01 (43) / 2024

CZASOPISMO RYNKU SECURITY

a&S POLSKA

RAPORT: TRANSPORT I LOGISTYKA W POLSCE

Czy zapowiadane osłabienie rynku niemieckiego przyniesie poprawę u polskich przewoźników? Co jeszcze wpłynie na stan branży TSL w Polsce?

JAKI BĘDZIE ROK 2024 DLA POLSKIEJ BRANŻY SECURITY?

Eksperci branży ocenili rok 2023 jako trudny, 2024 rysuje się niewiele lepiej, choć w drugiej połowie spodziewana jest niewielka poprawa.

O(D)PORNOŚĆ W BEZPIECZEŃSTWIE

Co należy zrobić, aby być bezpiecznym w obliczu zagrożeń teleinformatycznych? I czy ten stan jest w ogóle realny do osiągnięcia?

www.aspolska.pl

20 zł
(w tym 8% VAT)

ISSN 2451-5175

TRANSPORT I LOGISTYKA

WARSAW SECURITY SUMMIT

Największa
Konferencja
Branży
Zabezpieczeń
Nowa
Formuła

06/06/2024

SZCZEGÓŁY WKRÓTCE

Życie w drodze

„Po asfalcie czy przez piach, gładko czy po kocich łbach, taki mi się trafił fach, życie w drodze" śpiewał Marian Szyguła, kierowca bazy transportowej PKS w filmie „Droga". Kocich łbów już dawno nie ma, a i dróg piaszczystych coraz mniej. Po polskich drogach jeszcze nie mkną automatyczne ciężarówki, ale zapewne jest to kwestią czasu. Coraz częściej słyszy się o tym, że problem ostatniej mili rozwiążą drony.

Branża TSL w Polsce wykorzystała czas transformacji ustrojowej i rozwinęła się nad podziw okazale. Jednak globalizacja powoduje, że polskie firmy muszą się zmagać z konkurencją, ale nie tylko... Przed jakimi wyzwaniami stanie sektor w roku 2024?

Digitalizacja procesów – ta branża również przechodzi gwałtowną cyfryzację. Co za tym stoi? Przede wszystkim automatyzacja i robotyka procesów logistycznych, coraz większa rola algorytmów SI używanych do optymalizacji operacji w łańcuchu dostaw, umożliwiających przy okazji reagowanie na wydarzenia na trasie czasie rzeczywistym, ale także analizę predykcyjną. Narzędzia oparte na sztucznej inteligencji będą stosowane do optymalizacji tras, prognozowania popytu, zarządzania zapasami oraz konserwacji predykcyjnej. To z kolei przyczyni się do oszczędności kosztów, skrócenia czasu dostaw oraz redukcji przestojów. Potencjał ma też blockchain, który służyć może m.in. do transparentności łańcucha dostaw. Poprzez zapewnienie bezpiecznego i odpornego na manipulacje rejestru przepływu towarów blockchain może zwiększyć zaufanie, ograniczyć oszustwa i usprawnić procedury celne, sprzyjając lepszej współpracy między partnerami w łańcuchu dostaw.

Cyfryzacja nie zmieni jednak faktu, że jak w każdej innej gałęzi gospodarki, tak transport, jak i logistyka będą odczuwać niedobory siły roboczej. Wynika to z wielu różnych czynników, w tym starzenia się społeczeństwa, braku wykwalifikowanych pracowników oraz konkurencji ze strony innych branż. Swoje zrobiła też sytuacja geopolityczna, odpowiedzialna również (przynajmniej częściowo) za rosnące koszty paliwa. Nic nie wskazuje, by ta wyraźna w ubiegłym roku tendencja miała się odwrócić. Podniesie to koszty działalności firm dostawczych, co może się przełożyć na wyższe stawki za fracht, które – zgodnie z efektem domina – wpłyną na ceny końcowych produktów. Więcej na ten temat w raporcie: *Transport i logistyka w Polsce 2024* (str. 12). Również w nim głosy ekspertów na temat stanu bezpieczeństwa transportu w Polsce. Obraz tego przedstawia raport TAPA z dziewięciu miesięcy ubiegłego roku. Jego omówienie znajduje się na str. 20.

Jak na tle branży TSL wyglądają tegoroczne perspektywy całej branży bezpieczeństwa? Odpowiedzi na to pytanie udzielają eksperci polskiego rynku security (str. 34). Warto także wsłuchać się w głos branży (str. 28), który zdecydowanie najgłośniej wybrzmi podczas Warsaw Security Summit. Już teraz zapraszamy do wzięcia udziału w wydarzeniu.

Redakcja

CZASOPISMO RYNKU SECURITY

a&S POLSKA

01 (43) / 2023

SPIS TREŚCI

RAPORT: TRANSPORT I LOGISTYKA

REDAKCJA

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

info@aspolska.pl
www.aspolska.pl

PREZES ZARZĄDU
Mariusz Kucharski

REDAKTOR NACZELNA
Marta Dynakowska

Z-CA RED. NACZELNEGO
Jan T. Grusznic

REDAKCJA
Monika Żuber-Mamakis
Adela Prochyra

DZIAŁ REKLAMY
Iwona Krawiec

DZIAŁ PROJEKTÓW SPECJALNYCH
Jolanta A. Kucharska
Aleksandra Czapska

CENTRUM KOMPETENCJI
Jacek Grzechowiak

KOREKTA
Jolanta Kucharska

PROJEKT GRAFICZNY I SKŁAD
Bogusław Kalwala

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

www.sensgroup.pl

BCS VIEW ITC

Najwyższa skuteczność w każdym… znaku

» Więcej przeczytasz na stronie 8

POLSKA MARKA BCS

BCS

www.bcs.pl

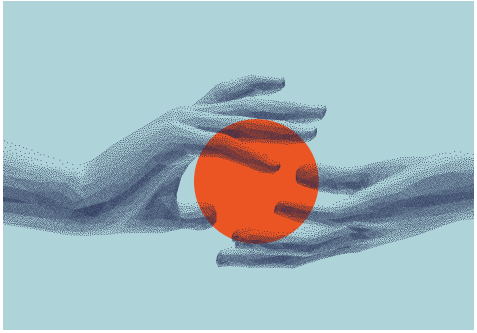
www.facebook.com/bcspl

CZASOPISMO RYNKU SECURITY

a&S POLSKA

01 (43) / 2023

SPIS TREŚCI



System kontroli dostępu RACS 5 w sektorze komercyjnym

roger
Intelligence for Building

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

Wybrane realizacje






ALNET SYSTEMS

Alnet PRS do rozpoznawania tablic rejestracyjnych

Alnet PRS to moduł pozwalający na odczytywanie i analizę danych z tablic rejestracyjnych pojazdów samochodowych. Jest dostępny bezpłatnie w każdej wersji oprogramowania VMS NetStation zawierającej minimalną licencję na 8 kamer.

Rozbudowana funkcjonalność ułatwia tworzenie raportów i szybką analizę zgromadzonych danych. Jednocześnie na jednym serwerze NetStation można uruchomić do 16 kanałów LPR. Tablice są odczytywane w czasie rzeczywistym i umieszczane w bazie danych wraz ze zdjęciem tablicy.

Moduł wyposażono w wyszukiwarkę i tworzenie rozbudowanych raportów. Istnieje możliwość automatycznego otwierania bram oraz aktywowania innych urządzeń współpracujących z systemem, np. blokowanie dystrybutora paliw czy automatyczne drukowanie dokumentów dla danego pojazdu. Inne zalety modułu:

- Możliwość tworzenia grup użytkowników
- Zgłaszanie zdarzeń krytycznych dla wykrytych tablic (wymagany CMS HUB)
- Generowanie raportów dla tzw. czarnej listy tablic rejestracyjnych (wymagany CMS HUB).
- Obsługa poprzez aplikację mobilną CMS 4 Mobile
- Synchronizacja tablic między wieloma serwerami (wymagany CMS HUB)
- Monitorowania czasu pobytu pojazdu w strefie.

Więcej na www.alnetsystems.com

AXIS COMMUNICATIONS

Radar AXIS D2210-VE

AXIS D2210-VE jest radarem wysokiej częstotliwości, który pozwala na dokładne wykrycie oraz klasyfikację obiektów. Wykorzystuje zaawansowaną technologię niezależną od widoczności, która ponadto umożliwia obniżenie kosztów energii.

Radar AXIS D2210-VE oferuje pole widzenia 95° i podaje pozycję obiektu przez całą dobę niezależnie od warunków atmosferycznych i oświetleniowych. Może wykrywać ludzi z odległości do 60 m i pojazdy z odległości do 90 m. Dodatkowo, po włączeniu profilu monitorowania dróg, zasięg wykrywania pojazdów wzrasta do 150 m. Radar ten może być również używany do wyzwalania zdarzeń i gromadzenia bardziej wiarygodnych statystyk ruchu przez całą dobę.

Wbudowane funkcje analityczne oparte na głębokim uczeniu pozwalają na dokładną klasyfikację obiektów przy niskim wskaźniku fałszywych alarmów. Obsługa radaru ma do wyboru jeden z dwóch profili: monitorowanie obszaru w celu wykrywania ludzi i pojazdów o małej prędkości oraz profil monitorowania drogi w celu wykrywania pojazdów poruszających się z większą prędkością.

Dzięki inteligentnej funkcji koegzystencji możliwe jest połączenie do ośmiu radarów AXIS D2210-VE w bliskiej odległości. Fale radiowe z urządzeń radiowych Axis są nieszkodliwe. Nawet przy ciągłej ekspozycji czy nagromadzeniu kilku radarów w jednym obszarze ludzie mogą się do nich zbliżyć bez żadnego ryzyka.

Radar AXIS D2210-VE można wtopić w różne otoczenie lub w razie potrzeby, wyróżnić, owijając go kolorową, niemetalową folią na bazie węgla.

Więcej na: www.axis.com/pl-pl

BCS

BCS-V-TIP72VSR4-ITC – kamera z serii BCS View z funkcją ANPR

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

Jest to kamera o rozdzielczości 2 Mpix, dzięki której można łatwo zautomatyzować wjazd na obiekt i wyjazd z niego. Taka rozdzielczość w zupełności wystarczy do prawidłowego odczytu tablic rejestracyjnych, skuteczność działania poprawia prędkość przechwytywania obrazu sięgająca 50 kl./s.
Odpowiednio skonfigurowana i prawidłowo zamontowana kamera odczyta numer tablicy rejestracyjnej i odpowiednio na tę informację zareaguje. Jest wyposażona w moduł wejścia/wyjścia (1 we/1 wy), dzięki czemu po rozpoznaniu numerów rejestracyjnych może sterować barierą. Model ten został wyposażony w obiektyw z motozoomem o ogniskowej 2,8-12 mm oraz promiennik podczerwieni o zasięgu do 40 m.

Kamera umożliwia filtrowanie numerów tablic rejestracyjnych. Wykorzystuje w tym celu białą i czarną listę z przypisanymi do nich numerami tablic pojazdów. Lista może zawierać do 10 000 wpisów. Rozpoznanie tablicy odbywa się nawet w przypadku pojazdu w ruchu przejeżdżającego przed kamerą. 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 niesprzyjających warunkach zapewnić skuteczne rozpoznanie numeru rejestracyjnego.

Więcej na: www.bcs.pl

ALNET SYSTEMS

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

www.alnetsystems.com

HIKVISION

Przełączniki sieciowe Hikvision serii Smart Management

Nowe zarządzalne przełączniki sieciowe Hikvision serii smart to ciekawa alternatywa dla typowych rozwiązań stosowanych w systemach monitoringu wizyjnego.

W tej ofercie produktowej do wyboru jest wiele modeli. Urządzenia są dostępne w konfiguracji od 10 do 48 portów PoE oraz budżetem mocy dochodzącym do 470 W.

Zarządzalne switche serii smart pomagają zrealizować system transmisji, który w jednym oprogramowaniu VMS integruje zarządzanie samą siecią oraz kamerami i rejestratorami. Funkcja wizualizacji graficznej topologii pozwala na łatwą i intuicyjną pracę z każdym węzłem i urządzeniem sieciowym. Po dodaniu urządzeń do aplikacji VMS topologia generowana jest automatycznie. Urządzania Hikvision, takie jak NVR, kamery itp., są rozpoznawane automatycznie.

Funkcja monitorowania sieci pozwala na szybką identyfikację problemu, np. o zbyt dużym zużyciu pasma, co podnosi efektywność zarządzania systemem. W przypadku wystąpienia nieprawidłowości generowany jest komunikat push, a na obrazie topologii wyświetlany jest aktualny stan urządzeń w sieci. Umożliwia to szybką identyfikację źródła problemu.

Zarządzanie przełącznikami może odbywać się również zdalnie za pomocą aplikacji. Ta funkcjonalność zapewnia szybką reakcję w razie jakichkolwiek problemów, bez potrzeby przebywania w danej lokalizacji. Typowym przedstawicielem serii smart jest model DS-3E1526P-SI dysponujący 24 portami PoE o przepustowości 1 Gb oraz budżetem mocy 370 W. Przełącznik oferuje również wszystkie funkcje opisane wyżej.

Więcej na: www.hikvision.com/pl

LINC POLSKA

HONEYWELL | Kamery IP 2024 – seria 35

Rozwój technologii cyfrowej niesie nowe zagrożenia w postaci nasilonej liczby cyberataków. Przestępcy cybernetyczni coraz częściej wykorzystują do tego celu urządzenia IP działające w sieci, np. kamery systemów monitoringu wizyjnego.

Czy jesteśmy w stanie zapobiegać takim procederom i skutecznie chronić się przed atakami? Tak. Odpowiedzią może być seria urządzeń firmy Honeywell oferująca najwyższe standardy bezpieczeństwa i zgodność z amerykańską dyrektywą NDAA. Kamery z serii 35 to zaawansowane technologicznie urządzenia z wbudowaną analityką wideo opartą na algorytmach AI. Serię 35 wyposażono w inteligentne wykrywanie ruchu oparte na rozpoznawaniu typów obiektów – ludzi i pojazdów.

Zakres szyfrowania strumieni wizyjnych został powiększony ze standardowego 128 do 256 bitów, a wszystkie kamery mają zabezpieczenia hasła w postaci osobnego szyfrowanego chipsetu TMP.

Kompleksowy system ochrony obejmuje kamery, rejestratory, czujki oraz wideonadajniki. Wszystkie deklaracje firmy Honeywell dają nam pewność, że wybieramy producenta, który bezpieczeństwo i odpowiedzialność stawia na pierwszym miejscu.

Więcej na: www.linc.pl

TP-LINK

TP-Link VIGI C540S – zewnętrzna, kolorowa, obrotowa kamera sieciowa

TP-Link VIGI C540S to dwuobiektywowa, obrotowa kamera sieciowa. Technologia ColorPro Night Vision umożliwia doskonałe odwzorowanie kolorów nawet w całkowitej ciemności. Obudowa ma klasę szczelności IP66, co zapewnia odporność na trudne warunki atmosferyczne oraz stabilne działanie na zewnątrz budynku.

Kamerę wyposażono w obiektyw o rozdzielczości 4 Mpix, czuły przetwornik oraz 2 wbudowane diody LED światła punktowego. Może być zasilana poprzez PoE lub klasyczny zasilacz 12 V DC.

Kamera ma opcję tworzenia tras patrolu, jest wyposażona w mikrofon oraz głośnik, a także alarm dźwiękowy i świetlny do odstraszania intruzów. Umożliwia wykrywanie: wtargnięcia na wyznaczony teren, przekroczenia linii, wejścia do strefy oraz jej opuszczenia, pozostawienia przedmiotu lub jego zabrania. Wykrywa również osoby, które w podejrzany sposób krążą po pewnym obszarze przez dany czas oraz zmianę sceny, kiedy ktoś np. zasłoni kamerę. Nagrania z kamery mogą być rejestrowane na rejestratorze sieciowym NVR oraz lokalnie na kartach microSD (do 256 GB).

Kamera wykorzystuje kompresję H.265+, co zmniejsza obciążenie sieci i obniża koszty monitoringu bez utraty jakości obrazu. Jest zgodna ze standardem ONVIF, dzięki czemu współpracuje z kamerami i rejestratorami różnych producentów.

Dzięki aplikacji VIGI na urządzenia przenośne z systemem iOS lub Android, produktami z tej serii można w prosty i kompleksowy sposób zarządzać z poziomu urządzenia mobilnego, z dowolnego miejsca na świecie. Kamera jest objęta 3-letnią gwarancją.

Więcej na: www.tp-link.com/pl

Honeywell

35 SERIES
ZWIĘKSZ ŚWIADOMOŚĆ - NIE KOSZTY

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

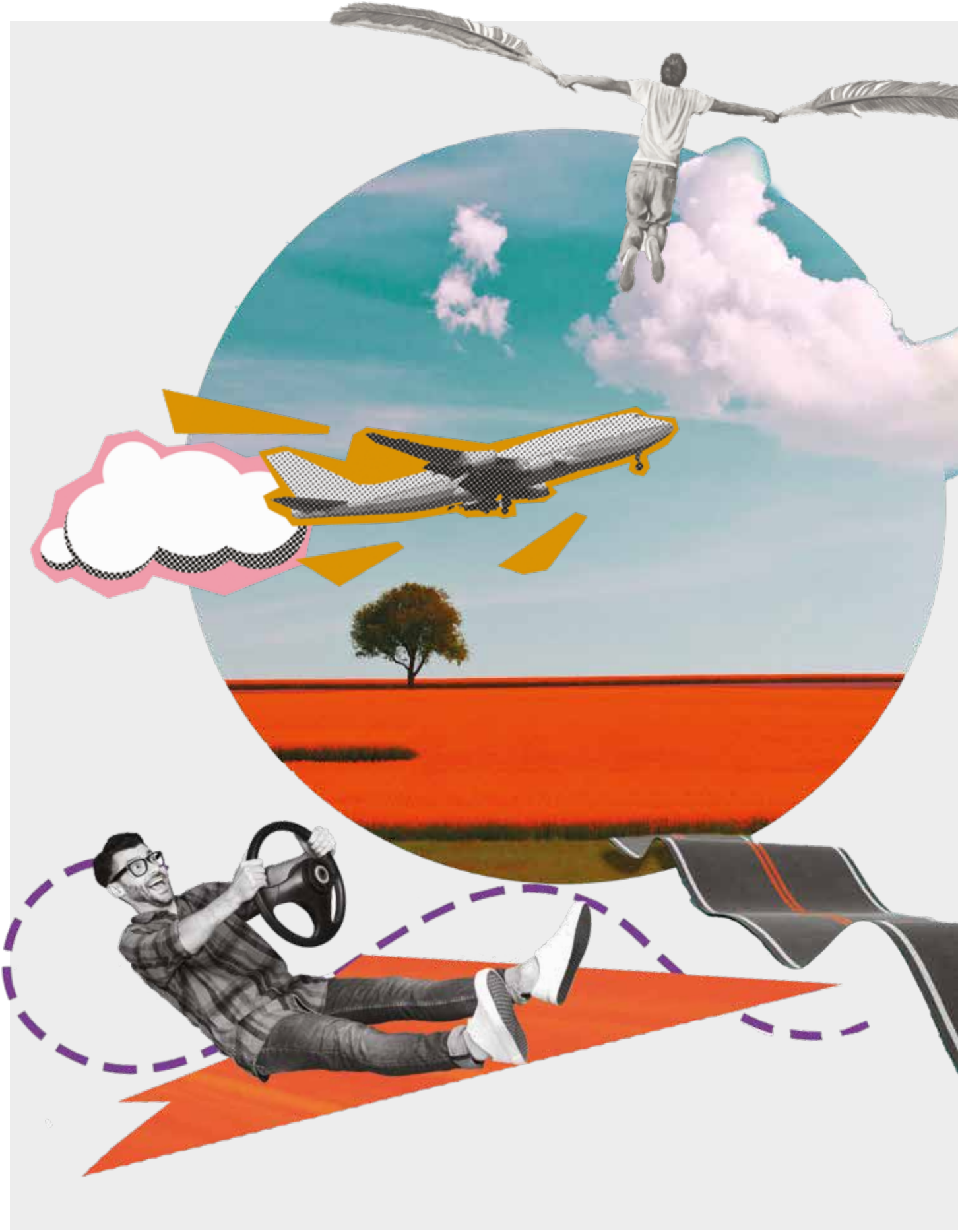
- Doskonała jakość obrazu do 8MP
- Elastyczny nadzór
- Wbudowana pamięć wideo
- Inteligentna detekcja ruchu i analityka
- Łatwy w instalacji i obsłudze

5 YEAR WARRANTY | SECURE BY DEFAULT | ONVIF | SGT

Premium security distributor:

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

Linc Polska Sp. z o.o.



Raport: Transport i logistyka w Polsce 2024

Po raz pierwszy w historii „a&s Polska" przed rokiem przygotowaliśmy przekrojowy raport o branży transportowo-logistycznej w naszym kraju. Padło w nim wiele pytań o przyszłość, sporo kwestii pozostało otwartych. Minione 12 miesięcy przyniosło pewne odpowiedzi, lecz w większości nie były one zbyt pozytywne. Co przyniesie rok bieżący?

Adela Prochyra, Jan T. Grusznic, a&s Polska

Eksperci branży ocenili rok 2023 jako trudny, 2024 rysuje się niewiele lepiej, choć w drugiej połowie spodziewana jest niewielka poprawa.

Zacznijmy od umiarkowanie dobrych wieści. Agencja badawcza Transport Intelligence prognozuje, że w 2024 r. rynek europejskiego transportu drogowego wzrośnie o 1,7% (dla porównania – w 2023 r. było to 1,4%, ale w 2022 – 3,5%, średnia w okresie 2000–2019 – 3,8%). Nominalnie nie jest to może dużo, ale jeśli wziąć pod uwagę wyhamowanie w ostatnich latach, może cieszyć odbicie i tendencja powolnego wzrostu. Wszystkie światowe organizacje finansowo-handlowe, takie jak Międzynarodowy Fundusz Walutowy (IMF), Światowa Organizacja Handlu (WTO) czy Organizacja Współpracy Gospodarczej i Rozwoju (OECD) prognozują spowolnienie w handlu towarowym, minimalne wzrosty światowego PKB oraz PKB w strefie euro oraz spadki w światowym eksporcie i imporcie, co bezpośrednio odczuje branża transportowa.

Pogłoski o kryzysie w polskim transporcie – prawdziwe czy mocno przesadzone?

Jeśli chodzi o polski transport, jego kondycja na koniec 2023 r. nie jest najlepsza. Tak twierdzą przedsiębiorcy, a co mówią liczby? Jeszcze w 2022 r. polscy przewoźnicy utrzymali pewną zwyżkę (1,4% wzrostu) pracy przewozowej na tle spadku w całej Unii (-0,04%). Z wynikiem 385 088 mln km i poziomem 20,05% całkowitej pracy przewozowej (dane Eurostatu) w transporcie towarów w ramach Unii Europejskiej udało się nam zachować pozycję lidera. W roku 2023 Transport Intelligence prognozował wolumen przewozów o wartości ok. 389,3 mld euro (brak danych GUS i Eurostatu za zeszły rok), co ponownie zagwarantowało polskim przewoźnikom pierwszą pozycję na kontynencie. Nic nie zapowiada, że tegoroczne osiągnięcia będą w jakikolwiek sposób zagrożone. Rynek przewozów drogowych odczuwa spowolnienie, a mimo to odnotowuje niewielką zwyżkę.

Należy mieć na względzie uwarunkowania zewnętrzne, które wpływają na kształt tego rynku, oraz wielkość sektorów współpracujących, jak chociażby przemysł i budownictwo, które mierzyły się w ostatnim czasie z pewnym przestojem. Na branży TSL odbiły się także inne globalne procesy:

– wojna w Ukrainie,
– wybuch wojny na Bliskim Wschodzie,
– wysoka inflacja w Polsce i w Europie,
– spowolnienie gospodarcze w Polsce oraz krajach ościennych,
– gwałtowny wzrost cen paliw,
– zaostrzone wymogi środowiskowe w UE,
– wzrost płacy minimalnej w Polsce,

a także specyficzne dla TSL:

– podwyżka myta w Niemczech,
– strajk na granicy polsko-ukraińskiej,
– spowolnienie gospodarcze w Niemczech.

Pozostając w obszarze liczb, przyjrzyjmy się cenom w branży. Weźmy np. *Road Freight Rate Development Benchmark* (Wskaźnik Rozwoju Stawek Przewozu Drogowego), który opiera się na analizie 750 mln różnych cen na kluczowych europejskich korytarzach transportowych. Indeks stawek spotowych osiągnął w III kwartale 2023 r. poziom 125,4 pkt, co oznacza spadek o 1,2 pkt w porównaniu do II kwartału i aż o 14,8 pkt mniej niż rok wcześniej. Obniżka indeksu spotowego jest naturalną reakcją rynku na niski popyt na usługi transportowe. To wynik sytuacji gospodarczej w Europie charakteryzującej się niskim poziomem produkcji przemysłowej, stłumioną konsumpcją, wysokimi kosztami życia itp. Warto zaznaczyć, że tempo spadku się zmniejszyło – przewoźnicy już zaakceptowali niższe ceny usług transportowych, które wydają się dostosowywać do mniejszego poziomu popytu. Stawki kontraktowe z kolei lekko wzrosły, ich wskaźnik zwiększył się o 1,4 pkt, osiągając 128,1 pkt. Aktualny poziom jest niemal taki jak w poprzednim roku, różniąc się zaledwie o 0,4 pkt w dół. Należy jednak zauważyć, że skala zarówno wzrostów, jak i spadków różni się w zależności od kierunku. Najciekawsze obecnie procesy zachodzą za naszą zachodnią granicą.

OKIEM SECURITY

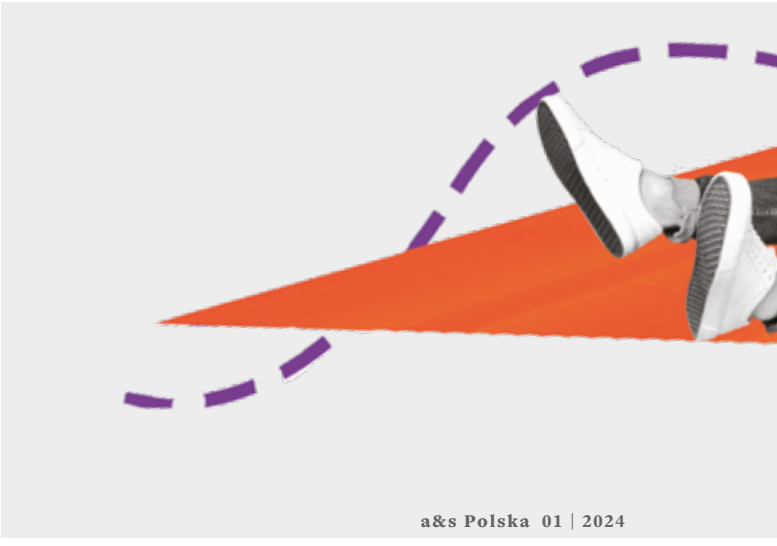
BEZPIECZEŃSTWO TRANSPORTU W POLSCE

Stan transportu w Polsce to nie tylko wskaźniki wzrostu, ale też bezpieczeństwo ludzi i towarów. Od 1 stycznia 2022 do 9 sierpnia 2023 r. zgłoszono do TAPA EMEA Intelligence System (TIS) w regionie Europy, Bliskiego Wschodu i Afryki (EMEA) 24 926 kradzieży ładunków wymierzonych w łańcuchy dostaw. TAPA podaje, że spośród tych incydentów tylko dla 17% z nich możliwe było uzyskanie danych o stratach finansowych. Całkowita wartość produktów, które zostały skradzione i dla których dostępne są dane (czyli 4241 zarejestrowanych przestępstw), wyniosła 332 460 061 euro.

Do kradzieży dochodzi przede wszystkim w Europie Północnej i na Wyspach Brytyjskich. Choć w Polsce towarzystwa ubezpieczeniowe od lat nie notują większej liczby napadów na transport drogowy, to nasz kraj nie jest postrzegany jako bezpieczny. Porównanie całkowitej liczby zgłoszonych przestępstw w Polsce z ogólną statystyką dla regionu EMEA (222 vs. 24 926) wykazuje zastanawiająco niski poziom zgłoszeń. Według analiz TAPA w Polsce (tak samo jak w Europie) dochodzi do znacznie większej liczby kradzieży ładunków, niż sugerują to te dane.

W badanym okresie do TAPA EMEA zgłoszono 222 incydenty kradzieży ładunków w Polsce. Dla 130 z nich, czyli 58,5% przestępstw, dostępne są informacje o poniesionych stratach finansowych. Całkowita strata wyniosła 4 974 495 euro. Średnia strata w przypadku przestępstw dotyczących towarów o wartości 100 000 euro lub więcej wyniosła 517 182 euro.

Malejące bezpieczeństwo przewozów w Polsce staje się coraz większym problemem. Dane prezentowane przez TAPA EMEA wyraźne wskazują na znaczący wzrost zainteresowania transportem coraz bardziej zorganizowanych i wyspecjalizowanych grup przestępczych. Większa specjalizacja wiąże się z bardziej wysublimowanymi sposobami pozyskiwania informacji o ładunku i metodami jego kradzieży. Dlatego tak istotne jest budowanie systemu bezpieczeństwa. Jego elementami są środki transportu, odpowiednio przeszkolony personel oraz infrastruktura parkingowa.



Kierunek: Niemcy

Szykuje się zmiana na najważniejszym kierunku, jeżeli chodzi o import i eksport z Polski, czyli Niemcy. Dane wskazują, że pozycja wieloletniego lidera może zostać zachwiana, a co za tym idzie – może także się zmienić wolumen transportu między Wisłą a Renem. W roku 2023 wielkość eksportu do zachodniego sąsiada wyniosła 229,9 mld zł, co stanowiło 28% ogółu polskiego eksportu (dane sygnalne GUS za I–VI 2023). Wielkość importu z Niemiec w tym okresie wyniosła 159,4 mld zł, co stanowiło 19,9% całego polskiego importu. Równocześnie wartość prestiżowego wskaźnika PMI – gdzie wynik powyżej 50 oznacza dobrą koniunkturę, poniżej zaś sygnalizuje słabnącą sytuację gospodarczą – dla Niemiec wynosił 42,6 w listopadzie i 43,3 w grudniu, i nie były to wypadki przy pracy. Tak niskie, a nawet niższe poziomy utrzymują się od miesięcy. Międzynarodowy Fundusz Walutowy prognozuje co prawda wzrost gospodarczy w Niemczech na poziomie 8% w latach 2019–2028. Inne gospodarki mają jednak wzrosnąć znacznie bardziej, np. Stanów Zjednoczonych o 17%, Holandii o 15%, a Polski o blisko 30%. Niemcy wchodzą w okres spowolnienia gospodarczego, a to odbije się na łańcuchach dostaw w całej Europie.

Zmniejszający się handel towarowy prowadzi do spadku zapotrzebowania na usługi transportowe i logistyczne, co wyraźnie odczuwają sektory automotive i budowlany z powodu zmniejszenia liczby zamówień. Dla rynków takich jak Polska i inne kraje Europy Środkowo-Wschodniej osłabienie niemieckiej dominacji może stanowić szansę na rozwój. Dotychczas Polska była postrzegana jako wsparcie dla niemieckiego przemysłu, np. poprzez produkcję foteli samochodowych czy pasów bezpieczeństwa. Z końcem ery taniej ropy i taniego gazu w Niemczech otwiera się możliwość przejęcia większej części rynku i przeniesienia produkcji do Polski, zwłaszcza produktów o wysokiej wartości. To zmieni strukturę eksportu i importu, a więc także branżę TSL.

OKIEM SECURITY

WYZWANIA POLSKIEGO TRANSPORTU

Zapotrzebowanie na usługi z branży TSL w Polsce rośnie. Aby firmy transportowe mogły sprostać rosnącym wymaganiom klientów oraz szybszemu tempu pracy, konieczna jest automatyzacja.

Z automatyzacją procesów w firmach transportowych, logistycznych i spedycyjnych jeszcze do niedawna można było spotkać się jedynie w obrębie funkcjonowania magazynów czy centrów dystrybucyjnych. Jednak z roku na rok zakres wdrożeń znacznie się poszerza, obejmując również transport drogowy. Dzięki mapom czy nawigacjom można zlokalizować pojazd, a także zoptymalizować trasę. Coraz częściej systemy zarządzania transportem usprawniają pracę między przewoźnikami a producentami. Programy TMS oferują użytkownikom nadzór nad terminami płatności, możliwość wystawiania faktur, planowanie tras przewozu, monitorowanie zleceń, nadzór nad aplikacjami dla kierowców i telematyką.

Wszystkie te połączone technologie obiecują ogromne korzyści, ale niosą również wyzwania związane z cyberbezpieczeństwem. Systemy, które wcześniej nie były narażone na ataki sieciowe, są teraz podłączone do internetu, a to stwarza zagrożenie. Jeśli potencjalni hakerzy znajdą ich słabe punkty, mogą je wykorzystać w każdym obszarze ataku. Dlatego na wszystkich szczeblach sektora transportowego, od inżyniera torów po kierownictwo wyższego szczebla, należy włożyć znacznie więcej pracy w kampanie uświadamiające i edukację, aby pomóc ludziom zrozumieć zagrożenie dla cyberbezpieczeństwa. Ludzie, procesy i technologia muszą być brane pod uwagę przy podejmowaniu skutecznych środków bezpieczeństwa. Należy opracować programy szkoleniowe, które nie są częścią jednorazowego procesu wdrażania: regularne monitorowanie i wyniki powinny być wbudowane w kluczowe wskaźniki efektywności personelu.

Istotne jest również, aby zasady uwzględniania bezpieczeństwa już w fazie projektowania były również szerzej stosowane. Wdrażając nowe rozwiązania, należy wprowadzić strategie oceny i ograniczania ryzyka na każdym etapie procesu projektowania. Oznacza to również uwzględnienie sposobu, w jaki nowe systemy integrują się ze starszymi.

» Aby firmy transportowe mogły sprostać rosnącym wymaganiom klientów oraz szybszemu tempu pracy, konieczna jest automatyzacja. «

Problem brakujących kierowców nierozwiązany

Sygnalizowany właściwie stale problem braku kierowców zawodowych na trasach międzynarodowych był paląco aktualny w 2023 r. i wygląda na to, że taki pozostanie także w roku 2024. Według szacunków Międzynarodowej Unii Transportu Drogowego (IRU) w 2023 r. na świecie brakowało ok. 2,8 mln kierowców zawodowych. Zgodnie z danymi IRU deficyt w Europie wynosił ok. 233 tys. osób, z czego w Polsce nawet 150 tys. Branża transportowa jest dobrze opłacana, ze średnim wzrostem płac powyżej średniej krajowej – ponad połowa kierowców zarabiała ponad 7700 zł netto, przy średniej wynoszącej 7671 zł już w 2022 r. Kierowcy pracujący w najbardziej uciążliwych systemach (3/1 i 4/1, czyli 3 lub 4 tygodnie w trasie i tydzień odpoczynku) mogli liczyć na zarobki sięgające niemal 10 tys. zł.

Dobre i stabilne zarobki są fundamentem utrzymania pracowników w firmach, ale to nie wystarcza. Właściciele i organizacje zrzeszające przewoźników coraz bardziej świadome sytuacji, pragnąc jej zaradzić, opracowali poradnik „50 sposobów, jak zatrzymać kierowcę w firmie i doprowadzić do jej rozwoju", w którym pojawiają się pomysły mające pomóc zatrzymać pracowników w firmach i przyciągnąć do pracy innych. Pewnym rozwiązaniem jest zatrudnianie obcokrajowców – w 2022 r. w Polsce pracowało 160,6 tys. kierowców z innych państw, głównie Ukrainy i Białorusi. Te kierunki zdają się już wyczerpywać, dlatego firmy transportowe rozważają zatrudnianie kierowców zawodowych spoza Unii. Przeszkodą w zatrudnianiu nie-Polaków jest administracja, której wymogi są czaso- i kosztochłonne. Kandydat musi zdobyć tzw. kod 95, który jest odpowiednikiem karty kwalifikacji kierowcy. Następnie stara się o kartę kierowcy (tacho), co jest niezbędne do uzyskania certyfikatu kierowcy i uprawnień do kierowania pojazdem. Dodatkowo, osoby posiadające międzynarodowe prawo jazdy wraz z prawem jazdy krajowym, mogą prowadzić pojazd tylko przez 183 dni. Po tym czasie muszą zdać egzamin teoretyczny, aby otrzymać polskie prawo jazdy. Po jego zdobyciu wymagane jest uzyskanie nowej karty tacho. W tym okresie kierowca nie może pracować, a przewoźnik ponosi związane z tym koszty.

Regulacje wbrew branży?

Od roku 2020 wchodziły w życie kolejne elementy Pakietu Mobilności, który m.in. wymusił jednolite zasady wynagradzania kierowców, w tym także obcokrajowców spoza UE, którzy jeżdżą u naszych przewoźników. W roku 2023 był to obowiązek wyposażenia wszystkich nowo zarejestrowanych pojazdów w tachografy piątej generacji, które miały zastąpić urządzenia analogowe i automatycznie rejestrować moment przekroczenia granicy. Niestety brakuje ich na rynku i wiele pojazdów nadal nie spełnia nowych unijnych norm. Urządzenia miały być połączone systemem nawigacji satelitarnej Galileo, jednak wystąpiły problemy z jego pełnym wdrożeniem przez Europejską Agencję Kosmiczną. Bez zagłębiania się w szczegóły techniczne tzw. tachografy inteligentne drugiej generacji (G2V2) napotykają problem uzyskania uwierzytelnienia pozycji ciężarówki, ponieważ jeszcze nie zostały ukończone prace nad technologią OSNMA, która to umożliwia. Unijna komisarz ds. transportu Adina Vălean nie zgodziła się na odroczenie obowiązku do końca 2023 r.

Od 31 grudnia 2024 r. będą obowiązywać dwie kolejne zasady:

- zakres kontroli na drodze zostanie zwiększony z 28 do 56 dni,
- inteligentne tachografy drugiej generacji powinny być instalowane również w pojazdach starszych, wykorzystywanych do transportu międzynarodowego, które do tej pory nie były wyposażone w tego typu urządzenia.

OKIEM SECURITY

SPOSOBY ZABEZPIECZANIA PRZEWOZÓW

W codziennej pracy kierowcy zawodowego na pierwszy rzut oka nie zawsze widać nic nadzwyczajnego ani niebezpiecznego. Długie odcinki autostrad, monotonne postoje w różnych miejscach, powtarzalne krajobrazy – to wszystko zdaje się pozbawione emocji. Jednakże ci, którzy wybierają tę profesję, każdego dnia narażeni są na różnorodne zagrożenia. Im bardziej wartościowy i rozpoznawalny jest przewożony ładunek, tym większe ryzyko ataku podczas postoju. Zorganizowane grupy przestępcze, operujące nie tylko na polskich drogach, ale także w całej Europie, stosują przemoc lub podstęp, aby przejąć ładunki z ciężarówek. Dla kierowców ciężarówek ryzyko może występować w każdym miejscu, zwłaszcza z uwagi na to, że złodzieje potrafią wykorzystać różne metody, takie jak sfingowane wypadki drogowe, aby przejąć towar. Statystyki pokazują, że problem kradzieży dotyka aż 75% firm specjalizujących się w Polsce w międzynarodowym przewozie.

W obliczu rosnących zagrożeń kradzieżą firmy spedycyjne i transportowe wybierają rozwiązania techniczne mające realny wpływ na poprawę bezpieczeństwa. Zaczynając od rozwiązań przeciwdziałających kradzieży paliwa (specjalne sitka lub zabudowy całego zbiornika) czy blokad służących do trwałego zabezpieczenia drzwi od środka podczas snu kierowcy, przez systemy do monitoringu GPS, zamki elektroniczne, kończąc na systemach alarmowych. Najczęściej wykorzystywany jest monitoring GPS pozycji ciężarówki i naczepy, natychmiast alarmujący o zatrzymaniu w niedozwolonym miejscu lub podejrzanym ruchu. Innym jest wandaloodporny czujnik otwarcia drzwi oparty najczęściej na technologii zbliżeniowej. Informacja o każdym otwarciu naczepy trafia do centrum monitorowania, a także np. do aplikacji spedytora, na telefon kierowcy czy do osoby odpowiedzialnej za transport. Doposażenie tego rozwiązania w system alarmowy (aktywowany i deaktywowany automatycznie, przez kierowcę, spedytora lub np. firmę świadczącą usługi ochrony transportu) umożliwia nadzór tylko nieautoryzowanego otwarcia drzwi naczepy i w razie potrzeby uruchomienia alarmu w pojeździe.

Komisja Europejska stwierdziła, że w Unii brakuje 100 tys. miejsc parkingowych (na 300 tys. zbudowanych). Szacuje się, że w Polsce potrzeba dodatkowo kilkunastu tysięcy miejsc. Choć jak wykazują dane ubezpieczycieli, ryzyko kradzieży w większym stopniu jest związane z rodzajem przewożonych ładunków niż ze specyfiką danego kraju. Do kradzieży dochodzi na przygodnych, niestrzeżonych parkingach. Niebezpieczne jest każde miejsce nietypowe, czyli nieogrodzone, nieoświetlone i niedozorowane. Do wielu kradzieży dochodzi także w miejscu rozładunku, gdzie pojazd parkowany jest wzdłuż drogi dojazdowej do odbiorcy, a kierowca nie ma już czasu, by zaparkować pojazd w bezpiecznym miejscu.

Ograniczenie ryzyka w transporcie to więcej niż tylko zabezpieczenie pojazdów. Konieczne jest skoncentrowanie się na odpowiednim przeszkoleniu kierowców, dbałości o staranność na każdym etapie transportu. Niedopuszczalne jest samowolne zmienianie trasy, przerywanie postoju czy

oddalanie się od pojazdu w czasie odpoczynku. Kierowcy powinni być czujni i muszą unikać rozmów z niepowiązanymi osobami na temat ładunku i trasy. Sprawdzenie stanu plomb przed wyjazdem w trasę jest kluczowe. Specjaliści zalecają firmom transportowym, aby unikały pośpiechu i dokładnie weryfikowały swoich kontrahentów, co pozwoli na zminimalizowanie potencjalnych zagrożeń.

Środowisko zagraża transportowi

Unia Europejska od pewnego czasu wprowadza szereg regulacji mających na celu ochronę środowiska, w tym także wprowadza opłaty za emisję dwutlenku węgla. Tym właśnie jest myto. Jak ostrzegają eksperci, koszt tego domiaru odbije się na gospodarkach Unii. Większa część kosztów związanych z opłatą za emisję CO_2 zostanie przeniesiona na konsumentów końcowych poprzez handel detaliczny. To z kolei będzie nadal przyczyniać się do wzrostu inflacji.

O jakich kosztach podstawowych mowa? Z obliczeń Polskiej Izby Spedycji i Logistyki wynika, że po podniesieniu stawek myta koszt przejazdu na terenie Niemiec ciężarówką o masie 40 ton i spełniającą normę Euro 6 wzrośnie z 19 eurocentów do 35,40 eurocenta, co stanowi wzrost o 86%. Oznacza to, że koszt przejazdu tranzytowego takim pojazdem zwiększy się o 123 euro. W rezultacie opłaty za frachty drogowe mogą podnieść się o 4–7%, a w przypadku przewozów kabotażowych w Niemczech nawet o 10%. Zachodzi obawa, że mali przewoźnicy – a takich jest w Polsce większość – mogą nie przetrwać tych podwyżek lub próbować przerzucić je na swoich

» Ograniczenie ryzyka w transporcie to więcej niż tylko zabezpieczenie pojazdów. Konieczne jest skoncentrowanie się na odpowiednim przeszkoleniu kierowców, dbałości o staranność na każdym etapie transportu. «

→

kontrahentów lub pracowników, np. rozwiązując z nimi umowy o pracę, płacąc „pod stołem" lub manipulując przy czasach przejazdu. Podwyżka cen myta i wprowadzenie opłaty za emisję dwutlenku węgla mają być zachętą do zmiany floty na taką o napędzie elektrycznym, na co branża nie jest gotowa.

OKIEM SECURITY

KOSZTY PROWADZENIA BIZNESU

Automatyzacja pozwala na obniżenie kosztów personalnych nawet o 40–70%. Koszt pracowników stanowi prawie połowę wszystkich kosztów. Automatyzacja operacji przeładunkowych oznacza zredukowanie czynnika ludzkiego potrzebnego do pracy, np. przy obsłudze urządzeń rozładunkowych oraz zarządzających tym zespołem. Według szacunków ekspertów w 2040 r. większość obiektów zostanie zautomatyzowana pod względem urządzeń technicznych, systemów zarządzania oraz infrastruktury, zapewniając szybszą identyfikację pojazdu i naczepy, odprawę kierowcy, krótszy czas załadunku i mniejszą liczbę błędów. Warto pamiętać o ograniczeniach automatyzacji takich jak trudność w reagowaniu na nieprzewidziane zmiany, ryzyko związane z dostawami energii elektrycznej, dostępem do Internetu, zwiększone ryzyko ataków hakerskich, a także obawa ludzi o utratę stanowiska. Jednakże przy zwiększonych wolumenach w transporcie oraz braku pracowników w logistyce i transporcie – automatyzacja jest niezbędnym i kolejnym elementem w czasach rewolucji przemysłowej 4.0.

Z technicznego punktu widzenia najważniejsze wymogi niezbędne do realizacji ciężarowej rewolucji są już w zasięgu ręki. Autonomiczne samochody dostawcze to coraz częstszy widok w Stanach Zjednoczonych. Również Francja i Szwecja wprowadziły przepis pozwalający na poruszanie się po drogach zdalnie sterowanym pojazdom ciężarowym. Samochody ciężarowe bez kierowcy poruszają się już w wielu kontrolowanych środowiskach, takich jak porty czy duże tereny przemysłowe. Oczywiście, taka technologia nie jest jeszcze obecna na rynku, a wszystkie kursy odbywają się na zasadzie testów. Niemniej jednak to spory krok w kierunku rozwoju technologii transportu towarów. Planowym terminem całkowitego wdrożenia zdalnie sterowanych i nieposiadających kabin samochodów ciężarowych jest rok 2030. Dzisiaj na coraz większą skalę wykorzystywane są zrobotyzowane ciągniki siodłowe służące do przestawiania naczep w parku logistycznym na wzór podobnych używanych w magazynach do transportu towaru.

Trendy na 2024: Nearshoring i automatyzacja

Nearshoring, czyli przenoszenie produkcji i dystrybucji blisko rynków zbytu, okazał się trwałym trendem. Zapoczątkowany po pandemii, nadal się utrzymuje i rozwija. Choć nie odbywa się on bezkosztowo, bo wymaga przeorganizowania procesów i początkowych inwestycji w uruchomienie nowych miejsc produkcji, kolejne duże firmy wyrażają zainteresowanie nieruchomościami komercyjnymi w środkowo-wschodniej części Europy. W analizie opłacalności nearshoringu, gdzie krótsze trasy obniżają koszty i zwiększają terminowość dostaw, kluczowe są niższe koszty transportu. Sprzyja mu budowa nowych korytarzy transportowych w Europie, np. Via Carpatia łącząca litewską Kłajpedę z Salonikami. To zwiększa atrakcyjność inwestycyjną regionu.

Polska, z rozwiniętym rynkiem magazynowym i niższymi niż na Zachodzie kosztami wynajmu, stała się ważnym europejskim hubem e-commerce oraz kluczowym rynkiem w elektromobilności, produkującym chociażby znaczną część baterii litowo-jonowych do samochodów elektrycznych. Pod koniec października 2023 r. w Brukseli zaprezentowano raport agencji Reuters Events *Czy Polska może się stać bijącym sercem europejskiej produkcji?* Wyniki są jednoznaczne: przez swoje centralne położenie geograficzne i dobre połączenia transportowe, a także dostępność wykwalifikowanej kadry pracowniczej oraz zapasy powierzchni magazynowej może bardzo skorzystać w najbliższej przyszłości.

Eksperci Cushman & Wakefield uznali nearshoring za trwały trend na kontynencie europejskim. Różnica kosztów produkcji między Azją a Europą nie jest już tak ogromna, a firmy coraz częściej biorą pod uwagę czynniki pozaekonomiczne, takie jak zrównoważony rozwój. Ponadto coraz częściej wykorzystują do produkcji nowoczesne technologie, co wpływa na obniżenie kosztów. W obliczu wzrostu kosztów pracy i spadku dostępności specjalistów, takich jak kierowcy i spedytorzy, automatyzacja powtarzalnych zadań wydaje się naturalnym posunięciem. Część rozwiązań transportowych, m.in. giełdy transportowe czy systemy do zarządzania transportem (TMS), już została zautomatyzowana, jednak branża wciąż jest na początku tej drogi. Piotr Hunker, lider firmy Trans.eu, stwierdził: *Cały czas brakuje nam głównego elementu, tzw. digital connectivity, i standardów wymiany danych.* Jego wypowiedź znalazła się w raporcie *Rynek transportowo-logistyczny w Europie 2023–2024.*

OKIEM SECURITY

BEZPIECZEŃSTWO PONAD WSZYSTKO

Kluczem do sukcesu jest zwiększenie bezpieczeństwa. Dlatego już w grudniu 2017 r. zostało uruchomione narzędzie do zwalczania przestępczości w transporcie drogowym: Automatyczny System Rozpoznawania Numerów Rejestracyjnych (*Automatic Number Plate Recognition System* – ANPRS). System ten wykorzystuje to, że we wspólnej sieci są połączone polskie, estońskie, łotewskie i litewskie systemy rozpoznawania numerów rejestracyjnych. Dostarcza on informacji niezbędnych w walce z przestępczością zorganizowaną dzięki możliwości śledzenia pojazdów i reagowania na nieprawidłowości w czasie rzeczywistym. Są one weryfikowane pod kątem wystąpienia jakichkolwiek nieprawidłowości (m.in. czy pojazd został zgłoszony jako skradziony, porusza się z fałszywymi tablicami, podejrzane pojazdy podążające za transportem lub go poprzedzające).

Działanie systemu opiera się na kamerach sczytujących numery tablic pojazdów samochodowych. Urządzenia te są rozmieszczone na granicach zewnętrznych UE i głównych szlakach komunikacyjnych, na granicach wewnętrznych, a także w samochodach operacyjnych Krajowej Administracji Skarbowej. Dane gromadzone poprzez ten system ułatwiają wykrywanie międzynarodowych szlaków przemytniczych. ANPRS stał się również jednym z elementów szerszego projektu monitorowania drogowego przewozu towarów. •

» Według szacunków ekspertów w 2040 r. większość obiektów zostanie zautomatyzowana pod względem urządzeń technicznych, systemów zarządzania oraz infrastruktury, zapewniając szybszą identyfikację pojazdu i naczepy, odprawę kierowcy, krótszy czas załadunku i mniejszą liczbę błędów. «

Przestępczość na trasie. Jesteśmy w pierwszej dziesiątce. I to niedobrze

Skradzione paliwo, uszkodzona plandeka, zniszczona naczepa, zerwana plomba, zrabowany towar – do takich zdarzeń na polskich drogach dochodzi nad wyraz często. Kierowcy ciężarówek, chcąc dowieźć towar na miejsce, muszą mieć oczy dookoła głowy.

Raport przygotowany przez TAPA za 2023 rok *Who's more… resilient?* nie pozostawia złudzeń. Przestępczość wymierzona w transport drogowy rośnie. Na europejskich, czyli także na polskich drogach, a precyzyjnie na parkingach i miejscach postojowych dochodzi do wielu incydentów zagrażających ciągłości łańcucha dostaw. W czasie pandemii mieliśmy okazję się przekonać, jak wrażliwy jest to łańcuch. Wystarczy drobne zdarzenie, by naruszyć jego ciągłość. Konsekwencje mogą być różne – od przykrej niedogodności, jak brak świeżych bułek na śniadanie, po prawdziwy problem, czyli unieruchomiony zakład produkcyjny i straty idące w miliony złotych.

The Transported Asset Protection Association (TAPA) zostało założone w 1997 r. w odpowiedzi na rosnące na całym świecie zagrożenia związane z przewozem produktów. Pierwotnie TAPA przede wszystkim zajmowała się zagrożeniami dotyczącymi zaawansowanej, a tym samym drogiej elektroniki, potem także po prostu towarami o wysokiej wartości. Organizacja działa w zasadzie na całym świecie i koncentruje się na identyfikacji potencjalnych zagrożeń, a także na ochronie przed kradzieżą lub zniszczeniem przewożonych oraz magazynowanych

towarów. Sukcesywnie gromadzi również informacje o przestępstwach przeciwko mieniu, do jakich dochodzi w trakcie transportu. Dane te służą do tworzenia raportów pokazujących, na jakie ryzyko związane z transportem wystawiona jest branża TSL. Z danych zgromadzonych przez TAPA dotyczących pierwszych dziewięciu miesięcy 2023 r. (raport podsumowujący cały rok jeszcze nie został opublikowany) wynika, że był to dla branży TSL rok niespokojny.

Kosztowny rok

Nas oczywiście interesuje przede wszystkim rynek EMEA. Co na jego temat mówi raport TAPA? Otóż od stycznia do końca września 2023 r. do bazy TAPA EMEA Intelligence System (TIS) trafiły informacje o 49 366 atakach skierowanych przeciwko łańcuchowi dostaw, do jakich doszło w 67 różnych krajach regionu EMEA. I choć tylko w niewiele ponad 4% przypadków zgłaszający podali wartość strat, to były to straty na łączną kwotę 552 199 741 euro (!). A w przypadku 48 incydentów odnotowano straty przekraczające 1 milion euro. Kolejne 202 przestępstwa dotyczyły kradzieży produktów o wartości 100 000 euro lub większej.

» Od stycznia do końca września 2023 r. do bazy TAPA EMEA Intelligence System (TIS) trafiły informacje o 49 366 atakach skierowanych przeciwko łańcuchowi dostaw, do jakich doszło w 67 różnych krajach regionu EMEA. «

Gdzie jest najwięcej incydentów?

Niechlubny rekord należy do Republiki Południowej Afryki. W raportowanym okresie Policja Południowoafrykańska (South African Police – SAP) dodała do bazy TAPA informacje o ponad 40 tys. incydentów. Dotychczas dane dotyczące przestępczości TAPA EMEA w Południowej Afryce skupiały się głównie na znaczącej liczbie porwań ciężarówek i napadów na transporty pieniężne. Teraz SAP raportuje także kradzieże, napady na obiekty niemieszkalne, włamania do obiektów niemieszkalnych i kradzieże bydła. To ma wpływ na wynik rankingu, ale trochę go zaburza. Skupmy się więc na pozostałych krajach obecnych na liście tych z największą liczbą odnotowanych incydentów od stycznia do września 2023 r. Ranking otwiera Wielka Brytania z liczbą 3397 zdarzeń, po niej są Niemcy – 1170 zdarzeń. W pierwszej dziesiątce jest też niestety Polska, ale 115 zaraportowanych do TAPA incydentów wydaje się liczbą bardzo skromną w porównaniu z wynikami brytyjskim i niemieckim.

Skąd aż takie różnice? Być może wynikają ze skrupulatności raportowania. Tak przynajmniej przypuszcza prezes TAPA EMEA. Jeśli prezes EMEA się nie myli, nie jest to dobra wiadomość dla branży security. Z tej przyczyny, że specjaliści zajmujący się bezpieczeństwem łańcucha dostaw mogą skutecznie zarządzać ryzykiem i zapobiegać stratom tylko wtedy, gdy znają najbardziej prawdopodobne zagrożenia. Niezależnie od jakości raportowania nie powinien nas cieszyć fakt, że Polska znalazła się obecnie w pierwszej dziesiątce najbardziej niebezpiecznych krajów. W roku 2019 zajmowaliśmy 15. miejsce.

Więcej kradzieży paliwa, ale bezpieczniejsze parkingi

Zgodnie z danymi TAPA w 2023 r. nastąpił znaczny wzrost liczby kradzieży paliwa. Przyczyna wydaje się prozaiczna – dużo wyższe ceny paliwa wynikające m.in. z sytuacji geopolitycznej. TAPA EMEA otrzymała zgłoszenia 1526 takich incydentów w 27 krajach, a ponad 87% przestępstw zarejestrowano tylko w trzech z nich: Wielkiej Brytanii, Niemczech i Francji. Choć wartość skradzionego paliwa nie była duża, jest to jedno z takich wydarzeń, które znacząco negatywnie wpływają na bezpieczeństwo i odporność łańcucha dostaw. Unieruchomiona przez brak paliwa ciężarówka nie tylko nigdzie nie pojedzie. Może się też okazać, że złodzieje paliwa spowodowali jakieś uszkodzenie. To angażuje nie tylko kierowcę, ale także serwis spedytora. Przypadków kradzieży paliwa odnotowano więcej, ale za to zmniejszyła się liczba przestępstw związanych z niezabezpieczonymi miejscami parkingowymi.

Ważne pytania

Bezpieczeństwo łańcucha dostaw w dużej mierze zależy od tego, co dzieje się na drogach, choć wpływ mają także braki kadrowe, w tym brak kierowców, wysoka cena paliwa, ekstremalne i nieprzewidywalnie zmienne warunki pogodowe, wspomniane wcześniej kradzieże paliwa i ataki na kierowców odpoczywających na parkingach, ale też wtargnięcia imigrantów, takie jak choćby te z 23 listopada, o których pisała polska prasa.

Z perspektywy zapobiegania kradzieżom towarów autorzy raportu TAPA zadają pytania, na które powinni odpowiedzieć profesjonaliści ds. bezpieczeństwa łańcucha dostaw. Te pytania to m.in. jakie systemy i procesy bezpieczeństwa są najlepsze w przypadku środków transportu? Czy można ufać dostawcom? Czy nie doszło do nieautoryzowanego outsourcingu ze strony firmy świadczącej usługi transportowe. No i jedno z najważniejszych, czy została przeprowadzona ocena ryzyka całej trasy, którą towar podąża do odbiorcy. Odpowiedzi na te pytania pozwolą lepiej chronić cały łańcuch dostaw. •

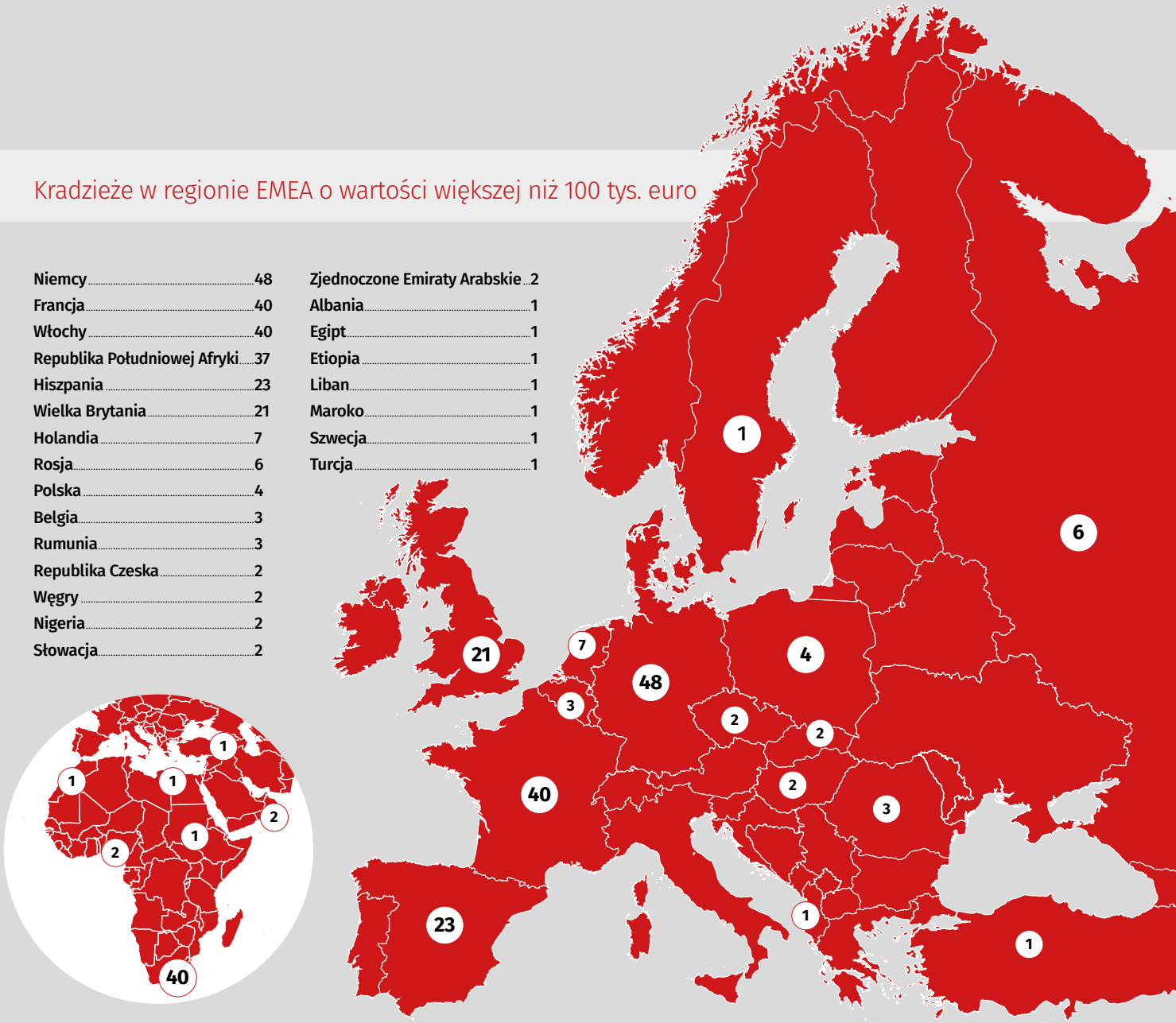
Na bazie raportu TAPA oprac. Monika Żuber-Mamakis

TOP 10 - Kraje z największą liczbą indcydentów zgłoszonych do TAPA EMEA

Kraj	Liczba incydentów	% wartości	Łączna wartość [€]	Średnia wartość przestępstw (powyżej 100 tys. €)
RPA	40742	0,31	18 507 521,00	145 728
Wlk. Brytania	3397	8,45	79 573 384,00	3 620 054
Niemcy	1770	34,12	134 066 965,00	2 652 959
Francja	814	39,43	41 034 658,00	88 527
Szwecja	682	1,76	563 334,00	370 221
Włochy	588	47,1	20 638 167,00	424 555
Hiszpania	481	34,9	21 670 057,00	827 607
Polska	115	61,7	2 210 163,00	353 138
Holandia	90	30	2 873 923,00	375 062
Rosja	81	66,6	4 358 498,00	664 033

Kradzieże w regionie EMEA o wartości większej niż 100 tys. euro

Niemcy	48
Francja	40
Włochy	40
Republika Południowej Afryki	37
Hiszpania	23
Wielka Brytania	21
Holandia	7
Rosja	6
Polska	4
Belgia	3
Rumunia	3
Republika Czeska	2
Węgry	2
Nigeria	2
Słowacja	2
Zjednoczone Emiraty Arabskie	2
Albania	1
Egipt	1
Etiopia	1
Liban	1
Maroko	1
Szwecja	1
Turcja	1



STRATA CAŁKOWITA: **524 186 212 €**

Incydenty zgłoszone do systemu TAPA EMEA Intelligence System

- 49 366 ataków przestępczych na łańcuchy dostaw w regionie EMEA w ciągu 273 dni
- Kradzieże ładunków zarejestrowane w 67 krajach
- Tylko w przypadku 4,4% podano wartość strat
- Łączna wartość strat dla tych 4,4% = 552 199 741 euro
- Średnia strata w przypadku poważnych przestępstw o wartości 100 tys. euro lub więcej = 2 096 744 euro
- Średnia dzienna strata od stycznia do września 2023 r. = 1 828 475 euro
- W 48 incydentach odnotowano straty przekraczające 1 mln euro
- 202 przestępstwa odnotowały straty >100 tys. euro

Hikvision Parcel Tracking: wydajniejsze śledzenie paczek w systemach magazynowych

Bezpieczeństwo magazynu oraz efektywność operacji to priorytety operatorów magazynowych. Hikvision oferuje im kompleksowe rozwiązanie – Hikvision Parcel Tracking.

Bartłomiej Skórski

Rozwiązanie oferowane przez Hikvision skupia się na czterech kluczowych obszarach związanych z obsługą przesyłek wewnątrz magazynu: podniesieniu ogólnego poziomu bezpieczeństwa za pomocą zaawansowanych rozwiązań z zakresu ochrony, usprawnieniu zarządzania ruchem w magazynie, zwiększeniu możliwości planowania operacji w dokach załadunkowych oraz monitorowaniu przesyłek. Całość stanowi kompleksowe rozwiązanie do zarządzania magazynem, którego celem jest uzyskanie maksymalnie bezpiecznego i inteligentnego środowiska magazynowego.

Wydajne rozwiązania z funkcją wizualizacji

Każdego dnia operatorzy centrów dystrybucyjnych napotykają różne wyzwania związane z niezadowalającymi doświadczeniami klientów oraz skargami wynikającymi z utraty lub uszkodzenia towarów. Istniejące na rynku systemy zarządzania magazynem oraz systemy

Funkcje systemu

- **PRECYZYJNE WYSZUKIWANIE PACZEK** dzięki zapisowi wideo prowadzonemu w punktach kontrolnych umożliwia szybkie rozpatrywanie problemów.
- **POŁĄCZONE WIDEO NA WĘZŁACH PRZENOŚNIKOWYCH** zapewnia śledzenie całego procesu.
- **STATYSTYKI OBSŁUGI PACZEK NA KAŻDYM WĘŹLE** umożliwiają, w porównaniu z innymi systemami, lepszą weryfikację ilościową.

monitoringu wizyjnego działają niezależnie od siebie, co może prowadzić do braku dowodów wideo oraz komplikacji w odzyskiwaniu konkretnej informacji na temat paczek lub nagrań w celu ustalenia źródła problemu i identyfikacji odpowiedzialnych osób. Niemożność śledzenia paczek podczas ich transportu przenośnikiem, szczególnie gdy jest on np. wielowęzłowy, może prowadzić do zablokowania przenośnika lub skierowania przesyłek ich w błędne miejsce.

Hikvision zapewnia wydajne rozwiązanie do śledzenia przesyłek z funkcją wizualizacji, które usprawnia monitorowanie łańcucha dostaw, poprawiając jednocześnie ogólną wydajność. Dane z systemu monitoringu wizyjnego i systemu odczytu kodów kreskowych są dopasowywane i archiwizowane na platformie HikCentral według czasu, miejsca, identyfikatora przesyłki i wideo. Co więcej, system monitoringu wizyjnego można zintegrować z wieloma systemami odczytu kodów kreskowych innych firm, by zwiększyć jego elastyczność.

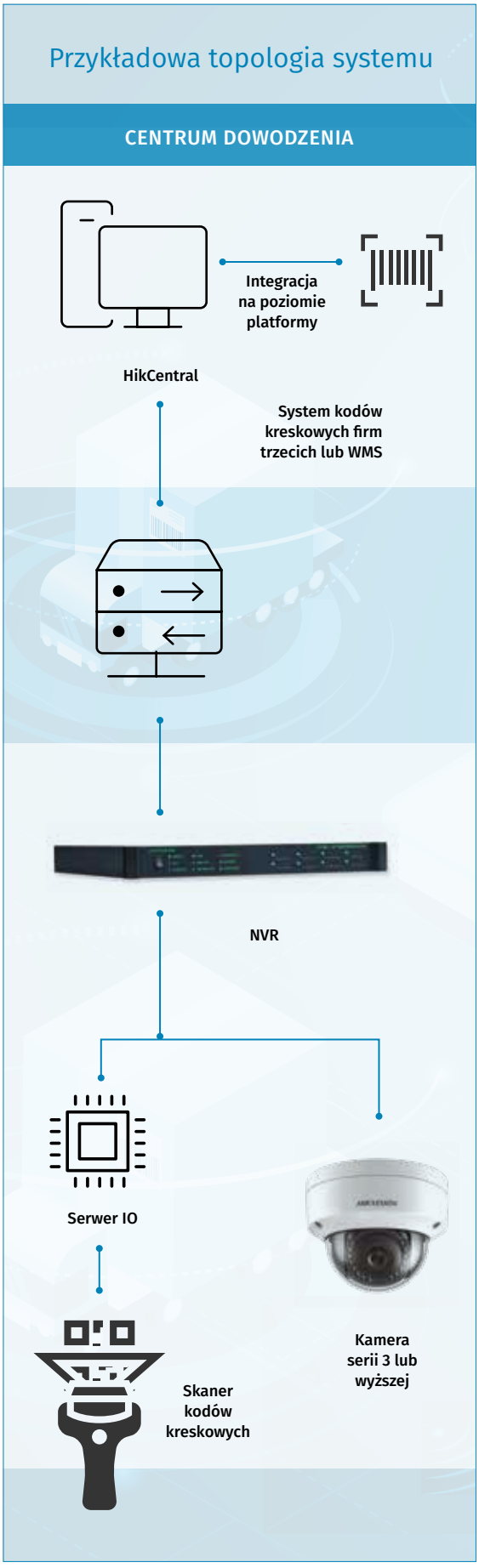
Śledzenie przesyłek

Korzyści z wdrożenia systemu Hikvison Parcel Tracking to m.in. przyspieszenie rozpatrywania spraw klientów dzięki zintegrowanemu systemowi i szybkiemu zlokalizowaniu wideo paczek na podstawie identyfikatorów paczek, a także możliwość śledzenia ruchu paczek niezależnie od tego, jak skomplikowany jest system przenośnikowy. Do śledzenia wykorzystywane są widzenie maszynowe i kamery konwencjonalne. Hikvision Parcel Tracking ułatwia przeprowadzanie inwentaryzacji liczby paczek oraz szybkiego wykrywania utraty lub przypadkowego pomijania przesyłek za pomocą zintegrowanej platformy HikCentral służącej do zarządzania wszystkimi systemami.

Śledzenie przesyłek na stanowiskach kontroli jakości i pakowania zapewnia łatwe rozpoznawanie i śledzenie paczek na każdym etapie ich drogi przez magazyn. Możliwa jest także archiwizacja i dopasowanie danych: czas, miejsce, indentyfikator paczki, materiał wideo. Wszystko dzięki integracji systemu monitoringu wideo (śledzenie przesyłek) z systemem odczytu kodów kreskowych. Śledzenie ruchu paczek na stanowiskach pakowania jest bardziej efektywne dzięki połączeniu kamer Hikvision i skanerów kodów z tym samym rejestratorem wideo oraz integracji z systemami odczytu kodów kreskowych firm trzecich. Dzięki statystykom obsługi paczek na każdym węźle weryfikacja ilościowa jest efektywniejsza w porównaniu z innymi systemami przenośnikowymi.

Śledzenie przesyłek na systemach przenośnikowych jest intuicyjne nawet w przypadku funkcjonowania bardzo złożonych systemów przenośnikowych. Możliwe jest np. śledzenie całej trasy paczki niezależnie od tego, jak skomplikowany jest system przenośnikowy oraz odtworzenie wideo z zapisem trasy dowolnej paczki uwiecznionym przez serię połączonych kamer; wszystkie powiązane nagrania mogą być łączone i eksportowane jako jeden plik do łatwego przejrzenia. W tym celu wystarczy wyposażyć węzły początkowe i krzyżowe na taśmie przenośnikowej w inteligentne czytniki kodów i kamery IP, a resztę taśmy w kamery konwencjonalne. Ponadto dzięki integracji z systemami odczytu kodów kreskowych firm trzecich można szybko kontrolować liczbę przesyłanych paczek dzięki statystykom obsługi paczek na każdym węźle. ●

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



Rozwiązania w zakresie bezpieczeństwa dla kolei i metra

Dla operatorów kolejowych i metra bezpieczeństwo infrastruktury, w tym tuneli kolejowych i przejazdów, jest priorytetem. W Europie główną przyczyną śmiertelnych wypadków na terenach kolejowych jest wtargnięcie osób nieuprawnionych. Zapobieganie tego typu incydentom nabiera dużego znaczenia.

Do wykrywania intruzów w tunelach stosuje się zaawansowane technologie, takie jak detektory laserowe REDSCAN Pro firmy OPTEX. Urządzenia te wykorzystują analizę danych i odpowiednio dopasowane algorytmy detekcji do precyzyjnego wykrywania osób, ignorując jednocześnie ruch pociągów.

Wykrywanie intruzów wewnątrz tuneli

Tunele kolejowe i tunele metra to zamknięte, ciemne i często wilgotne przestrzenie. Warunki oświetlenia nie mają wpływu na działanie detektorów laserowych, co czyni je rozwiązaniem idealnym do tego rodzaju zastosowań. Ponadto detektory LiDAR są wyposażone w funkcję analizy środowiska, co umożliwia im dostosowanie strefy detekcji, automatyczne adaptowanie się do zmian oraz informowanie systemu zabezpieczeń o potencjalnych zakłóceniach, takich jak zabrudzenie soczewki.

Detektory laserowe z serii REDSCAN Pro analizują rozmiar i odległość wykrywanych obiektów, co oznacza, że śledzą je w obrębie obszaru detekcji i rozpoznają zależność między rozmiarem obiektu a jego odległością od detektora. Daje to możliwość precyzyjnego wykrywania obiektów różnej wielkości zarówno oddalonych, jak i znajdujących się blisko detektora. W przypadku tunelu oznacza to np. możliwość odróżnienia osoby od pociągu.

Prawidłowo działająca detekcja nieuprawnionego wejścia do tunelu musi ignorować pociągi, wykrywając osoby, a funkcję tę spełnia specjalnie opracowany algorytm. Jeśli ruchomy obiekt wielkości pociągu znajdzie się w tunelu, alarm nie zostanie wygenerowany. Jeśli jednak do tunelu wejdzie obiekt wielkości człowieka, nawet gdy równocześnie będzie wjeżdżał pociąg, osoba ta zostanie wykryta, co spowoduje włączenie alarmu.

Bezpieczniejszy przejazd kolejowy

Bezpieczeństwo przejazdów kolejowych jest również kluczowe. Laserowe systemy detekcji REDSCAN Pro zostały zastosowane na ponad 400 przejazdach w Wielkiej Brytanii. Umożliwiają one wykrywanie niebezpiecznych sytuacji, takich jak kierowcy próbujący ominąć szlabany oraz piesi lub rowerzyści, którzy mogą utknąć między szlabanami. Systemy LiDAR potrafią wykrywać na torach nawet małe dzieci. Dzięki integracji czujek LiDAR z systemami telewizji dozorowej operatorzy mogą „obejrzeć" przebieg zdarzenia, unikając poważnego wypadku i ostrzegając zawczasu maszynistę nadjeżdżającego pociągu. Uzyskane w ten sposób obrazy można wykorzystać w postępowaniu przeciwko osobie kierującej pojazdem, która naruszyła przepisy.

Układ sygnalizacji informuje system LiDAR, gdy przejazd kolejowy jest aktywny, a system detekcji skanuje obszar przejazdu znajdujący się między szlabanami. Jeśli przejazd jest „czysty" lub jeżeli na przejeździe nie znajdują się żadne osoby lub inne obiekty, semafor zmienia kolor na zielony, a pociąg może bezpiecznie przejechać. W przypadku wykrycia obiektu bariery podnoszą się, umożliwiając pieszemu lub pojazdowi opuszczenie monitorowanego obszaru, zanim będzie możliwy przejazd pociągu. Jeśli obiekt jest nieruchomy, a system wykona trzy cykle detekcji, możliwe jest wysłanie komunikatu ostrzegającego maszynistę i nakazującego mu jazdę z prędkością nieprzekraczającą 8 km/h w celu rozpoznania obiektu, który znalazł się na torach. ●

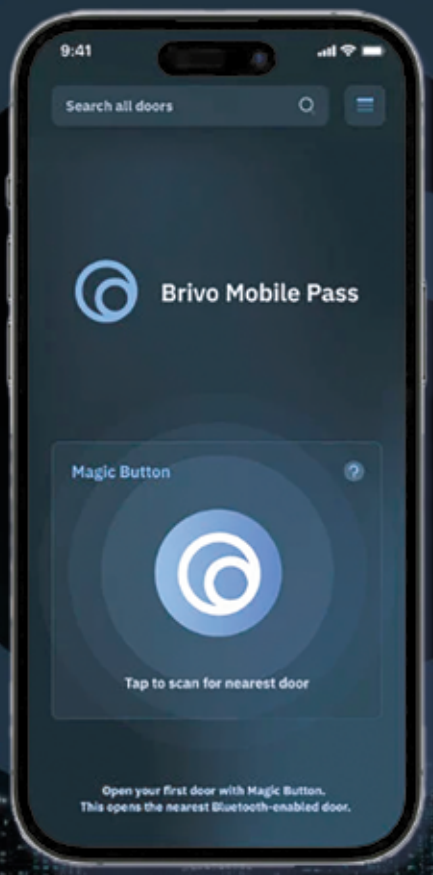
OPTEX Security
ul. Sielecka 35, 00-738 Warszawa
optex@optex.com.pl
www.optex.europe.com/pl

brivo

smart-i

DOSTĘP JEST PRZYSZŁOŚCIĄ INTELIGENTNYCH BIUR

ZOPTYMALIZUJ SWOJE NIERUCHOMOŚCI DZIĘKI KONTROLI DOSTĘPU BRIVO



Technologia zabezpieczeń klasy korporacyjnej dla każdego rodzaju obiektu

60+

KRAJÓW NA CAŁYM ŚWIECIE

Kontrola dostępu i dane wideo, dzięki którym Twoje budynki staną się bardziej inteligentne

90+

TYSIĄCE WDROŻEŃ

Możliwości integracji, aby połączyć istniejące inwestycje technologiczne

450Mkw

NIERUCHOMOŚCI W ZARZĄDZANIU

brivo

866.692.7486 | brivo.com

Brivo oferuje kompleksowy zestaw narzędzi dostosowanych do Twoich potrzeb w zakresie kontroli dostępu. Dowiedz się więcej na

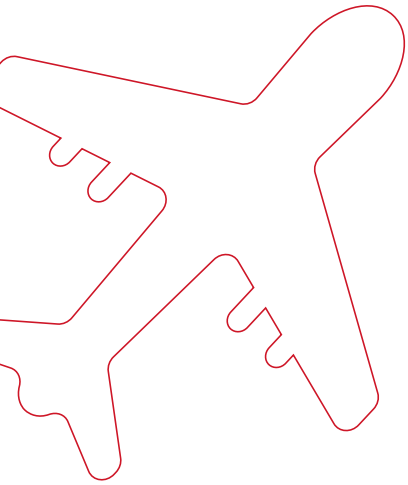
www.brivo.com/solutions/commercial-real-estate/

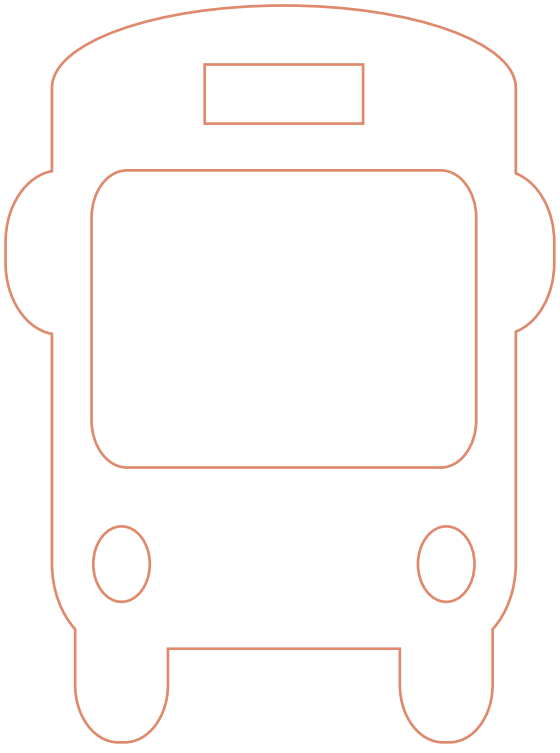
PARTNER:

smart-i | Ul. Marii Rodziewiczówny 1/810, 04-187 Warszawa | www.smart-i.pl

głos branży

Eksperci sektora transportowo-logistycznego ocenili rok 2023 jako trudny, niewiele lepiej zapowiada się rok 2024. Jednak stan transportu w Polsce to nie tylko wskaźniki finansowe, ale też bezpieczeństwo ludzi i towarów. O tym, jak firmy radzą sobie z coraz trudniejszymi wyzwaniami, mówią przedstawiciele branży.





Jacek Tyburek
DHL

Niezbędna jest weryfikacja

Ostatnio w mediach społecznościowych rozgorzała dyskusja na temat doskonale zorganizowanej kradzieży cargo. Firma transportowa od wielu miesięcy pracowała w zasadzie bez zarzutu. Zawsze chętna do pracy, zawsze na czas i co najważniejsze, w bardzo przystępnych cenach. Nagle pewnego dnia powierzony towar, w tym przypadku komponenty do fotowoltaiki, po załadowaniu w porcie w Rotterdamie zniknął w drodze na Śląsk. Okazało się, że w tym czasie takich zniknięć było znacznie więcej. W sumie wartość strat oszacowano na kilkanaście milionów złotych. Jak im to się udało? Poszkodowani spedytorzy zgodnie twierdzą, że pracowali z firmą od dłuższego czasu, wszystkie dokumenty (NIP, Regon, KRS, licencje transportowe) były w porządku.

Dopiero śledztwo dziennikarskie wykazało, że spółka transportowa w międzyczasie zmieniała właścicieli, a nowi zniknęli, pozostawiając niezapłacone rachunki za wynajem biura, schowanego gdzieś na Podhalu w budynku przylegającym do hurtowni metalowej. Firma Złodziej w jednym tygodniu „trafiła" ponad 50 firm spedycyjnych z całego kraju na łączną kwotę kilkunastu milionów złotych.

W tym konkretnym przypadku nie znamy wszystkich szczegółów, ale detale w materiale prasowym wskazują, że firma wystawiała się na giełdzie transportowej, a tam miała dobre opinie. Nagłe zaginięcia towaru, brak kontaktu z kierowcami i właścicielami pokazuje jednak, że przed zleceniem transportu należy przeprowadzić rzetelną weryfikację, z dbałością o detale. Dla małych firm, które pracują w potwornym stresie i reżimie czasowym, przeprowadzenie pełnego sprawdzenia jest prawie niemożliwe. Dlatego proces wchodzenia w nowe relacje z przewoźnikami, szczególnie nowymi, jest prawdziwym wyzwaniem. Budowanie własnych baz danych przewoźników, stały z nimi kontakt, wizyty w siedzibach firm, przeprowadzanie audytów bezpieczeństwa to są warunki brzegowe. Bardzo pracochłonne i czasochłonne, czasami wymagające niemałego budżetu, ale owocujące minimalizacją ryzyka utraty ładunku. Bo te, szczególnie w przypadku High Value, liczone są w milionach. Świadoma i konsekwentna polityka zarządzania relacjami z przewoźnikami musi być nasycona elementami security. Stosowanie narzędzi kontrolnych, uzupełnianie wiedzy o przewoźniku, jego kierowcach, budowanie wzajemnego zrozumienia i zaufania, z jednoczesnym nieustępliwym kontrolowaniem jest jedynym skutecznym podejściem.

Dlatego też z jednej strony firmy logistyczne muszą nieustannie pracować nad bazami przewoźników i ich weryfikacją. Z drugiej – klienci zlecający transporty dla własnego dobra, przede wszystkim dla utrzymania ciągłości działania, powinny wnikliwie badać, jak ich logistyczny partner ogranicza ryzyka związane z przewozem towaru.

TAPA od pewnego czasu alarmuje o rosnącym zjawisku kradzieży cargo w całym regionie EMEA. Przestępcy stosują coraz bardziej wysublimowane metody. Do tego dochodzą sytuacja rynkowa i zbliżająca się fala upadków małych firm transportowych. Na rynku zaroi się od podmiotów lub pozostałościach po podmiotach transportowych gotowych kontynuować działalność z nowym właścicielem. To bardzo niebezpieczny moment, Carrier Managerowie i Security Managerowie będą mieli co robić.

Paweł Pechorzewski
ZALANDO

Stare i nowe wyzwania

Rok 2024 w sektorze transportu i logistyki zapowiada się jako kontynuacja dotychczasowych wyzwań. To branża, dla której krajobraz zagrożeń dość mocno ewoluował w ostatnich latach, i zdaje się, że zmiany będą dotyczyć głównie prawdopodobieństwa bądź możliwych skutków poszczególnych zagrożeń.

Przykładem takiego dobrze znanego ryzyka, którego nie można pominąć w budowaniu planów na ten rok, jest działalność zorganizowanych grup przestępczych w tych miejscach, gdzie transportowany i przechowywany jest towar. Analizując dostępne statystyki (m.in. dane udostępniane przez TAPA), można zaobserwować, że przestępcy stają się nie tylko bardziej zuchwali, ale również coraz mniej wybredni, jeśli chodzi o kategorie kradzionych produktów. W związku z tym szerokie grono przedsiębiorstw aktywnych we wszystkich ogniwach łańcucha dostaw jest zmuszone do refleksji nad skutecznymi strategiami zapobiegania różnym incydentom, ich wykrywania i zwalczania.

Podstawowe elementy systemów bezpieczeństwa, takie jak odpowiednie procedury, ochrona fizyczna, zabezpieczenia mechaniczne i elektroniczne, okazują się w dzisiejszych czasach jedynie fundamentem, a nie rozwiązaniem kompleksowym pozwalającym stawić czoła coraz bardziej wyspecjalizowanej i skutecznej przestępczości zorganizowanej. W sektorze TSL wciąż istnieje duży potencjał do doskonalenia oraz przestrzeń dla inwestycji, szczególnie w rozwiązania zapewniające bezpieczeństwo przewożonego towaru i przede wszystkim osób realizujących takie transporty.

Ponieważ do znaczącego odsetka włamań do naczep i pojazdów dochodzi na niestrzeżonych i niewyposażonych we właściwą infrastrukturę parkingach, a liczba tych bezpiecznych, spełniających międzynarodowe standardy (np. TAPA PSR lub SSTPA) jest wciąż niewystarczająca, zarządzający bezpieczeństwem aktywnie poszukują rozwiązań chroniących przed takim scenariuszem.

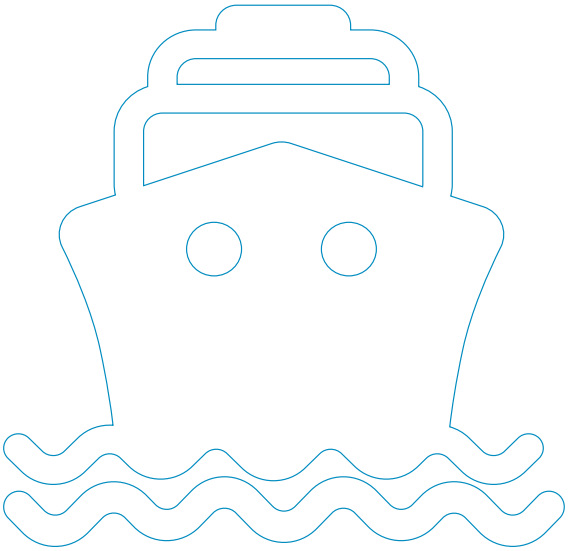
Usługi wspierające proces zarządzania ryzykiem poprzez dostarczanie aktualnych informacji umożliwiających optymalne zaplanowanie trasy i uniknięcie gorących punktów, telematyka, monitoring ładunków w czasie rzeczywistym z opcją interwencji, systemy zamknięć czy wreszcie szkolenia to dziedziny, w które inwestycje zwiększą bezpieczeństwo oraz pozwolą na osiągnięcie większej efektywności operacyjnej.

Andrzej Żochowski
NIEZALEŻNY EKSPERT
DS. BEZPIECZEŃSTWA

Czynniki wpływające na bezpieczeństwo

W minionym roku w branży logistyki dało się zauważać zagrożenia dobrze znane zarządzającym bezpieczeństwem logistyki. Liczne były tzw. kradzieże magazynowe, najczęściej dokonywane przez tzw. pracowników czasowych (elektronika użytkowa – telefony, tablety, nośniki pamięci itp.), próby przemytu papierosów, narkotyków i wszelkiego rodzaju dopalaczy, najczęściej z Polski do krajów Europy Zachodniej oraz Wielkiej Brytanii i USA. Mnożyły się próby wyłudzania niewielkich opłat za np. niedoręczoną przesyłkę przez firmę kurierską czy dostawę przez operatora logistycznego za pomocą SMS o treści typu „Twoja przesyłka jest już gotowa do doręczenia, jednak wymaga dopłaty 16 zł tytułem opłaty celnej" itp. Odnotowano też, na szczęście nieudane,

→



próby ataków hakerskich na sieci informatyczne firm łańcucha dostaw w celu jego zaburzenia lub jak najdłuższego przerwania. Obserwuje się wzrost przestępstw „internetowych" najczęściej w odniesieniu do dużych operatorów telefonii komórkowej w Polsce. Oszust zdalnie zamawiał u operatora nowy telefon komórkowy, posługując się najczęściej skanami fałszywych dokumentów tożsamości, przygotowanymi na podstawie skradzionych wcześniej danych osobowych.

Ponadto w drugiej połowie 2023 r. powoli zaczął się odbudowywać i funkcjonować cywilny „łańcuch dostaw" pomiędzy Ukrainą a Europą i USA. W zasadzie w 100% oparty na transporcie drogowym z Ukrainy do Polski, a dalej lotniczym lub drogowym z wykorzystaniem międzynarodowych firm kurierskich oraz logistycznych. W tym obszarze dało się zauważyć próby przesyłania z Ukrainy do Europy i poza nią tzw. towarów, materiałów zabronionych w transporcie lotniczym oraz drogowym, wobec których wymagane są zgodnie z przepisami celnymi lub tzw. kontrolą eksportu specjalne pozwolenia lub dedykowany transport lotniczy lub drogowy. W przesyłkach stwierdzano m.in. magazynki na amunicję do broni maszynowej, nieuzbrojone granaty moździerzowe oraz łuski z amunicji artyleryjskiej i karabinowej lub nie w pełni zniszczone podczas wybuchu granaty moździerzowe – artystycznie pomalowane jako ozdoby do mieszkania czy prezenty.

Zważywszy na powyższe zagrożenia zaobserwowane w ubiegłym roku, należy spodziewać się, iż w 2024 r. zagrożenia te będą dalej występować. Należy także zakładać, że z uwagi na łatwość popełniania przestępstw przez oszustów „internetowych" i tzw. niższą kwalifikację tych przestępstw oraz ciągły rozwój narzędzi – usług zdalnych – ta kategoria z kolei będzie stopniowo wzrastać i narażać sektor logistyki na zwiększone ryzyka „roszczenia" z tytułu reklamacji w odniesieniu do operatorów logistycznych i firm kurierskich.

Z jednej strony powinniśmy brać pod uwagę przeciągający się konflikt militarny w Ukrainie i ponawiane próby ataków hakerskich, których celem nieustannie będzie przerwanie łańcucha dostaw zaopatrujących Ukrainę w sprzęt i uzbrojenie. Z drugiej – cały czas obserwujemy wspomnianą wcześniej odbudowę cywilnego łańcucha dostaw z Ukrainy do Europy i innych krajów. Proces ten także będzie obarczony ryzykiem wzrostu liczby przesyłek z towarami i materiałami zabronionymi. To może zwiększać ryzyko operacji transportowych drogowych i lotniczych, a także narażać reputację firm logistycznych na utratę wizerunku oraz kary finansowe z tytułu naruszenia przepisów m.in. celnych, skarbowych oraz tzw. kontroli obrotu (towary podwójnego zastosowania, uzbrojenie).

Należy także podkreślić, że oprócz wymienionych czynników wpływających na bezpieczeństwo firmy logistycznej, a tym samym procesy bezpieczeństwa tych organizacji biznesowo będzie obciążać postępujący wzrost kosztów głównie ochrony fizycznej, która już od kilku lat z uwagi na podnoszenie tzw. minimalnych stawek wynagrodzeń staje się coraz bardziej usługą „ekskluzywną" w sektorze logistyki. Tym samym należy zakładać, iż usługa ta będzie w większym stopniu zastępowana elektronicznymi systemami zabezpieczeń (CCTV z elementami analizy obrazu, zaawansowane systemy kontroli dostępu z biometrią) czy kompleksową ochroną obiektów logistycznych sprawowanych – zdalnie – z Centrum Monitorowania Alarmów firm ochrony, które, tam gdzie będzie to możliwe, korzystają ze zdalnego monitorowania systemów zabezpieczeń w 100% bez udziału pracowników ochrony w obiekcie. Takie rozwiązania pozwolą sukcesywnie obniżać wysokie koszty ochrony fizycznej przy jednoczesnym zapewnieniu akceptowalnego poziomu bezpieczeństwa centrów logistycznych.

Piotr Rusin
AUTOSTRADA EKSPLOATACJA

Wsparcie systemów zabezpieczeń technicznych

Bezpieczeństwo w transporcie i logistyce jest kluczowe dla funkcjonowania gospodarki i społeczeństwa. Jednak bezpieczeństwo to nie tylko kwestia bezpiecznych dróg i autostrad, ale także odpowiedniego zabezpieczenia firm utrzymujących infrastrukturę drogową.

W najbliższej przyszłości jednym z największych wyzwań w obszarze ochrony fizycznej będzie dostępność zasobów ludzkich. Niski poziom bezrobocia i rosnące wymagania związane z obsługą systemów ochrony znacząco utrudniają znalezienie pracowników. Jednocześnie skomplikowana sytuacja geopolityczna sprawia, że bezpieczeństwo infrastruktury krytycznej i firm, które za nią odpowiadają, staje się kwestią wykraczającą poza sferę biznesu, mając kluczowe znaczenie dla państwa i społeczeństwa. W tej sytuacji z pomocą przyjdzie szerokie zastosowanie nowoczesnych rozwiązań technicznych wspierających pracowników ochrony w ich codziennej pracy.

Jednym z elementów zabezpieczeń, który warto wdrażać, jest zintegrowany system bezpieczeństwa i automatyki, który pozwala na sterowanie i nadzór nad różnymi urządzeniami, takimi jak kamery, czujniki, czytniki kontroli dostępu, windy itp. Zintegrowany system bezpieczeństwa i automatyki umożliwia pracownikom ochrony łatwiejsze i szybsze reagowanie na sytuacje awaryjne i kryzysowe.

Niezbędnymi systemami, które gwarantują odpowiedni poziom bezpieczeństwa, są systemy telewizji dozorowej, kontroli dostępu, sygnalizacji włamania i napadu, wydawania kluczy służące do ograniczania i monitorowania dostępu do chronionych obiektów i urządzeń, takich jak budynki, magazyny, pojazdy, maszyny itp. Systemy te zwiększają również bezpieczeństwo i ochronę wartościowych zasobów, takich jak wyposażenie, towar, dokumenty, dane itp. Wspierają pracowników ochrony, ponieważ ułatwiają im zarządzanie dostępem do obiektów i urządzeń, alarmują i powiadamiają w razie zagrożenia.

Warto zwrócić uwagę na ochronę obwodową, która zabezpiecza granicę chronionej posesji przed nieuprawnionym dostępem. System ten powinien być połączony z innymi systemami zabezpieczeń, takimi jak monitoring wizyjny, system alarmowy, system kontroli dostępu itp. Ochrona obwodowa ogrodzeń zapewnia szybką i skuteczną reakcję na intruzów, zanim dotrą oni do wejścia do obiektu.

Podsumowując, wszystkie wymienione systemy zabezpieczeń są niezbędne dla zapewnienia odpowiedniego poziomu bezpieczeństwa firm. Systemy te wspierają pracowników ochrony, ponieważ ułatwiają im wykonywanie zadań, zwiększają ich skuteczność i bezpieczeństwo, a także skracają czas reakcji na zagrożenia. Systemy te przyczyniają się również do rozwoju sektora transportu drogowego, który staje się coraz bardziej nowoczesny, efektywny i bezpieczny. Aby w pełni wykorzystać potencjał systemów zabezpieczeń, należy jednak zadbać o ich odpowiedni dobór, instalację, konserwację i obsługę, a także o szkolenie i doskonalenie pracowników w zakresie ich obsługi i wykorzystania. Inwestycja zarówno w rozwiązania technologiczne, jak i kompetencje ludzi z nich korzystających będzie niezbędnym krokiem w 2024 r.

Marcin Walczuk
BCS

Nowoczesna technologia w transporcie

Bezpieczny transport to taki, który minimalizuje ryzyko wypadków, zanieczyszczeń i strat ekonomicznych. Aby zapewnić maksymalny poziom bezpieczeństwa, niezbędne są odpowiednie środki prawne, organizacyjne i techniczne. Wśród nich coraz większą rolę odgrywają rozwiązania BCS wykorzystujące nowoczesne technologie, takie jak sztuczna inteligencja (AI), autonomiczne pojazdy czy elektryfikacja floty.

Sztuczna inteligencja może być wykorzystywana w transporcie do wielu celów, takich jak optymalizacja tras i zarządzanie ruchem drogowym, monitorowanie stanu technicznego pojazdów i infrastruktury, wspieranie bezpieczeństwa kierowców i pasażerów czy automatyzacja procesów transportowych. Technologia SI sprawia, że transport jest bardziej efektywny, ekologiczny i bezpieczny.

Pojazdy autonomiczne potrafiące poruszać się bez ingerencji człowieka, wykorzystując do tego różne czujniki, kamery, radary, mapy i algorytmy, mogą przyczyniać się do poprawy bezpieczeństwa transportu. Ich użycie eliminuje błędy ludzkie, zwiększa wydajność transportu, zmniejszając tym samym jego koszty. Oferują przy tym nowe możliwości, przez co transport może być bardziej komfortowy, elastyczny i innowacyjny.

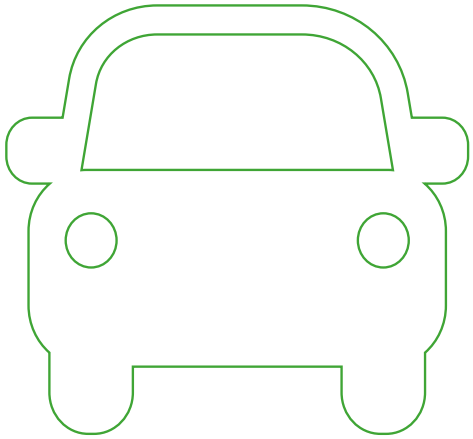
Z kolei elektryfikacja floty to proces zastępowania pojazdów napędzanych paliwami kopalnymi pojazdami napędzanymi energią elektryczną. Ma to korzystny wpływ, ponieważ redukuje emisję gazów cieplarnianych i zanieczyszczeń powietrza, obniża poziom hałasu, zmniejsza zależność od importu ropy naftowej i stymuluje rozwój innowacyjnych technologii.

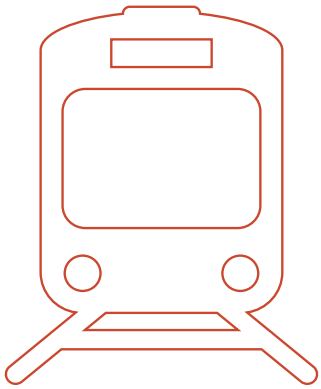
Podsumowując, nowoczesne technologie są nie tylko ciekawym zjawiskiem, ale także niezbędnym narzędziem do zapewnienia rozwoju transportu. A to przekłada się na poprawę w każdym względzie, co podnosi jakość życia i wpływa na rozwój gospodarki.

Bartłomiej Skórski
HIKVISION POLAND

Rozwiązania podnoszące bezpieczeństwo

Branża transportu jest dziś otwarta na stosowanie nowoczesnych technologii, a rozwiązania systemów zabezpieczeń mogą dostarczać skuteczne narzędzia do poprawy bezpieczeństwa, monitorowania i zarządzania w tym sektorze rynku. Aby zapewnić odpowiedni





poziom bezpieczeństwa polecamy zastosowanie następujących rozwiązań:

Kamery monitoringu HD i PTZ. Zapewniają wysoką jakość obrazu i elastyczność monitorowania obszarów transportu. Kamery PTZ umożliwiają zdalne dostosowywanie kierunku i przybliżenia, co jest przydatne w dynamicznych środowiskach transportowych.

Kamery termowizyjne. W warunkach nocnych lub trudnych warunkach atmosferycznych kamery termowizyjne Hikvision mogą dostarczyć informacji o źródłach ciepła, co jest istotne dla bezpieczeństwa i monitorowania, np. ładujących się magazynowych wózków widłowych czy monitorowania temperatury przewożonych ładunków.

Systemy śledzenia i zarządzania flotą. Hikvision oferuje zaawansowane systemy, które integrują kamery z systemami GPS, umożliwiając pełną kontrolę nad trasami, bezpieczeństwem i efektywnością floty.

Inteligentne oprogramowanie analizy obrazu. Dzięki analizie AI obrazu można identyfikować potencjalne zagrożenia, takie jak intruzi czy awarie, co pozwala na szybką reakcję i zwiększa poziom bezpieczeństwa.

Dobrym rozwiązaniem podnoszącym bezpieczeństwo w transporcie i logistyce jest integracja systemów monitoringu wizyjnego z systemami zarządzania flotą. Pozwala to na uzyskanie kompleksowej wizji operacji transportowych. W ten sposób menedżerowie ds. bezpieczeństwa mogą efektywnie monitorować, analizować i reagować na sytuacje awaryjne, zwiększając zarówno bezpieczeństwo, jak i efektywność logistyczną.

Jarosław Sapko
AXIS COMMUNICATIONS

Kamery dozorowe nie tylko do monitorowania

Monitoring wizyjny w transporcie i logistyce nie skupia się wyłącznie na obrazie dostarczanym z kamer. Coraz częściej systemy dozorowe są źródłami danych na temat natężenia ruchu na określonej trasie, mogą dotyczyć np. wyboru danej drogi, prędkości w danym miejscu czy średniej prędkości na danym odcinku.

Dzięki wbudowanym algorytmom analitycznym kamery umożliwiają nie tylko detekcję jazdy pod prąd, ale też zbierają różne dane analityczne. Mogą dotyczyć np. liczby samochodów wybierających dany pas czy dany kierunek na skrzyżowaniu, natężenia ruchu o danych porach dnia lub informacje na temat regionu czy kraju pochodzenia pojazdów poruszających się w danym obszarze.

Kamery z oprogramowaniem do rozpoznawania tablic rejestracyjnych mogą służyć już nie tylko do detekcji, czy dany pojazd znajduje się w określonej strefie lub mieście. Dzięki metadanym i możliwości łączenia różnych informacji obraz z kamery może zawierać dodatkowe informacje. Dzięki nim możliwa jest integracja z radarem, co pozwala na pomiar prędkości pojazdu. Połączenie z urządzeniem ważącym i naniesienie na obraz informacji o wadze pojazdu podczas wjazdu i wyjazdu pozwala na usprawnienie procesu rozliczania załadunku ciężarówek. Integracja kamery z termometrem umożliwia kontrolowanie temperatury w pojazdach typu chłodnia i zapobieganie ich rozmrożeniu. Natomiast najbardziej oczywiste połączenie informacji z nadajnika GPS z kamerą pozwoli określić położenie pojazdu w momencie danego zdarzenia.

Artur Nowakowski
LINC POLSKA

Ochrona centrów logistycznych z wykorzystaniem sztucznej inteligencji

W dzisiejszym dynamicznym świecie biznesu, gdzie szybkość dostaw i sprawność logistyczna są kluczowym warunkiem sukcesu, ochrona centrów logistycznych oraz łańcucha dostaw staje się niezmiernie istotnym elementem strategii biznesowej. Jest nie tylko kwestią bezpieczeństwa fizycznego, ale również zagadnieniem związanym z ochroną danych, technologii oraz całego systemu logistycznego. Dane udostępnione przez organizację TAPA EMEA nie pozostawiają złudzeń – liczba kradzieży z roku na rok rośnie i nic nie wskazuje na to, żeby ta tendencja miała się zmienić. Niedawno w programie „Interwencja" został przedstawiony przykład przedsiębiorstwa z Podhala, które najprawdopodobniej rozpłynęło się wraz z towarem wartym setki tysięcy złotych. Takich sytuacji będzie coraz więcej, dlatego przed branżą logistyczną stoi nie lada wyzwanie, jakim jest ochrona dóbr klientów w kolejnych punktach łańcucha dostaw.

Elektroniczne systemy alarmowe oraz monitoring wizyjny, będące uzupełnieniem szeroko rozumianej ochrony fizycznej, stanowią istotny element w zabezpieczeniu centrów logistycznych. Dostarczają informacji o bieżących wydarzeniach, ale również

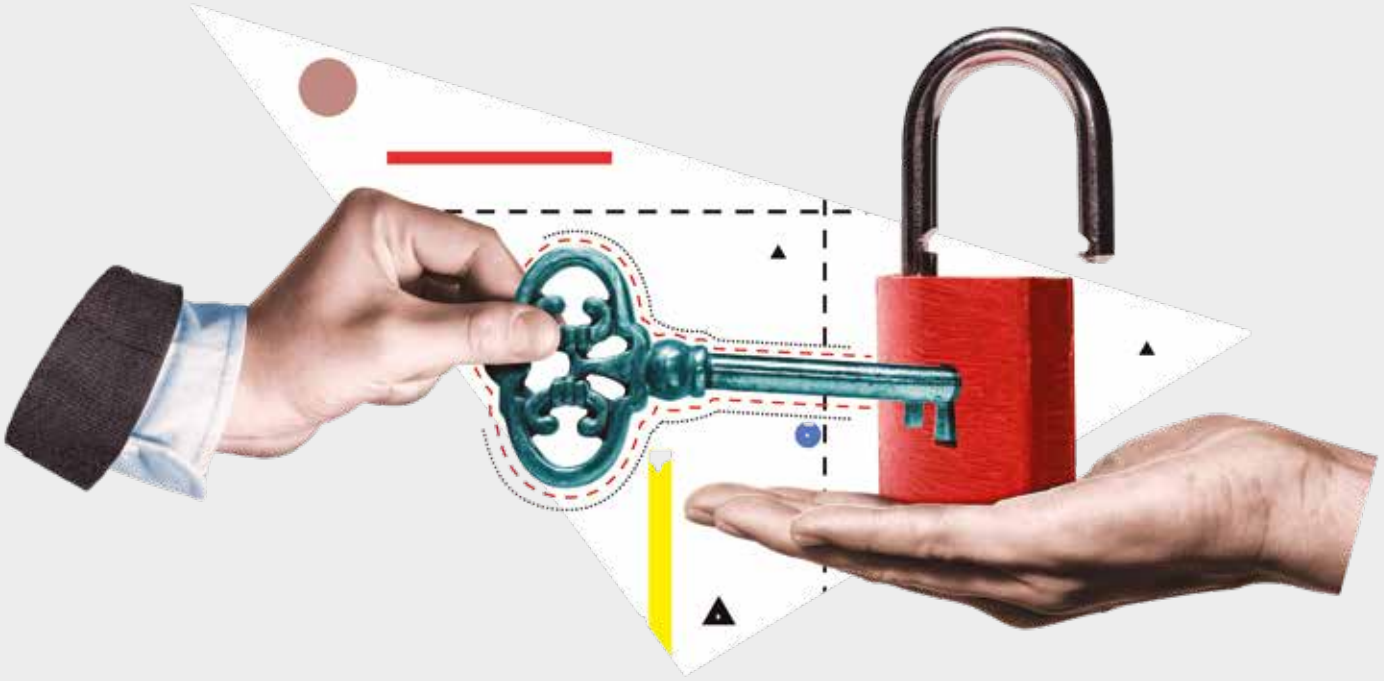
pełnią funkcję prewencyjną, przyczyniając się do zwiększenia bezpieczeństwa i efektywności operacyjnej. Są one częścią ekosystemu IT, obok innych systemów informatycznych odpowiedzialnych za zarządzanie operacjami czy śledzenie przesyłek, dlatego należy zwrócić uwagę na to, żeby systemy te same w sobie były również bezpieczne, spełniały wymogi stawiane w NIS2 oraz były wygodne dla użytkowników. Przykładem takiego systemu jest na pewno najnowsza seria 35 kamer i rejestratorów sieciowych firmy Honeywell, która nie tylko spełnia wszystkie funkcjonalne potrzeby monitoringu wideo wspieranego sztuczną inteligencją, ale również odpowiada wymogom NIS2 dotyczącym cyberbezpieczeństwa.

Kolejnym elementem ochrony centrów logistycznych są zabezpieczenia strefy perymetrycznej. Zastosowanie kamer do monitorowania tych terenów jest powszechne, natomiast są one używane bardziej do weryfikacji zdarzenia po fakcie niż realnej ochrony i zapobiegania incydentom. Dlatego istotne jest, aby maksymalnie wykorzystać możliwości, które oferuje sztuczna inteligencja. Te same kamery, wyposażone np. w Hub Camect, dają informację o wtargnięciu intruza na chroniony teren w czasie rzeczywistym, dzięki czemu ochrona może podjąć natychmiastowe działania. System ten nie generuje fałszywych alarmów wywoływanych przez trawy, drzewa czy nawet zwierzęta, jak to ma miejsce w typowych systemach CCTV. Jeżeli chcemy pójść jeszcze dalej, możemy wykorzystać systemy napłotowe wspierane sztuczną inteligencją do wykrywania intruzów, którzy dopiero próbują przedostać się przez ogrodzenie. Ochrona zostaje zaalarmowana szybciej – już podczas próby przedostania się intruza otrzymuje informacje, dzięki czemu ma więcej czasu na reakcję, a w takim przypadku każda minuta może okazać się kluczowa.

Przenosząc temat ochrony z obszaru perymetrycznego na rozległe tereny o dużej powierzchni, mamy do dyspozycji systemy radarowe, które uzupełnione o algorytmy AI po wykryciu intruza wykorzystują kamerę do potwierdzenia, czy wykryty obiekt jest faktycznie człowiekiem, a nie np. zwierzęciem.

Skuteczna ochrona centrów logistycznych wymaga kompleksowego podejścia, które łączy bezpieczeństwo fizyczne, perymetryczne i cybernetyczne. Wprowadzenie nowoczesnych technologii, w tym sztucznej inteligencji, pozwala znacząco podnieść poziom bezpieczeństwa, a tym samym zwiększyć skuteczność reakcji na wszelkie zagrożenia. ●

Jaki będzie rok 2024 dla polskiej branży security?



Zdaniem wielu ekonomistów gospodarka powoli wychodzi z okresu spowolnienia, co pozwala na optymistyczne prognozy na najbliższe miesiące. Czy sprawdzą się też na polskim rynku security? Zapytaliśmy o to przedstawicieli największych firm branżowych. Głosów ekspertów wysłuchała Iwona Krawiec, a&s Polska.

W tym roku Komisja Europejska prognozuje dla Polski wzrost gospodarczy z PKB na poziomie 2,7%. Na poprawę kondycji polskich firm mają wpłynąć m.in. zwiększona konsumpcja oraz odblokowanie środków unijnych z KPO. To z kolei może się przełożyć na wzrost w wybranych sektorach.

Od czego zależy wzrost wartości rynku?

Wśród czynników wspierających rozwój rynku eksperci wymieniają m.in. zainteresowanie gospodarek europejskich polskim rynkiem produkcyjnym. Reshoring, czyli proces powrotu produkcji i logistyki do Europy, daje się zauważyć już od pewnego czasu.

– *Atrakcyjny rynek pracy i duży rynek wewnętrzny sprawiają, że sporo powracających inwestycji pojawia się właśnie w Polsce. Każda nowa inwestycja oznacza kolejne zamówienia dla sektora security, co bez wątpienia będzie motorem napędowym branży przez następne lata* – zauważa Tomasz Kaliński, wiceprezes Alnet Systems.

Do rozwoju rynku security z pewnością przyczyni się coraz większe zastosowanie urządzeń wyposażonych w najnowsze rozwiązania techniczne. – *Perspektywy na 2024 r. wyglądają obiecująco dla całej branży security, ale też IT. Świadomość korzyści wynikających z zastosowania nowoczesnych technologii, zarówno wśród klientów prywatnych, jak i przedsiębiorstw, będą szansą na tegoroczny rozwój* – stwierdził Robert Gawroński, SMB Channel Manager, TP-Link Polska.

Dynamiczny wzrost w sektorze systemów zabezpieczeń w Polsce przewiduje też Wojciech Weissenberg, CTO, squareTec. Zwraca uwagę na coraz większe zapotrzebowanie na rozwiązania nieszablonowe. – *Rok 2024 przyniesie zapewne większy nacisk na integrację technologii i bezpieczeństwo danych. Już dzisiaj prowadzone przez nas projekty koncentrują się na efektywnym wykorzystaniu sztucznej inteligencji, kluczowym aspekcie budowanych przez nas rozwiązań opartych na wiedzy* – wskazuje Wojciech Weissenberg.

Czynnikiem napędzającym branżę z pewnością będzie też zwiększone zainteresowanie cyberbezpieczeństwem. W rosnących nakładach na systemy chroniące przed cyberatakami szansę rozwoju widzi Jarosław Grzybowski, Channel Sales Director, Hikvision Poland. – *Szans na pewno należy upatrywać w rosnącej świadomości użytkowników w kwestiach ochrony danych. Spodziewamy się szybko rosnącej liczby cyberataków, w tym również na elektroniczne systemy zabezpieczeń, co zmusi producentów do nieustannego dostosowywania się do nowych wyzwań. Niezbędne staną się nowe regulacje dotyczące ochrony danych, które będą dużym wyzwaniem dla całej branży security* – dodaje Jarosław Grzybowski.

Gotowość klientów w wielu sektorach rynku do redefiniowania i ujednolicania standardów bezpieczeństwa ze względu na stale rosnące ryzyko cyberprzestępczości zauważa też Dagmara Pomirska, szefowa sprzedaży na Polskę, Ukrainę i Kraje Bałtyckie w Axis Communications. – *Ten rok minie pod znakiem dalszych inwestycji w obszarze automatyzacji pracy, zwłaszcza w firmach produkcyjnych, ponieważ koszty ochrony fizycznej stale rosną* – wyjaśnia.

Rynek zabezpieczeń technicznych ulega dynamicznej transformacji. Wybuch wojny w Ukrainie przyśpieszył proces modyfikacji starych systemów zabezpieczeń technicznych budowanych przez lata, zarówno w obiektach publicznych, jak i wielu przedsiębiorstwach prywatnych. Znaczna część tych systemów jest nie tylko modernizowana, ale też integrowana z innymi rozwiązaniami.

W roku 2023 firmy wprowadzały wiele rozwiązań wykorzystujących najnowsze technologie. Jakimi produktami byli zainteresowani klienci w Polsce? Jaką ofertę przygotowały firmy w tym roku?

Tomasz Kaliński, Alnet Systems

W tym roku postaramy się zaoferować klientom nowe moduły analizy obrazu oraz więcej dedykowanych rozwiązań dla stacji benzynowych, handlu detalicznego i ośrodków logistycznych. Ponadto będziemy kontynuowali pracę nad integracją naszego systemu VMS NetStation z innymi systemami budynkowymi, takimi jak windy, systemy klimatyzacji czy zarzadzania energią.

Dagmara Pomirska, Axis Communications

Klienci poszukują produktów z funkcjami analityki typu DLPU. Skalowalne rozwiązania Axis pomagają automatyzować dozór, zapewniając jednocześnie maksymalną wydajność. AXIS Camera Application Platform, otwarta platforma wspierająca większość produktów Axis, umożliwia naszym partnerom opracowywanie inteligentnych, skalowalnych aplikacji analitycznych. Do wyboru są liczne scenariusze, np. detekcja przekroczenia linii, obiekt w obszarze, zajętość obszarów, nowa analiza czasu przebywania w obszarze itp. Razem z szeroką gamą funkcji bezpieczeństwa, ochrony i efektywności operacyjnej otwiera to nieograniczone możliwości dla klientów z wielu sektorów.

Kamil Kierzkowski, Hanwha Vision Europe

Znacząca większość ostatnio realizowanych projektów miała wspólny mianownik: cyberbezpieczeństwo i analiza wideo SI. Koszty utrzymania wykwalifikowanego operatora systemu VSS stają się wyzwaniem, co skłania firmy do poszukiwania systemów, które mogą wysyłać powiadomienia o zdarzeniach, jednocześnie nie wymagając ciągłej obsługi i długotrwałego monitorowania. Wspólnie z naszymi partnerami rozwijamy coraz bardziej zaawansowane rozwiązania umożliwiające analizę gromadzonych danych i automatyczne wyzwalanie konkretnych działań. To kolejny krok w kierunku dostarczania inteligentnych, efektywnych i samodzielnych systemów dla naszych klientów.

→

> *W miarę postępu technicznego rośnie świadomość zagrożeń, co powoduje, że firmy, instytucje, a także inwestorzy prywatni będą nadal inwestować w nowoczesne rozwiązania zabezpieczeń.*

– To wielka szansa dla nas, jako pioniera rozwiązań PSIM, a co najważniejsze w 100% polskiego podmiotu, który aktywnie inwestuje w bezpieczeństwo i rozwój. Możliwości ekspansji upatrujemy w dalszym przyśpieszeniu procesów ochrony krytycznych aktywów naszego kraju, jak również w stale rozwijającej się świadomości potrzeb bezpieczeństwa użytkowników. W kwestii zagrożeń widziałbym tutaj proces zahamowania globalnego poziomu inwestycji w kraju i osłabienia dynamiki wzrostu PKB. Takie czynniki zawsze wyhamowują inwestycje w bezpieczeństwo – twierdzi Kamil Barański, członek Zarządu ds. Business Development, Megavision Technology.

Zmiany geopolityczne i pojawiające się kolejne regulacje wymuszają wprowadzenie nowych standardów, aby dostosować się do zmieniających się potrzeb klientów.

– Użytkownicy systemów dozoru wizyjnego dokładniej analizują dostępne opcje pod kątem spełniania standardów bezpieczeństwa. Coraz częściej kryterium wyboru jest nie tylko cena, ale również dłuższy okres gwarancji, u nas standardowo jest 5 lat, certyfikacja UL CAP oraz FIPS-140-2 czy certyfikaty potwierdzające spełnianie norm jakościowych. Nasze rozwiązania zawsze cechowały się najwyższą jakością, więc obecne zmiany na rynku traktujemy jako szansę na dalszy rozwój – podkreśla Kamil Kierzkowski, Country Manager Poland & Baltics, Hanwha Vision Europe.

Trzy czynniki wpływające na rozwój rynku security w Polsce zauważa Harald Dingemans, dyrektor zarządzający Linc Polska.

– Pierwszym czynnikiem jest wzrost płacy minimalnej, która powoduje wzrost stawki za ochronę fizyczną. Dlatego klienci wycofują się z usług ochrony fizycznej na rzecz systemów zabezpieczeń elektronicznych. Zastępowanie osób techniką to trend, który widzimy już od kilku lat. Drugim czynnikiem jest wojna w Ukrainie. Ponieważ Polska jest granicą NATO, musi inwestować w najnowsze rozwiązania zapewniające najwyższy stopień bezpieczeństwa. Ochrona obiektów infrastruktury krytycznej i obiektów o znaczeniu militarnym zwiększa zainteresowanie najnowocześniejszymi systemami zabezpieczeń i jest szansą dla naszej branży. Trzecim czynnikiem jest niestabilna sytuacja gospodarcza, która wpływa na pogorszenie sytuacji finansowej wielu Polaków. Obserwujemy coraz większą liczbę kradzieży w sklepach, a to wymusza zwiększone inwestycje w systemy zabezpieczeń – wskazuje Harald Dingemans.

W miarę postępu technicznego rośnie świadomość różnych zagrożeń, co powoduje, że firmy, instytucje, a także inwestorzy prywatni będą nadal inwestować w nowoczesne rozwiązania zabezpieczeń, w tym w systemy sygnalizacji pożarowej.

– Zdajemy sobie sprawę, że w obliczu coraz większych zagrożeń, także wojny w Ukrainie, współpraca między różnymi sektorami gospodarki, w tym publicznym i prywatnym, powinna stać się w 2024 r. jeszcze bardziej istotnym elementem skutecznego zarządzania szeroko pojętym bezpieczeństwem – komentuje Robert Pestka, dyrektor wsparcia sprzedaży, POLON-ALFA.

Pandemia przyczyniła się do wzrostu zainteresowania bezdotykowymi systemami kontroli dostępu. To kierunek zauważalny również na rynku polskim. Jakie prognozy przewidują eksperci dla tego sektora?

– W naszej ocenie w 2024 r. rynek kontroli dostępu nadal będzie się rozwijał, szacujemy wzrost na poziomie 10–15%. Czynnikami, które niewątpliwie będą wpływać na wzrost zainteresowania systemami zabezpieczeń, będzie wejście w życie dyrektywy NIS 2 oraz niepewna sytuacja geopolityczna – uważa Łukasz Kanarek, dyrektor sprzedaży krajowej i obsługi klienta, Roger.

– W tym roku spodziewamy się wzrostu popytu na rozwiązania z zakresu cyberbezpieczeństwa, zwłaszcza w sektorze infrastruktury krytycznej. Dodatkową perspektywą rozwoju jest wykorzystanie smartfonów zamiast standardowych kart. A możliwość zastosowania Apple Wallet już na zawsze zmieni sposób używania tego medium. Wśród klientów z sektora prywatnego, którzy mają wiele oddziałów w rozproszonych lokalizacjach, spodziewamy się większego zainteresowania rozwiązaniami w chmurze – mówi Anna Twardowska, Regional Sales Manager Central & Eastern Europe, Nedap Security Management.

Jedni wróżą wzrost, inni spodziewają się spadków

Nie wszyscy eksperci podzielają ten optymizm. Niektórzy podkreślają, że perspektywy rozwoju branży security w dużym stopniu zależą od sytuacji gospodarczej.

– Przyszłość jest nadal niepewna. Mimo chwilowego spadku inflacja prawdopodobnie utrzyma się na wysokim poziomie. Duży wpływ na gospodarkę będzie miał rozwój sytuacji politycznej w kraju i na świecie. W wielu krajach europejskich odnotowano symptomy recesji, a jak wiadomo polski rynek jest silnie z nimi skorelowany. Dużym problemem są i będą występujące zatory płatnicze – komentuje Jacek Karcewicz, dyrektor handlowy, Miwi Urmet.

Wzrost wynagrodzenia minimalnego z pewnością spowoduje podniesienie stawek za niektóre usługi. To z kolei może mieć korzystny wpływ na zmianę podejścia do wcześniej obranych form zabezpieczeń.

– *Dynamiczny wzrost płacy minimalnej sprawia, że nikogo już nie dziwi ograniczanie ochrony fizycznej na placach budów, terenach rozległych parków logistycznych czy nawet w obiektach użyteczności publicznej. Coraz popularniejsze stają się wirtualne recepcje, zdalne obchody pracowników ochrony czy monitoring wizyjny realizowany online z poziomu stacji monitorowania. Łączenie różnych systemów zabezpieczeń staje się standardem, więc czymś naturalnym jest otwartość producentów na wszelkiego rodzaju integracje, nierzadko z urządzeniami konkurencyjnymi* – ocenia Andrzej Laskowski, dyrektor operacyjny, NSS.

Nie tylko wzrost stawki minimalnej spędza sen z powiek wielu menedżerów. Dobra kadra, tj. wykwalifikowana i zaangażowana, widząca swoją przyszłość w tej branży, to coś, czego zaczyna wyraźnie brakować. A widać to zwłaszcza w sektorze ochrony fizycznej. – *Bez wątpienia w tym roku zasoby ludzkie stanowią coraz większe wyzwanie. Obawiam się jednak, że nie zmieni się to bez gruntownej zmiany postrzegania zawodu pracownika ochrony. Paradoksalnie podczas pandemii pracownicy ochrony pozostali na posterunkach, na pierwszej linii. Był to swoisty sygnał do otoczenia mówiący o tym, że są i mogą być bardzo ważni. Warto o tym pamiętać* – podkreśla Krzysztof Bartuszek, prezes zarządu Securitas w Polsce. I dodaje: – *Wyzwania w sektorze ochrony fizycznej od lat pozostają te same. Przede wszystkim branży potrzebne są zmiany prawa. Po pierwsze dostosowanie archaicznej już nieco Ustawy o ochronie osób i mienia do realiów cyfrowego świata, po drugie pełne oskładkowanie wszystkich umów i uporządkowanie kwestii związanych z zakładami pracy chronionej. Byłby to dobry krok w kierunku walki z patologiami. To samo dotyczy powrotu do licencji pracownika ochrony lub innej formy profesjonalizacji tego zawodu. Czy stanie się to w 2024 r., nie wiem, ale miałbym takie życzenie. Jeśli chodzi o zagrożenia, są to standardowe ryzyka biznesowe, a kierunki i trendy, jakie obrała branża, są niezmienne od lat. Nie doszukiwałbym się w tej kwestii specjalnych, nowych wyzwań.*

Niepewna sytuacja dotyczy także sektora systemów zabezpieczeń przeciwpożarowych. – *Branża systemów bezpieczeństwa pożarowego jest ściśle uzależniona od nowych inwestycji kubaturowych pojawiających się na rynku. Widoczne w 2023 roku lekkie spowolnienie w zakresie planowania nowych projektów wpłynie negatywnie na wolumen realizacji inwestycji w tym roku. Jednak zauważam również pozytywne czynniki związane z ożywieniem gospodarczym czy odblokowaniem środków z funduszy unijnych. To może zrównoważyć oddziaływanie negatywnych aspektów roku 2023* – prognozuje Michał Sidor, prezes Zarządu Schrack Seconet Polska.

Rok pod znakiem sztucznej inteligencji

Jak wynika z badania KPMG w Polsce, przeprowadzonego we współpracy z Microsoftem, pt. *Monitor Transformacji Cyfrowej Biznesu*, w polskich firmach rośnie znaczenie algorytmów sztucznej inteligencji (SI). Z tej technologii w 2023 r. korzystało 15% organizacji, a 13% planowało ją wdrożyć do końca roku. W Polsce sztuczna inteligencja jest najczęściej wykorzystywana w marketingu, produkcji i planowaniu łańcucha dostaw. Duże nadzieje firmy pokładają w usługach chmurowych, których wykorzystanie w ostatnim roku wzrosło.

Jarosław Grzybowski, Hikvision Poland

Hikvision nie ustaje w pracach nad produktami opartymi na najnowszych technologiach. Dzięki temu klienci znajdą w naszej ofercie szeroką gamę produktów dedykowanych do różnego rodzaju zastosowań. Oczywiście z naszej perspektywy wciąż niezmiennie największym zainteresowaniem cieszą się rozwiązania przeznaczone do monitoringu wizyjnego, ale jednocześnie bardzo dynamicznie rośnie zainteresowanie naszymi wideodomofonami, systemami kontroli dostępu, oprogramowaniem zarządzającym oraz wszelkiego rodzaju monitorami i wyświetlaczami.

Harald Dingemans, Linc Polska

W tym roku będziemy kontynuować współpracę z firmami ochrony. Naszą ofertą dla nich są mobilne wieży monitoringu z zaawansowanymi funkcjami analitycznymi.
Rozwijamy również ofertę dla sektora infrastruktury krytycznej, które wymagają zapewnienia odpowiedniego poziomu bezpieczeństwa. Dywersyfikujemy naszą ofertę, aby mieć rozwiązania z różnych dziedzin. Rozwijamy również eksport naszych urządzeń na rynku europejskie. Renomę zdobywamy dzięki udanym inwestycjom i poleceniom naszych partnerów.

Kamil Barański, Megavision Technology

Obecnie klienci koncentrują się na nawiązaniu relacji z partnerami, za którymi stoi nie tylko marketing, ale przede wszystkim wiedza ekspercka, doświadczenie zdobyte we wdrożeniach, a także – i co równie istotne – produkt. Kombinacja tych czynników to ważny element sukcesu zarówno dla nas, jak i klienta, który wdraża rozwiązania security. Absolutnym priorytetem wielu podmiotów jest integracja systemów bezpieczeństwa, a my mamy dla nich doskonale przygotowany, otwarty, elastyczny i profesjonalny produkt #VENOM PSIM.

Jacek Karcewicz, Miwi Urmet

W tym roku przewiduję dalszy wzrost zainteresowania systemami ochrony perymetrycznej wzbogaconymi sztuczną inteligencją, integracją systemów zabezpieczeń oraz zaawansowaną analityką obrazu. Nasi najwięksi dostawcy urządzeń i systemów (m.in. Motorola, ICT) już w ubiegłym roku wprowadzili wiele innowacji w swoich produktach, a w tym roku zapowiadają kolejne wdrożenia najnowszych technologii.

→

> *W polskich firmach rośnie znaczenie algorytmów sztucznej inteligencji. Z tej technologii w 2023 r. korzystało 15% organizacji, a 13% planowało ją wdrożyć do końca roku.*

Ta tendencja jest zauważalna również w branży security. Eksperci w jednej kwestii są zgodni: rok 2024 będzie też okresem wzrostu znaczenia sztucznej inteligencji w systemach zabezpieczeń.

– *Nowe algorytmy analizy obrazu, takie jak Yolo czy G-RCNN, wprowadzają nową jakość pod względem skuteczności oraz lepszej klasyfikacji obiektów. Bez wątpienia SI zostanie zaprzęgnięta do szukania korelacji danych pochodzących z różnych systemów, takich jak SSWIN, CCTV, KD, SSP oraz automatyka budynku. To da nową jakość, pomoże zredukować liczbę personelu przy jednoczesnym zapewnieniu wyższego poziomu bezpieczeństwo i predykcji zagrożeń* – tłumaczy Tomasz Kaliński.

Nie ma już odwrotu od sztucznej inteligencji, której powstanie i rozwój są uznawane za współczesną rewolucję przemysłową. – *Spodziewamy się, że rola SI w wykrywaniu zagrożeń za pośrednictwem systemów zabezpieczeń, takich jak monitoring wizyjny, będzie dynamicznie rosła. Światowi liderzy w wielu branżach inwestują ogromne środki w jej rozwój, więc nadejście przełomowych rozwiązań i nowych możliwości sztucznej inteligencji to tylko kwestia czasu* – podkreśla Jarosław Grzybowski.

Wzrost znaczenia sztucznej inteligencji w całej branży, również w sektorze bezpieczeństwa pożarowego, dostrzega też Michał Sidor. – *Jeśli miałbym wskazać jeden konkret, który będzie charakteryzował naszą branżę w 2024 roku, będzie to kontynuacja rozwoju rozwiązań opartych na algorytmach sztucznej inteligencji.*

W Unii Europejskiej zauważalny jest wzrost zainteresowania technologią 5G.

– *To kierunek, którego spodziewamy się też w Polsce. Dzięki szybszej transmisji i zwiększonej przepustowości rejestracja materiału wizyjnego łącznie z analityką będzie możliwa bezpośrednio w kamerze, a także od razu w chmurze. Również zaawansowane funkcje analityczne, które do tej pory mogły działać tylko w chmurze, teraz będą mogły działać w kamerze. W tym zakresie na pewno spodziewam się rozwoju w tym roku* – ocenia Harald Dingemans.

Inwestycje w bezpieczeństwo cyfrowe, wdrożenie sieci 5G czy implementacja SI w różnych gałęziach gospodarki zdominują rynek w tym roku. – *W sektorze security obserwujemy postępujący rozwój sztucznej inteligencji, który w monitoringu wizyjnym jest alternatywą dla ochrony fizycznej. Pandemia czy wojna wymusiły w wielu przedsiębiorstwach zmianę trybu pracy (praca zdalna, automatyzacja czy identyfikacja osób to tylko niektóre z nich). Bez wątpienia sztuczna inteligencja to przyszłość i obszar ekspansji oraz nowych możliwości dla szeroko pojmowanej całej branży zabezpieczeń* – twierdzi Andrzej Laskowski.

– *W obliczu dynamicznie rosnących kosztów zatrudnienia pracowników firmy coraz częściej poszukują możliwości automatyzacji procesów wewnętrznych. Obecnie obserwujemy, że ten trend staje się bardziej wyraźny niż kiedykolwiek wcześniej. Kluczowym elementem automatyzacji procesów jest z kolei efektywna analiza wideo, zdolna znacząco redukować liczbę fałszywych alarmów* – zauważa Kamil Kierzkowski.

Może nie hurraoptymizm, ale nie warto tracić nadziei

Z pewnością najbliższe miesiące pokażą, czy spowolnienie gospodarcze, które nastąpiło w 2023 r., już minęło, a jeżeli nie, to kiedy to się wydarzy. – *Według mnie rok 2024 upłynie pod znakiem nadziei. W porównaniu z innymi państwami z naszego regionu w Polsce w branży technologicznej nie odczuliśmy tak dużego zastoju. Zatem jest nadzieja, ale połączona z działaniami, które sprawią, że ten prognozowany przez wielu wzrost gospodarczy w tym roku rozpocznie się jak najszybciej i przełoży się na stabilny rozwój biznesu w Polsce* – twierdzi Robert Gawroński.

Z tym samym optymizmem na ten rok patrzy Robert Pestka, dyrektor wsparcia sprzedaży, POLON-ALFA. – *Mam nadzieję, że rok 2024 zapoczątkuje liczne inwestycje, związane chociażby z finansowaniem ze środków z KPO, a to przełoży się na wzrost zapotrzebowania na usługi w zakresie projektowania i instalowania systemów przeciwpożarowych w nowych obiektach. W kontekście ogólnego wzrostu świadomości ekologicznej, kryzysu klimatycznego firmy powinny również zwracać uwagę na zrównoważone rozwiązania w dziedzinie ochrony przeciwpożarowej, przede wszystkim w obszarze technologii energooszczędnych. To postawi przed nami nowe wyzwania, ale jednocześnie otworzy nowe możliwości biznesowe* – podkreśla Robert Pestka.

Przewiduje się, że w tym roku zostanie odblokowanych wiele inwestycji finansowanych z budżetu państwa. – *Będzie to motywowało nas do jeszcze większej aktywności handlowej i marketingowej. Zwiększymy liczbę spotkań z naszymi partnerami handlowymi, do których zaliczamy głównie projektantów i integratorów. Będziemy też uczestniczyć w wielu konferencjach i szkoleniach* – deklaruje Jacek Karcewicz.

Wielu przedsiębiorców wychodzi z założenia, że jedynie koncentracja na silnym innowacyjnym produkcie ma szansę powodzenia na rynku w Polsce.

– *Jako producent aktywnie stawiamy na rozwój naszego oprogramowania i wyposażenie go w elementy i funkcjonalności AI pozwalające wesprzeć pracę operatorów systemów bezpieczeństwa. Jeśli połączymy to z doświadczeniem polskich specjalistów w obszarze*

bezpieczeństwa, którzy pracują w naszej firmie, mamy gwarantowany wspólny sukces budowany partnersko z użytkownikami infrastruktury krytycznej i czołowymi firmami, dla których bezpieczeństwo jest priorytetem – zapowiada Kamil Barański.

Oczekiwania w stosunku do systemów security

Jakość produktów systemów zabezpieczeń rośnie nie tylko z roku na rok, ale także z generacji na generację. To ze strony producentów działanie konieczne i oczywiste, wymuszone przez silną konkurencję funkcjonującą globalnie.

Użytkownicy systemów monitoringu wizyjnego oczekują coraz lepszej jakości materiału dowodowego, a z uwagi na cyberbezpieczeństwo wielu klientów zaczyna też zwracać uwagę na kraj pochodzenia urządzeń.

– Naszym atutem jest fakt, że jesteśmy marką szwedzką, a produkcja urządzeń odbywa się też w Polsce. W celu usprawnienia naszego łańcucha dostaw w najbliższym czasie planujemy otworzyć centrum logistyczno-konfiguracyjne usytuowane niedaleko polskich fabryk – podkreśla Dagmara Pomirska.

Obecnie korzyści z usług chmurowych stały się jeszcze bardziej oczywiste, a zaufanie do tego modelu znacząco wzrosło.

– Reagując na rosnące zainteresowanie klientów, już od pewnego czasu na rynku amerykańskim oferujemy usługę VaaS. Zauważamy także, że część naszych klientów przenosi swoje standardowe systemy oparte na oprogramowaniu VMS na serwery wirtualne w chmurze, co jest wyraźnym sygnałem zmian w preferencjach rynkowych. Dodatkowo wprowadziliśmy innowacyjne rozwiązanie Solid Edge w kamerze kopułkowej wyposażonej w dysk SSD z preinstalowanym VMS-em WAVE. To fascynujące rozwiązanie stanowi alternatywę dla klientów poszukujących rozproszonych systemów, pragnących jednocześnie zachować kontrolę nad przechowywaniem danych w swojej infrastrukturze. Solid Edge umożliwia klientom stworzenie prywatnej chmury – podsumowuje Kamil Kierzkowski.

Zainteresowanie zaawansowanymi rozwiązaniami wykorzystującymi najnowsze zdobycze technologii zauważa się też w kontroli dostępu.

– Zainteresowanie klientów integracją systemu kontroli dostępu z systemami bezpieczeństwa oraz systemami zarządzania budynkiem obserwujemy od wielu lat. Dlatego też już pod koniec 2022 r. wprowadziliśmy do oferty platformę oprogramowania VISO SMS, która służy do monitorowania i wizualizacji systemów zabezpieczeń. Wnioski, jakie nasuwają się po analizie wyników sprzedaży za rok 2023 r., to podniesienie świadomości klientów w kwestii bezpieczeństwa widoczny w znaczących wzrostach sprzedaży czytników obsługujących szyfrowane połączenia z kontrolerem, bezpieczne karty (MIFARE® DESFire®) oraz technologia identyfikacji mobilnej (BLE/NFC/QR) – wymienia Łukasz Kanarek.

Jaki będzie ten rok dla sektora systemów przeciwpożarowych w Polsce?

– Sektor ppoż. będzie kontynuował rozwijanie i wdrażanie nowoczesnych technologii, takich jak zaawansowane systemy detekcji pożarowej, inteligentne systemy zarządzania sytuacją kryzysową czy rozwiązania oparte na sztucznej inteligencji. Innowacyjne technologie z pewnością poprawią już i tak wysoką skuteczność elektronicznych i technicznych systemów zabezpieczeń, a także działań ratowniczych, tak aby jak najskuteczniej minimalizować ryzyko pożaru i jego skutki – zauważa Robert Pestka.

Andrzej Laskowski, NSS

Poszukiwane są nowe urządzenia wielozadaniowe, które spełniają funkcje, do jakich jeszcze niedawno trzeba było zastosować kilka różnych narzędzi oraz fizyczną obecność człowieka. To wzór idealnego połączenia zabezpieczeń i inteligentnej technologii. Wieże mobilne BCS są przykładem, gdzie coraz skuteczniejsza inteligentna analityka obrazu pozwala całodobowo monitorować znaczne obszary, ograniczając przy tym koszty dla inwestorów. W spółce NSS rozwijamy polską myśl technologiczną, wykorzystując zespół specjalistów z branży IT oraz własny park produkcyjny. Znając rynek i jego wymogi, nieustannie poszerzamy nasz asortyment: zbudowaliśmy własny system alarmowy, rejestrator wspomagany naszą analityką, całą rodzinę nadajników GPS wraz z miniaturową wersją do zastosowania w rowerach elektrycznych. A to jeszcze nie koniec naszych ambicji.

Robert Pestka, POLON-ALFA

Zapewniamy wysoką jakość produktów i usług przez nas oferowanych, co przekłada się na zadowolenie klientów, którzy regularnie do nas wracają z nowymi zamówieniami. W tym punkcie muszę zwrócić uwagę na nasz zespół, naszych pracowników. Ich rozwój, zdobywanie nowych umiejętności i rozwijana kreatywność pomagają nam w zdobywaniu przewagi konkurencyjnej. Dobra atmosfera wewnątrz naszego zespołu oraz pozytywne relacje z klientami przekładają się na satysfakcję i lojalność wobec firmy POLON-ALFA. Jak widać, jest to skuteczna strategia w ciągłym pozyskiwaniu klientów i budowaniu marki.

Łukasz Kanarek, Roger

W ostatnim czasie klienci szczególnie zwracają uwagę na bezpieczeństwo cybernetyczne posiadanych i nowo instalowanych systemów, dlatego spora część wdrożonych już systemów jest aktualizowana do najnowszej wersji, tak aby zapewnić najwyższy poziom bezpieczeństwa. Ponadto klienci oczekują, by system był otwarty na integrację, dawał możliwości raportowania i analizowania danych w oprogramowaniu, obsługiwał identyfikację mobilną oraz oferował dodatkowe funkcjonalności, np. obsługę szafek czy depozytorów kluczy. Poza rozwiązaniami, które są dostępne w ramach systemu, klienci cenią wsparcie techniczne zapewnione przez producenta.

Podniesienie stawki minimalnego wynagrodzenia będzie miało znaczący wpływ na branżę ochrony.

– Duży wzrost minimalnej płacy to, co do zasady, dobry kierunek w długiej perspektywie. W końcu chcemy, aby pracownicy zarabiali godnie, a poza tym gonimy Europę. Szybki wzrost kosztów płacowych to z jednej strony ryzyko związane z redukcją i optymalizacją tej części działalności, z drugiej – szansa na rozwój w zakresie zabezpieczeń technicznych. Każda tego typu zmiana to szansa dla kreatywnych firm i branż na rozwój – poszukiwanie nowych rozwiązań, ale jednocześnie to również ryzyko otwierania szarej strefy, likwidacji miejsc pracy czy też upadku małych firm, których nie będzie stać na udźwignięcie inwestycji technologicznych. Takie trendy to możliwość synergii w branży, budowania standardów przez duże podmioty, przy jednoczesnym osłabieniu mniejszych lokalnych biznesów – ocenia Krzysztof Bartuszek.

Dyrektywa NIS 2

Dyrektywa NIS2 to ogólnounijne przepisy dotyczące cyberbezpieczeństwa. Przewiduje ona środki prawne mające na celu zwiększenie ogólnego poziomu cyberbezpieczeństwa w całej Unii Europejskiej. Dyrektywa weszła w życie 16 stycznia 2023 r., a termin wdrożenia nowych wymagań mija 17 października 2024 r. Po upływie tej daty nowe przepisy będą obowiązywać we wszystkich krajach Unii Europejskiej.

Czy rodzime firmy branży security są gotowe do spełnienia wymagań dyrektyw NIS2? Oto wypowiedzi kilku z nich.

– Już od 2016 r. produkty i wewnętrzne procesy Axis spełniały dyrektywę NIS, a obecnie także NIS2. Wdrażamy dobre praktyki dotyczące zarządzania i reakcji na podatności wykryte w produktach, aby zminimalizować ryzyko po stronie użytkowników (Security Notification Service oraz Vulnerability Management Policy). Mamy także własną linię produkcyjną oraz własny, dedykowany chip ARTPEC – jeden z najważniejszych elementów stawiających Axis na szczycie oceny pod względem cyberbezpieczeństwa – podkreśla Dagmara Pomirska.

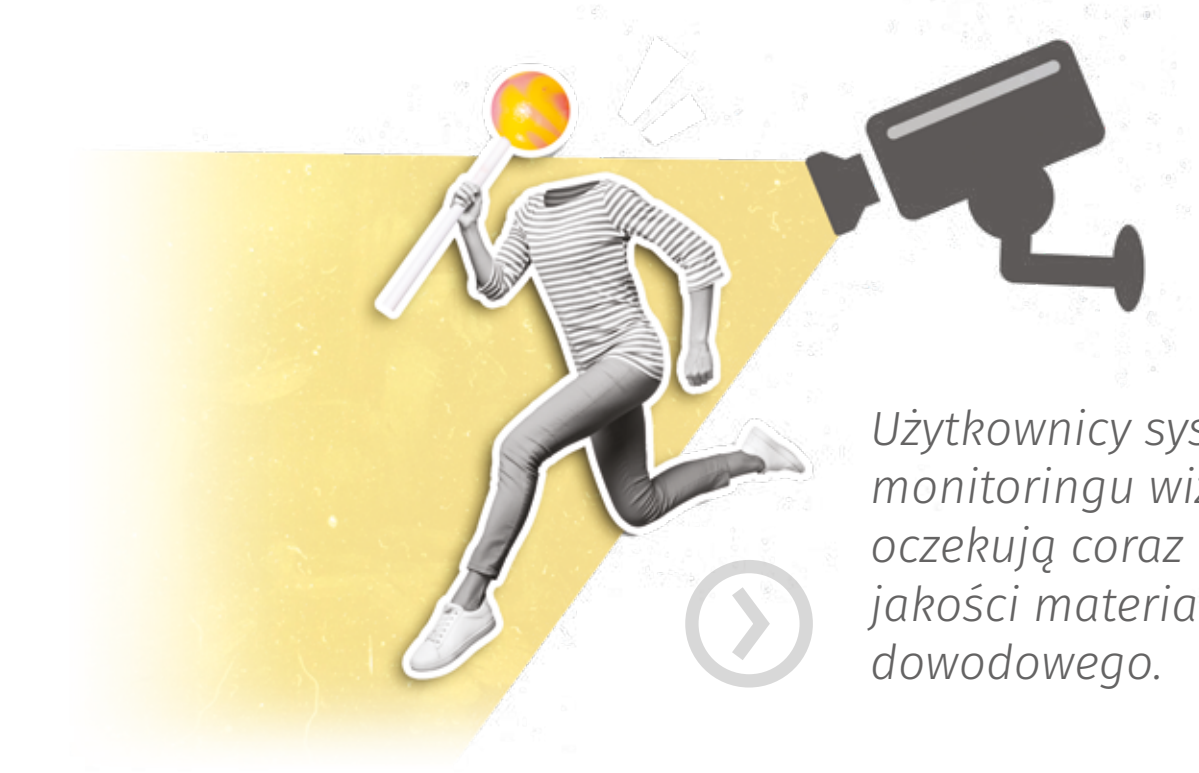
– Dyrektywa obejmuje wiele podmiotów, w tym infrastrukturę krytyczną, m.in. energetykę, służbę zdrowia, bankowość oraz transport. W tych sektorach gospodarki Miwi Urmet ma w ostatnim okresie wiele wdrożeń i liczymy na dalszą współpracę – mówi Jacek Karcewicz.

– Megavision Technology od początku swojej działalności stara się koncentrować na rozwiązaniach z rynku USA czy Korei. Rozwiązania te są w pełni gotowe w zakresie spełnienia wymagań NIS2. Ponadto, jako twórca oprogramowania klasy PSIM, wątek cyberbezpieczeństwa jest dla nas kluczowym elementem zarówno polityki, jak i kierunku rozwoju – podkreśla Kamil Barański.

– W Hanwha Vision zawsze dostarczaliśmy rozwiązania o wysokim poziomie cyberbezpieczeństwa. Od wielu lat w strukturach firmy działa zespół S-CERT, który odpowiada za cyberbezpieczeństwo naszych urządzeń. Jesteśmy członkiem programu Common Vulnerabilities and Exposures (CVE®), przedsięwzięcia, które w sposób transparentny publikuje wykryte zagrożenia nie tylko w elementach systemów bezpieczeństwa, ale również w językach programowania. Aktywne działania w obszarach bezpieczeństwa pozwalają nam zapewnić najwyższy poziom ochrony naszych rozwiązań. Funkcjonując na rynku już ponad 30 lat jako producent systemów dozoru wizyjnego, budujemy biznes w oparciu o zaufanie naszych partnerów – zaznacza Kamil Kierzkowski.

– Dyrektywa NIS 2 wymaga od systemów kontroli dostępu wysokiego poziomu bezpieczeństwa cybernetycznego. System RACS 5 wymóg ten spełniał od początku pojawienia się na rynku, tj. już w 2016 r. Wraz z kolejnymi aktualizacjami Roger wprowadza do systemu najnowsze technologie pozwalające na utrzymanie ochrony cybernetycznej na poziomie zgodnym z aktualnymi trendami – mówi Łukasz Kanarek.

– Coraz częściej spotykamy się z oczekiwaniem ze strony inwestorów zagranicznych, jak również instytucji publicznych, że elementy składowe systemu dozoru wizyjnego nie mogą pochodzić z chińskich fabryk. Jako znaczący dostawca urządzeń do monitoringu wizyjnego wprowadziliśmy do oferty nową linię urządzeń BCS ULTRA produkowanych w Korei Południowej. Połączenie urządzeń z rodowodem



Użytkownicy systemów monitoringu wizyjnego oczekują coraz lepszej jakości materiału dowodowego.

koreańskim oraz autorskiego oprogramowania BCS MANAGER rozwijanego przez własny zespół programistów pozwala nam dostosowywać ofertę BCS do zmieniającego się otoczenia prawnego w zakresie cyberbezpieczeństwa – wyjaśnia Andrzej Laskowski.

– Hikvision bardzo poważnie podchodzi do wszelkich kwestii związanych z cyberbezpieczeństwem. Dlatego przede wszystkim zadbaliśmy o to, aby osiągnąć pełną gotowość do wprowadzenia zmian niezbędnych do zapewnienia zgodności z NIS2. Ponadto Hikvision przestrzega uznawanych na całym świecie standardów cyberbezpieczeństwa, takich jak ISO 27001, ISO 27701 i CSA STAR, a także zapewnia bezpieczny cykl życia oprogramowania oraz zasady bezpiecznego projektowania. Staramy się też wspierać naszych partnerów w przygotowaniu się na nowe ramy regulacyjne, oferując im specjalistyczną wiedzę w zakresie nie tylko nowej dyrektywy, ale również szeroko pojętego cyberbezpieczeństwa – podkreśla Jarosław Grzybowski.

– Firma Linc spełnia wymagania dotyczące bezpieczeństwa urządzeń od początku jej powstania. Do oferty wprowadzamy urządzenia od zaufanych producentów. Podkreślamy ich profesjonalizm nie tylko w kwestii użytkowania i gwarancji urządzeń, ale także w kwestii etycznej. Wybieramy tylko cyberbezpieczne produkty – zaznacza Harald Dingemans.

Wpływ zmian na światowym rynku security

Światowy rynek zabezpieczeń technicznych zmienia się pod wpływem postępu technologicznego, zmian geopolitycznych oraz rosnącego nacisku na integrację i etykę. Zauważalna jest też konsolidacja firm. Jaki to będzie miało wpływ na rynek w Polsce?

– Zmiany geopolityczne powodują problemy związane z bezpieczeństwem, ale równocześnie postęp technologiczny napędza rozwój systemów go zapewniających. To również ogromne możliwości dla branży security, która wchodzi na coraz wyższy poziom i usprawnia cyfrową transformację rynków wertykalnych, takich jak energetyka, logistyka, przemysł i produkcja, handel, edukacja, służba zdrowia itp. – mówi Andrzej Laskowski.

– Ostatnie lata pokazały, że polski rynek security, mimo wielu różnego rodzaju zagrożeń, z którymi mieliśmy do czynienia, radzi sobie bardzo dobrze i szybko adoptuje się do zmieniających się realiów biznesowych. Z całą pewnością postęp technologiczny czy też zmiany geopolityczne będą miały istotny wpływ i wymuszą na polskich firmach konieczność dostosowania się do nowych standardów, rozwijanie innowacji oraz zwiększenie świadomości w dziedzinie bezpieczeństwa. Możemy więc spodziewać się, że to przyczyni się do dalszego dynamicznego rozwoju oraz dostosowywania się branży security do globalnych trendów – zapowiada Jarosław Grzybowski.

– Na światowym rynku systemów zabezpieczeń zauważalna jest konsolidacja firm. Najwięksi gracze przejmują mniejsze firmy, zapewniając im środki finansowe na rozwój technologiczny. Należy przypuszczać, że w najbliższej perspektywie duże firmy będą wyznaczały kierunki rozwoju branży na całym świecie. Podsumowując, z dużym optymizmem wchodzimy w rok 2024. Liczymy na to, że będzie on nie tylko dla naszej firmy, ale również dla całej branży co najmniej równie dobry jak rok miniony – mówi Jacek Karcewicz.

– Moim zdaniem wpływ postępu technologicznego i konsolidacji firm będzie skutkował bardziej konkurencyjnym rynkiem w Polsce. Firmy muszą pozostać elastyczne, innowacyjne i gotowe do dostosowania się do nowych warunków, aby utrzymać dynamiczny rozwój w sektorze security oraz włączać bezpieczeństwo techniczne w obszar cyberbezpieczeństwa – podkreśla Wojciech Weissenberg. ●

NA POLSKIM RYNKU SECURITY

Krzysztof Bartuszek, Securitas

Cały czas reagujemy na zmieniające się otoczenie i słuchamy naszych klientów. Staramy się inwestować i wyprzedzać rynek. Branża ochrony w Polsce jest cały czas młoda w porównaniu z innymi krajami Europy Zachodniej. Oczekiwania, które pojawiają się na Zachodzie, prędzej czy później pojawiają się i u nas, a w ostatnich latach – prędzej. Z drugiej strony na globalizującym się rynku kwestie standaryzacji sposobu realizacji usług są bardziej niż oczywiste. Paradoksalnie indywidualizacja na poziomie klienta też ma przyszłość. Innymi słowy, indywidualne podejście do potrzeb klienta przy zachowaniu jednolitych standardów tam, gdzie to możliwe.

Wojciech Weissenberg, squareTec

Nasi klienci interesują się rozwiązaniami opartymi na sztucznej inteligencji, pracującymi w środowisku rozproszonym, ale też poszukują wyższego stopnia synergii między systemami. Odpowiadamy na to zapotrzebowanie, opracowując własne rozwiązania programistyczne integrujące urządzenia i systemy. Przykładem może być plug-in integrujący depozytory SAIK w systemie kontroli dostępu Genetec zapewniający pełne wykorzystanie możliwości depozytora jako pełnoprawnego elementu SKD. Innym rozwiązaniem jest ANPR Dashboard, system typu Big Data umożliwiający szybkie wyszukiwanie pojazdów z dużych baz danych i zapewniający integrację wielu dostawców ANPR, MMR i IoT.

Robert Gawroński, TP-Link Polska

Wiodącymi produktami w naszej ofercie, które cieszą się największym zainteresowaniem klientów z branży security, są przełączniki, przede wszystkim te wykorzystujące technologię PoE. Jest to niewątpliwie szkielet służący do integracji wielu różnych systemów stosowanych w obiektach czy przedsiębiorstwach, ale także w domach jednorodzinnych. Coraz większe zainteresowanie budzą również nasze rozwiązanie do monitoringu wizyjnego z serii VIGI. Oferta tych produktów rozwija się dynamicznie i będzie stanowić ciekawe uzupełnienie naszej oferty kierowanej do klientów z sektora MŚP.

Trzy czynniki, które miały największy wpływ na sektor ochrony w 2023 roku

Najważniejsze zjawiska, których wzrost kształtował w zeszłym roku branżę ochrony osób i mienia, to koszty prowadzenia działalności, liczba kradzieży w obiektach handlowych oraz *job hopping* pracowników. Branża, która ma istotny wpływ na stabilność życia w kraju, musiała więc walczyć o swoją pozycję na rynku.

– Od jesieni prowadzimy intensywne rozmowy z klientami dotyczące konieczności waloryzacji, czyli przywrócenia pierwotnej wartości naszych kontraktów i powrotu do równowagi ekonomicznej między stronami z dnia podpisywania umowy. To warunek niezbędny, byśmy mogli utrzymać wysoki standard usług. Tymczasem klienci – jeśli nawet zgadzają się płacić więcej – wiążą podwyżkę jedynie z podniesieniem płacy minimalnej, nie uwzględniając innych czynników makroekonomicznych – podkreśla Paweł Korzybski, prezes Polskiego Związku Pracodawców Ochrona.

Ceny w kraju wciąż rosną – już wiadomo, że średnia wartość inflacji w 2023 r. wyniosła 11,6%. Tymczasem składowe cen w branży ochrony – czyli koszty zarówno bezpośrednie (m.in. pracownicze, wyposażenia, paliwa), jak i pośrednie (m.in. nadzór, księgowość, kadry) – w latach 2021–2023 zwiększyły się o kilkadziesiąt lub kilkaset procent. Rachunki za energię były wyższe o 36%, za utrzymanie lokalizacji – o 27%, a najbardziej (o 305%) wzrosły koszty finansowania działalności.

Więcej kradzieży w obiektach handlowych

Dane CBOS z maja ub.r. wskazują, że wśród osób, które w ostatnich 5 latach padły ofiarą przestępstwa, najwięcej (12%) doświadczyło właśnie kradzieży. W porównaniu z wynikami badania z 2022 r. dwukrotnie zwiększył się odsetek ankietowanych, którzy zostali napadnięci i obrabowani (z 1 do 2% – wg danych CBOS). Z kolei najnowsze statystyki Komendy Głównej Policji wskazują, że w ubiegłym roku liczba kradzieży sklepowych wzrosła o 22,2% względem 2022 r.

Dla sektora ochrony wzrost kradzieży oznaczał konieczność inwestycji w szkolenia pracowników – stanowiskowe oraz dotyczące wykorzystania technologii takich jak analiza obrazu czy systemy zabezpieczeń. Musiały również powstać dodatkowe grupy kontrolne, które analizują zaistniałe zdarzenia i przygotowują materiał dowodowy dla policji.

Coraz większe znaczenie rynku pracownika

W roku 2023 nasiliło się również zjawisko *job hoppingu* – coraz więcej osób szukało nowej pracy w okresie zatrudnienia i często zmieniało pracodawców w celu podniesienia zarobków i skrócenia drogi awansu. Pracownicy sektora ochrony łatwo znajdowali zatrudnienie w takich branżach jak transport i logistyka. Według danych Job Market Insights tylko w IV kwartale 2023 r. zamieszczono w Internecie ponad 70,6 tys. ogłoszeń z ofertami pracy w tych branżach. Ten trend będzie się nasilać.

Opisane zjawiska spowodowały, że przedsiębiorstwa z branży ochrony weszły w rok 2024 z dużym niepokojem i niepewnością. Tymczasem ustabilizowanie sytuacji w tym sektorze jest niezbędne, by mógł on na bieżąco reagować na zmieniającą się sytuację i nadal zapewniać wysoki poziom bezpieczeństwa w kraju. ●

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

POLON-ALFA

dobrze zaprojektowane BEZPIECZEŃSTWO

KOMPLEKSOWE
SYSTEMY SYGNALIZACJI POŻAROWEJ

• PRODUKCJA • SERWIS • SZKOLENIA
• WSPARCIE TECHNICZNE I PROJEKTOWE

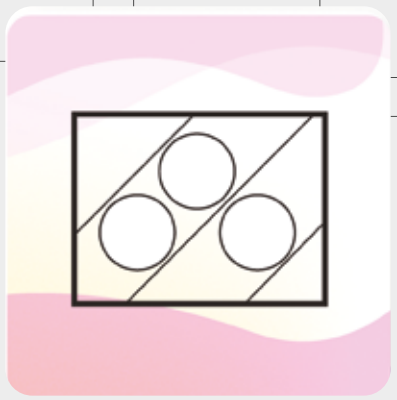
AUTOMATYKA POŻAROWA

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

5 trendów bezpieczeństwa

Innowacje techniczne to jednej strony ogromne możliwości, z drugiej nowe wyzwania. Każda innowacja niesie zmianę, co oznacza konkretne konsekwencje dla dostawców, klientów i organów regulacyjnych, a ta z kolei wymaga skupienia, energii i staranności w działaniu.

Kluczowe trendy technologiczne, które naszym zdaniem będą miały wpływ na sektor bezpieczeństwa w 2024 r., odzwierciedlają to szybko zmieniające się środowisko. Jak zawsze, są one mieszanką pozytywnych możliwości, które należy wykorzystać, a także wyzwań, którymi należy się zająć.



Perspektywa „całego systemu”

Wpływ każdego aspektu systemu bezpieczeństwa będzie podlegał wzmożonej kontroli, a dostawcy i klienci będą musieli monitorować, mierzyć i w coraz większym stopniu raportować szeroki zakres czynników. Zasadnicze znaczenie będzie miało przyjęcie całościowej perspektywy systemowej.

Dobrym przykładem jest zużycie energii. Kamera wideo zużywa stosunkowo niewielką ilość energii, jednak perspektywa się zmienia, kiedy spojrzymy holistycznie na cały system i weźmiemy pod uwagę również serwery, przełączniki, koncentratory oraz routery, przez które przesyłane są dane, znajdujące się w dużych centrach danych, a te wymagają chłodzenia. Świadomość tego oznacza innowacje w zakresie nowych technologii, które przyniosą wszystkim korzyści. Dobrym przykładem są kamery, które dynamicznie modyfikują prędkość transmisji, zajęcie pamięci masowej i obciążenie serwera w celu zmniejszenia wymagań dotyczących chłodzenia serwera.

Wszyscy zgadzamy się, że całkowity koszt posiadania (TCO) jest ważną miarą, ale dostawcy zabezpieczeń będą w coraz większym stopniu musieli brać pod uwagę (i być przejrzyści) całkowity wpływ własności, biorąc pod uwagę aspekty niefinansowe, w tym środowiskowe i społeczne. Dostawcy nie będą już mogli działać w oderwaniu od własnych łańcuchów wartości i łańcuchów wartości swoich klientów.

Nie mamy wątpliwości, że w 2024 r. nastąpi dalszy postęp technologiczny, a wraz z nim kolejne wyzwania dla wszystkich. Jak zawsze z niecierpliwością czekamy na współpracę z naszymi partnerami i klientami, aby zapewnić pozytywne wyniki dla wszystkich, w sektorze i poza nim.

Efektywność zarządzania architekturą hybrydową

Architektura hybrydowa łącząca zalety technologii lokalnych, chmurowych i brzegowych jest obecnie uznawana za nowy standard w wielu rozwiązaniach zabezpieczających. Stosowana jest tam, gdzie zapewnia największą wydajność, wykorzystując to, co najlepsze z każdej instancji w systemie, zwiększając przy tym poziom jego elastyczności. Ostatecznie architektury systemów powinny służyć potrzebom klienta, a nie preferowanej przez dostawcę strukturze.

W dużej mierze jest to kwestia dostępności. Im więcej rozwiązań funkcjonuje w środowiskach łatwo dostępnych zarówno dla dostawców, jak i klientów, tym większe możliwości mają dostawcy w zakresie zarządzania elementami systemu, biorąc większą odpowiedzialność i zmniejszając obciążenie klientów.

Architektura hybrydowa wykorzystuje algorytmy sztucznej inteligencji w zakresie automatyzacji zarządzania rozwiązaniami oraz ich obsługą. Zwiększona dostępność systemu jest cenna zarówno przy wsparciu ludzkim, jak i sztucznej inteligencji, ponieważ wykorzystuje mocne cechy obu stron.

Regulacje i zgodność z przepisami wpływają na rozwój technologii

Mówiąc o zgodności, globalne środowisko regulacyjne ma coraz większy wpływ na rozwój technologii, jej zastosowanie i wykorzystanie. Zgodność z nimi jest czymś, czego dostawcy i użytkownicy końcowi muszą być świadomi. Sztuczna inteligencja, cyberbezpieczeństwo, zrównoważony rozwój, ład korporacyjny to obszary, które podlegają wielu regulacjom. Dostawcy muszą opracowywać własne technologie i prowadzić własną działalność w sposób zgodny z regulacjami.

Geopolityka i stosunki handlowe między państwami prowadzą również do regulacji, które wymagają przejrzystości na poziomie komponentów, jeśli dostawcy chcą zachować licencję na prowadzenie działalności na kluczowych rynkach międzynarodowych.

Dobrym przykładem wprowadzanych rozwiązań jest np. dyrektywa w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii Europejskiej, tzw. dyrektywa NIS2. Na mocy wprowadzonych dyrektywą przepisów przedsiębiorstwa wskazane jako operatorzy usług kluczowych w sektorach, tj. energia, transport, woda, bankowość, finanse czy infrastruktura cyfrowa, będą musiały podjąć odpowiednie środki bezpieczeństwa i powiadamiać właściwe organy krajowe o poważnych incydentach.

Potencjał generatywnej sztucznej inteligencji w sektorze bezpieczeństwa

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.

Rośnie potencjał sztucznej inteligencji i głębokiego uczenia w sektorze bezpieczeństwa, ze szczególnym uwzględnieniem zaawansowanej analityki na brzegu sieci, np. w wykorzystaniu urządzeń takich jak kamery. To rozprzestrzenianie się głębokiego uczenia na brzegu sieci wciąż przyspiesza. Praktycznie każda nowa kamera sieciowa została wyposażona w tę funkcję, co znacznie zwiększa dokładność analiz. Daje to podstawy do tworzenia skalowalnych rozwiązań chmurowych, ponieważ minimalizuje wymagania dotyczące przepustowości, zmniejszając przy tym przetwarzanie w chmurze, i sprawia, że system jest bardziej niezawodny.

Jeśli chodzi o sztuczną inteligencję, w ubiegłym roku do powszechnej świadomości wręcz wdarły się duże modele językowe jako podstawa generatywnej sztucznej inteligencji. Ta forma AI wspiera tworzenie nowych treści – słów, obrazów, a nawet wideo.

Większość branż przygląda się możliwościom zastosowania generatywnej sztucznej inteligencji. Sektor bezpieczeństwa nie jest wyjątkiem. W roku 2024 zobaczymy aplikacje skoncentrowane na bezpieczeństwie oparte na dużych modelach językowych i generatywnej sztucznej inteligencji. Prawdopodobnie AI będzie używana w roli asystenta dla operatorów, pomagając im dokładniej i wydajniej interpretować to, co dzieje się w scenie, oraz jako interaktywna obsługa klienta.

Ochrona zawsze, ale bezpieczeństwo także

Bezpieczeństwo i ochrona są ze sobą powiązane. Mimo to należy pamiętać, że bezpieczeństwo wiąże się z zapobieganiem celowym działaniom – włamaniom, wandalizmowi, agresji wobec ludzi itp. Ochrona jest związana z niezamierzonymi zagrożeniami i incydentami, które mogą wyrządzić szkodę ludziom, mieniu i środowisku.

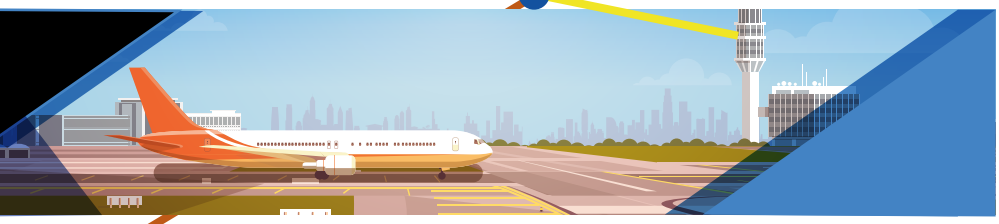
Z wielu powodów wykorzystanie dozoru wizyjnego i analityki w przypadkach użycia związanych z ochroną szybko rośnie i będzie się rozwijać. Jednym z powodów są niestety zmiany klimatyczne. W związku z ekstremalnymi warunkami pogodowymi powodującymi powodzie, pożary, osuwiska, lawiny i inne dozór wideo, czujniki środowiskowe i analityka będą coraz częściej wykorzystywane do wczesnego ostrzegania o potencjalnych katastrofach i błyskawicznej reakcji na nie.

Zarządzanie ryzykiem, zgodność z dyrektywami dotyczącymi zdrowia i bezpieczeństwa oraz wymogami regulacyjnymi to kolejny kluczowy powód wzrostu liczby przypadków zastosowań związanych z ochroną. Monitoring wizyjny będzie szeroko wykorzystywany w organizacjach w celu zapewnienia przestrzegania zasad BHP i bezpiecznych praktyk pracy, takich jak noszenie wymaganych środków ochrony osobistej (PPE). Tam, gdzie dojdzie do incydentów, monitoring wizyjny będzie coraz bardziej użytecznym i ważnym narzędziem w dochodzeniach. ●

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

Wavestore VMS – bezpieczne oprogramowanie dla infrastruktury krytycznej

Zakłócenia w funkcjonowaniu obiektów infrastruktury krytycznej mogą wywołać poważne konsekwencje, dlatego tak ważne są odpowiednie ich zabezpieczenie i ochrona. W tym celu stosuje się różnego rodzaju systemy elektroniczne, które gwarantują sprawne funkcjonowanie tych obiektów.



Efektywne zarządzanie systemami dozoru wizyjnego odgrywa kluczową rolę w dostarczaniu dokładnej informacji sytuacyjnej i wizualnego potwierdzenia ewentualnego zagrożenia. W przypadku instalacji, w której skład wchodzi wiele kamer, ważne, by system oferował inteligentne narzędzia do wyszukiwania, będące w stanie skutecznie i szybko znaleźć wymagane informacje. Ponadto istotne jest to, by system był zawsze dostępny, a jednocześnie chroniony przed nieautoryzowanym dostępem. Ważne jest również, by platforma do zarządzania materiałem wizyjnym była zdolna do integracji z innymi systemami.

W obliczu wielu różnych zagrożeń, nie tylko naturalnych, np. powodzi czy huraganu, ale również, a może przede wszystkim tych, których sprawcą są ludzie (ataki cybernetyczne, akty wandalizmu), przy projektowaniu systemów zabezpieczających należy kierować się przestrzeganiem norm i standardów. Dlatego w przypadku obiektów wrażliwych wykorzystuje się kamery mające niezbędne certyfikaty, wyposażone w obudowę wandaloodporną, wodoodporną, pyłoszczelną, a nawet przeciwwybuchową.

Wavestore VMS na straży ochrony obiektów infrastruktury krytycznej

Wavestore to produkowane w Wielkiej Brytanii nowoczesne oraz wszechstronne oprogramowanie do zarządzania materiałem wizyjnym (VMS), które zdobyło uznanie i popularność dzięki zaawansowanym funkcjom i możliwościom bezproblemowej integracji. Zostało zaprojektowane do obsługi różnych zadań związanych z monitorowaniem różnej wielkości instalacji, zarówno niewielkich, jak i rozległych. Platforma umożliwia zarządzanie, nagrywanie i analizowanie strumieni wizji pochodzących z kamer i enkoderów różnych producentów. Dzięki temu stanowi elastyczne rozwiązanie dla użytkowników już dysponujących infrastrukturą monitoringu wizyjnego. Zastosowanie inteligentnej analizy, łatwa integracja oraz przyjazny interfejs powodują, że Wavestore ustanawia nowe standardy, dostarczając użytkownikom narzędzi niezbędnych do zapewnienia bezpieczeństwa. Twórcy oprogramowania szczególną uwagę poświęcili ochronie danych, wykorzystując ich szyfrowanie i bezpieczne mechanizmy uwierzytelniania. Dzięki przestrzeganiu powszechnie stosowanych praktyk branżowych związanych z bezpieczeństwem Wavestore dba o integralność danych i eliminuje ryzyko nieautoryzowanego dostępu.

VMS Wavestore to nowoczesne i wydajne oprogramowanie, które znakomicie sprawdzi się w ochronie obiektów infrastruktury krytycznej. Oferuje szeroki zakres funkcji i możliwości, które pozwalają na skuteczne zarządzanie systemem monitoringu wizyjnego i reagowanie na zagrożenia. Wavestore polecany jest m.in. do:

- ochrony elektrowni i zakładów energetycznych w celu monitorowania obiektów i instalacji elektroenergetycznych, a także do wykrywania i reagowania na zagrożenia, takie jak pożary, sabotaż czy ataki cybernetyczne;
- ochrony obiektów przemysłowych w celu monitorowania hal produkcyjnych, magazynów i innych obiektów przemysłowych, a także do wykrywania i reagowania na zagrożenia, jak kradzieże, sabotaż czy awarie urządzeń;
- ochrony obiektów rządowych, takich jak urzędy, ambasady czy lotniska, a także do wykrywania i reagowania na zagrożenia związane z terroryzmem, szpiegostwem czy atakami cybernetycznymi.

Aby odpowiednio zabezpieczyć obiekty czy instalacje wchodzące w skład infrastruktury krytycznej, należy wykorzystać systemy niezawodne i umożliwiające szybkie reagowanie na zagrożenia. Taką gwarancję daje Wavestore VMS.

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

wavestore
Innovation with integrity

Wavestore VMS

inteligentne oprogramowanie do zarządzania wideo

- Elastyczne zarządzanie pamięcią masową z poziomu oprogramowania
- Skalowalność - łączna pojemność dyskowa systemu do 520 PB
- Integracja z systemami różnych producentów
- Zaawansowana, inteligentna analiza wideo

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

urmet MIWI

Axxon One 2.0: nowa generacja oprogramowania VMS

Axxon One to oprogramowanie do zarządzania materiałem wizyjnym, odpowiednie zarówno dla małych, jak i dużych instalacji, także w przypadku wdrożeń obejmujących wiele lokalizacji. Wersja VMS Axxon One 2.0 wnosi kolejne ulepszenia, czyniąc to oprogramowanie jeszcze bardziej inteligentnym.

Wśród nowych funkcji oprogramowania VMS Axxon One na szczególną uwagę zasługują integracja z wieloma systemami bezpieczeństwa fizycznego, nowe możliwości funkcji analitycznych bazujących na sztucznej inteligencji, zwiększony poziom cyberbezpieczeństwa, lepsza wydajność i rozszerzone możliwości chmury.

Integracja z systemami bezpieczeństwa fizycznego

Axxon One 2.0 integruje się z systemami różnych producentów oraz uniwersalnym interfejsem OPC Data Access Wrapper. Obejmuje to systemy kontroli dostępu, przeciwpożarowe, antywłamaniowe oraz systemy ochrony obwodowej. Program odczytuje ustawienia podłączonych urządzeń, automatycznie dodając je do swojej konfiguracji. Tworzy powiązania między sygnałami z kamer a zdarzeniami z systemów zintegrowanych, umożliwiając konfigurację interakcji za pomocą automatycznych scenariuszy.

Integracje z urządzeniami IP

Sterowniki Generic do urządzeń ONVIF i wiodących producentów kamer umożliwiają obsługę niemal wszystkich kamer IP. Axxon One odbiera także dane z urządzeń POS i koreluje je z materiałem wideo, zapewniając pełny obraz zdarzeń, do jakich dochodzi przy kasach, i ułatwia wykrywanie naruszeń.

Analityka wideo z wykorzystaniem algorytmów SI

Nowe funkcje obejmują dynamiczne maskowanie prywatności, rozpoznawanie marki i modelu pojazdu oraz wyszukiwanie po podobieństwach *(Similarity Search)*. Wprowadzono również funkcję dynamicznego maskowania prywatności – zoptymalizowany algorytm maskuje poruszające się obiekty w czasie rzeczywistym, korzystając z minimum mocy obliczeniowej.

Detekcja SI znajduje zastosowanie w maskowaniu specyficznych klas obiektów (np. osób), a także w rozpoznawaniu w czasie rzeczywistym klasy, marki, modelu i koloru pojazdów, nawet tych będących w ruchu.

Na sztucznej inteligencji bazuje także wyszukiwanie wg podobieństw. Pozwala ono błyskawicznie wyszukać osoby o podobnej sylwetce na podstawie klatki wideo lub zdjęcia. Wyszukiwanie zdarzeń tworzonych przez analityki SI jest możliwe zarówno w wersji działającej lokalnie na komputerze, jak i w wersji webowej programu.

Zwiększone cyberbezpieczeństwo

Axxon One 2.0 zapewnia bezpieczne połączenia *end-to-end* przy użyciu protokołu HTTPS i szyfrowania TLS oraz bezpieczne połączenia kamer z serwerami Axxon One VMS. Aplikacja wymusza okresową zmianę haseł i wymaga ustawiania silnych haseł.

Większa wydajność

Axxon One może teraz odbierać i przetwarzać trzy lub więcej strumieni wizyjnych z kamery IP, optymalizując zużycie zasobów. GreenStream działa precyzyjniej, dobierając optymalny strumień do wyświetlania. Wprowadzono też liczne poprawki efektywności i wydajności analityki wideo wykorzystującej algorytmy SI.

Poprawione walory użytkowe

Zarządzanie prawami użytkowników zostało przebudowane tak, aby ułatwić administrowanie dużymi systemami monitoringu wizyjnego. Wprowadzono domyślne prawa dostępu do kamer, zależne od uprawnień użytkowników (zniesiono limit jednej roli na użytkownika). Pracę ułatwiają także wielopoziomowe interaktywne mapy obsługujące OpenStreetMap i Google Maps.

Praca w chmurze oraz klient webowy

Zainstalowany lokalnie klient może łączyć się z serwerami umieszczonymi w wielu lokalizacjach za pośrednictwem prywatnej chmury. Klient webowy obsługuje wyświetlanie wielu kamer jednocześnie w trybach na żywo i archiwum.

Dekodowanie wideo w formacie H.265 może odbywać się poprzez kartę graficzną (GPU), co zmniejsza obciążenie procesora (CPU). AxxonVSaaS Datacenter oferuje nowe możliwości połączeń *camera-to-cloud* oraz zgodność z wiodącymi usługami masowego przechowywania danych w chmurze. ●

AxxonSoft Polska
ul. Olszańska 5H
31-513 Kraków
https://pl.axxonsoft.com/

AI BOX PRO 2. generacji – nowy wymiar inteligentnego monitoringu

W roku 2023 trendy na rynku systemów zabezpieczeń technicznych zostały zdominowane przez analizę wideo i algorytmy oparte na sztucznej inteligencji.

Można zaryzykować stwierdzenie, że zmieniły one polski rynek zabezpieczeń, powodując, że mamy teraz do czynienia z coraz większą liczbą nadzorowanych zdalnie obiektów wyposażonych w rejestratory sieciowe i kamery IP analizujące obraz samodzielnie lub wysyłające strumienie do różnego rodzaju systemów analizujących.

W ten trend wpisuje się całkowicie nowatorskie rozwiązanie – nowy model inteligentnego nadajnika wideoalarmów AI BOX 2.1. Zastosowanie procesora Texas Instruments z serii automotive pozwala na większy zakres temperatury pracy od -30° do +70°C. Większa liczba punktów AI to więcej aplikacji analitycznych pracujących jednocześnie. Nowy procesor zapewnia zgodność urządzenia z dyrektywą NDAA *(National Defense Authorization Act)*. Jest to akt prawny wydany przez Stany Zjednoczone, jednakże jego wpływ w Europie jest coraz bardziej odczuwalny.

Więcej algorytmów AI

AI BOX 2.1 oferuje nowe aplikacje bazujące na analizie układu ciała człowieka i sposobu jego gestykulacji. Do tej pory stosowano rozwiązanie polegające na przypisywaniu obiektów do określonej grupy (np. ludzi) i sprawdzeniu, czy znajdują się w określonym obszarze, czy też przekraczają dozwoloną granicę. Najnowsze algorytmy behawioralne badają układ ciała człowieka, jego ułożenie oraz gestykulację. To zupełnie nowy wymiar analizy. Dzięki temu model AI BOX oferuje funkcje umożliwiające sprawdzenie, czy nie doszło do:

- naruszenia granicy strefy dłonią lub stopą (akt wandalizmu),
- celowego spoglądania w określonym kierunku,
- bezpośredniego zagrożenia (dwie osoby stoją naprzeciwko siebie, jedna z nich trzyma ręce podniesione, co może sugerować grożenie niebezpiecznym przedmiotem).

W najnowszym modelu AI BOX poprawiono skuteczność aplikacji z zakresu BHP, wyposażając je w funkcję rozpoznawania braku osobistej ochrony oraz upadku osoby. Na rynku jest coraz większe zapotrzebowanie na tego typu analizę. Wraz z detekcją dymu i ognia daje to pełny zestaw aplikacji zabezpieczających np. place budów. To zupełnie nowy kierunek rozwoju i poszerzenie oferty dla instalatorów oraz agencji ochrony.

W tym wydaniu AI BOX dostępne są też aplikacje skierowane do firm z sektora sprzedaży detalicznej. Umożliwiają np. pomiar liczby osób przebywających w sklepie, z podziałem na ich płeć, a dzięki mapom ciepła możliwy jest pomiar odwiedzania określonych obszarów w funkcji czasu. Dane zebrane przez wspomniane aplikacje mogą posłużyć do analizy skuteczności akcji promocyjnych, odpowiedniego obsadzenia stanowisk sprzedażowych czy też wspomóc podejmowanie decyzji dotyczących rozłożenia produktów. Dopracowany został również filtr obiektu minimalnego i maksymalnego. Pozwala to na uwzględnienie zmiany wielkości obiektów wraz ze zmianą odległości od kamery.

Idealne zastosowanie dla wież mobilnych

AI BOX 2.1 został zaprojektowany specjalnie dla wież mobilnych, których liczba w Polsce stale wzrasta. Urządzenie jest wyposażone w modem LTE oraz odbiornik GPS z antenami zewnętrznymi, a także dysk twardy SSD do rejestracji wideo. Tym samym AIBOX 2.1 stanowi autonomiczną jednostkę centralną, eliminując konieczność stosowania dodatkowych urządzeń typu router czy rejestrator. Niewielki pobór mocy 16 W sprawdzi się na wieżach, które w zdecydowanej większości są pozbawione zasilania sieciowego i bazują na energii z akumulatorów, paneli fotowoltaicznych lub ogniw paliwowych. ●

CBC (Poland)
Ul. Rydygiera 8 bud.17, 01-793 Warszawa
handlowy@cbcpoland.pl
www.cbcpoland.pl

Głos się niesie, czyli donośna rola głośników IP

Do czasu pojawienia się głośników IP systemy wizyjne miały w zasadzie dwie funkcje. Pierwsza, umożliwienie pracownikom ochrony zdalnej obserwacji terenu i podjęcie decyzji, czy należy wyruszać z interwencją. Druga, nagrywanie obrazu. Dzięki głośnikom IP ochrona może od razu interweniować. Czasami bowiem wystarczy stanowcze polecenie, by wandal odstąpił od czynu, a złodziej odłożył rzeczy na półkę.

Jan T. Grusznic, a&s Polska

Głośniki IP okazały się nieocenionym narzędziem służącym bezpieczeństwu. Mogą odtwarzać nagrane komunikaty, ale posłużą też operatorowi, aby zareagować na bieżąco na to, co widzi dzięki systemom wizyjnym. W efekcie ułatwiają zapobieganie niepożądanym incydentom i kradzieżom. Doświadczenie firm świadczących usługi ochrony dowodzi, że w połowie przypadków komunikat z głośnika odstraszył intruza lub złodzieja.

Zastosowanie systemów audio może różnić się w zależności od przyjętych rozwiązań, poziomu integracji z innymi urządzeniami lub platformami oraz procedur. Pełna automatyzacja zakłada, że konkretne, zdefiniowane wcześniej zdarzenie (np. wykrycie ruchu w kamerze, aktywacja czujki ruchu, naruszenie bariery itp.) spowoduje odtworzenie komunikatu. Komunikaty głosowe na żywo zakładają zestawienie aktywnego połączenia audio między głośnikiem IP a urządzeniem (np. stacja wywoławcza IP albo telefon VoIP po protokole SIP) lub oprogramowaniem (np. VMS za pomocą *ONVIF audio backchannel*), dzięki temu operator może użyć głośnika.

Głośniki IP są idealnym dodatkiem do systemów dozoru wizyjnego, a ochrona obwodowa jest ważnym, ale nie jedynym przykładem ich zastosowania. Dzięki nim można np. szybko informować duże grupy osób o grożącym im niebezpieczeństwie. Możliwe jest też automatyczne odtworzenie wiadomości dźwiękowej w sytuacji awaryjnej (np. informującej o wycieku niebezpiecznej substancji).

Więcej niż głośnik

Określenie „głośniki IP" nie do końca oddaje prawdziwy charakter tych urządzeń. W istocie każdy taki głośnik jest zaawansowanym urządzeniem audio z wbudowanym wzmacniaczem, cyfrowym procesorem sygnału i zasilanym przez PoE. Ponieważ są to urządzenia sieciowe, możliwe jest zdalne sterowanie nimi, a co za tym idzie zarządzanie plikami audio, ustawianie priorytetów komunikatów i harmonogramów oraz monitorowanie stanu urządzeń. Niektóre mają funkcję automatycznego testu. Są też takie, które umożliwiają tworzenie stref audio. W tym ostatnim przypadku jeden z głośników staje się dla pozostałych „serwerem", umożliwiając zsynchronizowane emitowanie komunikatów i odtwarzanie muzyki. Podział systemu na strefy umożliwia dostosowanie głośności do różnych typów komunikatów (np. alarmowy głośniejszy) oddzielnie dla każdej strefy. Zmiany w konfiguracji strefy wprowadzane są bez konieczności instalacji nowego okablowania oraz fizycznej obecności obsługi.

W przypadku dźwięku sieciowego sygnał jest przesyłany cyfrowo, bez konwersji sygnału analogowego na cyfrowy i odwrotnie. Dlatego sygnał pozostaje silny bez względu na to, jak długie są kable, a dźwięk wydobywający się z głośnika jest wyraźny.

W głośnikach IP na ogół nie chodzi o szeroki zakres częstotliwości czy uzyskanie dźwięku stereo. Dla celów bezpieczeństwa maksymalizuje się głośność tego zakresu częstotliwości, w przypadku którego ludzka mowa jest najbardziej zrozumiała: od ok. 85 Hz (najniższa dla mężczyzny) do ok. 8 kHz (dla kobiety). Nawet, gdy głośnik IP jest używany do odtwarzania muzyki w tle, natężenie dźwięku jest dość niskie. Głośniki sieciowe są wyposażone w funkcje cyfrowego przetwarzania sygnału zapewniające optymalizację częstotliwości (dzięki czemu każde urządzenie ma taką samą charakterystykę, bez konieczności ręcznego dostrajania lub konfigurowania), kompensację głośności (przy niskim poziomie dźwięku niektóre częstotliwości są mniej słyszalne dla ludzkiego ucha – kompensacja wzmacnia te częstotliwości, aby komunikaty, mimo muzyki w tle były zrozumiałe) i kontrolę zakresu dynamiki (wygładza poziomy), aby zapewnić wysoką jakość dźwięku w niemal każdym środowisku.

Nie zawsze im głośniej, tym lepiej

Głośniki różnią się między sobą formą, ciśnieniem akustycznym, czułością, charakterystyką częstotliwości czy możliwościami montażu. Niektóre ich typy będą bardziej odpowiednie do nadawania komunikatów w hałaśliwym otoczeniu, a inne lepiej się sprawdzą w małych przestrzeniach.

Głośnik tubowy ma wysoki poziom ciśnienia akustycznego (>110 dB) i maksymalizuje głośność tych częstotliwości, na które ludzkie ucho jest najbardziej wrażliwe. Oznacza to, że wiadomość może być przekazywana tak wyraźnie, jak to tylko możliwe. Ze względu na swój kształt głośnik kieruje cały dźwięk w jednym kierunku, co dodatkowo zwiększa ciśnienie akustyczne. Głośnik tubowy może być używany w pomieszczeniach z wysokim poziomem tła akustycznego, takich jak magazyny i fabryki, lub w instalacjach zewnętrznych.

Głośniki zabudowane (w obudowie) oraz sufitowe zapewniają średni poziom ciśnienia akustycznego (<100 dB) i powinny być stosowane w cichszych miejscach, takich jak szpitale, szkoły, sklepy detaliczne lub budynki biurowe. Z uwagi na szeroki zakres częstotliwości lepiej nadają się do odtwarzania muzyki od głośników tubowych.

Poza oczywistą różnicą między sieciowymi a analogowymi systemami audio wynikającymi ze sposobu komunikacji nie istnieją inne znaczące. Do głównych zalet wynikających z wykorzystania komunikacji przez IP należą elastyczność i skalowalność: swoboda łączenia i możliwość optymalizacji lub rozbudowy systemu do dowolnego rozmiaru.

Planując sieciowy system audio, należy wziąć pod uwagę kilka kwestii:

1. **Przeznaczenie**. Czy system ma służyć tylko do nadawania komunikatów, czy będzie także odtwarzać muzykę? W pierwszym przypadku wystarczy minimalna konieczna liczba głośników. W drugim, musi być ich więcej, tak by muzyka brzmiała wszędzie tak samo.
2. **Poziom tła dźwiękowego**. Komunikaty głosowe będą zrozumiałe, jeśli będą o ok. 12 dB głośniejsze niż dźwięki z otoczenia.
3. **Współczynnik odbicia.** Duże powierzchnie odbijające mogą wprowadzać pogłos, a większe przestrzenie opóźnienie (efekt echa). Na zewnątrz można zainstalować zatem mniej głośników. We wnętrzach najlepsze jest umieszczenie głośnika tak, by dźwięk rozchodził się daleko w głąb pomieszczenia. Fala dźwiękowa rozprzestrzeni się swobodnie, ewentualne odbicie będzie niezauważalne. Umieszczenie głośnika w rogu pomieszczenia spowoduje nierównomierne wzmocnienie niskich częstotliwości i znaczne pogorszenie jakości dźwięku.
4. **Częstotliwość próbkowania.** Przy niskiej częstotliwości próbkowania części dźwięku nie są przechwytywane, a ogólna jakość dźwięku będzie gorsza. Przy wyższej częstotliwości próbkowania strumień audio może być bardziej poprawnie odtworzony, zapewniając wyższą jakość.
5. **Zastosowany kodek.** Do odtwarzania muzyki zalecany jest AAC *(Advanced Audio Coding)*, znany również jako MPEG-4 AAC. G.711 i G.726 to kodeki używane głównie w telefonii IP. Mają one niższe opóźnienie i wymagają mniej mocy obliczeniowej niż AAC, ale skutkiem tego jest gorszej jakości dźwięk.

Przykłady głośników tubowego i w obudowie prezentujemy na następnej stronie. →

ASCS

Głośnik tubowy IP – VCLH301P

Cecha	VCLH301P
Wzmacniacz	klasa D, 10 W
Charakterystyka częstotliwości	350-10 kHz
Maks. poziom ciśnienia dźwięku	120 dB
Czułość	110 dB (1W/1M)
Standard PoE	802.3af klasa 0
Wbudowany mikrofon	Nie, 1x wejście mikrofonowe
Liczba wewnętrznych komunikatów	64
Priorytety komunikatów	Tak
Grupowanie głośników w strefę	Tak
Kompresja audio	g.711a, g.711u, g.726, g.722
Liczba wejść / wyjść	17/3
Obsługa ONVIF	Nie
Obsługa protokołu SIP	Tak
Klasa szczelności	IP-66
Temperatura pracy	Od -40°C do 70°C

VCLH301P jest głośnikiem tubowym IP wykonanym z samogasnącego ABS zgodnie z normą UL94V0. Posiada stopień ochrony IP-66, może więc być stosowany zarówno wewnątrz, jak i na zewnątrz obiektu.
Głośnik może zostać zarejestrowany w serwerze V-Cast, usłudze chmurowej V-Cast Cloud lub na dowolnym serwerze SIP. Może również pracować w trybie bezserwerowym *Peer-To-Peer* (P2P). Głośnik umożliwia realizację połączeń indywidualnych, wywołań grupowych i ogólnych, a także przechowywanie nagranych komunikatów alarmowych w wewnętrznej pamięci. Komunikaty mogą być odtwarzane w zależności od aktualnego stanu głośnika, aktywowane podczas połączenia (DTMF) lub za pośrednictwem wywołań http oraz poprzez protokół Modbus IP. Po podłączeniu mikrofonu istnieje możliwość wykonywania testu tonowego oraz prowadzenia nasłuchu czy rozmowy.

Więcej na www.v-cast.pl/produkty

Axis Communications

Sieciowy projektor dźwięku – AXIS C1610-VE

Cecha	AXIS C1610-VE
Wzmacniacz	klasa D, 7 W
Charakterystyka częstotliwości	200Hz do 16 kHz
Maks. poziom ciśnienia dźwięku	106 dB
Czułość	-
Standard PoE	802.3af/802.3at, klasa 3
Wbudowany mikrofon	Tak
Liczba wewnętrznych komunikatów	50
Priorytety komunikatów	Tak
Grupowanie głośników w strefę	Tak
Kompresja audio	AAC, G.711, G.726
Liczba wejść / wyjść	2 konfigurowalne
Obsługa ONVIF	Nie
Obsługa protokołu SIP	Tak
Klasa szczelności	IP66, IK10
Temperatura pracy	Od -40° do + 55°C

AXIS C1610-VE jest sieciowym projektorem dźwięku do instalacji wewnątrz oraz na zewnątrz pomieszczeń. Gwarantuje czyste brzmienie komunikatów głosowych oraz nadawanej muzyki. Wbudowane wzmacniacz, cyfrowy procesor dźwięku oraz oprogramowanie do zarządzania małymi i średnimi systemami audio pozwalają na szybką i łatwą implementację jako elementy systemu audio.
Dzięki zastosowaniu otwartych standardów głośnik ten można łatwo zintegrować z systemami dozoru wizyjnego, kontroli dostępu oraz VoIP (obsługa protokołu SIP).

Więcej na www.axis.com/pl-pl

Nowy system audio IP od Hanwha Vision

Hanwha Vision, globalny dostawca rozwiązań wizyjnych, wprowadził na rynek nowy system audio IP. Dodaje on atrakcyjne możliwości audio do wiodącej oferty Hanwha Vision w zakresie dozoru wizyjnego, podnosząc bezpieczeństwo na kolejny poziom. System może być obsługiwany niezależnie, jako samodzielne rozwiązanie, lub może być połączony z systemem monitoringu wizyjnego. Obsługuje również protokół SIP *(Session Initiation Protocol)*, który jest standardem dla połączeń internetowych *(VoIP-Voice over IP)*.

System umożliwia instalację od 1 do 512 głośników. Maksymalnie 256 głośników może być obsługiwanych bez serwera audio, w razie większej liczby głośników (do 512) wymagany jest serwer audio.

System IP Audio może nadawać komunikaty w czasie rzeczywistym lub nagrane wcześniej, w tym komunikaty TTS (zmiana tekstu na mowę) wydawane przez centrum sterowania. Oprócz komunikatów publicznych mogą one zapobiegać przestępczości lub zachowaniu antyspołecznemu. Komunikaty mogą być również nadawane przez mikrofon.

Może być stosowany do udostępniania wiadomości lub muzyki w miejscach publicznych, w tym na dworcach kolejowych, w małych obiektach handlowych, szpitalach, szkołach i innych. W połączeniu z monitoringiem wizyjnym, system uzupełnia ochronę strefową o ostrzeżenia dźwiękowe w przypadku wykrycia potencjalnego naruszenia granic określonego obszaru wirtualnego. Jeśli system wykryje na wyznaczonym obszarze ludzką aktywność, która wskazuje na możliwe naruszenie granicy, może przekazać komunikat dźwiękowy z prośbą o zaprzestanie działania.

Integracja z funkcjami analitycznymi oferuje kilka zastosowań. Umożliwia np. wykrycie osoby, która stoi zbyt blisko innej osoby podczas korzystania z bankomatu. W tym przypadku emitowane jest ostrzeżenie dźwiękowe zalecające zachowanie odpowiedniej odległości. Oferuje też możliwości, z których mogą skorzystać sprzedawcy w małych obiektach handlowych. Przykładowo, jeśli klient stoi i patrzy na produkt z zainteresowaniem przez dłuższy czas, może zostać nadana wiadomość do klienta o specjalnych ofertach w sklepie, które mogą przekonać go do zakupu. Podobnie, jeśli konieczna jest ewakuacja sklepu lub centrum handlowego, instrukcje mogą być jasno przekazane za pośrednictwem systemu.

Intuicyjny pulpit nawigacyjny pozwala operatorom szybko skontrolować poszczególne głośniki, graficzny pasek pokazuje sygnał wyjściowy głośnika. Operatorzy mogą szybko zweryfikować, że głośnik emituje dźwięk zgodnie z oczekiwaniem, nawet jeśli nie są na miejscu.

Bezpieczeństwo fizyczne w pracy hybrydowej: zagrożenia i środki ochrony

Praca hybrydowa, czyli taka, która łączy pracę zdalną i obecność w biurze, stała się codziennością w erze cyfrowej, a jej popularność zwiększyła się po pandemii COVID-19. Ten model oznacza nowe wyzwania dotyczące bezpieczeństwa fizycznego osób pracujących hybrydowo.

Piotr Świderski

Jednym z takich wyzwań jest zmierzenie się z zagrożeniami bezpieczeństwa fizycznego, zarówno w miejscu pracy, jak i podczas pracy z domu. Przyjrzymy się, jakie konsekwencje niosą te zagrożenia oraz jakie środki ochrony możemy wdrożyć, aby zminimalizować ryzyko.

Praca hybrydowa i jej wpływ na sektor security

Praca hybrydowa powoduje, że pracownicy pojawiają się w biurze nieregularnie, często w długich odstępach czasu. To oznacza, że ewentualne zgubienie karty dostępu przez długi czas pozostaje niewykryte. W wyniku tego aktywna karta może krążyć bez nadzoru i może zostać użyta przez osobę nieupoważnioną. System tzw. gorących biurek powoduje, że pracownicy nie zawsze się osobiście znają, co prowadzi do tego, że nie reagują na widok obcych twarzy. To z kolei oznacza ryzyko, że osoby spoza firmy mogą swobodnie przemieszczać się po jej terenie, zwłaszcza jeśli dysponują kartą zgubioną wcześniej przez uprawnionego użytkownika.

Organizacja biur w stylu open space w połączeniu z tym, że w firmie funkcjonuje np. tylko jeden punkt kontroli dostępu (lub jest ich niewiele), ułatwia dostęp do całej biurowej przestrzeni. W efekcie wzrasta ryzyko, że w firmie będą się poruszać osoby nieuprawnione, szczególnie jeśli niedostateczne reguły bezpieczeństwa powodują, że pracownicy mają takie same prawa dostępu do różnych pomieszczeń. Realne ryzyko związane z taką sytuacją powinno stanowić dla naszej branży impuls do podjęcia działań prewencyjnych.

To oczywiste, że optymalizacja wykorzystania powierzchni biurowych, jaką umożliwia praca w systemie hybrydowym, może przynieść znaczne oszczędności. Jednocześnie rośnie ryzyko, że nieuprawniony dostęp osób trzecich do stref chronionych i swobodne poruszanie się po nich staje się bardzo prawdopodobne. Może to prowadzić np. do fali kradzieży. W wielu firmach jest przecież możliwość wypożyczenia krzesła czy monitora do domu, a do tego prawie każdy pracownik po zakończonej pracy zabiera swój komputer. Dlatego nieznana osoba wychodząca z biura z komputerem nie wzbudzi niczyjej obawy – to sytuacja normalna.

Analogicznie jest z dokumentami i danymi, kary za ich utratę mogą być ogromne, nie wspominając o reputacji firmy.

Wpływ nowych technologii na sektor bezpieczeństwa fizycznego

Brak wytycznych dotyczących stosowanych w firmach rodzajów kart dostępu może powodować, że mogą być kopiowane za pomocą powszechnie dostępnych narzędzi. Kopiowanie kart starszego typu trwa zazwyczaj krócej niż 3 s. A nie jest praktyką rynkową ich okresowa wymiana. W firmach często są używane karty, które zostały wprowadzone wraz z uruchomieniem danego biura (czy systemu SKD) i stosuje się je przez cały okres działania systemów. I o ile za zwyczajne uważamy aktualizację oprogramowania komputera czy telefonu, które ma uczynić urządzenie bezpieczniejszym, o tyle nie ma zwyczaju aktualizacji kart dostępu.

Korzystanie z systemów i rozwiązań, które oferuje budynek

Często wystarczy fakt, że budynek ma system kontroli dostępu służący także do obsługi dostępu do wynajętej powierzchni. Takie rozwiązanie powoduje, że w proces nadawania dostępów, zmiany uprawnień karty lub wydania karty zaangażowane są osoby zajmujące się obsługą nieruchomości. Brak bezpośredniego zarządzania systemami kontroli dostępu powoduje, że zmiany w systemie nie są w 100% widoczne dla firmy użytkującej powierzchnię biurową. Nie może więc ona dokonać fizycznego sprawdzenia, czy zagubiona karta została zablokowana w systemie. Pozostaje weryfikacja raportów. A to oznacza, że ewentualne błędy mogą zostać wykryte w późniejszym czasie.

Należy też zwrócić uwagę na bezpieczeństwo pracy w biurze domowym. Po wejściu w życie przepisów regulujących pracę hybrydową pracodawca jest zobowiązany m.in. do zapewnienia pracownikowi zdalnemu materiałów i narzędzi pracy, w tym urządzeń technicznych, niezbędnych do pracy zdalnej. Regulacje dotyczą jednak głównie BHP, a co z sektorem security? Ten aspekt wymaga jeszcze wypracowania przez branżę dobrych praktyk. Warto wiedzieć, że zgodnie z informacją opublikowaną w sierpniu 2023 r. przez Państwową Inspekcję Pracy od momentu ogłoszenia stanu zagrożenia epidemicznego, czyli od 14 marca 2020 r., podczas wykonywania pracy zdalnej doszło do 23 wypadków, w których śmierć poniosło 17 osób.

» W obliczu rosnącego ryzyka ważne, aby firmy skoncentrowały się na wdrożeniu skutecznych środków ochrony, takich jak nowoczesne technologie, zaktualizowane procedury bezpieczeństwa oraz regularne szkolenia pracowników. «

Co można zrobić, by zmniejszyć ryzyko zagrożeń związanych z pracą hybrydową? Na to pytanie odpowiedzi będą zapewne różne w zależności od wyników analizy ryzyka przeprowadzonej w firmie, jednak część zaleceń będzie wspólna. Rekomendowane działania to m.in.:

- wprowadzenie odpowiednich procedur bezpieczeństwa, takich jak polityka czystego biurka;
- zarządzanie kartami dostępu wspomagane automatyczną kontrolą statusu pracownika, który można uzyskać poprzez łączenie się z bazą prowadzoną np. przez dział HR;
- korzystanie z oddzielnych stref dostępu do pomieszczeń biurowych i zarządzanie nimi z poziomu firmy;
- wprowadzenie kart mobilnych na telefonach służbowych;
- zmniejszenie czasu aktywności kart dla osób niekorzystających z biur (np. karta nieużywana przez 30 dni zostaje automatycznie zablokowana);
- ustalenie fizycznego standardu kart (aby wyeliminować te rozwiązania, co do których wiadomo, że umożliwiają kopiowanie kart lub ich emulację);
- wprowadzenie anonimizacji karty (brak możliwości połączenia znalezionej karty dostępu z danym pracownikiem lub konkretnym biurem);
- wprowadzenie cyklicznych szkoleń dla pracowników o zagrożeniach wynikających z pracy hybrydowej;
- wprowadzenie identyfikatorów dla pracowników;
- uruchomienie numerów alarmowych służących do zgłaszania podejrzanego zachowania;
- wprowadzenie kontroli dostępu z funkcją Anti Passback;
- w przypadku niektórych stref wprowadzenie podwójnej weryfikacji (np. karta i kod dostępu).

Adaptacja do hybrydowego modelu pracy stawia przed sektorem zabezpieczeń nowe wyzwania. W obliczu rosnącego ryzyka ważne, aby firmy skoncentrowały się na wdrożeniu skutecznych środków ochrony, takich jak nowoczesne technologie, zaktualizowane procedury bezpieczeństwa oraz regularne szkolenia pracowników. Bezpieczeństwo fizyczne w pracy hybrydowej staje się kluczowym obszarem, który wymaga ciągłego dostosowywania się do zmieniającego się otoczenia, aby skutecznie chronić pracowników, sprzęt i dane firmowe. ●

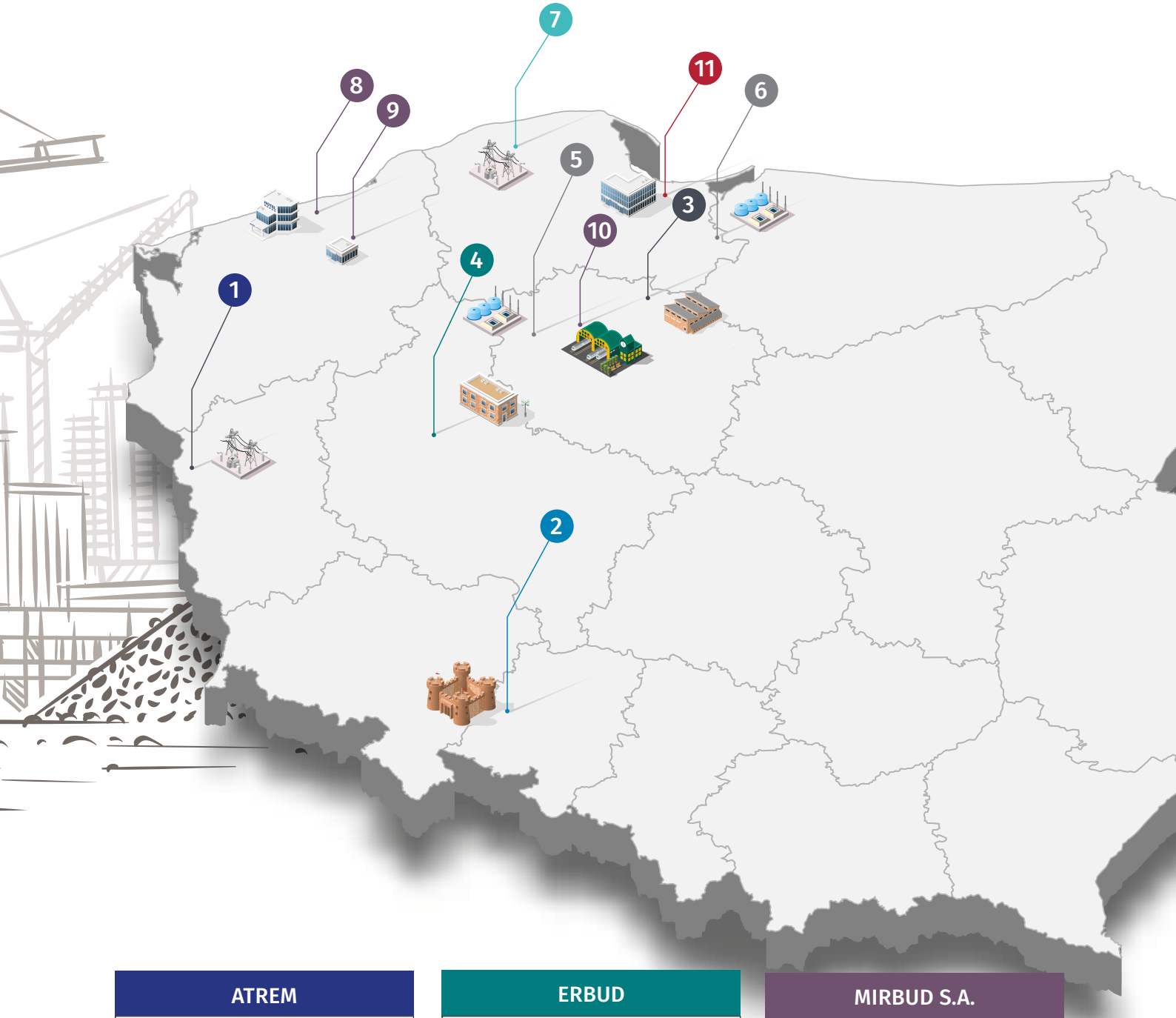
Piotr Świderski

Absolwent PW Wydział Mechatroniki (mgr inż.). Ponad 10 lat doświadczenia w sektorze bezpieczeństwa. Obecnie Territory Security Leader w PwC.

Mapa inwestycji

W „A&S Polska” już po raz siódmy prezentujemy mapę dużych inwestycji, które są obecnie realizowane lub dopiero się rozpoczynają. Włączyliśmy do naszego zestawienia projekty, których zakończenie planowane jest nie wcześniej niż w drugim kwartale 2024 roku. Warto zaznaczyć, że nasza selekcja nie jest ograniczona do branży przemysłowej. Koncentrujemy się na dużych inwestycjach prowadzonych przez renomowane firmy, które mogą stanowić potencjalne możliwości współpracy dla przedsiębiorstw działających w sektorze bezpieczeństwa. Ponadto zachęcamy do zapoznania się z wcześniejszymi numerami „a&s” z ubiegłego roku, w których omawialiśmy inne długoterminowe projekty, uwzględniając Państwa zainteresowania oraz profil działalności.

Adela Prochyra, a&s Polska



ATREM

Co: **BUDOWA GPZ SŁUBICE STREFA Z POWIĄZANIAMI LINIOWYMI 110 KV I 15 KV**

Gdzie: Słubice

Kiedy: 120 tygodni od 11.12.2023

1

B-ACT S.A.

Co: **PRZEBUDOWA BUDYNKU DAWNEGO GIMNAZJUM PIASTOWSKIEGO W BRZEGU WRAZ Z ADAPTACJĄ NA CELE MUZEALNE I ZAGOSPODAROWANIEM TERENU DLA MUZEUM DZIEDZICTWA I KULTURY KRESÓW**

Gdzie: Brzeg

Kiedy: brak informacji

2

DEKPOL S.A.

Co: **WYKONANIE W FORMULE „ZAPROJEKTUJ I WYBUDUJ" DWÓCH HAL MAGAZYNOWO-PRODUKCYJNYCH Z ZAPLECZAMI SOCJALNO-BIUROWYMI WRAZ Z INFRASTRUKTURĄ TOWARZYSZĄCĄ**

Gdzie: Swarożyno, gmina Tczew

Kiedy: I etap – II kwartał 2024
II etap – realizacja drugiej hali jest opcjonalna i jej zakończenie nastąpi w terminie 7,5 miesięca od daty wywołania do realizacji

3

ERBUD

Co: **ROZPOCZĘCIE REWITALIZACJI STAREJ RZEŹNI W POZNANIU**

Gdzie: Poznań

Kiedy: 6 lat

4

MDI ENERGIA S.A.

Co: **BUDOWA ELEKTROCIEPŁOWNI NA BIOGAZ ROLNICZY O MOCY 0,999 MW WRAZ Z URUCHOMIENIEM**

Gdzie: Bagdad w gminie Wyrzysk

Kiedy: 4 miesięcy od dnia podpisania umowy (29.08.2023)

5

Co: **BUDOWA ELEKTROCIEPŁOWNI NA BIOGAZ ROLNICZY O MOCY 0,999 MW WRAZ Z URUCHOMIENIEM**

Gdzie: Półwieś, w gminie Zalewo

Kiedy: 14 miesięcy od dnia podpisania umowy (29.08.2023)

6

POLIMEX MOSTOSTAL S.A.

Co: **BUDOWA PRZYŁĄCZA LĄDOWEGO (CZĘŚĆ LNIOWA I CZĘŚĆ STACYJNA) WRAZ Z OKABLOWANIEM DLA MFW BALTICA-2**

Gdzie: Choczewo

Kiedy: 1.02.2028

7

MIRBUD S.A.

Co: **BUDOWA W SYSTEMIE POD KLUCZ OBIEKTU APARTAMENTOWEGO I HOTELOWEGO, TJ. ZESPOŁU BUDYNKÓW LECZNICTWA UZDROWISKOWEGO PRZY UL. MORAWSKIEGO W KOŁOBRZEGU**

Gdzie: Kołobrzeg

Kiedy: brak informacji

8

Co: **UZBROJENIE TERENÓW INWESTYCYJNYCH POD FUNKCJĘ PRZEMYSŁOWĄ W PÓŁNOCNEJ CZĘŚCI MIASTA SŁUPSKA W SYSTEMIE ZAPROJEKTUJ – WYBUDUJ**

Gdzie: Słupsk

Kiedy: 32 miesiące od podpisania umowy (30.11.2023)

9

Co: **BUDOWA, PRZEBUDOWA ORAZ ZMIANA SPOSOBU UŻYTKOWANIA OBIEKTÓW ZAJEZDNI TRAMWAJOWEJ PRZY UL. TORUŃSKIEJ 278 W BYDGOSZCZY – ETAP 1**

Gdzie: Etap 1

Kiedy: Będzie podany po podpisaniu umowy

10

UNIBEP S.A.

Co: **REALIZACJA W TECHNOLOGII MODUŁOWEJ BUDYNKU USŁUGOWEGO ORAZ CZTERECH BUDYNKÓW MIESZKALNYCH WIELORODZINNYCH**

Gdzie: Gdańsk

Kiedy: 9 miesięcy od podpisania umowy (1.12.2023)

11

O(d)porność w bezpieczeństwie

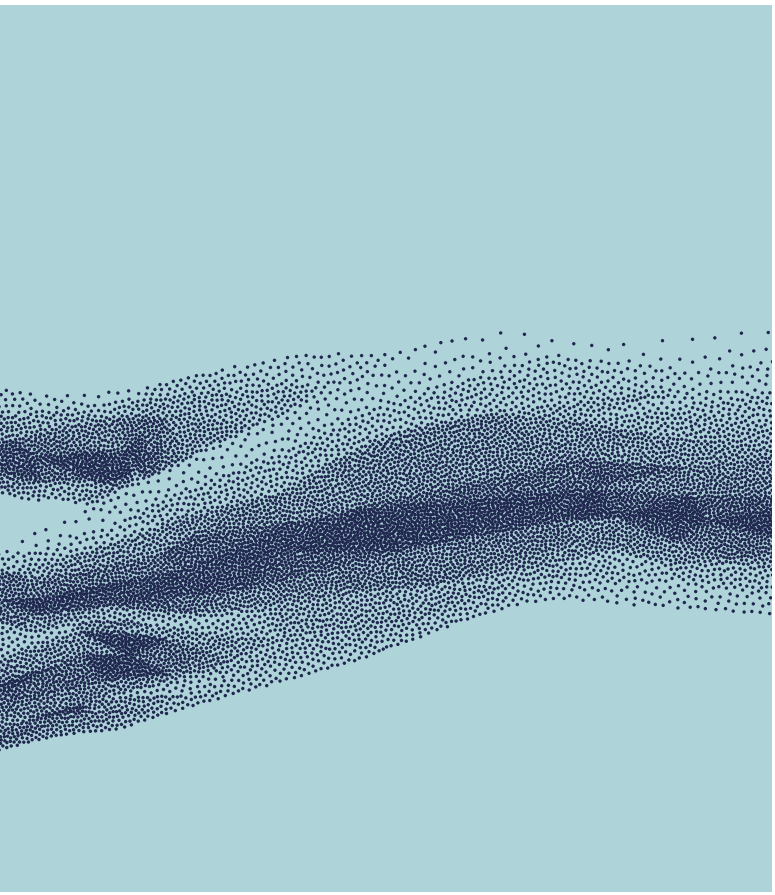
Krajobraz zapewniania szeroko rozumianego bezpieczeństwa się zmienia. Nietrudno zauważyć, że w ostatnim czasie dynamika tych zmian nabiera tempa. W ostatnich miesiącach doszło do dwóch dużych wycieków danych, które powinny zainteresować specjalistów z obszaru security.

Tomasz Dacka

Mowa oczywiście o atakach typu *ransomware* wymierzonych w firmy Naftor oraz ALAB. W związku z tymi incydentami nasuwa się pytanie, ile sił i środków powinniśmy poświęcać na typowo defensywne zadania, a ile na zwinną umiejętność do poruszania się w środowiskach skompromitowanych lub uznanych za skompromitowane. Jak powinien układać się między nimi podział procentowy?

Czym jest odporność?

Wiele już napisano i powiedziano o odporności. Wciąż natomiast odnoszę wrażenie, że nie do końca wiadomo, czym tak naprawdę jest odporność, jakie korzyści zapewnia, a jakie pociąga koszty. Pierwsze, co przychodzi na myśl (w większości znanych mi przypadków), kiedy mowa o odporności, to typowa defensywa. Budujemy mur, wykopujemy fosę, stawiamy straż i nikt nam nic nie zrobi, przetrwamy. Zakładam, że nawet w czasach, gdy rzeczywiście takie aktywności miały miejsce, i tak to do końca nie działało. Obecne struktury organizacyjne są na tyle skomplikowane, że nawet same dla siebie stanowią pewne wyzwanie. Najlepiej widać to chociażby



po środkach bezpieczeństwa bazujących na systemach zabezpieczeń elektronicznych. Dość szybko ewoluowaliśmy od ogólnego pojęcia system „cyfrowy" do pojęcia integracji, unifikacji i dalej sztucznej inteligencji opartej na sieciach neuronowych. Ponieważ trudno nam zrozumieć i z zyskiem wykorzystać nowe technologie, to stajemy się narażeni na materializację ryzyk, jakie za sobą owe pociągają. Czy jesteśmy w stanie z ręką na sercu stwierdzić, że nasza sieć bezpieczeństwa nie była, nie jest i zapewne nie będzie skompromitowana i wszystkie przetwarzane w niej dane czy uprawnienia są bezpieczne? Byłbym daleki od takiego optymizmu nawet, jeśli korzystamy z najnowszych wytycznych, protokołów, aktualnych systemów (mury, fosa, wieże). Osobiście staram się nie mylić zbytniej pewności siebie ze świadomością sytuacyjną.

Ostatnie ataki na infrastrukturę teleinformatyczną świadczą o tym, że budowane latami mury w obliczu konfrontacji z nowymi zagrożeniami są dziurawe, a ich pokonanie, z perspektywy atakującego, jest w zupełności wystarczające do odniesienia celu ataku, stanowi tzw. SPOF *(Single Point of Failure)* rozumiany tutaj jako pojedynczy punkt, którego pokonanie (awaria) skutkuje poważnymi konsekwencjami z perspektywy bezpieczeństwa.

Należy więc odpowiedzieć na pytania, jak się w tym wszystkim odnaleźć i czy warto inwestować środki w defensywę. Odpowiedzi są łatwe i wiążą się z całą filozofią odporności. Celowo pominę, na potrzeby artykułu, kwestię analizy ryzyka czy BIA *(Business Impact Analysis,* analiza wpływu na biznes, głównie kluczowych procesów dla danej organizacji).

Skupiając się na systemach bezpieczeństwa fizycznego, mając za sobą wykonane wyżej wymienione analizy, możemy dobrać odpowiednie środki, które:

- odstraszą potencjalnego intruza;
- wykryją nieuprawniony dostęp (lub jego próby);
- wydłużą czas potrzebny napastnikowi do przejścia przez zabezpieczenia (dając nam tym samym więcej czasu na reakcję);
- uniemożliwią wykonanie zaplanowanych przez złych aktorów działań (np. dostęp do chronionych aktywów, zniszczenie lub kradzież mienia).

Wszystko to każdy z nas wielokrotnie przerabiał. Naturalną koleją rzeczy nasuwa się kolejne pytanie, co zrobić, kiedy wszystkie wymienione wyżej metody zawiodą. Jak mamy się zachować (w rozumieniu ludzi i obsługiwanych przez nich systemów), kiedy ryzyko zmaterializowało się tu i teraz. Z dużą dozą prawdopodobieństwa wdrożone są standardy, polityki, wytyczne. Tyle papier. Ale w naszej organizacji mamy realny problem, taki jak choćby testowanie oprogramowania na produkcji. Czy tego chcemy, czy nie, musimy uznać, że obecnie pracujemy w środowisku skompromitowanym teleinformatycznie, personalnie i to wcale nie jest takie straszne, jak brzmi w pierwszym czytaniu. Musimy wypracować realne scenariusze i przygotować się na nie najlepiej, jak potrafimy. Trudno zaadresować nawet 90% zagrożeń, lepiej się skupić na tych najbardziej prawdopodobnych, takich jak nagła odmowa świadczenia usługi systemu VMS, nieuprawniony dostęp z wykorzystaniem kart dostępu, ataki socjotechniczne na pracowników firmy oraz współpracujących firm trzecich, zagrożenie wewnętrzne wywołane redukcjami etatów lub awansami/podwyżkami (ktoś niestety w takich przypadkach może poczuć się pominięty).

Im szybciej organizacja będzie w stanie dostosować się do realnych zagrożeń z wysokim ryzykiem, tym bardziej będzie odporna. A jeśli już incydent nastąpi, należy się (jakkolwiek to brzmi) do zaistniałej sytuacji dostosować zamiast z nią uparcie walczyć. A gdy jesteśmy świadomi tego, że nasze zabezpieczenia nie są wystarczające i na co dzień pracujemy w środowiskach narażonych, tym bardziej rozumienie odporności w wyżej wymieniony sposób będzie pożądanym wyjściem. Druga strona medalu może w tym przypadku okazać się równie wymagająca. Odporności organizacyjnej nie zbuduje się tylko działem bezpieczeństwa, jedynie holistyczne podejście do zagadnienia, angażujące kluczowe działy, da nam w tym przypadku wymierne efekty. I tu dochodzimy do sedna tego, kto w danej organizacji odpowiada za jej bezpieczeństwo i od kogo zlecenie koordynacji wszystkich opisanych wyżej działań powinno wyjść.

Odporność, ale na co?

Zostając w tematyce zagrożeń stricte związanych z systemami zabezpieczenia technicznego opartych na sieciach teleinformatycznych, warto zadać sobie pytanie, czy ja jako osoba odpowiedzialna za ten obszar jestem rzeczywiście narażony na tego typu ataki. Jak najbardziej tak, powodów jest wiele np.

1. Coraz bardziej wysublimowane rozwiązania z dziedziny cyberbezpieczeństwa przesuwają wagę działań intruzów w kierunku fizycznej infiltracji swoich celów.
2. Dane przetwarzane w systemach są cennym źródłem informacji i ułatwiają późniejsze działania (*vide* punkt pierwszy).
3. Łatwy dostęp do tych sieci pozwala złym aktorom np. na próbę uzyskania uprawnień a tym samym ich eskalację, spreparowanie fałszywych nagrań na podstawie tych pozyskanych.
4. Testowanie wdrożonych procedur bezpieczeństwa (czy działają i jak są realizowane).
5. Poznanie, np. poprzez biały wywiad/OSINT *(Open Source Intelligence,* pozyskiwanie informacji z ogólnie dostępnych źródeł), nawyków danej organizacji, a co za tym idzie wykorzystanie ich m.in. w postaci ataku socjotechnicznego.

→

Budowanie odpowiednich mechanizmów wymaga czasu. Najpierw jednak należy poznać celowość oraz korzyści z wdrażanych rozwiązań i koszty z nimi związane. Niezmiennie pozostaje więc pytanie…

...jak to zrobić?

Obawiam się, że formuła artykułu jest niewystarczająca do zgłębienia tematu. Pozostając jednak w obszarze bezpieczeństwa fizycznego/technicznego, możemy aspekt ten podsumować, dzieląc wysiłki ukierunkowane na elementy:

- organizacyjne,
- techniczne,
- ludzkie.

Zakładając, że mamy świadomość tego, gdzie jesteśmy, oraz tego, do czego dążymy, jesteśmy w stanie określić nasze zarówno słabe, jak i mocne strony. Teraz wypadałoby się zabrać za to, w czym jesteśmy najlepsi: zabezpieczenia. Te nie zawsze muszą oznaczać tony sprzętu wiszącego na płotach i ścianach. Ograniczając rozważania do środków elektronicznego zabezpieczenia, możemy zwrócić uwagę na szereg zagadnień, w tym na te trochę mniej oczywiste, takie jak:

Dostawca

W środowisku sprzedażowym jeszcze do niedawna pokutowała strategia bycia ekspertem/doradcą rozwiązań dla klienta końcowego. Taka osoba, w rozumieniu strony, np. producenta/dystrybutora, ma za zadanie poznać wymagania klienta i przedstawić ideę/ofertę. Z perspektywy użytkownika końcowego jest to jednak droga na skróty, często prowadząca na manowce. Dostawca jest absolutnie ważnym elementem układanki, ale jako jeden element, a nie twórca mozaiki zabezpieczenia. Jest narzędziem, a nie solucją. W związku z tym powinien podlegać szczegółowej analizie m.in.:

- aspektów prawnych;
- potwierdzenia jakości dostarczanych rozwiązań popartych realnymi wdrożeniami na rynku polskim lub bliźniaczym;
- zachowania bezpieczeństwa łańcucha dostaw pod kątem zastosowanych elementów hardware oraz software;
- wdrożenia wbudowanych zabezpieczeń związanych z wymianą uszkodzonego elementu, aktualizacją oprogramowania firmware, możliwości zastosowania certyfikatów czy szyfrowania danych;
- polityki aktualizacji, reagowania na wykryte podatności;
- zgłoszonych wcześniej podatności (ich wagę);
- możliwości migracji do rozwiązań chmurowych lub hybrydowych;
- wsparcia przy implementacji.

Chciałbym dłużej pozostać przy implementacji, mimo że na pierwszy rzut oka sprawa wydaje się jasna. Wielu dostawców na rynku polskim taką usługę wszak posiada, bazując głównie na konfiguracji. Niemniej jednak to użytkownik końcowy określa wymagania, a jak pokazała sprawa związana z protokołem OSDP wykorzystywanym w systemach kontroli dostępu, diabeł tkwi w szczegółach. Drugim przykładem jest „utwardzanie" systemów (hardening, proces polegający na odpowiedniej konfiguracji systemów w celu zminimalizowania potencjalnych wektorów ataku). Warto zatem wiedzieć, czego należy oczekiwać, i wymagania te egzekwować najpierw na etapie podpisywania, a później realizacji umowy.

Fizyczne testy penetracyjne

Z nieskrywanym zawodem przyznaję, że jest to czynnik kontrolny, który jest bardzo często pomijany w programach ochrony (a przynajmniej tam, gdzie nie jest wymagany odgórnie). Rzadko też występuje jako usługa branży ochrony fizycznej. Jakkolwiek trudno sobie wyobrazić, aby agencja ochrony testowała samą siebie, o tyle zlecenie stronie trzeciej takiej usługi wydaje się już bardziej racjonalne. Testy penetracyjne kojarzą się głównie z intencjonalnymi, legalnymi próbami włamań do sieci informatycznych. Dlaczego zatem nie testować zabezpieczeń fizycznych/technicznych w ten sam sposób? Każda szanująca się instytucja zajmująca się profesjonalnymi pentestami obszaru IT ma również w swojej ofercie zakres obejmujący zabezpieczenia fizyczne. Co więcej, jest to traktowane jako niesamowicie ciekawy sposób docierania do celu. Dlaczego zatem branża macierzysta wciąż nie dostrzega tego potencjału?

Testy penetracyjne działom odpowiedzialnym za ochronę:

- pokażą, czy wdrożone środki spełniają swoje zadania;
- zdemaskują niedociągnięcia lub zwyczajne błędy we wdrożonych systemach;
- wskażą te aspekty, które nie zostały uwzględnione przy budowie planów ochrony;
- mogą stanowić kartę przetargową w rozmowach o budżetach.

W przypadku osób odpowiedzialnych za bezpieczeństwo testy penetracyjne:

- wskażą poziom bezpieczeństwa i pomogą porównać go z tym, do jakiego organizacja chce dążyć;
- są źródłem niezależnych informacji;
- potwierdzą zaangażowanie najwyższego kierownictwa;
- są dobrym dowodem w przypadku procesu śledczego lub ubezpieczeniowego;
- są ewidentnym przykładem dojrzałości programów ochrony.

» Najlepiej uczyć się na cudzych błędach, aczkolwiek nie jest to proste. Co zrobić, aby ustrzec się tego, co spotkało innych? Należy przeanalizować swoją sytuację, zgromadzone dane, zebrać informacje, na podstawie których będzie można wyciągnąć wnioski. «

Do fizycznych testów penetracyjnych (podobnie jak ich odpowiednik w IT) należy skrupulatnie się przygotować, ponieważ ich przeprowadzenie może (aczkolwiek nie powinno) wpłynąć na ciągłość działania organizacji. Dlatego najważniejszym etapem jest przygotowanie się do testów, określenie ich celu, zakresu oraz sposobu, w jaki zostaną przeprowadzone. Osoby chętne zgłębienia tematu odsyłam do niedawno wydanego przez organizację ISACA dokumentu *Physical Penetration Testing: The Most Overlooked Aspect of Security.*

Cykl Deminga

Mówi się, że bezpieczeństwo jest zmienną w czasie. Oznacza to mniej więcej tyle, że cały czas należy je „badać". Każdy problem, każdy projekt można albo rozwiązać lub solidnie przeprowadzić, albo „odfajkować". Z pomocą przychodzi metodyka ciągłego ulepszania opracowana przez Williama Edwardsa Deminga, amerykańskiego specjalistę, statystyka pracującego w Japonii. Od jego nazwiska metoda ta nazywana jest cyklem Deminga. Bardzo sobie ją cenię za prostotę. Cykl Deminga składa się z czterech następujących po sobie etapów:

- ***Plan* (planuj)** – każde działanie musi poprzedzać faza planowania, moim zdaniem najważniejsza ze wszystkich etapów.
- ***Do* (zrób)** – po etapie planowania należy zacząć wdrażać przyjęte założenia.
- ***Check* (sprawdź)** – odbiór prac nie jest etapem końcowym, wdrożone rozwiązanie należy sprawdzić pod kątem przyjętych założeń, zgodności z obowiązującymi regulacjami wewnętrznymi oraz zewnętrznymi.
- ***Act* (popraw)** – wszystkie wykryte nieprawidłowości, niedociągnięcia muszą zostać poprawione.

PDCA to cykl, nie ma więc końca, powinien być powtarzalny. System VMS/CCTV zawsze można przecież rozbudować o kolejne punkty kamerowe, wdrożyć analizę zawartości obrazu lub zintegrować z systemem trzecim, generując wartość dodaną dla danego procesu biznesowego. Ciągle pojawiają się coraz to nowe podatności, zagrożenia, które wymagają zaadresowania.

Nauka na błędach...

...najlepiej cudzych, aczkolwiek nie jest to proste. Co zrobić, aby ustrzec się tego, co spotkało innych? Najlepiej przeanalizować swoją sytuację, zgromadzone dane, zebrać informacje, na podstawie których będzie można wyciągnąć wnioski (np. za pomocą analizy ryzyka) i udać się do osób decyzyjnych z gotowymi propozycjami. Organizacja dojrzała w swej odporności doskonale wie, na czym stoi. Nie oznacza to, że nagle zacznie inwestować duże środki w bezpieczeństwo, ale to właśnie bezpieczeństwo powinno te dane osobom decyzyjnym dostarczać (w sposób zwięzły i klarowny). Jeśli inna firma z naszej branży stała się celem ataku, warto skorzystać np. z usług typu CTI (*Cyber Threat Intelligence,* analiza zagrożeń dotycząca danych aktorów, sektorów, typów ataków), aby znać przyczyny, sposoby i cele tego typu ataków.

Wspomniany wcześniej model PDCA również służy jako tzw. lessons learned, co w wolnym tłumaczeniu można przełożyć na wyciąganie wniosków ze zdarzeń (wcale nie musi to być poważny incydent, nie każda podatność jest wykorzystywana). „Kto nie wyciąga wniosków z przeszłości, skazany jest na jej powtarzanie".

Rys. Cykl Deminga

Inwestycja w przeszłość

Firmy, chcąc nie chcąc, muszą nauczyć się funkcjonować w turbulentnym środowisku z wiedzą, że złośliwa infiltracja ich zasobów jest realnym zagrożeniem, kolejną dobrą praktyką jest budowa takiej architektury, która pozwoli na jak najszybszy powrót do punktu przed atakiem. Można tego dokonać m.in. poprzez:

- redundancję,
- kopie zapasowe.

Oba działania są trudne i kosztowne, ale najważniejsze, aby były efektywne. Muszą mieć cel, odpowiednie procedury oraz być iteracyjnie sprawdzane. Trudno o większy zawód, jeśli rozwiązanie, które miało dać nam swego rodzaju ubezpieczenie, zawiedzie w momencie, kiedy tak bardzo będzie potrzebne.

Obydwa rozwiązania można realizować na różne sposoby. Na pewno nie powinno się przechowywać kopii zapasowych w tym samym miejscu co dane źródłowe. Dobrą praktyką jest szyfrowanie backupu, natomiast musi to być zrobione w przemyślany sposób (najczęściej w koordynacji z zespołami IT).

Trudno jednoznacznie stwierdzić, co należy zrobić, aby być bezpiecznym w obliczu zagrożeń teleinformatycznych. I czy ten stan jest w ogóle realny do osiągnięcia? Ludzie, procedury, wielowarstwowe modele ochrony, kampanie – to wszystko bezwzględnie wpływa na stopień ochrony tu i teraz. Większość tych działań jest natomiast ukierunkowana na budowanie murów, podczas gdy *gros* zagrożeń może już od jakiegoś czasu dojrzewać wewnątrz organizacji. Można z tym walczyć, można uznać za siłę wyższą i próbować się odnaleźć. Każda organizacja musi sama się zdefiniować, co dla niej oznacza odporność. ●

Tomasz Dacka

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

CBC RELACJA

Połączenie mocy CBC i Next!

Firma CBC Poland Sp. z o.o., oddział japońskiej Grupy CBC Co. Ltd., wybrała Next! Software na swojego strategicznego partnera w zakresie oprogramowania do monitoringu wizyjnego i zarządzania stacjami monitorującymi. Jednocześnie Ganz Security by CBC Poland został mniejszościowym (10%) udziałowcem NEXT! Software Sp. z o.o. oraz KRONOS Security Polska Sp. z o.o.

Połączenie mocy obu firm ogłoszono na uroczystej gali, która odbyła się 29 listopada br. w Bielsku-Białej. Była to również okazja do premiery prototypu AutoOperatora – modułu rozszerzającego platformę do monitoringu ALICE, który pozwoli obsługiwać alarmy w pełni automatycznie, bez udziału operatora.
Na gali zaprezentowano też najnowszą generację urządzeń AI BOX – inteligentnych nadajników wideoalarmów umożliwiających dozbrojenie istniejącego systemu monitorowania w profesjonalną i precyzyjną analitykę obrazu, bez konieczności wymiany kamer lub rejestratorów.

– Bardzo się cieszę z wzajemnej współpracy CBC i Next! Ta synergia i wspólna budowa kompletnego ekosystemu spowodują, że ścieżka rozwoju produktów obu firm będzie jaśniej zdefiniowana – powiedział Krzysztof Skowroński, dyrektor zarządzający CBC Poland. *– Pierwszym efektem współpracy jest stworzenie GANZ Secure Cloud, rozwiązania umożliwiającego łączność z poziomu platformy ALICE z kamerami zainstalowanymi na obiekcie bez stałego adresu IP i bez konieczności zastosowania rozwiązań opartych na publicznej chmurze oraz serwerach P2P w bliżej nieokreślonych lokalizacjach.*

– Integracja NEXT i CBC na poziomie produktowym i biznesowym oznacza wiele korzyści – komentuje Sławomir Piela, współwłaściciel Next! *– Wzajemny dostęp do zasobów i doświadczeń firm umożliwia stworzenie lepszego, bardziej zintegrowanego środowiska ochrony.*

– Wymiana doświadczeń pomiędzy naszymi firmami oznacza szersze spojrzenie na rynek i możliwość zwiększenia aktywności na rynkach zagranicznych. Dzięki temu platforma ALICE, uzupełniając portfolio firmy CBC, ma szansę stać się marką globalną – dodaje Bartłomiej Dryja, współwłaściciel Next!

Po uroczystościach firmowych gości zaproszono na spektakl teatralny pt. Boeing, Boeing, w wykonaniu aktorów Teatru Polskiego w Bielsku-Białej. ●

TARGI KIELCE

POLSECURE w 2024 roku

Tematyce nowoczesnego sprzętu i szeroko pojętego bezpieczeństwa będzie poświęcona kolejna edycja targów POLSECURE. Obok ważnego wsparcia Komendy Głównej Policji organizatorzy mogą również liczyć na zaangażowanie innych służb.

Zaplanowane w terminie od 23 do 25 kwietnia Targi Polsecure będą doskonałą okazją do zapoznania się z ofertą firm specjalizujących się w produkcji wyposażenia specjalnego, środków ochrony osobistej, sprzętu ratowniczego, oprogramowania służącego łączności, dowodzeniu czy kontroli, ale także do wymiany doświadczeń i rozmów o rzeczywistych potrzebach służb mundurowych. ●

GLOBAL SECURITY PARTNER

Forum Projektów Systemów Niskoprądowych

2. Forum Projektów Systemów Niskoprądowych odbyło się 8-9 grudnia 2023 r. w Kątach Rybackich. W wydarzeniu, które zorganizowała firma Global Security Partner, uczestniczyło ponad 60 osób.

Swoje rozwiązania prezentowali najwięksi producenci z branży security: BAS-IP, Hikvision, Scylla, Salus Controls, D+H, Protec, Hanwha Vision oraz Grupa Romi. Uczestnicy Forum rozmawiali o największych wyzwaniach stojących przed rynkiem zabezpieczeń technicznych w kraju.

Wśród omówionych tematów znalazły się m.in.:

- systemy wykrywania broni oparte na algorytmach sztucznej inteligencji, które charakteryzują się niskim wskaźnikiem fałszywych alarmów,
- wideodomofony IP, które umożliwiają użytkownikom komunikację z gośćmi i kontrolę dostępu za pomocą smartfonów oraz jednorazowych identyfikatorów typu QR code, PIN lub link wysłany na smartfon,
- najnowsze urządzenia monitoringu wizyjnego,
- systemy audio IP do wysyłania komunikatów informacyjnych i alarmowych,
- inteligentna automatyka sterująca,
- innowacyjne systemy przeciwpożarowe,
- pasywne rozwiązania dla firm elektroenergetycznych i IT,
- systemy zasilania bezprzerwowego.

Organizatorzy zapraszają na następne Forum, które planowane jest na wiosnę 2024 r. ●

LINC POLSKA

Nowy w rodzinie – CAMECT 96

Do rodziny inteligentnych hubów serii Camect (Camect 24 i Camect 60) dołączył nowy model – Camect 96.

Camect to najlepsze rozwiązanie do wideoanalizy oferujące skuteczność detekcji na poziomie 99,7%. Nie tylko niemal bezbłędnie wykrywa intruza, ale także rozróżnia ponad 30 typów obiektów. To właśnie sprawia, że jego skuteczność jest tak wysoka. Każdy z typów może mieć przypisaną inną akcję alarmową, więc to, co jest faktycznie alarmem, zależy od konfiguracji urządzenia i potrzeb użytkownika.

Nowy model umożliwia obsługę nawet 96 megapikseli analityki w jednym urządzeniu. W standardzie jest wyposażony w dwa gigabitowe interfejsy sieciowe, które umożliwiają jego wykorzystanie w rozbudowanych instalacjach bezpieczeństwa. Urządzenie oferuje dwie opcje dysków 4 i 8 TB w technologii SSD.

Camect oferuje nie tylko wysoką skuteczność, ale również bardzo intuicyjny interfejs użytkownika. Obsługa systemu, przeglądanie zarejestrowanych zdarzeń i nagrań nie wymaga zaawansowanej wiedzy czy wtyczek. Bez problemu poradzi sobie z tym przeciętny użytkownik na rozwiązaniach zarówno Android, Apple, Windows, jak i Linux.

Cechą wyróżniającą urządzenie jest wysyłanie wyłącznie zweryfikowanych alarmów. System sam eliminuje nieistotne zdarzenia i wysyła alert jedynie w przypadku tych istotnych. Zdarzenia mogą być dostarczone jako e-mail, powiadomienie push czy komunikat na telegramie. To samo zdarzenie może być równolegle zapisywane na dysku sieciowym lub GoogleDrive.

Te i inne funkcjonalności znajdziesz w Camect, bo Camect jest po prostu smart! ●

ROGER

Oprogramowanie VISO 2.0.8 do RACS 5

Wersja 2.0.8 oprogramowania VISO polskiej platformy zarządzania bezpieczeństwem, kontroli dostępu oraz automatyki budynkowej wprowadza szereg nowych funkcji i udoskonaleń.

Wśród najważniejszych są:

- obsługa sieciowego klucza sprzętowego RLK-1;
- integracja z systemami ppoż. POLON 4000 i POLON 6000 (POLON-ALFA);
- integracja z systemem ppoż. Integral EvoxX (Schrack Seconet);
- obsługa rejestratorów i kamer firm Milestone, Bosch, Tiandy;
- integracja z systemem windowym KCEGC GCAC/RCGIF (KONE);
- obsługa kodów PIN pod przymusem (wymaganie Grade IV);
- rozszerzenie funkcjonalności VISO SMS.

Dodanie obsługi sprzętowego klucza licencyjnego RLK-1 jest odpowiedzią na potrzeby rynku, w którym klienci coraz częściej decydują się na instalowanie oprogramowania zarządzającego systemem kontroli dostępu na maszynach wirtualnych. Klucz RLK-1 jest podłączany do sieci komputerowej Ethernet, a komunikacja z nim jest realizowana przy użyciu szyfrowanej komunikacji zapewniającej najwyższy poziom odporności cybernetycznej.

Integracje z systemami ppoż., kamerami CCTV, platformami VMS oraz zaawansowanymi systemami windowymi stanowią istotne elementy każdego profesjonalnego systemu kontroli dostępu. Dodanie integracji z kolejnymi wiodącymi dostawcami rozwiązań CCTV sprawia, że system kontroli dostępu RACS 5 jest jeszcze bardziej zaawansowaną i funkcjonalnie rozbudowaną platformą zarządzającą bezpieczeństwem w obiektach klasy biznesowej.

Funkcje systemu kontroli dostępu RACS 5 oraz modułu VISO SMS kwalifikują nasze rozwiązanie do stosowania na obiektach wymagających najwyższego stopnia bezpieczeństwa i niekwestionowanie podnoszą poziom ochrony osób i mienia tam, gdzie zintegrowane zarządzanie systemami z poziomu jednej platformy ma kluczowe znaczenie. ●

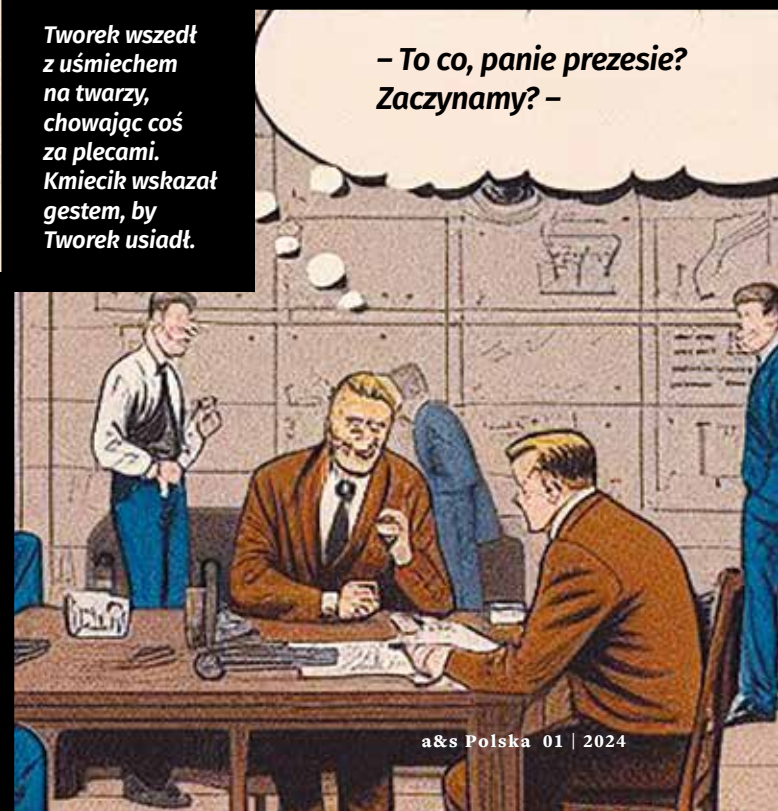
Spotkanie zapowiadało się na burzliwe. Jacek Kmiecik, właściciel i szef dużej firmy biotechnologicznej, wiedział, że łatwo z Tadeuszem Tworkiem nie będzie. Ten drugi kierował firmą świadczącą usługi ochrony na terenie laboratorium. I od pewnego czasu trudno im się było dogadać.

O wyższości pączków z nadzieniem

Dla Kmiecika najważniejsze było bezpieczeństwo biznesu. Firmę rozwijał od wielu lat i odpukać w niemalowane, szło mu coraz lepiej. Pojawiali się nowi kontrahenci, zakład rósł, pracowników przybywało. W zasadzie Kmiecik nie mógł narzekać. W odróżnieniu od Tworka, który ciągle marudził. Ostatnio biadolił, że... Kmiecik nie mógł sobie przypomnieć, na co też Tworek narzekał. Rozmyślania przerwało mu pukanie do drzwi.

Tworek wszedł z uśmiechem na twarzy, chowając coś za plecami. Kmiecik wskazał gestem, by Tworek usiadł.

– To co, panie prezesie? Zaczynamy? –



Ale Tworek miał inny plan.

– Przyniosłem coś. Pogadamy jak Polak z Polakiem.

– Panie Tadku, ale ja w pracy nie piję! – Kmiecik gwałtownie zaoponował.

– Eeee, jakie picie, pączki przyniosłem. Przecież dziś tłusty czwartek. – Tworek roześmiał się rubasznie. Wszyscy znali jego słabość do słodyczy.

– Jak pączki to musowo. – Jacek Kmiecik też cukrem nie gardził. – Ale zaczynajmy, bo przed nami ważne sprawy. Pan wie, że ja się martwię? – Kmiecik przeszedł od razu do rzeczy.

– To tak jak ja. Ja też się martwię. – Tworek pokiwał głową ze zrozumieniem.

– To martwimy się obaj? – Prezes lubił być precyzyjny.

– Ano, obaj. – potwierdził Tworek z pewnym trudem, bo w ustach miał duży kęs pączka i ochotę, by oblizać palce z lukru, choć nie wypadało.

– No tak. – westchnął Kmiecik i też sięgnął po lukrowane cudo, a potem gwałtownie zapytał: – Bez nadzienia nie było? Wolę takie bez.

– Bez nadzienia są beznadziejne! – Tworek omal się nie zakrztusił i zapytał gwałtownie: – To jeszcze pewnie pan na kanapce kładzie najpierw ser, a potem wędlinę?

– Nie jem mięsa. – wyjaśnił Kmiecik.

– Panie prezesie, to jak my się mamy dogadać w tak błahej sprawie jak ochrona firmy, kiedy my się różnimy w tych najważniejszych. – Tworek się szczerze roześmiał.

Tak naprawdę obaj panowie znali się już wiele lat i szanowali. Dlatego każde służbowe spotkanie lubili zacząć od wyjaśnienia kwestii fundamentalnych, życiowo najważniejszych, np. na co najlepiej łapią się pstrągi. By przejść potem do takich drobiazgów, jak zakup nowych kamer (Kmiecik ich nigdy nie potrzebował, a Tworek zawsze), albo tego, że znowu ktoś próbował wedrzeć się na teren zakładu (tu panowie się zgadzali, że to niepokojące), albo dlaczego pracownicy na rampie nie noszą identyfikatorów (Kmiecik argumentował, że przecież wszyscy się znają, na co Tworek przewracał oczami).

Tym razem sprawa była poważniejsza. Kmiecik miał bowiem nadzieję, że namówi szefa ochrony na działanie nie do końca zgodne z ustawą o ochronie osób i mienia. Na co Tworek żadną miarą przystać nie chciał. „Trzymasz się tych przepisów jak pijany płotu", zarzucił mu nawet kiedyś Kmiecik, na co szef ochrony całkiem przytomnie odpowiedział, że jakby puścił, toby upadł, czyli zbankrutował.

– Tadziku – zaczął przymilnie Kmiecik – wiesz, że w ostatnich czasach mieliśmy kilka dziwnych incydentów na terenie zakładu.

– Nie na terenie tylko poza, bądźmy precyzyjni. – Tworek czuł przez skórę, do czego zmierza prezes.

– Oj tam, oj tam. Metr w tę czy w tamtą stronę. – Kmiecik wiedział, że wygaduje dyrdymały, ale musiał jakoś przekonać Tworka, by trochę mniej dosłownie traktował przepisy.

– Panie Jacku, to tak nie ma, że metr w tę czy w tamtą. Tu nie o metr chodzi, i pan to wie – Tworek postanowił przyjąć ton bardziej oficjalny, bo przez skórę czuł, że Jacek Kmiecik chce wykorzystać fakt, że się lubią. – Mnie obowiązują przepisy ustawy o ochronie mienia. Jak je złamię, to się pożegnam z koncesją, a pan ze mną i ze świętym spokojem, bo wprawdzie firm takich jak moja jest dużo, ale tego, że inne pracują tak sumiennie jak moja, to głowy nie dam. – Tworek poczuł, że się nakręca.

– Ja to wszystko rozumiem, ale sam popatrz. – Kmiecik poderwał się od stolika, na którym zostało tylko wspomnienie po sześciu pączkach, i podszedł do komputera. Gwałtownym ruchem odwrócił monitor. – No popatrz, rosyjscy szpiedzy, fałszywe kamery, drony szpiegujące. A my tu mamy wrażliwą produkcję. Szpiegowanie to jedno, ale musimy dbać o łańcuch dostaw. My nie możemy sobie pozwolić na żadne przerwy. Produkcja musi być ciągła. Przecież wiesz.

– Wiem, wiem doskonale. Ale wiem też, że mnie ograniczają przepisy. – Tworek westchnął ciężko.

– Ciebie ograniczają przepisy, mnie też. Ale jak wyniosą receptury, to ty będziesz odpowiadać. – Kmiecik poczuł, że zaczyna ogarniać go złość.

– Ja?! – Tworek zdziwił się niepomiernie. – A to moi pracownicy nie przestrzegają zasady czystego biurka? To moich ludzi trzeba błagać, by chowali wszystkie ważne papiery i nie wynosili ze sobą służbowych pendrivеów? To moi ludzie robią głupie miny przed kamerami i wyłączają czujki ppoż., bo palą papierosy po kątach? A może to moi ludzie nie chcą nosić identyfikatorów i wciąż gubią karty dostępowe?

Kmiecik nawet nie zaprotestował na tę tyradę, tylko raz jeszcze głęboko westchnął i po chwili rzekł:

– Tadeuszu, masz rację. Trzeba tutaj zmian. W granicach prawa – dodał szybko, widząc, że rozmówca zamierza coś powiedzieć. – Musimy mieć lepszy system. Zróbmy tak. Ja opiszę wrażliwe punkty naszego

biznesu. Ty sprawdzisz, czy coś jeszcze możecie dla nas zrobić. Potem będziemy negocjować cenę, okej? – Już wyciągał rękę, gdy zobaczył, że palce ma w lukrze.
– Przestań, mnie się też ręka lepi od cukru. – Tworek uścisnął dłoń szefa laboratorium. – Dobrze jest martwić się na zapas. – I dodał tonem wyjaśnienia: – Jak się jest szefem ochrony. Ty masz się martwić o…
Sygnał telefonu przerwał Tworkowi. Kmiecik odebrał i przez chwilę milczał, słuchając osoby po drugiej stronie, potem wymownie spojrzał na Tworka i powiedział do słuchawki: Mówisz, że to konkurencja? Hm, jest tu przy mnie szef firmy ochroniarskiej, chętnie usłyszy, co się stało.

Czy faktycznie warto się martwić na zapas? I czym jest ten tajemniczy system, o którym mówił Kmiecik. Na te i inne pytania odpowiedzi poznali uczestnicy naszego Security Forum.

Opracowała Monika Mamakis na bazie scenariusza Jacka Grzechowiaka

Marek Białek, Axis Communications
Z punktu widzenia firmy uczestniczącej bardzo wysoko oceniam szkolenie. Znakomicie zorganizowane i sprawnie poprowadzone przez Jacka Grzechowiaka. Podobała mi się nowatorska metoda pokazywania konkretnego problemu. Wyjście od tego, co chcielibyśmy uzyskać w ustawie, a później weryfikacja, co de facto dana ustawa wnosi. Pozytywna jest także idea i sposób udziału partnerów tego wydarzenia, zarówno firm, które pomagają w ochronie fizycznej, jak i dostawców rozwiązań technologicznych w zakresie bezpieczeństwa, czyli nas.

Paweł Grzywa, Securitas Polska
Szkolenie było interesujące ponieważ mogliśmy posłuchać nie tylko przedstawicieli branży logistycznej, ale także produkcyjnej, w której procesy logistyczne również występują i są istotne ze względu na zabezpieczenie ciągłości działania biznesu. Wymieniliśmy się doświadczeniami związanymi z występującymi obecnie zagrożeniami oraz rozmawialiśmy o wyzwaniach i sposobach zabezpieczeń, które mogą skutecznie zminimalizować ryzyko strat. Bardzo ciekawe były przykłady analizy zagrożeń w segmencie logistycznym w kontekście obecnej sytuacji geopolitycznej i zwiększonej aktywności obcych służb.

Andrzej Pecio, Philip Morris
Szkolenie było bardzo interesujące i mówię to z perspektywy z mojego wieloletniego doświadczenia. Podobało mi się dlatego, że byli tu ludzie, którzy rozumieli o czym mówiłem, a ja rozumiałem to, o czym oni mówili. W luźnej atmosferze można było wymieniać się doświadczeniami. Niewątpliwą zaletą był fakt, że byliśmy blisko siebie, a to rzadko się zdarza. Zazwyczaj prelegent siedzi gdzieś daleko od słuchaczy, nikt z uczestników się nie odzywa. Natomiast tutaj było to naprawdę tak, jakbyśmy siedzieli i rozmawiali wśród przyjaciół. Było super, bardzo dziękuję za zaproszenie.

Waldemar Linka, Nagel Polska
W mojej ocenie szkolenie było bardzo przydatne i rozwojowe. Wiele zagadnień zostało pokazanych w zupełnie nowy sposób. To bardzo pomocne w budowie nowoczesnego podejścia do zabezpieczeń. Bo przecież świat się zmienia, żyjemy w zupełnie nowej rzeczywistości. Kiedyś wojny były daleko od nas, nie wpływały na nasze życie. Teraz mamy ją tuż za naszą granicą, więc zagrożenia się zmieniły. Wymiana doświadczeń z uczestnikami szkolenia jest tym, co jest nam dziś bardzo potrzebne.

Michał Badke, Allegro
Szkolenie bardzo mi się podobało. To świetna okazja do spotkania się z ludźmi, którzy robią to co ja, ale w innych przedsiębiorstwach, więc mają inne doświadczenia. Możliwość wymiany doświadczeń z nimi jest czymś niesamowitym. Na pewno dużo daje skorzystanie z ich wiedzy i porad. Sama formuła i prowadzenie szkolenia jest super, to zupełnie coś innego, przez co bardziej wartościowego.


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

SMF

SYSTEM MONITOROWANIA FLOT

to między innymi:

- Eco-Driving – **analiza stylu jazdy** kierowcy
  Wyznaczenie geostref pracy
- **Lokalizowanie** pojazdu
  Szczegółowa **historia**
- **e-Toll**
  Rozbudowany system raportowania
  Monitoring **Sent-Geo**
- Powiadamiamie o **sytuacjach alarmowych**
- Zdalne pobieranie **plików DDD** z tachografów
- Kontrola **gospodarki paliwowej**

... i wiele innych funkcjonalności, które czekają abyś je **odkrył**

www.smfonline.pl
www.omtech.pl