek zabezpieczeń.

– Zakłócenia łańcucha dostaw komponentów było faktycznie dużą bolączką dla producentów oraz resellerów. Na niektóre produkty czas oczekiwania zwiększył się nawet kilkunastokrotnie. Przewiduję, że również w bieżącym roku problemy te będą występowały, choć w ograniczonym zakresie – komentuje Jacek Karcewicz z Miwi-Urmet.

Podobnego zdania jest Marek Piotrowski, który uważa, że problemy z łańcuchem dostaw jeszcze jakiś czas się utrzymają. Ma jednak nadzieję, że pod koniec drugiego kwartału sytuacja się poprawi. Przypomina też, że najwięksi producenci mający siedzibę w Chinach dopiero rozkręcają swoją produkcję po ograniczeniach wynikających z lockdownu. Jednak rosną ograniczenia z dostępem do surowców pochodzących z Rosji czy Ukrainy. – Zmiana źródła dostaw surowców i komponentów oraz odpowiednie dostosowanie produkcji do zjawisk zachodzących na światowych rynkach to procesy długotrwałe – uważa.

Trudnej sytuacji związanej z dostawami komponentów i zakłóceniami w łańcuchu dostaw doświadczyły zwłaszcza polskie oddziały dużych firm zagranicznych. W związku z tym większość z nich optymalizuje procesy logistyczne.

– W pierwszym kroku zwiększyliśmy liczbę dostawców poszczególnych komponentów, aby móc bardziej elastycznie planować i realizować zamówienia. Rozpoczęliśmy również proces umożliwiający przeprojektowywanie produktów, w którym będziemy w stanie wymienić brakujący element na inny, takiej samej jakości – wyjaśnia Dagmara Pomirska.

Monika Stanosz z Suma Solutions podkreśla, że chociaż firma w pierwszej połowie 2022 r. odczuwała jeszcze problemy z dostępnością sprzętu u dostawców, to w kolejnych miesiącach sytuacja się poprawiała: – W tym momencie nie przewidujemy niespodziewanych braków czy opóźnień w dostawach.

Skutki zakłóceń w dostawach pomogły złagodzić zapasy, które firmy zgromadziły w swoich lokalnych magazynach. Wiele firm planuje długofalowo, rezygnując chwilowo z metody just-in-time. Tak m.in. czynią Hikvision czy Roger. Przedstawiciele obu firm podkreślają, że zwiększenie zapasów magazynowych pozwoliło im firmom utrzymać dostępność urządzeń. Piotr Rogalewski podkreśla: – Dzięki zapasom nasi klienci odczuli globalne perturbacje w znacznie mniejszym stopniu. Światowym łańcuchom dostaw daleko jeszcze do stanu sprzed pandemii, ale śledząc trendy długoterminowe, jesteśmy umiarkowanymi optymistami.

W podobnym tonie wypowiada się Łukasz Kanarek: – Naszą przewagą jest to, że już kilka lat temu zdecydowaliśmy się na zwiększenie zapasów magazynowych, co pozwoliło na utrzymanie dostępności naszych urządzeń na poziomie kilku dni roboczych. Jesteśmy w tej komfortowej sytuacji, że mamy na miejscu swój dział badań i rozwoju, który szybko reaguje i przeprojektowuje nasze urządzenia. Przy współpracy z działem zakupów pozwala to skutecznie i z wyprzedzeniem zabezpieczyć ciągłość produkcji.

Nowa, nieprzewidywalna sytuacja związana z nieterminowością dostaw czy brakiem komponentów z jednej strony jest problemem, z drugiej – dla wielu firm okazała się szansą.

– Dobrze zaopatrzony magazyn stanowiący dla nas bufor bezpieczeństwa pozwolił nam na nieprzerwaną produkcję urządzeń i terminową realizację zamówień. Dało to naszym klientom możliwość wywiązania się ze swoich zobowiązań wobec inwestorów – podkreśla Robert Pestka.

O dostępność komponentów do produkcji urządzeń nie muszą martwić się firmy korzystające z dostawców lokalnych. Do takich przedsiębiorstw należy m.in. C&C Partners wchodzący w skład holdingu TKH Group. – Jesteśmy w niewielkim gronie firm, których



W Polsce działa obecnie ok. **3,8 tys. firm** zarejestrowanych jako **agencje ochrony osób i mienia**.

produkty zarówno hardware'owe, jak i oprogramowania mają pochodzenie europejskie, co w dzisiejszych czasach ma krytyczne znaczenie – mówi Artur Hejdzysz. – Dlatego nie dotknęły nas problemy logistyczne. Przygotowaliśmy się do sytuacji właściwie, a dostępność towaru jest naszym atutem. Elastyczność oraz własne zaplecze produkcyjne umożliwiły nam w tym trudnym czasie realizację wielu projektów.

Na koniunkturę w branży mogą wpłynąć różne czynniki. Wśród najczęściej wymienianych z negatywnym wpływem znalazły się kłopoty w budownictwie, wzrost cen, a także niepewna sytuacja geopolityczna. Nasi rozmówcy podkreślają jednak, że istnieje ryzyko, że przy tak słabej koniunkturze w budownictwie rynek będzie się zmniejszał, a jednocześnie będzie coraz bardziej wymagający. Artur Stępowski wyraża obawę, że z powodu stale wzrastających kosztów urządzenia tanie będą droższe, tym samym różnica w cenie pomiędzy wyrafinowanymi rozwiązaniami a produktami, gdzie cena była głównym motorem sprzedaży, będzie się zmniejszać.

W nieco innej sytuacji znalazły się firmy ochrony, które obok globalnych problemów zmagają się również z polskimi realiami. Co jest ich główną bolączką, poza ewentualnymi problemami z dostawami? To oczywiście: braki kadrowe. O trudnościach związanych z niedoborem wykwalifikowanych pracowników mówi m.in. Krzysztof Bartuszek, który podkreśla, że branża musi borykać się z paradoksem coraz większych oczekiwań jakościowych ze strony klientów przy jednoczesnym oczekiwaniu utrzymania niskich cen, a w tym samym czasie rosnących oczekiwań płacowych. Nadchodzące miesiące pokażą, czy zapowiadana recesja zmieni nieco tę sytuację.

Sytuacja sprzyja branży zabezpieczeń

Aktualna sytuacja geopolityczna mimo poważnych problemów, jakie powoduje, sprzyja branży zabezpieczeń. Infrastruktura krytyczna, obiekty publiczne, ale także duże podmioty prywatne inwestują duże kwoty w szeroko rozumiane bezpieczeństwo, w tym także zaawansowane środki ochrony technicznej. – Rośnie popyt na systemy ochrony perymetrycznej wspomagane sztuczną inteligencją (m.in. redukcja fałszywych alarmów), zaawansowaną analizę obrazu (np. scenariusze behawioralne, w tym detekcja paniki) czy monitoring termowizyjny. Coraz częściej pojawiają się też wymagania realizacji zaawansowanej konwergencji międzysystemowej i nacisk na dostarczenie kompleksowego i w pełni zintegrowanego systemu zabezpieczeń, a nie jego osobnych elementów, jak CCTV, kontrola dostępu i SSWiN. Niebagatelną rolę odgrywają tu możliwości dostosowania dokładnie do potrzeb klienta nie tylko urządzeń, ale także oprogramowania – komentuje Piotr Rogalewski.

Inna rzecz, że według opinii Jacka Karcewicza zapotrzebowanie na rozwiązania z zakresu systemów zabezpieczeń było bardzo różnicowane w zależności od sektora gospodarki. – Z naszych doświadczeń wynika, że największe inwestycje miały miejsce w obiektach infrastruktury krytycznej – zauważa.

Wiele zależy też od grupy produktowej. – Na rynku CCTV obserwujemy wzrost zainteresowania rozwiązaniami z funkcjami AI, co jest potwierdzeniem kierunku rozwoju systemów telewizji dozorowej – twierdzi Artur Stępowski. W obszarze SSWiN następuje zmiana, która będzie widoczna nie tylko w roku 2023, ale i w kolejnych latach. System alarmowy staje się podstawowym elementem wyposażenia mieszkania, domu, biura, punktu usługowego, sklepu. Coraz większym uznaniem cieszą się rozwiązania proste i łatwe w obsłudze,



Robert Gawroński, TP-Link Polska

Z pewnością zapotrzebowanie na rozwiązania z branży security będzie nadal rosnąć. Ewentualnym czynnikiem hamującym wzrosty może być zmniejszona dostępność i rosnące koszty kredytów. Trudno przewidzieć, co dokładnie wydarzy się w 2023 r. W ostatnich dwóch latach doświadczyliśmy trudności, o których wcześniej nikt nie myślał. Przykładem może być np. zablokowany na kilka tygodni Kanał Sueski. Brak komponentów nie dotknął nas tak bardzo w ubiegłych latach, jedynie zwiększony popyt spowodował krótkotrwałe problemy z dostępnością części produktów z naszej oferty. W tym roku nie spodziewamy się poważniejszych problemów z produkcją i dostępnością naszego sprzętu.



Robert Pestka, Polon-Alfa

Rok 2023 wygląda obiecująco. Jestem przekonany, że nasz nowy, adresowalny system sygnalizacji pożarowej POLON 3000, stworzony z myślą o małych i średnich obiektach, pozwoli na zwiększenie grona naszych klientów i dalsze umocnienie pozycji lidera, również w tym obszarze rynku. Bardzo trudno jest natomiast w obecnym czasie ocenić i dyskutować o zagrożeniach, które możemy zastać w przyszłości. Niepewność geopolityczna na świecie, wojna w Ukrainie, ciągle nieopanowana pandemia są czynnikami nieprzewidywalnymi. Każda ich analiza i próba przygotowania się może okazać się zarówno słuszną, jak i zupełnie nietrafioną. Niestety ten obszar niepewności zostanie z nami w tym roku.



Łukasz Kanarek, Roger

W naszej ocenie rynek kontroli dostępu w 2023 r. nadal będzie się rozwijał, jednak liczymy się z możliwą korektą i spadkiem wzrostu sprzedaży do poziomu kilku procent. Będziemy kontynuowali kilka naście projektów rozpoczętych w latach ubiegłych, głównie z uczelniami wyższymi, sektorem bankowym, szpitalami i infrastrukturą krytyczną. Po znacznym wzroście sprzedaży w roku 2021 w sektorze budownictwa biurowego w roku 2022 zaobserwowaliśmy niewielkie spowolnienie. Spodziewamy się, że spadkowy trend w tym sektorze będzie się utrzymywał również w roku bieżącym, jednak nie będzie on dla nas tak odczuwalny, ponieważ zwiększyliśmy swój udział w innych obszarach rynku. W pierwszej połowie 2023 r. planujemy rozpocząć sprzedaż nowego hybrydowego systemu RVOS, który będzie oferował popularne rozwiązania kontroli dostępu. W ofercie pojawi się również nowa linia wzornicza czytników oraz nowy kontroler przeznaczony do małych instalacji.



ale jednocześnie nowoczesne i umożliwiające sterowanie systemem za pośrednictwem aplikacji mobilnych. Według Artura Stępowskiego systemy GPS przechodzące kryzys od momentu zapaści na rynku motoryzacyjnym odnajdują się dzięki innym zastosowaniom, np. w sektorze profesjonalnych maszyn budowlanych i rolniczych czy całkowicie odmiennej branży motoryzacyjnej z motorami, skuterami, elektrycznymi rowerami i hulajnogami, które są łatwym łupem dla złodziei.

Klienci coraz częściej szukają rozwiązań zintegrowanych, którymi można zarządzać z jednego miejsca. Widoczne jest rosnące zainteresowanie kompleksowymi rozwiązaniami *end-to-end*, które umożliwiają stworzenie systemu zabezpieczeń integrującego kamery dozorowe, oprogramowanie zarządzające i kontrolę dostępu. Ten trend zauważa m.in. Axis Communications. – *Stale wzmacniamy i rozbudowujemy ofertę w tym zakresie* – wyjaśnia Dagmara Pomirska i podkreśla, że ogromnym zainteresowaniem cieszą się także funkcje analityczne w kamerach, które nie służą już tylko do przesyłania obrazu. Dzięki nim można zebrać istotne informacje z różnych aspektów naszego życia, np. ochrony zdrowia, poprawy jakości powietrza czy bezpieczeństwa w ruchu drogowym. Systematycznie rośnie zapotrzebowanie na rozwiązania z zakresu CCTV, konsumenci poszukują kamer wysokiej rozdzielczości wyposażonych w pakiety inteligentnych funkcji. Dostrzega to również Monika Stanosz z Suma Solutions. – *Największe zainteresowanie naszymi produktami zauważyliśmy w sektorze publicznym, który postawił na niezawodność i stabilność* – ocenia.

W minionym roku zwiększyło się także zainteresowanie kontrolą dostępu, zwłaszcza rozwiązaniami mobilnymi. – *Zaobserwowaliśmy*



Według danych statystycznych opublikowanych przez Komendę Główną Policji w 2022 r. doszło do 71 625 kradzieży z włamaniem, z czego wykryto sprawców 50,8% przestępstw.



W 2022 roku strażacy interweniowali ponad 608 tys. razy. Wystąpiło 135 968 pożarów, 424 956 miejscowych zagrożeń oraz 47 895 fałszywych alarmów.

wzrost zainteresowania klientów oferowaną przez nas kontrolą dostępu (wzrost o 12%) oraz wysoki popyt na kompleksowe rozwiązania dotyczące zabezpieczenia parkingów (10%). Praca zdalna spowodowała wzrost zainteresowania systemami opartymi na Web serwerze i rozwiązaniami w chmurze – mówi Marek Piotrowski.

Z kolei Łukasz Kanarek podkreśla: – *Rynek potrzebował narzędzia integrującego wszystkie systemy zabezpieczeń w jednym miejscu. Dlatego też w drugiej połowie 2022 r. wprowadziliśmy do oferty nową wersję systemu RACS 5 v2 wzbogaconą o zaawansowany moduł wizualizacji pozwalający na centralne wizualizowanie systemów pożarowych oraz współpracę z systemami CCTV* – mówi.

Anna Twardowska zauważa, że z perspektywy Nedap Security Management największy wzrost inwestycji odnotowano w sektorze infrastruktury krytycznej, co jest w jej opinii dobrym znakiem, ponieważ firmy tego sektora powinny mieć najlepsze rozwiązania w zakresie cybersecurity, także w zakresie systemów bezpieczeństwa. – *Widzimy, że organizacje, które do tej pory używały kart bez szyfrowania, dokonują zmian na bezpieczne technologie. Coraz częściej przy wyborze systemów kontroli dostępu wymagany jest Grade 4 według europejskiej normy EN60839-11-1 dotyczącej systemów kontroli dostępu* – wyjaśnia.

Kolejną kategorią, w której nastąpiła pewna zmiana w postrzeganiu ich znaczenia, są systemy przeciwpożarowe. Zmiana ta dotyczy szczególnie końcowych odbiorców systemów ppoż. Okazuje się, że niezawodny system sygnalizacji pożarowej przestał być traktowany jako zbędny koszt, który musi ponieść inwestor. Firmy dostrzegają, że jest to inwestycja w bezpieczeństwo własnego biznesu, budowanie marki i przewagi konkurencyjnej.

– *Konsumenci poszukują dobrych, sprawdzonych rozwiązań, które spełnią te wymagania przez kolejne lata, a nawet dziesiątki lat, jak w przypadku produkowanych przez nas urządzeń* – zauważa Robert Pestka.

Do podobnego wniosku dochodzi Michał Sidor: – *W roku 2022 obserwowaliśmy zwiększony popyt na wysokiej klasy rozwiązania techniczne w branży bezpieczeństwa pożarowego. Dało się też*

zauważyć duży wzrost zainteresowania rozwiązaniami umożliwiającymi zdalny nadzór nad bezpieczeństwem pożarowym budynków. Powodzeniem wśród klientów końcowych cieszyły się certyfikowane systemy integrujące urządzenia przeciwpożarowe (SIUP), co przełożyło się na znaczny wzrost wdrożeń naszego systemu SIS-FIRE. Kompleksowe rozwiązania cieszą się uznaniem, szczególnie w sektorze przemysłowym, który obok sektora obiektów magazynowych miał największy udział w naszej sprzedaży w 2022 roku.

Cyberprzestępcy kontra cyberochrona

Liczba cyberataków na całym świecie konsekwentnie rośnie. Do tego stanu przyczyniła się m.in. rosnąca popularność pracy zdalnej. W związku z tym zabezpieczenia infrastruktury sieciowej były jednym z najczęściej wybieranych rozwiązań. Rośnie też świadomość klientów w zakresie cyberbezpieczeństwa.

– *Technologia analityczna, sztuczna inteligencja wspomagają pracę człowieka w zabezpieczeniu obiektów i ułatwiają współpracę z użytkownikiem. Jest to trend, który będzie się rozwijać przy jednoczesnym wykorzystaniu instalacji w „chmurze” prywatnie czy też komercyjnej* – podkreśla Artur Hejdysz. Łączy się z tym znacznie większe zapotrzebowanie na urządzenia z obszaru security i IT. Podobne spostrzeżenie poczynił Robert Gawroński, którzy przyznał, że w zasadzie we wszystkich kategoriach produktowych TP-Link odnotował kilkudziesięcioprocentowe wzrosty. Przy czym, jak podkreśla, nabywcami były zarówno korporacje czy instytucje publiczne realizujące duże projekty, jak i mniejsze firmy instalacyjne obsługujące odbiorców indywidualnych, modernizujących infrastrukturę w domach jednorodzinnych.

Jest popyt, rośnie rynek

Sytuacja ekonomiczna, inflacja, wojna to elementy, które w istotny sposób wpływają na sytuację gospodarczą, m.in. wzrost przestępczości, który generuje straty. Dlatego firmy ochrony nadal będą miały co chronić. Krzysztof Bartuszek nie ma wątpliwości. – *Popyt na ochronę jest, choć nie nazwałbym go istotnie rosnącym. W trudnych czasach ochrona zaczyna być traktowana poważniej, a to ma wpływ zarówno na zapotrzebowanie, jak i na zmienne oczekiwania co do samej efektywności zastosowanych rozwiązań. Ochrona fizyczna oparta na pracy człowieka jest coraz droższa, a i rozwiązania, jakie może zaoferować, mają pewne ograniczenia. Dlatego też innowacyjność zaczyna być w cenie. Obserwujemy wzrost zainteresowania usługami z zaangażowaniem narzędzi, które mogą ograniczać czynnik ludzki w miejscach, gdzie do tej pory występowało zapotrzebowanie na proste usługi ochrony. Głównym celem nie są jednak oszczędności, ale optymalne wykorzystanie możliwości, jakie daje rewolucja przemysłowa i zwiększenie efektywności ochrony* – podkreśla.

Technologia zmienia świat. W codziennym życiu spotykamy już samoobsługowe kasy w sklepie, możliwość samodzielnego zameldowania się w hotelu czy roboty sprząające. Naturalną kolejną rzeczą jest wdrażanie najnowszych rozwiązań do systemów zabezpieczeń technicznych.

– *Często byłem świadkiem ożywionej dyskusji, czy technologia zastąpi człowieka i czy pracownicy uważają ją za zagrożenie. Z doświadczeń ostatnich lat widać, że rozwiązania z zastosowaniem najnowszych technologii są koniecznością, aby zapewnić najwyższy poziom bezpieczeństwa i ułatwić pracę wielu osobom, np. operatorom w centrum monitoringu* – mówi Harald Dingemans z Linc Polska. ●



Marek Piotrowski, ZKTeco

W tym roku przewidujemy niewielki wzrost sprzedaży (ponad poziom inflacji), o ile nie wystąpią kolejne nieprzewidziane negatywne zjawiska. Dalsza eskalacja konfliktu w Ukrainie czy tworzenie nowych ognisk konfliktów zbrojnych spowoduje wzrost zainteresowanie produktami przeznaczonymi dla wojska i innych służb mundurowych. Blisko spokrewnione z tymi służbami działy bezpieczeństwa obiektów infrastruktury krytycznej powinny zainteresować się bliżej produktami z naszego sektora.



Michał Sidor, Schrack Seconet Polska

Z miesiąca na miesiąc widzimy poprawę stabilności dostaw i wierzymy, że rok 2023 nie przyniesie żadnych niespodzianek i cała branża wróci do szeroko pojętej normalności. Niewątpliwie należy się spodziewać coraz większej ekspansji rozwiązań sztucznej inteligencji (AI), która będzie zwiększać niezawodność i funkcjonalność szeroko pojętego bezpieczeństwa. Polski rynek będzie jednym z tych, w których nowe technologie i rozwiązania będą pojawiać się na początku. Snując przewidywania co do roku 2023, nie sposób nie uwzględnić tego, co będzie się działo w światowej polityce. A ponieważ sytuacja jest tak dynamiczna, zostawię prognozowanie specjalistom.



Harald Dingemans, Linc Polska

W przyszłości będziemy widzieć coraz więcej autonomicznych rozwiązań stosowanych do zabezpieczeń, np. drony, roboty sprząające w centrach handlowych lub dużych biurach. Wzrośnie zapotrzebowanie na rozwiązania w chmurze, które łączą sygnały z wielu czujników i mogą podejmować decyzje automatycznie.



Artur Hejdysz, C&C Partners

Pytanie o perspektywę rozwoju polskiego rynku security nie jest łatwe. Jako C&C Partners pracujemy nad wieloma ciekawymi projektami, które będą realizowane w najbliższych latach. Kontynuujemy współpracę ze strategicznymi klientami. Natomiast nowe kontrakty z zakresu infrastruktury krytycznej czy inwestycje prywatne stoją, moim zdaniem, pod dużym znakiem zapytania. Uważam, że niestabilność ekonomiczna spowoduje spowolnienie rynku w perspektywie krótkoterminowej, natomiast zmieniająca się technologia, zagrożenia wewnętrzne i skracające się łańcuchy dostaw będą pozytywnie stymulować nasz wzrost w przyszłości.



Security się zbroi

Przed nami rok pełen wyzwań



Michał Badke
Regional Loss Prevention
Specialist w Allegro



Tomasz Grzelak
inspektor
ds. bezpieczeństwa w DPD



Mateusz Jurczyk
specjalista ds. bezpieczeństwa
fizycznego w Comarch



Wojciech Kawa
specjalista ds. bezpieczeństwa
w Volkswagen



Marek Malczewski
Security Manager
w Banku Millennium



Patryk Polt
Komendant Straży Miejskiej
w Łodzi



Ireneusz Rupik
specjalista ds. bezpieczeństwa
w Grupie TAURON



Piotr Sitko
z-ca dyrektora Biura Ochrony
i Bezpieczeństwa w PWPW

Podniesienie płacy minimalnej, wzrost poziomu przestępczości w odpowiedzi na coraz trudniejszą sytuację gospodarczą oraz niepewna sytuacja geopolityczna, a wraz z nią zwiększone ryzyko cyberataków – to najważniejsze wyzwania, z jakimi w tym roku będą się mierzyć szefowie bezpieczeństwa.

Michalina Nowak, a&s Polska

Niemal wszyscy, z którymi rozmawialiśmy, spodziewają się, że najbliższe miesiące przyniosą zwiększenie wydatków na systemy zabezpieczeń.

Płaca minimalna – maksymalne skutki

W roku 2023 płaca minimalna zostanie podniesiona aż dwa razy. Od stycznia br. minimalne wynagrodzenie wyniosło 3490 zł brutto. Druga podwyżka do 3600 zł brutto nastąpi w lipcu. Będzie to miało ogromne znaczenie dla rynku pracy i przełoży się na duże zmiany w sposobie funkcjonowania branży. – Tak dużej podwyżki płacy minimalnej nie było od 2015 r. i wiele firm nie doszacowało jej skali w analizach. Pytanie brzmi, na ile agencje ochrony będą w stanie utrzymać stan liczbowy pracowników, dostosować się do prawa i nowych

regulacji dotyczących najniższej krajowej pensji oraz zaoferować konkurencyjne stawki zleceniodawcom – zastanawia się Mateusz Jurczyk, specjalista ds. bezpieczeństwa fizycznego w firmie Comarch.

Oprócz kolejnej podwyżki minimalnego wynagrodzenia rynek od lat boryka się również z niedoborem pracowników. – Sytuacja na rynku pracy i związane z nią rosnące koszty zatrudnienia oraz trudności w pozyskaniu wykwalifikowanych pracowników mogą rzutować na jakość dostarczanych przez agencje ochrony usług i bezpieczeństwo procesów w 2023 r. – ocenia Michał Badke, Regional Loss Prevention Specialist w Allegro.

Zmiana minimalnego wynagrodzenia może mocno wpłynąć na kondycję finansową firm ochrony. Do stołu negocyjacyjnego ze swoimi kontrahentami będą siadać dwukrotnie w ciągu zaledwie kilku miesięcy.

→ – Prowadzone na koniec 2022 r. procesy renegotiacji umów lada dzień będą wznawiane. Od marca trzeba będzie planować waloryzację kontraktów o następną podwyżkę płacy minimalnej zaplanowaną od lipca 2023. Niektóre firmy będą zmuszone do wypowiedzania umów i redukcji zatrudnienia. Pomimo zmiany wysokości uposażeń konieczne będzie zapewnienie ciągłości działania i utrzymania wysokich standardów usług świadczonych klientom przez firmy ochrony – ocenia Wojciech Kawa, specjalista ds. bezpieczeństwa w Volkswagen.

Realne obawy o wzrost przestępczości

Sytuacja w Polsce nie napawa optymizmem. Nie każdy ekonomista wprowadzie określa ją mianem kryzysu gospodarczego, ale z pewnością nie będzie to łatwy rok – przy rekordowo wysokiej inflacji i bardzo wysokich kosztach kredytów poziom życia Polaków będzie się obniżał. W związku z tym pojawią się wyzwania, z którymi będą się mierzyć security menedżerowie.

» Trudna sytuacja gospodarcza może wpłynąć na wzrost bezrobocia i większy poziom ubóstwa w Polsce. To niestety zawsze skutkuje wzrostem przestępczości. «

– Obecna sytuacja gospodarcza w kraju pozwala zaobserwować narastającą tendencję zdarzeń o charakterze rozbójniczym – zauważa Marek Malczewski, security menedżer w Banku Millennium. Jego zdaniem należy przygotować się na trudny pod tym względem rok. Podobnie uważa Patryk Polit, komendant Straży Miejskiej

w Łodzi. – Trudna sytuacja gospodarcza może wpłynąć na wzrost bezrobocia. Sprawi również, że zwiększy się poziom ubóstwa w Polsce, a to zawsze idzie w parze ze wzrostem szeroko pojętej przestępczości. To najważniejsze wyzwanie, z którym będziemy musieli się zmierzyć, jako odpowiedzialni za bezpieczeństwo obywateli w miastach – mówi.

Obawy o większą liczbę incydentów wyraża również Michał Badke z Allegro. Odpowiedź na oszustwa i kradzieże musi być stanowcza i adekwatna do czasów.

– Trudne czasy skłaniają przestępców do jeszcze większej kreatywności, a to oznacza, że aby skutecznie przeciwdziałać zagrożeniom i być o krok przed wszelkiej maści oszustami, będziemy musieli niejednokrotnie zrewidować utarte schematy zabezpieczeń i zacieśnić współpracę z dostawcami usług i technologii – zapowiada.

Sz szczególnie narażeni na drobne oszustwa, ale też zakrojone na szeroką skalę kradzieże danych są klienci e-commerce i firm logistycznych.

– Nie możemy lekceważyć dobrze nam znanych mechanizmów, czyli ludzi podszywających się pod pracowników firm logistycznych lub kurierskich, którzy wysyłają fałszywe informacje o konieczności dopłaty określonej kwoty do zamówionej paczki. Wzrost bezrobocia oraz zubożenie społeczeństwa może tylko zwiększyć tego typu incydenty, dlatego musimy być czujni – podkreśla Tomasz Grzelak, inspektor ds. bezpieczeństwa w DPD.

Gdzie człowiek nie może, tam robota pośle

Brak rąk do pracy, wysokie koszty zatrudnienia i niepewna sytuacja gospodarcza w Polsce mogą być źródłem nie tylko obaw i problemów – dają także nadzieję na kolejny skok technologiczny.

– Obecna sytuacja, czyli stan podwyższonego zagrożenia i spadek poczucia bezpieczeństwa uzasadniają przyspieszenie pewnych zmian. Należy zapewnić wsparcie pracowników ochrony fizycznej środkami technicznymi, a w konkretnych sytuacjach nawet ich zastępowanie poprzez odpowiednie systemy – wyjaśnia Ireneusz Rupik, specjalista ds. bezpieczeństwa w Grupie TAURON.

Według najnowszego raportu World Robotics 2022 Międzynarodowej Federacji Robotyki (International Federation of Robotics – IFR) w ubiegłym roku w zakładach na całym świecie pojawiło się 517 385 nowych robotów przemysłowych. Oznacza to wzrost o 22% wobec rekordowego dotychczas roku 2018 r.

– Z powodu rekordowo niskiego bezrobocia są trudności w pozyskaniu odpowiednich kandydatów do pracy w sektorze ochrony mienia, w szczególności w przypadku kwalifikowanych pracowników ochrony z bronią, pracowników grup interwencyjnych, konwojentów czy operatorów systemów zabezpieczenia technicznego. Jednym z rozwiązań jest rozszerzanie usług ochrony o rozwiązania techniczne. Mogą być one receptą na czas kryzysu. To realna alternatywa dla tradycyjnych sprawdzonych rozwiązań, umożliwiająca też redukcję kosztów. Należy jednak pamiętać, że takie narzędzia powinny być zawsze precyzyjnie dopasowane do zagrożeń i specyfiki ochranianej branży. Inteligentne systemy bezpieczeństwa jeszcze długo nie będą w stanie całkowicie zastąpić człowieka. W krytycznych momentach to ocena sytuacji i decyzja pracownika ochrony

jest kluczowa dla działania adekwatnego do zagrożenia – ocenia Wojciech Kawa.

Globalny rynek automatyzacji procesów na świecie przekroczy 24 mld dolarów w 2030 r. – przewiduje Strategic Market Research. To kierunek, w którym zmierza cały świat.

– Dynamiczny rozwój narzędzi i algorytmów ML/AI, przenikających wręcz niepostrzeżenie do życia codziennego, stwarza szereg interesujących szans dla branży. Poczynając od automatyzacji detekcji zagrożeń, poprzez analizę machine data w poszukiwaniu anomalii, skończywszy na narzędziach wspierających podejmowanie decyzji. Te narzędzia mogą przynieść ogromne korzyści, szczególnie w dużych, rozproszonych geograficznie strukturach, w których liczba zdarzeń oraz poziom złożoności współzależnych elementów wymaga obecnie dużych nakładów pracy wykwalifikowanego personelu – podkreśla Marek Malczewski.

Zwraca także uwagę na fakt, że technologia niesie pewne inherentne zagrożenia. Jej fundamentem są rozwiązania informatyczne, same w sobie obciążone dużą liczbą zagrożeń i wysokim ryzykiem.

– Trzeba uważać na zjawisko uzależnienia technologicznego oraz pokładania przesadnej wiary w technologię. Zagrożeniom o charakterze fizycznym nie sposób przeciwdziałać wyłącznie wirtualnie. Do tego dochodzi kwestia naruszenia praw osobistych i prywatności – wiele z zaawansowanych narzędzi w tej chwili wymaga olbrzymich zasobów obliczeniowych, które często są realizowane w chmurze. Pokusa wykorzystania takich rozwiązań może doprowadzić do wycieku informacji lub złamania stosownych dyrektyw mających chronić dane osobowe. Sama technologia z pewnością zostanie kreatywnie wykorzystana przez przestępców (co już w praktyce ma miejsce), ale z pełną skalą tego zjawiska dopiero przyjdzie nam się zmierzyć. Techniki takie jak deep fake, symulacja głosu oraz generowanie obrazu, wraz ze wzrostem poziomu wyrafinowania i dostępnością narzędzi, będą coraz częściej służyły wyłudzeniom i oszustwom – podsumowuje Marek Malczewski.

W dobie rewolucji przemysłowej 4.0 automatyzacja jest obecna w każdym sektorze gospodarki. Transport i logistyka zasługują na miano liderów głównie za sprawą pandemii. To ta gałąź gospodarki będzie również coraz chętniej korzystała z rozwiązań technicznych w branży security.

– Logistyka to m.in. odpowiednie zarządzanie dostarczaniem do klientów milionów paczek na całym świecie, dlatego tak ważna jest kontrola nad tym procesem od nadawcy do odbiorcy, z zapewnieniem odpowiedniego poziomu bezpieczeństwa. W usprawnieniu tego procesu z pewnością bardzo pomocna będzie automatyzacja, która może zapewnić jeszcze lepszą kontrolę nad dystrybucją przesyłek. Systemy do odczytu tablic rejestracyjnych, automatyczne awizacje, inteligentne systemy wizyjne z pewnością pomogą firmom stworzyć bezpieczny i zautomatyzowany proces zarządzania towarami i w nich upatruję dużej szansy na rozwój w najbliższym roku – podkreśla Tomasz Grzelak.

W obliczu wojny i cyberwojny

O działaniu w cieniu wojny w Ukrainie branża bezpieczeństwa mówi od miesięcy. Lada dzień minie dokładnie rok od rozpoczęcia

» Od października 2022 r. liczba cyberataków wzrosła dwukrotnie – z 1214 prób tygodniowo do rekordowego poziomu 2316. «

rosyjskiej agresji. Sporo lekcji w ciągu tych 12 miesięcy już odrobiliśmy, ale wciąż mamy przed sobą kolejne związane z tym wyzwania.

– Żyjemy w cieniu konfliktu za naszą wschodnią granicą, który być może nie ma już tak medialnej nośności jak w ubiegłych miesiącach, ale należy spodziewać się, że na wiosnę może wkroczyć w nowy etap i wpłynąć na sytuację w kraju. Potencjalny pobór rezerwistów może w znacznym stopniu ograniczyć nie tylko dostępność usług ochrony fizycznej, ale także potencjał całej branży. Dalszy rozwój konfliktu odbije się na nastrojach społecznych, zapotrzebowaniu na pewne kategorie dóbr, a także dostępie do gotówki. Wraz ze wspomnianym wcześniej zaburzonym potencjałem branży ochrony oraz usług powiązanych może przynieść kaskadowy efekt, stwarzający unikatowe wyzwania o dużym wpływie i skali. Korzystając z już nabytych doświadczeń z ubiegłego roku, należy zrewidować plany ciągłości działania oraz zarządzania kryzysowego – ocenia Marek Malczewski.

Choć mija rok, Polska wciąż boryka się z ogromnym problemem związanym z napływem imigrantów.

– Ich uwarunkowania kulturowe, regulacje prawne i przyjęte zwyczaje różnią się od polskich na tyle, że musimy liczyć się z tym, że będziemy coraz częściej wchodzić w interakcję z obywatelami Ukrainy. Zdarza się, że pewne zachowania, które u nas są społecznie nieakceptowalne, u nich są traktowane z przyzwyczajeniem, a wtedy musimy reagować. Nasza chęć pomocy jest olbrzymia, ale należy pamiętać, że ład, porządek i przepisy prawne obowiązują wszystkie osoby, które przebywają na terytorium naszego kraju. Upatruję jednak w tym także szansy do rozwoju, ponieważ my, jako Straż Miejska w Łodzi, rozpoczęliśmy kurs języka ukraińskiego – podkreśla Patryk Polit.

Czujność – to słowo klucz wielu „bezpieczników”, z którymi rozmawiamy o wyzwaniach na 2023 r. Pada ono najczęściej w kontekście cyberzagrożeń, z którymi muszą się liczyć wszyscy bez wyjątku. Od wybuchu wojny w Ukrainie nasz kraj jest jednym z kluczowych celów cyberprzestępców. Izraelska firma Check Point Research alarmuje, że od października 2022 r. liczba cyberataków wzrosła dwukrotnie – z 1214 prób tygodniowo do rekordowego poziomu 2316.

» Wydatki na projekty związane z poprawą bezpieczeństwa fizycznego obiektów, w tym obiektów infrastruktury krytycznej, będą w tym roku rosły. «

→ Dużym wyzwaniem jest to, co dzieje się za naszą wschodnią granicą. Będziemy dbali o to, żeby obiekty infrastruktury krytycznej były przygotowane na różne ewentualności związane z toczącą się wojną. Kolejna kwestia to sprawy związane z cyberbezpieczeństwem. Widzimy, że tych zagrożeń jest coraz więcej, i też pracujemy nad tym, aby jak najlepiej stać na straży bezpieczeństwa danych, którymi operujemy w Polskiej Wytwórni Papierów Wartościowych – mówi Piotr Sitko, PWPW, zastępca Dyrektora Biura Ochrony i Bezpieczeństwa.

Jak podają eksperci Noventiq, Polska zajmuje szóste miejsce w Europie pod względem zagrożeń cybernetycznych, obok Węgier, Cypru, Słowacji, Estonii i Białorusi. Dane wskazują, że w 2022 r. polskie firmy doświadczały ataków hakerskich średnio co 9 minut.

W kontekście cyberbezpieczeństwa i w dobie przemysłu 4.0 powinno dojść do integracji systemów zabezpieczenia na poziomie systemów kontroli dostępu, monitoringu CCTV, systemów alarmowych i przeciwpożarowych, infrastruktury produkcyjnej i budynkowej – podkreśla Wojciech Kawa.

Rok zakupów w security

Lista wyzwań stojących przed security menedżerami w 2023 r. jest bardzo długa. Oznacza to rok wzmożonej aktywności, ale też zakupów.

Wydatki na projekty związane z poprawą bezpieczeństwa fizycznego obiektów, w tym obiektów infrastruktury krytycznej, będą w tym roku rosły – prognozuje Ireneusz Rupik.

Rok 2023 przyniesie także rozwój narzędzi prewencji i ścigania, a co za tym idzie ogólną poprawę bezpieczeństwa.

Można powiedzieć, że 2023 r. będzie oznaczał zwiększenie wydatków na bezpieczeństwo w naszym sektorze – dodaje Michał Badke.

Tej pewności nie ma jednak Wojciech Kawa. Podkreśla on, że w dobie kryzysu potrzebne jest nieco szersze spojrzenie na bezpieczeństwo. Z uwagi na wysokie koszty funkcjonowania przedsiębiorstw w 2023 r. może dochodzić do racjonalizacji i optymalizacji kosztów, m.in. wydatkowanych na ochronę i bezpieczeństwo, ale rozwiązania techniczne, o czym mówiliśmy wszyscy, mogą stanowić realną alternatywę dla tradycyjnych rozwiązań.

Całościowe podejście do koncepcji ochrony opiera się na najnowocześniejszych technologiach oraz wynika z norm prawnych i obowiązujących standardów.

Punktem wyjścia do prac związanych ze wzmocnieniem ochrony procesów i danych w przemyśle jest podejście uwzględniające koncepcję tzw. głębokiej ochrony, czyli Defense in depth, która oznacza kompleksowe podejście do bezpieczeństwa. Ochrona informacji i ciągłości procesów przemysłowych musi zacząć się od audytu i oceny stanu bezpieczeństwa. Strategia głębokiej ochrony opiera się na trzech głównych zasadach i politykach bezpieczeństwa. Są to: ochrona integralności sieci ogólnej z siecią produkcyjną, wprowadzenie stref szczególnej ochrony oraz zabezpieczenie fizycznego dostępu do infrastruktury. Ponadto w należyty sposób należy zabezpieczać łańcuch dostaw przed kradzieżami i innymi zagrożeniami w transporcie, a także prowadzić politykę szkoleniową dla pracowników, aby uświadamiać im zagrożenia. To kosztuje, ale zapewnia ciągłość działania przedsiębiorstwa. Odpowiednio przygotowane procedury i procesy bezpieczeństwa stają się spoiwem łączącym usługę bezpieczeństwa ochrony z procesami biznesowymi. Poniesione na ten cel nakłady finansowe przestają być jedynie pozycją kosztową w budżecie, a stają się inwestycją w rozwój firmy – twierdzi Wojciech Kawa.

Nie wszyscy security menedżerowie są optymistyczni w kwestii wydatków na bezpieczeństwo, choć każdy podkreśla ich zasadność.

Niestety szukając oszczędności, firmy mogą chcieć ograniczać swoje budżety na bezpieczeństwo. Z pewnością wzrost płacy minimalnej, a co za tym idzie wzrost stawki za roboczogodzinę może spowodować redukcję etatów wśród pracowników ochrony. Jednocześnie być może to właśnie idealny moment na inwestycję w zabezpieczenia techniczne, automatyzację i specjalizację pracowników. Należy pamiętać, że często pozorne oszczędności mogą przynieść nam więcej szkody niż pożytku, a życie lub zdrowie ludzkie jest po prostu bezcenne, dlatego przestrzegalbym przed wielkimi cięciami budżetów i ograniczaniu wydatków na bezpieczeństwo – zaznacza Tomasz Grzelak.

Warto zauważyć, że raz wydane fundusze będą przynosić oszczędności przez kilka lub nawet kilkanaście kolejnych lat. ●

Linc
Polska Sp. z o.o.

MAGOS

SR-150
MAŁY RADAR
O DUŻYCH
MOŻLIWOŚCIACH

KORZYŚCI TECHNOLOGII RADAROWEJ:



ZASIĘG DETEKCJI

150 m człowiek / pojazd



KĄT POKRYCIA

120° w poziomie, 30° w pionie,
połączenie 3 radarów daje
pełne pokrycie 360°



DOKŁADNOŚĆ

poniżej 1m



PLUG & PLAY

łatwa instalacja
i wsparcie większości
kamer i VMS



HOLISTYCZNY SYSTEM

MASS jest integralną
częścią VMS



WYSOKA SKUTECZNOŚĆ

minimum fałszywych
alarmów niezależnie
od warunków pogodowych



TECHNOLOGIA AI

rozpoznawanie i identyfikacja
intruzów z wykorzystaniem
technologii AI



Przewidywanie jest bardzo trudne,
szczególnie jeśli idzie o przyszłość

Niels Bohr, duński fizyk, noblista

Od sztucznej inteligencji przez metawersum do osobliwości

Jakie technologie zyskują na znaczeniu? Na jakie najważniejsze trendy firmy powinny zwrócić uwagę? Wszystko wskazuje na to, że AI będzie priorytetem, blockchain już okrzepł i nie wywołuje w liderach biznesu większych emocji. Obecnie tematem numer jeden są NFT i metawersum. Ważna jest także kwestia braków kadrowych, szczególnie dotkliwych dla polskiej branży logistycznej.

Monika Mamakis, a&s Polska

1

**ARTIFICIAL INTELLIGENCE,
CZYLI SZTUCZNA
INTELEGENCJA CORAZ MNIEJ
SZTUCZNA**

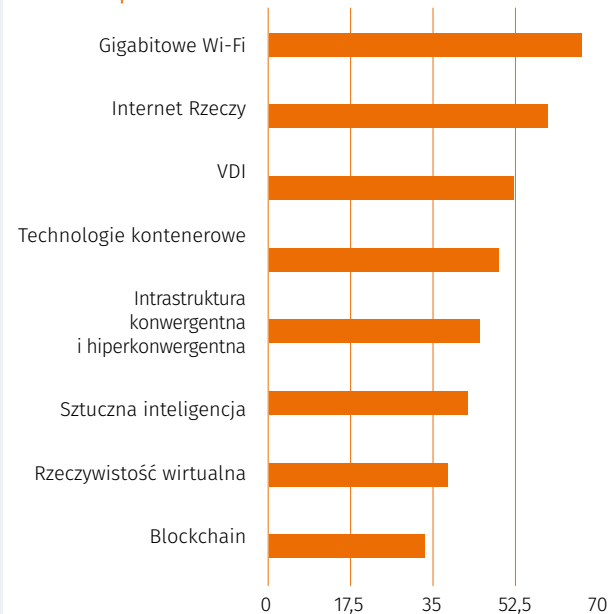
Sztuczna inteligencja (*Artificial Intelligence*, AI) stała się częścią codziennego życia, znajdując zastosowanie praktycznie wszędzie – od centrów obsługi klienta po algorytmy mediów społecznościowych. Na początku tego roku dużym medialnym echem odbiło się uruchomienie Chat GPT (*Generative Pre-trained Transformer*), czyli chatbota zaprojektowanego przez OpenAI w taki sposób, by tworzył teksty do złudzenia przypominające pisane przez ludzi. Owszem, ta konkretna AI jeszcze nie radzi sobie z tekstami specjalistycznymi, ale krótkie opisy produktowe wychodzą jej całkiem nieźle. Chat GPT pokazuje kierunek, w którym zmierza rozwój AI – będzie coraz bardziej ludzka.

Pojawiające się nowe generacje AI, tzw. adaptacyjne AI (*Adaptive AI*), są coraz mądrzejsze. Adaptacyjne AI wykorzystuje informacje zwrotne, analizując je w czasie rzeczywistym, aby uczyć się i dostosowywać swoje wyniki na bieżąco. Innymi słowy, adaptując się do zastanych warunków. Nie zastąpi ono funkcjonującego już modelu AI, ale jego stosowanie stanie się popularne w dynamicznie zmieniających się środowiskach, np. w firmach z branży TSL.

Jakie zagrożenie wiąże się z rozwojem AI? Według Gartner Group aż 41% badanych organizacji doświadczyło naruszenia prywatności AI lub incydentu związanego z bezpieczeństwem. Dlatego dla wielu organizacji istotnym wyzwaniem będzie teraz zarządzanie zaufaniem, ryzykiem i bezpieczeństwem sztucznej inteligencji (AI Trust, Risk and Security Management, AI TRISM). W miarę jak coraz więcej projektów AI przechodzi z fazy projektu do fazy rzeczywistego użycia, organizacje będą zabiegać o zapewnienie niezawodności modelu, wiarygodności wyników, bezpieczeństwa i ochrony danych.



Trendy w technologiach IT w USA i Europie na rok 2023



Tylko 35% respondentów odpowiadających na pytanie Statisty stwierdziło, że ich firma planuje wdrożenie rozwiązań bazujących na łańcuchu bloków. (Źródło: Statista.com)

2

BLOCKCHAIN

Czy popularność blockchaina zmaleje? Zdania w tej kwestii są podzielone. Zestawienie serwisu Statista nie pozostawia złudzeń. W zeszłym roku najpopularniejszym trendem informatycznym w krajach Ameryki Płn. i Europy była gigabitowa sieć Wi-Fi (czyli Wi-Fi 6), a następnie automatyzacja IT. Blockchain, który sprawdził się choćby w firmach z branży Fin-Tech czy TSL, wg Statisty nie będzie się cieszyć w roku 2023 szczególnym zainteresowaniem, a inwestycje w jego wdrożenie zmaleją.

Innego zdania są eksperci Business Research Company. Według nich światowy rynek usług blockchain wzrośnie z 3,28 mld USD w 2022 r. do 4,7 mld USD w 2023 roku i do oszałamiającej kwoty prawie 20 mld USD do 2027 r.

Dla branży TSL blockchain okazał się narzędziem niezwykle przydatnym. Łańcuch bloków zapisywanych w sposób zdecentralizowany i niepodatnych na manipulację umożliwia śledzenie i udokumentowanie każdej transakcji czy wymiany, jaka ma miejsce w łańcuchu dostaw. Blockchain może być wykorzystywany do rejestrowania w zasadzie wszystkich informacji dotyczących transportowanych towarów, magazynów, tras pojazdów itp. Oznacza to np. dokładniejsze śledzenie dostaw produktów i surowców. Weryfikacja łańcucha dostaw to jedno, ale dodatkowym wsparciem dla branży TSL mogą być inteligentne kontrakty (*smart contracts*), również wykorzystujące

blockchain. Temu rozwiązaniu warto się w roku 2023 uważnie przyjrzeć. Inteligentny kontrakt to program komputerowy, który pozwala na zawieranie i weryfikację umów pomiędzy stronami. Bez żadnego pośrednika i całkowicie zdalnie. Finalizacja takiej umowy następuje po spełnieniu określonego w programie warunku, typu „Jeśli przesyłka zostanie dostarczona i przyjęta bez zastrzeżeń, wykonaj przelew”.

3

CYBERBEZPIECZEŃSTWO – BARDZIEJ AKTYWNA OCHRONA PRZED ATAKAMI

W styczniu br. zespół CERT Polska donosił o pojawieniu się nowego wariantu klasycznego phishingowego oszustwa. Tym razem hakerzy wybrali metodę „na Ministerstwo Finansów”. Oszuści przekierowują ofiary do fałszywej strony internetowej, by wyłudzić dane bankowe pod pozorem udzielenia jednorazowego świadczenia finansowego.

Phishing jest jednym z najbardziej popularnych rodzajów ataków dokonywanych przez cyberprzestępców. Według raportu sporządzonego przez Slashnext, organizację zajmującą się zwalczaniem tego typu zagrożeń, w 2022 r. przeprowadzono ponad 225 mln ataków phishingowych (sic!). Autorzy raportu podkreślają, że dotychczasowe sposoby zapobiegania atakom, takie jak firewalle i serwery proxy, przestają być skuteczne, ponieważ przestępcy coraz częściej przeprowadzają ataki z serwerów zaufanych oraz firmowych i osobistych aplikacji do przesyłania wiadomości. Dzieje się tak m.in. za sprawą rozpowszechnienia pracy zdalnej, ale też coraz większej popularności modelu *bring your own device* (BYOD), czyli wykorzystywania prywatnych urządzeń w ramach firmowej sieci.

Na co w takim razie powinny zwrócić uwagę firmy, które chcą się ustrzec przed atakiem, i jakie trendy, jeśli chodzi o cyberbezpieczeństwo, są wiodące? W tym celu powinny podjąć następujące działania:

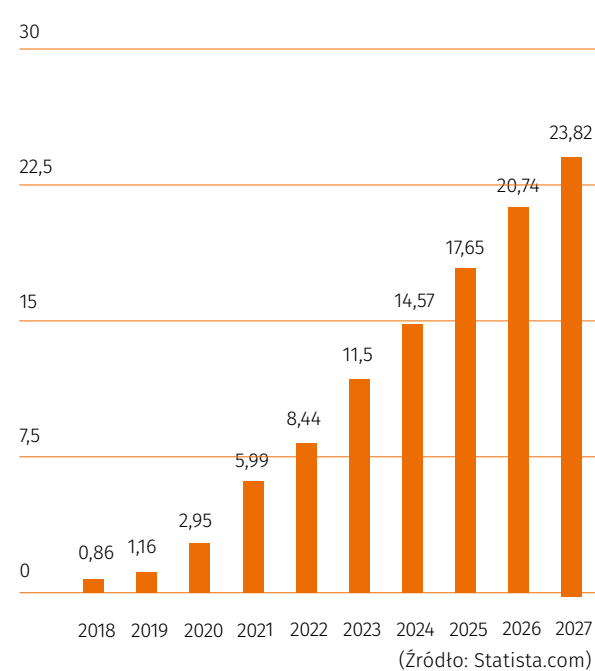
Zamiast VPN wprowadź politykę zero zaufania. Ekspert ds. cyberbezpieczeństwa radzą wdrażanie polityki *zero trust*, czyli „nigdy nie ufaj, zawsze weryfikuj”, co oznacza, że każdy dostęp do zasobów firmowych będzie wymagać pełnego, minimum dwustopniowego uwierzytelnienia i zostanie on ograniczony tylko do danych wynikających z restrykcyjnie nadanych uprawnień. Polityka „zero zaufania” wymaga wielokrotnej weryfikacji uprawnień użytkowników i autoryzacji za pomocą wielu różnych metod uwierzytelniania.

Stosuj narzędzia do predykcji zagrożeń i wczesnego reagowania. Nie warto pytać, czy dojdzie do cyberataku, tylko zastanowić się, kiedy do niego dojdzie i co wówczas się stanie. Jednym ze sposobów zapobiegania atakom jest identyfikacja nietypowej aktywności w całej infrastrukturze IT, w warstwie zarówno programowej, jak i sprzętowej. Na popularności zyskują więc narzędzia *Endpoint Detection and Response* (EDR). EDR umożliwiają wykrywanie i reagowanie na nietypowe, potencjalnie groźne działania w infrastrukturze IT. W wersji XDR dochodzi automatyczne nadawanie priorytetów alertom, a w niektórych przypadkach również możliwość definiowania automatycznych akcji.

Monitoruj ryzyko cybernetyczne ze strony partnerów. Wielu cyberprzestępców obchodzi wyrafinowane zabezpieczenia stosowane przez duże przedsiębiorstwa, włamując się do systemów

Liczba cyberataków rośnie i rosnać będzie

Estymowany koszt cyberprzestępczości globalnie (w mld USD)



(Źródło: Statista.com)

mniejszych organizacji obecnych w łańcuchach dostaw, które mają dostęp do tych samych platform co ich duzi partnerzy, ale niestety nie dysponują równie zaawansowanym systemem ochrony. Ataki na łańcuch dostaw w roku 2021 wzrosły czterokrotnie. Organizacje od dawna korzystają z aplikacji firm trzecich w celu zwiększenia produktywności, ale takie narzędzia mogą mieć szereg luk, które atakujący mogą wykorzystać, aby uzyskać dostęp do środowisk ofiar. Nic dziwnego, że powodzeniem cieszą się narzędzia służące do monitorowania ryzyka cybernetycznego ze strony mniejszych firm stanowiących kolejne ogniwa łańcucha dostaw.

4

CHMURY NA BIZNESOWYM NIEBIE

Obliczenia chmurowe stały się niezbędnym narzędziem dla biznesu, pomocnym w przechowywaniu i udostępnianiu danych. W zasadzie każda firma korzysta z jakiejś chmury: większe zazwyczaj z chmur prywatnych bądź hybrydowych, mniejsze – z publicznych. Kolejne lockdowny i praca zdalna przyspieszyły adaptację tego rozwiązania w przedsiębiorstwach. Nic dziwnego, ponieważ chmura obliczeniowa oznacza brak konieczności inwestycji we własną infrastrukturę IT. W zamian za odpowiednie kwoty firmy mają do dyspozycji, na wyciągnięcie ręki, wydajność olbrzymich serwerów, miejsce na dane, dostęp do wielu różnych aplikacji.

Jednocześnie coraz popularniejszy staje się związany z chmurą model ITaaS. W modelu ITaaS (*IT as a Service*) całą infrastrukturę IT, zarówno sprzętową, jak i oprogramowanie, zapewnia dostawca

zewnątrzny. Bez chmury taki model nie mógłby funkcjonować. Na ITaaS składa się infrastruktura traktowana jako usługa (IaaS), platforma jako usługi (PaaS) oraz oprogramowanie oferowane również w modelu usługowym (SaaS). Ogólnie biznes dąży do jak największej ilości usług świadczonych jako serwis.

Najważniejsze trendy w chmurze obliczeniowej, na które należy zwrócić uwagę w 2023 r., to rozwój usług wykorzystujących algorytmy AI oraz *machine learning*, coraz większa popularność platformy Kubernetes, a także rozwiązania wielochmurowe i chmury hybrydowe.

Te ostatnie zyskują na popularności w branży zabezpieczeń fizycznych. Badania pokazują, że w ciągu najbliższych dwóch lat 66% firm tego sektora przejdzie do zarządzania lub przechowywania większej ilości zasobów w chmurze. Nie wszystkie firmy chcą lub mogą (np. ze względu na obowiązujące w danym kraju prawo) przejść na infrastrukturę wyłącznie chmury. Wiele zależy od kwestii prawnych, możliwości inwestycyjnych, a nawet przepustowości łącza. Jednak niewiele firm zamierza pozostać tylko przy zasobach przechowywanych we własnych data center.

Na biznesowym niebie można się spodziewać pojawienia się jeszcze jednego rodzaju chmur. To chmury branżowe. Do roku 2027 ponad 50% przedsiębiorstw będzie korzystał z platform chmury branżowej, łączącej SaaS, PaaS i IaaS. Mogą one zapewnić firmom elastyczność i wydajność potrzebną, by wprowadzać innowacyjne, unikatowe rozwiązania skierowane do klienta, jednocześnie unikając uzależnienia od dostawcy chmury.

5

KOMUNIKACJA – WI-FI 6 JEST NA TOPIE

Komunikacja bezprzewodowa Wi-Fi 6 bazująca na standardzie IEEE 802.11ax zapewnia pojemność, wydajność, zasięg i wydajność oczekiwaną przez najbardziej nawet wymagających użytkowników. A tych przybywa wraz z coraz większą liczbą urządzeń Internetu Rzeczy (*Internet of Things*, IoT).

Od momentu wprowadzenia Wi-Fi w 1997 r. przez amerykańską organizację pozarządową Instytut Inżynierów, Elektryków i Elektroników (IEEE) jest to jedna z najpopularniejszych i najsukcesowniejzych technologii bezprzewodowych. Wi-Fi 6 (802.11ax) to najnowsza wersja standardu używanego do łączenia urządzeń z bezprzewodową siecią lokalną (WLAN). Pierwszą różnicą są szybkość i pojemność. W przeciwieństwie do poprzednich wersji tego protokołu Wi-Fi 6 wykorzystuje szerszy kanał do przesyłania danych (160 MHz zamiast 40 MHz) i tym samym umożliwia przesyłanie większych pakietów (2560 bajtów zamiast 1280 bajtów), co przekłada się na szybszą transmisję danych (powyżej 10 Gb/s). Daje to Wi-Fi 6 nawet czterokrotnie większą prędkość i pojemność w porównaniu z poprzednimi wersjami. Naturalnym środowiskiem, w jakim funkcjonuje Wi-Fi 6, są smartfony, tablety i komputery, ale jest ono używane przez wiele innych urządzeń, takich jak kamery monitoringu wizyjnego, bramki dostępowe, inteligentne urządzenia domowe czy systemy alarmowe. Dlatego niezwykle ważne jest to, że w najnowszej generacji tego standardu wprowadzono



kilka zmian mających na celu poprawę niezawodności i bezpieczeństwa. Wiele punktów dostępowych może teraz „rozmawiać ze sobą” bezpośrednio, bez przechodzenia przez router, jednocześnie korzystając ze scentralizowanego interfejsu zarządzania, pozwalającego m.in. na dynamiczne dostosowanie jakości usługi (*Quality of Service, QoS*) lub kształtowanie ruchu. Wi-Fi 6 jest też mniej podatne na zakłócenia, zwłaszcza w zatłoczonych miejscach, takich jak stadiony czy lotniska. Dla branży security to zdecydowanie dobra wiadomość.

6

TALENTY, A RACZEJ ICH BRAK

Branża security nie jest jedyną, która boleśnie odczuwa braki kadrowe. Pracodawcom nie sprzyjają pandemia, starzejące się społeczeństwo, wejście na rynek pracy specyficznego pokolenia Z, ale też zjawisko „cichych odejść” (*quiet quitting*), czyli sytuacji, w której pracownicy robią dokładnie tyle, ile muszą, nie angażując się w pracę. Zgodnie z danymi zawartymi w raporcie opracowanym przez Genetec 2022 State of Physical Security 50% respondentów stwierdziło, że ich zespół ds. bezpieczeństwa fizycznego napotkał w zeszłym roku wyzwania związane z zasobami ludzkimi. Liderzy borykali się z niedoborami personelu, trudnościami z zatrudnieniem i problemami z morale pracowników.

Remedium? Rozwiązania automatyzujące procesy i zwiększające wydajność zespołu. Ujednolicenie nadzoru wideo, kontroli dostępu, automatycznego rozpoznawania tablic rejestracyjnych, technologii komunikacyjnej i innych cennych funkcji może ułatwić pracę operatora. Zmniejsza to również koszty i szkolenia. Zespoły ds. bezpieczeństwa mogą jeszcze bardziej usprawnić operacje dzięki wbudowanym funkcjom analitycznym lub wspomagającym podejmowanie decyzji.

O ile w branży security można uzupełnić brak rąk do pracy, choćby częściowo, automatyzacją niektórych zadań, o tyle branża TSL może mieć kłopot. Już w lipcu 2021 r. firmy przewozowe biły na alarm, informując, że w Polsce brakuje ok. 150 tys. kierowców. Tutaj łatwego rozwiązania nie ma, a z pewnością nie są nim... ani drony, ani samochody autonomiczne.

Jak zauważają eksperci DHL, przygotowujący co dwa lata *The Logistics Trend Radar*, od prawie dekady mówi się, że drony mogłyby pracować dla organizacji logistycznych. I na mówieniu na razie się kończy. Barierą ich rzeczywistego zaangażowania są przepisy i technologia. Według autorów raportu drony mają na razie umiarkowany wpływ na logistykę, a ten stan może się zmienić najwcześniej za 5 lat, choć bardziej prawdopodobna jest kolejna dekada. Na razie drony są stosowane w niektórych miejscach na świecie, realizując dostawy na ostatniej mili. Pojazdy autonomiczne na radarze DHL nawet się nie pojawiły.

Brakuje nie tylko kierowców. Już w 2022 r. firmy z branży TSL narzekały na niedobór specjalistów ds. logistyki, specjalistów ds. planowania popytu oraz osób znających się na sprzedaży transportu (morskiego, lotniczego, drogowego) lub logistyce kontraktowej. I niestety wiele wskazuje na to, że w tym roku nie będzie

lepiej. Ten trend zapewne się utrzyma tak długo, jak długo za naszą wschodnią granicą będą trwać działania wojenne.

7

METAWERSUM

Do 2027 r. metawersum ma być wykorzystywane przez ponad 40% dużych organizacji na całym świecie. Połączenie Web3, chmury AR i cyfrowych bliźniaków w projektach funkcjonujących w metawersum ma oczywiście posłużyć zwiększeniu konkurencyjności na rynku. Firmy mogą wykorzystywać wirtualne światy do otwierania wirtualnych sklepów i showroomów w celu wystawiania produktów i reklamowania usług.

8

SUPERAPLIKACJE

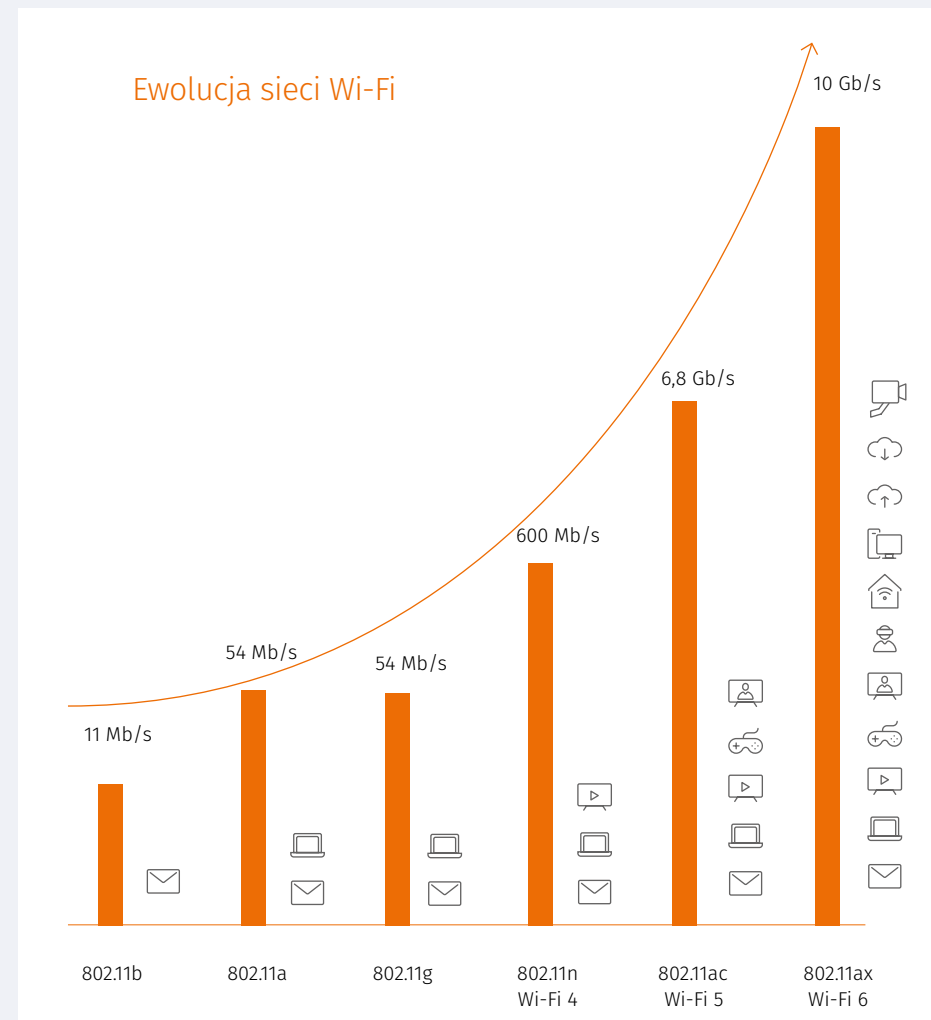
Te potężne aplikacje łączące cechy aplikacji mobilnej, platformy i biznesowego ekosystemu mają stać się dominującym rozwiązaniem w ciągu najbliższych 4 lat. Uważa się, że wszystkich superapps jest raptem 15. Jedną z nich jest Slack, drugą Microsoft Teams, ale najbardziej chyba znaną jest chiński WeChat. Wzrost ich popularności wynikał głównie z pracy zdalnej w pandemii.

9

APPLIED OBSERVABILITY, CZYLI OBSERWOWALNOŚĆ STOSOWANA

„Obserwowalność” jest słowem, które już w 2022 r. zaczęło robić karierę. Co ono oznacza? To zdecydowanie coś więcej niż monitoring sieci czy nadzór nad przepływem danych i pracą aplikacji. Obserwowalność pozwala na uzyskanie wglądu w systemy i zadawanie nowych pytań za pomocą metryk, logów lub śladów. W tym roku organizacje będą nadal wykorzystywać dane w celu usprawnienia procesu decyzyjnego, wykorzystując do tego właśnie proces zwany obserwowalnością. Decyzje będą podejmowane na bazie danych gromadzonych w całej organizacji, począwszy od wywołań interfejsu API, dzienników logów, przez czas przebywania użytkownika na stronie, każde działanie w punkcie styku z firmą będzie informacją wspomagającą podjęcie decyzji.

Ewolucja sieci Wi-Fi



10

ZABEZPIECZENIA TECHNICZNE – DUŻY RYNEK WRAŻLIWY NA ZAWIROWANIA

Zgodnie z danymi publikowanymi przez serwis Market Research Community globalna wielkość rynku zabezpieczeń technicznych została wyceniona na 102,3 mld USD w 2021 r., rejestrując CAGR na poziomie 6,5% w okresie prognozy (2022–2030), a do 2030 r. rynek ma osiągnąć wartość 180,3 mld USD. Niezależnie od wielkości jest to rynek również wrażliwy na różnego rodzaju zawirowania gospodarcze. Na branżę wpłynęły w ostatnich latach zarówno pandemia, jak i wojna w Ukrainie. Na co powinna przygotować się w tym roku?

Po pierwsze, coraz więcej organizacji modernizuje swoje systemy kontroli dostępu. Ostatnie badania wykazały, że 67% organizacji planuje inwestycję w modernizację kontroli dostępu, co pasuje do rozwiązanie na szczycie listy inwestycji technologicznych. Nowoczesne rozwiązania kontroli dostępu zapewniają wiele wbudowanych narzędzi

do cyberobrony i monitorowania stanu. Oferują również wyższy poziom automatyzacji w celu usprawnienia zadań kontroli dostępu.

Po drugie, wiele przedsiębiorstw już zauważyło, że monitoring wizyjny, kontrola dostępu i inne systemy zabezpieczeń technicznych to źródło cennych informacji. Jednak połączenie zbiorów danych pochodzących z różnych systemów pozwala na odkrycie niewidocznych na pierwszy rzut oka zależności i wprowadzenie rzeczywistych zmian w operacjach biznesowych. Przykładowo większość organizacji ma zainstalowany system dozoru wizyjnego, ale nieliczne potrafią „wyciągnąć” z tego faktu biznesową korzyść.

Po trzecie, IT i security zaczynają walczyć ramię w ramię z security. (O tym trendzie szerzej w artykule *Ochrona fizyczna i IT...* Tomasz Dacki, s. 74). Niwelowanie różnic pomiędzy zabezpieczeniami elektronicznymi a systemami informatycznymi jest bowiem coraz częstszym pomysłem na zapewnienie firmie pełnej ochrony. W miarę rozwoju Internetu rzeczy (IoT) i wzrostu zapotrzebowania na mobilność podatność na ataki będzie rosła. W tym roku coraz więcej organizacji będzie poszukiwać rozwiązań zapewniających skonsolidowany obraz zabezpieczeń technicznych i cyberbezpieczeństwa. Będziemy świadkami ściślejszej współpracy między zespołami security i cyberochrony, a nawet w pełni połączonych zespołów IT i zabezpieczeń technicznych. Wspólna praca zwiększy świadomość sytuacyjną i ograniczy ryzyko w całej organizacji. ●



Sześć kluczowych trendów technologicznych, które wpłyną na branżę security

Branża security wykorzystuje coraz bardziej inteligentne technologie, co jest nierozdzielnie związane z gromadzeniem danych wrażliwych. Jednocześnie, podobnie jak na inne dziedziny gospodarki, mają na nią wpływ zawirowania geopolityczne. Tegoroczne trendy dotyczące tej branży dotyczą przede wszystkim holistycznego podejścia do zagadnień ochrony firm.

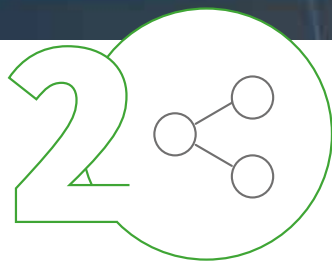


Analityka olbrzymich ilości danych, by ułatwić podejmowanie decyzji

Rosnące zastosowanie AI i uczenia maszynowego sprawiło, że w ostatnich latach skupiono się na możliwościach zaawansowanej analityki. W przyszłości nacisk zostanie przeniesiony na wykorzystanie wyników analizy do podejmowania decyzji. Nie chodzi bowiem o to, by wiedzieć, że coś jest nie tak, ale o to, by użytkownikowi ułatwić podjęcie decyzji.

Podstawowym powodem przemawiającym za zastosowaniem analityki jest ogromny wzrost ilości danych generowanych m.in. przez kamery dozoru wizyjnego. Ilość i charakterystyka gromadzonych danych powodują, że pracownik nie jest w stanie ich zinterpretować ani poddać ich analizie we właściwym czasie.

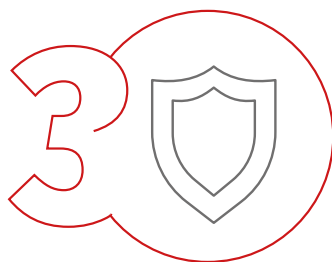
Zastosowanie AI i ML pozwala dokonać takiej analizy w czasie rzeczywistym, umożliwiając podjęcie błyskawicznych działań wspierających bezpieczeństwo, ochronę i efektywność operacyjną. Mowa m.in. o powiadamianiu służb ratunkowych, przekierowaniu ruchu w mieście, a nawet o oszczędzaniu energii w budynkach. Poza typowymi zadaniami analiza danych ułatwia pracę w sytuacjach nadzwyczajnych, np. wtedy, gdy trzeba sprawdzić obraz z kamer dozoru na żądanie uprawnionych do tego organów. Natomiast w wypadku zakładów produkcyjnych inteligentna predykcyjna analiza danych pozwala stosować tzw. konserwację zapobiegawczą chroniącą przed wystąpieniem rzeczywistej awarii.



Architektury hybrydowe dopasowane do potrzeb

W wyniku połączenia systemów bezpieczeństwa, serwerów lokalnych, obliczeń w chmurze i danych gromadzonych z urządzeń na brzegu sieci powstaje wyjątkowa hybrydowa architektura technologiczna. Nie ma jednak uniwersalnego modelu takiej architektury spełniającego wszystkie potrzeby użytkownika. Dlatego najpierw trzeba uwzględnić konkretne zastosowania, a dopiero potem zdefiniować rozwiązanie hybrydowe. Podczas projektowania należy wziąć pod uwagę szereg czynników. Jednym z nich jest wykorzystanie kamer dozoru wizyjnego. Zalety zaawansowanej analityki wbudowanej w kamery na brzegu sieci są oczywiste. Analiza najwyższej jakości obrazów w momencie ich przechwycenia daje organizacjom wyjątkową szansę na reagowanie w czasie rzeczywistym. Wymaga to jednak mocy obliczeniowej, którą oferują serwery chmurowe. Oczywiście trzeba brać pod uwagę ograniczenia – często określone przepisami – dotyczące prywatności i przechowywania danych, które różnią się w zależności od kraju i regionu. To one mogą zaważyć na tym, czy tego typu dane będą przechowywane lokalnie, czy w chmurze.

Najważniejsze są elastyczność i otwartość na różne rozwiązania tak, by były one dostosowane do konkretnych potrzeb.



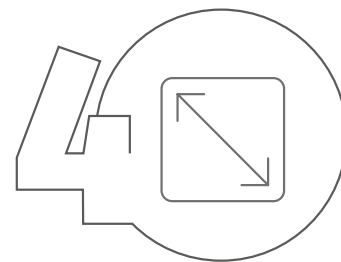
Bezpieczeństwo cybernetyczne

Cyberbezpieczeństwo nierozdzielnie wiąże się z koniecznością zachowania zgodności z przepisami. Proponowana przez Komisję Europejską ustawa o odporności (DORA) nakłada na producentów sprzętu i oprogramowania konkretne obowiązki niezależnie od sektora, w jakim działają. Ich zadaniem jest zapewnienie cyberbezpieczeństwa produktów poprzez zminimalizowanie możliwości ataków hakerskich, będących efektem np. luk w oprogramowaniu, oraz poprawę zarządzania cyberbezpieczeństwem przez cały cykl życia produktów. Odpowiedzialność ta spoczywa także na firmach z sektora bezpieczeństwa i dozoru.

Ustawa odzwierciedla zarówno znaczenie, jak i złożoność zagadnienia, jakim jest bezpieczeństwo cybernetyczne. Obecnie to kilka powiązanych ze sobą obszarów wymagających całościowego spojrzenia na kwestię bezpieczeństwa firmy. W przypadku dozoru wizyjnego środki bezpieczeństwa cybernetycznego służą zapewnieniu autentyczności danych przechwyconych przez kamery, stanowiąc źródło ich wiarygodności.

Stajemy się więc świadkami bardziej proaktywnego podejścia dostawców technologii do identyfikowania luk w zabezpieczeniach, a programy typu *bug bounty*, zachęcające podmioty zewnętrzne do wyszukiwania luk, staną się powszechne.

Jednocześnie klienci będą oczekiwać przejrzystości w zakresie stosowanych przez firmy rozwiązań zabezpieczających. Standardem ułatwiającym im ocenę bezpieczeństwa oprogramowania i zarządzania ryzykiem stanie się stosowanie Software Bill of Materials (SBOM to zestawienie materiałów użytych do opracowania konkretnego oprogramowania, które umożliwia wgląd w łańcuch dostaw oprogramowania oraz wszelkie zagrożenia związane ze zgodnością licencji, bezpieczeństwem i jakością).



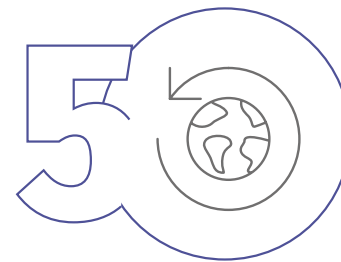
Wyjście poza tematykę ochrony fizycznej

Jednym z najbardziej znaczących trendów w sektorze security, a wraz z nim równie znaczących możliwości jest wyjście poza bezpieczeństwo fizyczne obiektów.

Kamery dozoru stały się potężnymi czujnikami. Jakość rejestrowanych przez nie informacji wideo wzrasta z roku na rok. Obecnie, dzięki zaawansowanej analityce, są źródłem olbrzymich ilości cennych danych, co stanowi ich wartość dodaną.

To oczywiście poprawia i zwiększa ich zdolność do wspierania bezpieczeństwa i efektywności operacyjnej. Współczesne urządzenia zapewniają połączenie danych zbieranych przez kamery dozoru z danymi z innych czujników monitorujących np. temperaturę, hałas, jakość powietrza i wody, wibracje, pogodę i inne, co tworzy zaawansowaną sieć sensoryczną umożliwiającą podejmowanie decyzji.

Widać już zastosowanie takich sieci w środowiskach przemysłowych poprzez monitorowanie procesów i wspieranie proaktywnej konserwacji. Na razie wykorzystanie takich danych jest ograniczone jedynie przez naszą wyobraźnię, ale bez wątpienia pomogą one w poprawie niemal każdego aspektu naszego życia, w tym bezpieczeństwa.



Zrównoważony rozwój zawsze, zmiany klimatyczne na czele

Zrównoważony rozwój pojawia się w wielu prognozach dotyczących trendów technologicznych. W nadchodzącym roku widać nie mniejszą potrzebę utrzymania rozmachu inicjatyw związanych z tematyką ESG. Zapewnienie, że organizacje będą nadal mierzyć i poprawiać praktyki środowiskowe, społeczne i zarządzania biznesem w firmach, będzie kluczowe dla poszanowania ludzi, bycia zaufanym partnerem biznesowym, wprowadzania odpowiedzialnych innowacji i ochrony naszej planety. Wszystkie te aspekty znajdują się pod coraz większą kontrolą ze strony klientów rozwiązań z zakresu ochrony i zabezpieczeń.

Biorąc pod uwagę ekstremalne warunki atmosferyczne, które wystąpiły w ubiegłym roku, można się spodziewać, że w 2023 r. organizacje skupią się na działaniach zapobiegających zmianom klimatycznym. Jest oczywiste, że nie robimy wystarczająco dużo, aby powstrzymać przyspieszenie globalnego ocieplenia, dlatego każdy sektor otrzyma zadanie podwojenia wysiłków zmierzających do ochrony środowiska naturalnego.

Dla Axis kluczowym krokiem było zaangażowanie się w inicjatywę Science-Based Targets Initiative (SBTI), w której ramach wyznaczamy cele w zakresie redukcji emisji nie tylko w naszej działalności, ale także w całym łańcuchu wartości. I to jest kluczowy punkt. Chociaż organizacje podejmują ogromne wysiłki w celu ograniczenia własnej emisji, to zostaną one zaprzepaszczone, jeśli ich dostawcy i partnerzy nie przyjmą tych samych wartości i nie będą dążyć do podobnego celu.

Dla firm technologicznych równie istotne będzie sprawienie, by ich produkty i usługi wspierały cele ESG ich klientów.



Zwiększony nacisk na regulacje prawne

Ze względu na wszechobecność i siłę sektor technologii trafił pod lupę organów regulacyjnych. Uważamy jednak, że istotą jest skupienie się na sposobach wykorzystania narzędzi cyfrowych, a nie na samych narzędziach. Komisja Europejska aktywnie zabiega o ochronę prywatności. Proponowana przez nią ustawa o sztucznej inteligencji, będąca częścią europejskiej strategii w tym zakresie, ma na celu przypisanie konkretnych kategorii ryzyka do zastosowań sztucznej inteligencji i stanowiłaby pierwsze ramy prawne dotyczące AI. Podobnie jak dyrektywa Komisji w sprawie odpowiedzialności za sztuczną inteligencję, ustawa o sztucznej inteligencji bez wątpienia będzie przedmiotem wielu debat, zanim stanie się obowiązującym prawem.

Niezależnie od tego, czy chodzi o AI, wymagania dotyczące bezpieczeństwa cybernetycznego, prywatności danych, ograniczania wpływu „wielkiej technologii” czy też ustanowienia suwerenności technologicznej, wiadomo, że firmy działające w sektorze bezpieczeństwa będą w coraz większym stopniu musiały przestrzegać coraz bardziej rygorystycznych przepisów. Należy to przyjąć z zadowoleniem, ponieważ zapewnienie przejrzystości biznesu i etycznych praktyk nadal ma kluczowe znaczenie dla przewagi konkurencyjnej.

Największą szansą dla naszego sektora pozostaje połączenie ciągłego sukcesu komercyjnego z odpowiedzialnością za rozwiązywanie krytycznych problemów, przed którymi stoi nasza planeta i ludność na całym świecie. Jak zawsze, jesteśmy optymistami. Wierzymy, że połączenie pomysłowości, postępu technologicznego i etycznych praktyk biznesowych wpłynie na poprawę środowiska naturalnego i życia ludzi. ●



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



O dobrej i złej synergii dotyczącej systemów zabezpieczeń

Synergia to współdziałanie różnych czynników, którego efekt jest większy niż suma poszczególnych oddzielnych działań. Ta zasada dotyczy systemów zabezpieczeń, ale też... działań przestępców.

Jacek Grzechowiak

Włamanie do obiektów magazynowych to bardzo często kwestia przypadku, wydarzenie, które ma miejsce trochę wg zasady, że „okazja czyni złodzieja”. Ale bywają i takie, które są efektem precyzyjnego planu przygotowanego przez profesjonalistę. Wśród złodziei znajdziemy więc specjalistów od intralogistyki (logistyki w obrębie obiektu), a także tych doświadczonych w operacjach „drogowych” albo takich, którzy wyspecjalizowali się w konkretnym mieniu – jedni kradną żywność, inni elektronikę, jeszcze inni odzież. Do wyboru, do koloru.

Obiekty magazynowe padają ofiarą różnego rodzaju ataków, poczynając od włamań pospolitych, często określanych mianem „na rympał” (te z kategorii „okazja czyni złodzieja”), takich jak to, do którego doszło w Łodzi w roku 2018. Wówczas łupem włamywacza padły elektronarzędzia o wartości 50 tys. zł. Ten akurat złodziej nie musiał się natrudzić – wystarczyło, że wybił szybę i przeciął niezbyt grubą kratę.

Nieco inaczej wyglądają włamanie „profilowane” dokonywane przez specjalistów. Te z reguły są już drobiazgowo przygotowywane, wymagają specjalistycznych narzędzi, niekiedy podrobienia dokumentów oraz wcześniejszej obserwacji obiektu. Takie włamanie są często efektem „zamówienia” na konkretny towar przechowywany w nieźle zabezpieczonych obiektach. Niekiedy nawet chronionych ponadprzeciętnie ze względu na rodzaj magazynowanego mienia, którego sposób zabezpieczenia jest regulowany prawnie, co zawsze oznacza wysokie wymagania w tym

zakresie. Dobrym tego przykładem, choć w tym przypadku nie chodziło o kradzież, jest zniszczenie składów broni przeznaczonej dla wojsk Ukrainy, do którego doszło w roku 2014 w czeskiej wiosce Vrbětice. To przypadek z kategorii krytycznych, ale i u nas mamy zastanawiające zdarzenia w podobnych obiektach, choć na szczęście nie o tak poważnym charakterze. Ciekawym przykładem jest incydent, do jakiego doszło w miejscowości Debrzn-Wieś, gdzie sprawcy włamali się do magazynu prywatnej firmy, w którym przechowywano uzbrojenie. Obiekt podlegający restrykcyjnym wymogom w zakresie zabezpieczenia, podlegający okresowym kontrolom wykonywanym przez policję, z powodzeniem może być celem napadu. Włamywaczom udało się pozyskać niemal cały arsenał składający się z kilkudziesięciu pistoletów maszynowych, amunicji, a nawet granatów.

Kradzież nie zawsze musi być jednak wynikiem włamania. Czasem jest to efekt wielomiesięcznego procederu. Takiego, jaki miał miejsce u renomowanego producenta samochodów, gdzie zginęło ponad 100 silników, aż 500 skrzyń biegów oraz innego sprzętu o łącznej wartości szacowanej na kilka milionów euro. Kradzież może być także wynikiem wadliwych procedur wewnętrznych, np. zarządzania stratami. W jednym z terminali proces ten wykorzystywano do celowego uszkodzenia opakowań produktów, by te znalazły się w strefie scrap (strefa przedmiotów wycofanych z obrotu), z której wyniesie ich było już znacznie łatwiejsze, bo przecież tam był – jak to określił jeden z menedżerów – „szmelc”, czyli wg niego towar bezwartościowy.



I tu dochodzimy do tytułowej synergii, ale... synergii działań środowisk przestępczych, wykorzystującej nie tylko słabe punkty zabezpieczeń, ale także wadliwe procedury i znajomość socjotechnik. W odpowiedzi na to organizacje również powinny myśleć o synergii, ale synergii zabezpieczeń.

Synergia działań przestępczych

W powszechnej opinii przestępcy działają dla pieniędzy. Czy zawsze? Przykład z czeskiej wsi Vrbětice pokazuje, że celem nie musi być kradzież, a sprawcą niekoniecznie musi być złodziej, może być to pracownik służb specjalnych. Motyw finansowy jest w wielu przypadkach oczywisty, lecz nie musi być jedynym, co dobitnie wykazało śledztwo przeprowadzone przez dziennikarzy i wolontariuszy z Belingcat, którzy ujawnili, iż w incydent w Vrbeticach byli zaangażowani funkcjonariusze rosyjskich służb specjalnych.

Najpierw pandemia, a potem wojna w Ukrainie potwierdziły to, co wiadomo od dawna – niespokojne czasy sprzyjają przestępczości. Szczególnie obecna sytuacja, wynikająca z działań wojennych w Ukrainie, dowodzi, że nawet położenie z daleka od linii frontu nie oznacza bezpieczeństwa.

Weźmy choćby przypadek ze Szwecji, gdzie odnotowano masową kradzież kamer DSLR (*Digital Single Lens Reflex*) zainstalowanych w fotoradarach. I to na skalę naprawdę dużą, bo samych okradzionych fotoradarów było ponad 150, a wartość strat wyceniono na 40 mln SEK. Takie same urządzenia ukraińskie ministerstwo obrony znalazło w zniszczonych rosyjskich dronach domowej roboty. SÄPO, czyli szwedzki kontrwywiad cywilny, zainteresował się sprawą i potraktował ją bardzo poważnie. A sprawa wydaje się jedynie pozornie odległa od biznesu, DSLR bowiem to nic innego jak... cyfrowa lustrzanka jednoobiektywowa. Skoro więc ktoś kradnie ten element z urządzenia zainstalowanego na ruchliwej autostradzie, to równie dobrze może pokusić się o jego kradzież z magazynu, czyli miejsca dużo spokojniejszego, w którym te aparaty są przechowywane hurtowo.

O jakiej synergii tu mowa? Otóż o takiej, która charakteryzuje działania przestępców, którzy zapewne kradną dla pieniędzy, ale przecież nie jest wykluczone, że dostają wsparcie zaawansowanych technologii wykorzystywanych przez służby specjalne. A to efekt synergii zdecydowanie wzmacnia, czyniąc zagrożenie dużo poważniejszym. Takim właśnie synergicznym działaniom muszą stawić czoła menedżerowie ds. ryzyka i bezpieczeństwa.

Jak synergii systemu zabezpieczeń powinni traktować menedżerowie ds. ryzyka

Biorąc pod uwagę przede wszystkim trzy składowe systemu zabezpieczeń: mechaniczny, elektroniczny i ludzki, bo zazwyczaj to między nimi oczekujemy zbieżności.

Czynnik mechaniczny, czyli drzwi, zamki, kłódki i klucze – tu synergii odnajdujemy coraz częściej w rozwiązaniach integrujących

mechanikę i elektronikę. Rozwiązania te są oparte na technologii bezprzewodowej, w której wymiana danych odbywa się online. W skład takiego rozwiązania wchodzi m.in. wyposażone we własne zasilanie wkładki elektroniczne, wymiarowo zgodne z ich mechanicznymi odpowiednikami. Do otwierania drzwi służą elektroniczne klucze wyposażone w chip z danymi dostępowymi. Aby otworzyć lub zamknąć drzwi, należy wsunąć elektroniczny klucz do wkładki i go obrócić, podobnie jak to robimy w przypadku wkładek mechanicznych. Na tym podobieństwa się kończą.

Jak więc widać, efekt synergii jest bezsprzeczny, a inteligentny system dostępowy (np. blueSmart) pozwala wzmocnić system bezpieczeństwa zarówno w warstwie bezpośredniego zamknięcia (konieczność zadziałania w tym samym czasie komponentu mechanicznego i elektronicznego), jak i minimalizowania potencjalnych ułomności czynnika ludzkiego, które mogą negatywnie wpłynąć na ten element, np. na skutek zgubienia klucza, a co gorsza, ukrycia tego faktu (bardzo często obserwowane przeze mnie podczas wykonywanych audytów bezpieczeństwa). Występuje tu oczywiście kilka warunków. Komunikacja pomiędzy identyfikatorami

a komponentami drzwiowymi musi odbywać się w sposób szyfrowany. Ważna jest też możliwość mobilnego zarządzania i zdalnego programowania nawet odległych komponentów drzwiowych, aby zminimalizować czas reakcji na incydenty (zagubienie klucza) i zmiany organizacyjne.

Czynnik elektroniczny – jednym z podstawowych narzędzi są w tym przypadku systemy dozoru wizyjnego (VSS), których mnogość sprawia, że mamy duże możliwości, z zastrzeżeniem jednak przywiązywania należytej uwagi do czynnika ludzkiego.

Jedną z ważniejszych cech tych systemów jest odpowiednia dynamika obrazu z kamer pozwalająca na uniknięcie problemów, jakie ochronie nastręcza... brak koordynacji pomiędzy różnymi działami już na etapie projektowania i budowy konkretnego

obiekta. Dość często są one przyczyną np. dużej zmienności intensywności oświetlenia sceny, co przy kamerach o niskiej dynamice spowoduje, że zamiast wyraźnego obrazu będzie widać białą plamę lub głęboką czerń. Dlatego parametrem kluczowym jest szeroki zakres dynamiki (WDR), tym bardziej że problemy z jakością obrazowania zdarzeń mogą wywołać nawet wózki widłowe, które mając reflektory skierowane w stronę kamery, potrafią zaburzyć obraz.

Jakość kamery jest niezmiernie istotna, gdy łączymy kwestie bezpieczeństwa z kwestiami jakościowymi, np. w przypadku weryfikacji zawartości opakowań. W tym przypadku liczba egzemplarzy wewnątrz opakowania ma znaczenie zarówno w kontekście prewencji antykradzieżowej czy wyjaśniania incydentów związanych z dokonaniem kradzieży, jak i dla kompletności. Odpowiednia rozdzielczość kamery pozwala na zarządzanie dwoma procesami naraz.

Gdy przyglądamy się rozwojowi systemów VSS, widać wyraźnie, że ostatnie lata to okres intensywnego rozwoju systemów

opartych na technologii IP. Efekt synergii jest tu oczywisty. Integracja infrastruktury ochronnej, zdalny dostęp to cechy, bez których dziś trudno się obejść. Coraz częściej systemy te bazują także na technologii chmurowej, więc siłą rzeczy są połączone ze światem zewnętrznym, stąd nic dziwnego, że także one podlegają zagrożeniom cybernetycznym.

Jest wiele metod ataków na kamery, poczynając od zastosowania prostych exploitów (aplikacji wykorzystujących błędy w oprogramowaniu urządzenia), kończąc na zaawansowanych technikach włamań informatycznych. Przykładem uznawanym za pierwszy tego typu atak na branżę security było włamanie przez tzw. *backdoor* do kamer znanego producenta, które miało miejsce w marcu 2017 r. Hakerzy uzyskali kontrolę nad kamerami, uzyskując wgląd do obiektu i możliwość sterowania kamerami.

Systemy security też mogą być celem ataków, jednak w tym przypadku konsekwencje mogą się okazać niezwykle groźne, ponieważ kamery można wykorzystać do identyfikacji pozostałych elementów zabezpieczeń stosowanych w obiekcie, takich jak zamki, rygle, strefy monitoringu SSWiN. Dotyczy to nawet urządzeń działających poza siecią. Co gorsza, możliwe jest wykorzystanie takiego włamania do zdalnego monitorowania działań pracowników ochrony, a złodzieje dostają niejako instrukcję, jak najszybciej i najbezpieczniej dokonać włamania, bądź gdzie są zlokalizowane towary najbardziej wartościowe. A nade wszystko zyskują przewagę nad zespołem ochronnym, mogą nie tylko monitorować jego działania (i to w czasie rzeczywistym), ale także wzbudzać fałszywe alarmy, kierując uwagę ochrony i ich fizyczną obecność do innych stref obiektu.

Ryzyko to może pochodzić z kamer w danym obiekcie, a także z obiektu znajdującego się w pobliskim sąsiedztwie lub wręcz z systemu monitoringu miejskiego. Tu niezamierzona synergia nieautoryzowanego dostępu do systemów zabezpieczeń technicznych obraca się przeciwko nam. Dlatego zmiana domyślnych haseł, aktualizacja oprogramowania, stała kontrola z poziomu SOC są wymogiem chwili i pewnym znakiem współczesnych czasów, pozwalając na utrzymanie systemów zabezpieczeń technicznych w stanie sprawności technicznej i operacyjnej oraz właściwej odporności na wykorzystanie ich przez przestępców do wsparcia własnych działań.

To wszystko skłania do postawienia jeszcze jednej ważnej tezy: kompetencje pracowników ochrony, którzy przecież są podstawową grupą użytkowników systemów zabezpieczeń technicznych, muszą zostać podniesione, i to z naciskiem na budowanie ich świadomości w zakresie cyberbezpieczeństwa.

W ten sposób doszliśmy do **czynnika ludzkiego**, którego znaczenie nie maleje. Odpowiedni poziom wiedzy pracowników ochrony zajmujących się ochroną obiektów i procesów logistycznych jest sprawą niezbędną. Dotyczy to m.in. znajomości najnowszych technik przestępczych oraz umiejętności wykorzystywania możliwości systemów zabezpieczeń w sposób czasami niestandardowy, lecz najlepiej pasujący do chronionego obiektu, procesu czy miejsca. Kwestie te wymagają realizacji kompleksowych programów szkoleniowych, poczynając od typowo ochronnych, przez szkolenia nt. aktualnych zagrożeń, po specjalistyczne szkolenia techniczne. ●

PRZYPISY

Artykuł wraz z przypisami znajdziesz na portalu aspolska.pl



» Kompetencje pracowników ochrony, którzy są przecież podstawową grupą użytkowników systemów zabezpieczeń technicznych, muszą zostać podniesione, i to z naciskiem na budowanie ich świadomości w zakresie cyberbezpieczeństwa. «

Jacek Grzechowiak

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





Polski system kontroli dostępu klasy *enterprise* na stadionie w Gdańsku

Stadion w Gdańsku to nie tylko arena zmaganiań piłkarzy, która uzyskała tytuł najpiękniejszego stadionu Euro 2012, to także miejsce organizacji wielu wydarzeń i codziennej pracy wielu ludzi.

Charakter tego obiektu wymusza szczególne wymagania wobec systemów zabezpieczeń technicznych, zwłaszcza systemu kontroli dostępu, umożliwiających wstęp do poszczególnych stref i pomieszczeń konkretnym grupom czy pojedynczym osobom.

Wymagania

W związku ze zmieniającymi się warunkami działalności stadionu pierwotnie zainstalowany system kontroli dostępu po latach intensywnego użytkowania wymagał modernizacji i rozbudowy. Pojawił się wówczas dylemat, czy inwestować w istniejący system mający swoje ograniczenia, choćby ze względu na wiek urządzeń, czy wymienić go na inny, bardziej dostosowany do aktualnych potrzeb i z większymi możliwościami.

Wymagania odnośnie do zmodernizowanego systemu nie były banalne. System miał zapewnić kontrolę nad ruchem ludzi w całym obiekcie. Kluczowym wyzwaniem była możliwość utworzenia zasad i harmonogramów otwarcia poszczególnych przejść w zależności od tego, jakiego rodzaju wydarzenie miało mieć miejsce na stadionie. Ponadto system miał poradzić sobie z obsługą zarówno wydarzeń, jak i codzienną, związaną z utrzymaniem obiektu w należytym stanie. Zgodnie z obowiązującymi trendami była też wymagana możliwość integracji z innymi systemami, głównie klasy SMS (*Security Management System*), poprzez otwarte API. Istotnym wymogiem stawianym przez inwestora był atrakcyjny, nowoczesny i elegancki wygląd instalowanych urządzeń, zwłaszcza czytników znajdujących się w miejscach ogólnodostępnych.

Bardzo ważny był także poziom bezpieczeństwa oferowany przez wybrane rozwiązanie, a także elastyczność w zakresie konfiguracji i rozbudowy uwzględniająca zmieniające się uwarunkowania pracy stadionu. Wymagania realizacyjne nakładały kolejne obostrzenia. Po pierwsze, dla użytkowników modernizacja miała przebiegać niezauważalnie – bez konieczności wymiany kart dostępu (pracujących w standardzie MIFARE®). Po drugie, modernizowane przejścia nie mogły pozostać pozbawione zabezpieczenia dłużej niż kilka godzin (maksymalnie 1 dzień). Po trzecie, nie bez znaczenia były koszty: modernizacji, bieżącego utrzymania systemu, ale też ewentualnej rozbudowy czy zmiany w związku z jego dostosowywaniem do przyszłych wymagań.

Zastosowane rozwiązania

Modernizowany system początkowo obejmował ok. 160 przejść i 1000 aktywnych użytkowników. Ostatecznie wybór padł na polskie rozwiązanie firmy Roger – system RACS 5 oferujący całociowe rozwiązanie w dziedzinie kontroli dostępu od strony zarówno sprzętowej, jak i programowej. Proces modernizacji rozpoczął się od realizacji 33 nowych przejść.

Takie podejście miało na celu objęcie kontrolą przejść nieujętych w pierwotnym projekcie oraz sprawdzenie, czy system RACS 5 będzie spełniać założone wymagania. Następnie dokonano pełnej modernizacji systemu poprzez wymianę dotychczasowego na nowy z jednoczesnym zwiększeniem maksymalnej liczby obsługiwanych użytkowników z 1000 do 2000.

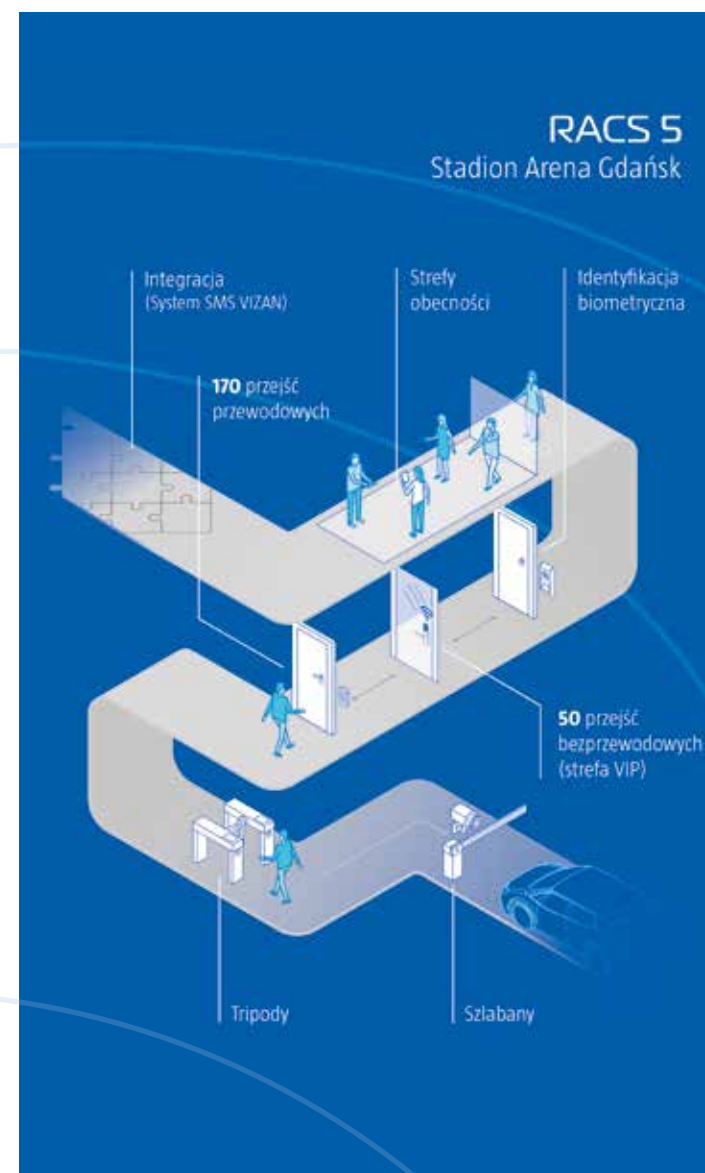
Oprócz „typowych” czytników zbliżeniowych MIFARE® (modele wewnętrzne i zewnętrzne) w kilku pomieszczeniach istotnych dla funkcjonowania stadionu, takich jak główna serwerownia, pomieszczenia styków z operatorami, zamontowano także czytniki linii papilarnych. W celu poprawy ich bezpieczeństwa wprowadzono podwójną identyfikację (odczyt karty plus odczyt linii papilarnych). Czytniki obsługują głównie wewnętrzne przejścia osobowe na drzwiach w systemie jedno- i dwukierunkowym oraz kołowrotki – tzw. tripody – z wykorzystaniem funkcjonalności przejścia dwukierunkowego w zależności od lokalizacji czytnika. Do obsługi kontroli dostępu do łoża VIP wybrano zamki bezprzewodowe RWL-2. Obecnie w systemie jest zainstalowanych ok. 170 przejść przewodowych i 50 bezprzewodowych. Na zewnątrz obiektu obsługiwana jest para szlabanów na parking sterowana z RACS-a w układzie dwukierunkowym. W systemie wykorzystano funkcjonalność przejść typu *anti-passback*, m.in. na parkingu, wykluczając tym samym możliwość ponownego użycia karty bez opuszczenia chronionej strefy. Zastosowano także „strefy obecności” w celu zliczania aktualnej liczby osób w danej strefie; w planach jest wykorzystanie tej funkcjonalności do ograniczania wejścia osób poza wyznaczony limit.

Pierwotnie na obiekcie została zainstalowana jedna z pierwszych wersji systemu RACS 5 podnoszona następnie do najnowszej w ramach bezpłatnych aktualizacji. Kontrola dostępu jest zintegrowana z systemem wizualizacji SMS VIZAN. Stanowiska operatorów zostały umieszczone w lokalnym centrum dozoru (LCN). Pozwalają na pełną wizualizację aktualnego stanu wszystkich przejść oraz obsługę zdarzeń alarmowych. Planowane jest utworzenie niezależnego stanowiska w recepcji w celu obsługi księgi gości. W trakcie realizacji nie obyło się bez problemów. Głównym były zakłócenia w transmisji danych dla czytników bezprzewodowych związane z konstrukcją obiektu – rozwiązano je poprzez wykonanie specjalnych mocowań koncentratorów bezprzewodowych we współpracy z producentem sprzętu. Zoptymalizowano także zużycie energii w zamkach/czytnikach bezprzewodowych, co pozwoliło na istotne wydłużenie czasu ich pracy na komplecie baterii. Dzięki dobrej współpracy z producentem – działem badań i rozwoju – otwartym na propozycje rozwoju produktu i jego doskonalenia wprowadzono wiele funkcjonalności pierwotnie nieistniejących, istotnych dla użytkownika końcowego oraz firmy wdrażającej rozwiązanie. Są to m.in. projektowanie i wydruk kart, zarządzanie uprawnieniami czasowymi – w systemie jest obecnie zdefiniowanych ok. 400 uprawnień czy wdrażana obecnie (na stadionie) księga gości – z możliwością przypisania uprawnienia dostępu do strefy i czasu nadawane dla każdej karty oddzielnie (z puli „wolnych”) oraz automatyczne generowanie „księgi wejść”.

Modernizacja systemu rozpoczęła się latem 2018 r., natomiast jej główny etap zakończył się w grudniu tego samego roku. Wymiana sprzętu (ok. 160 przejść) zajęła blisko 30 dni roboczych, całość z uruchomieniem ok. 2 miesięcy. W realizację projektu zaangażowanych było kilkanaście osób. Inwestor planuje dalszy rozwój systemu. Zamierza rozbudować go, w tym uruchomić system automatycznego rozpoznawania tablic rejestracyjnych (ANPR/LPR) w celu dalszego usprawnienia obsługi parkingu.

Korzyści

Wybór systemu firmy Roger pozwolił uzyskać mniejsze koszty wymiany na nowy system w stosunku do ewentualnej rozbudowy istniejącego.



Otrzymano rozwiązanie zaspokajające obecne potrzeby inwestora oraz gwarantujące stabilność przyszłych dostaw i wsparcia, oferujące najnowsze technologie oraz zgodność z aktualnymi uregulowaniami prawnymi. W trakcie modernizacji wykorzystano istniejącą infrastrukturę okablowania.

Nowe rozwiązanie wyeliminowało problemy z integracją i komunikacją z systemem SMS. Dzięki bliskości siedziby producenta i szybkości wsparcia – niezwłocznej reakcji na problemy zarówno programowe (wykryte błędy przy wdrożeniu/konfiguracji), jak i sprzętowe, czy to zdalnie, czy fizycznie – osiągnięto ciągłą pracę systemu. Gwarantuje to także elastyczność w rozbudowie o nowe przejścia czy w przypadku awarii – dostępność sprzętu „od ręki” – wysyłka NBD. Wdrożone rozwiązanie istotne jest także wizerunkowo dla miasta/samorządu – właściciela spółki Arena Gdańsk – poprzez promowanie polskiej marki Roger. ●



Roger
Gościszewo 59, 82-400 Sztum
roger@roger.pl
www.roger.pl



Inteligentny system ułatwiający szybką zmianę reguł dostępu

Elektroniczne systemy kontroli dostępu firmy Winkhaus są przeznaczone do stosowania w obiektach różnego typu i różnej wielkości, pozwalając bezpiecznie i wygodnie zarządzać dostępem do pomieszczeń w budynkach. Bezprzewodowa kontrola dostępu Winkhaus z powodzeniem działa na wielu stadionach w Europie.



Bukareszteński Stadion Narodowy chronią elektroniczne wkładki i klucze Winkhaus



Stadion Rhein Energie drużyny FC Köln od kilkunastu lat korzysta z elektronicznej kontroli dostępu Winkhaus

Przykładami takich realizacji są m.in. Stadion Narodowy w Bukareszcie, HDI Arena w Hanowerze, Rhein Energie Stadion w Kolonii czy Ghelamco Arena w Gandawie.

Z punktu widzenia osób zarządzających tego typu obiektami największą zaletą systemów Winkhaus jest ich elastyczność. Kilka razy w tygodniu, w zależności od imprez odbywających się w obiekcie, system kontroli dostępu może zostać błyskawicznie przeprojekтовany: możliwość wejścia do poszczególnych pomieszczeń jest przyznawana w ramach schematu obowiązującego dla danego wydarzenia. Zmiana odbywa się w komputerze administratora, wystarczy kilka kliknięć na klawiaturze. Tak programowane są też klucze dla użytkowników pomieszczeń. W taki sam sposób łatwo i szybko administrator przywraca schemat dostępu sprzed wydarzenia obowiązujący dla stałych użytkowników stadionu.

Atutem elektronicznych systemów dostępu jest brak konieczności wymiany wkładek w przypadku zagubienia klucza o wielu uprawnieniach. System Winkhaus umożliwia szybką i bezkosztową blokadę zagubionego klucza bez potrzeby wymiany wkładek zamontowanych w drzwiach. Ważną funkcją jest także rejestr wejść do każdego pomieszczenia, do którego ma wgląd administrator systemu. Dzięki zastosowaniu bezprzewodowej technologii tzw. sieci wirtualnej, system kontroli dostępu Winkhaus można zainstalować na dowolnym etapie inwestycji, także po jej zakończeniu. ●



Winkhaus Polska Beteiligungs
ul. Przemysłowa 1, 64-130 Rydzyna
bluesmart@winkhaus.pl
Bluesmart.winkhaus.com



8 smartfonami znajdującymi się jednocześnie w zasięgu czytnika. Wyeliminowanie konieczności przekazywania czytnika z jednego telefonu komórkowego na drugi likwiduje opóźnienia i awarie komunikacji.

WaveKey. Mobilny dostęp, na którym możesz polegać!

Smartfony są wszechobecne we współczesnym świecie. Są z nami stale, więc oprócz wykonywania rutynowych połączeń telefonicznych i sprawdzania wiadomości e-mail coraz częściej używamy ich do dokonywania płatności w sklepach, a także stają się doskonałym wyborem do kontroli dostępu. Mogą zastąpić kartę dostępu i są wygodniejsze oraz bezpieczniejsze w użyciu.

Według IHS Markit w 2018 r. tempo wzrostu rocznych pobrań mobilnych danych uwierzytelniających na całym świecie przekroczyło 150%, a wielkość rynku wzrosła do prawie 4,1 mln pobrań. Do 2023 r. liczba mobilnych danych uwierzytelniających wzrośnie z 1% wydawanych rocznie do 14% i zostanie wprowadzona jako znacząca alternatywa dla fizycznych poświadczeń na całym świecie. IHS Markit przewiduje, że do końca 2023 r. liczba rocznych pobrań mobilnych danych uwierzytelniających osiągnie ponad 120 mln.

Za tym zjawiskiem stoją różne czynniki, ale najważniejszy z nich to wygoda. Dla użytkownika oznacza to możliwość dostępu do budynku za pomocą smartfona, bez konieczności noszenia dodatkowych kart lub kluczy. Administrator bezpieczeństwa korzysta z opcji zdalnego wydawania i cofania mobilnych danych uwierzytelniających, a także z wysokiego poziomu bezpieczeństwa oferowanego przez poświadczenia Bluetooth.

WaveKey. Najszybsza mobilna kontrola dostępu oferowana przez 2N

2N, światowy lider w dziedzinie interkomów IP i systemów kontroli dostępu, wprowadził w 2022 r. WaveKey, opatentowaną technologię dostępu dla telefonów komórkowych. WaveKey rozwiązuje ograniczenia, które do tej pory dotyczyły kontroli dostępu opartej na funkcji Bluetooth. Ale ta technologia ma wiele zalet sprawiających, że jest to idealne rozwiązanie dostępu mobilnego, które warto rozważyć w swoich projektach.

Dzięki możliwości odblokowania drzwi w zaledwie 0,3 s WaveKey jest najszybszy na rynku i ma najwyższą w swojej klasie niezawodność, dzięki czemu nie ma żadnych problemów z jego użyciem w zatłoczonym środowisku biurowym. Sekret tej technologii 2N tkwi w unikatowym systemie wstępnego uwierzytelniania i komunikacji z maksymalnie

Odpowiednia równowaga pomiędzy wygodą a bezpieczeństwem

Znacznie szybsze uwierzytelnianie oznacza bezproblemowe przechodzenie przez budynek i szybkie otwieranie drzwi. Użytkownik nie musi nawet wyjmować smartfona z kieszeni lub torebki. Wystarczy dotknąć czytnika 2N i wejść. W ten sposób działa jeden z czterech trybów WaveKey, zwany **trybem dotykowym**.

Innym trybem, który mogą ustawiać administratorzy, jest tryb **Dotknij w aplikacji**. Zwiększa to bezpieczeństwo, ponieważ użytkownik musi odblokować telefon, aby wejść do aplikacji i otworzyć drzwi, naciskając wirtualny przycisk. Doskonale nadaje się on również do otwierania bram garażowych o większym zasięgu i barier parkingowych bezpośrednio z samochodu. Trzeci to tryb **Karta**, który jest czymś więcej niż pełnoprawnym zamiennikiem technologii NFC, gdyż działa na urządzeniach z systemem zarówno Android, jak i iOS na bardzo krótkim dystansie. Ostatni to tryb **Ruch** – całkowicie bezdotykowy sposób otwierania drzwi, który na wyższym poziomie podnosi wygodę, jaką zapewnia tryb dotykowy. Kamera w interkomie 2N uruchamia proces uwierzytelniania, oparty na wykrywaniu ruchu. Jeśli zbliżająca się osoba ma przy sobie autoryzowany telefon, może od razu otworzyć drzwi. ●



2N TELEKOMUNIKACE
Pod Vinicí 20, 143 01 Praha 4
Czech Republic
www.2n.com



Lufthansa Technik: jak zachować równowagę pomiędzy wolnością a wysokim poziomem bezpieczeństwa

Firma Lufthansa Technik funkcjonuje w ramach specjalnego sektora przemysłu lotniczego.

Potrzeby w zakresie kontroli dostępu do pomieszczeń stawały się coraz bardziej istotne, zwłaszcza w stosunku do osób z zewnątrz.

Kluczowym wyzwaniem dla firmy jest utrzymanie przyjaznego środowiska, wolnego od ograniczeń, przy jednoczesnym zapewnieniu najwyższych standardów bezpieczeństwa.

Firmie Lufthansa Technik zależy na ograniczeniu możliwości nieupoważnionego wstępu, a przy tym nieutrudnianiu codziennego funkcjonowania swoim pracownikom. Znalezienie równowagi pomiędzy bezpieczeństwem a wygodą, zapewniającej zarówno swobodę poruszania się, jak i poczucie bezpieczeństwa, jest bardzo istotne.

Kontrola dostępu ujednolicona we wszystkich oddziałach

Kluczowym celem nowego systemu kontroli dostępu było jego ujednolicenie. Lufthansa Technik działa w ponad 35 lokalizacjach na świecie, zatrudniając 100 tys. osób. W przeszłości każda placówka samodzielnie odpowiadała za swoje bezpieczeństwo. To czasami wymagało zatrudniania specjalistów rozwiązujących jednakowe problemy w różnych miejscach. Firma chciała tego uniknąć i zagwarantować nie tylko te same wysokie standardy bezpieczeństwa, ale także kulturę współdziałania, w której ramach ludzie w dowolnym oddziale będą mogli z łatwością komunikować się ze sobą i współpracować.

Dlatego też nadrzędnym celem firmy Lufthansa Technik była możliwość korzystania z jednego systemu kontroli dostępu i przestrzeganie tej samej polityki bezpieczeństwa w każdej placówce. Inną ważną kwestią było sprawienie, by jeden identyfikator Lufthansa Technik używany przez pracownika umożliwiał mu dostęp do każdego miejsca, po którym ma prawo się poruszać – w skali zarówno lokalnej, jak i międzynarodowej. Zmierzenie się z tym wyzwaniem nie było łatwe, zwłaszcza z powodu kwestii IT związanych z wdrażaniem ujednoliconego systemu KD w wielu miejscach na świecie.

Nedap i ich partnerzy koncentrują się na potrzebach klienta

Poszukiwania odpowiedniego systemu kontroli dostępu firma Lufthansa Technik rozpoczęła od dokładnego badania rynku i organizacji pogłębionego przetargu obejmującego różnych dostawców. Po dokładnych analizach wybrano Nedap.

– Byliśmy pod wrażeniem kultury korporacyjnej Nedap, skupienia się na aspektach praktycznych i indywidualnego podejścia. Bardzo starali się znaleźć rozwiązanie idealnie odpowiadające naszym potrzebom. Dlatego zdecydowaliśmy się wdrożyć system Nedap AEOS, który znacząco pomógł nam spełnić nasze kryteria i pozwolił stworzyć jednolity system – mówi Melf Westphal, kierownik ds. rozwiązań z zakresu bezpieczeństwa w Lufthansie.

Zapewnienie swobody pozwala ludziom rozwinąć skrzydła

Cele firmy Lufthansa Technik w zakresie kontroli dostępu pokrywają się ze skierowanym na ludzi podejściem Nedap w ramach rozwiązania „Bezpieczeństwo dla życia”. Nedap jest przekonany, że systemy bezpieczeństwa należy projektować z myślą o osobach, które będą z nich korzystać, a nie technologii, które będą je obsługiwać.

– Podejście „Bezpieczeństwo dla życia” podkreśla aspiracje Nedap do odciążenia personelu w zakresie dbania o kwestie bezpieczeństwa. To z kolei odzwierciedla dążenia firmy Lufthansa Technik do optymalizacji stosunku stopnia ochrony z wygodą. Za pośrednictwem ich sieci partnerskiej zyskaliśmy możliwość tworzenia spersonalizowanych rozwiązań poprzez integrację z produktami innych firm, które zaspokajają nasze potrzeby dotyczące zabezpieczeń – wyjaśnia kierownik ds. rozwiązań z zakresu bezpieczeństwa w Lufthansie.

Sprostanie wyzwaniom wymaga dużego wsparcia

Początkowo firma Lufthansa Technik uruchomiła projekt pilotażowy w celu wdrożenia systemu AEOS w Hamburgu, gdzie zatrudnionych jest 10 tys. osób, a następnie w czterech kolejnych oddziałach.

– Na początku nie wiedzieliśmy, jak się do tego zabrać. Jednak dzięki kompleksowej pomocy Nedap i ich partnerów było nam o wiele łatwiej przebrnąć przez etap wdrażania. Projekt pilotażowy pozwolił nam przezwyciężyć dwie istotne kwestie: jak wdrożyć kontrolę dostępu AEOS w naszej infrastrukturze informatycznej oraz jak zaangażować naszych pracowników – podkreśla M. Westphal. – Nedap wraz z partnerami wykonali solidną robotę. To, co nam zaprezentowali, to nie tylko dobre produkty. Dzięki ich wsparciu, a także pomocy ich oddanych partnerów mogliśmy uporać się ze wszystkimi problemami operacyjnymi. Za pośrednictwem ich sieci partnerskiej zyskaliśmy z kolei możliwość tworzenia spersonalizowanych rozwiązań poprzez integrację z produktami innych firm, które zaspokajają nasze potrzeby dotyczące zabezpieczeń. Oznacza to, że zamiast stawiania barier mamy relatywnie dużą wolność poruszania się. Czuję się bardzo bezpiecznie, jednak w razie potrzeby mogę korzystać z mojego identyfikatora, aby udać się w dowolne miejsce. Mamy fantastyczne rozwiązania oraz, co ważne, ten sam identyfikator Lufthansa Technik, który łączy nas wszystkich niezależnie od naszej lokalizacji.

Integracja firm trzecich zwiększa elastyczność

– Wdrożony przez firmę Lufthansa Technik system kontroli dostępu AEOS to więcej niż tylko ochrona drzwi, zainstalowano również dodatkowe komponenty, takie jak szafy na klucze oraz zarządzanie odwiedzającymi.

» *Jeżeli chodzi o bezpieczeństwo, moim mottem jest: Lepiej otwierać drzwi, niż je zamykać. Jest to dla mnie naprawdę ważne.* «

M. Westphal

AEOS okazał się wielką pomocą w tej kwestii, pozwolił nam na zaangażowanie usługodawców zewnętrznych. Ponieważ filozofią Nedap jest ścisła współpraca z zewnętrznymi partnerami technologicznymi, a AEOS łatwo integruje się z innymi systemami, nie byliśmy ograniczeni tylko do jednego rozwiązania. Zapewniło to nam elastyczność w stworzeniu dokładnie tego, czego oczekiwaliśmy – ocenia M. Westphal.

W skutecznych systemach to ludzie są najważniejsi

Dla firmy Lufthansa Technik kluczowym aspektem projektu pilotażowego i następującego po nim wdrożenia było przekonanie pracowników do pracy z nowym systemem kontroli dostępu. Uważa ona, że nawet najlepszy system KD traci na wartości, jeżeli ludzie z nim pracujący nie mają właściwego podejścia. Z tego powodu Lufthansa Technik poczyniła znaczące inwestycje w szkolenia, komunikację i akcje uświadamiające.

W pierwszej kolejności skupiały się one na zakomunikowaniu pracownikom tego, jak bardzo są cenni, jak ważne jest bezpieczeństwo i dlaczego wprowadza się zmiany w organizacji bezpieczeństwa. Uświadomiły im również znaczenie potencjalnych zagrożeń dotyczących bezpieczeństwa i ich własnej roli w systemie zarządzania bezpieczeństwem firmy Lufthansa Technik. Każdy pracownik jest zachęcany do brania udziału w tworzeniu bezpiecznego środowiska pracy. Są też szkoleni, jak reagować na alerty i jak zwracać się do nieupoważnionych osób zauważonych w zastrzeżonych miejscach. Co ważne, pracownicy rozumieją, że ich system kontroli dostępu AEOS służy w takim samym stopniu ochronie ich wolności i zapewnieniu im bezpieczeństwa. – Jeżeli chodzi o bezpieczeństwo, moim mottem jest: Lepiej otwierać drzwi, niż je zamykać. Jest to dla mnie naprawdę ważne – podkreśla M. Westphal.

Wdrożenie w skali globalnej

Następnym krokiem Lufthansa Technik jest kontynuowanie wdrażania AEOS na całym świecie.

– Sukces naszego nowego systemu bezpieczeństwa nie pozostał niezauważony. Inne zakłady firmy Lufthansa Technik dostrzegły skuteczność AEOS na przykładzie Hamburga, w zakładzie zatrudniającym 10 tys. pracowników. Widzimy również wzrost zainteresowania podobnymi systemami oddziałów na całym świecie. Naszym celem jest więc wdrożenie AEOS we wszystkich naszych zakładach, aby uzyskać ujednolicony system bezpieczeństwa, który spaja całą rodzinę Lufthansa Technik. System bezpieczeństwa, który pozwala nam otwierać drzwi, a nie je zamykać – podsumowuje M. Westphal, kierownik ds. rozwiązań z zakresu bezpieczeństwa w Lufthansie. ●



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



Bezpieczne lotnisko – obiekt i jego otoczenie pod specjalnym nadzorem

Zapewnienie bezpieczeństwa obiektów o znaczeniu krytycznym wymaga zintegrowania wielu warstw systemów zabezpieczeń, w tym ochrony perymetrycznej. Lotniska ze względu na strategiczne znaczenie są tą klasą obiektów, gdzie zagrożenie wtargnięciem na teren zastrzeżony nie może zostać zignorowane.

Obwód ochrony portu lotniczego jest wzmocniony urządzeniami monitorującymi służącymi do detekcji wtargnięć oraz informowania służb nadzorujących bezpieczeństwo obiektu. Inteligentne systemy i urządzenia SIOUX PRO2 i MICRO RAY zostały tak zaprojektowane, by mogły znajdować zastosowanie w ochronie obiektów wymagających najwyższego poziomu zabezpieczeń. Paweł Cendrowski, specjalista i dyrektor handlowy firmy CIAS, przedstawia rozwiązania sprzętowe spełniające wyżej postawione wymagania.

Czujniki systemu SIOUX PRO2 są instalowane na ogrodzeniach co 5 metrów. Wykorzystują w swoim działaniu technologię 3D MEMS. Dzięki niej oraz analizie sygnałów opartej na algorytmie FUZZY LOGIC system wykrywa próby wspinania się, przecinania lub obalania ogrodzenia, przy jednoczesnej odporności na warunki zewnętrzne, np. porywy wiatru, drgania wywołane przez przejeżdżające pojazdy. System pozwala na zastosowanie topologii pętlowej, co uodparnia go na przypadki utraty ciągłości działania magistrali sygnałowo-prądowej spowodowane usterką lub celowym uszkodzeniem.

W ciągu czujników można zastosować dodatkowe izolatory zwarć i moduły wejść pozwalające na zbieranie sygnałów alarmowych z czujek zewnętrznych, np. kontaktów zabezpieczających bramy wjazdowe. Jeden sterownik systemu SIOUX może nadzorować do 1400 m ogrodzenia i na tej długości pozwala wydzielić nawet 80 stref alarmowych o dowolnej długości, również z wykorzystaniem technologii TOUCH&ZONE. Sterowniki SIOUX można łączyć w system o dowolnej długości, co w przypadku lotnisk jest bardzo przydatne.

Sygnały alarmowe mogą być przekazywane do systemu nadrzędnego przez standardowe przekaźniki lub z wykorzystaniem integracji programowych. System może wówczas podać miejsce naruszenia z dokładnością do 1 metra, a nie do wyznaczonej strefy alarmowej. Najdłuższy system ochrony obwodowej oparty na czujniku SIOUX ma długość ponad 35 km i zabezpiecza jedno z największych lotnisk we Włoszech. Do zabezpieczenia odcinków ogrodzenia wykonanych z innych elementów niż siatka lub panele można zastosować bariery mikrofalowe MICRO-RAY. Pozwalają one na utworzenie

bardzo wąskiej strefy detekcyjnej o szerokości 1 m, długości do 100 m i wysokości do 3 m.

Jest to produkt unikatowy na skalę światową. Łączy wszystkie zalety barier mikrofalowych (niezawodne działanie w każdych warunkach pogodowych, nie reaguje na opady śniegu lub deszczu, mgłę, szron, szadź, warunki następczenia) i dostępną dotychczas jedynie dla barier podczerwieni wąską strefę detekcji. Rozwiązanie wielowiązkowe pozwala na rozdzielenie charakterystyki działania bariery.

Część dolna może wykrywać powolne przekradanie się przez strefę detekcji, górna – próby szybkiego jej pokonania. Obie skonfigurowane jako pracujące w przestrzeni, w której obecne są ptaki lub małe zwierzęta, minimalizują liczbę niepożądanych alarmów. Tak jak w przypadku wszystkich cyfrowych urządzeń firmy CIAS, również MICRO-RAY ma możliwość zasilania lokalnego napięciem 13,8 V lub poprzez PoE. Sygnały alarmowe są przekazywane do systemu nadrzędnego za pośrednictwem przekaźników lub transmisji cyfrowej przez dodatkowy moduł IP DOORWAY z wykorzystaniem Ethernetu.

Najważniejsze lotniska wojskowe i cywilne w Polsce są już chronione za pomocą urządzeń firmy CIAS. Urządzenia mikrofalowe wbrew rozpowszechnianym opiniom nie wywołują zakłóceń w działaniu innych systemów lotniskowych. Zakończono pomyślnie testy systemów CIAS w jednym z największych cywilnych portów lotniczych w Polsce, gdzie wkrótce znajdą zastosowanie w miejscach niedostępnych do objęcia ochroną przez dotychczas oferowane na rynku systemy. ●



CIAS
ul. Żeligowskiego 8/10, 90-753 Łódź
biuro@cias.com.pl
<http://www.cias.com.pl>

AVIGILON™

MOTOROLA
SOLUTIONSvenom
PSIM PLATFORM

Nowoczesne serwerownie wymagają systemu PSIM klasy High-End

Dowiedz się więcej na www.psim.pl





» *Bezpieczeństwo jest jedno, choć ma różne oblicza. Na koniec dnia istotny jest jednak ogólny stan zabezpieczenia chronionych aktywów.* «

czy SKD. Następnie zaczęto zauważać konieczność zabezpieczania systemów zabezpieczeń elektronicznych w obszarze bezpieczeństwa IT.

Bez względu na podejście do bezpieczeństwa motywem działań ochronnych zawsze były i nadal są zagrożenia, które zmieniając się w czasie, wymagają od nas coraz nowszych elementów kontrolnych, niekoniecznie związanych z zabezpieczeniami technicznymi, ale również (a może przede wszystkim) organizacyjnych.

To od osób odpowiedzialnych za bezpieczeństwo zależy, czy reakcja na zagrożenie będzie kompleksowa, czy szczątkowa, szybka, czy spowolniona. Czy byliśmy przygotowani na turbulentne, ciągle zmieniające się wektory ataków? I fundamentalne pytanie: czy jesteśmy w swych poczynaniach skuteczni (nie zawsze musi być to wszak zbieżne z wykonaniem wszystkich czynności zgodnie z przyjętymi krokami).

To oczywiste, że cyberbezpieczeństwo oraz ochrona informacji przetwarzanych w zabezpieczeniach elektronicznych zaczęły odgrywać coraz ważniejszą rolę w zapewnieniu ochrony organizacji, ale ich połączenie z fizycznymi systemami ochrony wywołuje pewien chaos organizacyjny. Kluczowy jak zawsze jest bowiem przepływ informacji, czego dowodem jest przytaczany poniżej przykład.

Pewnego razu w serwerowni

Przeanalizujmy obsługę przykładowego, uproszczonego incydentu. Jedna z usług świadczonych przez organizację przestaje działać, a to oznacza wymierne straty finansowe i wizerunkowe. Ustalono, że serwery, na których była postawiona usługa, przestały działać (serwer redundantny również nie podjął pracy). W dziale bezpieczeństwa fizycznego odetchnięto z ulgą, a koledzy z IT pogodzili się już z nadgodzinami.

Później jednak ustalono, że serwer został przypadkowo wyłączony przez pracownika technicznego, który prowadził prace w serwerowni. Rzecz w tym, że osoba ta nie miała uprawnień, by wejść do serwerowni. W tym momencie działy bezpieczeństwa fizycznego oraz IT zaczynają obarczać się odpowiedzialnością za incydent.

Biorąc pod uwagę stan bezpieczeństwa i zagwarantowanie zachowania ciągłości działania, istotne jest nie tyle, kto zawinił,

Konwergencja bezpieczeństwa

W ostatnich latach podejście do zarządzania bezpieczeństwem oraz kwestii samego bezpieczeństwa diametralnie się zmieniło. Bezpieczeństwo fizyczne nie jest już postrzegane wyłącznie przez pryzmat posterunków ochrony, a systemy ochrony elektronicznej zaczęły spełniać dodatkowe zadania: dostarczają informacje innym systemom i zapewniają organizacjom wartość dodaną.

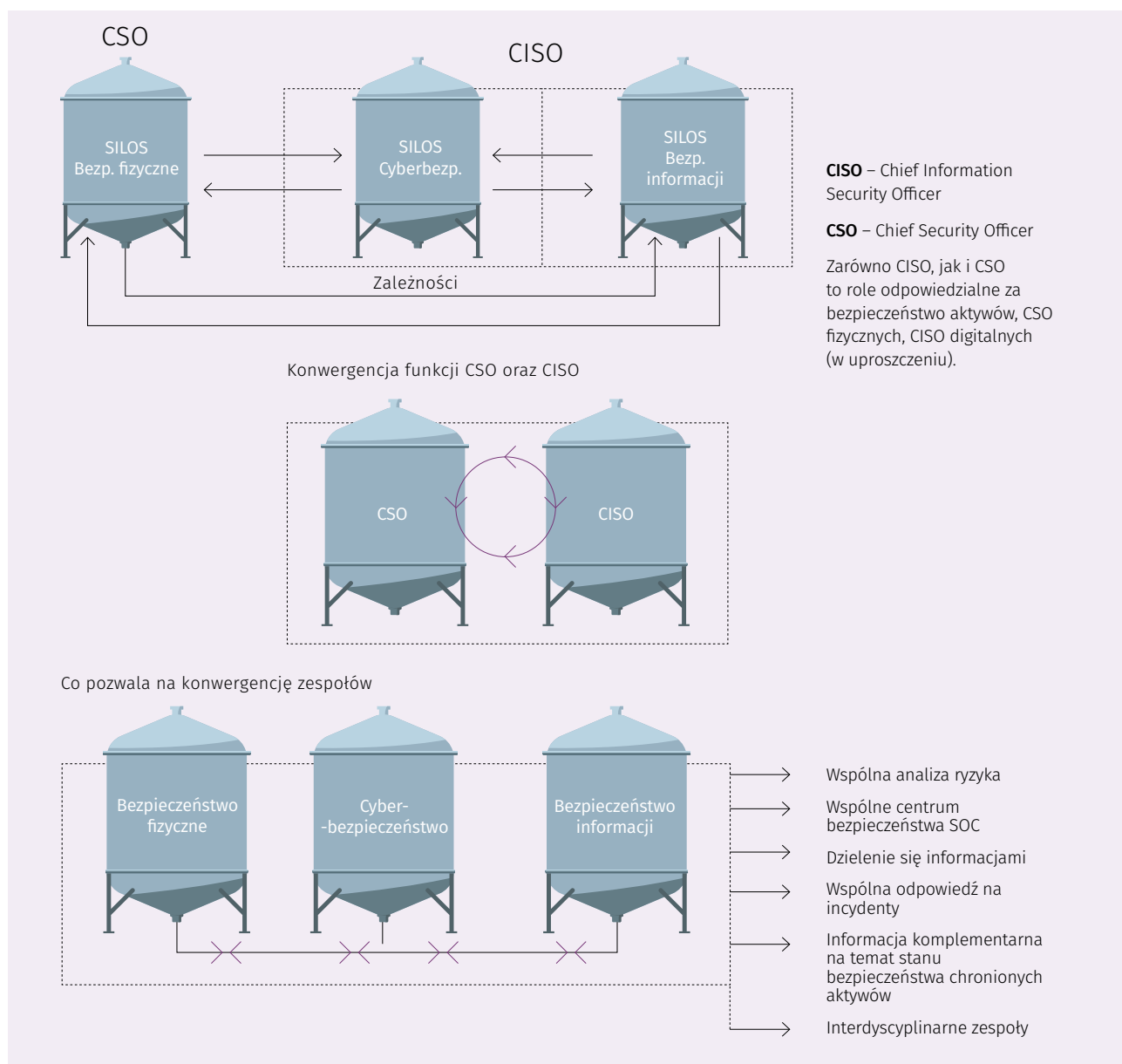
Tomasz Dacka

Bezpieczeństwo fizyczne, czyli technika i zasoby ludzkie, zostało objęte odpowiednimi procedurami, które wchodzi w skład polityki bezpieczeństwa organizacji. Wydaje się więc, że wszystko działa, jak powinno. Gdy jednak przyjrzymy się szczegółom, okazuje się, że jest coś, co można byłoby robić lepiej.

Na początku było...

Swego czasu każdy podsystem – czy to zabezpieczeń elektronicznych, czy ochrona fizyczna – działał w miarę niezależnie, spełniając swoje ściśle określone autonomiczne zadania. Postęp techniczny sprawił jednak, że coraz bardziej zaawansowane systemy elektroniczne zaczęły łączyć z posterunkami ochrony, zwiększając tym samym ich odpowiedzialność, a zarazem możliwości.

Coraz częściej mówiło się o ideach, takich jak integracja czy inteligentny system. Pojawiła się też potrzeba unifikacji systemów bądź opracowania wspólnego sposobu zarządzania zintegrowanymi podsystemami, np. za pomocą systemu Physical Security Information Management (PISM), czyli oprogramowania służącego do zarządzania informacjami spływającymi z podłączonych elektronicznych systemów zabezpieczeń, m.in. CCTV, SSWiN



ile dlaczego tak się stało. W tym przypadku zabrakło komunikacji i wzajemnego zrozumienia zagrożeń.

Nie zawsze musi to być atak hakerski, terrorystyczny czy tzw. insider threat (niepożądane działania spowodowane czynnikami wewnętrznymi, np. przez pracowników danej firmy). Większość incydentów wynika z przypadkowego działania człowieka. Jak zatem zapobiec takim sytuacjom?

Silosy kontra zwinność

Przez lata za utrzymanie bezpieczeństwa organizacji odpowiadały konkretne działy, tworząc tym samym kompetencyjne i komunikacyjne silosy (patrz rys.). Każdy w swoim zakresie kompetencji budował mury, wytyczał fosy, wznosił wieże. Już jednak w starożytnych Chinach oraz w XII wieku w plemionach Indian dostrzeżono potrzebę komunikacji pomiędzy sobą, w tym przypadku za pomocą znaków dymnych. Jakkolwiek technika od tamtych czasów poszła do przodu, o tyle potrzeba wymiany informacji pozostała równie ważna.

Rozwiązanie wydaje się zatem proste. Połączmy silosy ze sobą, tworząc kanały komunikacyjne. Takie rozwiązanie to jedynie krok w dobrym kierunku, ale nie przystanek końcowy. Każde takie połączenie tworzy zależność, a za zależnościami idą: problemy w komunikacji, rozmyta odpowiedzialność, niezrozumienie potrzeb obu stron, siłą narzucony sztuczny twór. Silosy nadal są silosami, nadal skupiają się głównie na swoich zadaniach z tą różnicą, że stworzone załączki zwinnej organizacji bezpieczeństwa zaczynają bardziej przeszkadzać, niż pomagać.

W obecnych turbulentnych warunkach od organizacji się wymaga, aby była jak najbardziej elastyczna i zwinna. Tak też powinny funkcjonować działy odpowiedzialne za jej bezpieczeństwo, powinny przewidywać i reagować, szybko i skutecznie.

Utrzymywanie silosów na to nie pozwoli. Lepiej zatem na ich bazie utworzyć jedno centrum kompetencji, zbudowane z transparentnych zespołów o krosfunkcyjnych kompetencjach, dające komplementarną odpowiedź na zagrożenie oraz informujące

w czasie rzeczywistym o stanie bezpieczeństwa aktywów. Przepływ informacji jest tutaj realizowany za pomocą jednej szyny danych zamiast topologii gwiazdy. Tym sposobem eliminujemy zależności, budujemy środowisko konwergentne.

Czy zatem oznacza to, że zadania, które dotychczas wykonywało trzech specjalistów, teraz ma wykonywać jeden? Oczywiście, że nie, i jest to element układanki, który najmniej podoba się biznesowi (aczkolwiek niesie korzyści ekonomiczne).

Co zamiast silosów?

Czym jest tak naprawdę konwergencja? To budowa czynników (procesy, ludzie, technika) związanych z bezpieczeństwem (również z zarządzaniem ryzykiem), współpracujących ze sobą w celu holistycznego adresowania celów oraz wyeliminowania błędów, dziur, podatności powstających pomiędzy tymi czynnikami. Konwergentny program/strategia zawiera elementy unifikacji oraz połączeń między czynnikami. Ważnym aspektem jest też zachowanie rozliczalności i spójności zarządzania, np. raportowanie do jednego Security Managera. Dzięki temu zachowamy wspólne procesy i, co ważniejsze, wspólną odpowiedzialność za nie.

Teoria a praktyka

Jak zatem wprowadzić zarządzanie bezpieczeństwem w modelu holistycznym przełamującym silosy? Na początku należy zacząć na ten temat rozmawiać. Należy mieć świadomość, że nie w każdej organizacji takie podejście musi być korzystne. W firmach budujących bezpieczeństwo na wzór wojskowy silosy mogą okazać się rozwiązaniem lepszym, a zmiana spowoduje chaos, a więc efekt odwrotny do zamierzonego.

Prostym, aczkolwiek skutecznym pomysłem jest ułożenie obok siebie działów odpowiedzialnych za bezpieczeństwo fizyczne i cyberochronę, pomaga to w zrozumieniu codziennych wyzwań poszczególnych komórek. Kolejnym przykładem jest implementacja zarządzania ryzykiem uwzględniająca wszystkie działy bezpieczeństwa, przenikająca przez różne zagrożenia, budująca kompleksową odpowiedź na nie, pozwalająca uniknąć sytuacji incydentu przywołanego we wcześniejszej części artykułu.

Jakie zatem korzyści niesie wprowadzenie konwergencji bezpieczeństwa?

- Zdecydowanie lepsze dopasowanie strategii bezpieczeństwa do celów organizacji
- Szybsza i efektywniejsza komunikacja
- Ustalenie wspólnych procesów, celów
- Budowa wszechstronnego zespołu, dzielenie się wiedzą i praktyką
- Większa elastyczność i zwinność działu bezpieczeństwa
- Większa rozliczalność oraz usprawniony sposób zarządzania obszarem bezpieczeństwa (tzw. *big picture*)

Z jakimi wyzwaniem możemy się zmierzyć?

- Nowy podział ról i obowiązków na początku może spowodować zamieszanie
- Rozmyty sposób raportowania w komunikacji wewnętrznej
- Problemy personalne wywołane zmianą

Bezsprzecznie konwergencja jest procesem dopasowania, modelowania do partykularnych wymagań każdej organizacji w ujęciu poszczególnych usług biznesowych, stąd z założenia nie jest

procesem łatwym. Aby się udała, musi posiadać zrozumienie i wsparcie osób decyzyjnych, za co odpowiadają poszczególne działy bezpieczeństwa, a te, w takim wypadku, powinny wypracować chęć do budowania wspólnych procesów i dzielenia się między sobą praktyką.

Dążenie do współpracy wydaje się w kwestii bezpieczeństwa organizacji naturalną kolejną rzeczą. Weźmy przykład samochodu. Zakładam, że każdy świadomy kierowca chciałby, aby jego auto było konwergentne pod względem bezpieczeństwa, czyli spełniało wszystkie poniższe warunki:

- było zbudowane z solidnych materiałów ze strefą zgniotu zapewniającą w razie wypadku wystarczający margines – to bezpieczeństwo fizyczne,
- było wyposażone w elektronikę, której można ufać, bez błędów oprogramowania w sterowaniu systemami bezpieczeństwa (np. kontrolą trakcji czy ABS) – to cyberbezpieczeństwo,
- spełniało normy spalania, było maksymalnie przyjazne środowisku, a do jego wytworzenia nie były wykorzystywane komponenty z niesprawdzonych źródeł – to bezpieczeństwo korporacyjne, regulacyjne, łańcucha dostaw.

Budowa i utrzymanie połączonych zespołów bezpieczeństwa wpływa również na koszty związane z ich utrzymaniem i obsługą procesów. Zgodnie z raportem *The State of Security Convergence in the United States*, opracowanym przez ASIS, połączenie zespołów bezpieczeństwa fizycznego i cyberbezpieczeństwa przyniosło kilkuprocentowy spadek kosztów ich utrzymania. Według organizacji ankietowanych przez ASIS aż 72% stwierdziło poprawę ogólnie pojętego bezpieczeństwa organizacji dzięki wprowadzonym zmianom.

Obecnie używane technologie wymiany informacji w branży zabezpieczeń elektronicznych są rozwiązaniami ze świata informatyki, coraz większą popularnością cieszą się również rozwiązania chmurowe. Urządzenia końcowe (np. kamery) są wyposażane w coraz wydajniejsze algorytmy analizy obrazu wideo. Wiąże się z tym zarówno korzyści, jak i zagrożenia, z którymi funkcjonujący w ramach silosu dział bezpieczeństwa fizycznego może sobie nie poradzić.

Sztuczna inteligencja poparta bardzo dużymi mocami obliczeniowymi w momencie nieautoryzowanego przechwycenia materiałów wideo z kamer może generować obraz identyczny z rzeczywistym lub na jego podstawie generować nowe zdarzenia, sprawiając, że system ochrony staje się wektorem ataku. Czy w pojedynkę, jako silos, jesteśmy w stanie efektywnie się przed tym obronić? ●



Tomasz Dacka

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



Jak otrzymać certyfikat B dla wyrobów stosowanych w systemach bezpieczeństwa pożarowego

Zadaniem odbiorcy wyrobu budowlanego, m.in. projektanta lub instalatora systemów przeciwpożarowych, jest sprawdzenie, czy wyrób ma odpowiednie właściwości użytkowe, czy został on oznaczony znakiem budowlanym B i czy wystawiono dla niego Krajową Deklarację Właściwości Użytkowych.

Grzegorz Mroczo

Krajowe systemy oceny i weryfikacji stałości właściwości użytkowych dotyczą tylko tych wyrobów budowlanych, dla których nie opublikowano europejskich norm zharmonizowanych (hEN) czy Europejskich Ocen Technicznych (EOT).

W Polsce obowiązek oceny wyrobów budowlanych w systemie krajowym został zapisany w ustawie o wyrobach budowlanych (Dz.U. z 2021 r., poz. 1213) i aktach wykonawczych. Przepisy te wskazują, że wyroby budowlane objęte jednym z krajowych systemów oceny – tzn. spełniające warunek braku norm hEN i EOT – powinny być oznakowane znakiem budowlanym B przed wprowadzeniem do obrotu.

Systemy oceny wyrobów budowlanych w Polsce

W Polsce funkcjonuje pięć systemów oceny stałości właściwości użytkowych (tabela: *Systemy oceny i weryfikacji stałości właściwości użytkowych*). Są one oznaczone numerami 1+, 1, 2+, 3, 4, przy czym przeprowadzenie oceny w systemie 4 jest dla producenta najłatwiejsze, a najbardziej wymagający jest system oceny 1+. To, według jakiego systemu oceniany będzie wyrób, zależy od złożoności wyrobu, jego funkcji i co za tym idzie, jaki wpływ będzie mieć dany produkt na to, czy obiekt spełnia podstawowe wymagania bezpieczeństwa pożarowego.

System 1 jest najczęściej stosowany

Większość wyrobów budowlanych stosowanych w systemach bezpieczeństwa pożarowego obiektów budowlanych jest oceniana za pomocą systemu 1. Tylko nieliczne podlegają ocenie za pomocą bardziej restrykcyjnych, lub odwrotnie, łagodniejszych kryteriów. Tak więc:

- kable w zależności od klasy reakcji na ogień oceniane są za pomocą systemów 1+, 3 bądź 4,
- kable, zespoły kablowe i puszki instalacyjne w zastosowaniach podlegających wymaganiom dotyczącym odporności ogniowej – w systemie 1+.

Schemat postępowania w krajowym systemie 1 oceny i weryfikacji stałości właściwości użytkowych



Wyrób

- zamierzone zastosowanie
- specyfikacja techniczna
- PN albo
- KOT



Badania laboratoryjne



Ocena zakładowej kontroli produkcji



Krajowy certyfikat stałości właściwości użytkowych KCSWU



Krajowa deklaracja właściwości użytkowych KDWU



Oznakowanie wyrobu znakiem budowlanym B



→ System oceny i weryfikacji stałości właściwości użytkowych

Stopień normy	Dokument upoważniający producenta do wystawienia krajowej deklaracji właściwości użytkowych	Dokument upoważniający producenta do wprowadzenia wyrobu do obrotu lub udostępnienia na rynku krajowym
1+ (system 1 rozszerzony o kontrolne badania próbek wyrobu w ramach nadzoru nad KCSWU)	Krajowy certyfikat stałości właściwości użytkowych wydany na zgodność z: • Polską Normą wyrobu albo • Krajową Oceną Techniczną w przypadku braku Polskiej Normy wyrobu	Krajowa deklaracja właściwości użytkowych wydana przez producenta wyrobu
1	Krajowy certyfikat stałości właściwości użytkowych wydany na zgodność z: • Polską Normą wyrobu albo • Krajową Oceną Techniczną w przypadku braku Polskiej Normy wyrobu	Krajowa deklaracja właściwości użytkowych wydana przez producenta wyrobu
2+	Krajowy certyfikat zgodności zakładowej kontroli produkcji wydany na zgodność z: • Polską Normą wyrobu albo • Krajową Oceną Techniczną w przypadku braku Polskiej Normy wyrobu	Krajowa deklaracja właściwości użytkowych wydana przez producenta wyrobu
3	• Sprawozdanie z oceny i weryfikacji wyrobu przez Laboratorium Badawcze na zgodność z Polską Normą albo • Krajowa Ocena Techniczna w przypadku braku Polskiej Normy wyrobu (ocena i weryfikacja wyrobu przez Laboratorium Badawcze jest wykonywana na potrzeby procesu udzielenia KOT)	Krajowa deklaracja właściwości użytkowych wydana przez producenta wyrobu
4	• Sprawozdanie z oceny i weryfikacji wyrobu przez producenta na zgodność z Polską Normą albo • Krajowa Ocena Techniczna w przypadku braku Polskiej Normy wyrobu (ocena i weryfikacja wyrobu przez producenta jest wykonywana na potrzeby procesu udzielenia KOT)	Krajowa deklaracja właściwości użytkowych wydana przez producenta wyrobu

Specyfikacjami technicznymi (nazywanymi też dokumentami odniesienia) w krajowym procesie oceny wyrobów budowlanych są Polskie Normy wyrobu albo Krajowe Oceny Techniczne. Dokumenty te wskazują m.in.:

- wymagania w zakresie konstrukcji wyrobu, funkcji oraz odporności i wytrzymałości wyrobu na warunki, jakie mogą wystąpić w przewidywanym środowisku pracy wyrobu zgodnie z zamierzonym jego zastosowaniem,
- system oceny i weryfikacji stałości właściwości użytkowych właściwy dla danego wyrobu,
- wymagania dla systemu zakładowej kontroli produkcji właściwe dla organizacji i kontroli produkcji danego wyrobu.

Na podstawie tych dokumentów ocenia się:

- wyrób – poprzez badanie wyrobu w laboratoriach badawczych i ocenę dokumentacji wyrobu oraz
- zakłady produkcyjne – w ramach oceny Zakładowej Kontroli Produkcji.

Polskie Normy wyrobu stosowane do oceny wyrobów budowlanych

W przypadku wyrobów służących do ochrony przeciwpożarowych opracowano niewiele Polskich Norm, a nieliczne stanowią normy europejskie nieposiadające statusu zharmonizowanego. Oznacza to, że większość wyrobów jest oceniania na podstawie Krajowych Ocen Technicznych. Ze względu na problemy z publikacją i harmonizacją norm europejskich część komitetów technicznych Europejskiego Komitetu Normalizacyjnego decyduje się na publikowanie norm jako niezharmonizowanych (czyli bez załącznika ZA). Kilka norm opublikowano

z załącznikiem ZA, mimo że nie zostały zharmonizowane. W efekcie nie zostały one zaakceptowane przez Komisję Europejską jako zharmonizowane, zatem nie opublikowano odniesienia do nich w Dzienniku Urzędowym Unii Europejskiej (*Official Journal of the European Union*). Oznacza to, że nie ustalono dla nich okresu przejściowego, ale też nie mogą być stosowane do oceny wyrobów w systemach europejskich prowadzących do oznakowania CE.

Normy te można natomiast z powodzeniem stosować w krajowych systemach oceny, a przepisy krajowe taką możliwość przewidują. Na przykład dla czujek ciepła liniowych kasowalnych normą niezharmonizowaną, którą można stosować w krajowych systemach oceny, będzie PN-EN 54-22+A1:2020, a dla kanałowych czujek dymu sięgnąć należy po normę PN-EN 54-27:2015. Osoby szukające normy dla urządzeń elektrycznych do wykrywania tlenku węgla w pomieszczeniach domowych powinny sięgnąć po dokument o numerze PN-EN 50291-1:2018+AC:2021.

Krajowe oceny techniczne

Krajowa ocena techniczna (KOT) to dokument opracowywany na zlecenie producenta lub dostawcy dla wyrobów, dla których została spełniona jedna z przesłanek:

- wyrób nie jest objęty Polską Normą,
- metoda oceny co najmniej jednej zasadniczej charakterystyki określona w PN tego wyrobu nie jest właściwa,
- brak w PN metody oceny co najmniej jednej zasadniczej charakterystyki tego wyrobu.

Wydanie KOT jest uregulowane rozporządzeniem Ministra Infrastruktury i Budownictwa z dnia 17 listopada 2016 r. w sprawie krajowych ocen technicznych (*Dz.U. z 2016 r., poz. 1968*). Krajowe oceny techniczne

są wydane przez jednostki oceny technicznej (JOT) lub krajowe jednostki oceny technicznej (KJOT) wyznaczone przez Ministra właściwego do spraw budownictwa, planowania i zagospodarowania przestrzennego oraz mieszkalnictwa. Wykaz takich jednostek można znaleźć na stronie Głównego Urzędu Nadzoru Budowlanego (www.gunb.gov.pl). Obecnie funkcjonuje łącznie osiem takich jednostek, z czego pięć upoważniono do wydawania europejskich ocen technicznych.

Proces udzielania krajowej oceny technicznej obejmuje m.in.

- analizę ryzyka przez określenie możliwych zagrożeń i korzyści związanych ze stosowaniem ocenianego wyrobu budowlanego przy wykonywaniu robót budowlanych,
- ustalenie kryteriów technicznych oceny właściwości użytkowych wyrobu budowlanego wynikających z przepisów techniczno-budowlanych i wiedzy technicznej,
- określenie metod oceny wyrobu budowlanego do oceny właściwości użytkowych wyrobu,
- określenie wymagań w odniesieniu do zakładowej kontroli produkcji w celu zapewnienia stałości właściwości użytkowych wyrobu budowlanego w procesie produkcyjnym tego wyrobu.

Krajowa Ocena Techniczna (KOT) zawiera m.in.

- oznaczenie typu i opis techniczny wyrobu budowlanego, którego dotyczy,
- zamierzone zastosowanie, zakres i warunki stosowania wyrobu oraz, w miarę potrzeb, warunki jego użytkowania, montażu i konserwacji,
- właściwości użytkowe wyrobu budowlanego wyrażone w poziomach lub klasach albo w sposób opisowy oraz metody ich badań i obliczeń,
- system oceny właściwy dla tego wyrobu,
- datę wydania i termin ważności KOT – standardowo 5 lat.

Krajowy certyfikat stałości właściwości użytkowych (KCSWU)

Proces oceny danego wyrobu w systemach 1 i 1+ kończy się wydaniem dla tego wyrobu krajowego certyfikatu stałości właściwości użytkowych. Zajmuje się tym jednostka mająca akredytację Polskiego Centrum Akredytacji (PCA) w zakresie danej normy wyrobu lub krajowej oceny technicznej. Bazę akredytowanych jednostek certyfikujących można znaleźć na stronie PCA.

Krajowa deklaracja właściwości użytkowych (DWU)

Po otrzymaniu certyfikatu producent powinien sporządzić dla wyrobu krajową deklarację właściwości użytkowych. Powinna być ona wystawiona w języku polskim i może być dostępna na stronie internetowej. Wzór krajowej deklaracji właściwości użytkowych jest zawarty w załączniku nr 2 do rozporządzenia Ministra Infrastruktury i Budownictwa z 17 listopada 2016 r. w sprawie sposobu deklarowania właściwości użytkowych wyrobów budowlanych oraz sposobu znakowania ich znakiem budowlanym (*Dz.U. z 2016, poz. 1966 z późn. zm.*).

Znakowanie wyrobu budowlanego znakiem budowlanym B

Po wystawieniu deklaracji właściwości użytkowych producent ma prawo umieścić na wyrobie znak budowlany B. W ten sposób przejmuje odpowiedzialność za zgodność wyrobu z deklarowanymi właściwościami użytkowymi.

Najważniejsze wnioski

- Krajowymi systemami oceny właściwości użytkowych objęte są wyroby budowlane, dla których nie istnieją normy europejskie wyrobu zharmonizowane z rozporządzeniem 305/2011 ani Europejskie Oceny Techniczne.
- Specyfikacjami technicznymi w procesie oceny wyrobu są Polskie Normy niezharmonizowane, a w razie ich braku – Krajowe Oceny Techniczne.
- W zależności od ustalonego dla wyrobu systemu oceny i weryfikacji stałości właściwości użytkowych producent musi uzyskać inne dokumenty upoważniające do wystawienia deklaracji właściwości użytkowych. W procesie oceny uczestniczą różne podmioty – producent, laboratorium badawcze, akredytowana jednostka certyfikująca system ZKP, akredytowana jednostka certyfikująca wyroby.
- W systemach 1 i 1+ producent jest zobowiązany uzyskać Krajowy Certyfikat Stałości Właściwości Użytkowych przed wystawieniem Krajowej Deklaracji Właściwości Użytkowych.
- Po wystawieniu KDWW producent może oznakować wyrób znakiem budowlanym B.
- Treść KDWW powinna być spójna z KCSWU i wymieniać te właściwości użytkowe wyrobu, które zostały potwierdzone certyfikatem.

Znak budowlany należy umieścić w sposób widoczny, czytelny i trwały bezpośrednio na wyrobie albo na etykiecie przymocowanej do tego wyrobu. Jeżeli umieszczenie znaku B nie jest możliwe ze względu na wielkość lub charakter wyrobu budowlanego, znak umieszcza się na opakowaniu jednostkowym lub zbiorczym wyrobu budowlanego albo na dokumentach towarzyszących wyrobowi.

Zadaniem odbiorcy wyrobu jest sprawdzenie, czy wyrób został oznakowany znakiem budowlanym B i wystawiono dla niego KDWW, a także czy wskazane w KDWW zamierzone zastosowanie wyrobu i jego właściwości użytkowe są odpowiednie dla danego miejsca zastosowania – rodzaj obiektu budowlanego, wymagania w zakresie wykonania obiektu, przewidywane warunki stosowania/działania wyrobu, adekwatność funkcji wyrobu, odporność na możliwe do wystąpienia warunki w miejscu instalacji (klasa środowiskowa, stopień ochrony obudowy, zimno, gorąco, wilgotność, w przypadku urządzeń elektrycznych odporność na zakłócenia elektromagnetyczne) itp. ●

mł. bryg. mgr inż. GRZEGORZ MROCZKO

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





Nowe wyzwania, nowe pomysły, innovacyjne rozwiązania! Nie zwalniamy tempa!

rozpoczynamy zatem, celebrując nasze 25-lecie jako polskiej spółki prawa handlowego. Będziemy świętować przez cały rok, spotykając się z naszymi klientami, partnerami, sympatykami i przyjaciółmi podczas licznych wydarzeń, które zaplanowaliśmy na najbliższe miesiące.

Po dwóch latach przerwy spowodowanej pandemią i jej długofalowymi skutkami, wróciliśmy do organizacji stacjonarnych szkoleń projektowych poza Warszawą, w największych miastach w kraju. Cykl spotkań z projektantami instalacji niskoprądowych rozpoczęliśmy w Poznaniu, w szkoleniu wzięło udział prawie 70 osób. Do czerwca br. odbędą się podobne prezentacje naszych rozwiązań i narzędzi do projektowania w Gdańsku, we Wrocławiu, w Krakowie, Katowicach i Rzeszowie. Udział w szkoleniu to okazja nie tylko do poznania najnowszej oferty Schrack Seconet, ale przede wszystkim możliwość spotkania z innymi specjalistami z danego regionu oraz przedstawicielami producenta. To także czas na wymianę doświadczeń i odpowiedzi na najczęściej pojawiające się pytania związane z projektowaniem i realizacją zabezpieczeń przeciwpożarowych.

Już w marcu spotkamy się podczas corocznego spotkania najlepszych partnerów z przedstawicielami firm reprezentujących Schrack Seconet na rynku polskim. To okazja do podsumowania minionego roku, analizy doświadczeń, wypracowania wspólnych wniosków, które pozwolą całej naszej grupie partnerskiej jeszcze lepiej i rzetelniej przygotować się do realizacji kolejnych, wymagających inwestycji. Schrack Seconet może poszczycić się doskonałą siecią partnerską, do której należą firmy, które charakteryzuje olbrzymie doświadczenie i doskonałe przygotowanie do świadczenia usług najbardziej wymagającym klientom. Kompetencje partnerów potwierdzają odpowiednie certyfikaty uzyskiwane po odbyciu szeregu szkoleń. Coroczne spotkania z przedstawicielami firm partnerskich to także okazja do przyznania nagród i wyróżnień firmom, które w minionym roku zrealizowały najwyższą sprzedaż czy wykonały najbardziej skomplikowane, nietypowe i wymagające instalacje.

Początek drugiego kwartału rozpoczną prace nad naszym największym projektem edukacyjnym – kolejną jubileuszową edycją Ogólnopolskich Dni Zintegrowanych Systemów Bezpieczeństwa Pożarowego – Schrack Seconet i Partnerzy. Zaangażowanie przedstawicieli wielu obszarów szeroko rozumianego rynku bezpieczeństwa, kilkunastu firm partnerskich, producentów, instytucji

Schrack Seconet to jeden z największych i najbardziej znanych producentów systemów ochrony przeciwpożarowej na świecie. Nasza siła to przede wszystkim najwyższej jakości niezawodne produkty oraz efektywne kompleksowe rozwiązania tworzone z myślą o indywidualnych potrzebach klientów.

Każdy kolejny rok przynosi nowe wyzwania. Stale poszerzamy gamę produktów dla wymagających i świadomych klientów w Polsce, organizujemy wydarzenia edukacyjne, wychodząc naprzeciw oczekiwaniom specjalistów działających w obszarze systemów bezpieczeństwa. Śledzimy na bieżąco sytuację ekonomiczną w kraju i na świecie, dostosowując nasze kolejne działania do aktualnych oczekiwań rynku.

Marka Schrack Seconet jest obecna na rynku polskim od ponad 35 lat. Pierwsze obiekty zabezpieczaliśmy w połowie lat 80. ubiegłego wieku, działając jako przedstawicielstwo firmy austriackiej.

W 1998 roku powstała Schrack Seconet Polska sp. z o.o., która rozwija się dynamicznie, ani na chwilę nie zwalniając tempa. Rok

i organizacji opiniotwórczych, jednostek certyfikujących oraz indywidualnych ekspertów gwarantuje najwyższy poziom edukacyjny wydarzenia. Jubileuszowa, dziesiąta już edycja odbędzie się w pierwszym tygodniu października w hotelu Windsor w Jachrance. Już dziś zapraszamy zainteresowanych pogłębieniem wiedzy i szczegółową analizą problemów pojawiających się w trakcie projektowania i realizacji obiektów różnego przeznaczenia.

Podczas tegorocznej edycji Ogólnopolskich Dni Zintegrowanych Systemów Bezpieczeństwa Pożarowego Schrack Seconet zaprezentuje kompleksowe i spójne rozwiązania techniczne, poczynając od detekcji pożaru (centrale INTEGRAL EvoX), poprzez zasilanie i sterowanie urządzeń ppoż. (centrala sterująco-zasilająca SIS-POWER), skończywszy na certyfikowanych systemach integrujących urządzenia przeciwpożarowe (SIUP) SIS-FIRE. Najnowszy produkt SIS Power umożliwia zasilanie i sterowanie takich urządzeń jak wentylatory oddymiające, napowietrzające, klapy na wentylacji pożarowej i inne zapewniające bezpieczeństwo ppoż. budynku oraz sterowanie nimi. SIS Power gwarantuje także bezpieczną ewakuację na wypadek pożaru. Możliwości wszystkich naszych rozwiązań, a także oferowanych przez partnerów naszego wydarzenia zostaną zaprezentowane podczas tegorocznej edycji największego w branży spotkania edukacyjnego.

W roku 2023 szczególną uwagę zwracamy także na tempo zmian, szybki rozwój technologiczny, pojawiające się coraz częściej najnowocześniejsze rozwiązania także w obszarze systemów bezpieczeństwa pożarowego. Tematem aktualnym jest dziś sztuczna inteligencja nazywana technologią przyszłości. Najprościej ujmując, to zdolność maszyn do wykonywania zadań wykonywanych przez ludzi, wymagających rozumowania, uczenia się, planowania i kreatywności. Czy i w jakim stopniu sztuczna inteligencja zastąpi w przyszłości człowieka, tego jeszcze nie wiemy, zdajemy sobie jednak sprawę, że już dziś umożliwia ona wielu systemom technicznym radzenie sobie z tym, co rejestrują, i rozwiązywanie pojawiających się problemów, dążąc przy tym do osiągnięcia określonego celu.

Mając to na względzie, musimy wdrażać w zarządzanie bezpieczeństwem pożarowym takie rozwiązania, które pozwolą na optymalizację obecności człowieka na etapie rozpoznawania zagrożenia. Udział człowieka nadal jest konieczny w momencie podejmowania decyzji strategicznych. Natomiast prace poboczne, zadaniowe, już dziś mogą być wykonywane, także zdalnie, dzięki wsparciu świetnie zaprogramowanych narzędzi.

Jako producent inteligentnych rozwiązań do zarządzania ochroną przeciwpożarową wprowadziliśmy na rynek polski platformę informatyczną S2Service pracującą w chmurze, z zastosowaniem najwyższych standardów bezpieczeństwa. Narzędzie ma szereg innowacyjnych funkcji poprawiających jakość usług na każdym etapie procesów wdrożeniowych i serwisowych. Umożliwia m.in. dostęp do dokumentacji projektowej, zarządzanie obiektami, analizę systemu, rozbudowę i modernizację, konserwację, pozwala także zdalnie zarządzać zdarzeniami. Platforma S2Service wspiera przede wszystkim zarządzanie ludźmi odpowiedzialnymi za bezpieczeństwo w poszczególnych obiektach, najczęściej rozproszonych. W tym roku będziemy wdrażać nasze inteligentne rozwiązania w kolejnych zaawansowanych technologicznie obiektach, żeby jeszcze bardziej ułatwić sprawne zarządzanie obiektem podczas pojawiającego się zagrożenia.

Rok 2023 to dla nas przede wszystkim czas wprowadzania rozwiązań innowacyjnych. Kolejne produkty pojawią się w ofercie Schrack Seconet, pracujemy też nad udoskonalaniem

OUR 25 YEARS BY SCHRACK SECONET

» Wspólnie
celebruje 25-lecie
Schrack Seconet
Polska jako polskiej
spółki prawa
handlowego. «

naszych sztanदारowych rozwiązań, będących trzonem oferowanego przez nas poczucia najwyższego bezpieczeństwa.

Nasza ponad 35-letnia historia działalności w Polsce pozwala spokojnie patrzeć w przyszłość. Zmierzyliśmy się z trudną, pandemiczną sytuacją, zawirowaniami na rynku międzynarodowym spowodowanymi przede wszystkim z dostępnością wielu komponentów i stale rosnącymi cenami. Mimo problemów z wydłużonymi terminami dostaw zakończyliśmy rok 2022 rekordową sprzedażą, co jest zdecydowanym sukcesem dla całej naszej grupy partnerskiej – wszystkich firm autoryzowanych, generalnych wykonawców i inwestorów, którzy zaufali nam i naszym rozwiązaniom.

Ostatnie 5 lat w historii firmy to szereg zmian, nowa siedziba główna w Warszawie, zmiana na stanowisku prezesa Schrack Seconet w Polsce, nowa osoba zarządzająca oddziałem w Gdańsku, kilku nowych pracowników. Zmieniamy się i jednocześnie rośniemy w siłę, wyciągamy wnioski z naszych doświadczeń, jeszcze lepiej planujemy przyszłość.

Już dziś zapraszamy serdecznie do naszej zmodernizowanej sali szkoleniowej w Warszawie. Można w niej zobaczyć cały przekrój działających systemów sygnalizacji pożarowej, od najstarszych jak BMZ 85, BMZ Compact, BMZ S2L, BMZ Integral, Integral Evolution, Integral IP aż po najnowocześniejszy Integral EvoX. Z przyjemnością zaprezentujemy także możliwości m.in. systemów przyzywowych Schrack Seconet, dźwiękowego systemu ostrzegawczego szwajcarskiego producenta g+m, certyfikowanego systemu zarządzania bezpieczeństwem pożarowym SIS-FIRE, centralę sterująco-zasilającą urządzeniami przeciwpożarowymi SIS-POWER i wszystkie narzędzia do zdalnego zarządzania bezpieczeństwem pożarowym.

Zapraszamy również do udziału we wszystkich wydarzeniach organizowanych przez Schrack Seconet w Polsce, podczas których będziemy wspólnie świętować nasz jubileusz. Lista zaplanowanych szkoleń jest dostępna na stronie: wydarzenia.schrack-seconet.pl.

O wszystkich pozostałych wydarzeniach będziemy informować w bieżących komunikatach. Zapraszamy do współpracy! ●



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



Część 1-1 normy Systemy dozoru wizyjnego stosowane w zabezpieczeniach dostępna już po polsku

Istotna dla branży zabezpieczeń norma Systemy dozoru wizyjnego stosowane w zabezpieczeniach (PN-EN 62676) dotychczas została przetłumaczona na język polski tylko w jednej części - czwartej. Teraz dołącza do niej także kolejna – część 1-1.

Waldemar Więckowski

Polski Komitet Normalizacyjny wygospodarował odpowiednie środki, dzięki czemu została przetłumaczona część 1-1, Wymagania systemowe – Postanowienia ogólne (PN-EN 62676-1-1).

Kto powinien sięgać po normę PN-EN 62676-1-1:2014-06P

Widniejący na stronie PKN opis tej części normy nie oddaje w pełni jej zakresu, ale zawiera zdanie, którego pierwsza część wskazuje, do kogo jest adresowana:

Niniejsza norma zawiera minimalne wymagania funkcjonalne i eksploatacyjne, do uzgodnienia w wymaganiach użytkowych między klientem, organami ścigania, jeśli dotyczy, a dostawcą, ale nie obejmuje wymagań dotyczących projektowania, planowania, instalowania, testowania, użytkowania ani konserwacji.

To, o czym mówi druga część zdania (wymagania dot. projektowania...), jest przedmiotem wcześniej przetłumaczonej czwartej części normy PN-EN 62676-4:2015-06P – Wytyczne stosowania.

Normy PN-EN 62676-1-1:2014-06P i PN-EN 62676-4:2015-06P zawierają informacje, które zasadniczo powinny wystarczyć inwestorowi do takiego zaplanowania i poprowadzenia inwestycji w system dozoru wizyjnego (VSS), aby mógł on precyzyjnie określić specyfikację zamówienia dla dostawcy. W przypadku rozbieżności norma udostępnia inwestorowi merytoryczne narzędzie ułatwiające rozstrzygnięcie sporu z dostawcą. (Pozostałe części normy PN-EN 62676 dotyczą szczegółowych zagadnień technicznych – w większości przypadków inwestor nie będzie potrzebował do nich sięgać, chyba że konsultant bądź projektant mu to wskażą).

O projektantach systemów dozoru wizyjnego jako o adresatach normy wspominam dla porządku, bo to oczywiste, że powinni się nią posługiwać.

Jak norma przedstawia system dozoru wizyjnego

Przyjrzyjmy się zawartym w normie PN-EN 62676-1-1:2014-06P „minimalnym wymaganiom funkcjonalnym i eksploatacyjnym, do uzgodnienia w wymaganiach użytkowych między klientem (...) a dostawcą”.

Kluczowe jest zrozumienie, z czego składa się system dozoru wizyjnego. Wbrew pozorom wcale nie jest to takie oczywiste, zapewne dlatego temu zagadnieniu poświęcono rozdział 4.

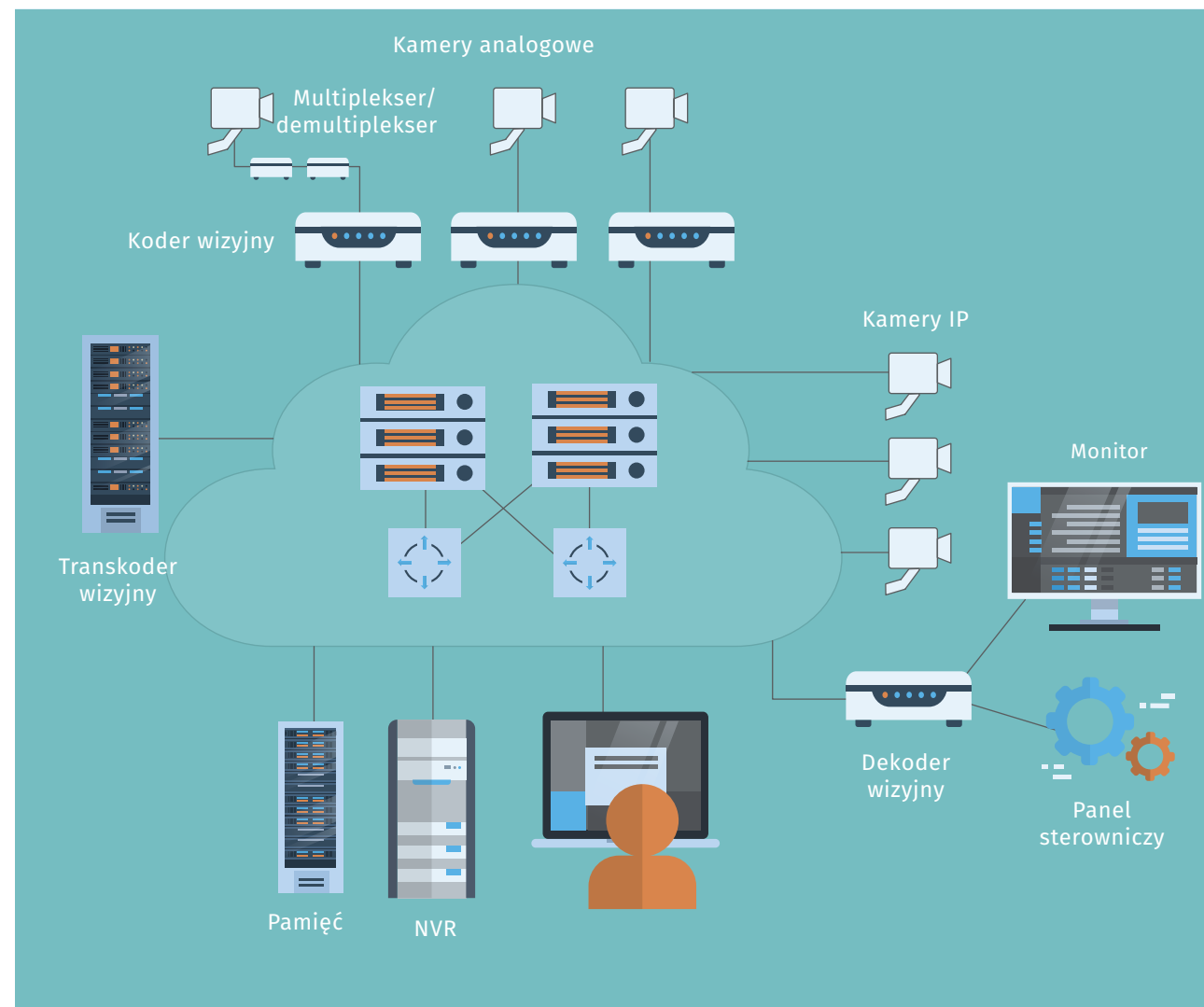
System dozoru wizyjnego przedstawia się jako bloki funkcjonalne oraz relacje między nimi. Obrazowo te bloki funkcjonalne, reprezentujące różne części i funkcje systemu pokazano w normie (patrz rys. *Bloki funkcjonalne...*) oraz szczegółowo opisano. Przedstawiony w normie model VSS abstrahuje od definiowania poszczególnych urządzeń i wymagań ich dotyczących. Wynika to z uznania faktu, że technologia, a wraz z nią sprzęt VSS i jego funkcjonalności rozwijają się i zmieniają zbyt szybko, aby je poddawać normalizacji. Funkcje realizowane przez VSS natomiast pozostają niezmienne niezależnie od tego, jakie urządzenia są dostępne na rynku w danym okresie.

Jak to się dzieje, że dla branży zabezpieczeń odpowiedź na pytanie, z czego składa się system dozoru wizyjnego, może nie być oczywista? Otóż wynika to z faktu swoistej narracji, która zdominowała branżę zabezpieczeń na temat VSS. Przez ostatnich 20 lat technologia ta rozwijała się niezwykle dynamicznie. W jej rozwój angażuje się coraz więcej producentów, a wielu z nich wywodzi się spoza branży zabezpieczeń. Rynek zabezpieczeń nieustannie rośnie, a konkurencja wśród producentów jest ostra. Nic więc dziwnego, że w dyskusji o nowościach i trendach dominują „prawdy” głoszone przez producentów sprzętu i oprogramowania. Siłą rzeczy w tej narracji na system nadzoru wizyjnego składają się przede wszystkim

Bloki funkcjonalne systemu dozoru wizyjnego



Sprzętowy model systemu dozoru wizyjnego



urządzenia i oprogramowanie (parametry techniczne i połączenia). Funkcje realizowane przez systemy dozoru wizyjnego w zabezpieczeniach schodzą na plan dalszy, jeżeli w ogóle są przywoływane.

Kształt systemu dozoru wizyjnego lansowany przez producentów można zilustrować za pomocą sprzętowego modelu VSS przedstawionego w normie PN-EN 62676-2-1:2014-06E – Protokoły transmisji wizji – Wymagania ogólne (patrz rys. powyżej).

Ta część normy jest poświęcona wspólnym ramom transmisji IP wizji, umożliwiającym osiągnięcie międzyoperacyjności (interoperability) wyrobów, a przywołany sprzętowy model stanowi przykład sieci urządzeń wizyjnych wyposażonych w interfejs IP i kodujących bądź dekodujących wizję (np. koder, dekodek, NVR, VMS).

Innymi słowy, sprzętowy model VSS to model prezentujący urządzenia nadające bądź odbierające sygnał IP wizji oraz kanały przesyłowe dla tego sygnału.

Istotna jest różnica zakresów zagadnień dotyczących systemów dozoru wizyjnego, które ilustrują oba modele, czyli ten opisany przez bloki funkcjonalne systemu dozoru wizyjnego i ten przedstawiony w sprzętowym modelu systemu dozoru wizyjnego.

Wszystkie zagadnienia, które opisuje sprzętowy model VSS, mieszczą się w części Środowisko wizyjne ujętej w modelu funkcjonalnym. Sprzętowy model VSS nie ujmuje bowiem zagadnień zarządzania oraz zabezpieczenia systemu dozoru wizyjnego.

Tymczasem producenci, ale także wielu projektantów, mówiąc o systemach dozoru wizyjnego, skupia się na sprzętowym modelu VSS. Z kolei użytkownik musi mieć na względzie znacznie szerszy zakres działania takiego systemu, czyli ten opisywany przez model bloków funkcjonalnych... I dlatego też powinien móc wyspecyfikować funkcje, które pozwolą zrealizować cele prowadzenia dozoru wizyjnego wyznaczone w systemie zabezpieczeń. Tworząc dokument Wymagania użytkowe (Program funkcjonalno-użytkowy), powinien poruszać się w szerokim obszarze zagadnień opisanych modelem funkcjonalnym.

Ocena ryzyka

Stopniowanie zabezpieczeń – jako element analizy zagrożeń i oceny ryzyka – w normie PN-EN 62676-4:2015-06P jest ujęte jako etap procedury wdrożenia VSS realizowany przed jego zaprojektowaniem. Ten etap ma pomóc w dokładnym określeniu celu stosowania

systemu dozoru wizyjnego i takiemu zaprojektowaniu VSS, które zmniejszy szacowane ryzyko. W odniesieniu do projektowania norma zawiera stwierdzenie, które warto polecić uwadze inwestorów: Nie istnieje jeden modelowy projekt dla VSS. Każdy VSS jest systemem „szytym na miarę” – planowanym, projektowanym i produkowanym jednostkowo. Zasady oceny ryzyka opisano w normie ISO 31000:2019.

Stopniowanie zabezpieczeń

Stopniowanie zabezpieczenia wprowadzono najpierw w 1997 r. – w SSWiN (EN 50131-1:1997). Następnie w VSS – w 2010 r. normą EN 50132-1:2010 (która po czterech latach została zastąpiona przez omawianą normę PN-EN 62676-1-1:2014-06P), a w roku 2013 w elektronicznych systemach kontroli dostępu (norma EN 60839-11-1:2013).

Celem stopniowania zabezpieczeń (security grading) jest pomoc w podjęciu decyzji odnośnie do rodzaju niezbędnego systemu zabezpieczenia. Stopniowanie we wszystkich ww. systemach uwzględnia poziom ryzyka, który zależy od prawdopodobieństwa wystąpienia incydentu i potencjalnej szkody z nim związanej. Innymi słowy, stopień zabezpieczenia jest miarą odporności (zabezpieczenia) na wpływy zewnętrzne i atak intruza. Stopień 1. obejmuje najniższe wymagania wobec systemu.

Podział ryzyka na cztery stopnie – dla każdego z wymienionych systemów – w pewnym sensie ułatwia specyfikację wymagań oraz projektowania dla tego samego obiektu.

Podmiot stopniowania (urządzenia, funkcje) jest różny dla SSWiN, VSS i EACS (SKD)! Niezrozumienie różnic może prowadzić do zasadniczych nieporozumień. Przykładem jest domaganie się certyfikatów wystawionych na zgodność z normą PN-EN 50131 – a więc dotyczącą SSWiN – dla urządzeń i systemów kontroli dostępu (objętych inną normą, PN-EN EN 60839-11).

W przypadku systemów dozoru wizyjnego stopniowaniu podlegają funkcje systemu, a nie jego elementy (urządzenia i oprogramowanie). Oczywiście nie sposób abstrahować od faktu, że funkcje są realizowane przez urządzenie i jego oprogramowanie. Dlatego norma PN-EN 62676-4:2015-06P zaleca, aby tam, gdzie ma to zastosowanie, stopień zabezpieczenia był przypisany elementom, podsystemom i funkcjom VSS. Stwierdzenie to nie podważa faktu, że stopniowaniu podlegają funkcje – przyjęte dla nich stopnie są następnie przypisywane do elementów VSS.

W konsekwencji takiego ujęcia zrozumiałe stają się ograniczenia sprzętowego modelu VSS stosowanego w zabezpieczeniach. Systemowi należy nadać stopień ogólny. Poszczególne funkcje mogą mieć inne, różne stopnie zabezpieczenia w ramach jednego systemu, odpowiednio do zakresu zadań realizowanych przez VSS, ale przypisane funkcjom stopnie należy stosować konsekwentnie w całym systemie. Wyjątkami są detekcja sabotażu i ochrona przed nim, jako że poszczególne części systemu mogą mieć różny stopień ekspozycji na atak.

Norma zezwala na elastyczność, ale zalecane jest podejście najprostsze. Jeśli jeden, ten sam stopień może być zastosowany dla

wszystkich funkcji w systemie, należy dokładnie rozważyć możliwość skorzystania z takiego rozwiązania.

Norma wymienia 18 funkcji poddawanych stopniowaniu. Wybrane dla nich stopnie powinny być uzgodnione pomiędzy inwestorem a projektantem i zapisane w Wymaganiach użytkowych lub w Projekcie wstępnym systemu.

Stopniowanie należy stosować, gdy VSS jest podstawowym środkiem ograniczania ryzyka, tzn. gdy stanowi on – zgodnie z definicją normatywną 3.1.118 – tzw. istotne zastosowanie zabezpieczeń. Według autorów normy należy też mieć na uwadze, że ryzyka szacowane w trakcie analizy zagrożeń mogą być najskuteczniej ograniczone za pomocą innych środków niż VSS. Może się zdarzyć, że w trakcie analizy zagrożeń dojdziemy do wniosku, że lepsze skutki w ograniczaniu ryzyka

można uzyskać, zabezpieczając obiekt inaczej niż za pomocą VSS.

Stopniowanie obejmuje nie tylko funkcje VSS stanowiące bezpośrednio o zabezpieczeniu obiektu. Dotyczy również funkcji decydujących o ochronie samego systemu VSS, w tym przede wszystkim o dostępie do systemu. System chroni więc obiekt przed intruzem zarówno zewnętrznym, jak i wewnętrznym.

Stopniowanie zabezpieczeń nie dotyczy jakości obrazu ani scen przechwytywanych przez VSS związanych z celami prowadzenia dozoru wizyjnego (zadaniami operatora). Te kwestie zostały drobiazgowo przedstawione w normie PN-EN 62676-4:2015-06P.

Stopniowanie zabezpieczeń nie dotyczy klas wydajności wizji IP przedstawionych w PN-EN 62676-4:2015-06P i szczegółowo omówionych w PN-EN 62676-1-2:2014-06E. Logiczne jest jednak powiązanie tych klas w trakcie projektowania ze stopniowaniem zabezpieczeń.

Wymagania funkcjonalne

W normie wymieniono 18 funkcji VSS, które są poddawane stopniowaniu, co szczegółowo przedstawiono w rozdziale 6. opisywanej normy, który w całości poświęcono omówieniu wszystkich funkcji zawartych w funkcjonalnym modelu VSS. W ten sposób funkcje podlegające stopniowaniu są prezentowane w kontekście systemowym, a odbiorca normy uzyskuje czytelny i zrozumiały obraz stopniowania VSS.

Tłumaczenie kolejnej części normy ułatwi funkcjonowanie osobom i firmom z branży zabezpieczeń – stąd mój apel, by osoby zainteresowane zaangażowały się finansowo w kolejne tłumaczenia. ●



Waldemar Więckowski

Członek Komitetu Technicznego nr 52 ds. Systemów Alarmowych Włamania i Napadu przy PKN.

AAT SYSTEMY BEZPIECZEŃSTWA

System wideodomofonowy serii 100 marki Novus

Przeznaczony do domów oraz osiedli domów jednorodzinnych

Najnowszy system hybrydowy marki Novus to nowoczesny system oparty na technologii IP. Monitory i wybrane panele obsługują Wi-Fi, dzięki temu mogą również pracować w sieci bezprzewodowej. Nowoczesny design oraz wysoka jakość wykonania gwarantują wysoki komfort użytkowania.

NAJWAŻNIEJSZE MOŻLIWOŚCI:

- podgląd wideo,
- funkcja DVR (detekcja ruchu),
- rejestracja gości,
- poczta głosowa,
- interkom
- wysoka jakość audio,
- tryb nocny,
- możliwości personalizacji ustawień.

Monitory mogą wyświetlać obraz z paneli oraz z zamontowanych wokół domu kamer IP. Dzięki detekcji ruchu oraz detekcji człowieka (dotyczy wyłącznie paneli) obiekt jest chroniony przed osobami niepowołanymi. Obraz jest nagrywany na kartę microSD. Podczas podglądu obrazu można również zarejestrować obserwowany moment. Nagrania można później odtworzyć np. na monitorze. System rejestracji gości pozwala na zapisanie wideo lub zdjęć z wizyty. Na czas nieobecności można również nagrać informację, np. dla klientów, która zostanie odtworzona z głośnika umieszczonego w panelu wejściowym. Dzięki zastosowaniu wysokiej jakości systemu audio rozmowa zarówno przez domofon, jak i nagranie brzmi czysto i wyraźnie.

System serii 100 marki Novus umożliwia dopasowanie pracy domofonu do trybu życia jego użytkowników. Przykładowo dzięki

uruchomieniu trybu nocnego, głośny dzwonek o północy nie postawi na nogi całego domu. A dzięki ustawieniu ulubionego zdjęcia jako tła monitora i ulubionej piosenki w roli dzwonka, domofon staje się miłym dodatkiem do wnętrza. Tym bardziej, że może także stać się atrakcyjnie wizualnym zegarem lub odtwarzać ulubione zdjęcia wgrane na kartę SD monitora.

APLIKACJA MOBILNA

System wideodomofonowy serii 100 marki Novus można z powodzeniem obsługiwać przez urządzenia mobilne. Aplikacja pozwala na przekierowanie połączeń z paneli, rozmowę z gośćmi, odtwarzanie nagrań z pamięci wewnętrznej monitorów lub paneli, sterowanie bramą i furtką, podgląd z paneli oraz kamer IP z możliwością zapisu zdjęć i nagrywania filmów. Powiadomienia alarmowe wywołane przez funkcję detekcji ruchu mogą być wysyłane w formie push bezpośrednio na ekran urządzenia. ●



AXIS COMMUNICATIONS

Stałoogniskowa kamera kopułkowa wyposażona w funkcję głębokiego uczenia od Axis

Axis Communications prezentuje nową serię kamer kopułkowych AXIS M32, pozwalających na przeprowadzanie zaawansowanych analiz na brzegu sieci. Kamery mają fabrycznie wbudowaną aplikację AXIS Object Analytics, która umożliwia detekcję i klasyfikację obiektów z podziałem na ludzi, pojazdy oraz typy pojazdów.

AXIS M3215-LVE i AXIS M3216-LVE oparte na procesorze ARTPEC-8 oferują znakomitą jakość obrazu – odpowiednio: 2 i 4 Mpix. Dzięki technologiom Axis Lightfinder, Axis Forensic WDR oraz Axis OptimizedIR urządzeniem niestraszne są nawet najtrudniejsze warunki oświetleniowe, szczegóły obrazu, które są widoczne nawet przy słabym świetle.

Ponadto kamery przystosowane są do wykonywania zaawansowanych obliczeń dzięki odpowiednio dużej pamięci masowej. Pozwala to na gromadzenie i analizowanie jeszcze większej ilości danych na brzegu sieci. Dodatkowo, dzięki obsłudze platformy ACAP w wersji 4, do systemu można doinstalować dedykowane aplikacje oparte na głębokim uczeniu.

NAJWAŻNIEJSZE CECHY URZĄDZEŃ:

- znakomita jakość obrazu o rozdzielczości 2 i 4 Mpix,
- aplikacje Lightfinder, Forensic WDR i OptimizedIR,
- obsługa zaawansowanych analiz brzegowych,
- złącza audio i we/wy,
- wbudowane cyberbezpieczeństwa.

Kamery zostały wykonane w klasie IK10 i wyposażone w dodatkową osłonę pogodową, co zabezpiecza je przed działaniem mocnego słońca, deszczu oraz śniegu. Zostały także wyposażone w funkcję cyberbezpieczeństwa, takie jak Axis Edge Vault, która chroni identyfikator urządzenia i upraszcza uwierzytelnianie produktów Axis w sieci. ●

ROGER

Zarządzanie systemami bezpieczeństwa w module VISO SMS firmy Roger

VISO SMS to platforma przeznaczona do monitorowania, wizualizacji i zarządzania bezpieczeństwem w obiekcie. Dzięki niej operator uzyskuje przejrzysty obraz sytuacji w danym obszarze, by móc szybko zareagować na zaistniałe zdarzenia, takie jak pożar, włamanie czy awaria.

VISO SMS JEST ZINTEGROWANY Z SYSTEMAMI:

- sygnalizacji pożarowej (SSP): Bosch, Siemens;
- sygnalizacji włamania i napadu (SSWiN): SATEL, Honeywell;
- kontroli dostępu (SKD): Roger;
- telewizji dozorowej (CCTV): Milestone, Dahua, Hikvision, BCS, IPOX, Provision-ISR, EVOS, ONVIF;
- komunikacji (VoIP, SMS, e-mail);
- automatyki budynkowej.

Moduł VISO SMS umożliwia operatorom realizację scenariuszy bezpieczeństwa, czyli podpowiada, jakie czynności powinny być wykonane w danej sytuacji, i jednocześnie rejestruje wszystkie działania w postaci raportów i zestawień do późniejszej analizy. Dodatkowo może być wykorzystany do prowadzenia ewidencji wykonanych i planowanych prac konserwacyjnych oraz naprawczych.

VISO SMS może być z powodzeniem stosowany w obiektach wymagających zarządzania różnymi systemami zabezpieczeń z poziomu jednego oprogramowania. Do tych obiektów zaliczają się przede wszystkim biurowce, zakłady przemysłowe, stadiony, muzea, budynki administracji państwowej, ale także inne obiekty wymagające zastosowania rozwiązań klasy SMS (Safety Management System). ●



LINC POLSKA

Teledyne FLIR Elara R-190 | NOWOŚĆ – RADAR

Teledyne FLIR to nie tylko światowy lider w produkcji kamer termowizyjnych, ale również producent radarów. Terminale towarowe i bocznicie kolejowe to miejsca, w których dość często dochodzi do wtargnięć, kradzieży i zniszczenia mienia.

Ochrona tego typu obiektów jest utrudniona m.in. ze względu na rozległy i zróżnicowany teren, brak wystarczających zabezpieczeń w postaci ogrodzenia czy też ograniczone oświetlenie zabezpieczonego terenu. Wszystko to powoduje, że trudno zapewnić takim obiektom ochronę przed kradzieżą czy też aktami wandalizmu.

Wobec tego, czy jedynym sposobem na skuteczne zabezpieczenie tych obiektów jest ochrona fizyczna? Odpowiedź brzmi – nie. Z pomocą przychodzą radary. Urządzenia tego typu umożliwiają automatyczną detekcję intruzów, zarówno osób, jak i pojazdów oraz ich śledzenie w każdych warunkach atmosferycznych, przez całą dobę, 365 dni w roku.

Marka Teledyne FLIR, która swoją rozpoznawalność zawdzięcza znakomitym kamerom termowizyjnym, swoje portfolio wzbogaciła o radary. Najnowszy radar Teledyne FLIR Elara R-190 umożliwia jednocześnie śledzenie do 32 wykrytych celów i lokalizację każdego z nich. Kolejnym atutem radaru jest niski pobór prądu i duży zasięg detekcji. Dodatkową funkcjonalnością jest możliwość zintegrowania go z rozwiązaniami firm trzecich, np. ze światłowodowym systemem detekcji czy z kamerami tradycyjnymi lub termowizyjnymi, umożliwiając weryfikację. Projektując system zabezpieczenia danego obiektu warto rozważyć zastosowanie radarów. Zachęcamy do ich testowania. ●



EVVA

EVVA Polska w nowej siedzibie!

Nowa siedziba EVVA Polska mieści się przy ul. Rzemieślniczej 12 w Warszawie. Uroczyste otwarcie, w którym wzięło udział ponad 60 gości, odbyło się 1 grudnia 2022 roku.



Uroczystego przecięcia wstęgi dokonali Dominika Zajączkowska, dyrektor zarządzająca EVVA Polska, wraz z Martinem Kerntalerem, dyrektorem ds. marketingu międzynarodowego EVVA GmbH. Gratulacje z okazji otwarcia biura przestał też Stefan Ehrlich-Adám, właściciel EVVA Sicherheitstechnologie GmbH.

– Dynamiczny rozwój firmy spowodował, że dotychczasowa siedziba nie była już wystarczająca. Potrzebowaliśmy powierzchni biurowej oraz magazynowo-produkcyjnej, która byłaby adekwatna do naszych potrzeb. Nowa siedziba oferuje lepsze warunki pracy dla całego zespołu, a także wygodne i przestronne wnętrza z miejscem

do prezentacji mechanicznych i elektronicznych systemów zamknięć i kontroli dostępu. Jest też miejsce do szkoleń naszych partnerów i klientów – podkreśla Dominika Zajączkowska.

Podczas uroczystości goście wysłuchali informacji o zrównoważonych rozwiązaniach wprowadzanych w fabrykach EVVA, która mocno inwestuje w rozwiązania proekologiczne. Mieli też okazję uczestniczyć w debacie „Porozmawiajmy o bezpieczeństwie”, poznać najnowsze trendy w projektowaniu wnętrz, a także wziąć udział w praktycznych pokazach wkładek bębnowych systemów Akura 44 i 4KS. ●



NEWSERIA.PL

Nadchodzi cyfrowa transformacja łańcucha dostaw

Lata 2020-2022 przyniosły nowe wyzwania w obszarze logistyki: pandemia, wojna w Ukrainie, konflikt Chiny-USA i wzrost cen paliw wzmogły potrzebę budowania odporności i bezpieczeństwa łańcucha dostaw. Według badań PwC Digital Global Trends in Supply Chain 2022 i IHS Markit najistotniejsze dla managerów, poza zwiększeniem odporności łańcucha dostaw, są: redukcja kosztów, automatyzacja i analityka. Odpowiedzią na te zagadnienia są cyfryzacja i wdrażanie technologii. Ten kierunek jest nieunikniony, ale to także inwestycja w bezpieczeństwo i stabilność.

Tradycyjne, zawodne i czasochłonne rozwiązania są wypierane przez technologię 4.0, która pomaga przewidzieć sytuacje niepożądane i im zapobiegać, co przekłada się na oszczędności i ograniczenie ryzyka strat. Badanie GEODIS pokazuje, że priorytetem technologicznym dla

41% respondentów jest analiza danych. Za nią plasują się: IoT (39%), chmura obliczeniowa (39%) i analityka predykcyjna (29%). Trzy najbardziej pożądane technologie wspierające pozyskiwanie danych i monitorowanie łańcucha dostaw:

1. **Internet of Things** (Internet Rzeczy) to niezbędny element wspierający nowoczesny łańcuch dostaw. Na każdym etapie zbiera dane i w czasie rzeczywistym monitoruje parametry takie jak temperatura, wilgotność i naświetlenie, umożliwiając ocenę stanu przesyłki. Dostarczane przez niego informacje o lokalizacji umożliwiają śledzenie przesyłki i łatwą identyfikację w czasie transportu czy magazynowania.
2. **Rozwiązania cloudowe** pomagają zbierać dane i korzystać z analityki oraz zapewniają możliwie największą ich dostępność z każdego miejsca na świecie. Aplikacje stworzone w tym środowisku znacznie łatwiej zaimplementować niż tradycyjne – są dostępne praktycznie od razu. Chmura pozwala zwiększać zasoby zależnie od aktualnych potrzeb, a renomowani dostawcy zapewniają bezpieczeństwo danych na wysokim poziomie.
3. Im proces bardziej zautomatyzowany, tym ryzyko wystąpienia błędów mniejsze. **Wykorzystanie sztucznej inteligencji i uczenia maszynowego w analizie predykcyjnej** do zoptymalizowania łańcucha dostaw może znaleźć zastosowanie już wkrótce. Szybka analiza danych, rozpoznawanie wzorców i trendów pozwala szybciej wprowadzać korekty, np. poprzez sugerowanie bardziej optymalnych tras, przewidywanie potencjalnych problemów. ●



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



Czym się kończy brak „bezpiecznika”

Ten dzień dla Aldony Kłosek nie zaczął się dobrze. Podczas porannego spaceru pies wytarzał się w padlinie, samochód nie odpalił, autobus się spóźnił, a w nowej kurtce zaciął się suwak. Na dodatek Aldona cały czas miała nieprzyjemne wrażenie, że za chwilę stanie się coś złego.



Aldona dotarła do pracy spóźniona, zła i spocona, bo okazało się, że zapowiadany mróz nie nadszedł, a kurtki za żadne skarby nie mogła rozpiąć. Dlatego, gdy do jej niewielkiego gabinetu wszedł prezes, z natury człowiek spokojny i łagodny, zastał główną księgową poirytowaną i, jak mu się wydawało, szukającą dziury w całym.



Niewielkie centrum logistyczne mające stałych, wiernych i całkiem licznych klientów zaczyna mieć kłopoty. Niby wszystko jest w porządku, ale... główna księgowa Aldona Kłosek czuje przez skórę, że coś jest nie tak. Niepokoi ją rosnąca szkodowość, choć teoretycznie wszystko jest w normie.

– Pani Aldono, dlaczego ma pani taką zaciętą minę? Stało się coś?
– Prezes zamierzał inaczej zacząć tę rozmowę, ale nie dało się ukryć, że widok złej jak chmura gradowa księgowej trochę go zaskoczył.



– *Sama nie wiem!* – Z wyraźną złością odezwała się Aldona, zazwyczaj opanowana ponad miarę. – Sprawdzam i czuję, że coś tu jest nie tak...
– *Ale co jest nie tak? Mamy jakieś kłopoty finansowe, coś z VAT-em, a może z tymi noooo... wie Pani* – prezes szukał słowa – *pitami dwa? Wiem, że trudno nad tym zapanować, może mógłbym jakoś pomóc?* – Szef nigdy nie uchylał się od pracy, choć przecież nie musiał w niczym pomagać głównej księgowej. Cenił jednak skrupulatną panią Aldonę, która zawsze wydawała mu się oazą spokoju, dlatego nie wahałby się zakasać rękawów i robić, co każe.
– *Eeee, nie z VAT-em wszystko okej, ale niech pan spojrzy na to pismo* – powiedziała Aldona i z rozmachem wręczyła prezesowi jakąś kartkę. Ten przeczytał raz, potem drugi i oddał Aldonie pismo, w dalszym ciągu nie rozumiejąc powodu jej zdenerwowania.

– *Przyznam, pani Aldono, że nie wiem, o co pani chodzi. To zwykle pismo od ubezpieczyciela. To oczywiste, że jak co roku musimy zapłacić składkę ubezpieczeniową. Co panią tak tu martwi?*
– *A zerknął pan na informację o naszej szkodowości? Proszę uważnie się czytać. Z miesiąca na miesiąc rośnie. Już od pewnego czasu czułam, że coś tu nie gra. Niby mieścimy się w założeniach, w Excelu wszystko się zgadza, nic się nie świeci na czerwono.* – W głosie księgowej słychać było wyraźne zmartwienie. – *Nie dziwi pana, że zainwestowaliśmy w szkolenia, lepsze oświetlenie, specjalne rękawice i buty, specjalne taśmy i takie tam, mamy też dodatek za pracę bezszkodową, a liczba szkód, za które płacimy klientom, nie tylko nie maleje, ale i rośnie?* – zapytała Aldona.

Prezesowi zrobiło się głupio, bo szczerze mówiąc, nie zastanawiał się nad tym. Szefował firmie od wielu lat i wiedział, że to po prostu taki biznes. Raz komuś coś wyleci z ręki, innym razem wózek widłowy wjedzie na paletę, czasami ktoś się zagapi i wpadnie na coś. Poczul się trochę wywołany tym pytaniem księgowej do tablicy.

– *Wie pani, taki biznes. Po to właśnie mamy to ubezpieczenie, żeby móc klientom płacić za straty, do których dochodzi na terenie magazynu. Przy okazji wymyśliła pani ten świetny sposób z aukcjami i nie tylko nie musimy płacić za zniszczenie towaru, ale jeszcze na tym ciut, ciut zarabiamy.*

Aldona wiedziała, o czym szef mówi. Była dumna z tego pomysłu. Towary w zniszczonych przez przypadek opakowaniach trafiały do magazynu rzeczy wycofanych z obrotu. Firma przez lata

płaciła za ich utylizację. Aldona wpadła na pomysł, by zorganizować wewnętrzne aukcje, tak by pracownicy mogli kupić to, co w innym przypadku trafiłoby do zniszczenia albo na śmietnik, a to dla centrum było kosztownym rozwiązaniem. Aukcje cieszyły się wielką popularnością. Magazyn scrap był sukcesywnie opróżniany, centrum logistyczne płaciło mniej za odpady, przy okazji odzyskując część pieniędzy, pracownicy byli zadowoleni z okazjnych zakupów. Jak mawiał jeden z wózkowych, „wilk syty i Manchester city”.

Jednak teraz Aldona nie do końca była przekonana, czy magazyn funkcjonował tak, jak powinien. Doradca ubezpieczeniowy, który zajmował się ich firmą, zadzwonił, by uważnie wczytała się w pismo. Wszystko wskazywało na to, że likwidowanych przez ubezpieczyciela szkód jest coraz więcej i za chwilę składka będzie jeszcze wyższa. To ją martwiło, bo przecież już teraz płacili sporo.

Gdy Aldona powtórzyła to prezesowi, ten również poczul się nieswojo.

– *Myśli pani, że kradną?* – Już gdy zadawał to pytanie, wiedział, że jest ono nie na miejscu.

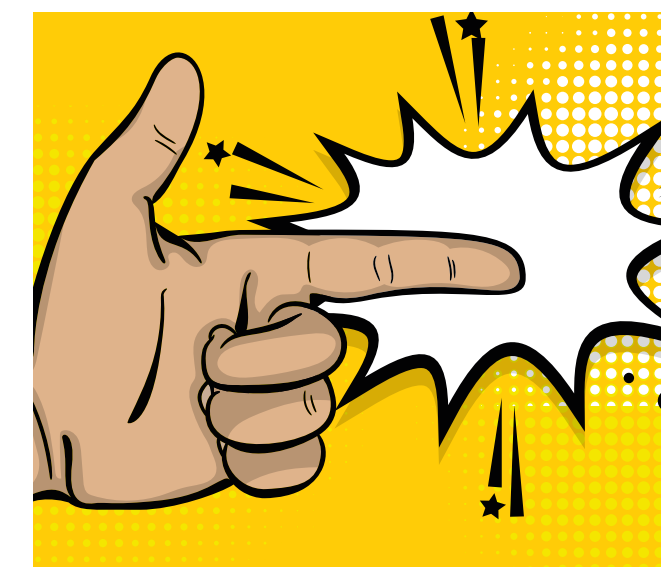
– *Ależ nie, skądże* – zachnęła się Aldona. – *Nikt nie kradnie. Sam pan wie, że pod tym względem jesteśmy dobrze zabezpieczeni. Mysz się nie prześlizgnie. Coś jednak działa nie tak, a mam na to inny dowód poza rosnącą szkodowością. Proszę spojrzeć na ten e-mail, przyszedł dosłownie przed sekundą.* – Aldona przekreśliła ekran w stronę prezesa.

Ten przeczytał raz, potem drugi, a na koniec trzeci. I poczul, że tym razem jego ogarnia złość, a ciśnienie rośnie mu jak w silniku parowym.

Pani Aldono! Jak to możliwe?! Przecież... my..., ale jak... kto? – Prezes czuł, że za chwilę eksploduje.

– *No cóż, panie prezesie, mówiłam, żeby zatrudnić opornika, tzn. bezpiecznika* – poprawiła się szybko pani Aldona. – *Kogoś, kto zadba o kompleksowe bezpieczeństwo naszej firmy, i dzięki któremu nie będziemy musieli się wstydić i tłumaczyć przed klientami. A kto wie, może i szkodowość będzie mniejsza.*

– *Myśli pani, że bezpiecznik pomoże? Skąd będziemy widzieli, że taka osoba zna się na rzeczy? Przecież naszym pracownikom ochrony nic nie dolega. Sama pani mówiła, że złodziejstwa w firmie nie ma.*





– Panie prezesie, ja się na ochronie nie znam, pan też nie bardzo. Pracownicy ochrony są nieźli, ale tu trzeba szerszego spojrzenia. Zatrudnijmy takiego, który ma stosowne doświadczenie, jakieś kursy, może certyfikaty. Kogoś, komu będziemy mogli zaufać, a przede wszystkim kogoś, kto nam pomoże zrozumieć, jak do tego doszło. – Księżkowa wskazała na ekran z nieprzyjemnym e-mailem od klienta.

– Skąd weźmiemy takiego człowieka? Sama pani wie, jak teraz wygląda rynek pracy. – Prezes zafrasował się nie na żary.

– Słyszałam o Centrum Kompetencji a&s Polska, które organizuje certyfikowane warsztaty, może nam kogoś polecić. Sprawdzić?

– Oczywiście, i to najlepiej dzisiaj. Pani ma zawsze świetne pomysły!
– No nie wiem – zawahała się Aldona. – Z tymi aukcjami to coś mi nie wyszło.



Opracowała Monika Mamakis na bazie scenariusza Jacka Grzechowiaka

- Co było w e-mailu od klienta, co tak bardzo zdenerwowało prezesa?
- Dlaczego Aldona uznała, że aukcja uszkodzonych towarów okazała się złym pomysłem?
- Dlaczego scrap to nie zawsze scrap?

Odpowiedzi na te pytania poznali uczestnicy strategicznych warsztatów Security Forum przeprowadzonych 30 stycznia przez Jacka Grzechowiaka, dyrektora Centrum Kompetencji a&s Polska.

Centrum Kompetencji a&s Polska organizuje szkolenia i warsztaty dla osób odpowiedzialnych za bezpieczeństwo fizyczne, cyfrowe i zabezpieczenia techniczne. Przekonaj się, co o warsztatach sądzą osoby, które wzięły w ich udział:

Agnieszka Gacka, Shein

W branży jestem od niedawna i to jedno z moich pierwszych szkoleń tego typu. Security Forum dostarczyło wiedzy i przykładów, które pozwolą mi rozwijać się na moim obecnym stanowisku specjalistki Loss Prevention w firmie Shein. Cieszę się więc, że mogę uczestniczyć w tym wydarzeniu i uczyć się nowych rzeczy od profesjonalistów. Czekam na kolejne edycje!



Victoria Moroz, DHL

To było naprawdę świetne szkolenie! Gdy byłam dzieckiem, chciałam zostać śledczą, a dzisiejszy omawiany przypadek i część dociekania, jak zapobiec czemuś, co się może wydarzyć, było niezwykle interesujące. Mogłam poczuć się jak detektyw! Bardzo się cieszę, że wzięłam udział w tych warsztatach – mamy trudne i pełne wyzwań czasy, więc takie szkolenie jest na wagę złota!



Mariusz Borowiak, ARVATO

Przykłady przedstawione przez Jacka Grzechowiaka z Centrum Kompetencji a&s Polska pokazują, że takie szkolenia są ważne i potrzebne, bo niewiedza Zarządu czasami powoduje, że trudno zdefiniować, co jest przyczyną powstawania „fraudów”.

Poza tym takie spotkania to doskonała przestrzeń do poznawania ludzi z innych firm i nawiązywania kontaktów. Gratuluję organizatorom i całej ekipie a&s Polska kolejnego, doskonałego szkolenia – tym razem w zupełnie nowej formule!



urmet MIWI

UNIWERSALNE ROZWIĄZANIA Z ZAKRESU ZINTEGROWANYCH SYSTEMÓW ZABEZPIECZEŃ

- infrastruktura krytyczna ► transport i logistyka
- przemysł i produkcja ► budynki użyteczności publicznej

Milesight

IndigoVision[®]
a Motorola Solutions Company

ICTProtege[®]

NUUO[®]

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





System Monitorowania Flot SMF to:

- lokalizowanie położenia pojazdu w czasie rzeczywistym
- historia tras przejazdu i postojów
- wyznaczanie geostref pracy kierowcy
- analiza stylu jazdy kierowcy
- rozbudowany system raportowania
- kontrola gospodarki paliwowej
- powiadamianie o zaistniałych sytuacjach alarmowych
- zdalne pobieranie plików DDD z tachografów
- funkcja Eco-Driving - monitorowanie stylu jazdy kierowcy
- monitoring Sent Geo
- e-TOLL - obsługa systemu poboru opłat elektronicznych
- i wiele innych

