04 (46) / 2024

CZASOPISMO RYNKU SECURITY

a&S POLSKA

RAPORT: NIS2 – JUŻ ZA CHWILECZKĘ, JUŻ ZA MOMENCIK

Czy jesteśmy gotowi na NIS2? Podmioty, które nie spełnią wymogów, będą musiały się liczyć z dotkliwymi karami finansowymi.

ROŚNIE WARTOŚĆ RYNKU KONTROLI DOSTĘPU

Współczesne systemy kontroli dostępu odzwierciedlają rosnące zapotrzebowanie na inteligentne i bezpieczne rozwiązania.

SECURITY W HOTELARSTWIE – PERSPEKTYWY

Branża security może odpowiedzieć na wiele nowych wymogów rynku, zapotrzebowanie, a także starych bolączek w hotelarstwie.

www.aspolska.pl

20 zł
(w tym 8% VAT)

ISSN 2451-5175 05
9 772451 517703


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

Za pięć dwunasta

Dyrektywa NIS2, która wkrótce wejdzie w życie w Unii Europejskiej, zapewne znacząco zmieni oblicze branży security, choć oczywiście nie tylko. To nie jest jedynie kolejna regulacja – to spora zmiana w podejściu do bezpieczeństwa, która wymusi na firmach z sektora ochrony zupełnie nowe spojrzenie na swoją rolę i kompetencje. Stanie się to już za chwilę. Czy branża security jest na ten fakt przygotowana? Czy wie, jakich zmian będą oczekiwać od niej jej klienci. Jak to mawiają: Pożyjemy, zobaczymy. Dokładnie przyjrzeliśmy się temu tematowi w najnowszym numerze magazynu „a&s Polska", którego uważną lekturę polecamy.

Przeciętny Kowalski wprowadzeniem NIS2 się nie zamartwia. On po prostu oczekuje, że będzie bezpiecznie w hotelach, bankach, sklepach wielkopowierzchniowych i innych obiektach użyteczności publicznej. Z jednej strony ma być bezpiecznie, z drugiej – z poszanowaniem prawa do prywatności, a o to coraz trudniej. Stąd właśnie dyrektywa NIS2, która obliguje firmy, by wprowadziły rozwiązania, które będą służyć skutecznej ochronie danych w naszym coraz bardziej zdigitalizowanym świecie. Więcej na ten temat w *Raporcie o NIS2 – już za chwileczkę, już za momencik* (str. 22).

Już teraz wiadomo, że znaczna część klientów firm branży security wraz z wejściem w życie nowych przepisów stanie przed nowymi wyzwaniami w zakresie cyberbezpieczeństwa. Weźmy np. typowy hotel należący do jednej z globalnie działających sieci (bo w rodzinnych pensjonatach może być różnie) – od systemów rezerwacji po zarządzanie dostępem do pokoi, zamawianiem towarów do kuchni, monitoringiem pomieszczeń – wszystko bazuje na technologii cyfrowej (więcej na ten temat w art. *Security w hotelarstwie*, str. 56). Podobnie jest w przypadku obiektów użyteczności publicznej, gdzie systemy kontroli i dane klientów są kluczowe dla codziennych operacji. NIS2 wymaga, aby na te obszary spojrzeć przez pryzmat cyberbezpieczeństwa, co stanowi niemałe wyzwanie dla tradycyjnie pojmowanej ochrony fizycznej.

Co dla jednych jest wyzwaniem, dla innych może być szansą. Firmy branży security, szczególnie te, które zajmują się produkcją systemów zabezpieczeń i szybko dostosują się do nowych wymagań, mogą znacząco wyróżnić się na rynku. Artykuły naszych partnerów dowodzą, że jest świadomość tych wyzwań. Drugiej szansy dla branży należy upatrywać w tym, że klienci będą poszukiwać takich firm, które nie tylko same zapewnią im fizyczne bezpieczeństwo, ale także pomogą im spełnić wymagania NIS2 w zakresie cyberbezpieczeństwa. To otwiera nowe możliwości biznesowe i może prowadzić do rozwoju nowych, lukratywnych strumieni przychodów.

Oczywiście, dostosowanie się do nowych wymagań oznacza inwestycje w rozwój kompetencji. Szkolenia z zakresu cyberbezpieczeństwa staną się równie ważne jak te z ochrony fizycznej. Konieczne może się okazać nawiązanie współpracy z ekspertami IT albo wzmocnienie kompetencji własnych specjalistów. A przypominamy, że termin pełnego wdrożenia NIS2 to 18 października 2024 r. Można rzec, że to ostatni dzwonek, by podjąć stosowne działania. NIS2 może być dla naszej branży okazją do przedefiniowania swojej roli w świecie, gdzie granica między bezpieczeństwem fizycznym a cyfrowym staje się coraz bardziej rozmyta. To okazja do pokazania, że możemy być liderem w adaptacji do nowych realiów cyfrowego świata. Branża security ma szansę wyjść z tej transformacji silniejsza niż kiedykolwiek, oferując klientom kompleksowe rozwiązania łączące ochronę fizyczną z cyberbezpieczeństwem. Warto jednak się pospieszyć, bo jest już za pięć dwunasta…

Redakcja

CZASOPISMO RYNKU SECURITY

a&S POLSKA

04 (46) / 2023

SPIS TREŚCI

RAPORT: Co warto wiedzieć o **NIS2**

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

NOWA SERIA
REJESTRATORÓW z TECHNOLOGIĄ AI

do 24 analizy kanałów AI

» Więcej przeczytasz na stronie 8

POLSKA MARKA BCS

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

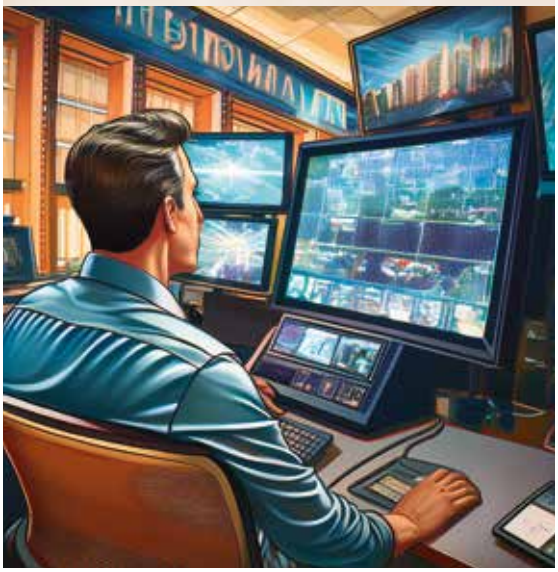
BCS®

CZASOPISMO RYNKU SECURITY

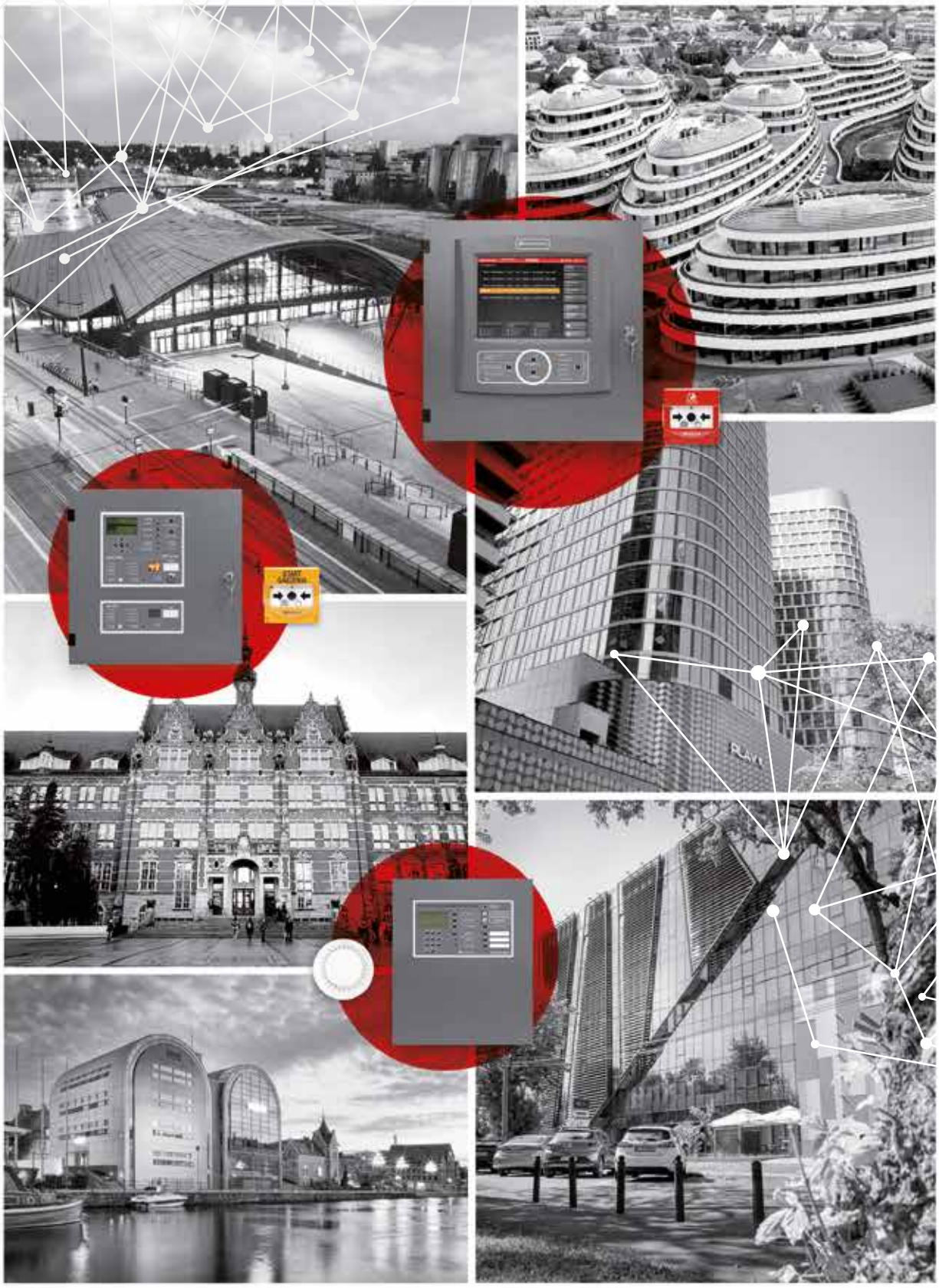
a&S POLSKA

04 (46) / 2023

SPIS TREŚCI



POLON-ALFA



tradycyjnie KOMPLEKSOWA OCHRONA

tysięcy obiektów w kraju i za granicą

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

AAT SYSTEMY BEZPIECZEŃSTWA

Kamery 6 Mpix NOVUS – jeszcze więcej detali monitorowanej strefy

Nowe wandaloodporne kamery 6 Mpix typu eyeball oraz bullet ze stałą ogniskową f=2.8 mm/F1.6 i zmienną ogniskową motor-zoom, f=2.8 ~ 12 mm/F1.6, zapewniając kąt widzenia blisko 100°, umożliwiają szczegółowy dozór pomieszczeń oraz rozległych otwartych obszarów.

Urządzenia pozwalają na przesyłanie obrazów z prędkością 30 kl./s lub 20 kl./s (w zależności od modelu) w rozdzielczości 3200 x 1800 (6 Mpix). Przetwornik CMOS wysokiej czułości z podwójnym skanowaniem oferuje zakres dynamiki 120 dB. Przy bardzo słabym oświetleniu sceny włącza się promiennik IR LED o zasięgu do 50 m dla modeli motor-zoom i do 30 m dla modeli stałoogniskowych. Uzupełnieniem oświetlaczy IR jest dioda światła białego *(WL – White Light)* o zasięgu do 40 m, pracująca w trybie SMART LIGHT.

Analiza obrazu InGenius stanowi pakiet funkcji, które rozróżniają ludzi i pojazdy, tym samym redukując liczbę fałszywych alarmów. W zależności od potrzeb można m.in. ustawić detekcję przekroczenia linii lub wtargnięcia do strefy.

Wybrane kamery 6 Mpix NOVUS dysponują jeszcze bardziej zaawansowanymi funkcjami InGenius Plus: detekcją twarzy, zliczaniem przekroczeń linii, statystyką obszaru, mapą ciepła, metadanymi oraz wykrywaniem nielegalnego parkowania. Możliwość bezpośredniego strumieniowania na platformie YouTube (RTMP) oraz obsługi z poziomu przeglądarki (HTML5). Dodatkowo wybrane modele obsługują łączenie przez protokół P2P. W ofercie dostępne są dwie wersje kolorystyczne obudowy: biała i szara.

Więcej na: www.aat.pl

AXIS COMMUNICATIONS

Kamera typu bullet AXIS Q1809-LE zapewniająca najwyższą szczegółowość

Wyposażona w podwójny system Axis system-on-chip, ta uniwersalna, gotowa do użytku na zewnątrz kamera typu bullet zapewnia doskonałą rozdzielczość 41 Mpix z ekstremalną szczegółowością na dużych odległościach i niezwykle wysoką gęstością pikseli.

Sprzętowa platforma cyberbezpieczeństwa Axis Edge Vault chroni urządzenie i oferuje certyfikowane przez FIPS 140-3 Level 3 bezpieczne przechowywanie kluczy i operacje. Ponadto wyjście PoE pozwala na podłączenie i zasilanie innego urządzenia bez dodatkowego okablowania.

Zalety:

- gotowość do pracy na zewnątrz po wyjęciu z pudełka,
- doskonała jakość obrazu w rozdzielczości 8K,
- przetwornik obrazu 4/3" o wysokiej światłoczułości,
- niezwykła szczegółowość przy dużych odległościach,
- wbudowane funkcje cyberbezpieczeństwa dzięki Axis Edge Vault.

Więcej na ww.axis.com/pl-pl

BCS

Nowe rejestratory BCS Line

W szerokiej gamie produktów BCS Line pojawiły się nowe rejestratory sieciowe. Modele serii L-NVR-4K-AI(2) są dostępne w wersjach 8-, 16-, 32-, 64-kanałowych z możliwością montażu 2, 4 lub 8 dysków twardych o pojemności do 20 TB każdy. W wersjach 8-dyskowych do dyspozycji jest system RAID.

Podstawową różnicą w porównaniu z modelami dostępnymi do tej pory jest obsługa kamer o zdecydowanie wyższej rozdzielczości. Poprzednie modele mogły współpracować z kamerami o maksymalnej rozdzielczości 16 Mpix, modele serii L-NVR-4K-AI(2) nie będą miały problemu z kamerami o rozdzielczości nawet 32 Mpix.

Urządzenia mają poprawione możliwości dekodowania i mogą wyświetlać dwa główne strumienie o rozdzielczości 32 Mpix. Kolejną zmianą jest poprawa przepustowości danych. Pasma wejściowe, wyjściowe i nagrywania mogą być przesyłane z prędkością 512 Mb/s. Dzięki temu nie trzeba zmniejszać jakości obrazu z kamer, aby zmieścić się w dostępnym w rejestratorze paśmie. To również pokazuje kierunek rozwoju produktów BCS.

Rejestratory L-NVR-4K-AI(2) są wyposażone w moduł sztucznej inteligencji pozwalający na uruchomienie funkcji zaawansowanej analizy wideo bez względu na to, czy podłączona do niego kamera jest z linii BCS, czy innego producenta z protokołem Onvif. Rejestrator może realizować funkcje SMD *(Smart Motion Detection)* i ochrony parametrycznej, może identyfikować twarze i gromadzić metadane i to przy niespotykanej dotąd liczbie kanałów: 24 kanały ochrony obwodowej, 8 kanałów identyfikacji i detekcji twarzy oraz 8 kanałów metadanych.

Więcej na: www.bcs.pl

camect

INTELIGENTNY HUB
efektywna i skuteczna detekcja zagrożenia

SZTUCZNA INTELIGENCJA
wbudowana, zaawansowana sztuczna inteligencja

ROZRÓŻNIA PONAD 30 TYPÓW OBIEKTÓW
ludzi, pojazdy, zwierzęta

WSPÓŁDZIAŁANIE
z różnymi kamerami IP

KOMPATYBILNOŚĆ
z SAFESTAR

OFICJALNY DYSTRYBUTOR:

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

www.linc.pl

WIĘCEJ O NAS:

Linc Polska Sp. z o.o.

HIKVISION POLSKA

Nowe czytniki serii DS-K1109

Czytnik w systemie kontroli dostępu jest jednym z nielicznych elementów, o którego wyborze decydują nie tylko parametry techniczne, ale także walory estetyczne.

Standardowe czytniki zazwyczaj pozwalają identyfikować użytkownika za pomocą kodu PIN, karty lub wzorca biometrycznego. W odpowiedzi na potrzeby swoich klientów firma Hikvision rozszerzyła ofertę czytników o serię DS-K1109. W tej grupie są czytniki z głowicami RFID: Unique 125 kHz, Mifare 13,56 MHz, Mifare Desfire, Felica dostępne w wersji z podświetlaną klawiaturą lub bez niej.

Na szczególną uwagę zasługuje czytnik z wbudowanym modułem Bluetooth (B), kamerą do odczytywania kodów QR (Q) i skanerem linii papilarnych (F) – w modelu DS-K1109DKFB-QR w jednej obudowie zaoferowano wiele różnych rozwiązań umożliwiających identyfikację użytkowników.

Moduł Bluetooth pozwala na identyfikację za pomocą identyfikatorów mobilnych. Obsługa tego modułu jest realizowana wtedy, gdy czytnik jest podłączony do kontrolera przez RS485. Dodatkowo czytnik z kontrolerem może się komunikować poprzez protokół Wiegand.

Stopień ochrony obudowy IP65 i możliwość pracy w temp. -40°C do 65°C pozwala na montaż czytników na zewnątrz. Kompaktowy design i wiele możliwych metod identyfikacji użytkownika sprawiają, że nowe czytniki stanowią doskonałe uzupełnienie aktualnej oferty kontroli dostępu firmy Hikvision.

Więcej na: www.hikvision.com/pl

LINC POLSKA

Thermal Radar – radarowy system ochrony do monitorowania dużych obszarów

Rozwiązania Thermal Radar to połączenie najlepszych cech kamery termowizyjnej i obrotowego radaru do skutecznego wykrywania intruzów oraz aktywnej ochrony. Dzięki technologii termowizyjnej kamera może wykrywać obiekty z odległości nawet 500 m. System działa niezależnie od oświetlenia, ponieważ moduł termowizyjny wykrywa ciepło poruszających się obiektów.

Dzięki temu, że moduł termowizyjny jest osadzony na głowicy rotacyjnej, obracając się, tworzy dookólny obraz 360 stopni obszaru o powierzchni przeszło 700 tys. m^2. Obraz jest łączony w całość i uzupełniany o mapę, poprawiając tym samym świadomość sytuacyjną pracowników ochrony.

Cały obraz termowizyjny jest poddawany obróbce przez wbudowaną analizę obrazu, która po wykryciu zdarzenia podejmuje natychmiastową reakcję. Alarm uruchamia tryb śledzenia, wykorzystując dodatkową kamerę światła widzialnego, która podąża za wykrytym celem i cały czas prowadzi jego obserwację.

System wysyła powiadomienie do operatora, jednocześnie może też zareagować alarmem na miejscu, np. uruchomić lokalną syrenę bądź wyemitować komunikat z głośnika. Thermal Radar jest zintegrowany z wiodącymi rozwiązaniami VMS czy PSIM. Ponadto oferuje podłączenie do dowolnego systemu wideomonitoringu jako kamera zgodna z Onvif.

Thermal Radar to idealne rozwiązanie do zastosowania wszędzie tam, gdzie potrzebny jest duży zasięg detekcji przy jednoczesnym pokryciu rozległego obszaru. Sprawdza się również w rozwiązaniach tymczasowych, np. z wieżami monitoringu, gdzie trzeba szybko uruchomić ochronę terenu.

Więcej na: www.linc.pl

&

TP-LINK

TP-Link VIGI C540-4G – zewnętrzna kamera sieciowa 4G

TP-Link VIGI C540-4G to obrotowa kamera sieciowa z łącznością 4G. Urządzenie ma obudowę o klasie 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 diody LED światła punktowego. Dzięki wbudowanemu modemowi LTE oraz zasilaniu poprzez klasyczny zasilacz DC 12 V VIGI C540-4G jest gotowa do pracy w miejscach, w których nie ma sieci lokalnej z dostępem do Internetu.

VIGI C540-4G ma opcję tworzenia tras patrolu. Wyposażono ją w mikrofon oraz głośnik, a także alarm dźwiękowy i świetlny do odstraszania intruzów. Kamera może wykrywać wtargnięcia na wyznaczony teren, przekroczenie linii, wejście do strefy oraz jej opuszczenie, pozostawienie przedmiotu lub jego zabranie. Wykrywa również osoby, które zachowują się podejrzanie, oraz zmianę sceny, gdy ktoś zasłoni kamerę. Potrafi także rozpoznawać ludzi i samochody. Nagrania z kamery mogą być rejestrowane lokalnie na kartach microSD (do 512 GB).

Tak jak pozostałe urządzenia z serii TP-Link VIGI 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 sposób zarządzać z poziomu urządzenia mobilnego, z dowolnego miejsca na świecie. Kamera jest objęta 3-letnią gwarancją.

Więcej na: www.tp-link.com/pl

SALTO WECOSYSTEM

Więcej niż tylko zamek do pokoju hotelowego – to zadowolenie gości.

Zwiększ dobre samopoczucie swoich gości dzięki SALTO, światowemu liderowi w dziedzinie kontroli dostępu dla branży hotelarskiej.

Nasze inteligentne bezprzewodowe i bezkluczowe zabezpieczenia zapewniają najwyższą kontrolę, a przy tym doskonale komponują się z wystrojem i stylem hotelu.

saltosystems.com

salto
INSPIRED ACCESS


WARSAW
SECURITY
SUMMIT

6 czerwca 2024 r. w niedawno otwartym Muzeum Historii Polski spotkali się przedstawiciele branży security. Powód mógł być tylko jeden – VIII Warsaw Security Summit. Była to edycja wyjątkowa zarówno ze względu na miejsce, liczbę gości, zaproszonych ekspertów, dobór tematów, jak i moment historyczny.

Wiedzą państwo zapewne, że jest to największa konferencja branży zabezpieczeń – przywitał gości prowadzący wydarzenie Maciej Dowbor ze sceny przestronnej auli MHP. Nie były to puste słowa. Aula była wypełniona po brzegi, a organizatorzy potwierdzili przybycie na to wydarzenie ok. 700 gości zajmujących się zawodowo kwestiami security. Wydarzenie ma już ugruntowaną renomę w środowisku, ale sama dobra reputacja nie jest gwarantem sukcesu frekwencyjnego ani merytorycznego. Dobór najlepszych ekspertów jako panelistów poruszających najbardziej aktualne tematy – już tak. Nieprzypadkowy był także wybór miejsca spotkania. Nowo otwarte muzeum znajdujące się niemal w centrum Warszawy, posiadające cenne zbiory i dysponujące ogromnymi powierzchniami do użytku publicznego samo w sobie stanowi ciekawy przypadek do branżowej analizy.

Mariusz Kucharski, prezes „a&s Polska", rozpoczął spotkanie od podkreślenia powagi sytuacji: *W tym roku spotykamy się w wyjątkowo trudnym czasie. Wojna w Ukrainie i towarzyszący jej chaos geopolityczny mocno namieszały w naszej rzeczywistości, zmieniły krajobraz zagrożeń, z którymi szefowie bezpieczeństwa różnych firm, instytucji państwowych, prywatnego biznesu mierzą się na co dzień. Jesteśmy też świadkami wzrostu liczby i skali ataków hybrydowych na infrastrukturę krytyczną i instytucje państwowe, a także prywatne biznesy. Coraz bardziej niebezpieczne stają się też działania hakerów. Także i my padliśmy ich ofiarą. Nasze serwery zostały pokonane. Jeden z serwerów został zainfekowany i z tego powodu nasz portal aspolska.pl został czasowo wyłączony. Staliśmy się celem ataku cyberprzestępców, podobnie jak Polska Agencja Prasowa i wiele innych firm i instytucji. Odczytujemy to jako znak, że dzisiejsze spotkanie wybitnych ekspertów i uczestników, profesjonalistów w branży bezpieczeństwa jest w tym roku bardziej potrzebne niż do tej pory. W obliczu tych wyzwań wydaje się, że mamy wspólnego wroga i musimy działać wspólnie.*

BLOK 1 – Wojna i pokój

Część merytoryczna rozpoczęła się od omówienia zagadnienia, które zajmuje uwagę chyba wszystkich w Polsce, a także wielu osób w Europie i na świecie. Wojna. Jak się okazuje, to czego obawiamy się najbardziej, czyli ataku ze strony Rosji, to zaledwie jedno z możliwych zagrożeń. Globalne wyzwania dla bezpieczeństwa należy rozpatrywać w szerokim sensie, są one bowiem obecnie liczne i jeszcze bardziej skomplikowane, co uświadomił zebranym pierwszy prelegent – gen. Mieczysław Bieniek w swoim wystąpieniu „Globalne wyzwania bezpieczeństwa w świetle wieloaspektowych zagrożeń. Efektywne przywództwo w XXI wieku, zarządzanie w sytuacji kryzysowej. Strategie wojskowe w biznesie". Było to bez wątpienia najbardziej wyczekiwane i najmocniejsze wystąpienie tego dnia.

Gen. M. Bieniek szczegółowo narysował mapę toczących się aktualnie konfliktów zbrojnych na świecie, tlących się potencjalnych ognisk zapalnych i trwających nieraz od dziesięcioleci regionalnych napięć. Uświadomił zebranym, że obecna sytuacja geopolityczna nie ogranicza się do zagrażającego nam bezpośrednio krwawego konfliktu między Rosją a Ukrainą, ale jest o wiele bardziej złożona, a przede wszystkim rozległa. To m.in. broń jądrowa, której na świecie jest wiele, a znane są jedynie szacunkowe liczby, zagrożenie proliferacją broni chemicznej i biologicznej, niekontrolowane migracje ludności, w tym uchodźców, terroryzm i cyberterroryzm, tyranie i dyktatury oraz zagrożenia płynące z chaosu po ich obaleniu, fundamentalizm islamski, państwa tzw. Sahelu, w których bieda i susza nasilają tendencje ekstremistyczne, niekończące się wojny arabsko-izraelskie, konflikt zbrojny izraelsko-palestyński i sytuacja na Bliskim Wschodzie, którą można porównać do beczki prochu, napięcia na Morzu Południowochińskim, narastające problemy żywnościowe, ekologiczne, surowcowe i ekologiczne, a także – *last but not least* – wyzwania związane z gwałtownym i niekontrolowanym rozwojem technologii oraz sztucznej inteligencji.

Nawet tak lakoniczna wyliczanka pokazuje, że świat jest wielocentryczny, czego zazwyczaj nie dostrzegamy z perspektywy Europy. W takim układzie trudno o uzgodnioną wizję zagrożeń. Mimo dynamicznie postępujących (czy też galopujących) zmian, które obejmują cały świat, należy pamiętać, że charakter wojny pozostaje niezmienny. Jej celem jest terytorium przeciwnika. Zmieniają się jedynie narzędzia, którymi się je zdobywa. W związku z tym warto sobie zadać pytanie o przygotowanie do odparcia ataku.

Jeżeli mowa o ataku konwencjonalnym, nie można ograniczyć się tylko do sił zbrojnych. Strefy bezpieczeństwa strategicznego przenikają całe państwo, a zaczynają się od ustroju politycznego. O stanie bezpieczeństwa i obronności państwa decyduje wiele czynników. Do istotniejszych należą siła i jakość przywództwa, w dalszej kolejności infrastruktura, administracja państwowa, przygotowanie ludności, a także mechanizmy stricte obronne – siły zbrojne, służby wewnętrzne, policja itd. Problem w tym, że w dzisiejszym świecie atak konwencjonalny jest tylko jednym z możliwych scenariuszy. Coraz częściej w grę wchodzą także ataki hybrydowe i cyberataki, nieraz bardzo trudne do wykrycia i unieszkodliwienia. Dopóki mamy do czynienia z technikami amatorskimi, dopóty jest to stosunkowo proste. Trudniej się robi, gdy w grę wchodzą najemni ochotnicy bądź cyberterroryzm finansowany przez państwa – to najwyższy stopień zagrożenia cybernetycznego.

To, co przede wszystkim wybrzmiało z tego niezwykle sugestywnego power speechu, to skala i różnorodność zagrożeń, z którymi musimy się coraz bardziej liczyć. Krajobraz bezpieczeństwa zmienia się na naszych oczach i wszystko wskazuje na to, że będzie coraz bardziej skomplikowany. Trudno przewidzieć, co powstanie z układanki przesuwających się stref wpływów politycznych, migracji dużych grup ludzi, powiększania się nierówności społecznych, państw o erodującej tożsamości narodowej, zmieniającego się klimatu, globalizującej się gospodarki, zmian energetycznych, gwałtownego rozwoju sztucznej inteligencji itd.

Nieco inaczej podszedł do zagadnienia wojny Jacek Bartosiak, założyciel Strategy & Future, ekspert Fundacji Pułaskiego. To, że ład międzynarodowy jest złamany, nie ulega wątpliwości – mówił. Oczywiście, ład europocentryczny. Konsekwencje tego stanu mogą oznaczać m.in. to, że zdolność zabijania ludzi w polityce stała się uprawnionym argumentem, a użycie przemocy fizycznej jest znów, po wielu latach, instrumentem polityki zagranicznej (Federacji Rosyjskiej). Wydaje się więc, że w tym kontekście najbardziej zagrażające są próby destabilizacji systemu bezpieczeństwa państwa. Agresor, podejmując działania poniżej konsensualnego progu otwartej wojny, szuka najsłabszego ogniwa na wschodniej

Mariusz KUCHARSKI, organizator konferencji

Jacek BARTOSIAK, Strategy & Future

flance. W całym regionie będą się działy dziwne rzeczy, np. porwania, niewyjaśnione pożary, awarie sieci teleinformatycznych. Tego typu zdarzenia mają przede wszystkim działać na wyobraźnię obywateli, pokazać im, że państwo jest zdestabilizowane, bezbronne i nie gwarantuje bezpieczeństwa. Wymarzoną wręcz przestrzenią dla takich działań jest cyberprzestrzeń, gdzie ataki pozostają znacząco poniżej poziomu otwartej agresji, na którą państwa sojusznicze musiałyby zareagować, ale mogą być niebezpieczne, a przede wszystkim obniżają społeczne morale i zaufanie do aparatu państwa. Według Jacka Bartosiaka odpowiedzią na to są procedury, które jasno określają role i zadania poszczególnych osób w przypadku kryzysu. – *Istota odporności państwa polega na tym, żeby agresorowi nie chciało się nawet próbować, bo jesteśmy tak zorganizowani, wszyscy wiedzą, co mają robić i żadne akcje nie mają sensu. Nie ma paniki, ucieczki, inflacji, ucieczki klasy politycznej, zakorkowanych dróg itd.* – podkreślał prelegent, po czym przeszedł do wygłoszenia tezy, jak sam określił, być może kontrowersyjnej: *Punktem ciężkości systemu odporności państwa jest bezpieczeństwo dzieci. Wyjaśnienie brzmi tak: Jeśli kobiety nie czują, że system szkolny jest bezpieczny i działa, dzieci nie idą do szkoły, a więc rodzice nie idą do pracy. Cała obrona cywilna spoczywa na barkach kobiet, bo one spajają rodziny.*

Łukasz Wojewoda z Ministerstwa Cyfryzacji opowiedział o fake newsach, dezinformacji i działaniach hybrydowych w cyberprzestrzeni. Dezinformacją zajmuje się instytut badawczy NASK. – *Są takie miejsca w przestrzeni medialnej, które fachowo zajmują się tym, aby walczyć z dezinformacją, ale dawać narzędzia do tej walki, aby wszyscy obywatele mogli aktywnie uczestniczyć w procesie, który pomoże przeciwdziałać [dezinformacji]* – wyjaśnił na początku swojego przemówienia. Dezinformacja nie jest techniką nową, działania infoopsowe znane są np. w wojskowości od dawna. Wrażenie, że pojawiły się niedawno, bierze się stąd, że techniki dotarcia do odbiorców bardzo się uprościły i dziś doświadczamy ich znacznie częściej niż w epoce przedinternetowej, oczywiście nie tylko w Polsce.

Na poziomie europejskim także istnieją jednostki walczące z dezinformacją. European Fact-Checking Standards Network przed wyborami do Parlamentu Europejskiego przeanalizowała narrację

→

Łukasz WOJEWODA, Ministerstwo Cyfryzacji

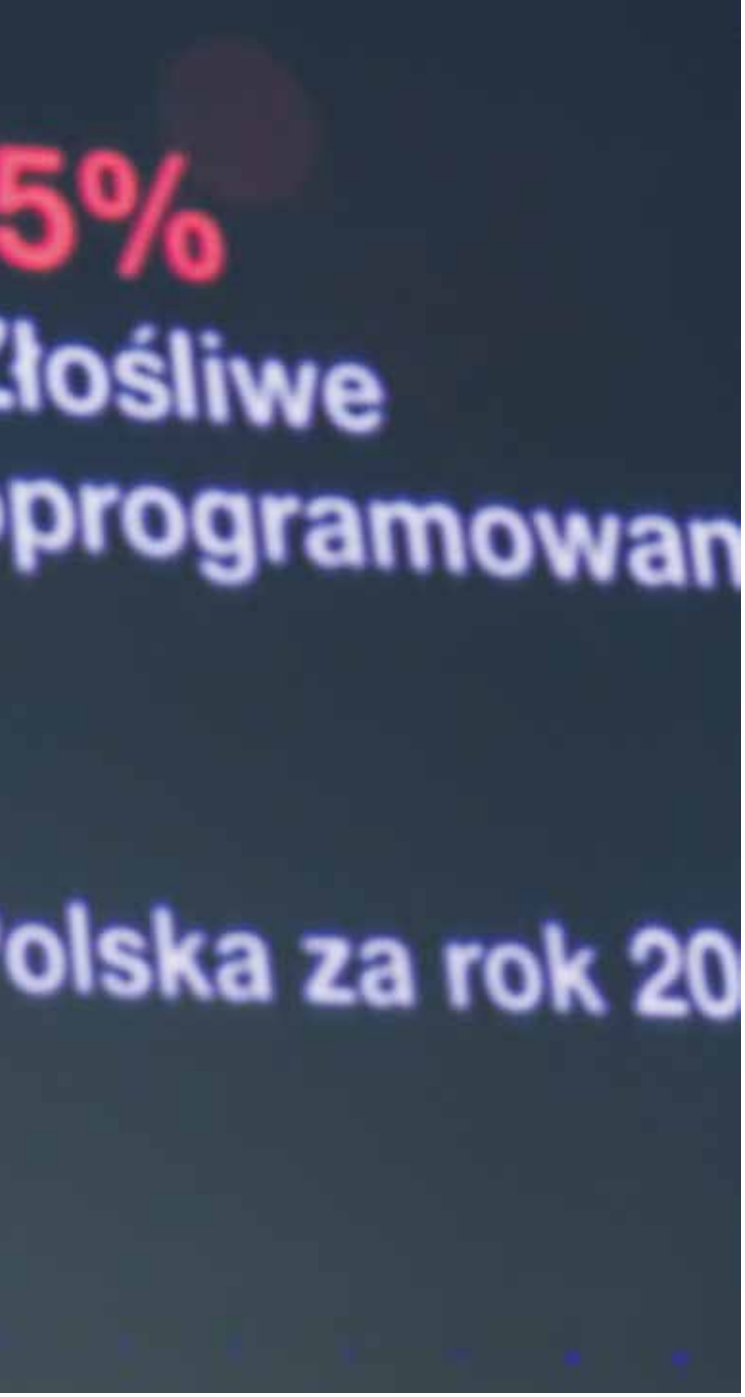
gen. Mieczysław BIENIEK, doradca MON

Daniel KAMIŃSKI z Orange Polska

medialną w Czechach, Niemczech, Chorwacji i Węgrzech i odkryła, że jedną z głównych narracji dezinformacyjnych w tamtym okresie była propaganda antyukraińska. Skala nadużyć była ogromna – aż 71% przeanalizowanych materiałów (1351) uznano za fałszywe, w 15% (281) brakowało właściwego kontekstu, a 8% było częściowo fałszywe (153). Diagnozą obecnych trendów dezinformacyjnych zajmuje się także EEAS – European External Action Service. Bada on m.in. to, jak działania na arenie międzynarodowej wpływają i przekładają się na aktywności pojedynczych obywateli. Nie zawsze chodzi o wywołanie paniki, ale często o sparaliżowanie działań, np. w przypadku Ukrainy – wstrzymanie działań pomocowych.

Działania trolli bywają wymierzone także w organizacje f*act-checkingowe,* jak chociażby w polskie: Demagoga, Konkret24, FakeNews.pl czy Pravdę. Robi się po to, aby osłabić ich pozycję i siłę opinii. Rok 2024 jest rokiem superwyborczym, co oznacza, że w wielu miejscach na świecie odbywają się wybory. Siłą rzeczy skala manipulacji z tym związanych jest ogromna. Sytuacja jest w tym momencie na tyle poważna, że same siły ministerialne nie wystarczą do odparcia ataków – do aktywnego działania potrzebne są organizacje pozarządowe, a także biznes. Dobrym tego przykładem jest Google, który


Aneta SADACH z Uniwersytetu Łódzkiego oraz Bartłomiej BZYMEK z Genetec



także włącza się w działania antydezinformacyjne (https://prebunking.withgoogle.com). Na polskim podwórku działa także miejsce, w którym można sprawdzić, czy dana informacja jest prawdziwa, lub zgłosić nadużycie bądź kampanię dezinformacyjną (https://www.bezpiecznewybory.pl). Zbliżony profil działania ma fundacja Digital Poland (https://digitalpoland.org/).

Wojewoda podkreślał, że znacznie łatwiej wywołać jakąś informacją efekt kuli śnieżnej niż później sprostować przekłamania. Powód jest prozaiczny – natura ludzka chętniej „chwyta" sensacje i ciekawostki niż żmudne wyjaśnienia.

Na zakończenie całej części merytorycznej mjr rez. dr hab. inż. Jarosław Stelmach – Safety Project, ekspert ds. antyterroryzmu i bezpieczeństwa obiektów użyteczności publicznej, opowiedział o dynamicznej perspektywie reagowania na zamachy. Kategorii zamachów jest nawet kilkadziesiąt, a w każdej z nich można wyróżnić po kilkanaście technik i narzędzi, którymi posługują się sprawcy. – *Nie jesteśmy w stanie przygotować się przez 24 godziny na dobę we wszystkich miejscach w Polsce na wszystkie działania sprawców, to jest niemożliwe* – podkreślił ze sceny. Nie oznacza to, że możemy nic nie robić. Sytuacja, w której się znajdujemy, jest co najmniej newralgiczna – sąsiednia Ukraina od dwóch lat jest bombardowana, niektóre z rakiet dolatują nawet do Polski, dwie osoby zginęły. – *Skoro tak jest, każdy obiekt, każda przestrzeń publiczna powinna mieć tak, że jak wchodzę do organizacji, to każdy pracownik doskonale wie, co znaczy modulowany dźwięk syreny, co ma zrobić, gdzie się udać, co ze sobą zabrać, jak długo tak przetrwa i jak państwo o niego zadba w tym zakresie* – mówił J. Stelmach i podkreślał, że nie jest rolą wyłącznie ustawodawcy zapewnienie tak pełnej świadomości i przygotowania, gdyż wiele z tego możemy zrobić samodzielnie. Mocnym punktem ułatwiającym takie przygotowania jest załącznik antyterrorystyczny planu ochrony obiektów. Aby był faktycznie użyteczny, powinien być przede wszystkim zrobiony z uwzględnieniem specyfiki obiektu i być jawny, czyli trafić do pracowników ochrony, którzy są faktycznie na placu boju, a scenariusze statyczne reagowania powinny zostać przetestowane w terenie. →

Konferencję prowadził Maciej DOWBOR

Przedstawiciele firmy Linc Polska

Networking we foyer

Przedstawiciele firmy Hikvision Polska

BLOK 2 – NIS2: wymogi prawne i przygotowania

Drugim gorącym tematem omawianym szeroko podczas WSS była dyrektywa NIS2 oraz związana z nią nowelizacja ustawy KSC. – *Temat jest bardzo nośny, a przecież NIS1 istnieje od kilku lat. Skąd teraz ten rumor?* – zauważył pierwszy z prelegentów w tym bloku Daniel Kamiński z Orange Polska. Wyjaśnienie tego fenomenu można by sprowadzić do tego, że wiele jest w związku z tą zmianą niejasności, ale w rzeczywistości obraz jest znacznie bardziej złożony. Daniel Kamiński, próbując go wyjaśnić, przytoczył fragment raportu CERT Orange Polska, z którego wynikało, że m.in. doszło do istotnej zmiany w krajobrazie cyberzagrożeń – do niedawna najczęstszym był spam. Teraz 44% stanowi *phishing*, którego głównym celem jest wyłudzenie pieniędzy. Sprawę komplikuje dodatkowo to, że przestępcom bardzo łatwo jest stworzyć pozory legalności, np. pod przykrywką sklepu czy serwisu internetowego. Koszt zbudowania strony internetowej z bramką do płacenia payU to koszt ok. 10 USD plus marketing. To stan na dziś, a scenariusze wyłudzeń są coraz bardziej rozbudowane. Zwiększa się także wolumen cyberprzestępczości – 10 lat temu największy atak DDoS w Orange miał wielkość 50 Gb/s, w tym roku 550 Gb/s. Przywracanie usługi trwało dwa tygodnie. W sytuacji, gdy siły zdają się tak nierówne między *good guys* a *bad guys*, jakiego rodzaju zabezpieczeń mogą używać ci pierwsi?

Z pomocą przychodzi Unia Europejska, która regulacjami dotyczącymi cyberodporności próbuje wspomóc bezpieczeństwo korzystania z sieci i świadczenia usług za jej pośrednictwem. Jedną z nich jest dyrektywa o odporności podmiotów krytycznych CER. Stąd też m.in. zmiany w NIS – *Network and Information Security.* Jest to jeszcze dyrektywa, która do 17 października 2024 r. ma zostać zaimplementowana, a jednocześnie trwają prace nad przekształceniem jej w ustawę. Niestety, udział środowiska security w tych pracach jest niewielki. O ile w NIS1 państwo wskazywało obiekty (400), które musiały zostać obowiązkowo objęte cyberzabezpieczeniami, o tyle NIS2 wymaga samozdefiniowania pod kątem tego, czy dana firma bądź instytucja powinna być nią objęta. Wiadomo, że obowiązek ma dotyczyć ok. 30 tys. podmiotów. Których dokładnie? Dobre pytanie. Znane są jedynie sektory.

Druga kontrowersja związana z tą dyrektywą polega na tym, że jednostki objęte NIS2 mają przechodzić obowiązkowe audyty, a także przekazywać do CSiRT informacje o zdarzeniu w ciągu 8, 12 lub 24 godzin od jego zajścia. Taka błyskawiczna reakcja ma pomóc organom powstrzymać rozprzestrzenianie się ataków na kolejne jednostki, inicjatywa jest więc słuszna. Brak zgłoszenia może skutkować wysoką karą pieniężną – system kar jest rozbudowany i w niektórych przypadkach obejmuje także, co niespotykane, także kierownictwo osobiście aż do sześciu miesięcznych pensji. Wygląda więc na to, że nadzór jest zaplanowany starannie, ale – i tu wracamy do punktu wyjścia – nad kim dokładnie? Jedno, co wybrzmiało bardzo stanowczo z przemówienia D. Kamińskiego, to to, że „cyberbezpieczeństwo jest ryzykiem biznesowym. To już nie jest wyimaginowane zagrożenie".

Piotr Rogalewski z Hikvision Polska omawiał z kolei NIS2 w kontekście zabezpieczeń technicznych. Pytanie, na które próbował odpowiedzieć w swoim przemówieniu, brzmiało „Czy urządzenie może być zgodne z NIS 2?". Ekspert rozprawił się z nim krótko:

„Nie ma czegoś takiego". O zgodności możemy mówić w kontekście standardów, które są kompatybilne z NIS2. Te są oceniane przez odpowiednie jednostki certyfikujące, ale nie ma dedykowanej normy dotyczącej bezpieczeństwa cybernetycznego systemów zabezpieczeń technicznych. Rozwiązanie, jakie podsunął zgromadzonym, to korzystanie z tego, co jest, czyli norm:

- ISO27001 – podany w projekcie ustawy o Krajowym Systemie Cyberbezpieczeństwa,
- ISO22301,
- PN-EN 50131 – SSWiN,
- PN-EN 62676 – CCTV,
- PN-EN 60839 – systemy KD,
- RODO.

Także ustawa o KSC w rozdziale 3 określa obowiązki operatorów kluczowych. Mówią o tym w szczególności art. 8 i art. 10. Dodatkowym zestawem zabezpieczeń czy raczej dobrych praktyk pozostają standardowe procedury, czyli:

- cykl Deminga: Zaplanuj – Wykonaj – Sprawdź – Popraw,
- standard DORI w kamerach CCTV,
- metody techniczne zabezpieczeń,
- metody operacyjne: dobra komunikacja, edukacja itd.

Piotr Rogalewski podkreślił, że warto także zadbać o to, aby przy instalacji i korzystaniu z urządzeń nie przerywać łańcucha: producent–dystrybutor–integrator/instalator–klient końcowy. Od dobrej łączności między kolejnymi jego ogniwami zależy skuteczność wykonanych zabezpieczeń. →

Artur BOGUSZ z Muzeum Historii Polski

Warsztaty Piotra KARPIŃSKIEGO z firmy STid

BLOK 3 – filmy z wzorcowych wdrożeń, wzorcowe praktyki w zakresie security

A skoro o urządzeniach mowa, Warsaw Security Summit 2024 był także areną, na której zaprezentowano najnowsze rozwiązania oferowane przez firmy i stosowane przez instytucje takie jak goszczące zebranych w Muzeum Historii Polski. O tym imponującym obiekcie opowiedział pokrótce Artur Bogusz, szef bezpieczeństwa MHP, po czym wyświetlono film, z którego zebrani mogli dowiedzieć się m.in. jak zabezpieczyć 44 tys. mkw., na których znajduje się skarbiec, cenne zbiory, taras o powierzchni 7300 mkw. i rzesza ludzi: pracowników, odwiedzających i gości? W tym obiekcie wszystkiego jest więcej niż w przeciętnym tego typu – liczba ludzi i kubatura budynku potęgują liczbę potencjalnych zagrożeń. Przygotowanie planu zabezpieczenia takiej powierzchni trwało dwa lata, choć, jak podkreślał w filmie A. Bogusz, praca nad nim nigdy tak naprawdę się nie kończy. Pomysł zabezpieczenia budynku bezpośrednio wywodzi się z jego przeznaczenia. Na to, do czego budynek będzie wykorzystywany, nakładane są plany ochrony. Zabezpieczenia są proste, ale skuteczne – to m.in. 500 kamer, 250 przejść, 800 zamków mechanicznych, strefa cargo, śluzy. Zabezpieczenia wykonał HID.

Drugim ciekawym case study było zabezpieczenie i optymalizacja budynku Wydziału Filologicznego Uniwersytetu Łódzkiego, o czym opowiedzieli – na żywo oraz w wyświetlonym filmie – Aneta Sadach, kierowniczka administracyjna z UŁ, i Bartłomiej Gzymek z Genetec. Z tego nowoczesnego budynku o charakterze smart building na porządku dziennym korzysta 3,5 tys. studentów i 400 pracowników. Główne potrzeby UŁ z nim związane to zapewnienie bezpieczeństwa

i ograniczenie kosztów eksploatacji budynku. Potrzeby szczegółowe, na które także odpowiedziały rozwiązania security, to: rozładowanie niedrożnego systemu wydawania kluczy z dyżurki, ochrona pomieszczeń, w których znajduje się sprzęt o dużej wartości (np. studio TV, kabiny translatorskie), ale też zarządzanie salami w kontekście sprzątania, zarządzanie parkingiem, monitorowanie zużycia wody, prądu, lepsza organizacja czasu i wykorzystania pomieszczeń.

Aby usprawnić działanie tak dużego obiektu, ważne było znalezienie odpowiedniego systemu, który to wszystko zepnie. Proces rozpoczął się od rezygnacji z tradycyjnej szatni na rzecz szafek samoobsługowych, a kolejne zastosowane rozwiązania to: elektroniczny dostęp do wszystkich sal i pomieszczeń (łącznie ponad 100 przejść), czytniki w gabinetach pracowniczych, monitoring wizyjny na parkingu głównym i studenckim – kamery pozwalają wykryć drobne incydenty i ich sprawców, część jest z detekcją ruchu. Genetec ma plug-in IoT, dzięki któremu widzi wykorzystanie wody, energii itd.

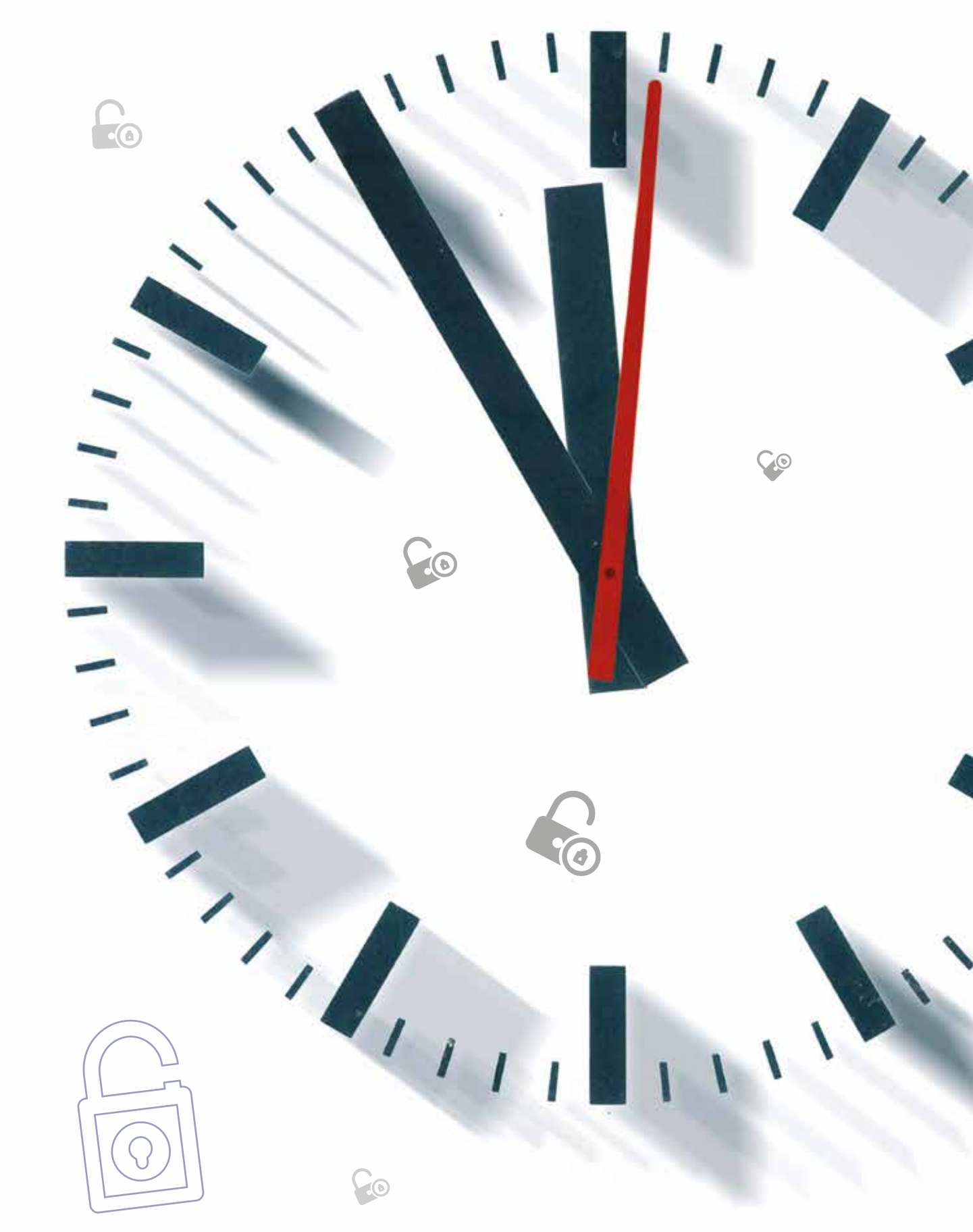
Arkadiusz Rymarski w imieniu firmy Linc w wystąpieniu partnerskim opowiedział o świadomości sytuacyjnej, tj. różnego rodzaju zabezpieczeniach, które stosujemy na co dzień, np. przegląd gazowy, serwis auta, płacenie ZUS-u, kask dla dziecka na rolki lub inwestycja w edukację. Niektóre z wymienionych zabezpieczeń wynikają z przymusu regulacyjnego, w innych przypadkach bywamy proaktywni. W przypadku zagrożeń cybersecurity warto przyjąć tę drugą postawę, przypominał prelegent. Są one jak najbardziej realne, a w przyszłości będą przybierać na sile i skali. Przytoczył szacunki, wg których już w tym momencie na świecie zapotrzebowanie na specjalistów cyberbezpieczeństwa sięga nawet 3,4 mln stanowisk! Swoje wystąpienie zakończył przywołaniem znanej historii Elishy Otisa, wynalazcy hamulca do wind, który konstruktor sam przetestował na oczach publiczności. Dzięki temu znacząco przyczynił się do zwiększenia zaufania do dźwigów osobowych, a tym samym do budowy wielopiętrowych wieżowców w Stanach Zjednoczonych.

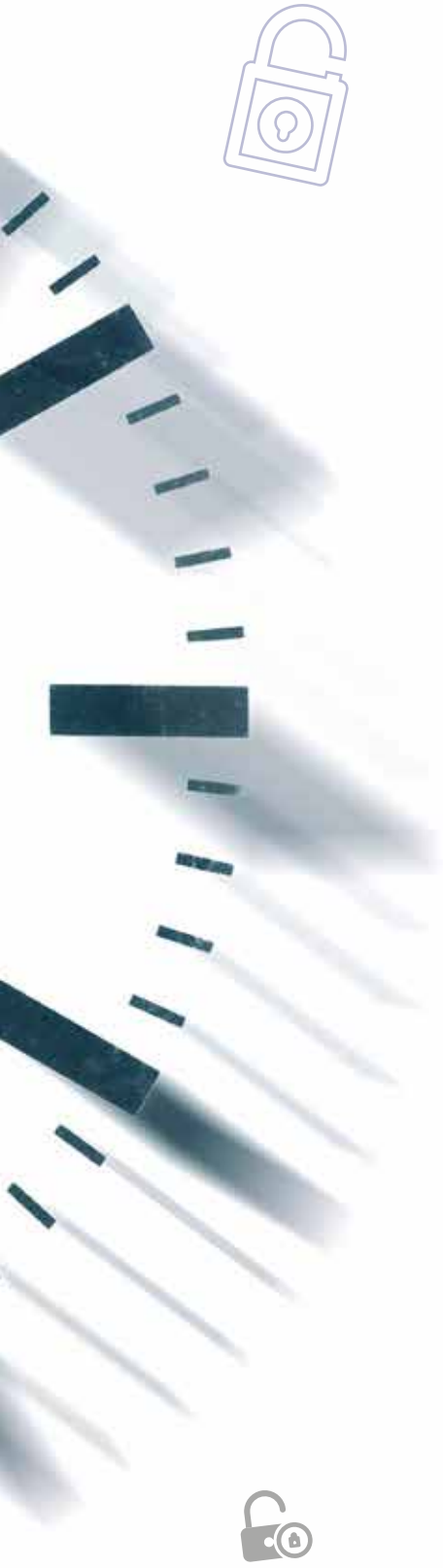
Warsaw Security Summit to także przestrzeń dla partnerów: Hikvision Polska, Linc Polska, Genetec, STid, EVVA, Hanwha Vision, Checly, HID, Novatel, a także Ministerstwa Cyfryzacji, które było patronem honorowym. Część z nich uczestnicy mogli poznać bliżej podczas warsztatów, które poprowadzili: Piotr Rogalewski z Hikvision, Artur Nowakowski, Michał Rzewuski, Wojciech Wesołek i Piotr Schwermer z Linc Polska, Łukasz Lik z Hanwha Vision oraz Piotr Karpiński ze STid.

Na zakończenie

Tegoroczny Warsaw Security Summit był poświęcony różnym aspektom bezpieczeństwa – od uwarunkowań prawnych po praktyczne rozwiązania, najnowsze z możliwych. Wnioski, jakie można wyciągnąć po wysłuchaniu wszystkich ekspertów, są takie, że mimo skomplikowanej sytuacji, w jakiej się jako kraj i jego obywatele znajdujemy, nie można uznać, że jesteśmy całkiem bezbronni wobec zagrożeń. Zarówno nowe technologie, jak i praktyki działania dają nam wiele możliwości zabezpieczenia się w różnych obszarach naszego życia. To zarówno ochrona przed dezinformacją, jak i fizyczna ochrona życia i mienia. Ze sceny MHP padło wiele podpowiedzi i konkretnych adresów, dalsza część była przekazywana w kuluarach, a w praktyce można było przećwiczyć podczas warsztatów. Wszystko to stanowi bezcenny zasób wiedzy, którego aktualizacja jest przewidziana za rok. ●

Networking we foyer





Raport: NIS2 – już za chwileczkę, już za momencik

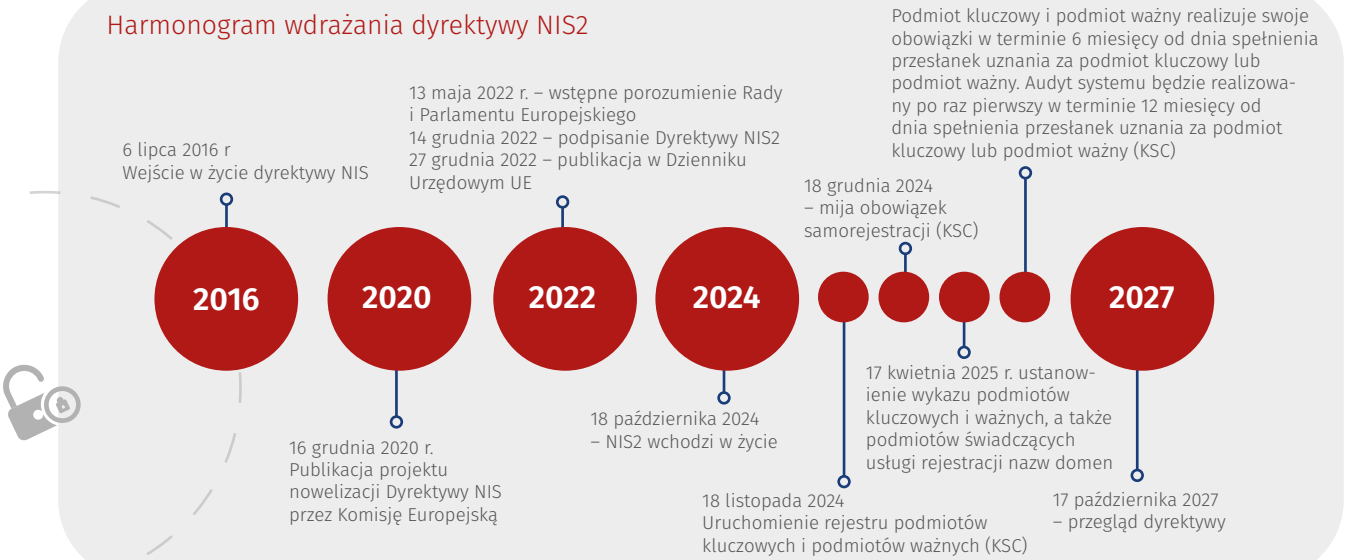
Dyrektywa NIS2 za 3 miesiące zacznie obowiązywać w Unii Europejskiej. Niektóre organizacje dążą do zapewnienia zgodności, inne mają trudności z wyjściem z bloków startowych. Zegar tyka i podmioty, które nie spełnią wymogów, będą musiały się liczyć z dotkliwymi karami finansowymi, a nawet z tymczasowym zawieszeniem świadczonych usług.

Jan T. Grusznic, a&s Polska

Dyrektywa Unii Europejskiej w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych (NIS) została przyjęta w 2016 r. Miała ona zapewnić wysoki poziom bezpieczeństwa sieci i systemów informatycznych w całej UE i wymagała wdrożenia środków bezpieczeństwa i obowiązków sprawozdawczych dla operatorów usług kluczowych i dostawców usług cyfrowych. Dyrektywa ta została wprowadzona do polskiego prawa jako ustawa o krajowym systemie cyberbezpieczeństwa, która zaczęła obowiązywać 28 sierpnia 2018 r.

Przeprowadzone kontrole i audyty funkcjonowania po wprowadzeniu dyrektywy NIS z 2016 r. w państwach członkowskich wykazały, że wdrożenie przepisów unijnych w zakresie cyberbezpieczeństwa odbywało się w różnym zakresie, nie zawsze spójnym, a ich egzekwowanie było, delikatnie rzecz ujmując, niewystarczające. W tym czasie świat cyfrowy uległ ogromnym zmianom w dużej mierze w związku

Harmonogram wdrażania dyrektywy NIS2

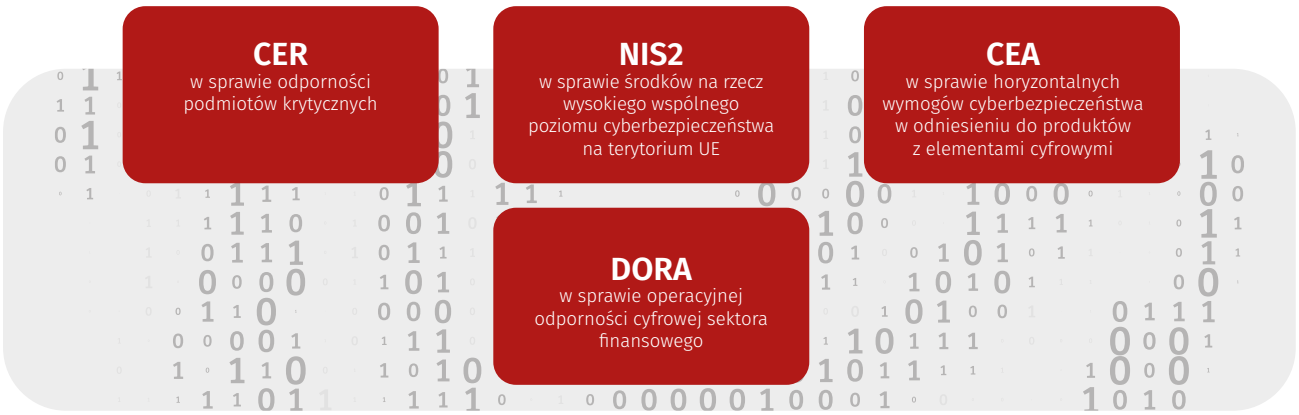


z pandemią, która uruchomiła lawinowy wzrost wykorzystania cyfrowych usług powszechnych. Jednocześnie następująca konwergencja obszarów automatyki przemysłowej, IoT z rozwiązaniami IT, transformacja do rozwiązań przemysłu 4.0, wykorzystanie sieci definiowanych programowo, a także postępująca praca zdalna oraz masowe upowszechnienie się rozwiązań i usług chmurowych, w tym SaaS, przyniosły skokowy wzrost liczby cyberzagrożeń zagrażających nie tylko obywatelom czy firmom, ale także, a może przede wszystkim ciągłości działania krytycznych z punktu państwa usług czy infrastruktury.

Według raportów czołowych producentów cyberzabezpieczeń i wywiadowni gospodarczych blisko 30% światowych organizacji może doświadczyć co najmniej jednego naruszenia w ciągu najbliższych 24 miesięcy. Średni koszt naruszenia bezpieczeństwa danych (w tym wykrycie, straty biznesowe, reagowanie po naruszeniu i powiadamianie) wyniósł 4,45 mln USD, osiągając najwyższy poziom w historii (*Cost of a Data Breach Report 2023,* IBM). W roku 2023 odnotowano 6077 naruszeń danych – co stanowi wzrost o 34,5% w porównaniu z 2022 r. Naruszenia danych są odpowiedzialne za wyciek ponad 17 mld rekordów. Ponad 70% tych incydentów było wynikiem nieautoryzowanego dostępu (*2024 Global Threat Intelligence Report,* Flashpoint). Utrata informacji poufnych może kosztować firmy miliony dolarów każdego roku. Jeden rekord danych, który wyciekł w 2023 r., kosztował średnio 165 USD, a cyberprzestępcy zwykle próbują przejąć najbardziej poufne informacje. W zeszłym roku 52% wszystkich incydentów naruszenia danych w globalnych organizacjach dotyczyło danych osobowych klientów, co czyni je najczęściej naruszanym rodzajem danych. Około czterech na dziesięć naruszeń danych dotyczyło danych osobowych pracowników. Co więcej, wg serwisu Statista aż 76% ataków socjotechnicznych spowodowało utratę danych uwierzytelniających.

Atakujący wykorzystują kilka metod naruszenia bezpieczeństwa systemów, począwszy od zestawów exploitów, skończywszy na blokadzie usługi w wyniku ataku DoS, do których doszło za pośrednictwem *phishingu* i oprogramowania *ransomware*. Wzrost liczby ataków jest związany z prostym faktem, że jest to dla atakujących działalność opłacalna. Przyjmuje się, że miesięczny przychód cyberprzestępcy wynosi około 90 tys USD. Z drugiej strony koszty ataków nie są wygórowane. Wystarczy 327 USD, aby poprowadzić tygodniowy atak DDoS na aplikację internetową, paraliżując firmę. Wykorzystanie botów – czyli zainfekowanych urządzeń – zaczyna się od 13 centów, dostęp do listy przejętych par login–hasło od niecałego 1 USD za 1000 pozycji. Nieco droższe są usługi *ransomware*.

Regulacje EU dotyczące budowania cyberodporności



Jednorazowa opłata „z góry” to ok. 66 USD (jest też opcja udziału w zyskach, sic!). Za pomyślne przejęcie konta dokonane w ramach *spearphishingu* trzeba zapłacić od 100 do nawet 1000 USD. Najdroższe jest wykorzystanie luk w zabezpieczeniach, tzw. *zero-days*. Koszt takiej usługi zależy od „istotności” urządzenia z podatnością oraz czasu, jaki minął od jej wykrycia, stąd dość szeroki zakres cenowy: od 5 tys. USD do nawet 7 mln USD.

Na takie usługi jest popyt, stąd konieczność usystematyzowanej obrony. Rosnące wyrafinowanie zagrożeń cybernetycznych i szybki postęp technologiczny ujawniły potrzebę bardziej kompleksowego i spójnego podejścia do problemu stworzenia i utrzymania wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych, co pośrednio przełoży się również na wzrost zaufania do cyfrowego rynku UE i konkurencyjności europejskich podmiotów cyfrowych na arenie globalnej. Dyrektywa NIS2 została opracowana w celu wyeliminowania niedociągnięć ujawnionych w raporcie oceniającym NIS1 i ustanowienia wyższego standardu odporności cybernetycznej w całej UE. Ma wspomóc w zwiększeniu ochrony i odporności na cyberzagrożenia, zwiększeniu zdolności i umiejętności do reagowania na incydenty i kryzysy cyberbezpieczeństwa oraz odbudowy po nich oraz zwiększeniu bezpieczeństwa i ochrony danych osobowych w cyberprzestrzeni. W przeciwieństwie do swojej poprzedniczki nowa dyrektywa rozszerza swój zasięg poza sektory infrastruktury krytycznej i zwiększa liczbę objętych sektorów gospodarki z 7 do 18, obejmując szerszy wachlarz dostawców usług cyfrowych i MŚP, uznając, że bezpieczeństwo jednego z nich jest powiązane z bezpieczeństwem wszystkich podmiotów łańcucha dostaw. Badania bowiem pokazują, że 62% naruszeń bezpieczeństwa ma charakter pośredni.

Kto będzie objęty NIS2?

NIS2 ma zastosowanie do wszystkich podmiotów zatrudniających co najmniej 50 pracowników i mających roczny obrót w wysokości 10 mln euro lub wyższy, które świadczą istotne usługi na rzecz europejskiej gospodarki i społeczeństwa, w tym przedsiębiorstw i dostawców, co obejmuje również organizacje mające siedzibę poza UE, ale świadczące usługi w UE. Chociaż dyrektywa zawiera wyłączenia dla małych organizacji, należy oczekiwać, że większe przedsiębiorstwa włączą kontrole NIS2 do swoich programów oceny ryzyka stron trzecich, a zatem większość organizacji będzie musiała zająć się NIS2, aby być konkurencyjna.

Sklasyfikowani w ramach NIS1 operatorzy usług kluczowych w NIS2 zostali uznani za podmioty kluczowe. Wraz z tą zmianą zostało wprowadzone pojęcie podmiotów ważnych. Na to, czy podmiot jest kluczowy, czy „tylko” ważny, wpływają obszar działalności w sektorach objętych dyrektywą oraz zasada wielkościowa, tj. spełnienie wymagań dla przedsiębiorstwa średniego wg zalecenia Komisji Europejskiej 2003/361. A zatem podmioty kluczowe to podmioty prowadzące działalność w co najmniej jednym sektorze: energetycznym, transportowym, bankowości, infrastrukturze rynków finansowych, opiece zdrowotnej, wody pitnej, ściekach, infrastrukturze cyfrowej, zarządzania usługami ICT, administracji publicznej lub przestrzeni kosmicznej oraz zatrudniające co najmniej 250 pracowników z obrotem rocznym min. 50 mln euro lub z roczną sumą bilansową nie mniejszą niż 43 mln euro. Podmioty niespełniające wymagań dla średniego przedsiębiorstwa, a prowadzące działalność w wymienionych sektorach zostają uznane za podmioty ważne. Podmiotami ważnymi wg dyrektywy są też te

Wykaz sektorów kluczowych i ważnych

firmy, których główna działalność mieści się w co najmniej jednym z 7 sektorów: usług pocztowych i kurierskich, gospodarce odpadami, produkcji i dystrybucji chemikaliów, produkcji i dystrybucji żywności, produkcji, dostawcy usług cyfrowych lub badań naukowych. Zasada wielkościowa nie dotyczy jednak kwalifikowanych dostawców usług zaufania i rejestrów nazw domen najwyższego poziomu, a także dostawców usług DNS, podmiotów wskazanych jako podmioty krytyczne na podstawie dyrektywy CER (Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych), podmiotów publicznych i innych, dla których zakłócenie świadczonej przez nich usługi mogłoby prowadzić do powstania poważnego ryzyka systemowego lub mieć znaczący wpływ na porządek, bezpieczeństwo lub zdrowie publiczne. Przekrój wielkości firmy względem sektorów z podziałem na podmioty kluczowe i ważne został zaprezentowany na rys. *Wykaz sektorów kluczowych i ważnych.*

→

9 punktów

zbliżających Twoją organizację do spełnienia wymogów dyrektywy NIS2

Zidentyfikuj, oceń i zajmij się ryzykiem: zidentyfikuj zagrożenia dla swojej organizacji, oceń ich wpływ i podejmij kroki w celu ich złagodzenia.

Oceń swój stan bezpieczeństwa: ocena ryzyka i bezpieczeństwa może pomóc w zidentyfikowaniu słabych punktów, takich jak niezarządzane hasła lub nieprawidłowo skonfigurowane, bądź nieaktywne konta, które są podatne na kradzież danych uwierzytelniających. Przeprowadź kompleksową ocenę bezpieczeństwa, aby ocenić stan bezpieczeństwa przedsiębiorstwa i zidentyfikować obszary wymagające poprawy, takie jak wprowadzenie czynników uwierzytelniania odpornych na *phishing*.

Podejmij kroki w celu zabezpieczenia dostępu uprzywilejowanego: cyberprzestępcy mogą wykorzystywać konta uprzywilejowane do organizowania ataków, wyłączania krytycznych elementów z punktu widzenia ciągłości działania i zakłócania podstawowych usług. NIS2 zaleca ograniczenie dostępu do kont na poziomie administratora i regularną zmianę haseł. Zabezpiecz uprzywilejowany dostęp poprzez wdrożenie najlepszych praktyk, takich jak dostęp z najmniejszymi uprawnieniami, ciągłe uwierzytelnianie i ograniczona liczba prób logowania.

Wzmocnij ochronę przed *ransomware*: kosztowne i wyniszczające ataki *ransomware* są głównym powodem do niepokoju organów regulacyjnych UE i jednym z głównych czynników napędzających dyrektywę NIS2. Wprowadź rozwiązania bezpieczeństwa i najlepsze praktyki, aby proaktywnie bronić się przed oprogramowaniem *ransomware*. Egzekwuj zasadę najmniejszych uprawnień, kontroluj działanie aplikacji i rozszerz posiadane oprogramowanie antywirusowe do nowej generacji *(Next-generation antivirus* – NGAV, który wykorzystuje zaawansowane metody detekcji i usuwania zagrożeń, aby wzmocnić ochronę przed atakami cybernetycznymi, i jest bardziej zorientowany na prewencję niż na reakcję), używaj narzędzi wykrywania i reagowania na podejrzane aktywności w punktach końcowych (EDR/XDR - *Endpoint/ Extended Detection and Response).*

Wprowadź strategię *Zero Trust:* w modelu zabezpieczeń obwodowych, w którym ufa się połączeniom po uwierzytelnieniu i przyznaje dostęp do całej sieci, wystawiając aktywa przedsiębiorstwa na potencjalne ataki cyberprzestępców. W architekturze *Zero Trust* zakłada się, że żadne połączenia, aktywa ani użytkownicy nie są godni zaufania dopóty, dopóki nie zostaną zweryfikowani. Przyjmij podejście *Zero Trust*, wdrażając kilka warstw obrony, takich jak dostęp z najmniejszymi uprawnieniami, dokładnie weryfikuj i analizuj zagrożenia w celu weryfikacji wszystkich prób dostępu.

Przeanalizuj łańcuch dostaw: zapewnienie integralności i bezpieczeństwa łańcucha dostaw jest fundamentalnym aspektem NIS2. Aby zminimalizować ryzyko cyberataków ze strony osób trzecich, wykraczaj poza przeprowadzanie regularnych ocen ryzyka w swoim łańcuchu dostaw. Kluczowe znaczenie ma zapewnienie, że wszyscy partnerzy w łańcuchu na co dzień spełniają wymogi NIS2. Wiąże się to z wdrożeniem środków bezpieczeństwa, takich jak przeprowadzanie ocen ryzyka i audytów dostawców, zawieranie umów określających konkretne wymogi bezpieczeństwa oraz utrzymywanie stałego monitorowania i komunikacji z dostawcami. Zapewniając, że dostawcy przestrzegają zaktualizowanych wymagań NIS2, skutecznie zmniejszysz ogólne ryzyko i wzmocnisz bezpieczeństwo swojej infrastruktury cyfrowej. Oczekuj od dostawców dostarczania raportów zgodnych ze standardami branżowymi, takimi jak ISO 27001, i raportów z zewnętrznych testów penetracyjnych. Umożliwiaj swoim klientom przeprowadzanie własnych testów penetracyjnych.

Wprowadź politykę informacyjną dotyczącą ewentualnych luk w cyberbezpieczeństwie: NIS2 wymaga posiadania przez organizację udokumentowanych, aktualizowanych analiz i oszacowania ryzyk oraz bezpieczeństwa systemów informatycznych: identyfikacji, analizy, planu łagodzenia. Dobrze przygotowana, przedyskutowana i uzgodniona z zarządem oraz udokumentowana analiza ryzyka pozwala na spełnienie wymagań NIS2, ale przede wszystkim jest najlepszym sposobem na przekonanie zarządu, że cyfrowe bezpieczeństwo czasami wymaga nakładów finansowych. W oszacowaniu budżetu i środków na minimalizację ryzyka wykorzystaj specyfikę organizacji, raporty o zagrożeniach czy przypadki cyberataków na podobne organizacje. Weź pod uwagę koszty przestojów, niedostępności usług, odzyskiwania danych i działań zmierzających do przywrócenia pracy. Uwzględnij szacunkowe koszty kar NIS2, szkody dla powiązanych przedsiębiorstw itp.

Wprowadź systematyczne szkolenia pracowników: dyrektywa wskazuje na obowiązek wykonywania cyklicznych szkoleń dla pracowników i współpracowników wszystkich szczebli. Dostosuj moduły szkoleniowe w zakresie podnoszenia świadomości użytkowników do specyfiki organizacji. Przeprowadź testy socjotechniczne jako element proaktywnej edukacji, aby określić, na jakie obszary cyberochrony należy zwrócić szczególną uwagę.

Wprowadź procedury bezzwłocznego powiadamiana o incydentach związanych z cyberbezpieczeństwem: NIS2 wymaga szybkiego zgłaszania incydentów o ich charakterze, wymagając złożenia wstępnego raportu w ciągu 24 godz. od zdarzenia, a następnie raportu technicznego w ciągu 72 godz. i pogłębionego, szczegółowego raportu w ciągu 30 dni. Aby sprostać temu wymaganiu, kluczowe jest ustanowienie dobrze zorganizowanego planu reagowania na incydenty. Zdolność do kompleksowego wglądu w próby autoryzacji i dostępu w różnych infrastrukturach i technologiach pomaga organizacjom w rekonstrukcji sieci lub zasobów, co jest kluczowym elementem raportowania incydentów. Aby zapewnić zgodność z wymogami NIS2, przeanalizuj powiadomienia o zdarzeniach, gromadź informacje i procedury raportowania. Regularne ćwiczenia mogą być również niezbędne do oceny i zwiększenia skuteczności planu reagowania.

Obowiązki podmiotów objętych NIS2

Dyrektywa nakłada na podmioty podlegające NIS2 obowiązek wdrożenia odpowiednich i proporcjonalnych środków technicznych, operacyjnych i organizacyjnych w celu ograniczenia zagrożeń bezpieczeństwa sieci i systemów informatycznych oraz środowiska fizycznego tych systemów przed incydentami. Nakłada również na organizacje obowiązek zgłaszania właściwym organom incydentów związanych z bezpieczeństwem i wprowadza bardziej rygorystyczne wymogi sprawozdawcze dla tych podmiotów.

W ramach środków regulacja wymienia:

- zarządzanie incydentami;
- opracowanie polityk analizy ryzyka i bezpieczeństwa systemów IT;
- opracowanie polityk i procedur ocen skuteczności środków zarządzania ryzykiem z zakresu cyberbezpieczeństwa;
- opracowanie polityk i procedur dotyczących stosowania kryptografii i szyfrowania;
- zapewnienie ciągłości działania firmy poprzez zarządzanie kopiami zapasowymi, przywracanie stanu sprzed awarii oraz zarządzanie kryzysowe;
- zapewnienie bezpieczeństwa łańcucha dostaw, włączając relacje z dostawcami usług;
- zapewnienie bezpieczeństwa w zakresie nabywania, rozwijania i utrzymywania sieci i systemów IT, wraz z obsługą podatności i ich ujawniania;
- dobre praktyki i szkolenia z zakresu cyberbezpieczeństwa;
- zabezpieczanie zarządzania zasobami, m.in. zasobami HR;
- stosowanie uwierzytelniania wieloskładnikowego lub uwierzytelniania ciągłego i bezpiecznych systemów komunikacji w organizacji.

Nie sposób w tym miejscu nie wspomnieć o ISO 27001, międzynarodowym standardzie zarządzania bezpieczeństwem informacji, który zapewnia ramy dla ustanawiania, wdrażania, utrzymywania i ciągłego doskonalenia systemu zarządzania bezpieczeństwem informacji. Norma ma na celu pomóc organizacjom w zarządzaniu ryzykiem związanym z bezpieczeństwem informacji i ochronie ich zasobów informacyjnych. NIS2 i ISO 27001 mają wspólny cel, jakim jest poprawa bezpieczeństwa sieci i systemów informatycznych. W związku z tym NIS2 można „nałożyć" na ISO 27001, umożliwiając organizacjom wykorzystanie istniejącej certyfikacji ISO 27001 do spełnienia wymagań NIS2.

Co robić? Jak żyć?

Bezpieczeństwo jest trudne, ponieważ wymaga poruszania się w temacie złożonej interakcji ludzi, procesów i technologii. W tym krajobrazie tożsamość odgrywa kluczową rolę jako kamień węgielny strategii cyberbezpieczeństwa i utrzymania solidnej higieny cybernetycznej przy jednoczesnym osiągnięciu zgodności z ramami regulacyjnymi takimi jak NIS2.

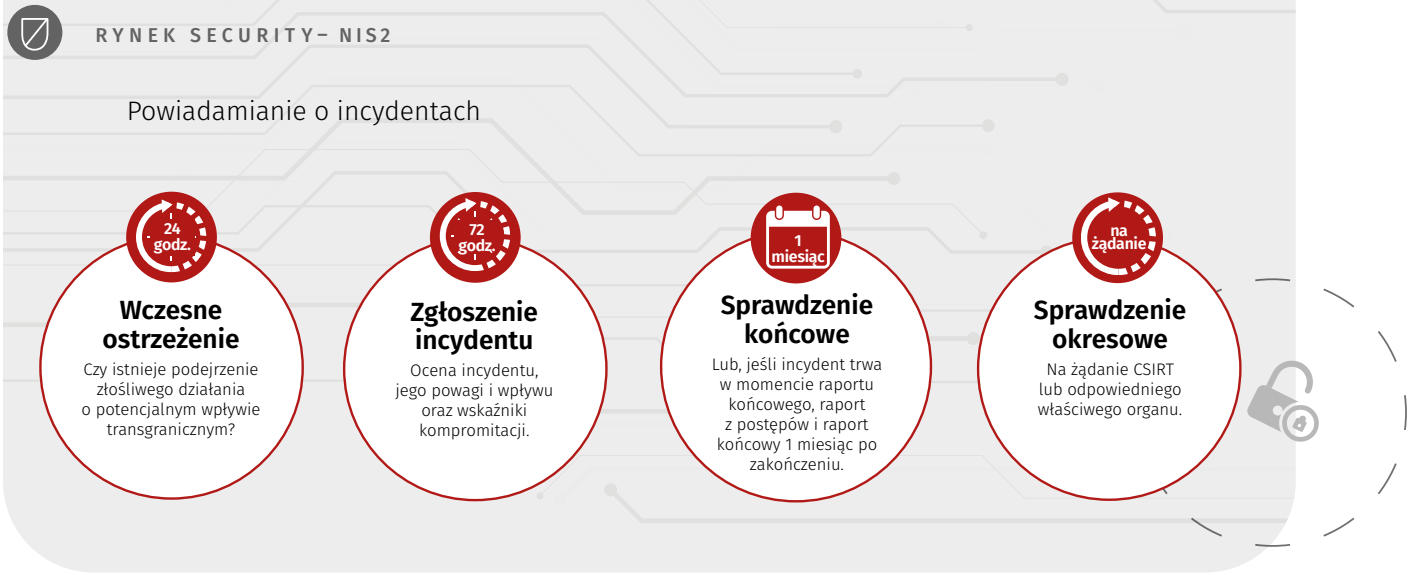
Tożsamość jest podstawą polityki bezpieczeństwa, procedur operacyjnych i systemów informatycznych regulujących dostęp do informacji krytycznych w organizacji. Obejmuje weryfikację tożsamości użytkowników, uwierzytelnianie ich dostępu, autoryzację ich działań i uprawnień oraz zarządzanie kontrolą dostępu. Skuteczne zarządzanie tożsamością zapewnia, że tylko upoważnione osoby otrzymują dostęp do określonych zasobów, umożliwiając im odpowiednie wykorzystanie tych zasobów przy najmniejszych uprawnieniach niezbędnych do wypełnienia ich obowiązków. Dodatkowe warstwy zabezpieczeń, takie jak uwierzytelnianie wieloskładnikowe, również zwiększają ochronę tożsamości. W kontekście zgodności z przepisami takimi jak NIS2 tożsamość stanowi potężne narzędzie do ograniczania ryzyka związanego z nieautoryzowanym dostępem. Ustanawia odpowiedzialność w organizacji, umożliwiając identyfikację osób odpowiedzialnych za działania, ułatwiając w ten sposób identyfikowalność. Ponadto zarządzanie tożsamością pozwala na efektywne zarządzanie użytkownikami, usprawniając procesy administracyjne przy jednoczesnym zachowaniu bezpiecznego środowiska organizacyjnego. Dobrze opracowane rozwiązanie do zarządzania tożsamością zapewnia łatwo dostępną ścieżkę audytu w aplikacjach krytycznych organizacji, które wykazują odpowiednią kontrolę dostępu i zarządzanie autoryzacją. NIS2 wymaga od organizacji wdrożenia środków zarządzania ryzykiem dla bezpieczeństwa sieci i systemów informatycznych. Zarządzanie tożsamością umożliwia organizacjom monitorowanie i audyt działań użytkowników zgodnie z wymogami regulacyjnymi, a także wykazanie odpowiedzialności poprzez udokumentowanie, kto i kiedy uzyskał dostęp do określonych zasobów.

> *» Należy oczekiwać, że większe przedsiębiorstwa włączą kontrolę NIS2 do swoich programów oceny ryzyka stron trzecich, a zatem większość organizacji będzie musiała zająć się NIS2, aby być konkurencyjna. «*

Egzekwowanie przepisów, czyli co grozi firmom, które się nie dostosują

Nieprzestrzeganie dyrektywy NIS2 może skutkować nałożeniem kar administracyjnych. W przypadku podmiotów kluczowych może to być grzywna w wysokości 10 mln euro lub 2% globalnego rocznego przychodu w zależności od tego, która z tych kwot jest wyższa. W przypadku podmiotów ważnych, czyli przedsiębiorstw funkcjonujących w sektorach takich jak dostawy żywności, chemikalia, usługi pocztowe, gospodarka odpadami, produkcja itp., kara może wynosić 7 mln euro lub 1,4% rocznego przychodu, w zależności od tego, która z tych kwot jest wyższa. Ponadto art. 32 ust. 5 przewiduje, że podmiot kluczowy, który nie zastosuje się do wymagań, może zostać ukarany tymczasowym zawieszeniem certyfikacji (w rozumieniu rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r.) lub zezwolenia na niektóre lub wszystkie usługi świadczone bądź na część lub całość działalności prowadzonej przez podmiot kluczowy. Certyfikaty mogą zostać zamrożone, a dyrektor generalny

→



lub przedstawiciel prawny może zostać czasowo pozbawiony możliwości wykonywania swoich funkcji kierowniczych.

Dyrektywa NIS2 a polskie prawodawstwo

W ślad za dyrektywą NIS2 pojawił się projekt nowelizacji Ustawy o Krajowym Systemie Cyberbezpieczeństwa (UKSC). Jego treść może się zmienić, ale na pewno będzie rewolucją dla wielu przedsiębiorstw. Ustawa ma wejść w życie 18 października 2024 r. Liczący 133 strony i datowany na 23 kwietnia 2024 r. projekt modyfikuje istniejącą Ustawę o KSC oraz wprowadza niewielkie zmiany do innych aktów prawnych. Dotyczy to przede wszystkim sektorów uznanych w dyrektywie NIS2 za ważne, a w polskiej propozycji zaklasyfikowano jako kluczowe, np. produkcja żywności, chemikaliów czy produkcja ogólna (np. pojazdów, maszyn, komputerów czy urządzeń elektrycznych), co zwiększa restrykcyjność regulacji polskich w stosunku do wymagań z NIS2. Organizacje będą zobowiązane złożyć wniosek o wpisanie do wykazu podmiotów kluczowych i ważnych w ciągu 2 miesięcy od spełnienia wymogów stawianych tym podmiotom (lub od wejścia ustawy w życie). Ustawa zobowiązuje również podmioty do stosowania systemu zarządzania ryzykiem na podobnych zasadach jak w NIS2. W tym zakresie istotnym novum jest określenie, że spełnienie wymagań określonych w Polskiej Normie PN-EN ISO/IEC 27001 oraz PN-EN ISO/IEC 22301 będzie uznawane za spełnienie wymogów w zakresie systemu zarządzania bezpieczeństwem informacji.

Podmioty kluczowe i ważne będą musiały zgłaszać incydenty odpowiednio w ciągu 24 godz. (wczesne zgłoszenie), 72 godz. (właściwe zgłoszenie) i miesiąca (sprawozdanie końcowe) zgodnie z NIS2, jednak w przypadku przedsiębiorców komunikacji elektronicznej i dostawców usług zaufania terminy te zostały skrócone. Pojawiała się możliwość nałożenia kary kwalifikowanej w wysokości do 100 mln zł w przypadkach, gdy naruszenie spowodowało m.in. bezpośrednie zagrożenie bezpieczeństwa państwa czy wywołania poważnej szkody majątkowej.

Największą kontrowersją jednak jest polecenie zabezpieczające, które w przypadku incydentów krytycznych obejmuje nakazy i zakazy różnych działań, w tym np. nakaz zastosowania określonej poprawki czy zakaz korzystania z określonych produktów lub usług ICT. UKSC wprowadza nieuregulowaną w dyrektywie NIS2 procedurę umożliwiającą uznanie danego dostawcy za dostawcę wysokiego ryzyka. Zastosowanie tzw. toolBox 5G (zestaw narzędzi określa szereg środków bezpieczeństwa, które mają na celu skuteczne ograniczenie ryzyka i zapewniają bezpieczne wdrożenie sieci 5G w całej Europie) we wszystkich 18 sektorach (a nie tylko z zakresu telekomunikacji) spowoduje wykluczenie wielu wytwórców z każdego z 18 sektorów w Polsce, podczas gdy ci sami dostawcy będą mogli bez przeszkód działać w innych krajach Unii Europejskiej. Takie postępowanie wiązałoby się z koniecznością pozbycia się takiego sprzętu w określonym czasie (co do zasady 7 lat) i nabycia nowego, powodując ogromne koszty, co nie zostało uwzględnione w Ocenie Skutków Ryzyka.

Nowe przepisy mają wejść w życie po upływie 1 miesiąca od dnia ogłoszenia, a podmioty objęte ustawą będą miały zaledwie 6 miesięcy na dopełnienie niektórych obowiązków wskazanych w projekcie ustawy.

NIS2 jako część systemu prawnego na rzecz cyberbezpieczeństwa

Proces transpozycji dyrektywy CER do prawa polskiego już się rozpoczął. Nowa dyrektywa została skorelowana z NIS2 i zachowuje spójne podejścia między Dyrektywą o odporności a Dyrektywą NIS2. Według przepisów Dyrektywy CER państwa członkowskie są zobowiązane do przyjęcia strategii mającej na celu wzmocnienie odporności podmiotów krytycznych, na których ciąży obowiązek ochrony infrastruktury niezbędnej do utrzymania usług kluczowych. Co ciekawe, podmioty objęte CER mogą liczyć na wsparcie finansowe ze strony państwa, jeśli będzie to uzasadnione bezpieczeństwem publicznym. Takie wsparcie nie zostanie potraktowane jako niedozwolona pomoc publiczna.

Pod koniec 2024 r. ma zostać uchwalony unijny akt w sprawie odporności cybernetycznej (CRA, Rozporządzenie Parlamentu Europejskiego i Rady w sprawie horyzontalnych wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi i zmieniające rozporządzenie UE 2019/1020), które będzie pierwszym na świecie rozporządzeniem określającym wymogi bezpieczeństwa dotyczące produktów, których spełnienie będzie niezbędne, by produkt mógł się pojawić na rynku. Innymi słowy: bez stosownych zabezpieczeń „produkty z elementami cyfrowymi" nie będą już mogły być oferowane w UE od 2027 r. Unijny akt o odporności cybernetycznej (CRA) został przyjęty przez Parlament Europejski 12 marca 2024 r. i czeka na zgodę Rady Europejskiej, aby zacząć obowiązywać we wszystkich państwach członkowskich UE, ponieważ w przeciwieństwie np. do NIS2 akt CRA nie jest dyrektywą, która musi być najpierw przeniesiona na grunt prawa krajowego, ale rozporządzeniem. Oznacza to, że po upływie 36-miesięcznego okresu przejściowego wymogi CRA będą miały zastosowanie do producentów produktów, których dotyczą zapisy. Oznacza to, że producenci będą musieli dostosować się do tych wymagań już od 2027 r. ●

SYSTEMY OCHRONY TECHNICZNEJ

TELBUD SA

PROJEKT - BUDOWA - INTEGRACJA

OCHRONA PERYMETRYCZNA
MONITORING WIZYJNY
SYGNALIZACJA WŁAMANIA I NAnapadu

SYSTEM PRZECIWPOŻAROWY
KONTROLA DOSTĘPU
SYSTEM ANTYDRONOWY

ARGUS

ZINTEGROWANE SYSTEMY BEZPIECZEŃSTWA OBIEKTÓW

MSPO

SPOTKAJMY SIĘ

podczas **Międzynarodowego Salonu Przemysłu Obronnego**
Kielce, 3-6 września 2024, **hala B stoisko 43**

www.telbud.pl

Gotowi na NIS2

Dyrektywa NIS2 jest dla bezpieczeństwa cybernetycznego tym, czym RODO stało się dla ochrony danych osobowych. To pierwsza tak poważna i kompleksowa próba stworzenia spójnego systemu odporności w zakresie bezpieczeństwa cybernetycznego na obszarze Unii Europejskiej.

Piotr Rogalewski

Dyrektywa została przyjęta 14 grudnia 2022 r., państwa członkowskie UE zaś muszą zaimplementować ją właściwym prawem lokalnym do 17 października 2024 r. W Polsce aktem implementującym NIS2 jest nowelizacja Ustawy o Krajowym Systemie Cyberbezpieczeństwa, której projekt zamieszczono na rządowych stronach. Konsultacje społeczne do projektu nowelizacji trwały do 24 maja i obecnie jest opracowywana ostateczna wersja tekstu ustawy, uwzględniająca wnioski z konsultacji. W artykule skupimy się przede wszystkim na technicznych konsekwencjach wprowadzenia NIS2.

„Nasze kamery są zgodne z NIS2", czyli jak nie robić marketingu

Podobnie jak przy innych zagadnieniach nowych dla branży zabezpieczeń technicznych, tak i przy okazji dyskusji o NIS2 pojawia się wiele nieporozumień, półprawd czy prób marketingowego wykorzystania sytuacji, włącznie z takimi pomysłami, jak deklaracje typu „nasze produkty są zgodne z NIS2" czy naklejki *NIS2 compliant* („zgodne z NIS2") umieszczane np. na opakowaniach kamer telewizji dozorowej, co jest przekazem absurdalnym, poieważ nie ma żadnej normy opisującej wymagania dotyczące bezpieczeństwa cyfrowego w urządzeniach zabezpieczeń technicznych. Nie ma więc nawet kryteriów, według których taką zgodność można by w ogóle badać.

To gdzie jest ta zgodność?

O czym możemy zatem rozmawiać w kontekście zgodności systemów zabezpieczeń technicznych z dyrektywą NIS2? O normach, które ustawa o KSC przywołuje literalnie, a także tych, które odnoszą się do poszczególnych elementów systemów zabezpieczeń technicznych. I tak np. w rozdziale 3 „Obowiązki operatorów usług kluczowych", w art. 8. ustawy o KSC czytamy:

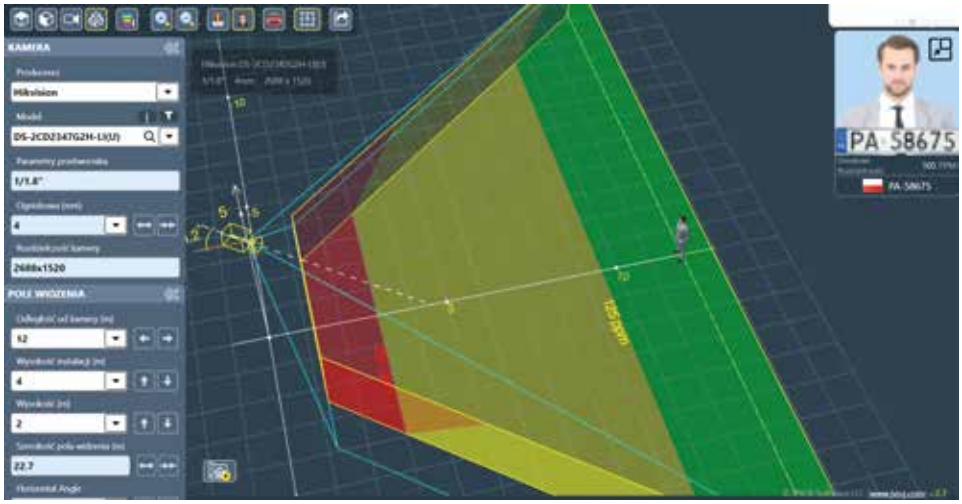
1. Podmiot kluczowy lub podmiot ważny wdraża system zarządzania bezpieczeństwem informacji w procesach wpływających na świadczenie usług przez ten podmiot, zapewniający: [tu następuje lista wymagań]
2. Wymagania, o których mowa w ust. 1, uznaje się za spełnione, gdy podmiot kluczowy i podmiot ważny zapewniają system zarządzania bezpieczeństwem informacji, z uwzględnieniem wymagań określonych w Polskiej Normie PN-EN ISO/IEC 27001 oraz PN-EN ISO/IEC 22301.

I dalej w art. 10:

(...) 2. Wymagania, o których mowa w ust. 1, uznaje się za spełnione, gdy podmiot kluczowy i podmiot ważny zapewniają system zarządzania bezpieczeństwem informacji, z uwzględnieniem wymagań określonych w Polskiej Normie PN-EN ISO/IEC 27001 oraz PN-EN ISO/IEC 22301.

Przywołano więc konkretne normy, których spełnienia wymaga się od operatorów usług kluczowych. Weźmy np. ISO/IEC 27001. Norma ta opisuje System Zarządzania Bezpieczeństwem Informacji, co jest pojęciem bardzo szerokim i obejmuje cały ekosystem organizacji. Jest więc zdecydowanie dobrym pomysłem, aby producenci urządzeń i usług wykorzystywanych przez operatora usług kluczowych także wdrożyli model ISO/IEC 27001 w swojej organizacji. Gwarantuje to kompatybilność procesów i zwiększa poziom bezpieczeństwa w całej relacji biznesowej producent – operator. A jeśli wspomniany producent jest

Rys. 1. Cykl Deminga jako fundament normy ISO/IEC 27001.
Źródło grafiki: www.wikipedia.com



Rys. 2. Kryteria DORI jako jeden z kluczowych elementów normy PN-EN 62676.
Źródło grafiki: www.jvsg.com

również dostawcą usług security o dużej skali (np. VSaaS czy chmura do obsługi urządzeń mobilnych), to – w pewnych okolicznościach – sam może wprost podlegać wynikającemu z NIS2 obowiązkowi zgodności z normą PN-EN ISO/IEC 27001.

Przy okazji dyskusji o ISO 27001 chyba najczęściej poruszanym obszarem jest przepływ informacji i dokumentów w organizacji. Warto jednak pamiętać, że obraz, dane z systemu kontroli dostępu czy zdarzenia SSWiN to także informacje. Tak, ISO 27001 dotyczy także systemów ochrony technicznej jako integralnej części infrastruktury technicznej organizacji, w której ten standard się wdraża. Z kolei cykl Deminga, będący fundamentem zarządzania bezpieczeństwem informacji, doskonale nadaje się do utrzymania systemów ochrony technicznej w kontekście wdrażania i systematycznej aktualizacji strategii bezpieczeństwa obejmującej te systemy.

Zgodnie z ideą cyklu Deminga na pierwszym etapie planuje się strategię bezpieczeństwa („Zaplanuj"), następnie wdraża się ją zgodnie z planem („Wykonaj"), później regularnie sprawdza, czy jest skuteczna, np. za pomocą audytów („Sprawdź"), by w razie potrzeby zmodyfikować ją, aby była bardziej skuteczna („Popraw"). A kiedy np. pojawią się nowe technologie albo wyzwania w ochronie obiektu, należy strategię bezpieczeństwa odpowiednio zaktualizować i cały cykl się powtarza.

Poza przywołanymi w ustawie o KSC normami 27001 i 22301 istnieje szereg innych standardów, których utrzymanie nie jest obowiązkowe (wynika to z dobrowolności stosowania norm, np. w systemach telewizji dozorowej – poza nielicznymi wyjątkami, np. rozporządzenie MSWiA dotyczące monitorowania imprez masowych). Zgodność z takimi standardami w sposób znaczący może jednak podnieść jakość i skuteczność działania systemu ochrony technicznej, co ma istotne znaczenie w kontekście zgodności z dyrektywą NIS2 całej organizacji i jej odporności na incydenty związane z bezpieczeństwem cybernetycznym. Przykładowe normy i standardy, o których mowa, to:

- PN-EN 50131 (systemy SSWiN),
- PN-EN 62676 (telewizja dozorowa),
- PN-EN 60839 (kontrola dostępu),
- Rozporządzenie RODO (w wielu obszarach komplementarne z NIS2).

Warto podkreślić, że zgodność ze standardami to nie tylko dobrej jakości sprzęt i oprogramowanie. To także właściwe podejście do projektowania i instalacji systemu.

Przykładowo, doskonałej jakości kamera o bardzo wysokiej rozdzielczości nie spełni swojego zadania, jeśli przy projektowaniu jej lokalizacji i doborze ogniskowej nie uwzględniono konkretnych kryteriów związanych z celem monitorowania danego obszaru, np. w oparciu o wytyczne DORI (Detekcja-Obserwacja-Rozpoznanie-Identyfikacja), zdefiniowane w normie PN-EN62676-4:2015. Centrala alarmowa wykonana w zgodzie z wymogami stopnia 4 (Grade 4) normy 50131-1 nie spełni swojej funkcji, jeśli okablowanie SSWiN nie będzie należycie zabezpieczone przed ingerencją z zewnątrz. Podobne przykłady można by mnożyć.

Hikvision – jesteśmy gotowi

Hikvision, jako globalny lider produkcji systemów ochrony technicznej, od kilku lat niezmiennie na pierwszym miejscu rankingu „AS Security 50", jest w pełni gotowy na nowe wymagania ujęte w dyrektywie NIS2. Gotowość ta wynika m.in. z następujących faktów:

- uzyskanie certyfikatów: ISO27001, ISO27701, CMMI Level 5, CSA STAR oraz *Common Criteria* na poziomach EAL3 i EAL3+ dla produktów sieciowych,
- udział w organizacji CVE jako członek NA *(Numering Authority)*,
- stosowanie modułów TPM *(Trusted Platform Module)* w wybranych modelach urządzeń,
- członkostwo w inicjatywie *Global Compact* prowadzonej przez ONZ.

Hikvision zapewnia zgodność swoich produktów z wszystkimi przywołanymi wyżej normami i standardami dotyczącymi telewizji dozorowej, systemów SSWiN, kontroli dostępu itd. Techniczne środki bezpieczeństwa, takie jak autentykacja EAP-TLS i 802.1x, filtrowanie ruchu sieciowego, szyfrowanie danych asymetryczne kluczem 256-bitowym, redundancja zapisu, wymuszanie komplikacji haseł, w dobie dzisiejszych standardów zabezpieczeń technicznych są standardem. Dla Hikvision nowa dyrektywa to oczywista konsekwencja zwiększania odporności naszej części świata na nowe, poważne wyzwania związane z bezpieczeństwem cybernetycznym. NIS2? Jesteśmy gotowi!

Jeśli chcesz uzyskać więcej informacji dotyczących zagadnień związanych z implementacją dyrektywy NIS2 w Polsce, zapraszamy do bezpośredniego kontaktu pod adresem support.pl@hikvision.com ●

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

Jak zarządzać zmieniającym się krajobrazem cyberbezpieczeństwa?

Specjaliści projektujący i wdrażający rozwiązania w zakresie systemów bezpieczeństwa na potrzeby przemysłu i infrastruktury krytycznej stoją w obliczu wyjątkowej presji. Fizyczna ochrona takich podmiotów jest oczywiście najważniejsza, ale dziś muszą mierzyć się z atakami w sferze cyfrowej.

Nie jest tajemnicą, że cyberataki są coraz liczniejsze i coraz bardziej wyrafinowane, podejmowane przez coraz szersze grono atakujących. Ze względu na globalny charakter łańcuchów dostaw niewielkie zakłócenie w jednym miejscu może mieć duży wpływ na inny, co znamy jako „efekt motyla".

Organy regulacyjne w obliczu wyzwań związanych z cyberbezpieczeństwem

Rządy i organy regulacyjne bez wątpienia starają się nadążyć za zmianami i rosnącym zagrożeniem dla cyberbezpieczeństwa. Coraz częściej ich reakcją jest zmiana sposobu regulacji kwestii bezpieczeństwa cyfrowego. Zamiast wprost określać, co dostawcy podstawowych usług muszą wdrożyć w odniesieniu do cyberbezpieczeństwa, tendencja w regulacjach polega na tym, że to na dostawcach spoczywa obowiązek udowodnienia, że posiadają niezbędne środki, aby zachować cyberbezpieczeństwo. Zmiana ta ma poważne konsekwencje dla firmy dostarczającej wiedzy i rozwiązań wszystkim odbiorcom działającym w ramach łańcucha dostaw. Każdy element łańcucha wartości zostanie poddany kontroli.

NIS2 jako przykład ewoluującego środowiska regulacyjnego

Dyrektywa NIS2, która weszła w życie w styczniu tego roku, a państwa członkowskie UE mają czas do października 2024 r. na wprowadzenie jej w życie, stanowi użyteczny przykład podkreślający konsekwencje nowych regulacji dla kluczowych podmiotów.

NIS2, będąca odpowiedzią na ewoluujący krajobraz zagrożeń, ma na celu podniesienie ogólnego poziomu cyberbezpieczeństwa w UE. Wypełnia luki widoczne w pierwotnej dyrektywie NIS. Dyrektywa ma na celu stworzenie „kultury bezpieczeństwa w sektorach o kluczowym znaczeniu dla naszej gospodarki i społeczeństwa, które w dużym stopniu opierają się na technologiach informacyjno-komunikacyjnych (ICT), takich jak energetyka, transport, gospodarka wodna, bankowość, infrastruktura rynków finansowych, opieka zdrowotna i infrastruktura cyfrowa".

Jest to wyraźny przykład uznania przez organy regulacyjne tego, jak bardzo każdy sektor jest uzależniony od technologii i jak wszelkie słabe punkty są stale wyszukiwane oraz wykorzystywane przez cyberprzestępców.

Zgodnie z dyrektywą państwa członkowskie UE zidentyfikują przedsiębiorstwa i organizacje, które są operatorami usług kluczowych, a organizacje te będą musiały podjąć odpowiednie środki bezpieczeństwa i powiadomić odpowiednie organy krajowe o wszelkich poważnych incydentach cyberbezpieczeństwa. Ponadto kluczowi dostawcy usług cyfrowych, takich jak usługi przetwarzania w chmurze, również będą musieli spełniać wymogi bezpieczeństwa i powiadamiania określone w dyrektywie. Rozszerzenie poza dostawców usług kluczowych i na cały łańcuch dostaw technologii jest oczywiste.

Rozwiązania w zakresie dozoru jako część łańcucha wartości istotnego podmiotu

Jak wspomniano, ochrona usług kluczowych zawsze była priorytetem. Fizyczne ogrodzenia i kontrola dostępu zostały ulepszone dzięki technologii z zaawansowanymi rozwiązaniami dozoru wizyjnego. Coraz bardziej połączony charakter tych rozwiązań sprawił, że znalazły się one na pierwszej linii cyberataków i pod kontrolą zmieniających się przepisów.

Architekci, inżynierowie oraz konsultanci projektujący i określający rozwiązania w zakresie dozoru wizyjnego ponoszą znaczną odpowiedzialność. Zapewnienie, że rozwiązania te są zaprojektowane nie tylko pod kątem dzisiejszych wymagań w zakresie bezpieczeństwa fizycznego i cybernetycznego, ale że będą one dostosowane do zmieniających się wyzwań, ma zasadnicze znaczenie dla zachowania zgodności z przepisami.

Wymaga to „myślenia systemowego". Konsultanci muszą postrzegać rozwiązanie bezpieczeństwa jako całość, a nie wybór oddzielnych urządzeń, a także brać pod uwagę oprogramowanie rozwiązania, wraz z jego integracją z szerszą infrastrukturą dostawcy podstawowych usług. Projektowanie, wdrażanie, integracja i konserwacja rozwiązań odgrywają istotną rolę w cyberbezpieczeństwie. Rozwiązanie, które pozostaje statyczne, będzie ostatecznie narażone na luki w zabezpieczeniach.

Co zmieniający się krajobraz oznacza dla projektantów rozwiązań do dozoru?

Osoby projektujące i określające rozwiązania mają obowiązek rozważyć potencjalne szersze zagrożenia stwarzane przez rekomendowaną przez nich ofertę techniczną. Podczas gdy rozwiązania powinny koncentrować się przede wszystkim na spełnieniu określonych wymagań operacyjnych, przepisy dotyczące IT i cyberbezpieczeństwa są obecnie niezbędne. Dzisiejsze specyfikacje muszą być dostosowane do przepisów, takich jak dyrektywa NIS2, aby wspierać zgodność organizacji.

W związku z tym konsultanci muszą być pewni, że produkty każdego dostawcy spełniają politykę bezpieczeństwa klienta indywidualnego, w tym wszystkie odpowiednie przepisy mające zastosowanie do organizacji klienta. Niezbędne jest przeprowadzenie odpowiedniej analizy *due diligence* podejścia do cyberbezpieczeństwa każdego rekomendowanego dostawcy.

Konsultanci muszą również starać się określić zasady i procesy dla dostawców technologii, których rekomendują, a także funkcje techniczne, które zapewniają. Funkcje takie jak bezpieczny rozruch, podpisane oprogramowanie układowe, komponenty zabezpieczające, które umożliwiają automatyczną i bezpieczną identyfikację urządzeń oraz moduł TPM *(Trusted Platform Module)* odnoszą się do zagrożeń stwarzanych obecnie i powinny zostać określone.

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

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

Łącznie te zasady i procesy pokazują dojrzałość cyberbezpieczeństwa organizacji i jej zdolność do dostosowywania się do zmieniającego się krajobrazu zagrożeń.

Zmiana ról w zmieniającym się środowisku cyberbezpieczeństwa

Dla każdego kraju znaczenie zminimalizowania potencjalnego zakłócenia podstawowych usług jest oczywiste i nie można go przecenić. Zakłócenie będzie miało niemal natychmiastowy wpływ na gospodarkę. Może to szybko przerodzić się w istotne kwestie społeczne oraz potencjalne zagrożenie zdrowia i życia ludzkiego.

Niezależnie od tego, skąd pochodzi zagrożenie, ochrona podstawowych usług i podmiotów, które je świadczą, ma zatem kluczowe znaczenie. Organy regulacyjne na całym świecie zdają sobie z tego sprawę, a zagrożenia pochodzą ze sfery zarówno fizycznej, jak i cyfrowej.

Uznały jednak również, że zagrożenia związane z cyberatakami ewoluują tak szybko, że wszelkie próby zdefiniowania środków cyberbezpieczeństwa będą nieaktualne, zanim zostaną opublikowane. W związku z tym zmieniono podejście regulacyjne, wymagając od dostawców podstawowych usług udowodnienia, że dysponują technologią, procesami i zasobami umożliwiającymi radzenie sobie z zagrożeniami.

W rezultacie każdy zaangażowany w łańcuch wartości istotnego podmiotu musi odpowiedzieć na to wyzwanie, w tym osoby projektujące i określające rozwiązania w zakresie dozoru. Ograniczanie ryzyka cyberzagrożeń to wspólna odpowiedzialność. Podczas gdy firmy są od tego zależne, konsekwencje dla społeczeństwa mogą być znacznie większe. ●

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

Ochrona tożsamości i dostępu w dobie NIS2

Chcesz wzmocnić bezpieczeństwo zgodnie z dyrektywą NIS2 i jednocześnie ułatwić życie użytkownikom, eliminując hasła? Zarządzanie tożsamością i dostępem oraz silne uwierzytelnianie to klucz do sukcesu!

Zarządzanie tożsamością *(Identity and Access Management* – IAM) to zestaw procedur i narzędzi, które umożliwiają bezpieczne zarządzanie dostępem do danych i usług w organizacji. Narzędzia te służą do zarządzania tożsamością osób mających dostęp do danego obiektu oraz do firmowych systemów informatycznych, wykorzystując do tego funkcje:

1. **Identyfikacji.** Baza danych zawiera informacje na temat wszystkich osób z nadanymi uprawnieniami. Informacje te obejmują m.in. imię i nazwisko, numer ID oraz tzw. rolę, na którą mogą się składać np. zajmowane stanowisko, przynależność do konkretnej grupy roboczej itp. Dostęp jest przydzielany zgodnie z funkcją pełnioną w firmie.
2. **Aktualizacji.** Zarządzanie cyklem „życia" tożsamości jest kluczowe, gdyż pracownicy i przypisane im role się zmieniają. Jeśli ktoś opuszcza firmę, dostęp takiej osoby jest dezaktywowany, a zmiana roli, np. awans, może oznaczać, że uprawnienia zastaną zmienione, będą np. większe.
3. **Uwierzytelniania.** Stosowanie IAM powoduje, że możliwe jest wdrożenie różnych sposobów uwierzytelniania, aby zawsze mieć pewność, że osoba korzystająca z dostępu ma do niego prawo.

Od czasu wprowadzenia systemów komputerowych uwierzytelnianie opierało się głównie na loginie i haśle. Niestety użytkownicy mają tendencję do używania tych samych haseł w wielu systemach, co zwiększa ryzyko naruszeń bezpieczeństwa. Rozwiązaniem tego problemu jest centralne zarządzanie poświadczeniami i uwierzytelnianie wieloskładnikowe *(Multifactor authentication* – MFA), które wymaga poświadczenia tożsamości za pomocą kilku różnych metod, które można stosować jednocześnie lub w różnych konfiguracjach. Te metody to:

- login, hasło, PIN;
- urządzenie mobilne, klucz U2F, token generujący kody jednorazowe;
- dane biometryczne, np. odcisk palca, rozpoznawanie twarzy.

Do uwierzytelniania wieloskładnikowego można wykorzystywać oprogramowanie, np. aplikację na smartfonie lub specjalne urządzenia, takie jak klucz U2F lub token sprzętowy. Rozwiązania bezhasłowe eliminują potrzebę wprowadzania haseł, używając kryptograficznych danych uwierzytelniających, takich jak klucz U2F odblokowywany odciskiem palca, skanem twarzy lub PIN-em, co zapewnia najsilniejszą ochronę. Nie można ich odgadnąć ani ponownie wykorzystać. Zmniejszają też ryzyko ataków typu *brute force* i niewłaściwego użycia, np. upowszechnienia danych dostępowych. A odcisk palca, twarz, kod PIN lub wzór są przechowywane lokalnie na urządzeniu.

Warto zauważyć, że nie wszystkie rozwiązania MFA zapewniają taką samą ochronę przed atakami. Wiele zależy od sposobu ich wdrożenia. Jednak przy prawidłowym wprowadzeniu MFA jest to system zapewniający organizacjom i użytkownikom wiele korzyści:

1. **Bezpieczeństwo** – eliminacja popularnych haseł, dostosowanie poziomu uwierzytelniania do uprawnień użytkownika, kontrola dostępu podwykonawców, wzmacnianie mechanizmów uwierzytelniania.
2. **Komfort użytkownika** – pojedyncze uwierzytelnianie dla wszystkich aplikacji, usprawnienie zarządzania hasłami, integracja danych biometrycznych (np. Microsoft Windows Hello, Apple TouchID/FaceID, FIDO2).
3. **Standaryzacja i zgodność** – zgodność z przepisami RODO, NIS2, CER, ułatwienie dostępu do aplikacji w kontekście zmian korporacyjnych.

Niektóre rozwiązania MFA łagodzą również ataki phishingowe. Zważywszy na jego powszechność odporność na *phishing* powinna być kluczowym czynnikiem przy wyborze rozwiązania silnego uwierzytelniania.

Uwierzytelnianie wieloskładnikowe nie jest jedynym rozwiązaniem ochrony tożsamości i dostępu, ale jest kluczowe do zapewnienia maksymalnie wysokiego poziomu bezpieczeństwa systemom i aplikacjom, a także kontroli nad fizycznym dostępem. W przypadku systemów informatycznych dobrym rozwiązaniem jest wprowadzenie zasady pojedynczego logowania (*Single Sign On* – SSO). Ważne, by aplikacje wykorzystujące to rozwiązanie mogły bezpiecznie zarządzać sesjami z limitami czasu bezczynności i maksymalnym czasem trwania sesji. Z kolei przy wdrażaniu MFA należy pamiętać o dokładnym kontrolowaniu zasobów wykorzystywanych do uzyskiwania dostępu, czyli zarówno urządzeń fizycznych takich jak tokeny i klucze U2F, jak i aplikacji oraz kart wirtualnych. System ten powinien również obsługiwać certyfikaty usług i urządzeń IoT. Właściwe wdrożenie zapewnia dwustronne uwierzytelnianie urządzeń, nawet bez dostępu do Internetu.

Łączymy technologie i doświadczenie, chroniąc ludzi i zasoby przed cyberatakami i zagrożeniami fizycznymi. Testujemy i udoskonalamy metody ochrony, reagujemy na incydenty i pomagamy bezpiecznie działać w dzisiejszym świecie. ●

squareTec
ul. Broniewskiego 4
85-316 Bydgoszcz
www.squaretec.pl

Nie daj się złowić!

Użyj wieloprotokołowego klucza bezpieczeństwa i przeciwdziałaj przejęciu kont.
Silne uwierzytelnianie dostępne od ręki.

dwuskładnikowe (2FA) | wieloskładnikowe (MFA) | bezhasłowe (FIDO2)

Konfigurowalny klucz bezpieczeństwa typu "wszystko w jednym"

Za pomocą jednego dotknięcia klucza YubiKey chroń dostęp do komputerów, sieci i usług online.

Łatwiejsze i bezpieczniejsze niż aplikacje uwierzytelniające

Koniec z sięganiem po smartfon lub ponownym wpisywaniem haseł. Po prostu podłącz swój YubiKey, dotknij a on zrobi resztę za Ciebie.

Współpracuje z setkami usług

YubiKey współpracuje z logowaniem Windows i Mac, Gmail, Dropbox, Facebook, Salesforce, Duo i wieloma innymi usługami.

Zerejestruj się na niedamsiezlowic.pl podaj kod i odbierz swój klucz*

AS42024

* Oferta ważna do wyczerpania zapasów

squareTec

squaretec.pl

Dyrektywa NIS2
a rozwiązania do kontroli dostępu, monitorowania i wizualizacji systemów bezpieczeństwa

Dyrektywa NIS2 wprowadza nowe podejście do cyberbezpieczeństwa, rozszerzając zakres podmiotów i branż objętych wymaganiami dyrektywy. Ponadto zgodnie z załącznikami I i II dyrektywa ta dzieli je na podmioty kluczowe (do których zalicza się firmy działające w takich branżach jak energetyka, transport, bankowość, infrastruktura rynków finansowych, opieka zdrowotna, gospodarka wodno-ściekowa, infrastruktura cyfrowa, zarządzanie usługami technologii informacyjnych i komunikacyjnych – ICT, administracja publiczna i przestrzeń kosmiczna) oraz podmioty ważne, do których należą m.in. usługi pocztowe i kurierskie, gospodarowanie odpadami, produkcja i dystrybucja chemikaliów oraz żywności, ogólnie pojęta produkcja, usługi cyfrowe oraz badania naukowe.

Każde z państw Unii Europejskiej (UE) jest zobowiązane do ustanowienia własnego wykazu przedsiębiorstw kluczowych i ważnych na bazie wytycznych dyrektywy. Dyrektywa NIS2 nakłada na takie podmioty obowiązek wdrożenia rozwiązań w zakresie analizy i zarządzania ryzykiem, tworzenia polityki bezpieczeństwa, obsługi incydentów, zabezpieczenia łańcucha dostaw oraz opracowania planu ciągłości działań.

Państwa członkowskie UE są z kolei zobowiązane do powołania organów, których zadaniem jest m.in. kontrola i audyty podmiotów objętych dyrektywą, przyjmowanie zgłoszeń o incydentach oraz koordynacja działań w zakresie cyberbezpieczeństwa na szczeblach krajowym i unijnym. Dyrektywa przewiduje również wysokie kary finansowe dla podmiotów nierealizujących podane w niej wymogi.

Dyrektywa NIS2 nie odnosi się bezpośrednio ani do systemów kontroli dostępu (KD), ani do monitorowania i wizualizacji systemów bezpieczeństwa w obiektach, typu SMS (*Security Management System*). Niemniej, zgodnie z ustępem 79, w zakresie zarządzania bezpieczeństwem wymagane jest uwzględnienie takich zagrożeń, jak m.in. kradzież, pożar oraz nieuprawniony dostęp fizyczny do infrastruktury informatycznej. W takim układzie prawidłowo funkcjonujący system kontroli dostępu o odpowiednim poziomie zabezpieczeń jest istotny w zakresie przeciwdziałania temu, by osoby niepożądane mogły swobodnie poruszać się po obiekcie, dokonywać kradzieży środków (np. laptopa) umożliwiających dostęp do sieci informatycznej, doprowadzić do uszkodzenia kluczowych elementów infrastruktury czy też podsłuchiwać komunikację, wpinając się do sieci informatycznej. Z kolei zastosowanie systemu do monitorowania i wizualizacji zagrożeń na mapach ułatwia detekcję oraz sprawną reakcję w sytuacjach awaryjnych.

Do oceny jakości i poziomu bezpieczeństwa oferowanego przez dane rozwiązanie najlepiej posłużyć się obowiązującymi normami. Systemy KD podlegają normie PN-EN 60839-11, która definiuje 4 stopnie zabezpieczenia. System RACS 5 umożliwia spełnienie wymogów dla wszystkich stopni, w tym również dla stopnia czwartego. Ponadto system RACS 5 oferuje takie funkcjonalności w zakresie cyberbezpieczeństwa, jak:

- obsługa kart zbliżeniowych w technologii MIFARE® DESFire®, na których dane są szyfrowane niezłamanym do tej pory systemem szyfrowania;
- szyfrowanie we wszystkich torach komunikacji systemu (m.in. AES128CBC, TLS 1.2);
- kontrolowanie wielopoziomowego dostępu do oprogramowania zarządzającego przez operatorów.

Oferowane przez firmę Roger system kontroli dostępu RACS 5 oraz system do monitorowania i wizualizacji VISO SMS mogą być stosowane przez podmioty zarówno krytyczne, jak i ważne, umożliwiając realizację wymogów dyrektywy NIS2 w zakresie podniesienia poziomu zabezpieczenia systemów informatycznych, zwłaszcza w odniesieniu do fizycznego dostępu do infrastruktury krytycznej i monitorowania zagrożeń. ●

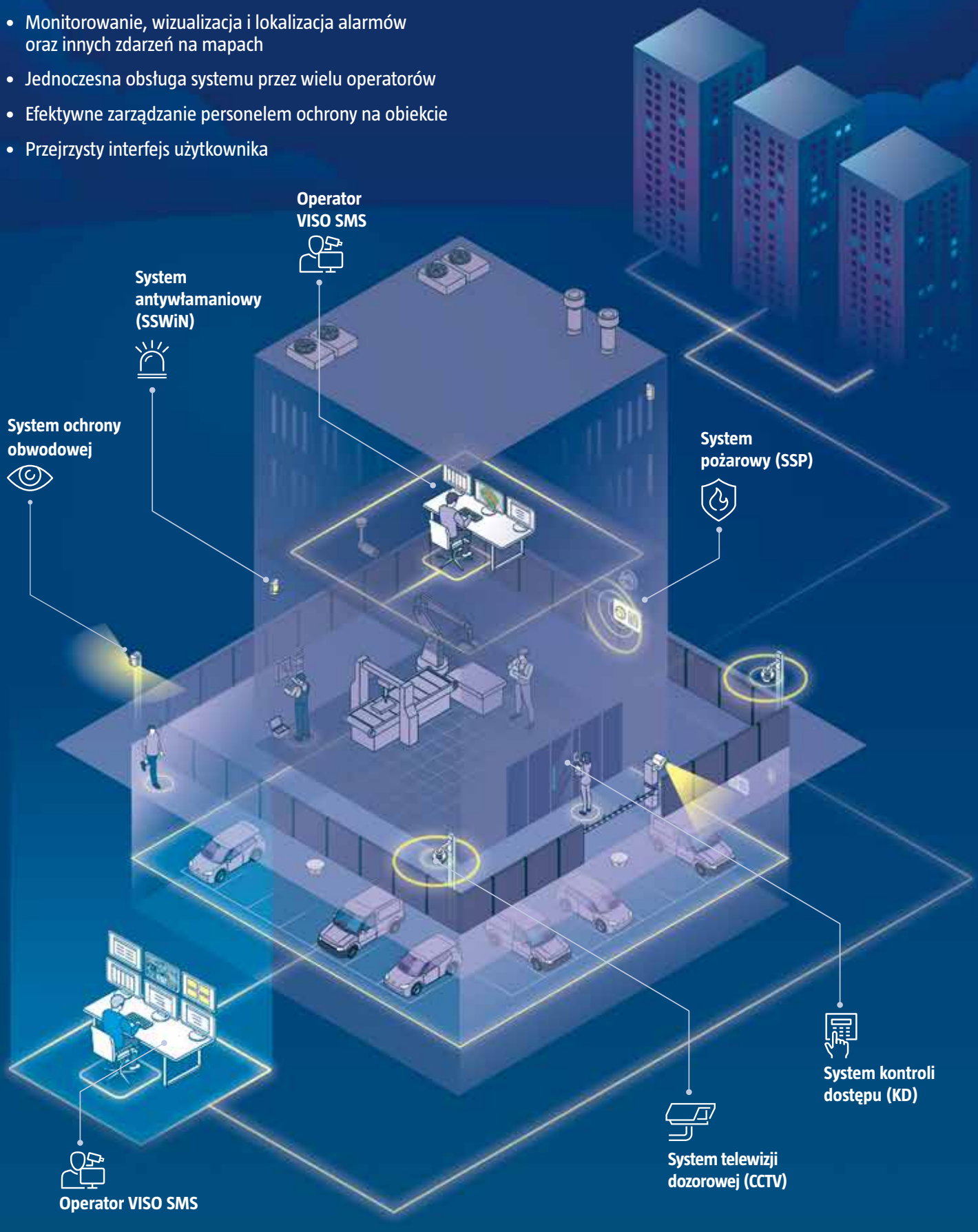
Roger
Gościszewo 59, 82-400 Sztum
roger@roger.pl
www.roger.pl

VISO SMS

Monitorowanie i wizualizacja systemów bezpieczeństwa

roger
Intelligence for Building

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



VIVOTEK gotowy na NIS2

W miarę, jak zagrożenia cybernetyczne stają się coraz bardziej zaawansowane, dyrektywa Unii Europejskiej dotycząca bezpieczeństwa sieci i informacji (NIS2) staje się kluczową legislacją mająca na celu zwiększenie bezpieczeństwa infrastruktury krytycznej oraz usług cyfrowych.

Istniejąca od 2000 r. tajwańska firma VIVOTEK, wiodący dostawca rozwiązań do monitoringu, jest liderem wprowadzania rozwiązań zgodnych z NIS2. Zaangażowanie firmy w zgodność z NIS2 podkreśla jej działania na rzecz zapewniania klientom bezpiecznych, odpornych i godnych zaufania produktów.

Dyrektywa NIS2 została opracowana w celu wzmocnienia pozycji organizacji w zakresie cyberbezpieczeństwa poprzez akcentowanie proaktywnego zarządzania ryzykiem, solidnego raportowania incydentów oraz zintensyfikowania współpracy między państwami członkowskimi UE. Rozumiejąc jest znaczenie, VIVOTEK wdrożył kompleksową strategię dostosowania swoich produktów i usług do wymagań NIS2.

Jednym z fundamentów tego podejścia jest wdrożenie normy ISO 27001. Ten międzynarodowy standard zapewnia, że systemy zarządzania bezpieczeństwem informacji VIVOTEK są solidne i niezawodne. Ponadto firma stosuje autoryzowany firmware, który gwarantuje autentyczność i integralność jej produktów przez cały cykl ich życia. Rozwiązania są wyposażone w mechanizmy bezpiecznego rozruchu gwarantujące, że podczas uruchamiania ładowane są tylko uwierzytelnione komponenty oprogramowania, co zmniejsza ryzyko nieautoryzowanego dostępu i manipulacji.

VIVOTEK priorytetowo traktuje również bezpieczeństwo infrastruktury sieciowej, utrzymywanie bezpiecznych połączeń konsolowych do swojej infrastruktury sieciowej. Stosowane przez firmę protokoły bezpieczeństwa sieciowego są zgodne z najlepszymi praktykami branżowymi, w tym IEEE802.1x do kontroli dostępu do sieci opartej na portach oraz HTTPS z TLSv1.3 służących do bezpiecznej komunikacji, zwiększając bezpieczeństwo infrastruktury sieciowej.

Zaangażowanie VIVOTEK w zapewnienie bezpieczeństwa obejmuje również Platformę Rozwoju Aplikacji (VADP), która oferuje zwiększoną ochronę w przypadku integracji z aplikacjami innych firm. Strategiczny sojusz z Trend Micro, wiodącą firmą z branży cyberbezpieczeństwa, pozwala wykorzystać wiedzę i zasoby partnera, by jeszcze skuteczniej zwalczać cyberzagrożenia i zapewnić jak najlepszą ochronę rozwiązaniom oferowanym klientom.

VIVOTEK opracował również rygorystyczne procedury zarządzania i raportowania podatności na cyberataki. Proaktywne podejście gwarantuje szybkie identyfikowanie ryzyka, ograniczenie konsekwencji, jakie ze sobą niesie, i błyskawiczne przekazywanie informacji o potencjalnych słabościach wszystkim zainteresowanym.

Firma niezmiennie przykłada ogromną wagę do zgodności z dyrektywą NIS-2. Priorytetem jest zapewnienie pełnej transparentności i spokoju ducha poprzez regularne informowanie o postępach w dostosowywaniu się do tych wymogów.

Proaktywne działania VIVOTEK w zgodność z NIS2 podkreślają dążenie do doskonałości w zakresie cyberbezpieczeństwa. Poprzez integrację zaawansowanych technologii, przestrzeganie rygorystycznych standardów oraz rozwój strategicznych partnerstw VIVOTEK służy temu, by klienci byli zawsze chronieni.

Więcej informacji na temat inicjatyw cyberbezpieczeństwa VIVOTEK oraz zgodności z NIS2 można uzyskać na oficjalnej stronie internetowej firmy. Wszelkich danych udziela też zespół wsparcia. ●

VIVOTEK
Marcin Kulik
marcin.kulik@vivotek.com
www.vivotek.com

ECHODYNE

EchoShield®

WIELOZADANIOWY RADAR 4D

EchoGuard®

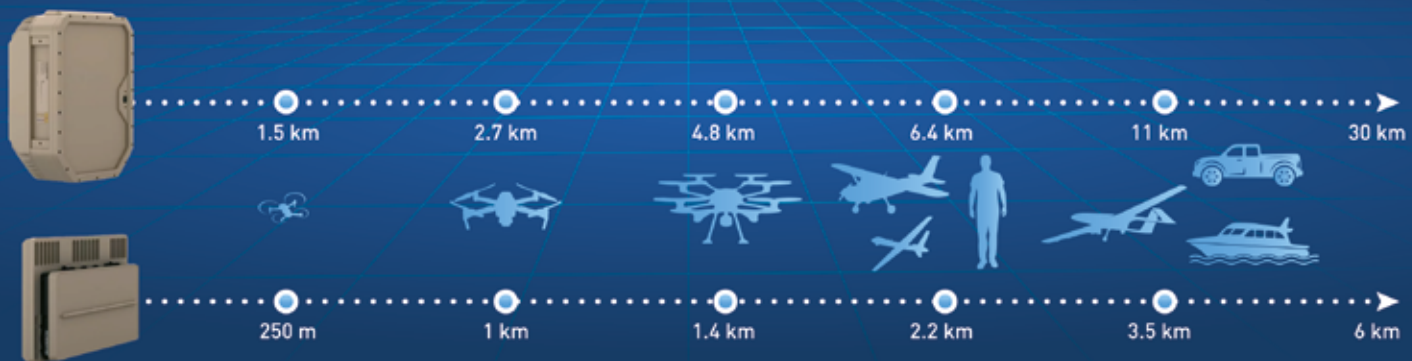
KOMPAKTOWY RADAR 4D

POLE WIDZENIA
do 130° w poziomie
do 90° w pionie

IDENTYFIKACJA I ŚLEDZENIE
do 40 obiektów o wysokim oraz do 1000 obiektów o niskim priorytecie

SKUTECZNOŚĆ
identyfikacja dronów do 100%

SYGNATURA µDOPPLER
klasyfikacja dronów, rozróżnienie od innych obiektów jak ptaki czy ludzie



OFICJALNY DYSTRYBUTOR:

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

www.linc.pl

WIĘCEJ O NAS:

Linc Polska Sp. z o.o.

Cyberodporność

Czy twoja firma jest gotowa na nowe wyzwania?

Już w tym roku na tysiące firm czekają wyzwania związane z zapewnieniem cyberbezpieczeństwa, m.in. wymagania dyrektywy NIS2. Jak budować firmową cyberodporność, by im sprostać?

Coraz większa liczba i skala cyberataków typu ransomware, DDoS czy phishingowych oraz będący często ich konsekwencją wyciek danych sprawiają, iż firmy i instytucje muszą lepiej zapobiegać przestępstwom w sieci. Według danych z raportu CERT Orange Polska najpowszechniejszym zagrożeniem pozostaje oparty na socjotechnice phishing, który w ubiegłym roku stanowił 44%. Za nim plasują się ataki DDoS (18%) oraz ataki z wykorzystaniem złośliwego oprogramowania (15%).

Zagrożenia te dotykają nie tylko indywidualnych internautów, ale także firmy. Stąd warto inwestować w działania ujawniające słabe punkty, doskonalące obronę i sprawiające, że zarówno rozwiązania technologiczne chroniące firmę, jak i dojrzałość oraz świadomość bezpieczeństwa w organizacji rozwijają się równolegle ze zmiennym krajobrazem zagrożeń.

Ile kosztuje brak cyberbezpieczeństwa?

To jedno z pytań, które obecnie powinni postawić sobie menedżerowie firm. Jeszcze kilka lat temu firmy, które stały się obiektem cyberataku, nie ujawniały informacji o poniesionych kosztach. Obecnie dużo łatwiej przytoczyć przykłady i konkretne kwoty, które obciążyły budżety ofiar ataku.

Ransomware – to już nie są tylko ataki na pojedyncze komputery. Teraz przestępcy przejmują kontrolę nad całą firmową infrastrukturą firmy, by zaszyfrować wszystkie komputery i serwery, najchętniej wraz z kopiami bezpieczeństwa. Liczą, że zaatakowana firma zapłaci za cenne dane lub informacje o swojej działalności, ponieważ zwykle samodzielne odzyskanie danych może oznaczać kilkutygodniowe zakłócenie jej działania i znaczne koszty.

Firmy, które padły ofiarą ataku zwykle starają się podnieść poziom bezpieczeństwa w organizacji. Niestety dopiero po szkodzie. Dlatego tak istotne jest konsekwentne budowanie świadomości zagrożeń i ochrony przed nimi m.in. poprzez wypracowanie odpowiednich nawyków, a także zastosowanie adekwatnych rozwiązań.

Jak budować cyberodporność

Aby zapewnić ciągłość działania i bezpieczeństwo firmowych danych warto zainwestować w audyty, testy, szkolenia i nowoczesne narzędzia ochrony, takie jak oferowane przez Orange Polska. Mogą pomóc firmie skutecznie dostosować się do nowych wymogów, a także zbudować cyberodporność całej organizacji. I tak np. Orange Internet Protection to ekonomiczne rozwiązanie pomagające redukować negatywne skutki ataków DDoS powodujących przerwy i zakłócenia w działaniu usług internetowych klienta. Ochrona przed atakami jest realizowana wewnątrz sieci Orange, dzięki czemu ataki są odpierane jeszcze przed dotarciem złośliwego ruchu do infrastruktury klienta. Z kolei Next Generation SOC wspiera realizację polityki bezpieczeństwa, a kluczowe wskazane przez klienta systemy biznesowe są monitorowane w trybie ciągłym. Najważniejszym elementem usługi jest natychmiastowe powiadamianie klienta o incydentach.

Trening i edukacja

Radą na powstrzymanie bądź minimalizację zagrożeń są oprócz rozwiązań technologicznych treningi i edukacja np. podczas symulowanych cyberataków phishingowych, które testują odporność pracowników firmy na socjotechnikę. Tego uczy także Centrum Doświadczeń Cyberbezpieczeństwa działające w Orange Polska. Umożliwia ono poznanie historii fikcyjnego ataku na firmę, a scenariusze wykorzystują analogię do codziennego życia. Przeprowadza uczestników przez najważniejsze wyzwania związane z cyberbezpieczeństwem ich firm oraz uczy, co powinni zrobić, by pokonać zagrożenia i odpowiednio chronić swoją organizację.

– *Podczas spotkania wyjaśniamy, jakie są straty związane z przestojem trwającym jeden dzień, tydzień oraz miesiąc. Wyniki są prezentowane dla każdej firmy indywidualnie, na bazie jej rocznych obrotów. W ten sposób uświadamiamy, ile kosztuje odtworzenie biznesu po ataku ransomware. Przedstawiamy fakty i liczby pomocne w podejmowaniu właściwych decyzji dotyczących budowania długoterminowej strategii cyberbezpieczeństwa* – mówi Daniel Kamiński, Senior Solutions Architect, Orange Polska. ●

Orange Polska S.A.
Aleje Jerozolimskie 160
02-326 Warszawa
www.orange.pl

ALNET SYSTEMS

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

www.alnetsystems.com

Zarządzanie systemami bezpieczeństwa w kompleksach wojskowych

IFTER od 25 lat produkuje rozwiązania przeznaczone do systemów bezpieczeństwa. Od początku naszym głównym klientem były jednostki wojskowe. Zaangażowanie w uwzględnienie potrzeb tego klienta doprowadziło do opracowania m.in. zaawansowanego systemu PSIM, który wdrażamy w kolejnych kompleksach wojskowych.

Jerzy Taczalski

Zadania stawiane przed systemami PSIM instalowanymi w obiektach militarnych przewidują dwa poziomy zabezpieczeń. Pierwszy obejmuje pojedyncze jednostki, drugi oznacza nadzór nad całym kompleksem prowadzony w Głównym Centrum Nadzoru (GCN) oraz ustanowienie Zapasowego Centrum Nadzoru (ZCN). System nadzorczy musi umożliwić integrację wszystkich systemów bezpieczeństwa: kontroli dostępu (SKD), systemu alarmowego (SSWiN), telewizji dozorowej (CCTV), sygnalizacji pożarowej (SSP), a także monitorowania systemów perymetrycznych i torów transmisji danych. Wszystkie muszą mieć pełną wizualizację, zarządzanie oraz tworzenie relacji między nimi.

Wizualizacja nie może odbywać się z poziomu przeglądarek WEB i musi być skalowalna. Musi mieć możliwość swobodnego definiowania kształtu i koloru ikon reprezentujących stan urządzenia, a możliwości prezentacyjne muszą być bardzo rozbudowane, ponieważ w dużych obiektach systemy obsługują ponad 10 tys. czujników,

modułów, czytników, kamer itp. Ważne jest również, aby niezależnie od wielkości systemu oraz czasu jego funkcjonowania system działał dokładnie tak samo szybko i sprawnie, jak na początku.

Ponadto kontrola dostępu musi spełniać wymogi normy PN-EN-60839-11 w klasie co najmniej 3., z pełnym szyfrowaniem na każdym etapie. System SKD musi też mieć strukturę rozproszoną z przechowywaniem pełnej konfiguracji w pojedynczych kontrolerach z dużym buforem do rejestracji zdarzeń, pozwalającym na autonomiczną pracę w przypadku braku połączenia z systemem zarządzającym.

W celu realizacji tych założeń opracowaliśmy linię produktów przeznaczonych do instytucji wojskowych. Bazowym rozwiązaniem jest IFTER EQU2 Military będący systemem klasy PSIM z wbudowaną technologią klastrową pozwalającą na obsługę rozproszonych systemów. Ideą technologii klastrowej jest decentralizacja bazy danych w celu zwiększenia niezawodności i stabilności rozwiązania. W poszczególnych jednostkach wojskowych znajdują się lokalne centra nadzoru (LCN) z jednym lub kilkoma stanowiskami do zarządzania bezpieczeństwem, obejmując wyłącznie daną jednostkę. Dlatego system ten ma własną bazę danych typu SQL z pełną obsługą urządzeń lokalnych i może pracować w pełnej autonomii w przypadku awarii połączenia między jednostką a GCN lub ZCN. Po odzyskaniu połączenia następuje automatycznie przesłanie informacji o zdarzeniach i zmianach w konfiguracji. W trybie pracy LCN komunikuje się jednocześnie z GCN i ZCN, korzystając z szyfrowania pakietów. Dzięki temu utrata połączenia z GCN nie zakłóca pracy ZCN. Z LCN do głównego centrum są na bieżąco przesyłane wszystkie zdarzenia i stany urządzeń. Z głównego centrum do LCN są przekazywane komendy sterujące pracą systemu bezpieczeństwa oraz zmiany konfiguracji.

Jeśli centrala alarmowa znajduje się w innym budynku niż LCN, to zaleca się stosowanie modułów RIIS obsługujących do dwóch central alarmowych zarówno po RS232, jak i Ethernet. Montuje się je jak najbliżej centrali alarmowej. Taki moduł ma niewielki pobór prądu i szeroki zakres zasilania od 10 do 60 VDC, dzięki czemu może być zamontowany w obudowie centrali i korzystać z jej zasilacza. Rozbudowana pamięć pozwala na przechowywanie do 100 tys. zdarzeń dla każdej centrali oraz całej konfiguracji. Moduł ma wbudowane dwa porty Ethernet i może obsłużyć równolegle do czterech centrów nadzoru równocześnie. Zasilanie, porty RS232 i Ethernet mają zabezpieczenia przeciwprzepięciowe.

Centra nadzoru zlokalizowane w GCN i ZCN zawierają konfigurację całego kompleksu. Za ich pomocą można monitorować stan bezpieczeństwa całego obiektu oraz wykonywać wszelkie sterowania lub zmiany w konfiguracji. Każde centrum może pracować na dwóch serwerach bazodanowych oraz dwóch serwerach integracji. W razie unieruchomienia jednego jego rolę przejmuje zapasowy. Funkcjonalność systemu się nie zmienia. Po przywróceniu działania system wyrównuje dane między serwerami.

IFTER EQU2 Military ma elastyczny mechanizm zarządzania dostępem do zdarzeń, grafik i stanów. Dzięki temu można zarówno ograniczać dostęp do danych w zależności od uprawnień, jak i blokować dane ze względów bezpieczeństwa. Jeżeli np. oficer dyżurny naciśnie przycisk napadowy, to na jego monitorze nie pokaże się alarm, ale będzie widoczny na pozostałych stanowiskach. Oprócz standardowych funkcji zarządzania bezpieczeństwem IFTER EQU2 Military umożliwia również kontrolę poprawności wykonania konserwacji. Jeżeli na jakimś czujniku w okresie konserwacji nie został wykonany alarm, jest to raportowane do administratora.

Integracja systemów to również tworzenie relacji między różnymi systemami, np. pomiędzy SKD a depozytorami. Osoba, która nie została zarejestrowana na wejściu do budynku, nie może pobrać klucza i w drugą stronę: nie oddając klucza, nie może opuścić budynku. Zaawansowane relacje można budować również między kamerami IP z analityką a systemami perymetrycznymi i centralą alarmową. W IFTER EQU2 Military można budować wirtualne strefy bezpieczeństwa, które analizują pobudzenia z powyższych systemów i np. w razie wykrycia intruza przez oba systemy wywoływany jest alarm. W wirtualnych strefach bezpieczeństwa można uzbrajać, rozbrajać lub blokować poszczególne elementy systemu.

Dostępne są trzy linie SKD. W przypadku obiektów militarnych warto zwrócić wagę na serię EQU ACC 400 spełniającą normę PN-EN-60839-11 w klasie 4. potwierdzoną Świadectwem Kwalifikacyjnym wydanym przez zakład TECHOM. Zgodnie z normą kontrolery obsługują czytniki po OSDPv2.2 z szyfrowaną transmisją danych (w klasie 4. nie wolno używać czytników z zastosowanym protokołem Wiegand), monitorują stan zasilacza i akumulatora, temperaturę pracy oraz wszelkie zakłócenia transmisji danych.

Kontrolery i moduły rozszerzeń mają dodatkową obudowę chroniącą przed uszkodzeniem elektroniki, można je mocować na szynie DIN, w skrzynkach spełniających IP4x i IK04, wyposażonych w szynę DIN oraz czujnik otwarcia i oderwania od podłoża.

Wszystkie wejścia monitorujące są parametryzowane i rozróżniają: sabotaż, zwarcie i rozwarcie, otwarcie, zamknięcie i antimasking czujnika. Kontrolery mają zabezpieczenie przeciwprzepięciowe dla portu Ethernet na poziomie 150 A (10/1000 µs), a dla interfejsów RS485 600 W (10/1000 µs) zgodnie z normą IEC61000-4-5.

Zakres temperatury pracy wnosi od -10°C do +40°C, a zasilanie może się zmieniać w zakresie od 10 do 28 VDC. Kontroler jest energooszczędny. Jego pamięć pozwala na przechowywanie pełnej konfiguracji, danych milionów kart oraz co najmniej 500 tys. zdarzeń. Zgodnie z PN-EN-60839-11 w klasie 4. kontroler ma pełną diagnostykę wszystkich podstawowych parametrów rejestrowanych w interwałach mniejszych niż 3 min, każdy parametr jest rejestrowany w logach po 1000 wpisów. Monitorowane są poziom poprawności transmisji danych po interfejsie Ethernet, poziom poprawności transmisji danych po interfejsie RS485, poziom poprawności transmisji danych z poszczególnymi modułami i czytnikami, napięcie na akumulatorze, napięcie na zasilaniu kontrolera, wynik testów akumulatora, temperatura wewnętrzna kontrolera, stan obciążenia procesora kontrolera, stan pamięci kontrolera.

System ma rozbudowane funkcjonalności, w tym Anti Passback globalny z możliwością definiowania obszaru obejmowania oraz zasad dezaktywacji lub odblokowania osób, awizację odwiedzających, zarządzanie biurami przepustek z obsługą czytników dowodów osobistych, aparatu fotograficznego czy też drukarki przepustek. System charakteryzuje się rozbudowanymi możliwościami w zakresie zarządzania obiektami rozproszonymi. Dzięki temu można łatwo raportować i lokalizować zarówno osoby, jak i sprzęt. ●

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

Zdalny monitoring autobusów

Komunikację międzymiastową na terenie Urugwaju zapewniają przede wszystkim przewoźnicy autobusowi. Jednymi z największych są CodelEste i Cromin. Wspólnie dysponują flotą ponad 250 nowoczesnych autokarów, oferując usługi 24 godziny na dobę i przez siedem dni w tygodniu. Obie firmy od wielu lat poszukiwały rozwiązania, które zapewniłoby zdalny całodobowy monitoring wizyjny pojazdów.

Tomasz Kaliński

Powodem tych poszukiwań była chęć poprawy bezpieczeństwa kierowców i pasażerów oraz podniesienie standardu obsługi klienta. Wymogiem kluczowym było przesyłanie obrazu „na żywo" z każdego autobusu do całodobowego centrum bezpieczeństwa. Istotne były też niska cena systemu (w przeliczeniu na jeden pojazd) oraz jego jak najprostsza instalacja.

Wyzwania

Monitoring pojazdów stanowi wyzwanie, ponieważ trzeba zapewnić komunikację pomiędzy kamerami zamontowanymi w pojazdach a jednostką rejestrującą obraz. Jest to dużo trudniejsze niż w przypadku monitorowania obiektu stacjonarnego. O ile w tym drugim przypadku wystarczy połączenie urządzeń w ramach sieci LAN, o tyle w przypadku pojazdów często jedynym sposobem komunikacji jest wykorzystanie transmisji danych przez sieć komórkową. Najczęściej stosowane są zatem dwie metody:

1. **Kamery znajdują się w pojeździe, rejestracja obrazu odbywa się na urządzeniu zamontowanym w pojeździe.**

W przypadku rejestracji na urządzeniu umieszczonym w pojeździe nie trzeba wysyłać obrazu z kamer poprzez GSM, co zmniejsza miesięczne koszty obsługi. Wymaga to jednak od użytkownika zakupu rejestratora z systemem tłumienia drgań. Trzeba pamiętać, że po wyłączeniu silnika rejestrator będzie zużywać energię z akumulatora. Można też zastosować kamery wyposażone w karty SD bez konieczności stosowania rejestratora. Jednak obsługa takiego rozwiązania może być kłopotliwa w perspektywie czasu.

2. **Kamery znajdują się w pojeździe, ale serwer rejestrujący znajduje się w centrum monitoringu.**

W przypadku rejestracji obrazu na zewnętrznym serwerze koszt jest niższy niż w przypadku rejestratorów w każdym pojeździe z osobna. Wymaga to jednak zastosowania odpowiedniego łącza GSM z nielimitowanym pakietem transmisji danych oraz modemu z odpowiednią anteną dla zapewnienia wystarczającego zasięgu. Oczywiście brak zasięgu sieci GSM będzie oznaczał brak transmisji wideo, a co za tym idzie niemożność transferu obrazu na serwer.

Oba rozwiązania mają zalety i wady, dlatego warto rozważyć system hybrydowy, czyli połączenie lokalnej rejestracji z możliwością wysyłania nagrań na serwer zewnętrzny. Taki właśnie system, bazujący na oprogramowaniu Alnet Systems NetStation Enterprise, został wdrożony we wspomnianych urugwajskich firmach.

W każdym autobusie znajdują się 3 kamery IP z opcją nagrywania na kartę SD *(EDGE Recording)*, modem GSM ze stałym publicznym adresem IP oraz switch POE. Natomiast w centrum monitoringu funkcjonującym w bazie autobusowej znajduje się serwer rejestrujący z oprogramowaniem VMS NetStation Enterprise z dostępem do Internetu.

Opis konfiguracji w pojeździe

Po montażu kamer z kartami SD i podłączeniu ich do switcha POE należy je tak skonfigurować sieciowo, aby była możliwość podłączenia się do nich z każdego miejsca na świecie. W większości przypadków wystarczą dwa porty komunikacyjne: port HTTP oraz port RTSP. O ile po stronie kamer mogą pozostać ustawienia domyślne portów, o tyle w przypadku modemu GSM dla każdej kamery osobno trzeba będzie skonfigurować zestaw dwóch portów. Dla przykładu:

		Port LAN kamera	Port WAN forwarding modem GSM
Kamera 1	HTTP	80	8010
	RTSP	554	8011
Kamera 2	HTTP	80	8020
	RTSP	554	8021
Kamera 3	HTTP	80	8030
	RTSP	554	8031

Podczas konfigurowania modemu GSM należy ustawić przekierowanie portów LAN 80 i 554 dla poszczególnych kamer na odpowiednie porty WAN. Umożliwi to komunikację poprzez Internet z każdą z kamer osobno.

Opis konfiguracji po stronie jednostki rejestrującej

Po stronie serwera należy jedynie dodać kamery, pamiętając o podaniu adresu IP WAN modemu GSM oraz odpowiednich portów i włączyć opcję pobierania nagrań z karty SD w konfiguracji programu.

Powyższa konfiguracja jest wystarczająca do rejestracji obrazu w czasie rzeczywistym. W razie utraty połączenia brakujące nagrania zostaną odzyskane, gdy tylko zostanie przywrócone połączenie z kamerą. W przypadku awarii modemu albo zaniku sieci GSM materiał zapisany na kartach SD zostanie zgrany automatycznie przez Wi-Fi, gdy autobus wróci do bazy pojazdów.

W każdym autobusie są dodatkowo monitorowane przycisk napadu, otwarcie kasy gotówkowej, otwarcie klapy silnika, otwarcie klapy zbiornika paliwa. Ponadto system jest wzbogacony o przełącznik, którym kierowca sygnalizuje opuszczenie pojazdu. Po jego użyciu w centrali monitoringu pojawia się obraz pojazdu, z którego kierowca wysiadł, co ułatwia jego monitorowanie przez pracowników ochrony. Trwają też testy akcelerometru, który może wykrywać nagłe hamowanie i kolizje, co spowoduje, że centrum ochrony od razu otrzyma obraz z pojazdu, a na zapisie wideo pojawi się specjalny znacznik ułatwiający lokalizację zdarzenia.

Opisana aplikacja została wdrożona w firmach zajmujących się przewozem osób, ale z powodzeniem może być stosowana również w firmach logistycznych, zajmujących się przewozem towarów, dążących do jak najwyższego standardu ochrony własnych pracowników i powierzonego im mienia. ●

Alnet Systems
Olivia Business Centre
al. Grunwaldzka 472B, 80-309 Gdańsk
www.alnetsystems.com

Rośnie wartość rynku kontroli dostępu

Wartość światowego rynku kontroli dostępu wzrośnie z 10,4 mld USD w 2024 r. do 15,2 mld USD w 2029 r. To oznacza, że średnia roczna stopa wzrostu w latach 2024-29 wyniesie ok. 7,8%. Tak twierdzą eksperci firmy badawczej Marketsandmarkets.

Skąd ten wzrost? I czy jest to stały trend, czy raczej chwilowy pik wywołany np. sytuacją geopolityczną? W których branżach można spodziewać się największego wzrostu inwestycji w systemy kontroli dostępu, a w których już jest on wyraźny?

Iwona Krawiec

Biorąc pod uwagę zalety systemów kontroli dostępu, nie dziwi fakt, że zainteresowanie nimi wzrasta. Sektorem, który najwięcej w nie inwestuje, jest przemysł, szczególnie ten najbardziej innowacyjny, bliski idei Przemysłu 4.0, gdzie systemy dostępowe coraz częściej są zintegrowane z innymi cyfrowymi rozwiązaniami stosowanymi przez przedsiębiorstwa. Za sprawą algorytmów AI i uczenia maszynowego możliwe jest bardziej zaawansowane i efektywne zarządzanie dostępem do poszczególnych stref w obiektach zakładów przemysłowych.

Kolejnym sektorem są obiekty infrastruktury krytycznej. Tutaj też nakłady rosną, co nie powinno dziwić. Ma na to wpływ sytuacja geopolityczna. Niezależnie od tego, w której części świata usytuowany jest obiekt IK, każdy nim zarządzający, widząc to, co dzieje się w globalnej wiosce, będzie dążyć do wzmocnienia ochrony. Patrząc na polskie albo szerzej europejskie podwórko, znaczący wzrost inwestycji w zaawansowane systemy kontroli dostępu jest związany z oczekiwaną nowelizacją ustawy o krajowym systemie cyberbezpieczeństwa (w związku z dyrektywą NIS2) i zmianą wymogów dla polskich przedsiębiorstw.

– Firmy w tym sektorze stawiają na systemy, które oferują zaawansowane rozwiązania cybersecurity, integrację z istniejącymi systemami bezpieczeństwa IT i zaawansowane metody uwierzytelniania wieloskładnikowego. Ponadto firmy w tej branży są zainteresowane

» *Niezależnie od tego, w której części świata usytuowany jest obiekt IK, każdy nim zarządzający, widząc to, co dzieje się w globalnej wiosce, będzie dążyć do wzmocnienia ochrony.* «

systemami wspierającymi import certyfikatów autentykacyjnych przygotowanych przez klientów i podpisanych przez zaufane Certificate Authority (CA). Obserwujemy także większe zainteresowanie mechanizmami umożliwiającymi przechowywanie kluczy szyfrujących karty na kontrolerach zamiast czytników (tryb transparenty). Takie podejście zapewnia wysoki poziom bezpieczeństwa, co jest kluczowe dla obiektów infrastruktury krytycznej – zauważa Anna Twardowska z Nedap Security Management.

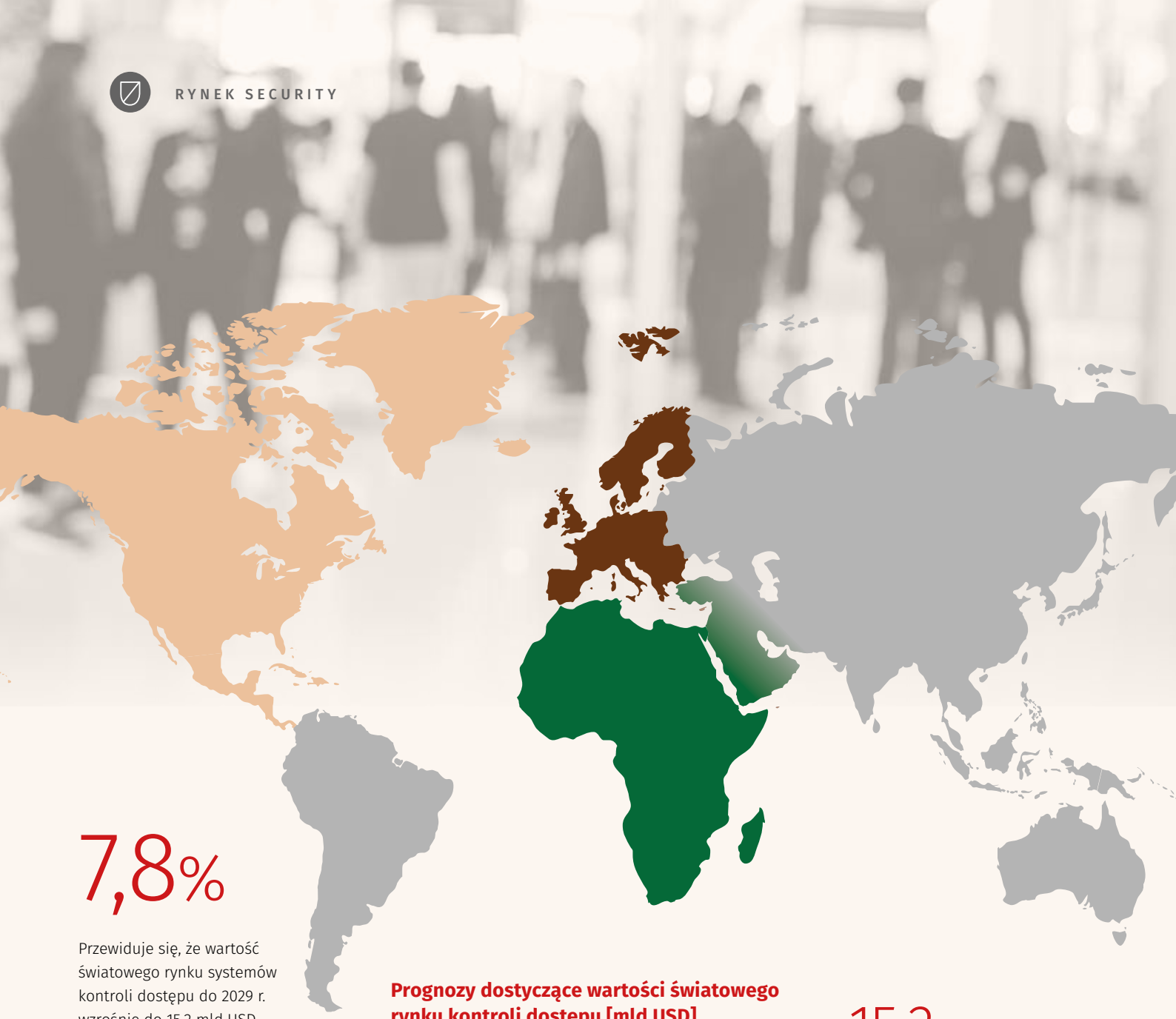
Na potrzebę stosowania rozwiązań wykorzystujących nowoczesne technologie, zwłaszcza w obiektach infrastruktury krytycznej, zwraca uwagę Marek Piotrowski z ZKTeco Europe.

– Od ubiegłego roku wprowadzamy wysoko zaawansowany, zarówno od strony technicznej, jak i zabezpieczeń, system kontroli dostępu ARMATURA (wkrótce z certyfikatem Grade 4). Spowodowało to, że naszymi systemami interesują się firmy z sektora infrastruktury krytycznej, które chcą kompleksowo realizować złożone projekty. To zjawisko nasili się z pewnością jesienią, kiedy wyjdą w życie wymagania postawione dla tego sektora przez NIS-2. Jesteśmy na to przygotowani, tym bardziej że jesteśmy liderami na światowych rynkach, jeśli chodzi o czytniki biometryczne, które gwarantują bardzo wysoki stopień zabezpieczeń – dodaje Marek Piotrowski.

Przeciętnemu użytkownikowi kontrola dostępu kojarzy się przede wszystkim z możliwością wejścia do budynku, np. biurowego. I słusznie. Coraz więcej firm decyduje się na unowocześnienie już funkcjonujących rozwiązań, które mają być jednocześnie elastyczne, łatwe dla użytkowników i skalowalne.

– W sektorze nowoczesnych biur, poza rozwiązaniami cybersecurity, obserwujemy rosnące zainteresowanie rozwiązaniami wykorzystującymi np. Apple Wallet. Jest to odpowiedź na potrzeby klientów, czyli najemców, oczekujących jednocześnie wygody i bezpieczeństwa. Apple Wallet pozwala na łatwe zarządzanie cyfrowymi kluczami dostępu, które można przechowywać na iPhone'ach lub smartwatchach Apple, eliminując potrzebę wprowadzania fizycznych kart dostępu. Organizacje wybierają to rozwiązanie ze względu na jego zaawansowane mechanizmy bezpieczeństwa – komentuje Anna Twardowska.

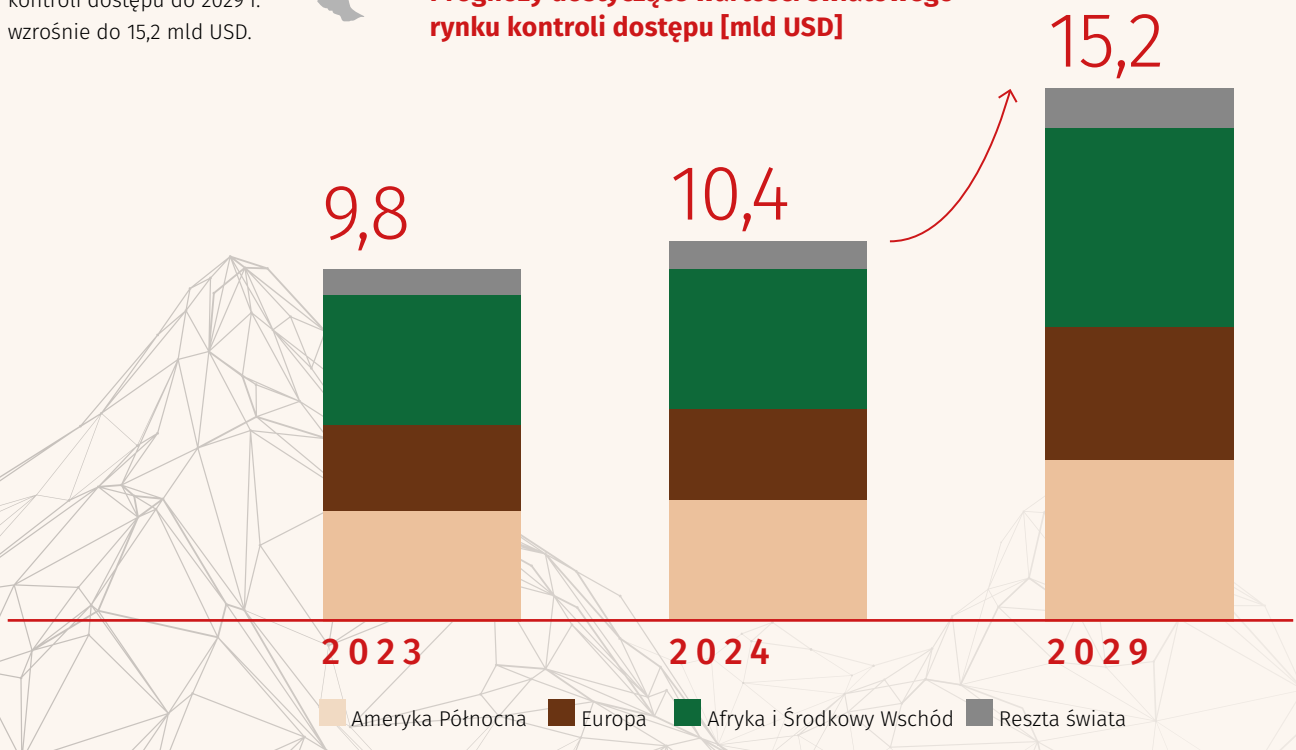
Wspomniana wcześniej globalna wioska korzysta z globalnego transportu. Ten sektor gospodarki zawsze był bardzo ważny, ale chyba dopiero nieszczęsna triada: brexit, pandemia, wojna w Ukrainie dobitnie uzmysłowiły wielu osobom i organizacjom, jak jest ważne, by transport i logistyka działały sprawnie. Ta sprawność wymaga pełnej ochrony łańcucha dostaw. To ważne z uwagi na dużą konkurencyjność w tym sektorze. Z kolei instytucje branży finansowej intensywnie →



7,8%

Przewiduje się, że wartość światowego rynku systemów kontroli dostępu do 2029 r. wzrośnie do 15,2 mld USD.

Prognozy dostyczące wartości światowego rynku kontroli dostępu [mld USD]



Źródło: www.marketsandmarkets.com

rozwijają systemy KD w celu ochrony danych klientów i zapewnienia bezpieczeństwa transakcji.

Sektor hotelarski, podobnie jak inne branże, również musi uwzględniać zmieniające się uwarunkowania geopolityczne, które wpływają na ruch turystyczny, a to na wyniki finansowe. Elastyczność i umiejętność szybkiego reagowania na zmiany stały się kluczowymi cechami skutecznego zarządzania w hotelarstwie. Technologia odgrywa coraz większą rolę w transformacji tego sektora, umożliwiając nie tylko poprawę bezpieczeństwa i komfortu gości, ale także optymalizację procesów operacyjnych i redukcję kosztów.

– Branża hotelowa w coraz większym stopniu kładzie nacisk na wdrażanie rozwiązań zwiększających bezpieczeństwo gości i pracowników oraz samych obiektów hotelowych. Nasi klienci i użytkownicy w szczególności cenią rozwiązania kontroli dostępu, które z jednej strony umożliwiają maksymalne ograniczenie kontaktu bezpośredniego, dzięki wdrożeniu szerokiej gamy rozwiązań opartych na technologii kluczy mobilnych, a z drugiej są w stanie objąć dozorem wszystkie części obiektu hotelowego z poziomu jednej platformy (od pokoi hotelowych, poprzez części konferencyjne i SPA, aż po zaplecze i strefy techniczne). W połączeniu z nowoczesnymi bezpiecznymi kartami i nośnikami zapewnia to najwyższy standard bezpieczeństwa – mówi Przemysław Dawidziuk z Salto Systems.

Te właśnie sektory gospodarki wykazują największą dynamikę w zakresie inwestycji w systemy kontroli dostępu, co wynika z potrzeby zwiększenia bezpieczeństwa i integracji z nowoczesnymi technologiami.

Dominujące trendy

Jak w przypadku każdej dziedziny gospodarki, tak i w sektorze kontroli dostępu da się zauważyć dominujące trendy. Nie dziwi fakt, że są zbieżne z najpopularniejszymi dominującymi na światowym rynku technologicznym. Jednym z nich jest presja na zachowanie integralności danych, które są generowane i gromadzone przez urządzenia kontrolujące, a także odporność na cyberataki tych urządzeń oraz systemów, w których ramach działają.

Każdy komponent systemu dostępowego, począwszy od kart dostępu, przez czytniki, skończywszy na kontrolerach i oprogramowaniu, wymaga szczególnej uwagi. Często nie zdajemy sobie sprawy, że tak wydawałoby się błaha rzecz, jak wybór karty dostępu, może okazać się kluczowa dla zachowania bezpieczeństwa całej firmy. Karta może być najsłabszym elementem, ponieważ można ją klonować i kopiować, a także manipulować nią, a ewentualny atakujący, jeśli wejdzie w jej posiadanie, uzyska wielogodzinny dostęp do zasobów firmy.

– Wybór odpowiednio zabezpieczonej karty, takiej jak Mifare Desfire, Mifare Plus, uniemożliwi skopiowanie karty, ale już niej jej kradzież – zauważa Piotr Karpiński z STid Security. *– Lepszym wyborem będzie karta wirtualna, aktywna po odblokowaniu telefonu biometrią lub FaceId. Takiej karty nie zgubimy, a w przypadku utraty telefonu można ją zdalnie dezaktywować. Dodatkowym atutem jest to, że jest ekologiczna i tańsza od jej plastikowego odpowiednika.*

Jak jednak sprawdzić, czy firma korzysta z rozwiązania odpornego na cyberzagrożenia?

– Kluczowe jest ustalenie wieku systemu lub daty ostatniej wymiany kart. Systemy młodsze niż 10 lat mogą być bezpieczne, o ile karty zostały odpowiednio dobrane. Starsze prawdopodobnie wymagają modernizacji – twierdzi Piotr Karpiński. *– Często też wystarczy do czytnika przyłożyć różne karty kredytowe, bankomatowe czy dowód osobisty. Jeśli czytnik zareaguje, to oznacza albo brak bezpieczeństwa, albo źle skonfigurowany system.*

A jakie rozwiązania zastosować, aby zabezpieczyć firmowy system KD przed cyberatakiem. Bartłomiej Bzymek z firmy Genetec radzi: *– Po pierwsze, wszelkie dane muszą być szyfrowane. Po drugie, przed udzieleniem dostępu do chronionego zasobu tożsamości użytkownika, serwera lub aplikacji klienckiej musi być weryfikowana. Po trzecie, system kontroli dostępu powinien być stale monitorowany pod kątem stanu i pojawiających się aktualizacji. I dotyczy to uaktualnień zarówno czytników, kontrolerów, jak i serwerów oraz jednostek klienckich.*

Integracja z technologiami AI i uczenia maszynowego jest kolejnym wyraźnym trendem. Wykorzystanie sztucznej inteligencji do analizy wzorców dostępu oraz wykrywania anomalii i możliwość szybkiej adaptacji do zmieniających się warunków są bardzo pomocne dla osób zarządzających obiektami.

> *» Współczesne trendy w kontroli dostępu odzwierciedlają rosnące zapotrzebowanie na inteligentne, elastyczne i bezpieczne rozwiązania. «*

Coraz większą popularność zyskuje biometryczna weryfikacja użytkowników. Najczęściej jest to rozpoznawanie twarzy oraz skanowanie tęczówki oka. Z uwagi na komfort zastosowania wzrasta zainteresowanie użytkowników poświadczeniami mobilnymi. Temu trendowi sprzyjają coraz bardziej zaawansowane smartfony. Wykorzystywanie ich jako kluczy podnosi komfort i elastyczność rozwiązania, w zamian za to redukuje jego koszt, ponieważ nie trzeba drukować kart dostępu, a proces przyznawania uprawnień odbywa się automatycznie. Coraz więcej firm decyduje się także na wprowadzenie systemów kontroli dostępu funkcjonujących w chmurze i przez aplikacje chmurowe zarządzanych. Chmura ma tę zaletę, że zazwyczaj oferuje taką moc obliczeniową, że kontrola nad obiektem może być prowadzona w czasie rzeczywistym.

– Kontrola dostępu w chmurze umożliwia łatwe zarządzanie systemem z każdego miejsca na świecie przez całą dobę. Gwarantuje to użytkownikom wyjątkową mobilność i elastyczność. Priorytetem w naszym systemie jest bezpieczeństwo. Dzięki zaawansowanym technologiom Microsoft Azure zapewniamy solidną ochronę przed nieautoryzowanym dostępem i cyberatakami. Nasi klienci doceniają też niższe niż w przypadku lokalnego systemu koszty początkowe wdrożenia, wygodną płatność subskrypcyjną oraz łatwą integrację z innymi systemami bezpieczeństwa. To znacznie ułatwia zarządzania przedsiębiorstwem – podkreśla Andrzej Mendak z UNICARD Systems.

Współczesne trendy w kontroli dostępu odzwierciedlają rosnące zapotrzebowanie na inteligentne, elastyczne i bezpieczne rozwiązania, które mogą sprostać wymaganiom nowoczesnych organizacji w zakresie ochrony zasobów fizycznych i cyfrowych. Skoro zaciera się granica między światem realnym a wirtualnym, to kompleksowe podejście do bezpieczeństwa, w tym cyberbezpieczeństwa, przestaje być luksusem, a staje się koniecznością. ●

Przepraszam, a pan do kogo?

Zapewne niejedna z czytających ten tekst osób ma w pamięci taki obrazek: na podwórku zabawa trwa w najlepsze, nikt nie zaryzykuje powrotu do domu po piłkę. Wystarczyło wtedy krzyknąć w stronę okna: „Maaaamo, daaaj... piłkę!". Czasami w zamian mama odkrzykiwała: „Jaaaanek, obiaaad!". A potem przyszła era domofonów. I na podwórkach zapadła cisza.

Monika Żuber-Mamakis

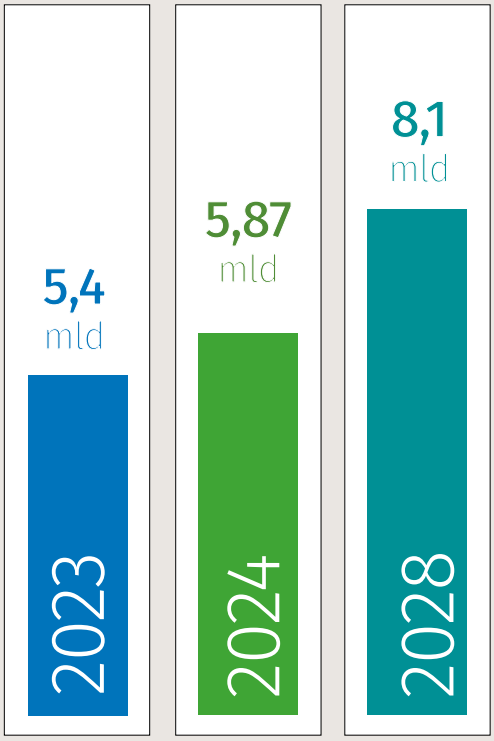
Nie trzeba już bowiem było krzyczeć. Wystarczyło zadzwonić domofonem. Można oczywiście było też przednio się bawić, dzwoniąc po kolei do wszystkich mieszkań w bloku albo domów przy ulicy. Pierwsze domofony w naszym kraju pojawiły się w latach 70. ubiegłego wieku. W serialu „Wojna domowa", który powstawał w latach 1965–66, domofon jest pokazywany zagranicznym gościom jako rzecz niebywała. Jednak tak naprawdę urządzenia te stały się popularne w latach 90. ubiegłego wieku. Mniej więcej w tym samym czasie, gdy na potęgę zaczęły powstawać szczelnie grodzone osiedla stawiane przez deweloperów. Wówczas mieszkańcy starych PRL-owskich uznali, że ich własność też musi być chroniona. Czasy gospodarczej transformacji wiele zmieniły. Nikt już teraz nie krzyczy „Jaaanek, obiad!". Do lamusa odchodzą też zwykłe domofony, sukcesywnie wypierane przez swoje lepsze, bardziej zaawansowane wersje, czyli wideodomofony.

Kogo tam niesie?

Lubimy czuć się bezpiecznie. Zwykły domofon nie gwarantuje, że odpowiedź na pytanie: „Kto tam?", będzie prawdziwa, tym bardziej że często pada enigmatyczne „ja", które prowadzi do innego równie popularnego pytania „Co za »ja«?". Wideodomofon dusi ten niezbyt mądry dialog w zarodku.

Nic dziwnego, że globalny rynek tych urządzeń miewa się świetnie, a wiele wskazuje na to, że mieć się będzie jeszcze lepiej (*patrz grafika*). Rosnącej sprzedaży sprzyja fakt, że wideodomofony dają poczucie, całkiem słuszne, że jesteśmy chronieni lepiej niż wtedy, gdy dostępu do nas bronią tradycyjny zamek i dzwonek do drzwi.

Przewidywania dotyczące światowego rynku systemów wideodomofonowych



• DUŻY WZROST
Oczekuje się, że rynek wideodomofonów wzrośnie do 8,1 mld dolarów do 2028 roku, przy CAGR wynoszącym 8,4%.

• POWODY WZROSTU
Wzrost rynku jest napędzany głownie rozwojem sektora inteligentnych domów

• GŁÓWNE TRENDY
Integracja asystentów głosowych, instalacje wielorodzinne, analityka oparta na AI, rozwiązania oparte na chmurze, zdalny dostęp i zarządzanie mobilne, inwestycje w bezpieczeństwo.

• NAJWIĘKSZY RYNEK
W roku 2023 najwięcej urządzeń zainstalowano w rejonie Ameryki Północnej.

Źródło: www.thebusinessresearchcompany.com/

Ważne, że ten rodzaj urządzeń przeszedł sporą metamorfozę. To już nie jest trochę lepszy dzwonek do drzwi zintegrowany z kamerą. Obecnie urządzenia te z powodzeniem mogą być stosowane jako element zarządzania bezpieczeństwem budynków komercyjnych, ponieważ można je zintegrować z systemami telewizji dozorowej, kontroli dostępu oraz zarządzania budynkiem. Systemy te oferują m.in. kolejkowanie połączeń alarmowych, przywoływanie oraz audiowizualne identyfikowanie gości. Ponadto mogą zdalnie odblokowywać drzwi za pomocą elektrycznego rygla, aby umożliwić gościom wejście do budynku, a także przekazywać informacje o gościach do wielu stacji za pośrednictwem standardowej stacji głównej lub aplikacji na urządzenia mobilne.

Nie bez znaczenia jest też to, że wideodomofony stają się coraz bardziej przystępne cenowo. Przeciętny Kowalski może sobie na takie urządzenie pozwolić. A malejąca różnica cenowa między nimi a tradycyjnymi domofonami zachęca konsumentów do inwestowania w te zaawansowane urządzenia, oferujące znacznie więcej możliwości. Argumentem za posiadaniem takiego urządzenia, i prywatnie, i w firmie jest też możliwość negocjowania składki ubezpieczeniowej.

Mysz się nie prześlizgnie

Producenci stale podnoszą poprzeczkę, jeśli chodzi o jakość obrazu i dźwięku. Na rynku pojawiają się modele z monitorami o przekątnej 10 cali, czyli ponad 25 cm. To już taka wielkość ekranu, która pozwala dostrzec nie tylko oko i ewentualnie nos osoby (i to jak przez obiektyw rybie oko), która chce wejść, ale także jej postać i upewnić się, że nikt nie czyha obok. Urządzenie może być też połączone z zainstalowanym w nieruchomości systemem smart home, zyskuje wtedy dodatkowe funkcje, którymi można zawiadywać z aplikacji na smartfonie, także zdalnie. Natomiast najnowszy trend do wideodomofony z funkcją rozpoznawania twarzy. Dzięki zastosowanym w oprogramowaniu urządzenia algorytmom AI kamera automatycznie rozpoznaje twarz osoby uprawnionej i zezwala na wejście. Kto został wcześniej zarejestrowany w systemie, ten wchodzi. Kto nie, ten musi czekać, aż ktoś mu otworzy drzwi. Mysz się nie prześlizgnie. Z kotami bywa różnie. To oczywiście stawia przed producentami zarówno urządzeń, jak i oprogramowania wyzwania w postaci zadbania o prywatność osób, które mają okazję być zarejestrowane przez kamerę wideodomofonu. Nic też nie stoi na przeszkodzie, by obraz rejestrowany przez kamerę został zapisany na serwerze lokalnym lub w chmurze. Takie nagranie może posłużyć na przykład jako materiał dowodowy.

Z tym ostatnim łączy się kwestia zachowania prywatności osób nagrywanych. Owszem, producenci skupiają się na zapewnieniu najwyższych standardów bezpieczeństwa danych i zgodności z przepisami RODO. Rejestrując jednak nagrania pochodzące z kamery, trzeba mieć na względzie, że dostęp do nich powinien być bardzo skrupulatnie strzeżony.

Rynek wideodomofonów ewoluuje w kierunku coraz bardziej zaawansowanych urządzeń zapewniających wyższy poziom bezpieczeństwa. To już nie modny gadżet, a coraz bardzie oczywisty element codziennego życia. ●

DAHUA TECHNOLOGY POLAND

Wielorodzinna stacja bramowa VTO6521K

Przedstawiamy jeden z nowych modeli wideodomofonu wielorodzinnego, zintegrowaną stację bramową przeznaczoną dla rozwiązań wielorodzinnych **VTO6521K** w standardzie IP, wykorzystującą technologię SIP. Obudowa stacji bramowej jest wykonana ze stali nierdzewnej klasy 316, dzięki temu ma klasę odporności mechanicznej IK08. Urządzenie zawiera w jednej obudowie moduł kamery, duży 4,3-calowy kolorowy wyświetlacz LCD, klawiaturę mechaniczną z kodem Braille'a oraz czytnik kart w standardzie Mifare. Ponadto klawiatura jest podświetlona na niebiesko. Stacja współpracuje ze wszystkimi monitorami IP oferowanymi przez Dahua Technology Poland. Możliwy jest montaż stacji w sposób podtynkowy i natynkowo. Są do tego celu dostępne odpowiednie akcesoria. Dodatkowym elementem jest doświetlenie widzialnym światłem białym.
Zasilanie stacji bramowej wynosi DC 12 V. W kamerze zastosowano przetwornik 2 Mpix. Możliwe jest kodowanie zarówno H.264, jak i H.265. Stacja jako serwer SIP może obsłużyć nawet do 500 urządzeń.
To pierwsza stacja w naszej ofercie, która oferuje tak dużo. Może obsłużyć nawet do 20 tys. użytkowników, w tym 10 tys. haseł i 10 tys. kart/breloków. Obsługuje również kody QR.
Na uwagę zasługuje możliwość otrzymywania powiadomień poprzez aplikację mobilną. Dzięki niej można zdalnie zobaczyć osobę dzwoniącą, odebrać rozmowę czy otworzyć drzwi. Najnowsza wersja *firmware* tej stacji oraz monitora w mieszkaniu zapewnia również wykorzystanie monitorów do połączenia z Internetem oraz aplikacją mobilną, a także dodatkową funkcjonalność dwukierunkowego połączenia pomiędzy aplikacją a monitorami. Wykorzystuje się do tego dwa interfejsy w monitorach – kablowy Ethernet do połączenia z pozostałymi monitorami i stacją bramową oraz Wi-Fi do podłączenia do routera i Internetu. Ta stacja jest odpowiednią propozycją zarówno dla instalatorów, jak i użytkowników końcowych.

Więcej na www.dahuasecurity.com

GDE POLSKA

Wideodomofony REVIZOOM

REVIZOOM to marka wywodząca się z systemów telewizji dozorowej, gdzie jakość obrazu, stabilność połączenia oraz bezpieczeństwo danych mają istotne znaczenie przy wyborze konkretnego rozwiązania. Produkty wideodomofonowe REVIZOOM przejmują te ważne cechy systemów CCTV, oferując niezawodność działania w połączeniu z ciekawymi rozwiązaniami funkcjonalnymi i nowoczesnym wyglądem. Prosta konfiguracja oraz kompatybilność elementów pozwala na wybór rozwiązania dopasowanego do potrzeb użytkownika. Monitory REVIZOOM serii SMART 4WIRE to główne „centrum dowodzenia" systemu wideodomofonowego. Poza oczywistymi funkcjami komunikacji z panelami wejściowymi mają możliwość integracji z kamerami dozorowymi CCTV, komunikację interkomową, pamięć zdarzeń z zapisem filmów z paneli wejściowych, funkcję detekcji ruchu, a także przekierowanie rozmów na urządzenia mobilne. Do wyboru są modele z ekranami dotykowymi w rozmiarach 7" oraz 10". System może być rozbudowywany o kolejne monitory (maks. 6) lub unifony (do komunikacji audio). System ma możliwość ustawienia czasu otwarcia wejścia, zaprogramowania komunikatów głosowych (np. w przypadku nieobecności użytkownika i nieodbierania połączenia), a także obsługi funkcji multimedialnych: odtwarzanie muzyki, zdjęć (ramka cyfrowa) i filmów.
Stacje bramowe to panele jednoabonentowe oraz 2- i 3-abonentowe. Rozdzielczość 2 Mpix gwarantuje wysoką jakość obrazu wyświetlanego na monitorach oraz urządzeniach mobilnych, a szeroki kąt widzenia kamery obejmuje większy obszar terenu przed wejściem. Model RC-411HD-CK jest wyposażony w klawiaturę numeryczną, umożliwiając zaprogramowanie i użycie do otwarcia wejścia do ponad 200 kodów użytkowników, a także w czytnik RFID pozwalający na otwarcie wejścia poprzez przyłożenie jednej z 200 zaprogramowanych kart/breloków.

Więcej na www..gde.pl

HIKVISION POLAND

System wideodomofonowy 2-wire HD

2-wire HD to system wideodomofonowy, który do komunikacji między poszczególnymi urządzeniami wykorzystuje 2 żyły. W zależności od okablowania i struktury systemu można uzyskać odległość między skrajnymi urządzeniami do 1760 m. Technologia 2-wire pozwala na stabilne i szybkie przesyłanie obrazu wysokiej rozdzielczości, dwukierunkowego audio i komend sterujących. System może być zbudowany w topologii gwiazdy, kaskady lub mieszanej. Uproszczona procedura konfiguracji, która nie wymaga od instalatora zaawansowanej wiedzy z zakresu IT, umożliwia intuicyjną konfigurację, a w czasie awarii szybką lokalizację usterki. Pojedynczy zasilacz DS-KAW150-4N może zasilić do 64 monitorów KH7300EY-TE2 i do 16 dystrybutorów piętrowych KAD7061EY. Mała liczba elementów pośrednich DS-KAD7060EY (główny dystrybutor), DS-KAD-7061EY (dystrybutor piętrowy), DS-KAD7060EY-S (dystrybutor do systemów wielobudynkowych) pozwala łatwo dobrać właściwe urządzenia. Adresowanie monitorów można wykonać za pomocą przełączników dziesiętnych zlokalizowanych w tylnej części obudowy. Konfigurację pozostałych funkcji można przeprowadzić z poziomu telefonu, po połączeniu telefonu z punktem dostępowym (tryb AP) udostępnionym przez stację bramową. Moduł stacji bramowej DS-KD7003EY-IME2, wyposażony w kamerę, można rozbudować o dodatkowe rozszerzenia, np. moduł wyświetlacza, moduł informacyjny, wizytownik z 6 przyciskami, klawiaturę mechaniczną, czytnik kart. Dostępne są 2 modele 7-calowych monitorów dotykowych o rozdzielczości 1024x600, z Wi-Fi lub bez, w kolorze białym lub czarnym. Wersja z Wi-Fi współpracuje z aplikacją Hik-Connect.
Te zalety umożliwiają zastosowanie systemu 2-wire HD nie tylko w nowych projektach, ale także w modernizowanych systemach, w których pojawiają się ograniczenia związane z już istniejącym okablowaniem, jego strukturą i odległościami. Ograniczenie kosztów związanych z okablowaniem, instalacją i konfiguracją gwarantuje, że system 2-wire HD jest atrakcyjnym uzupełnieniem oferty systemów domofonowych firmy Hikvision.

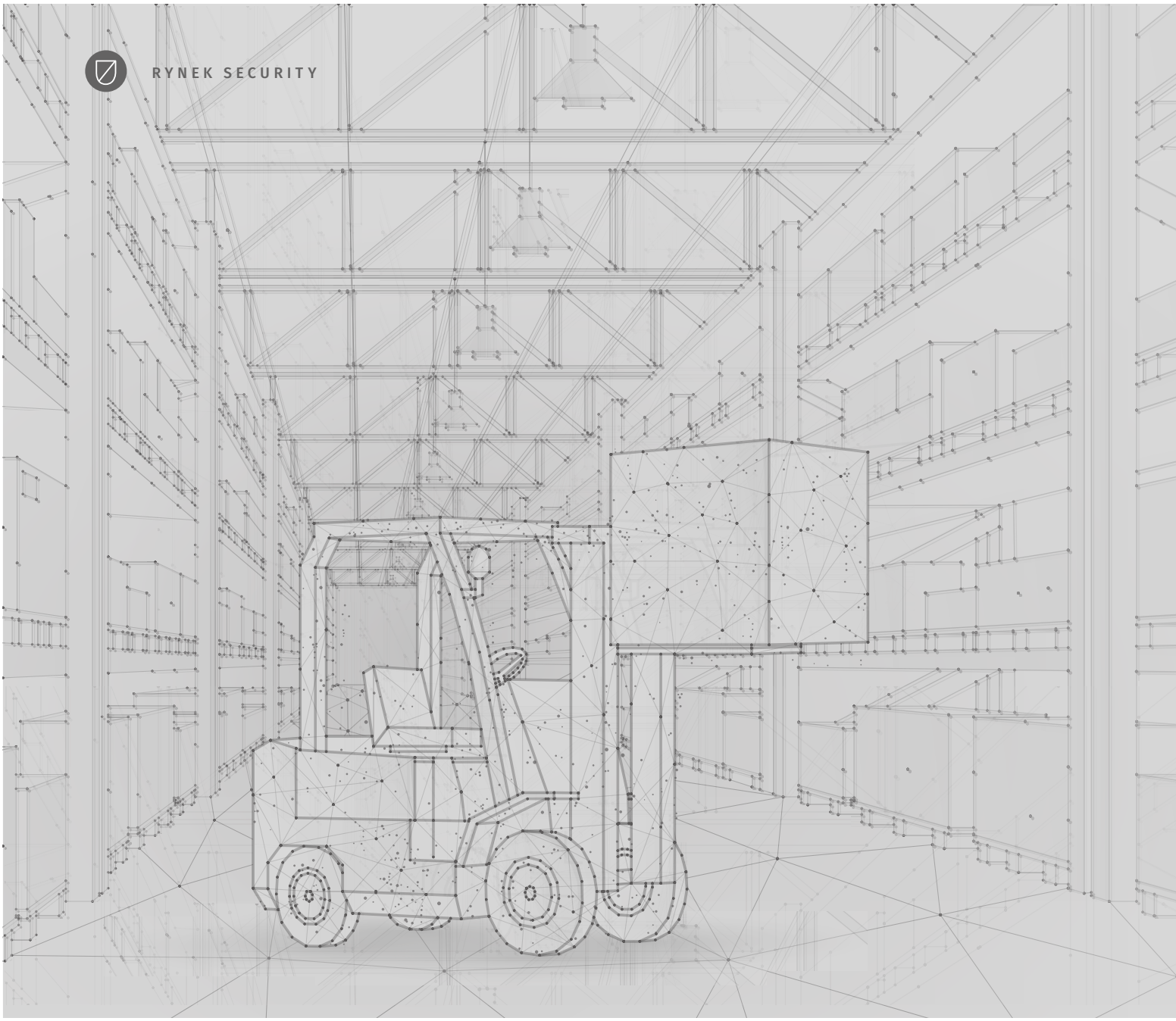
Więcej na www.hikvision.com/pl

ZKTECO EUROPE

Wideodomofony IP z oferty ZKTeco

Firma ZKTeco dysponuje szeroką ofertą wideodomofonów jedno- i wielolokatorskich, modelami z protokołem SIP2.0 czy też stanowiących element systemu kontroli dostępu. Podstawę oferty stanowią 2-żyłowe wideodomofony IP oparte na systemie Linux. Wśród nich VE01-B22L – panel z czytnikiem kart RFID, wyposażony w POE i możliwość pracy w standardzie SIP 2.0, VE01-B23L – o takich samych parametrach, jak VE01-B22L, ale zamiast czytnika RFID ma szyfrator, E01- B24L-W – nowy kompaktowy panel z interfejsem Wi-Fi na wypadek utraty połączenia przewodowego oraz funkcję wykrywania ruchu, VE01-B28L – wkrótce dostępny panel z wbudowaną pamięcią. Wszystkie te panele współpracują z wielofunkcyjnymi monitorami IP VT07-B22L i VT07-C22L wyposażonymi w ekran dotykowy o przekątnej 7 cali lub 10 cali, do których można dołączyć jeszcze do 8 kamer CCTV. Aluminiowe panele VEX-B21L wielolokatorskie są wyposażone w szyfrator, czytnik kart RFID, POE oraz możliwość zdalnego otwarcia drzwi. Integrują się z siecią telefonów IP i systemami z protokołem SIP. Dostępny jest też model VEX-B21A oparty na systemie Android. Wkrótce pojawią się w ofercie nowe eleganckie wielolokatorskie panele wykonane z aluminium i hartowanego szkła VEX-B24L i VEX B24A.
Panele wejściowe są wyposażone w funkcję *anti-spoofing* oraz kompensację oświetlenia tylnego. Firma ZKTeco stale pracuje nad linią wideodomofonów wykorzystujących protokół SIP2.0 (RFC3261) oraz linią urządzeń opartych na profesjonalnym autonomicznym terminalu kontroli dostępu i rejestracji czasu pracy F35 z kamerą o kącie widzenia 135°, czytnikiem linii papilarnych i kart RFID oraz szyfratorem dotykowym. Ważną cechą wideodomofonów ZKTeco jest możliwość ich współpracy z modułową platformą bezpieczeństwa ZKBioCVSecurity, dzięki czemu możliwa jest ich integracja z innymi produktami tej firmy. Dostępna jest też aplikacja ZSmart do ich zdalnej obsługi.

Więcej na www.zkteco.eu/pl/



Mapa inwestycji

Mimo zapowiadanego przez media kryzysu gospodarczego w branży budowlanej nie widać wielkiego spowolnienia. W całym kraju powstają nowe obiekty różnego przeznaczenia. W tym numerze informujemy m.in. o przedsięwzięciach dla branży kolejowej, wojskowej, energetycznej, a także budowlach codziennego przeznaczenia, jak hotele, obiekty sportowe czy urzędy. Tradycyjnie informujemy o najświeższych projektach, które dopiero ruszają bądź są jeszcze na etapie projektowania, których terminy zakończenia nie upływają przed początkiem 2025 r.

Adela Prochyra, a&s Polska

BUDIMEX

Co: **ROZBUDOWA I MODERNIZACJA STACJI PIŁA KRZEWINA WRAZ Z PRZEŁĄCZENIEM TORU LINII 400 KV PIŁA KRZEWINA-PŁEWISKA PRACUJĄCEGO NA NAPIĘCIU 220 KV NA NAPIĘCIE 400 KV**
Gdzie: Piła
Kiedy: 45 miesięcy od dnia zawarcia umowy (22.05.2024)
1

ERBUD

Co: **BUDOWA NOWEGO BUDYNKU ODDZIAŁU IPN**
Gdzie: Kraków
Kiedy: min. 42 miesiące od daty zawarcia kontraktu (07.07.2024)
2

Co: **WYBUDOWANIE BUDYNKÓW MIESZKALNEGO I HOTELOWEGO PRZY UL. SIENNICKIEJ 48 – UMOWA WARUNKOWA**
Gdzie: Warszawa
Kiedy: 18.11.2025
3

MIRBUD

Co: **BUDOWA/MODERNIZACJA INFRASTRUKTURY WODNOKANALIZACYJNEJ, DROGOWEJ, ELEKTRO-ENERGETYCZNEJ NA TERENIE DOLNOŚLĄSKIEJ STREFY AKTYWNOŚCI GOSPODARCZEJ**
Gdzie: Jawor
Kiedy: 13 miesięcy od dnia zawarcia umowy (05.06.2024)
4

Co: **PRZEBUDOWA STADIONU MIEJSKIEGO**
Gdzie: Chełm
Kiedy: 33 miesiące od dnia zawarcia umowy (22.05.2024)
5

MOSTOSTAL PŁOCK I MOSTOSTAL WARSZAWA

Co: **BUDOWA ZBIORNIKÓW MAGAZYNOWYCH DLA PERN S.A.**
Gdzie: Dębogórze
Kiedy: 72 tygodnie (data zawarcia umowy 04.06.2024)
6

Co: **BUDOWA I UTRZYMANIE OŚRODKA SPORTOWO-REKREACYJNEGO W FORMULE PPP**
Gdzie: Łódź
Kiedy: brak informacji
7

Co: **PODKARPACKIE CENTRUM LEKKIEJ ATLETYKI**
Gdzie: Rzeszów
Kiedy: 31.10.2026
8

MOSTOSTAL ZABRZE

Co: **DOKOŃCZENIE BUDOWY HOSPICJUM STACJONARNEGO PRZY UL. BARBÓRKI**
Gdzie: Rybnik
Kiedy: I kwartał 2026
9

P.A. NOVA

Co: **BUDOWA BUDYNKU PRODUKCYJNEGO Z ZAPLECZEM SOCJALNO-BIUROWYM WRAZ Z INFRASTRUKTURĄ TOWARZYSZĄCĄ**
Gdzie: Konieczki
Kiedy: III kwartał 2025
10

POZNAŃSKA KORPORACJA BUDOWLANA

Co: **BUDOWA HALI MAGAZYNOWO-PRODUKCYJNEJ WRAZ Z ZAPLECZEM SOCJALNO-BIUROWYM ORAZ INFRASTRUKTURĄ TECHNICZNĄ TOWARZYSZĄCĄ**
Gdzie: Ruda Śląska
Kiedy: 1 kwietnia 2025
11

Security w hotelarstwie – perspektywy

Branża hotelarska, podobnie jak wiele innych sektorów, przechodzi obecnie transformację. W ciągu ostatnich kilku lat zmieniły się realia i oczekiwania klientów. Hotele muszą teraz zaktualizować swoje standardy. Jednym z kluczowych aspektów tych zmian jest bezpieczeństwo, które zyskało na znaczeniu zwłaszcza w kontekście pandemii COVID-19 oraz rosnącej świadomości zagrożeń. Czy to oznacza nowe szanse dla branży security?

Adela Prochyra

Bazując na najnowszych raportach i analizach, przyglądamy się perspektywom, jakie rysują się przed branżą security w branży hotelarskiej. Czy zmiana nawyków i oczekiwań klientów wymusi na właścicielach sieci i pojedynczych obiektów nowe podejście do kwestii ochrony zdrowia, życia i mienia gości?

Rosnące wymagania gości

Oczekiwania są, i to niemałe. Goście hotelowi coraz częściej oczekują nie tylko komfortu, ale także, a może przede wszystkim, wysokiego stopnia bezpieczeństwa. Należy to rozumieć również w sensie dosłownym – jako fizyczne zabezpieczenie pokoju hotelowego przed włamaniem i kradzieżami, ochrona całego obiektu przed wtargnięciem osób niepowołanych, ale także jako ochrona zdrowia hotelowych gości. W luksusowych hotelach, gdzie standardy są szczególnie wysokie, goście nieraz chcą wiedzieć, jakie środki zostały podjęte, aby zapewnić im bezpieczeństwo.

Nowe standardy ochrony nieletnich

Od 15 lutego 2024 r. w Polsce obowiązują nowe standardy ochrony małoletnich w hotelach. Ostateczny termin wprowadzenia ich w życie mija 15 sierpnia. Tzw. Tak zwany Lex Kamilek ma być wyrazem formalnej troski państwa o najmłodszych i ma zabezpieczać ich przed wykorzystywaniem seksualnym. Stąd nowe wymagania wobec hotelarzy – personel musi być przeszkolony i przestrzegać nowych zasad, m.in. przy zameldowaniu zidentyfikować dziecko na podstawie dokumentów oraz ustalić relację dziecka z dorosłym.

Innowacje technologiczne

To nienowy temat, technologia bowiem już od jakiegoś czasu odgrywa coraz większą rolę w zapewnianiu bezpieczeństwa w hotelach. Inteligentne systemy bezpieczeństwa, takie jak bezkluczowy dostęp do pokoi, monitoring w czasie rzeczywistym oraz zintegrowane systemy alarmowe, stają się już standardem w nowoczesnych obiektach hotelowych. Wykorzystanie technologii bezkontaktowych, takich jak zameldowanie online, również przyczynia się do zwiększenia bezpieczeństwa gości, co wielu docenia zwłaszcza po latach pandemii. Wyższy poziom zaawansowania to weryfikacja biometryczna i szyfrowanie.

Zrównoważony rozwój i bezpieczeństwo

W kontekście zrównoważonego rozwoju hotele inwestują w ekologiczne i energooszczędne rozwiązania, które nie tylko są korzystne dla

PROGNOZY

PROGNOZY KRÓTKOTERMINOWE

STABILIZACJA POZIOMU OBŁOŻENIA
Krajowy ruch turystyczny odbił się po pandemii, a poziom obłożenia jest względnie stały.

WZROST RevPAR
Odbudowa popytu i wzrost cen przekłada się na wzrost średniego przychodu z pokoju hotelowego.

TURYSTYKA ZAGRANICZNA
Polskę odwiedza więcej zagranicznych turystów niż przed pandemią, między innymi ze względu na atrakcyjny stosunek ceny do jakości obiektów.

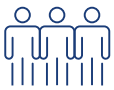
WYŻSZE KOSZTY UTRZYMANIA OBIEKTÓW
Koszty utrzymania obiektów hotelowych są coraz wyższe - mają na to wpływ głównie wyższe ceny prądu i innych mediów.

EKSPANSJA SIECI HOTELOWYCH
Baza obiektów międzynarodowych operatorów w Polsce się powiększa.

CONDOHOTELE
Rynek jest nasycony, więc podaż w tym segmencie będzie maleć (wyjątek: pas nadmorski).

PROGNOZY DŁUGOTERMINOWE

ESG
Standardy ESG wdrażane są na etapie projektowania, budowy, zarządzania oraz eksploatacji. Coraz więcej obiektów ma certyfikaty lLEED lub BREAM. Aspekty ekologiczne oraz energetyczne (popularyzacja niskoemisyjnych źródeł ogrzewania i chłodzenia) grają coraz większa rolę i przyczyniają się do zmniejszenia kosztów utrzymania budynków.



DEMOGRAFIA
Społeczeństwo się starzeje, więc obiekty hotelowe będą dostosowywać swoje oferty do potrzeb seniorów.

OBIEKT LUKSUSOWE
Postęp gospodarczy i zmiana pokoleniowa wymuszają zmianę preferencji wypoczynkowych. Zwiększy się popyt na obiekty o podwyższonym standardzie.

NOWOCZESNE TECHNOLOGIE
E-recepcja, elektroniczna karta meldunkowa czy systemy automatycznego zarządzania hotelem mogą okazać się standardem już w niedalekiej przyszłości.

Źródło: R*ynek hoteli w Polsce* - raport mBank (www.mbank.pl)

środowiska, ale także mogą poprawić bezpieczeństwo gości. Na przykład inteligentne systemy zarządzania energią mogą monitorować i kontrolować zużycie energii, co zmniejsza ryzyko awarii i pożarów.

Personalizacja i elastyczność

Personalizacja usług staje się coraz powszechniejszą praktyką w branży hotelowej. Hotele wykorzystują dane do lepszego zrozumienia i spełnienia indywidualnych potrzeb swoich klientów, dzięki czemu mogą oferować im bardziej spersonalizowane doświadczenia. Elastyczność operacyjna, w tym szybkie dostosowywanie się do zmieniających się warunków rynkowych, jest kluczowa dla utrzymania wysokich standardów bezpieczeństwa.

Wnioski

Branża security może odpowiedzieć na wiele nowych wymogów rynku, zapotrzebowanie klientów, a także starych bolączek w hotelarstwie. Zwłaszcza korzystnie zapowiada się mariaż bezpieczeństwa z technologią. Doświadczenie branży w połączeniu z możliwościami techniki mogą zapewnić hotelom szereg nowoczesnych rozwiązań, które ułatwią obsługę i zapewnią klientom komfort i bezpieczeństwo. Oprócz rozwiązań stricte produktowych warto zwrócić uwagę na inne obszary bezpieczeństwa w hotelach, które obejmują:

- Podnoszenie standardów ochrony związane z wprowadzeniem nowych procedur i przepisów, zwłaszcza dotyczących ochrony małoletnich. Tu branża security może posłużyć doradztwem w zakresie wdrożenia wymogów ustawowych i wypracowania własnych standardów opartych na przepisach prawa.
- Zrównoważony rozwój nie musi być pustosłowiem, może polegać na integracji ekologicznych rozwiązań z systemami bezpieczeństwa, np. monitorującymi zużycie wody, prądu czy gazu.
- Personalizacja usług to lepsze dostosowanie usług do indywidualnych potrzeb gości, w tym ich wymogów w zakresie bezpieczeństwa zarówno własnego, jak i mienia.

Podsumowując, przyszłość branży security w hotelarstwie będzie zależeć od zdolności do adaptacji, innowacji technologicznych oraz zrozumienia i spełnienia rosnących oczekiwań klientów w zakresie bezpieczeństwa. ●

Lepszy przycisk zamiast paniki

Gigant detaliczny Walmart jest przeciwny instalowaniu przycisków alarmowych w sklepach – elementu, który klienci w Nowym Jorku wkrótce mogą znaleźć na półkach. Przypadek Walmartu to dobry pretekst, by przyjrzeć się temu, jak w naszym kraju wygląda kwestia stosowania przycisków napadowych.

Monika Żuber-Mamakis

Na początku czerwca senat stanu Nowy Jork przegłosował ustawę wymagającą od większości dużych sieci handlowych, w tym Walmartu, umieszczenia przycisków alarmowych, tzw. *panic button*, w łatwo dostępnych miejscach oraz zapewnienia pracownikom przenośnych lub aktywowanych przez telefon komórkowy przycisków alarmowych. Miałyby one być zamontowane na stałe lub w formie przenośnej, umożliwiając wezwanie służb ratunkowych. Ta ustawa jest reakcją na rosnące zagrożenie dla pracowników handlu detalicznego ze strony klientów, a także próbą ochrony tych klientów, którzy mogliby się stać przypadkową ofiarą ataku.

Sprzeciw sieci handlowych

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 milion euro. Kolejne 202 przestępstwa dotyczyły kradzieży produktów o wartości 100 000 euro lub większej.

Gdzie jest najwięcej incydentów?

Sieci detaliczne, w tym Walmart, skrytykowały tę ustawę. Walmart argumentuje, że instalacja przycisków paniki byłaby kosztowna, a ponadto prowokowałaby wiele fałszywych alarmów. Biuro ds. Społeczności Departamentu Policji Nowego Jorku również sprzeciwia się przyciskom, twierdząc, że lepsze jest wykonanie telefonu na numer alarmowy, gdyż osoba dzwoniąca może przekazać więcej informacji. Z tym ostatnim stwierdzeniem można polemizować, gdyż sytuacja często jest dynamiczna i ofiara lub świadek może nie mieć szansy przekazania jakiejkolwiek informacji.

W Polsce jest bezpiecznie

Polska należy do najbezpieczniejszych krajów w Europie pod względem przestępczości. Według raportu Eurostatu tylko 4,4% Polaków doświadczyło aktów przemocy, przestępczości i wandalizmu, podczas gdy średnia unijna wynosi 11%. Statystyki Eurostatu wskazują, że Polska ma jeden z najniższych wskaźników przestępstw w Unii Europejskiej, tuż po Chorwacji i Litwie. Największą liczbę napadów w przeliczeniu na 100 tys. mieszkańców zanotowano w Belgii: 554 napady. Na kolejnych miejscach znalazły się: Niemcy (165), Luksemburg (101), Austria (42) i Holandia (26). Nasz kraj ma jeden z najniższych wskaźników pod tym względem – zaledwie 17 na 100 tys. mieszkańców.

» Osiem na dziesięć razy, gdy ktoś myśli, że coś się dzieje, tak naprawdę nic się nie dzieje.«

Dan Bartlett, wiceprezes wykonawczy Walmart ds. spraw korporacyjnych dla agencji Reuters

Niestety te dane pochodzą z roku 2021. Od tego czasu sytuacja się zmieniła, choć w dalszym ciągu uważamy nasz kraj za bezpieczny, a na pewno bezpieczniejszy w porównaniu z innymi państwami UE. W kwietniu 2023 r. CBOS przeprowadził badanie *Poczucie bezpieczeństwa i zagrożenia przestępczością*, z którego wynika, że „88% badanych uważa, że Polska jest krajem, w którym żyje się bezpiecznie, mniej niż co dziesiąty ma przeciwne zdanie (9%), a 3% nie ma opinii na ten temat. W stosunku do ubiegłego roku obserwujemy istotny wzrost poczucia bezpieczeństwa Polaków – o 5 punktów procentowych zwiększył się odsetek uważających Polskę za kraj bezpieczny, o 4 punkty zmalał udział będących przeciwnego zdania w tej sprawie. Aktualne oceny są bliskie tym z lat 2017 i 2019, kiedy niemal 90% badanych uważało Polskę za kraj bezpieczny. Oceny stanu bezpieczeństwa w naszym kraju od 2016 r. utrzymują się na wysokim poziomie (co najmniej 80% odpowiedzi pozytywnych)”.

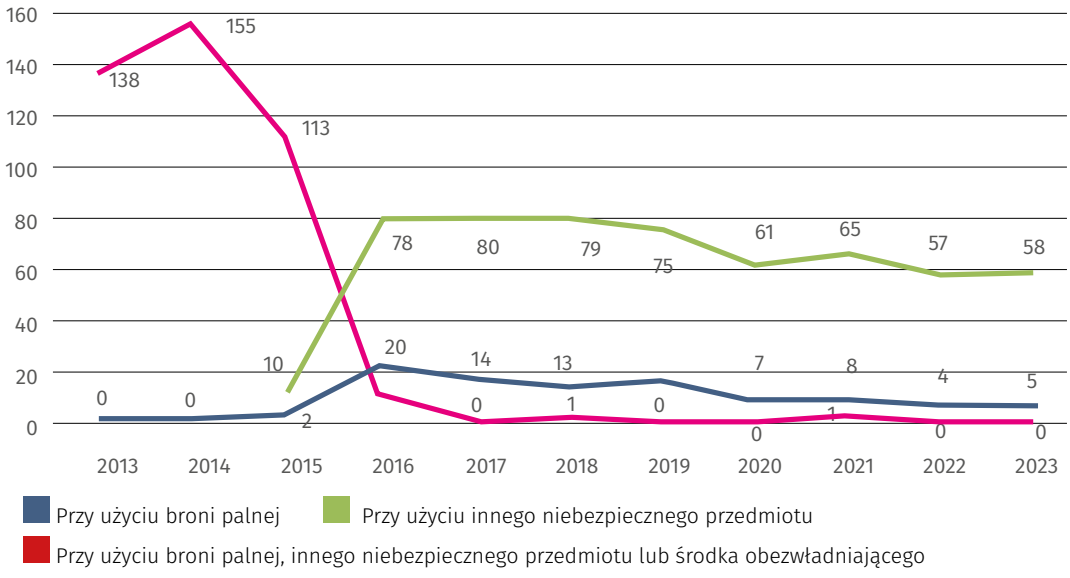
Naszego samopoczucia nie psuje fakt, że jednocześnie wg danych Komendy Głównej Policji w pierwszym półroczu 2023 r. odnotowano znaczący wzrost przestępstw kradzieży w sklepach w Polsce. Według KGP liczba przestępstw kradzieży wzrosła o 40% w porównaniu do tego samego okresu w 2022 r., osiągając prawie 24 tys. przypadków. Liczba wykroczeń związanych z kradzieżą (o wartości do 500 zł) również się zwiększyła o ok. 22%. Kradzieże dotyczą głównie żywności i produktów łatwych do szybkiej sprzedaży oraz towarów luksusowych, takich jak drogie alkohole, perfumy i elektronika (które często padają łupem zorganizowanych grup przestępczych). Są to więc kradzieże sklepowe. Kradzieże, ale nie napady, a ściśle rzecz biorąc, rozboje, bo o takim działaniu należy mówić. Rozbój zdefiniowany został w art. 280 Kodeksu karnego. Warunkiem uznania danego czynu za rozbój jest m.in. użycie przemocy. Złodzieje sklepowi, kradnący np. szynkę czy perfumy, przemocy nie używają. Nie znaczy to, że w naszym kraju nie występują napady na sklepy. Użycie tagu „napady na sklep” na stronie policja.pl, czyli pytanie o konkretne *modus operandi*, daje stosunkowo krótką listę 22 wyników. Czyżby faktycznie w Polsce do przestępstw tego typu dochodziło tak rzadko? Pewne światło rzuca na ten temat odpowiedź, jaką uzyskaliśmy na pytanie o statystyki napadów. Jak wyjaśnia Wydział Prasowo-Informacyjny Biura Komunikacji Społecznej Komendy Głównej Policji, uzyskanie precyzyjnej odpowiedzi na pytanie o liczbę napadów na sklepy jest trudne, ponieważ „wartości *modus operandi* nie są obligatoryjne przy rejestracji przestępstwa w Krajowym Systemie Informacyjnym Policji (KSIP), wobec czego liczba przestępstw stwierdzonych z uwzględnieniem jakiejkolwiek wartości *modus operandi* będzie pewną częścią stanu faktycznego poruszanego zagadnienia. Ponadto zastosowanie kryterium *modus operandi* może zniekształcić stan faktyczny ze względu na możliwość przypisania wielu wartości do jednej rejestracji przestępstwa (np. przestępstwo popełnione w mieście, w budynku mieszkalnym będzie wykazane w dwóch rubrykach)”. Mimo to uzyskaliśmy odpowiedź dotyczącą przestępstw podlegających karze z art. 280 kk. W roku 2023 było ich 63. Czy tę liczbę należy traktować w kategoriach „tylko”, czy raczej „aż”? Dane wskazują, że jednak „tylko”. Tendencja jest wyraźnie spadkowa (patrz. wykres *Przestępstwa stwierdzone, w których wystąpiły kryteria modus operandi).*

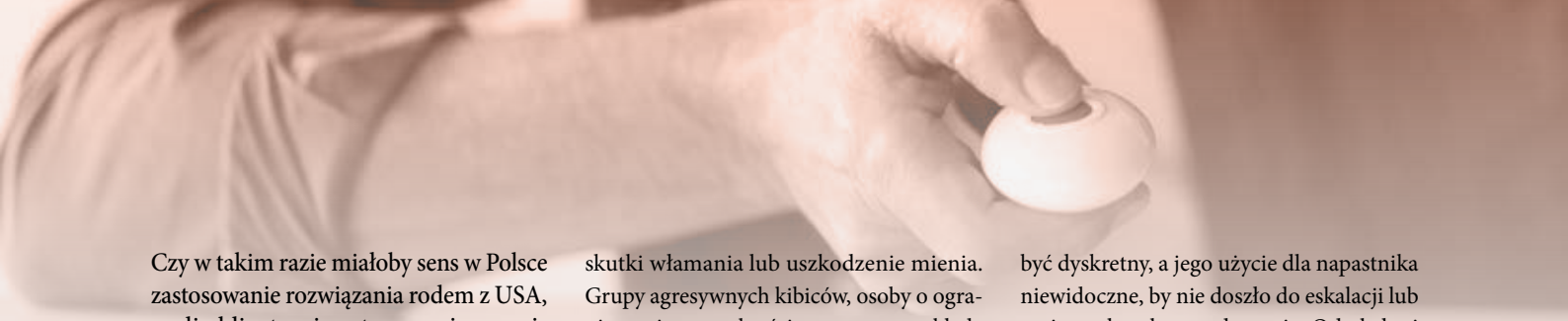
ART. 280

§ 1. Kto kradnie, używając przemocy wobec osoby lub grożąc natychmiastowym jej użyciem albo doprowadzając człowieka do stanu nieprzytomności lub bezbronności, podlega karze pozbawienia wolności od lat 2 do 12.

§ 2. Jeżeli sprawca rozboju posługuje się bronią palną, nożem lub innym podobnie niebezpiecznym przedmiotem lub środkiem obezwładniającym albo działa w inny sposób bezpośrednio zagrażający życiu lub wspólnie z inną osobą, która posługuje się taką bronią, przedmiotem, środkiem lub sposobem, podlega karze pozbawienia wolności na czas nie krótszy od lat 3.

PRZESTĘPSTWA STWIERDZONE, W KTÓRYCH WYSTĄPIŁY KRYTERIA MODUS OPERANDI





Czy w takim razie miałoby sens w Polsce zastosowanie rozwiązania rodem z USA, czyli obligatoryjne stosowanie przycisków napadowych tzw. panic button. O zdanie w tej kwestii zapytaliśmy eksperta Huberta Żaka.

Zna pan statystyki dotyczące przestępczości w Polsce, wie również, jak wygląda rynek ochrony. Czy przyciski napadowe są przydatne?
Nim odpowiem na to pytanie, przedstawię typowy scenariusz. W przypadku, w którym zaistnieje zdarzenie wyczerpujące znamiona sytuacji niebezpiecznej osoba zagrożona naciska przycisk – CMA przyjmuje zgłoszenie i weryfikuje rodzaj alarmu i jego zasadność. Jeśli alarm jest przypadkowy, zgłoszenie zostaje zamknięte. Jeśli jednak nikt nie reaguje, wysyłana jest lub zagrożenie zostanie potwierdzone zostaje wysłana załoga interwencyjna. Każda firma świadcząca tego rodzaju usługi ma załogi rozlokowane w optymalnych dla danego rejonu lokalizacjach. To nie znaczy, że taka załoga dotrze na miejsce błyskawicznie. Zazwyczaj sytuacja jest dynamiczna, więc patrol dociera post factum. Jest kilka elementów kluczowych dla tempa reakcji: liczba chronionych obiektów, wielkość obszaru, czas reakcji CMA, sytuacja na trasie. Dlatego mimo stałego procesu optymalizacji i wprowadzania szeregu coraz to nowszych rozwiązań np. planowanie alternatywnych tras dojazdu etc., nie należy oczekiwać, że załoga przyjedzie natychmiast, tuż po uruchomieniu przycisku/pilota.

Uważa pan, że przyciski nie mają sensu?
Wręcz przeciwnie. Jestem zdania, że zdecydowanie mają sens jako element podnoszący poziom bezpieczeństwa. W wielu obszarach są wręcz niezbędne. Natomiast należy pamiętać, że rzadko zdarza się, by patrol dotarł na miejsce, gdy zdarzenie trwa. W analizowanym przez nas spektrum raptem 14% zdarzeń trwało w czasie przyjazdu załogi. Na przykład napady rabunkowe i kradzieże to zdarzenia trwające od kilkudziesięciu sekund do maksymalnie kilku. To z reguły za mało czasu, by załoga dotarła na miejsce. Większość sytuacji trwających wystarczająco długo na przybycie załogi w czasie przebiegu zdarzenia to awantury, nietrzeźwi klienci, agresywne grupy, osoby bezdomne lub po wpływem substancji odurzających, skutki włamania lub uszkodzenie mienia. Grupy agresywnych kibiców, osoby o ograniczonej poczytalności to typowe przykłady i wcale nierzadkie. W takich przypadkach, ze względu na dynamikę ich przebiegu przycisk napadowy bardzo się przydaje. Osobiście uważam, i często rekomenduję, że jeden to za mało.

Jeden przycisk to za mało?
Będzie skuteczny w jakimś zakresie, ale spójrzmy na realia. Ceny usług ochrony nie należą do wyśrubowanych. Dla dużych firm, np. rozległych obiektów hotelowych, konferencyjnych albo zajmujących się wynajmem powierzchni biurowych, sieci sklepów, restauracji czy klubów, to nie są znaczące w budżecie pieniądze. Jeśli jednak rejon chroniony przez firmę ochroniarską jest rozległy, a tak bywa, to od powiadomienia załogi do jej przybycia może minąć kilka minut, czasami bezcennych. Choćby dlatego, że załoga może właśnie realizować zgłoszenie w innym rejonie, a CMA musi wysłać załogę zastępczą z innego obszaru, co wydłuża czas reakcji. Zatem jeśli jednak skorzystamy z usług dwóch albo trzech firm ochrony, a żadnych ograniczeń w tej kwestii nie ma to cóż złego może się zdarzyć? Przyjadą 3 załogi jednocześnie i bardzo dobrze. Szczególnie, kiedy okazuje się, że jeden zespół to za mało i przydałoby się wsparcie. Oczywiście nie należy tu w żadnym momencie zapominać o nadrzędnej roli służb państwowych. To policja jest właściwym ustawowo organem do realizacji zadań w obszarze bezpieczeństwa, więc w każdym momencie należy ocenić sytuację i podjąć właściwe kroki w zakresie informowania służb, jeśli jest ono zasadne.

Co w takiej sytuacji daje przycisk napadowy?
Przede wszystkim pewność, że ktoś nam pomoże. Na osoby postronne liczyć nie Jako uczestnicy zdarzenia w pierwszej kolejności powinniśmy zadbać o bezpieczeństwo nasze i osób w naszym otoczeni. Podjęcie działań może jednak wiązać się z bezpośrednim ryzykiem oraz eskalacją zagrożenia, które ciężko nam będzie zahamować. Tu oczywiście kłaniają się procedury, które powinny iść w parze z wyposażeniem w system napadowy. Szkolenie obsługi w zakresie działania i odpowiednich algorytmów postępowania w konkretnych sytuacjach. Dobrze wiemy, że ludzie szybciej zareagują na okrzyk „Pali się!" niż na wołanie o pomoc. Przycisk powinien być dyskretny, a jego użycie dla napastnika niewidoczne, by nie doszło do eskalacji lub zmiany charakteru zdarzenia. Od obsługi nie oczekujemy bohaterstwa, tylko zdrowego rozsądku i działania według procedur. Przycisk to nie wszystko, absolutnie niezbędne jest szkolenie w zakresie użycia, działania i zachowania.

Czy coś się zmieniło w ostatnich latach, jeśli chodzi o przestępczość? Według CBOS jesteśmy przekonani, że żyjemy w kraju bezpiecznym.
Takie mamy wrażenie i na to też wskazują statystyki, ale... zawsze jest jakieś „ale". Po pierwsze, i to nie jest moje spostrzeżenie, a kwestia ogólnodostępnych danych. Obserwujemy duży wzrost liczby kradzieży sklepowych, agresywnych zachowań oraz przestępczości chuligańskiej czy kradzieży i uszkodzenia mienia. Jest to o tyle martwiące, że może prowadzić do eskalacji przemocy. W obliczu zagrożenia ludzie reagują różnie – strachem, paniką, ale także agresją. Przycisk napadowy może być tym narzędziem, które pozwoli uniknąć rozwoju sytuacji w złą stronę. Dlatego uważam, że z przyciskiem napadowym i z umową na taki zakres i usługę, jest jak z ubezpieczeniem. Lepiej mieć niż nie mieć. Poza tym jest jeszcze jeden ważny aspekt, który rzadko jest brany pod uwagę, w kontekście tzw. *panic button.*

Czyli?
Po polsku mówimy o przyciskach napadowych, w języku angielskim są to *panic button,* czyli gdybyśmy tłumaczyli wprost „przyciski paniki". Nie zawsze przecież mamy do czynienia z napadem, awanturą czy kradzieżą. Czasem klient traci przytomność, dostaje udaru lub potyka się i przewraca. Jedni ludzie są opanowani i radzą sobie ze stresem, potrafią zadzwonić na służby alarmowe i z sensem opowiedzieć, co się dzieje. Tymczasem są takie osoby, które z trudem nacisną przycisk, tu rola załogi może okazać się bezcenna. Gdyby go nie było…

…**byłoby źl**e?
No właśnie. Lepiej zatem wyposażyć się w taki system niż ryzykować jego brak. Nie jestem jednak przekonany, że należy takie rozwiązanie wprowadzać na mocy ustawy – raczej kampanii reklamowych i społecznych, zwiększających wiedzę o takiego rozwiązania. Na szczęście nie mieszkamy w Stanach Zjednoczonych. •

głos branży

W najbliższym czasie czeka nas sporo wyzwań. Spełnienie wymagań dyrektywy NIS 2, dostosowanie systemów zabezpieczeń do pojawiających się nowych zagrożeń, zwłaszcza tych cybernetycznych, spędza dziś sen z powiek nie tylko menedżerom security. Jak zadbać o odpowiedni poziom bezpieczeństwa w takich obiektach, jak hotele, banki czy biurowce, radzą eksperci branży.

Bogumił Szymanek
AXIS COMMUNICATIONS

Spełnienie wymagań Dyrektywy NIS2

Dyrektywa NIS2, mająca na celu wzmocnienie bezpieczeństwa sieci i systemów informatycznych w UE, kładzie szczególny nacisk na ochronę infrastruktury krytycznej. Axis oferuje zaawansowane rozwiązania dostosowane do spełnienia wymagań tej dyrektywy.

Infrastruktura krytyczna, obejmująca takie sektory, jak energetyka, transport, zdrowie i finanse, wymaga ciągłej ochrony przed cyberzagrożeniami i naruszeniami fizycznymi. Nasza firma dostarcza systemy dozoru wizyjnego, które nie tylko monitorują i zabezpieczają obiekty, ale także umożliwiają wczesne wykrywanie anomalii i potencjalnych zagrożeń. Kamery wyposażone w zaawansowane funkcje analityczne mogą identyfikować podejrzane zachowania i monitorować procesy, co jest kluczowe w utrzymaniu bezpieczeństwa operacyjnego.

W kontekście dyrektywy NIS2 wymagającej od organizacji przeprowadzania regularnych ocen ryzyka i wdrażania planów reakcji na incydenty takie rozwiązania są nieocenione. Nasza oferta obejmuje zarówno urządzenia, jak i kompleksową dokumentację oraz przejrzystość w kwestiach stosowanych komponentów i łańcucha dostaw. Takie elementy pomagają organizacjom w spełnieniu wymogów regulacyjnych.

Piotr Rogalewski
HIKVISION

Zarządzanie bezpieczeństwem

W przededniu implementacji dyrektywy NIS2 nowelizacją Ustawy o Krajowym Systemie Cyberbezpieczeństwa podmioty sklasyfikowane jako ważne i kluczowe mają mnóstwo pracy, szczególnie jeśli do tej pory nie traktowały z należytą uwagą wdrażania i rozwijania w swoich organizacjach kompleksowych strategii bezpieczeństwa. Ale NIS2 i wszystko, co się z wdrożeniem tej dyrektywy wiąże, to nie tylko zagadnienia obejmujące obiekty infrastruktury krytycznej czy dostawców kluczowych usług cyfrowych. Dobra strategia bezpieczeństwa, poparta sprawdzonymi w praktyce procedurami i konkretnymi wnioskami dla wszystkich szczebli zarządzania, w dzisiejszej rzeczywistości powinna stanowić elementarz dla wszystkich podmiotów – także tych, których rola w codziennym funkcjonowaniu państwa i społeczeństwa wydaje się mniej istotna niż podmiotów kluczowych i ważnych.

Dla codziennego życia statystycznego obywatela dostępność usług kosmetycznych czy noclegowych może być bowiem równie istotna jak możliwość zatankowania auta. Można to było wielokrotnie obserwować w czasie pandemii COVID-19. Kompleksowa strategia bezpieczeństwa to także doskonała podstawa do zapewnienia organizacji czegoś, co określa się angielskim słowem resilience. Często tłumaczy się je po prostu jako odporność, jednak resilience to także elastyczność, sprężystość, żywotność. Ta wieloznaczność doskonale opisuje to, jak powinna funkcjonować organizacja w warunkach współczesnych, wielowymiarowych zagrożeń. Bo chodzi tu nie tylko o zdolność ich eliminacji czy minimalizacji (na tyle, na ile to realnie możliwe), ale także o gotowość (czujność) i wiedzę, jak postępować w przypadku ewentualnych incydentów, jak sobie radzić z potencjalnymi problemami z dostępem do danych, utrzymaniem ich integralności i poufności czy wreszcie, jak zbudować zdolność właściwego zachowania się w przypadku bezpośredniego zagrożenia fizycznego w postaci klęski żywiołowej, napadu, ataku terrorystycznego czy nawet konfliktu zbrojnego.

Szeroko rozumiane bezpieczeństwo to najczęściej poważna inwestycja nie tylko w sprzęt i systemy ochrony technicznej, ale także we wdrożenie mechanizmów zarządzania bezpieczeństwem na poziomie organizacji (np. ISO27001) czy kompleksowe szkolenia pracowników i budowanie ich świadomości na wszystkich szczeblach. Trzeba sobie jednak jasno powiedzieć, że w obecnej rzeczywistości alternatywy dla takich inwestycji po prostu nie ma.

Krzysztof Bartuszek
SECURITAS POLSKA

Wspólny mianownik zagrożeń

Hotele, banki i biura to obiekty, które łączy wspólny mianownik w zakresie zagrożeń. Są to przede wszystkim zagrożenia pożarowe, kradzieże i wandalizm, choć ich charakter różni się w zależności od typu obiektu.

W hotelach kradzieże są często związane z pracownikami, choć nieuczciwi klienci również mogą powodować straty, które są zazwyczaj wkalkulowane w koszty prowadzenia działalności. Hotele są miejscem organizacji różnych wydarzeń i imprez, co czasami prowadzi do aktów wandalizmu. Ponadto, ze względu na dużą rotację gości, mogą tam wystąpić przypadki przemocy, sutenerstwa, a nawet gwałtów. Dlatego niektóre hotele w celu zwiększenia bezpieczeństwa wprowadzają piętra wyłącznie dla kobiet. Renomowane hotele szczególnie dbają o bezpieczeństwo, aby zapewnić powroty zadowolonych gości. W bankach wirtualny pieniądz zredukował ryzyko napadów, uwypuklając jednocześnie inne formy kradzieży, w tym fraudy pracownicze,

→

które stanowią główne zagrożenie. Klienci banków również mogą być źródłem ryzyka, od oszustw po konflikty w oddziałach. Z kolei przedsionki bankomatowe często są miejscami aktów wandalizmu. Skimming w bankomatach nie pozostaje bez znaczenia. Warto pamiętać, że banki coraz częściej funkcjonują jak biura, gdzie ryzyko wycieków danych osobowych i informacji o klientach jest istotnym zagrożeniem.

Biura są stosunkowo bezpiecznymi miejscami, zwłaszcza tam, gdzie procedury, szkolenia i kontrola dostępu są na wysokim poziomie. Niemniej kradzieże biurowe są powszechne, zarówno wewnętrzne (np. „pożyczanie" materiałów biurowych), jak i zewnętrzne (kradzież laptopów i sprzętu). Wandale mogą również zniszczyć mienie, wyrządzić szkody parkingowe, zdewastować toalety czy wykonać graffiti.

Współczesne zabezpieczenia techniczne odgrywają kluczową rolę w zapewnianiu bezpieczeństwa obiektów. Systemy nie tylko obejmują kontrolę dostępu, ale także umożliwiają efektywne zarządzanie obiektami i generowanie oszczędności. Przykładowo, bezobsługowe hotele pozwalają gościom na rezerwację i dostęp do pokoi za pomocą kodów QR otrzymanych online. W biurach systemy zarządzają przydziałem miejsc parkingowych, automatycznym otwieraniem szlabanów, kontrolą wind i powiadomieniami o przybyciu gości.

Banki korzystają z rozbudowanych systemów kamer z zaawansowaną analityką umożliwiającą szybkie reagowanie na niepożądane działania, np. wandalizm w przedsionkach bankomatów. Zliczanie osób w budynku jest podstawową funkcją systemów bezpieczeństwa wykorzystywaną do celów ewakuacyjnych.

Możliwości stosowania systemów zabezpieczeń technicznych są ogromne. Przy odpowiednim zaplanowaniu mogą one znacząco ograniczyć, a w niektórych przypadkach nawet wyeliminować potrzebę interwencji ludzkiej, bez uszczerbku dla bezpieczeństwa. W przyszłości sztuczna inteligencja jeszcze bardziej zwiększy efektywność tych systemów – zresztą wiele z tych rozwiązań jest już dostępnych i stosowanych.

Krzysztof Łęcki
TAURUS OCHRONA GROUP, PIO

Skuteczna ochrona obiektu

Hotele, banki i biurowce są obecnie narażone na coraz częstsze zagrożenia, m.in. włamania, kradzieże, wandalizm, sabotaż oraz ryzyko ataków terrorystycznych i zagrożeń pożarowych. Jednak każdy obiekt ma specyficzne potrzeby, dlatego nasze podejście do ochrony musi być dostosowywane indywidualnie.

W hotelach priorytetem jest bezpieczeństwo gości i ochrona ich mienia, ponieważ często dochodzi do kradzieży w pokojach hotelowych czy samochodów na parkingach. Istnieje także ryzyko dostępu osób nieuprawnionych do stref zastrzeżonych, takich jak zaplecza kuchenne czy magazyny. W bankach głównym wyzwaniem jest ochrona wartości pieniężnych, danych osobowych klientów, a także zapewnienie bezpieczeństwa fizycznego osobom przebywającym w miejscu napadu lub kradzieży. Włamania do bankomatów i ataki cybernetyczne są również częste. W biurowcach koncentrujemy się na ochronie osób przebywających w budynku, zapewniając skuteczną ewakuację, kontrolę dostępu do stref szczególnie chronionych oraz zapobieganie kradzieży i niszczeniu mienia.

Nowoczesne technologie znacznie zwiększają efektywność działań firm ochrony, jednocześnie obniżając koszty. Dzięki nim pracownicy ochrony mogą skupić się na działaniach i udzielaniu informacji klientom, gościom oraz odpowiednim służbom zamiast na monitorowaniu sygnałów i zdarzeń.

Systemy monitoringu wizyjnego, kontroli dostępu i sygnalizacji włamania z czujkami ruchu są kluczowymi narzędziami w naszej codziennej pracy. Systemy połączone w jeden zintegrowany system zarządzania budynkiem dostarczają istotnych informacji, na które pracownicy ochrony muszą natychmiast reagować. Skorelowanie różnych sygnałów umożliwia planowanie działań i tworzenie scenariuszy postępowań w sytuacjach krytycznych, co jest nieocenione dla pracowników ochrony i personelu.

Behawioralna analiza obrazu oparta na sztucznej inteligencji pozwala na rejestrowanie zdarzeń, przewidywanie i szybkie reagowanie na potencjalne zagrożenia. AI skutecznie rozpoznaje podejrzane zachowania i identyfikuje osoby, co jest szczególnie przydatne w hotelach, bankach i biurowcach.

Rozwój nowoczesnych technologii jest kluczowy dla zapewnienia bezpieczeństwa, zwłaszcza w kontekście rosnących zagrożeń sabotażowych i terrorystycznych. Inwestowanie w te technologie nie tylko zwiększa bezpieczeństwo klientów, ale także buduje zaufanie. Warto pamiętać, że efektywność systemów zależy też od umiejętności i regularnego szkolenia pracowników zarówno w obszarze zaawansowanych systemów zabezpieczeń, jak i w zakresie procedur reagowania na awarie i sytuacje kryzysowe. Integracja wiedzy i doświadczenia z nowoczesnymi technologiami jest kluczem do skutecznej ochrony każdego obiektu.

Karol Marcinkowski
MBANK SA

Zapobieganie incydentom w placówkach bankowych

Rozwój i coraz większa dostępność technologii powodują nieustanną zmianę rodzajów zagrożeń. Obserwujemy spadek przestępczości w placówkach, przestępcy już dawno przenieśli swoje działania do sieci, wykorzystując nowe metody oszustw i manipulacji. Banki aktywnie walczą z wszelkimi formami przestępstw, wprowadzając nowe metody zabezpieczeń swoich serwisów i aplikacji oraz zaawansowane systemy detekcji wspierane przez AI.

Choć klasyczne napady odeszły już do lamusa, nie możemy jednak wykluczyć incydentów fizycznych w placówkach. W ostatnich latach wzrasta liczba zdarzeń powodowanych przez agresywnych klientów. Groźby wobec pracowników, nękanie i roszczeniowość lub nagrywanie smartfonem w celu publikacji w mediach społecznościowych stają się codziennością w sklepach, bankach, a nawet urzędach. Takich przykładów zdarzeń jest znacznie więcej, a jak wszyscy wiemy, od agresywnego zachowania do incydentów zagrażających bezpieczeństwu pracowników i klientów jest tylko krok.

W zapewnieniu odpowiedniego poziomu bezpieczeństwa ważną funkcję pełnią rozwiązania wykorzystujące nowe technologie. Niestety nie idą z nimi w parze obowiązujące przepisy, które nie są dostosowane do realiów. Dodatkowo ograniczone uprawnienia do podejmowania działań przez pracowników ochrony wykorzystują „trudni klienci", którzy dobrze wiedzą, co mogą, a czego nie mogą pracownicy ochrony czy służby.

Kolejnym rodzajem zagrożeń są celowe prowokacje, które można nazwać „testowaniem możliwości obsługi klienta" w placówce. W niektórych regionach funkcjonują grupy, których członkowie regularnie pojawiają się w bankach, próbując na podstawie różnorodnych dokumentów otwierać rachunki lub dokonywać transakcji pieniężnych. Minimalizowanie ryzyka i zapobieganie takim zdarzeniom to w znaczącej mierze przeprowadzanie wyspecjalizowanych szkoleń dla pracowników oddziałów banku, budowanie świadomości bezpieczeństwa w całej organizacji oraz odpowiednich kampanii informacyjnych kierowanych do klientów.

Marcin Walczuk
BCS

Bezpieczny hotel

Z uwagi na specyfikę działalności stale rozwijająca się branża hotelarska szczególną uwagę musi zwracać na zapewnienie najwyższego poziomu bezpieczeństwa gościom. Osoby korzystające z usług hotelu, poza wygodą, chcą czuć się pewnie i bezpiecznie. Stąd w hotelach montowane są najwyższej klasy systemy zabezpieczeń, począwszy od systemów kontroli dostępu do pokojów gościnnych, systemów przeciwpożarowych, alarmowych oraz telewizji dozorowej.

BCS w swojej ofercie ma pełną gamę urządzeń, które idealnie sprawdzą się w zabezpieczaniu nawet największych tego typu obiektów. Rejestratory nawet 128-kanałowe pozwolą na monitorowanie średnich hoteli. Za pomocą aplikacji BCS Manager można połączyć więcej tego typu urządzeń i całość systemu obsługiwać z poziomu jednej stacji roboczej. W takim przypadku ograniczeniem będzie tylko moc wspomnianej stacji potrzebna do wyświetlenia odpowiedniej liczby kanałów. Doskonałą jakość obrazu zapewnią kamery o rozdzielczości nawet do 12 Mpix.

Proponujemy rozwiązania, które spełnią oczekiwania najbardziej wymagających klientów. Kamery specjalnego przeznaczenia, np. do rozpoznawania i identyfikacji twarzy, pozwolą na porównanie osób przebywających na terenie hotelu z bazą danych gości i wychwytywanie osób niepożądanych. Kamery do liczenia ludzi pomogą sprawdzić, czy liczba osób w hotelu odpowiada liczbie osób w nim zameldowanych lub w razie ewakuacji, czy wszystkie osoby opuściły budynek. Kamery BCS AI z zaimplementowanym algorytmem sztucznej inteligencji umożliwią natychmiastową reakcję na takie zdarzenia, np. przekroczenie linii, wtargnięcie czy zbyt długie przebywanie w strefie, monitorowanie pozostawionych lub skradzionych przedmiotów. Przy monitorowaniu parkingów nieodzowna będzie kamera do rozpoznawania tablic rejestracyjnych, która w połączeniu z BCS Managerem pozwoli w łatwy sposób monitorować i przyznawać dostęp autom o właściwych numerach rejestracyjnych.

Paweł Korzybski
POLSKI ZWIĄZEK PRACODAWCÓW OCHRONA

Bezpieczeństwo jest najważniejsze

Najczęstsze zagrożenia, z jakimi spotykają się pracownicy ochrony w obiektach hotelowych, dotyczą interwencji wobec osób będących pod wpływem alkoholu czy środków odurzających, które swoim agresywnym zachowaniem zagrażają personelowi oraz gościom hotelu. Kolejną kategorią zagrożeń są czynności związane z interwencjami w ramach naruszenia systemów ppoż., aktywowanych poprzez zbicie ROP-a (Ręcznego Ostrzegacza Pożarowego) lub powstaniem fizycznego zagrożenia pożarowego bądź zalaniem chronionych powierzchni. Nie zapominajmy również o aktywnym uczestniczeniu w akcjach ewakuacyjnych na chronionym obiekcie.

Jedne z najnowszych zagrożeń występujących w obiektach hotelowych, biurowych czy bankowych, tam, gdzie dana lokalizacja dysponuje własnym parkingiem (w tym podziemnym), jest możliwość wystąpienia samozapłonu samochodów elektrycznych podczas ich ładowania, postoju bądź kolizji na parkingu podziemnym. Niedawny incydent to niekontrolowane uderzenie auta w pojazdy w strefie ładowania aut elektrycznych, w wyniku czego stacja ładowania została wyrwana z podłoża, powodując realne zagrożenie pożarowe i ewentualne źródło rażenia prądem osób postronnych. Pracownik ochrony, który podejmuje interwencję, w pierwszej kolejności musi zadbać o bezpieczeństwo swoje oraz osób postronnych, zabezpieczyć miejsce zdarzenia oraz współpracować ze służbami (w tym przypadku ze strażą pożarną i z policją). Następnie opracowuje stosowną dokumentację i zabezpiecza materiał CCTV.

Zagrożeniem najwyższej skali w przypadku obiektów bankowych są próby napadu z użyciem niebezpiecznego narzędzia czy broni oraz ewentualne wzięcie zakładników. W lutym tego roku we Wrocławiu pracownik ochrony jednej z firm zrzeszonych w PZP Ochrona skutecznie udaremnił próbę takiego napadu z bronią w ręku, obezwładnił napastnika i przekazał go policji.

Osobna kategoria zagrożeń to zagrożenia związane z transportowaniem gotówki i bezpośrednią próbą napadu na konwojentów. By skutecznie przeciwdziałać takim incydentom, profesjonalne firmy z rynku ochrony osób i mienia mają do dyspozycji cały arsenał nowoczesnych zabezpieczeń elektronicznych. Począwszy od systemów kamer, środków łączności, pilotów napadowych, dzięki którym pracownik ochrony i banku może wezwać wsparcie (grupę interwencyjną oraz policję), systemy GPS, walizki transportowe zawierające ładunki uwalniające niezmywalny materiał barwiący złodzieja lub pieniądze czy urządzenia unieruchamiające zdalnie pojazdy wykorzystywane do transportu wartości pieniężnych.

Elektroniczne systemy zabezpieczeń są dziś nieodzownym elementem skutecznego systemu ochrony, który wspomaga pracę i realne działania pracowników służby ochrony. Umożliwiają one m.in. preselekcję zdarzeń, ustalanie, czy mają one charakter incydentalny, czy powtarzalny. Pozwalają rejestrować, raportować zdarzenia z konkretnych check pointów, ze szczególnym wskazaniem stref, których one dotyczą. Dane zbierane przez systemy sygnalizacji włamania i napadu, telewizji dozorowej, kontroli dostępu stanowią materiał dowodowy w sprawach związanych z konkretnymi interwencjami.

Wywołane alarmy związane z naruszeniami systemów ppoż. czy SSWiN, wsparte nowoczesnymi systemami monitoringu wizyjnego pozwalają na szybsze przeprowadzenie weryfikacji ich powstania i jednocześnie podejmowanie skutecznego działania zmierzającego do ograniczania ewentualnych strat. Narzędziem, które stało się w zasadzie nowoczesnym *must have,* jest analityka obrazu, która w ostatnich latach w znaczący sposób ewoluowała i jest dziś nieodzownym wsparciem. Kolejnym elementem nowoczesnych rozwiązań stosowanych w skutecznych systemach ochrony są kamery termowizyjne. To one pozwalają na skuteczne monitorowanie zmian temperatury, np. w strefie klimatyzatorów zewnętrznych czy śmietnikach zlokalizowanych blisko budynku, do których niestety mogą mieć łatwy dostęp osoby postronne i szybko wywołać ich pożar. To dzięki wspomnianym rozwiązaniom można skutecznie zabezpieczyć się przed incydentami lub zdarzeniami losowymi, które prowadzą do zagrożenia kradzieży lub pożaru.

Systemy elektroniczne mogą także alarmować o blokowaniu dróg ewakuacyjnych, wspomagać wykrywanie dymu, rozpoznawać twarz osób wchodzących na teren chronionego obiektu, dokonywać automatycznego odczytu tablic rejestracyjnych – wszystko to znacznie wspomaga naszą pracę, podnosi również poziom realizowanych usług. Nowoczesne systemy elektroniczne pozwalają także ograniczyć koszty związane z czynnikiem ludzkim.

Piotr Matuszewski
ELA-COMPIL

Pożary w Polsce – wzmocnienia systemów ochrony przeciwpożarowej

Polska w ostatnim czasie zmaga się z serią pożarów hal magazynowych i produkcyjnych, które wywołały zaniepokojenie i spekulacje o możliwych przyczynach tych zdarzeń. Do głośniejszych incydentów należy pożar w firmie Aksam, produkującej „Paluszki Beskidzkie".

Chociaż dane Komendy Głównej Państwowej Straży Pożarnej wskazują, że liczba takich pożarów nie wzrosła znacząco w porównaniu do lat poprzednich, a nawet spadła, to politycy i eksperci

zwracają uwagę na potencjalne zagrożenie, jakim może być działalność dywersyjna obcych służb, co sugeruje możliwość działań w ramach wojny hybrydowej. Od 1 stycznia do 15 lipca 2024 r. ogólna liczba pożarów obiektów produkcyjnych i magazynowych sięgnęła 51; 32 z nich straż pożarna zakwalifikowała jako duże pożary, a 19 jako bardzo duże.

Pożary w zakładach przemysłowych i magazynach generują ogromne straty materialne, często sięgające kilku milionów złotych. Stanowią one 1% wszystkich pożarów, ale odpowiadają za 22% strat. Kluczowym elementem w minimalizowaniu strat jest szybka reakcja na pożar. Choć nie zawsze przepisy tego wymagają, to w celu zminimalizowania ryzyka powstania pożaru i szybkiego ugaszenia jego zarzewia obiekty tego typu powinny być wyposażone w systemy wykrywania pożaru oraz stałe urządzenia gaśnicze (SUG), takie jak tryskacze czy zraszacze, które umożliwiają szybkie rozpoczęcie akcji gaśniczej.

Przepisy dotyczące ochrony przeciwpożarowej koncentrują się głównie na ochronie życia, ale ubezpieczyciele często wymagają instalacji zaawansowanych systemów gaśniczych. Inwestorzy powinni znać te wymagania i uwzględniać je w planowaniu inwestycji. Ważne są również regularne przeglądy i konserwacja systemów ochrony przeciwpożarowej, aby zapewnić ich skuteczność w przypadku wykrycia i rozwoju pożaru.

Obecność SUG może znacznie obniżyć straty materialne powstałe w wyniku pożaru. Przykład z Koźmina Wielkopolskiego, gdzie brak systemu gaśniczego doprowadził do dużych strat, podkreśla konieczność ich instalacji. Zakłady wyposażone w SUG mają większe szanse na skuteczne opanowanie pożaru, co jest kluczowe dla ochrony życia i mienia. Ważnym aspektem jest także edukacja pracowników w zakresie procedur przeciwpożarowych i ewakuacyjnych.

Ostatnie pożary hal przemysłowych w Polsce podkreślają potrzebę wzmocnienia systemów ochrony przeciwpożarowej. Inwestycje w odpowiednie systemy gaśnicze są kluczowe dla bezpieczeństwa pracowników i minimalizacji strat materialnych, a także dla zapewnienia ciągłości działania przedsiębiorstwa. Wprowadzenie i utrzymanie wysokich standardów ochrony przeciwpożarowej powinno być priorytetem dla wszystkich zakładów przemysłowych. ●

Wszystko o bezpieczeństwie pożarowym

Firma Schrack Seconet Polska, światowy producent zaawansowanych technologicznie systemów bezpieczeństwa pożarowego, we współpracy z innymi liderami branży bezpieczeństwa (w tym roku 11 Partnerów technologicznych!) oraz ekspertami reprezentującymi najbardziej opiniotwórcze instytuty w kraju, organizuje już XI edycję Ogólnopolskich Dni Zintegrowanych Systemów Bezpieczeństwa Pożarowego – Schrack Seconet i Partnerzy. Tegoroczne spotkanie odbędzie się 9–10 października 2024 r. w hotelu Windsor w Jachrance.

Tegoroczna edycja pozostanie w formule merytorycznych spotkań. Uczestnicy Ogólnopolskich Dni Zintegrowanych Systemów Bezpieczeństwa Pożarowego – Schrack Seconet i Partnerzy zapoznają się ze wszystkimi produktowymi nowościami, z aktualnymi wytycznymi i dobrymi praktykami w zakresie projektowania, realizacji i eksploatacji systemów bezpieczeństwa. Podobnie jak w latach poprzednich nie zabraknie szczegółowo omówionego współdziałania systemów bezpieczeństwa i instalacji technicznych w przypadku różnych typów zagrożeń w obiektach budowlanych. Zostaną przeanalizowane studia przypadków przedstawiające dokładne zalecenia dla projektantów, instalatorów, inwestorów i użytkowników w zakresie integracji systemów bezpieczeństwa. Zespoły ekspertów dokonają analizy przypadków zastosowania urządzeń służących ochronie zdrowia, życia i mienia (w tym procesów technologicznych) w obiektach różnego przeznaczenia. Szczegółowa analiza studiów przypadków zostanie zaprezentowana podczas pokazu zadziałania zintegrowanych ze sobą różnych systemów bezpieczeństwa. Do grona specjalistów dołączą w tym roku kolejni eksperci z zakresu bezpieczeństwa pożarowego, ochrony osób i mienia oraz ubezpieczycieli. W drugiej połowie każdego dnia szkolenia uczestnicy będą mogli wziąć udział w sesjach warsztatowych poszczególnych Partnerów technologicznych i merytorycznych.

Podczas dwóch dni słuchacze zapoznają się z najnowszymi wytycznymi dotyczącymi projektowania, instalacji oraz użytkowania takich systemów jak sygnalizacji pożarowej, sterowania gaszeniem, DSO, kontroli rozprzestrzeniania dymu i ciepła, integracji urządzeń przeciwpożarowych (SIUP), sterowania urządzeniami przeciwpożarowymi i innymi instalacjami użytkowymi obiektu, dozoru wizyjnego, kontroli dostępu, okablowania strukturalnego i przemysłowych rozwiązań infrastruktury sieciowej. Zostaną poruszone m.in. takie zagadnienia jak:

- zasady wdrażania zintegrowanego systemu bezpieczeństwa pożarowego i zarządzanie procedurą ewakuacji z poziomu SIUP;
- współdziałanie systemów bezpieczeństwa pożarowego w zakresie ochrony przeciwpożarowej instalacji fotowoltaicznej i magazynów energii;
- zasady integracji podstawowej i rozszerzonej systemów bezpieczeństwa pożarowego oraz systemów Security (SKD, CCTV/VSS);
- specjalne rozwiązania detekcji pożaru (wczesna detekcja dymu, płomienia, ciepła);
- systemy detekcji pożaru z wykorzystaniem kamer termowizyjnych radiometrycznych;
- dźwiękowy system ostrzegawczy – współdziałanie z SIUP i trudne przypadki projektowe;
- zintegrowane systemy detekcji i sterowania gaszeniem – gaszenie jedno- i wielostrefowe;
- systemy i urządzenia gaśnicze gazowe i na mgłę wodną;
- systemy gaszenia lokalnego;
- sterowanie urządzeniami automatyki pożarowej i zasilanie ich;
- systemy sterowania i układy zasilania zapewniające ciągłość działania krytycznych procesów i systemów;
- rozwiązania w systemach okablowania strukturalnego i przemysłowej infrastrukturze sieciowej;
- współdziałanie systemów security podczas bieżącej eksploatacji oraz różnych typów zagrożeń w obiekcie budowlanym;
- przypadki specjalnych zastosowań systemów bezpieczeństwa.

Współorganizatorami tego największego w branży przedsięwzięcia edukacyjnego będą następujący producenci i dystrybutorzy:

BELIMO Siłowniki – światowy lider w dziedzinie opracowywania, produkcji i sprzedaży urządzeń do energooszczędnych instalacji grzewczych, wentylacji i klimatyzacji. Firma powstała w 1975 r. w Szwajcarii, obecnie zatrudnia ok. 2000 osób w 80 krajach, oferuje m.in. siłowniki do przepustnic powietrza i klap ppoż., zawory regulacyjne, czujniki oraz liczniki energii termicznej.

DALLMEIER electronic – od 1984 r. pionier w dziedzinie najnowocześniejszych rozwiązań CCTV/IP, w tym inteligentne oprogramowanie zarządzające oraz wysokiej jakości technologia nagrywania materiałów wizyjnych z kamer. Klientami firmy są największe kasyna, lotniska, miasta i stadiony świata, a także setki małych i średnich przedsiębiorstw oraz organizacji każdej wielkości.

DCNART – działania firmy są odpowiedzią na potrzeby wielu organizacji, które oczekują profesjonalnego wsparcia na wszystkich etapach budowania swojej infrastruktury IT. Jej głównym celem jest podnoszenie świadomości na temat rozwiązań sieciowych w Polsce i podkreślanie, jak krytycznym elementem dla poprawnej eksploatacji

i długoletniego poprawnego działania jest odpowiednie przygotowanie infrastruktury fizycznej.

DEKK Fire Solutions – głównym celem działalności firmy jest wdrażanie najskuteczniejszych zabezpieczeń pożarowych, w tym instalacji tryskaczowych, instalacji gaszenia gazem, systemów sygnalizacji pożarowej, systemów zasysających oraz innych zabezpieczeń ppoż. Firma uruchomiła zakład prefabrykacji rurociągów z malarnią proszkową. We współpracy z wiodącymi producentami i dystrybutorami urządzeń przeciwpożarowych utrzymuje wysoki standard usług.

Fire & Gas Detection Technologies Inc. (FGD) – firma dostarcza innowacyjne rozwiązania w zakresie wykrywania i analizy płomieni, które zapewniają najwyższy poziom bezpieczeństwa w obiektach zarówno przemysłowych, jak i komercyjnych. Urządzenia FlameSpec są wykorzystywane m.in. do wykrywania pożarów wodorowych przy zachowaniu bardzo wysokiej odporności na fałszywe alarmy (IR3), jak również obszary z występującymi wyładowaniami łukowymi (UV/IR).

FRONIUS Polska – Fronius Solar Energy od 30 lat oferuje nowatorskie produkty, rozwiązania i narzędzia cyfrowe służące do rentownego i inteligentnego generowania, przechowywania, dystrybuowania i zużywania energii słonecznej. Nazwa firmy jest synonimem innowacji, które wpływają na działania konsumentów prywatnych i firm do korzystania z energii słonecznej zgodnie z filozofią zrównoważonego rozwoju i hasłem Energize your life.

INSTAC – zajmuje się bezpieczeństwem pożarowym od 25 lat, lider rynku wysokociśnieniowej mgły wodnej, wykonawca klasycznych systemów tryskaczowych i prefabrykowanych rurociągów. Firma działa kompleksowo – od projektu, przez kompletację i montaż, po uruchomienie i serwis obiektu. Jej misją jest ochrona ludzi, mienia i ciągłości biznesowej klientów.

Nedap Security Management – światowy lider w dziedzinie systemów kontroli dostępu. Oferuje Nedap AEOS, innowacyjny i skalowalny system kontroli dostępu spełniający najwyższe wymagania bezpieczeństwa, co potwierdza grade 4 wg europejskiej normy EN60839. AEOS to także certyfikowany (grade 3) system sygnalizacji włamania i napadu oraz szafki depozytowe. Do unikalnych cech systemu należy skalowalność (brak limitu użytkowników) oraz otwartość na integracje z innymi systemami bezpieczeństwa (windy, SAP, CCTV).

PANDUIT – lider w dziedzinie produktów i usług. W roku 1955 wprowadził na rynek pierwszy produkt pod nazwą Panduct Wiring Duct, który w unikalny sposób organizował okablowanie w panelach sterowania oraz umożliwiał szybkie i sprawne dodawanie nowych przewodów. Firma nadal jest zaangażowana w dostarczanie innowacyjnych rozwiązań w zakresie infrastruktury elektrycznej i sieciowej. Klienci cenią Panduit jako zaufanego doradcę, który współpracuje z nimi w rozwiązaniu najważniejszych problemów biznesowych w środowiskach przemysłowych oraz Data Center.

PARTNER – jeden z wiodących polskich producentów rozwiązań dźwiękowych systemów ostrzegawczych, Public Address i tła muzycznego. Firma zajmuje się produkcją głośników od prawie 20 lat, produkty są certyfikowane zgodnie z normą europejską EN 54-24, przechodzą proces badań potwierdzanych dokumentami CPR/CPD oraz świadectwami dopuszczenia wydawanymi przez CNBOP-PIB.

URKOM Systemy Teleinformatyczne – specjalizuje się w dostarczaniu systemów zabezpieczeń obiektów, automatyki budynkowej, instalacji elektrycznych, telekomunikacji, technologii VoIP oraz systemów teleinformatycznych. Oferta firmy jest dostosowywana do indywidualnych potrzeb klientów, a doświadczenie zdobyte w ciągu prawie 25 lat działalności gwarantuje sprostanie największym wyzwaniom.

Wsparcie merytoryczne podczas tegorocznej edycji szkolenia zapewnią Partnerzy merytoryczni: **Stowarzyszenie Inżynierów i Techników Pożarnictwa – Izba Rzeczoznawców, Polska Izba Systemów Alarmowych, Instytut Bezpieczeństwa Pożarowego NODEX, HESTIA Loss Control, VdS Schadenverhütung** oraz eksperci reprezentujący **Centrum Naukowo-Badawcze Ochrony Przeciwpożarowej – Państwowy Instytut Badawczy.** Przedstawiciele tych instytucji wezmą udział w sesji zarówno wykładowej, jak i warsztatowej.

Patronat Specjalny nad wydarzeniem objął Wydział Handlowy Ambasady Austrii.

Podobnie jak w latach poprzednich wartość merytoryczna oraz edukacyjny charakter spotkania będą sprawą nadrzędną. W częściach szkoleniowych, które wprowadzą uczestników w najnowsze zmiany i wytyczne dotyczące inteligentnych zabezpieczeń obiektów, nie będą poruszane sprawy marketingowe poszczególnych firm – współorganizatorów szkolenia.

Informacje bieżące będą publikowane na stronie internetowej: wydarzenia.schrack-seconet.pl oraz na kanale LinkedIn. Szczegółowy plan spotkania zostanie opublikowany w drugim tygodniu września br. W tym samym czasie zostanie uruchomiona REJESTRACJA ONLINE. ●

Schrack Seconet Polska
Ul. Adama Branickiego 15
02-972 Warszawa
https://wydarzenia.schrack-seconet.pl/

Jubileuszowe Warsztaty POLON-ALFA

Blisko 500 osób zainteresowanych tematyką pożarową wzięło udział w Ogólnopolskich Warsztatach „Sygnalizacja i Automatyka Pożarowa SAP 2024" zorganizowanych przez firmę POLON-ALFA SA. Jubileuszowe 30. warsztaty odbyły się w miejscu pod wieloma względami wyjątkowym, czyli w budynkach dawnej Cukrowni Żnin, będącej obecnie centrum konferencyjno-wypoczynkowym.

Tematem wiodącym tegorocznych warsztatów były zabezpieczenie przeciwpożarowe obiektów, w których panują specyficzne, trudne warunki pracy, a ich eksploatacja wymaga sporej uważności. O dobrych praktykach w zabezpieczaniu magazynów wysokiego składowania mówił Mariusz Sobecki, kwestię ochrony ppoż. stacji ładowania i postoju pojazdów elektrycznych omówił Paweł Janik, a Kamil Kwosek zaprezentował sposoby zabezpieczania obiektów, w których występuje np. duże zapylenie i związana z tym gorsza widoczność. Z dużym zainteresowaniem spotkało się wystąpienie Marka Podgórskiego na temat systemów detekcji zagrożeń w obiektach jądrowych. Z kolei Krzysztof Sitek omówił działanie zasysających czujek dymu w obiektach typu szyby wind i chłodnie. Równie ważny temat zabezpieczenia ppoż. przestrzeni pod podłogami technicznymi, nad sufitami technicznymi oraz w pomieszczeniach central systemu sygnalizacji pożarowej zreferował Ryszard Małolepszy. Osoby zainteresowane tematem ochrony przepięciowej w systemach sygnalizacji pożarowej w świetle obowiązujących przepisów z zaciekawieniem wysłuchały wykładu Jarosława Wiatera. O różnych aspektach funkcjonowania sygnalizatorów adresowalnych i nieadresowalnych mówił z kolei Tomasz Wdowiak.

Wszyscy z zainteresowaniem słuchali wykładów ekspertów

Przy skręcaniu mebli ogrodowych dla dzieci z Rodzinnego Domu Dziecka w Bydgoszczy radości było co niemiara

Uroczystą kolację uświetnił występ zespołu Electric Girls

Gratulacje z okazji 30. edycji wydarzenia podczas uroczystej kolacji odebrał Mariusz Raczyński, prezes Zarządu POLON-ALFA S.A. (na zdj. z rektorem, komendantem Akademii Pożarniczej st. bryg. dr. inż. Tomaszem Klimczakiem)

– Bogata oferta merytoryczna wykładów stanowi odpowiedź na zapotrzebowanie naszych klientów. Tematy wystąpień często konsultujemy z przedstawicielami Komendy Głównej PSP i Akademii Pożarniczej, a także rzeczoznawcami ds. zabezpieczeń przeciwpożarowych – podkreśla Robert Pestka, dyrektor wsparcia sprzedaży POLON-ALFA. – *Zawsze staramy się, aby warsztaty dostarczyły ich uczestnikom jak największej dawki aktualnej wiedzy, nie tylko teoretycznej, ale też praktycznej.*

Podczas warsztatów gospodarze umożliwili zwiedzanie zakładu produkcyjnego POLON-ALFA w Bydgoszczy. Goście mogli zobaczyć linie produkcyjne i laboratoria, w których są testowane urządzenia projektowane i produkowane przez POLON-ALFA. Niezwykle ciekawy był również pokaz pożarów testowych, który przeprowadzono w zakładowej komorze spalania.

Wysoka jakość produkowanych urządzeń to znak rozpoznawczy „polonowskich" systemów sygnalizacji pożarowej. Warto podkreślić, że już w 1998 roku w firmie został wdrożony system zarządzania jakością ISO 9001 gwarantujący wysoką jakość urządzeń schodzących z linii produkcyjnej POLON-ALFA. Wszystkie urządzenia wytwarzane w bydgoskim zakładzie poddawane są certyfikacji na zgodność z normami europejskimi w notyfikowanych w Unii Europejskiej jednostkach certyfikujących i mają 5-letnią gwarancję. Potwierdzeniem najwyższej jakości całej produkcji jest również uzyskanie przez firmę koncesji na wytwarzanie urządzeń ważnych dla obronności kraju.

Kilka słów o firmie

POLON-ALFA to największy polski producent systemów sygnalizacji pożarowej i aparatury dozymetrycznej oferujący swoje wyroby na rynek zarówno krajowy, jak i zagraniczny. Już w 1956 r. firma zajęła się opracowywaniem i produkcją aparatury do pomiarów promieniowania jonizującego. Po kilku latach profil produkcji został rozszerzony o urządzenia do wykrywania i sygnalizowania pożaru. Produkcja kompletnych systemów sygnalizacji pożarowej, w których skład wchodzą centrale, czujki, ręczne ostrzegacze oraz akcesoria, stanowi do dziś główny zakres działalności firmy.

POLON-ALFA nie ogranicza się jedynie do odbiorców krajowych. Firma aktywnie działa na rynkach międzynarodowych, gdzie jej produkty cieszą się dużym uznaniem. Dziś eksport stanowi istotną część działalności POLON-ALFA, a zdobywanie kolejnych rynków zagranicznych jest jednym z jej głównych celów strategicznych.

To już 30 lat

Skróconą historię warsztatów przybliżył uczestnikom tuż po rozpoczęciu części wykładowej Mariusz Radoszewski. Pełen opis tego, jak to wszystko się zaczęło i trwa do dzisiaj, znajduje się materiałach SAP 2024 wydanych z okazji odbywania się tej imprezy.

Na początku lat dziewięćdziesiątych bydgoski POLON przejął rolę organizatora spotkań firm instalujących i konserwujących SSP po Zjednoczeniu „SUPON". Pierwsze, jeszcze wspólnie organizowane, odbywały się w firmowym ośrodku wypoczynkowym SOKOLE KUŹNICA usytuowanym nad Zalewem Koronowskim. Jednak w 1993 roku w związku z dużym jak na tamte czasy zainteresowaniem postanowiono przenieść je w miejsce o większych możliwościach noclegowych do Zacisza w Borach Tucholskich. I właśnie od tego roku, kiedy to POLON-ALFA samodzielnie zorganizował tę imprezę, zaczęliśmy liczyć kolejne edycje. Po roku 2009 chętnych było tak wielu, że niezbędne było znalezienie obiektu, który bez trudu pomieściłby rosnącą z roku na rok liczbę uczestników. Warsztaty przez te wszystkie lata organizowano w różnych miejscach na terenie całego kraju, by w 2022 r. przenieść się do Cukrowni Żnin, gdzie odbywają się przez ostatnie trzy lata.

– Pamiętam, jak na pierwsze spotkanie Zygmunt Boiński, późniejszy prezes POLON-ALFA, zapraszał uczestników, dzwoniąc po prostu do zaprzyjaźnionych firm – opowiada Elżbieta Czajka, menedżer ds. marketingu. – *Z roku na rok warsztaty zaczęły stawać się coraz bardziej popularne, a lista chętnych zaczęła się regularnie wydłużać. Przez te wszystkie lata poruszyliśmy wiele ciekawych, niekiedy wzbudzających dużo kontrowersji tematów. Wśród wykładowców byli przedstawiciele CNBOP PIB, ITB, Szkoły Głównej Służby Pożarniczej (dziś Akademii Pożarniczej), SITP, Instytutu Łączności, Narodowego Instytutu Muzealnictwa i Ochrony Zbiorów Publicznych, Politechniki Krakowskiej, Politechniki Białostockiej i wielu innych. Dziś, na tę w pewnym sensie kultową imprezę, profesjonaliści zgłaszają się sami. Zdarza się, że wyjeżdżając z warsztatów, już chcą poznać datę i miejsce spotkania w kolejnym roku. To chyba najlepiej świadczy o corocznym sukcesie tego wydarzenia.*

Organizując warsztaty, dbamy o to, by zawsze było to wydarzenie wysokiej klasy. Poruszane podczas spotkań tematy to skutek wsłuchiwania się w głosy naszych klientów. Aby po warsztatach został jakiś ślad, w 1997 roku zaczęliśmy wydawać podręcznik z materiałami zawierającymi tematyczne wykłady. Każdego roku taki podręcznik dostają wszyscy uczestnicy warsztatów, ale także szkoły pożarnicze i uczelnie, w których eksperci POLON-ALFA są wykładowcami.

KOBIETY W MĘSKIEJ BRANŻY

Przez 30 lat w warsztatach POLON-ALFA uczestniczyło w sumie ponad 6 tys. osób z blisko 3,5 tys. firm. I choć branża jest zdominowana przez panów, to przez wszystkie te lata w wydarzeniach wzięło udział 347 pań, czyli blisko 6% gości.

Systemy hybrydowe to najbliższa przyszłość branży ochrony

Rynek oczekuje od branży ochrony wprowadzania nowych rozwiązań, w których praca człowieka będzie wspomagana przez nowoczesne systemy analityczne (AI). Tylko w ten sposób można sprostać wyzwaniom, nadążyć za zmianami rynku i być konkurencyjnymi dla naszych klientów, nie tracąc na jakości usług – mówi Paweł Korzybski, prezes Zarządu Polskiego Związku Pracodawców Ochrona.

To główne przesłanie, jakie przyświecało rozmowom przedstawicieli największych działających w Polsce firm z branży ochrony, zrzeszonych w Polskim Związku Pracodawców Ochrona (PZP Ochrona), podczas dorocznej konferencji, która w tym roku odbyła się pod hasłem „Technologiczna transformacja sektora ochrony w Polsce".

Jarosław Kur, wiceprezes PZP Ochrona, podkreśla, że w branży ochrony przez ostatnie 30 lat dokonała się ogromna rewolucja. *– Poczynając od tego, że początkowo nie było praktycznie żadnych ustaw, żadnych przepisów wykonawczych dla branży ochrony, a kończąc na technologii. Kiedy zaczynaliśmy na początku lat dziewięćdziesiątych, to właściwie słowo „monitoring" kojarzyło się z czymś z przyszłości, a telefony komórkowe z filmami science fiction. Dziś rozmawiamy o technologiach chmurowych, dronach, sztucznej inteligencji. To jest niewyobrażalny postęp* – mówi Jarosław Kur.

Podczas konferencji swoje rozwiązania przeznaczone dla branży ochrony zaprezentowało wiele firm technologicznych. Urządzenia i systemy takie, jak chmurowe wspomaganie zarządzaniem danymi, mobilne wieże monitoringowe, drony czy nawet monokulary lub lornetki z kamerą nokto- lub termowizyjną w ostatnich latach przestały być nowinkami, stając się praktycznie wyposażeniem standardowym.

– Cały czas szukamy nowych rozwiązań, by odpowiedzieć na to, czego oczekuje rynek. Wydaje się, że obecnie są to hybrydowe systemy ochrony, które łączą pracę dobrze wyszkolonego człowieka z zaawansowanym monitoringiem, wykorzystującym inteligentną analizę ogromnej ilości danych, pozyskiwanych z systemów CCTV, SSWiN oraz KD – podkreśla Paweł Korzybski, prezes Zarządu PZP Ochrona. *– Wyzwaniem jest także wprowadzanie omawianych rozwiązań technologicznych w taki sposób, by pomagały one w wykonywaniu naszych podstawowych zadań, tj. ochrony osób i mienia, ale także pozwalały być konkurencyjnymi poprzez znalezienie się w budżetach naszych klientów mimo ciągłych zmian legislacyjnych powodujących znaczny wzrost kosztów wynagrodzeń pracowników.*

Edyta Bujak-Ciebiera, dyrektor handlowy firmy członkowskiej PZP Ochrona, podkreśla, że jednym z efektów zmian jest wzrost zainteresowania tematem sztucznej inteligencji, widoczny od kilku lat.

– Zdecydowanie widzimy dużą transformację, jeżeli chodzi o technologie. Mamy coraz więcej producentów oferujących urządzenia i usługi wykorzystujące sztuczną inteligencję. Sami jesteśmy dostawcą platformy, która operuje wysoko zaawansowaną analityką korzystającą z systemów sztucznej inteligencji i ma na celu głównie wsparcie w analizie obrazu, aby wykluczyć jak najwięcej fałszywych alarmów i wspierać pracowników stacji ochrony w procesach analizy sygnału wideo – mówi Edyta Bujak-Ciebiera. *– Ostatecznie to człowiek podejmuje decyzję, czy należy interweniować, czy nie, natomiast dzięki wsparciu AI ta decyzja może być łatwiejsza* – dodaje.

Problem analizy ogromnej ilości danych spływających z monitoringu i odróżnienia alarmów prawdziwych od fałszywych (np. wywoływanych przez dzikie zwierzęta czy przedmioty poruszane przez wiatr) pojawia się m.in. w przypadku monitorowania farm fotowoltaicznych położonych często z dala od ośrodków miejskich. ●

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

ROGER

VISO SMS – zaawansowane monitorowanie i wizualizacja systemów bezpieczeństwa

Skuteczne zabezpieczenie obiektu często wymaga jednoczesnej współpracy wielu systemów.

Znacznie wygodniej jest korzystać z jednego narzędzia, dlatego firma Roger wprowadziła do swojej oferty oprogramowanie VISO SMS, które umożliwia monitorowanie i wizualizację systemów bezpieczeństwa z poziomu jednej platformy. Dzięki temu rozwiązaniu możliwe jest szybkie otrzymywanie powiadomień o alarmach i awariach, wizualizacja zagrożeń na mapach obiektu oraz ich weryfikacja w systemie telewizji dozorowej. Ponadto oprogramowanie to pozwala na opracowywanie i wyświetlanie procedur postępowania dla operatora w momencie wystąpienia danego zdarzenia.

Gotowy scenariusz bezpieczeństwa zawiera listę czynności do wykonania, a także umożliwia operatorowi interaktywne wykonanie telefonu do przełożonego, wysłanie SMS-a lub e-maila, wygenerowanie raportu obecności itp. Narzędzie to usprawnia również rejestrację i organizację prac serwisowo-konserwacyjnych, umożliwiając dodawanie notatek dotyczących czujek, przejść czy kamer oraz rejestrując zadymienie czujek pożarowych.

VISO SMS może funkcjonować jako platforma nadzorująca różne systemy bezpieczeństwa lub jako integralny element systemu kontroli dostępu RACS 5. Rozwiązanie wspiera pracę osób odpowiedzialnych za bezpieczeństwo obiektu, umożliwiając im monitorowanie i wizualizację systemów:

- sygnalizacji włamania i napadu;
- ochrony obwodowej;
- kontroli dostępu;
- sygnalizacji przeciwpożarowej;
- telewizji dozorowej.

VISO SMS jest z powodzeniem stosowane m.in. przez Uniwersytet Ekonomiczny we Wrocławiu, zakład produkcyjny Kupiec czy Gdański Park Naukowo-Technologiczny. ●

SAFETY PROJECT

Kongres Safe Place 2024

VII Międzynarodowy Kongres Safe Place 2024: *Odporność obiektów użyteczności publicznej i infrastruktury krytycznej wobec zagrożeń wojennych, hybrydowych i kryminalnych* odbędzie się 27–28 listopada w Centrum Kongresowym hotelu Windsor w Jachrance k. Warszawy.

W programie kongresu znajdzie się:

- 11 nowych sesji tematycznych z wystąpieniami i debatami eksperckimi z możliwością interaktywnej dyskusji;
- 4 warsztaty praktyczne i konkurs dla uczestników z łączną wartością nagród przekraczającą 20 tys. Zł;
- prelekcje ekspertów polskich i zagranicznych, m.in. z USA, Izraela, Wielkiej Brytanii i Ukrainy;
- stoiska edukacyjne Safety Project, Centrum Ratownictwa, wirtualna strzelnica oraz prezentacja innowacji w branży zabezpieczeń technicznych firm: Nedap, RCS Engineering, Idesco Oy, Bosch Security and Safety Systems, DFE Security, Aritech oraz wielu innych producentów i dystrybutorów;
- dedykowana strefa networkingowa w gronie ponad 300 osób z interaktywnym warsztatem;
- bankiet taneczny i konkursy indywidualne.

Kongres Safe Place to największe w Polsce wydarzenie poświęcone bezpieczeństwu obiektów użyteczności publicznej i infrastruktury krytycznej, odbywające się pod patronatem instytucji gwarantujących najwyższy poziom obrad. Każdego roku w wydarzeniu bierze udział kilkuset przedstawicieli kluczowych obiektów użyteczności publicznej, infrastruktury krytycznej oraz rynku komercyjnego, a także naukowców i ekspertów. Tematem tegorocznej edycji będzie budowanie odporności obiektów użyteczności publicznej i infrastruktury krytycznej na zagrożenia wojenne, hybrydowe i kryminalne.

Główna tematyka tegorocznych obrad jest skupiona wokół następujących obszarów:

- Przygotowanie obiektów do wojny, zagrożeń hybrydowych i kryminalnych
- Budowanie odporności obiektów i przestrzeni na zamachy
- Zarządzanie bezpieczeństwem w infrastrukturze krytycznej i obiektach podlegających obowiązkowej ochronie oraz w obiektach niechronionych obowiązkowo
- Budowanie odporności powiatów, gmin i miast
- Bezpieczeństwo pożarowe obiektów i przestrzeni
- Zagrożenia i szanse dla branży security w obliczu implementacji Dyrektyw NIS2, CER i DORA
- Rola i zadania liderów w zarządzaniu bezpieczeństwem w obiektach i przestrzeniach
- Innowacje i najnowsze technologie w budowaniu odporności obiektów i przestrzeni
- Wyzwania dla architektów i projektantów obiektów oraz instalacji zabezpieczeń technicznych w dobie współczesnych zagrożeń
- Reagowanie na zamachy na życie i zdrowie
- Pierwsza pomoc w reagowaniu na zamachy

Patronaty Honorowe objęli: Dyrektor Rządowego Centrum Bezpieczeństwa, Dyrektor NATO Deep eAcademy, JM Rektor Uniwersytet WSB Merito Wrocław, Instytut Zachodni, Polskie Towarzystwo Nauk o Bezpieczeństwie.

Organizatorami są:

- Uniwersytet WSB Merito Wrocław
- Wojskowa Akademia Techniczna w Warszawie
- Akademia Policji w Szczytnie
- Akademia Pożarnicza w Warszawie
- NATO Deep eAcademy
- Safety Project ●

AXIS COMMUNICATIONS

Wysokowydajna kamera typu bullet

Kamera AXIS Q1808-LE jest wyposażona w przetwornik obrazu 4/3 cala, który zapewnia wyjątkowe parametry pracy w słabym oświetleniu. Dzięki technologii OptimizedIR urządzenie pozwala uzyskać ostry i wyraźny obraz w całkowitej ciemności bez stosowania dodatkowego oświetlenia.

Technologie Lightfinder 2.0 i Forensic WDR pozwalają uzyskać realistyczne kolory i wiernie odwzorowane szczegóły w trudnych warunkach oświetleniowych lub niemal całkowitej ciemności. Kamera jest dostępna z obiektywem szerokokątnym do obserwacji otwartych przestrzeni lub teleobiektywem umożliwiającym prowadzenie dozoru na odległość.

Ta wysokowydajna kamera zawiera jednostkę głębokiego uczenia, która zwiększa jej możliwości w zakresie przetwarzania. Pozwala to na gromadzenie i analizowanie jeszcze większej ilości danych na brzegu sieci, czyli w samej kamerze. Ponadto kamera dostarcza cenne metadane, ułatwiając prowadzenie szybkich i efektywnych prac wyjaśniających. Aplikacja AXIS Object Analytics umożliwia detekcję i klasyfikację poruszających się obiektów. Ponadto dzięki obsłudze platformy ACAP w wersji 4 można instalować specjalnie opracowane aplikacje oferowane przez Axis i naszych partnerów, które wykorzystują mechanizm głębokiego uczenia na brzegu sieci.

AXIS Q1808-LE gotowa do montażu na zewnątrz oferuje klasy ochrony IP66, IP67, IK10 oraz NEMA 4X i może pracować w temperaturze od -40°C do 60°C. Technologia Zipstream H.264/ H.265 znacznie zmniejsza zapotrzebowanie na przepustowość i pamięć masową. Włączony profil przechowywania zapewnia optymalny poziom działania technologii Zipstream pod kątem przechowywania materiału wizyjnego niezależnie od oprogramowania do zarządzania materiałem wizyjnym. Ponadto funkcja Axis Edge Vault zabezpiecza urządzenie i umożliwia bezpieczne przechowywanie kluczy dzięki certyfikatowi FIPS 140-2 poziom 2. ●

AXIS COMMUNICATIONS

Nowe kamery kopułkowe z wbudowanym mikrofonem

Axis Communications rozszerza serie urządzeń AXIS P32 i AXIS M30 o dwa nowe modele kamer kopułkowych z wbudowanym mikrofonem oraz gotową do użycia aplikacją AXIS Audio Analytics.

Kamery AXIS M3086-V Mic oraz AXIS P3267-LVE Mic oferują te same funkcje co wersje standardowe i są wyposażone we wbudowany mikrofon, który upraszcza korzystanie z funkcji analizy dźwięku.

Obie kamery są fabrycznie gotowe do użycia z aplikacją AXIS Audio Analytics wykorzystującą adaptacyjną detekcję dźwięku do generowania alarmów w przypadku nagłego wzrostu głośności. Dzięki klasyfikatorom opartym na algorytmach sztucznej inteligencji aplikacja może wykrywać oraz rozróżniać krzyk (najczęściej zawiera komunikat, jest zazwyczaj bardzo głośny, może wyrażać pozytywne i negatywne emocje) i wrzask (najczęściej nie zawiera komunikatu, jest zabarwiony negatywnie emocjonalnie).

Dodatkowo obie kamery oferują obsługę inteligentnych funkcji analitycznych, które dostarczają cenne metadane ułatwiające szybkie, łatwe i wydajne wyszukiwanie kryminalistyczne na zarejestrowanych materiałach wideo oraz na żywo.

Aplikacja AXIS Audio Analytics jest podstawową funkcją systemu AXIS OS, dlatego obie kamery są gotowe do współpracy z tą aplikacją od razu po wyjęciu z opakowania. Co ważne – aplikacja przesyła tylko metadane, zapewniając pełną ochronę prywatności. W razie potrzeby można szybko włączyć i wyłączyć zarówno AXIS Audio Analytics, jak i strumieniowe przesyłanie dźwięku. ●

HANWHA VISION

Nowa kamera naścienna z AI

Frima Hanwha Vision wprowadziła na rynek TNV-C8011RW – 5-Mpix kamerę naścienną AI na podczerwień, idealną do montażu przy wejściach i wyjściach, w punktach sprzedaży detalicznej, przejazdach, kasach samoobsługowych i innych miejscach, w których do identyfikacji niezbędny jest wyraźny widok twarzy.

W przeciwieństwie do kamer montowanych wysoko na ścianach, które zazwyczaj zapewniają widok z góry na dół, TNV-C8011RW została zaprojektowana do montażu na poziomie oczu, umożliwiając szeroki i wyraźny obraz twarzy, nawet gdy osoby mają na głowie kapelusze lub używają parasoli.

Panoramiczny obiektyw zapewnia prawie 180-stopniowe pole widzenia, z regulowanym kątem nachylenia obiektywu wynoszącym około 25∞, co eliminuje martwe punkty. Rozdzielczość 5 Mpix gwarantuje wszystkie szczegóły wymagane do identyfikacji osób będących przedmiotem zainteresowania, co zwiększa bezpieczeństwo i komfort obsługi klienta. Oświetlacze IR doświetlają scenę na odległość do 15 m, co zapewnia wyraźny obraz także w zmiennych warunkach oświetleniowych.

Poza optymalnym montażem do celów identyfikacji, TNV-C8011RW wykorzystuje sztuczną inteligencję wspomagającą identyfikację osób i innych obiektów, poprawiając efektywność operatora. Dzięki temu może skupić się na zadaniach o wyższym priorytecie, ponieważ inteligentne rozwiązanie ostrzega tylko o zdarzeniach wymagających uwagi.

Wyszukiwanie za pomocą metadanych generowanych przez kamerę skraca czas, jaki operatorzy muszą poświęcić na wyszukiwanie określonych zdarzeń, ponieważ analiza AI jest przeprowadzana w kamerze, eliminując koszty utrzymania oddzielnej infrastruktury komputerowej. Technologia kompresji WiseStream III znacznie zmniejsza wielkość danych i szerokość pasma przy jednoczesnym zachowaniu wysokiej jakości obrazu, zapewniając wydajną i ekonomiczną ofertę.

Kamerę wyposażono w funkcje inteligentnej analizy, takie jak liczenie osób i pojazdów, monitorowanie długości kolejek czy tworzenie map cieplnych. Są one idealne do stosowania w wejściach i wyjściach, holach, punktach sprzedaży detalicznej i przejazdach, umożliwiając przewidywanie okresów wzmożonego ruchu, informowanie o harmonogramach zatrudnienia i poprawę obsługi klienta.

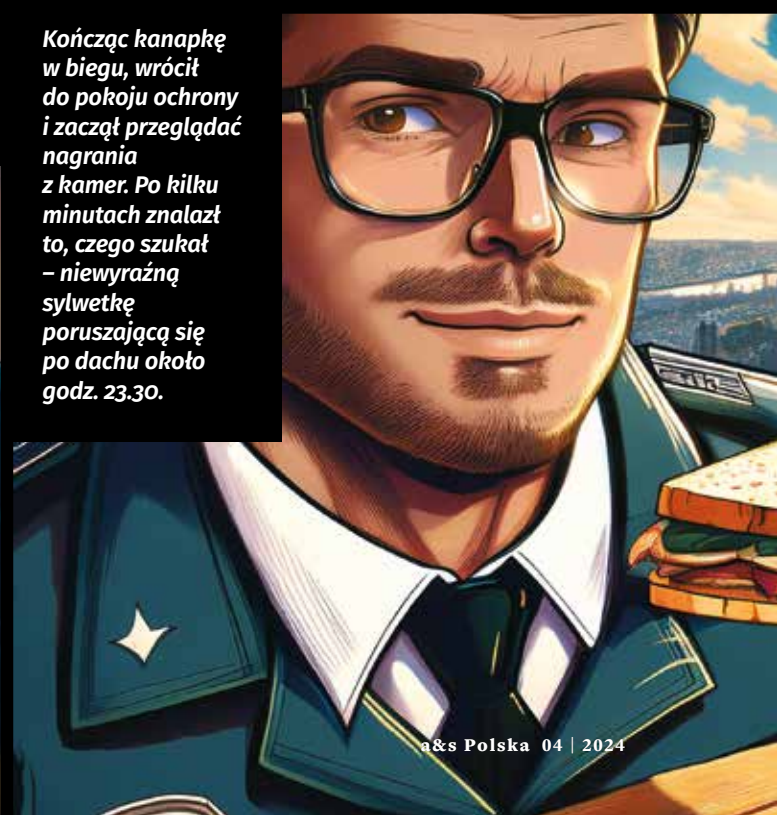
Podobnie jak wszystkie produkty Hanwha Vision, kamera oferuje najwyższy poziom cyberbezpieczeństwa dzięki funkcjom bezpiecznego przechowywania, uwierzytelniania użytkownika i sieci, ochrony danych i identyfikacji urządzenia (*Hanwha Private Root CA*). ●

Nocny kowboj

Marcin Kowalski, doświadczony pracownik ochrony hotelu Panoramix (właściciel hotelu ewidentnie był fanem pewnego francuskiego komiksu), siedział w pokoju ochrony na parterze, monitorując ekrany. Mimo że hotel był niewielkim czteropiętrowym obiektem, jego luksusowy charakter wymagał najwyższych standardów bezpieczeństwa.

Było tuż po północy, kiedy Marcin wyszedł na rutynowy obchód. Dla towarzystwa zabrał kanapkę z jajkiem na twardo i jabłko. Noc była przyjemnie ciepła. „Cisza i spokój, tak lubię", pomyślał i dziarskim krokiem wkroczył na jasno oświetlony parking. I dalej byłoby cicho i spokojnie, gdyby nie to, że jego uwagę przykuł dziwny cień. Coś było nie tak. Instynktownie spojrzał w górę i na krawędzi dachu dostrzegł coś niepokojącego. Nie był pewien, co dokładnie widzi, ale jego doświadczenie podpowiadało mu, że to nie jest zwykła gra światła i cienia.

Kończąc kanapkę w biegu, wrócił do pokoju ochrony i zaczął przeglądać nagrania z kamer. Po kilku minutach znalazł to, czego szukał – niewyraźną sylwetkę poruszającą się po dachu około godz. 23.30.



Diabli nadali

Nie czekając ranka, głodny jak wilk, bo kanapka była tylko jedna, Marcin Kowalski złożył szczegółowy raport kierownikowi ochrony Piotrowi Nowakowi.

– Panie Nowak… – zaczął Marcin, który doskonale wiedział, że jego szef tej formy nie cierpiał, ale prywatnie się przyjaźnili i lubił od czasu do czasu podrażnić się z kolegą.

– Ty mnie tu nie „nowakuj", tylko wal, z czym przychodzisz. Pewnie jakiś urlopik, co? – Piotr Nowak znał Marcina jak zły szeląg i wiedział, że „nowakowanie" zawsze oznacza jakiś problem.

– Eeee, żaden urlopik. Otóż w nocy ktoś nam chodził po dachu. – Kowalski aż parsknął, widząc, jak Nowakowi brwi podjeżdżają do góry. „Dobrze, że nie jest łysy, bo spadłyby mu na potylicę", pomyślał, ale tę uwagę zostawił dla siebie.

– Jesteś pewien? Przecież nie można wejść tak sobie na dach. Znaczy się rozumiem, co do mnie mówisz, ale… – Nowak nie bardzo wiedział, co ma o tym sądzić.

– Tak, jestem pewien. Mamy nagrania i zdjęcia – odpowiedział Marcin. – Zaloguj się do systemu, to sam zobaczysz.

Piotr westchnął ciężko i mrucząc pod nosem, zaczął wpisywać login.

– I diabli wzięli święty spokój. No dobra, trzeba się naradzić i wyjaśnić, jakiż to Batman podziwiał panoramę nocą.

Spider-Man, Batman czy ki czort?

Godzinę później zespół ochrony zebrał się w kanciapce, w której przebywał zazwyczaj jeden pracownik, za to było mnóstwo sprzętu, który podkręcał temperaturę we wnętrzu. Atmosfera była napięta, można rzec gorąca, a pytania mnożyły się z każdą minutą.

– Może to był pracownik hotelu? – zasugerowała Anna Naiwna, nowa w zespole, której nazwisko pasowało do niej jak ulał.

– Niemożliwe – odparł Tomasz Speck, specjalista od systemów zabezpieczeń. – Dostęp na dach jest ściśle kontrolowany.

Karol, drugi nocny strażnik, siedział z nogami na stole, żonglując trzema długopisami.

– Wiecie co? Może to był jakiś superbohater na emeryturze. Stare nawyki ciężko wykorzenić. Wszyscy zbiorczo przewrócili oczami, a Nowak rzucił mu ostrzegawcze spojrzenie. Karol westchnął i zdjął nogi ze stołu, ale nie przestał żonglować.

– A tak na serio – kontynuował Karol – a jeśli to był jakiś szalony sportowiec? Słyszałem, że ci parkourowcy potrafią się wspinać po ścianach jak Spider-Man.

Anna zachichotała jak pensjonarka.

– Karol, to nie jest film akcji.

– No właśnie! – Karol znacząco podniósł brwi. – Rzeczywistość czasem przerasta fikcję! Jak pracowałem…

Tym razem było słychać zbiorowy jęk. Wszyscy na pamięć znali opowieści Karola, o wdzięcznym nazwisku Błąd. Karol Błąd, mistrz opowieści szpiegowskich i dowcipów z brodą.

Piotr potarł skronie.

– Karol, zlituj się, naprawdę uważasz, że na dachu był Spider-Man?

Karol złapał wszystkie długopisy jedną ręką i zamyślił się na moment.

– Cóż, jeśli mówimy poważnie, to może powinniśmy sprawdzić, czy ktoś nie próbował zainstalować jakiegoś sprzętu szpiegowskiego? Widok z naszego dachu jest idealny do obserwacji kilku ważnych budynków w okolicy. Choćby ta firma z naprzeciwka, wiecie, ta wielka firma farmaceutyczna.

Owszem, wiedzieli. Wiedzieli też, że Karol miał słabość do jednej z recepcjonistek z firmy, i miał na nią wyjątkowo czujne baczenie.

Piotr zamrugał, zaskoczony.

– To… to faktycznie jakaś myśl.

Piotr zaczął chodzić po niewielkim pomieszczeniu, a w zasadzie dreptać w miejscu

– Podsumujmy, co wiemy – powiedział poważnym tonem. Intruz pojawił się około 23.30. Nie został wykryty przez czujniki ruchu. Kamery zarejestrowały tylko niewyraźną sylwetkę. Marcin osobiście zauważył coś podejrzanego na dachu. Nie ma śladów włamania ani uszkodzenia drzwi. To wygląda na profesjonalne działanie – stwierdził z całą mocą i od razu zadał pytanie: – Ale po co ktoś miałby się włamywać na dach hotelu? Czy naprawdę chciał tam coś zamontować? Trzeba sprawdzić.

Nagle Speck zbladł jak ściana i wyszeptał cicho:

– Czerpnie…

– Czerwie? – Zdziwił się Karol.

– Na dachu są czerpnie systemu wentylacyjnego całego obiektu – wyjaśnił Tomek. – Ktoś mógłby przez nie rozpylić niebezpieczne substancje w całym budynku.

W sali zapadła cisza.

– Musimy natychmiast wszystko sprawdzić! – krzyknął Piotr.

W małym pomieszczeniu zrobił się tumult. Nowak rzucił się do komputera. Naiwna i Błąd usiłowali jednocześnie wyjść przez wąskie drzwi, by pognać na dach. Tylko Kowalski stał niewzruszony, bo nie mógł sobie przypomnieć, co zrobił z jabłkiem, a coraz bardziej ssało go w żołądku. „Już dawno powinienem być w domu", pomyślał.

Jakiś czas później...

Uważna inspekcja dachu w towarzystwie techników policyjnych nie wykazała nic nadzwyczajnego. Nie było śladów włamania. Żadnych śladów stóp. Przy czerpniach powietrza nie znaleziono niczego podejrzanego. Analiza powietrza w systemie też wypadła bez zarzutu. Nowak jednak czuł, że coś tu jest „nie halo". Po co ktoś właziłby po nocy na dach hotelu? Owszem luksusowego, ale dach to dach. I choć wszyscy odetchnęli z ulgą, to Nowak nie wyglądał na zadowolonego. Cały czas dręczyło go dziwne przeczucie… Niepokojące mrowienie w stopach, jakiego doświadczał np. na widok ślimaka bez skorupki.

I trwało aż do tego piątkowego poranka, gdy przy śniadaniu sięgnął po komórkę, by zobaczyć „Co tam, panie, w polityce". Prawie zakrztusił

się herbatą, a pijał wrzątek, gdy trafił na duży nagłówek z napisem „PILNE". Portal informacyjny donosił, że doszło do włamania do siedziby dużego koncernu farmaceutycznego. Włamywacze ponoć dostali się przez dach. Co wyniesiono? Teoretycznie nic cennego. Z wypowiedzi rzecznika firmy wynikało, że jakąś nieistotną dokumentację. „Tu was mam! Nieistotną dokumentację, powiadacie", pomyślał Nowak. „To nie o nasze czerpnie chodziło", odetchnął z ulgą. Sięgnął po telefon i zadzwonił do Marcina.

– Widziałeś? – Nawet nie musiał wyjaśniać.
– Ano widziałem. Ale…
– …ale i tak trzeba wzmocnić ochronę
– Ano trzeba.
Panowie rozumieli się prawie bez słów.

O co mogło chodzić? Po co ktoś wszedł na dach hotelu? I czy Wy, Szanowni Czytelnicy, wiecie dokładnie, jak chronione są czerpnie powietrza w obiektach pozostawionych waszej opiece? Bo tym razem skończyło się dobrze, ale…

Opracowała Monika Mamakis na bazie scenariusza Jacka Grzechowiaka

Security Forum to warsztaty, podczas których omawiamy nietypowe przypadki i przedstawiamy różne scenariusze, najczęściej z życia wzięte. Oto, co o Security Forum mówią zaproszeni przez nas eksperci.

Paweł Nowik, EST Polska

Szkolenie było bardzo merytoryczna, ożywiona dyskusja poruszyła wiele ciekawych zagadnień. Na udział zdecydowaliśmy się, ponieważ chcieliśmy pogłębić naszą wiedzę odnośnie do wyzwań, które stoją przed naszymi klientami. Chcieliśmy poznać trendy, które panują obecnie, ponieważ branża security cały czas się zmienia. Pojawiają się nowe zagrożenia, rozwijają się nowe technologie. W trakcie takich spotkań pogłębiamy naszą wiedzę i budujemy świadomość, z czym się mierzy rynek i do których sektorów skierować naszą ofertę.

Marek Skowronek, Securitas

Każda forma spotkania z menedżerami security, kiedy możemy porozmawiać o ich potrzebach, jest dla nas bardzo cenna. To jest inspirujące i takie właśnie było to spotkanie. Wśród uczestników wywiązała się zażarta dyskusja, co wskazuje, że poruszane tematy były ważne. Wiedza wyniesiona z takich rozmów jest bardzo cenna i przydatna zarówno dla uczestników, jak i dla nas. Z Security Forum wynosimy masę inspiracji, ciekawe kontakty i deklarujemy swój udział w kolejnych tego typu spotkaniach.

Maciej Oleszczak, Ghelamco

Dzisiejsze szkolenie dało mi obraz bezpieczeństwa z punktu widzenia innych obiektów niż budynki biurowe. Dowiedziałem się, skąd czerpać informacje dotyczące dobrych praktyk i jak je stosować. Dla mnie bardzo cenne było wyjście poza świat biurowy i posłuchanie o tym, co dzieje się w innych branżach. Bo często jest tak, że działamy sztampowo, robimy coś według schematu. A dziś trzeba iść do przodu i czerpać z doświadczeń innych, żeby móc ocenić, czy to, co robimy na tę chwilę, jest wystarczające, czy powinniśmy coś zmienić.

Michał Adamczyk, Credit Suisse

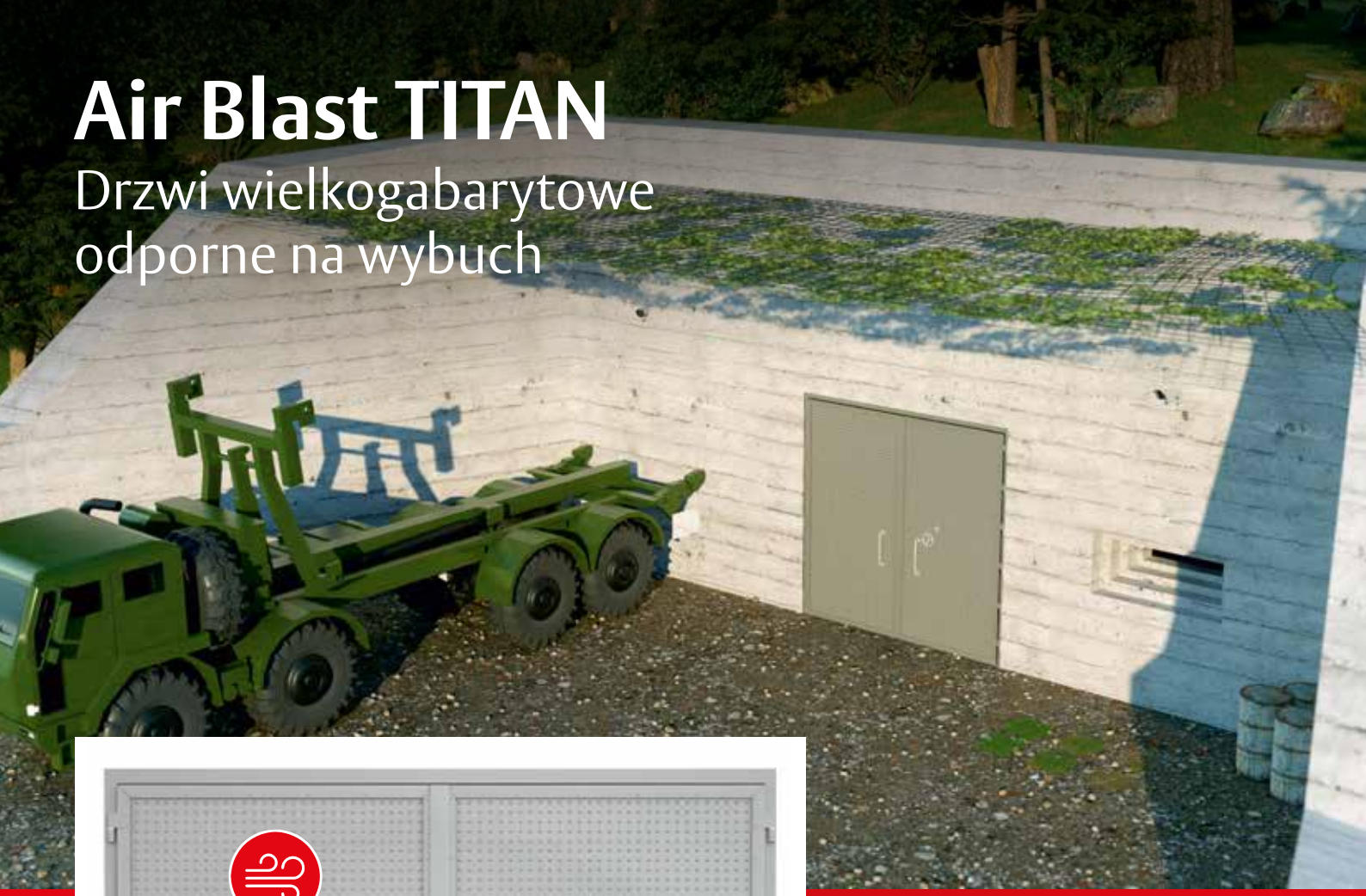
Jak zawsze ciekawa prezentacja Jacka Grzechowiaka wzbogaciła mnie o wiedzę o tym, na jakie zagrożenia może być narażony hotel czy biuro, z których nie zdajemy sobie sprawy i nie zawsze jesteśmy na nie przygotowani. Osobiście dość dużo podróżuję i hotele są częścią mojego życia. Dlatego omawiane incydenty bardzo mnie zaciekawiły. Bardzo cenna jest dla mnie również wymiana doświadczeń z innymi security managerami, którzy mają inną perspektywę i inne spojrzenie na bezpieczeństwo.

Lidia Fałtyn, mBank

Dzisiejsze szkolenie było bardzo wartościowe, bo dało mi możliwość kontaktu z innymi menedżerami i spojrzenia z różnych perspektyw na zagrożenia, które mogą nas dotyczyć. Zaprezentowane zostały trzy różne incydenty, z których każdy dotyczył innego aspektu zabezpieczeń. Podobała mi się otwartość szkolenia, bo każdy z uczestników mógł się wypowiedzieć i jego głos został doceniony. Jestem wielką fanką takich spotkań i bardzo dziękuję za zaproszenie.

Air Blast TITAN

Drzwi wielkogabarytowe odporne na wybuch



DONIMET
ASSA ABLOY

Experience a safer and more open world

Jakość potwierdzona badaniami

Przetestowane na wojskowym poligonie przez zespół doświadczonych specjalistów **Zakładu Badań Materiałów Wybuchowych Wojskowego Instytutu Technicznego Uzbrojenia** i uzyskały certyfikaty wydane przez Warszawski Instytut Technologiczny.

Zastosowanie

Air Blast TITAN to rozwiązanie kierowane do armii, ale sprawdzi się również wszędzie tam, gdzie występuje ryzyko wystąpienia wybuchu o znacznej sile. **Wytrzymują wybuch ładunku 20 kg TNT** w bezpośrednim sąsiedztwie drzwi, po czym pozostają szczelne i bezpieczne.

DOWIEDZ SIĘ WIĘCEJ:

BCS ULTRA

Nowa linia produktowa
pochodząca z **Korei Południowej**
w ofercie **marki BCS** spełniająca
najwyższe wymagania
norm cyberbezpieczeństwa,
a także dyrektywy **NDAA**.

POLSKA MARKA BCS

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

BCS®