CZASOPISMO BEZPŁATNE ISSN: 1505-2419 DWUMIESIĘCZNIK NR 3(115)/2017

ZABEZPIECZENIA

WWW.ZABEZPIECZENIA.COM.PL • E-MAIL: ZABEZ@ZABEZPIECZENIA.COM.PL

TEMAT NUMERU – NOWE PRODUKTY W SYSTEMACH KONTROLI DOSTĘPU I ROZWIĄZANIA DLA HOTELI

- Bezpieczeństwo informacji w chmurze (część 1)
- Podstawy przeprowadzania audytu dotyczącego zarządzania bezpieczeństwem obiektów
- A ty, jaki masz nadajnik alarmowy?

BE READY FOR AN EXTRA-ORDINARY NEW WORLD

- **Extra**-competitive
- **Extra**-light
- **Extra**-compact
- **Extra**-flexible

Nowe kamery MAXIMUS MMX pozwolą na realizację nawet najbardziej skomplikowanych zadań w portach, na nabrzeżach i pokładach okrętów oraz w instalacjach przemysłowych, w których panują bardzo trudne warunki eksploatacyjne.

MAXIMUS MMX CAMERA

ATEX

c UL us LISTED

IECEx

EAC Ex

VIDEO SECURITY PRODUCTS

www.videotec.com

Made in Italy

VIDEOTEC

Więcej możliwości dzięki nowej linii kamer Mx6.

Więcej zdjęć w każdym świetle, w każdym standardzie.

Więcej inteligencji w zasięgu wzroku.

Nowa linia kamer 6MP Mx6 firmy MOBOTIX zapewnia większą wydajność. Dzięki nawet dwukrotnie większej liczbie klatek na sekundę można jeszcze lepiej uchwycić szybki ruch i uzyskać doskonałą jakość zdjęć – jednocześnie w MxPEG, MJPEG i po raz pierwszy także w standardzie przemysłowym H.264. Innowacyjna linia kamer Mx6 jest szybsza, wydajniejsza i bardziej efektywna, co otwiera nowe możliwości zastosowania i integracji przy spełnieniu wszystkich wymogów.

MOBOTIX AG • Langmeil, Germany • www.mobotix.com

MOBOTIX

SPIS TREŚCI 03 2017

AXIS P13
rozwinięcie serii cenionych kamer 4K o rozdzielczości 5 MP

Kompaktowa kamera sieciowa AXIS P1367 oraz kamery **AXIS P1367-E** i **AXIS P1368-E** to najnowsze urządzenia przeznaczone do pracy na zewnątrz budynków, należące do cenionej serii **AXIS P13.** Dzięki zwiększonej światłoczułości oraz lepszej jakości obrazu umożliwiają one obserwację dużych przestrzeni nawet w niekorzystnych warunkach oświetleniowych. Kamery powstały z myślą o miejskich systemach monitoringu, a także transporcie i handlu. Mogą służyć np. do obserwacji zatłoczonych parkingów, dworców kolejowych czy często uczęszczanych rejonów miast.

Kamery P1367 i P1367-E mogą pracować z obiektywami z uchwytami CS oraz i-CS, zaś P1368-E ma wbudowaną optykę tylko i-CS. W P1367-E oraz P1368-E zastosowano innowacyjne rozwiązania ułatwiające dostęp do kamer i pozostawiające więcej miejsca na obiektyw. Wbudowane szyny umożliwiają instalację obiektywów zmiennoogniskowych.

Bezpośr. inf. Axis Communications

Zmiany w strukturach sprzedażowych firmy
Axis Communications

Firma **Axis Communications** poinformowała o zmianach w polskim dziale sprzedaży. **Agata Majkucińska**, która do tej pory zajmowała stanowisko Key Account Managera, awansowała na pozycję Distribution Account Managera w regionie Europy Wschodniej i będzie odpowiedzialna za rozbudowę sieci dystrybucyjnej w Polsce, krajach bałtyckich i na Ukrainie, współtworzonej przez firmy z branży IT i branży zabezpieczeń. Równocześnie z początkiem drugiego kwartału 2017 roku do zespołu dołączył **Karol Dominiczak**, który objął stanowisko Key Account Managera. W Axis Communications będzie zajmował się współpracą z kluczowymi integratorami w Polsce, a w szczególności tworzeniem zindywidualizowanych rozwiązań z zakresu bezpieczeństwa i kontaktami z klientami końcowymi.

– Awans Agaty to naturalny krok dla Axis Communications – przez lata udowodniła swoje najwyższe kompetencje i wiedzę, które teraz będzie mogła wykorzystać, rozbudowując naszą sieć dystrybucyjną w całym regionie Europy Wschodniej. Jestem przekonany, że doskonale poradzi sobie z nowymi wyzwaniami i wydatnie przyczyni się do dalszej ekspansji Axisa na tych rynkach – powiedział Jakub Kozak, Sales Manager – Poland, Ukraine, Baltics w Axis Communications. – *Niezmiernie cieszę się także z faktu, że dołączył do nas Karol Dominiczak. Jego doświadczenie, znajomość rynku oraz najnowszych trendów branżowych, tak w Polsce, jak i w innych krajach naszego regionu, z pewnością przyniesie wiele korzyści naszym klientom.*

Agata Majkucińska jest związana z Axis Communications od 2009 roku. Jako pierwsza osoba zatrudniona przez tę firmę w Polsce była odpowiedzialna za rozwój biznesu i pozyskanie partnerów biznesowych. Wcześniej pracowała na stanowiskach menadżerskich w firmie wdrożeniowej Komtech, gdzie była odpowiedzialna za strategię marketingową, sprzedaż oraz tworzenie układów partnerskich z innymi firmami. Agata Majkucińska jest absolwentką Akademii Ekonomicznej w Krakowie (aktualnie jest to Uniwersytet Ekonomiczny) na kierunku zarządzanie i marketing (specjalizacja – zarządzanie firmą). Prywatnie jest zamężna, ma dwójkę dzieci, a czas wolny poświęca na czytanie i podróże.

Karol Dominiczak, który dołączył do Axis Communications, ma ponad jedenastoletnie doświadczenie w branży technologicznej. Ostatnio pracował w firmie IBM, gdzie odpowiadał za kompleksową obsługę klientów z sektora SMB. W zakres jego obowiązków wchodziła sprzedaż wyposażenia serwerowni, rozwiązań z zakresu bezpieczeństwa, a także systemów wspomagających biznes. Wcześniej był związany z firmą medyczną Grifols, gdzie odpowiadał za uruchomienie działu diagnostycznego oferującego zrobotyzowany system do badania grup krwi.

Bezpośr. inf. Axis Communications

Hanwha Techwin Security Business Group
nawiązuje globalne relacje partnerskie
z liderem w dziedzinie sztucznej inteligencji – firmą NVIDIA

Firma **Hanwha Techwin** (Security Business Group, prezes Lee Man-Seob) zawarła umowę o globalnej partnerskiej współpracy z firmą **NVIDIA**, która jest liderem w dziedzinie sztucznej inteligencji, co przyczyni się do wzmocnienia konkurencyjności produktów i rozwiązań z dziedziny zabezpieczeń, w których wykorzystuje się sztuczną inteligencję (AI – od ang. *artificial intelligence*).

Firma NVIDIA ma swoją siedzibę w Stanach Zjednoczonych i jest pionierem w dziedzinie nowoczesnej grafiki komputerowej. Osiągnęła sukces, projektując i produkując karty graficzne. Ostatnio NVIDIA wyprowadza technologię AI poza zamknięte pomieszczenia, wytwarzając procesory graficzne nie tylko do komputerów, lecz także do robotów i samochodów autonomicznych. Wykorzystują one algorytmy uczenia się (ang. *deep learning*).

Globalne partnerstwo umożliwi firmom Hanwha Techwin i NVIDIA planowanie współpracy dotyczącej platformy inteligentnej analizy treści obrazu, którą NVIDIA aktualnie rozwija.

Platforma firmy NVIDIA przeznaczona do inteligentnej analizy treści obrazu będzie obejmować procesory graficzne AI z algorytmami głębokiego uczenia maszynowego zastosowane w urządzeniach zabezpieczających (kamerach i nośnikach pamięci masowej). Dzięki temu możliwa będzie szybsza i dokładniejsza analiza materiału wizyjnego będącego źródłem informacji.

Hanwha Techwin będzie koncentrować się na rozwoju kamer AI i urządzeń pamięci masowej, które będą mogły autonomicznie wykrywać nietypowe ruchy i sytuacje w materiale wizyjnym dostarczanym przez kamery.

– *Współpraca z firmą NVIDIA to krok ku systemom bezpieczeństwa opartym na sztucznej inteligencji i dokładnemu uczeniu się, który wzmocni naszą technologiczną konkurencyjność na tym rynku* – powiedział Lee Man-Seob, prezes i dyrektor generalny Hanwha Techwin Security Business Group.

Bezpośr. inf. Hanwha Techwin

MAXIMUS MMX
nowy iskrobezpieczny punkt kamerowy firmy Videotec

Videotec, czołowy producent wysokiej klasy produktów do nadzoru wizyjnego, oferuje nowy iskrobezpieczny punkt kamerowy **MAXIMUS MMX**, który wyróżnia się wyjątkowo korzystnym i dotychczas niespotykanym stosunkiem jakości do ceny.

MMX znakomicie nadaje się do efektywnego nadzoru wizyjnego i kontrolowania procesów w trudnych warunkach, tzn. w miejscach, w których obecność gazów lub łatwopalnego pyłu może doprowadzić do wybuchu. Urządzenie ma certyfikaty ATEX/IECEx (Exd IIB, Ext IIIC) i UL Hazardous Location for America and Canada (Class I, Zone 1, Class I, Div. 2 and Class II, Zone 21, Class II Div. 2).

Jego instalacja jest maksymalnie uproszczona i tania dzięki niewielkiej wadze i rozmiarom. Ponadto wielofunkcyjny uchwyt umożliwia montaż na dowolnej powierzchni – na ścianie, suficie lub gzymsie, stosownie do potrzeb. W celu ograniczenia czasu i kosztu montażu dostępne są różne typy okablowania.

Moduł kamerowy w urządzeniu MMX wytwarza obraz o rozdzielczości Full HD, umożliwia zdalną regulację ogniskowej i obejmuje zakresem obserwacji kąt 90 stopni. Zapewnia najwyższą jakość obrazu w strumieniu wizyjnym skompresowanym metodą H.264/AVC. Jego obudowa jest wykonana w całości z odpornej na korozję stali nierdzewnej AISI316L o klasie szczelności IP66/68. Może być zasilany ze źródła o napięciu 24 V_{AC} lub 24 V_{DC} albo metodą PoE Plus.

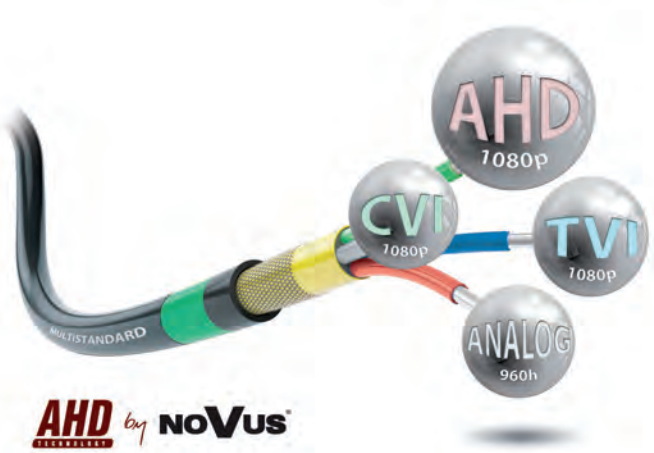
Zastosowanie punktu kamerowego MAXIMUS MMX jest rozwiązaniem korzystnym ze względu na koszt. Można go wykorzystać w nadzorze wizyjnym w najtrudniejszych warunkach – na lądzie, morzu i w przemyśle.

Bezpośr. inf. Videotec
Tłumaczenie: Redakcja

Kamera Novus Multistandard AHD
typu rybie oko

Kamera NVAHD-2DN5103MV/IR-1 generuje sygnały wizyjne w różnych standardach. W celu poszerzenia zakresu zastosowań kamer AHD marki **NOVUS** wszystkie wprowadzane modele kamer będą kompatybilne z rejestratorami pracującymi w natywnym standardzie AHD 1080p oraz zgodnie ze standardami TVI i CVI 1080p. Pozwoli to na współpracę z większością rejestratorów analogowych o rozdzielczości HD (1080p), które są dostępne na rynku. Dodatkowo kamery AHD Multistandard będą wstecznie zgodne z systemami analogowymi o niskiej rozdzielczości.

Kamera została wyposażona w obiektyw typu rybie oko o ogniskowej 1,6 mm i przysłonie 1,4. W połączeniu z przetwornikiem CMOS 1/2.9" firmy Sony generuje ona obraz o szerokim kącie widzenia równym 178 stopni. Umożliwia to eliminację martwych stref i obserwację całego pomieszczenia za pomocą jednej kamery. Kamera może być sterowana z wykorzystaniem protokołu COAX, więc można konfigurować ją za pomocą kompatybilnego rejestratora AHD.



Kamera Novus Multistandard AHD może być stosowana na zewnątrz budynków dzięki możliwości pracy w temperaturach od -30°C do 40°C oraz klasie szczelności IP55. Rekomendowane miejsca instalacji to m.in. balkony, loggie, wykusze chroniące przed deszczem.

Bezpośr. inf. Patryk Gańko
AAT HOLDING

System EntraPass KANTECH zintegrowany
z centralami alarmowymi DSC Power Neo

Z przyjemnością informujemy, że nowa rodzina central alarmowych **DSC Power Neo** została zintegrowana z systemem **KANTECH EntraPass w wersji V7**. Elementem łączącym oba systemy jest moduł TCP/IP o symbolu TL280(R).

Moduł TL280(R) jest połączony z centralą alarmową osobnym przewodem (dostarczanym wraz z modułem). Z systemem EntraPass może być skomunikowany na dwa sposoby.

Pierwszy wariant to połączenie TL280(R) z kontrolerami KT-1, KT-400 lub KT-NCC. Posiadają one porty RS232, które mogą być wykorzystywane między innymi do tego celu. Druga możliwość to połączenie z portem RS232 (lub wirtualnym interfejsem COM) komputera z zainstalowanym programem bramki EntraPass Gateway. Program EntraPass w obu ww. rozwiązaniach udostępnia opcję integracji poprzez IP. Taki sposób komunikacji modułu TL280(R) z systemem EntraPass spowoduje, że integracja będzie jeszcze łatwiejsza niż dotychczas.

Opisane połączenie gwarantuje dwukierunkową wymianę danych pomiędzy centralą alarmową a systemem EntraPass. Dzięki temu możliwe są następujące funkcje: pełna kontrola i wizualizacja na mapach obiektu stanu czujek systemu alarmowego, włączanie w dozór/wyłączanie z dozoru podsystemu (za pomocą czytnika i karty lub przez operatora w menu kontekstowym na mapie) oraz zarządzanie kodami użytkowników.

Z systemem EntraPass można zintegrować wiele central alarmowych DSC Power Neo i zarządzać nimi z jednego stanowiska operatora systemu KD. Centrale mogą być równocześnie obsługiwane za pomocą fizycznych klawiatur rozmieszczonych w wybranych punktach obiektu oraz skomunikowane ze stacją monitorowania. Integracja central alarmowych z systemem EntraPass przynosi korzyści i ułatwia zarządzanie systemem zabezpieczeń elektronicznych.

Bezpośr. inf. Ryszard Sobierski
AAT HOLDING

AHD TECHNOLOGY by NOVUS®

MULTI STANDARD

MULTISTANDARD – JEDNA KAMERA WIELE MOŻLIWOŚCI PODŁĄCZENIA

AAT HOLDING S.A.
PRODUCENT I DOSTAWCA ELEKTRONICZNYCH SYSTEMÓW ZABEZPIECZENIA MIENIA
www.aat.pl

Maksymalna ochrona portu lotniczego
dzięki połączeniu zaawansowanych rozwiązań firm Crisma Security i Videotec

Crisma Security, firma, która specjalizuje się w projektowaniu systemów zabezpieczeń przeznaczonych do użycia w miejscach o szczególnym przeznaczeniu, zintegrowała swój **Navtech Radar** z głowicami **PTZ ULISSE THERMAL RADICAL** produkowanymi przez firmę **Videotec**, twórcę profesjonalnego sprzętu do nadzoru wizyjnego.

Ta kombinacja zaawansowanych technologii daje w efekcie wyjątkowe i elastyczne rozwiązanie umożliwiające kontrolowanie dużych obszarów infrastruktury krytycznej.

Navtech Radar to innowacyjny system radarowy pracujący na falach milimetrowych. Pomaga chronić zabezpieczane miejsca przed intruzami i odznacza się dużym stopniem zautomatyzowania wykonywanych czynności i niezawodnością działania.

Navtech Radar może automatycznie wykryć intruza w promieniu maksymalnie 1000 m, zarówno w dzień, jak i w nocy, a także w każdych warunkach pogodowych (m.in. gdy pada deszcz albo śnieg, we mgle). Każdy czujnik radarowy w ciągu sekundy wykonuje jeden 360-stopniowy skan obserwowanego obszaru. Dzięki temu urządzenie może wskazać położenie każdego obserwowanego obiektu (np. pojazdu, człowieka) na tym obszarze, a także określić szybkość i kierunek jego przemieszczania się. Cały obserwowany obszar może być podzielony na mniejsze podobszary, w których czujniki mogą określić różne parametry wykrywanych obiektów na podstawie różnych kryteriów, w zależności od przyjętych procedur wykrywania nienormalnych sytuacji, zasad alarmowania etc.

Wykrywanie obiektów z użyciem radaru jest połączone z obserwowaniem ich za pomocą termowizyjnej kamery PTZ typu ULISSE THERMAL RADICAL, która dzięki wysokiej precyzji mechanicznej, wysokiej czułości i szerokiemu polu widzenia jest w stanie tworzyć obrazy ludzi i innych wykrytych obiektów w zupełnej ciemności lub w złych warunkach pogodowych.

Zintegrowany system złożony z urządzeń Navtech Radar i ULISSE THERMAL RADICAL może działać w ten sposób, że Navtech Radar naprowadza głowicę ULISSE i wykorzystuje oprogramowanie w celu przesłania dokładnie określonych współrzędnych celu, który ma być śledzony natychmiast i w sposób ciągły. Umożliwia to obserwację wykrytego obiektu w czasie rzeczywistym.

Działanie radaru Navtech Radar i kamery termowizyjnej zainstalowanej w głowicy ULISSE THERMAL RADICAL jest perfekcyjnie zsynchronizowane. Współrzędne określane prze Navtech Radar służą do szybkiego naprowadzania głowicy ULISSE na śledzony cel.

Ciągłe wyostrzanie obrazu jest możliwe dzięki wyjątkowemu systemowi automatycznej regulacji ogniskowania, który umożliwia szybkie dokonywanie właściwych ustawień ostrości.

Zintegrowany system utworzony przez firmy Crisma Security i Videotec został przetestowany z pomyślnym rezultatem na jednym z włoskich lotnisk, gdzie zapewnił wysoki poziom zabezpieczenia, monitorując wrażliwe obszary.

System szybko informuje o obecności intruzów. Umożliwia ciągłą obserwację w czasie rzeczywistym oraz wykrywanie i ustalanie miejsca znajdowania się celu na obserwowanym obszarze na bieżąco. Umożliwia również wczesną, szybką interwencję oraz zapewnia pełne i ciągłe objęcie obserwacją elementów infrastruktury znajdujących się na zewnątrz.

Bezpośr. inf. Videotec
Tłumaczenie: Redakcja

Advanced
The Standard in Fire Systems

NAJWYŻSZY POZIOM OCHRONY

SYSTEM SYGNALIZACJI POŻARU

Axis EN

ZETO-PROJEKT

WYŁĄCZNY PARTNER FIRMY ADVANCED NA TERENIE POLSKI:
P.U.I. ZETO-PROJEKT SP. Z O. O.
UL. KOLEJOWA 20, 55-075 BIELANY WROCŁAWSKIE
WWW.ZETO-PROJEKT.COM.PL
BIURO@ZETO-PROJEKT.COM.PL

Dynamiczna zmiana parametrów zapisu i graficzne wyszukiwanie materiału

dzięki nowym rejestratorom marki NOVUS z serii 6000

Rejestratory marki **NOVUS** należące do nowej serii 6000 zapewniają obsługę kamer o rozdzielczości do 5 Mpx (2592x1944) dla każdego strumienia i metodę kodowania H.264/H.264+/H.265. Wszystkie strumienie mogą być nagrywane z prędkością do 30 kl./s niezależnie od rozdzielczości. Modele 4- i 8-kanałowe zostały wyposażone w przełącznik sieciowy służący do zasilania kamer i komunikacji z nimi.

Na szczególną uwagę zasługują dwie funkcje rejestratorów z nowej serii. We współpracy z kamerami serii 3000 urządzenia te dynamicznie zmieniają parametry pierwszego strumienia wizyjnego w zależności od aktywności alarmowej, tzn. w przypadku detekcji ruchu lub aktywacji wejścia alarmowego kamery mogą zwiększyć rozdzielczość, prędkość transmisji i poprawić jakość rejestrowanego materiału. Dzięki temu możliwe jest optymalne zarządzanie dostępną przestrzenią dyskową.

Drugą praktyczną funkcją rejestratorów jest możliwość wyszukiwania materiału poprzez stopniowe zawężanie kolejnych przedziałów czasowych. Na podstawie pojedynczych zdjęć z poszczególnych kamer operator zawęża zakres czasowy, jakiego będzie dotyczyć przeszukiwanie danych, do wybranego miesiąca, dnia, godziny i minuty.

Rejestratory umożliwiają zdalny dostęp w trybie na żywo i odtwarzanie materiału archiwalnego z użyciem urządzeń przenośnych (smartfonu, iphone'a) – za pomocą aplikacji SuperLive Plus w trybie P2P, tzn. bez konieczności przekierowywania portów oraz posiadania publicznego adresu IP.

Bezpośr. inf. Patryk Gańko
AAT HOLDING

VENO

szereg innowacyjnych zmian

Do wersji 1.10.34 oprogramowania **VENO** służącego do wizualizacji i integracji systemów zabezpieczenia mienia wprowadzonych zostało wiele pozytywnych zmian. Stworzyliśmy zupełnie nowy moduł o nazwie *Grupy i operatorzy*, przeznaczony do zarządzania uprawnieniami do dostępu do funkcji systemu. Dzięki niemu można w szybki i intuicyjny sposób zmieniać uprawnienia do określonych elementów widocznych na panelach dla całej grupy, czyli dla wielu operatorów jednocześnie.

Kolejną nowością w oprogramowaniu jest opcja *Stos zdarzeń bieżących*, która zastępuje wysłużony *Dziennik zdarzeń*. Umożliwia ona szybką obsługę zdarzeń zachodzących w wielu systemach. Dzięki nowej szacie graficznej oraz takim opcjom jak filtrowanie czy przejście do elementu na panelu operator jest w stanie skutecznie reagować na zaistniałe sytuacje alarmowe.

Istotnym udogodnieniem dla osób, które z programem VENO integrują urządzenia marki **DSC Power Neo**, jest wprowadzenie opcji edycji uprawnień użytkowników z poziomu interfejsu VENO. Do dyspozycji są m.in. możliwość wprowadzenia kodu użytkownika, kodu alarmu w sytuacji przymusu czy też kodu dostępu do odpowiedniej partycji.

Aktualna wersja oprogramowania oraz dodatkowe informacje dotyczące programu VENO są dostępne na stronie *www.venois.pl.*

Bezpośr. inf. Piotr Olejarz
AAT HOLDING

INTEGRACJA SYSTEMÓW BEZPIECZEŃSTWA

JEDNO OPROGRAMOWANIE – WIELE SYSTEMÓW
JEDEN CEL: EFEKTYWNE ZARZĄDZANIE OBIEKTEM

AAT HOLDING S.A.
PRODUCENT I DOSTAWCA ELEKTRONICZNYCH SYSTEMÓW ZABEZPIECZENIA MIENIA
www.aat.pl

Konferencja WiseNet STAR 2017
podsumowanie

29 marca br. w Centrum Olimpijskim w Warszawie odbyła się jubileuszowa, piąta edycja konferencji **WiseNet STAR 2017** (poprzednio Samsung STAR).

W imieniu polskiego zespołu **Hanwha Techwin Europe** uczestników i gości powitał Sławomir Szlufik, Country Manager – Poland & Baltics. W konferencji wzięło udział 220 osób.

Na samym wstępie prowadzący podkreślili, że sukcesem firmy Hanwha jest tworzenie rozbudowanej, wielopoziomowej sieci partnerskiej. Firmy uczestniczące w programie partnerskim Hanwha STEP mają zapewnioną pięcioletnią gwarancję na produkty. Stanowi to podstawę bezpiecznej i stabilnej polityki marketingowej wobec inwestorów i użytkowników końcowych.

W części technicznej konferencji zaprezentowane zostały najnowsze kamery z serii WiseNet X, w których zastosowano procesor DSP piątej generacji. Duża moc obliczeniowa tego procesora umożliwia nie tylko uzyskanie obrazu o bardzo wysokiej jakości, ale także realizację funkcji analizy treści obrazu już w kamerze. Dzięki takiemu rozwiązaniu można odciążyć serwery systemowe oraz uzyskiwać bardzo szybką reakcję na wydarzenia zachodzące na danym obszarze. Wszystkie funkcje analityczne są dostępne bez jakichkolwiek dodatkowych opłat czy licencji.

Równie ciekawe są funkcje alarmowe, w których do wykrywania niebezpiecznych sytuacji wykorzystana została analiza dźwięku. Kamery mają wbudowane mikrofony i na podstawie analizy sygnału akustycznego są w stanie odróżnić dźwięk wystrzału czy panicznego krzyku od normalnego tła akustycznego, z jakim mamy do czynienia w miejscach publicznych.

Zastosowanie wydajnego procesora WiseNet 5 umożliwiło znaczną poprawę dynamiki obrazu w stosunku do wcześniejszych rozwiązań. Poszczególne klatki wyjściowego strumienia wizyjnego są tworzone na podstawie aż czterech klatek składowych. W ten sposób osiągnięta została dynamika równa 150 dB, co na współczesnym rynku wizyjnych systemów dozorowych stanowi swoisty rekord.

Usprawniono także metody kompresji i techniki strumieniowania danych wyjściowych z kamer. Kompresja metodą H.265 w połączeniu z techniką WiseStream II pozwalają na redukcję przepływności oraz potrzebnego miejsca w rejestratorach wizyjnych o 75% w stosunku do metody H.264.

Bardzo istotnym usprawnieniem najnowszych kamer z serii WiseNet jest zastosowanie żyroskopowej stabilizacji obrazu. Jest to metoda pozwalająca niemal zupełnie wyeliminować wpływ drgań konstrukcji wsporczych, na których zamocowane są kamery. Ma to bardzo istotne znaczenie w systemach służących do obserwacji ruchu ulicznego, podczas którego samochody, tramwaje i inne ciężkie pojazdy są źródłem silnych

drgań. Metoda żyroskopowa jest o tyle skuteczniejsza od metod optycznych, że system reaguje na faktyczne drgania, a nie na zmiany w obrazie spowodowane przez te drgania.

W części konferencji dotyczącej produktów zaprezentowane zostały nowe kamery WiseNet z serii P. Mają one rozdzielczość 12 Mpix i mogą wytwarzać obraz w formacie 4K. Model PTZ jest wyposażony w obiektyw zmiennoogniskowy o krotności 20x, sprzężony optomechanicznie z oświetlaczem pracującym w podczerwieni, który ma zasięg 200 m. Oświetlacz modyfikuje kąt promieniowania w zależności od chwilowej długości ogniskowej obiektywu.

Model panoramiczny ma pole widzenia równe 180 stopni i zastosowano w nim cztery oddzielne przetworniki obrazu. Dostępny jest także inny model panoramiczny – o podobnej konstrukcji, lecz mający pole widzenia równe 360 stopni. W obu przypadkach wynikowy obraz jest otrzymywany przez połączenie odpowiednio obrobionych czterech obrazów składowych.

Model hemisferyczny z obiektywem typu „rybie oko" o polu widzenia równym 360 stopni został zaprojektowany z myślą o obserwacji obiektów handlowych. Ma on funkcje analityczne pozwalające zliczać klientów, kontrolować ich ruch, tworzyć mapy cieplne etc.

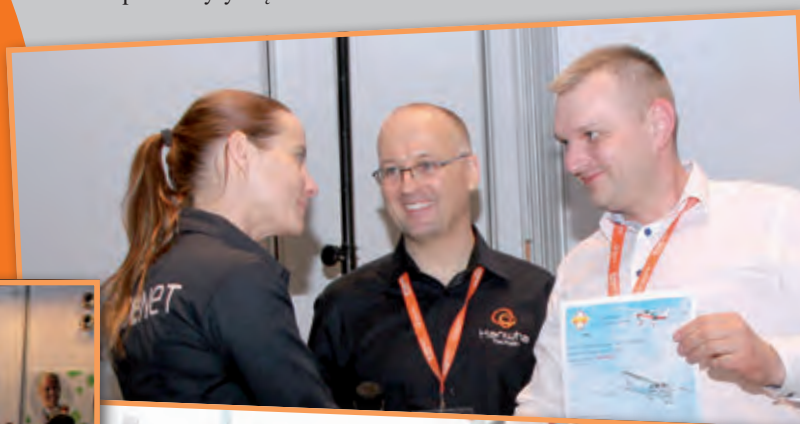
Zaprezentowane zostały także nowe rejestratory obrazów z serii X i P. W celu zapewnienia redundancji zapisu rejestratory mogą być łączone w grupy zgodnie z zasadą n+1, to znaczy n rejestratorów roboczych i jeden zapasowy. W razie awarii jednego z rejestratorów roboczych jego rolę przejmuje rejestrator zapasowy, co odbywa się bez udziału personelu obsługującego system.

Innym sposobem na podwyższenie stopnia niezawodności systemu jest użycie kart SD umieszczonych w kamerach. W przypadku awarii sieci IP strumienie danych są rejestrowane w kamerach i przenoszone do rejestratorów natychmiast po naprawie.

Dużym zainteresowaniem uczestników konferencji cieszyły się urządzenia mobilne z certyfikatami dopuszczającymi je do użycia na kolei. Przykładem może być rejestrator typu SRM-872, który dodatkowo ma jeszcze certyfikaty dopuszczające go do użycia w obiektach NATO.

W części konferencji poświęconej oprogramowaniu systemowemu zaprezentowany został pakiet SSM w różnych wersjach – znane i popularne wersje SSM Professional i Enterprise, wersja SSM Transportation przeznaczona do wykorzystania w kolejnictwie i transporcie, wersja SSM Retail dostosowana do obiektów handlowych, w których prowadzona jest sprzedaż detaliczna, SSM Banking dla banków i SSM City do wykorzystania w miejskich systemach monitorowania wizyjnego.

Zaprezentowany został także nowy system do rozpoznawania tablic rejestracyjnych pojazdów. Innowacja polega na tym, że kontrolowane pojazdy mogą poruszać się z dużą prędkością, do 120 km/h, zaś tablice rejestracyjne mogą zawierać znaki pisane cyrylicą.



Na konferencji głos zabrał także gość specjalny – Peter McKee (z działu Business Development Europe firmy Veracity UK), który omówił urządzenia z serii Veracity Coldstore. Są to rozbudowane rejestratory dyskowe, w których zastosowano innowacyjną metodę bezpośredniego sterowania głowicami w napędach HD, tak aby zapis odbywał się w uporządkowany sposób, bez konieczności częstej zmiany ustawienia głowic. Przekłada się to na znaczne wydłużenie żywotności dysków, bardzo znaczne zmniejszenie zużycia energii i obniżenie temperatury pracy rejestratora. Przykładowo 15-dyskowy model umieszczony w obudowie o wysokości 3U pobiera tylko 60 W mocy w przypadku pełnej obsady dysków.

Spotkanie zakończyło się losowaniem nagród, wśród których był np. przelot szybowcem. Zwycięzcom gratulujemy, a polskiemu zespołowi Hanwha Techwin Europe życzymy pomyślności i sukcesów.

Redakcja

Zapraszamy do obejrzenia fotorelacji na stronie www.zabezpieczenia.com.pl.

MOBOTIX Innovation Roadshow 2017
podsumowanie

W dniu 12 kwietnia odbyła się w Warszawie pierwsza konferencja z cyklu **MOBOTIX Innovation Roadshow 2017**. Jej uczestnicy mieli okazję zapoznać się z najnowszymi kamerami z serii Mx6, które w istocie stanowią połączenie dwóch niezależnych modułów optycznych z silnym procesorem obrabiającym strumienie wizyjne.

Na spotkaniu położono duży nacisk na prezentację kamer termowizyjnych, których użycie znacznie usprawnia ochronę perymetryczną rozległych obiektów.

Ponadto wyświetlono krótki film pokazujący proces produkcji i testowania urządzeń MOBOTIX. Warto zwrócić uwagę na podejście firmy MOBOTIX do zagadnień związanych z kompresją strumieni wizyjnych. Twórcy oprogramowania za cel postawili sobie możliwość uzyskania dostępu do każdej klatki wizyjnej, co może mieć kluczowe znaczenie w przypadku wykorzystania materiału wizyjnego do celów sądowych, dlatego MOBOTIX nie stosuje popularnych metod różnicowych, takich jak H.265.

Podczas spotkania swoje wyroby zaprezentowały firmy współpracujące z MOBOTIXEM, takie jak Wavestore i QNAP.

Redakcja

Zapraszamy do obejrzenia fotorelacji na stronie www.zabezpieczenia.com.pl.

Milestone Partner Open Platform Days
podsumowanie

W dniu 29 marca br. w warszawskim hotelu Golden Tulip odbyła się konferencja w ramach **Milestone Partner Open Platform Days**. Wzięło w niej udział kilkunastu dostawców sprzętu i oprogramowania do wizyjnych systemów dozorowych oraz niemal setka zaproszonych gości. Elementem łączącym wszystkie wystąpienia i prezentacje była otwarta platforma **Milestone**, dzięki której systemy różnych producentów mogą być integrowane i łączone w spójną całość.

Podczas poszczególnych prezentacji można było dostrzec bardzo znaczny rozwój oprogramowania do identyfikacji osób na podstawie zarejestrowanych obrazów twarzy. Takie oprogramowanie było przedmiotem wielu prezentacji.

Bardzo ciekawy wykład na temat warunków pracy dysków twardych w wizyjnych systemach dozorowych wygłosił przedstawiciel firmy Western Digital. Nie mniej ciekawa była prezentacja firmy QNAP poświęcona jednostkom pamięci masowej z dyskami WD.

Mimo iż spotkanie trwało od rana do późnego popołudnia, większość słuchaczy nie opuściła sali wykładowej, co świadczy o randze imprezy.

Andrzej Walczyk
Redakcja

SPIN Extra 2017 – podsumowanie

W dniach 15–16 marca 2017 r. w Hotelu Aquarius w Kołobrzegu odbyło się Spotkanie Projektantów Instalacji Niskoprądowych – **SPIN Extra 2017**. Organizatorem była firma **Lockus**. Wydarzenie umożliwiło podzielenie się wiedzą i nawiązanie kontaktów. Wzięło w nim udział ponad 210 uczestników: projektanci, producenci, dystrybutorzy i branżowi eksperci. Prelekcje wygłosiło 25 prelegentów, a 28 firm zaprezentowało swoje rozwiązania na stoiskach wystawienniczych. Program wydarzenia wzbogaciły dwa panele eksperckie.

W trakcie dwudniowego spotkania omówiono nowinki techniczne z zakresu rozwiązań niskoprądowych. Wśród partnerów tegorocznej, północnej edycji znaleźli się:

– Złoci Partnerzy: BKT Elektronik, Dahua Technology, Hikvision, Pulsar, QNAP z Western Digital,
– Srebrni Partnerzy: ABB, ATEN, BCS, Bosch, BT Electronics, Corning Optical Communication, Impakt z PowerWalker, Polon-Alfa, Polvision, Promise Technology z AxxonSoft, ROGER, TP-Link, Veracomp z Extreme Networks, WILKA,
– Brązowi Partnerzy: Ambient System, Extron Electronics, MERAWEX, MKJ, SafeKey, SALTO Systems.

Prelegenci omówili standardy i dobre praktyki związane z projektowaniem bezpiecznej infrastruktury teleinformatycznej w środowisku medycznym, projektowanie współczesnych sieci komputerowych oraz praktyczne zastosowanie inteligentnej analizy obrazu w projektach komercyjnych. Zaprezentowane zostały także innowacyjne techniki monitorowania, najnowsze rozwiązania z zakresu elektronicznych depozytorów

kluczy i przedmiotów, nowe zasilacze do systemów zabezpieczeń, przełomowe techniki ochrony, rejestracji i archiwizacji materiału wizyjnego oraz wiele innych.

Wiedzą ekspercką z uczestnikami podzielili się Marcin Cisek ze Szkoły Głównej Służby Pożarniczej, który omówił scenariusze pożarowe dotyczące obiektów wielkopowierzchniowych, oraz Piotr Zychowicz ze Stowarzyszenia Budowniczych Telekomunikacji, który mówił na temat praktycznego podejścia do aktualnych wymagań formalno-prawnych dotyczących projektowania i budowy instalacji telekomunikacyjnych w budynkach.

Uczestnicy otrzymali pakiet materiałów firmy Linearic oferującej kompleksowe zaopatrzenie w urządzenia audio, systemy, kable i akcesoria potrzebne do instalacji AV.

Spotkanie umilił wieczorny bankiet i część integracyjna. Na scenie wystąpili finaliści telewizyjnych talent shows Must Be the Music i Mam Talent – Dziubek Band.

Zachęcamy do obejrzenia zdjęć ze SPIN Extra 2017: *http://bit.ly/2o6MPRR*.

Zapraszamy do udziału w kolejnej edycji SPIN-u. Jesienią tego roku odbędzie się ona na południu Polski. Szczegóły na temat 15. Spotkania Projektantów Instalacji Niskoprądowych już wkrótce!

Bezpośr. inf. Edyta Marek
Lockus

Konferencja
Różne typy obiektów i sposoby ich zabezpieczenia
podsumowanie

Firma **EBS** już od siedmiu lat organizuje spotkania branżowe. Początkowo były przeznaczone tylko dla jej największych klientów. Obecnie wśród słuchaczy są wszystkie agencje ochrony powiązane z siecią dystrybucji produktów firmy EBS oraz firmy zainteresowane poruszaną tematyką. Tegoroczna konferencja EBS i Orange zgromadziła blisko 200 osób z 78 firm.

Ta edycja była wyjątkowa. Agenda konferencji nie tylko obejmowała najważniejsze problemy i zagadnienia dotyczące ochrony w obecnych realiach, ale również wskazywała rozwiązania i kierunki rozwoju.

O wysoki poziom merytoryczny tegorocznej konferencji zadbali eksperci, m.in. z Auchan Polska, McDonald's, Raiffeisen i Pekao. Partnerzy – Orange, Hikvision, Protect oraz DMSI – zaprezentowali swoje produkty.

Jednym z celów konferencji *Różne typy obiektów i sposoby ich zabezpieczenia* było spotkanie się dostawców rozwiązań technicznych i usług z ich potencjalnymi klientami.

Celem firmy EBS, będącej pomysłodawcą i organizatorem wydarzenia, jest wywieranie pozytywnego wpływu na branżę zabezpieczeń w Polsce, tym bardziej, że wkrótce nastąpią zmiany prawne i technologiczne, które jej dotyczą.

Wystąpienia naszych prelegentów były ciekawe, a niektóre wzbudziły wiele emocji i sprowokowały do dyskusji.

Serdecznie dziękujemy za patronat nad naszą konferencją stowarzyszeniu Polski Związek Pracodawców Ochrona, magazynom branżowym *a&s Polska* i *Zabezpieczenia* oraz firmie SASMA.

Bezpośr. inf. EBS

Zapraszamy do obejrzenia fotorelacji na stronie: www.zabezpieczenia.com.pl.

TEMAT NUMERU

Trendem dominującym we współczesnych systemach zabezpieczeń jest integracja rożnych technik wykrywania intruzów oraz dążenie do ograniczenia ruchu osobowego na terenie chronionych obiektów. Coraz trudniej stwierdzić, gdzie kończy się system kontroli dostępu, a zaczyna wizyjny system dozorowy lub system sygnalizacji włamania, gdyż wszystkie te techniki przenikają się wzajemnie i tworzą jedną, spójną całość. Wiele firm ma oddziały rozsiane po wszystkich zakątkach świata. Pojawia się problem ujednolicenia zabezpieczeń i działania na wspólnej platformie softwarowej. Znacznym metamorfozom uległy zwykłe mechaniczne klucze i zamki drzwiowe, które obecnie stanowią składnik zabezpieczeń elektronicznych. Wszystkie te zagadnienia są omówione w najnowszym numerze naszego pisma.

Redakcja

czytaj więcej

NOWE PRODUKTY W SYSTEMACH KONTROLI DOSTĘPU I ROZWIĄZANIA DLA HOTELI

Interkomy IP firmy 2N w dystrybucji firmy Arpol

Asortyment oferowanych przez firmę **Arpol** urządzeń do systemów zabezpieczeń został poszerzony o rodzinę **Interkomów 2N Helios IP**.

2N Helios IP Vario oraz modułowy 2N Helios IP Verso to modele o zaawansowanych funkcjach i estetycznym wyglądzie, przeznaczone do zastosowania w budynkach rezydencjonalnych oraz biurach o wysokim standardzie. Dwa modele do zadań specjalnych, odporne na uszkodzenia mechaniczne (IK10) i warunki pogodowe (IP69K), to 2N Helios IP Force oraz alarmowy 2N Helios IP Safety. Przykładowe miejsca ich zastosowania to zakłady przemysłowe oraz punkty alarmowe przy autostradach i w przestrzeni miejskiej. Dostępne są także dwa prostsze modele – 2N Helios IP Base oraz 2N Helios IP Uni, wykorzystywane głównie w jednorodzinnych budynkach mieszkalnych. Do rodziny modeli 2N Helios IP należą także dwa urządzenia w wersji OEM – 2N Audio Kit i 2N Video Kit, które umożliwiają przekształcenie istniejącej instalacji domofonowej w nowoczesny system IP.

Interkomy IP 2N wykorzystują najnowsze osiągnięcia techniki w dziedzinie bezpieczeństwa i łączności. Są w nich stosowane kamery HD zgodne ze specyfikacją ONVIF. Połączenia telekonferencyjne są zestawiane z użyciem protokołu SIP. Umożliwia to wykorzystanie smartfonów jako terminali odbiorczych w systemach interkomowych.

Firma Arpol jako oficjalny dystrybutor urządzeń marki 2N TELEKOMUNIKACE zapewnia pełne wsparcie przed- i posprzedażowe, szkolenia handlowe oraz techniczne, a także serwis gwarancyjny i pogwarancyjny.

Bezpośr. inf. Arpol
tel. 61 84 62 100
info@arpol.pl

Nowe systemy MAP z serii 5000 marki Bosch

Systemy sygnalizacji włamania i napadu są ważnym ogniwem w systemach zabezpieczeń. W związku z tym firma **Bosch** oferuje dwa nowe produkty – **MAP 5000 S i MAP 5000 SC** – dostosowane do małych i średnich instalacji, np. w szkołach, małych biurach i sklepach czy w galeriach sztuki. Wprowadzone wcześniej, starsze systemy MAP 5000 są przeznaczone do zabezpieczania większych obiektów, takich jak lotniska czy centra handlowe, a zatem nowe produkty stanowią uzupełnienie oferty.

MAP 5000 SC ułatwia umożliwia komunikację ze stacjami monitorującymi za pośrednictwem zintegrowanego urządzenia do przesyłu alarmów przez sieć IP lub łącze GPRS. MAP 5000 S nie ma takiego zintegrowanego komunikatora alarmowego. Jest przeznaczony do współpracy z systemem zarządzania budynkiem zawierającym zewnętrzne urządzenie do powiadamiania o alarmach w miejscowym centrum sterowania. Oba nowe systemy są kompatybilne z urządzeniami peryferyjnymi MAP m.in. klawiaturami, modułami i czujkami, i są skalowane (maksymalnie 600 adresów i jeden moduł LSN ze 127 elementami magistral). Dzięki modularnej strukturze mogą zostać rozbudowane, gdy zmienią się wymagania (maksymalnie 500 partycji i 1000 użytkowników). MAP 5000 S i MAP SC są sterowane za pomocą dwóch wielojęzycznych dotykowych interfejsów użytkownika.

Bezpośr. inf. Bosch Security Systems

Sprawdź, kto stoi przed drzwiami

Videodomofon dla budynków wielorodzinnych

- do 25 mieszkań
- opcjonalny moduł czytnika kart Mifare
- opcjonalny moduł czytnik linii papilarnych (do 3000 użytkowników)

VTH1550CH
Monitor wewnętrzny dotykowy 7”

VTO2000A-B
Moduł przycisków abonenckich
IP54, IK07

VTO2000A-R
Moduł czytnika kart Mifare
13,56 MHz
IP54, IK07

VTO2000A-K
Moduł klawiatury numerycznej
IP54, IK07

VTO2000A-F
Moduł czytnika linii papilarnych
IP54, IK07

CE FC ISO 9001:2000

www.dahuasecurity.com/pl

Dahua Technology Poland Sp. z o.o.
ul. Salsy 2, 02-823 Warszawa
tel. +48 22 395 74 00, fax +48 22 395 74 10
e-mail: biuro.pl@global.dahuatech.com
www.dahuasecurity.com/pl

Bosch Remote Services
przyszłość nowoczesnych systemów przeciwpożarowych

Dzięki najnowszemu zestawowi usług firmy **Bosch** dla zarządzających wieloma systemami przeciwpożarowymi w różnych lokalizacjach klient może uzyskać stałe zdalne wsparcie techniczne i większą wydajność swojego systemu przy jednoczesnym ograniczeniu kosztów konserwacji i obsługi administracyjnej. Zdalne usługi firmy Bosch wspomagają zdalne monitorowanie, konserwację i obsługę sprzętu do wykrywania pożarów.

Remote Connect – bezpieczne zdalne połączenie internetowe poprawiające wydajność pracy i umożliwiające integratorom systemów zdalny podgląd odpowiednich instalacji. Pozwala ono lepiej planować, dostarczać i raportować usługi. Bezpieczne połączenie zdalne obejmuje serwis, usuwanie usterek i łatwą konfigurację w ciągu 30 minut. Usługa jest dostosowana do płynnej integracji z systemem RPS.

Remote Maintenance – usługa wykorzystująca połączenie Remote Connect, polegająca na dostarczaniu w czasie rzeczywistym danych dotyczących systemów przeciwpożarowych w formie cyfrowej i graficznej, a także narzędzi do analizy danych w celu przeprowadzenia konserwacji systemu. Dzięki tej usłudze skuteczność obsługi serwisowej zwiększa się o co najmniej 25%. System umożliwia tworzenie podczas testowania szczegółowej dokumentacji konserwacji z wykorzystaniem zoptymalizowanego interfejsu zainstalowanego na tablecie, a historia serwisowania jest zapisywana w portalu, w którym udostępniane są usługi Remote Services. Ponadto usługa umożliwia połączenie z centralą podczas konserwacji systemu.

Remote Alert – usługa umożliwiająca otrzymywanie natychmiastowych powiadomień wysyłanych z zainstalowanych systemów przeciwpożarowych poprzez SMS i e-mail. Dzięki niej możliwe jest szybkie podjęcie działań zapobiegawczych. Mogą z niej skorzystać integratorzy i właściciele firm.

Opisane usługi umożliwiają zarządzanie wieloma systemami przeciwpożarowymi w rożnych lokalizacjach, stałe zdalne wsparcie techniczne i wyższą wydajność przy jednoczesnym ograniczeniu kosztów konserwacji i obsługi administracyjnej. Usługi Remote Services firmy Bosch wspomagają zdalne monitorowanie, a także ułatwiają konserwację i obsługę sprzętu do wykrywania pożarów.

Bezpośr. inf. Bosch Security Systems

Bezprzewodowy wideodomofon
firmy Dahua Technology

Firma **Dahua Technology**, światowy lider w dziedzinie nowatorskich rozwiązań z dziedziny zabezpieczeń, wprowadziła na polski rynek **wideodomofony IP** pracujące z użyciem zarówno sieci kablowej Ethernet, jak i bezprzewodowej Wi-Fi.

Parametry Wi-Fi stacji bramowej **VTO2111D-WP** mogą być w prosty sposób ustawione z użyciem kablowego złącza ethernetowego. Tak przygotowana stacja może być zainstalowana natynkowo przy bramie lub drzwiach wejściowych i wymaga jedynie doprowadzenia zasilania. Stację wyposażono w kamerę o rozdzielczości 1 MP oraz szerokokątny obiektyw o ogniskowej 2,2 mm. Moduł ma wbudowany czytnik kart Mifare. Całość jest zamknięta w estetycznej obudowie o wysokiej klasie szczelności.

Zastosowanie stacji bramowej VTO2111D-WP może być dwojakie. Można ją obsługiwać poprzez aplikację mobilną,

bez potrzeby używania monitora, lub lokalnie, z wykorzystaniem wewnętrznego monitora.

W pierwszym przypadku sygnał dzwonienia dociera poprzez Internet do aplikacji mobilnej abonenta, który może zobaczyć, kto stoi przed drzwiami, porozmawiać z tą osobą i ewentualnie otworzyć jej drzwi.

W drugim przypadku sygnał dzwonienia jest wysyłany zarówno do telefonu komórkowego abonenta, jak i do odpowiednio skonfigurowanego monitora dotykowego VTH5221D o przekątnej 7", który ma nie tylko funkcje wideodomofonu – może być zintegrowany z wewnętrznym systemem alarmowym (sześć wejść i jedno wyjście) oraz zapewnia podgląd obrazów z kamer IP, które pracują w sieci wewnętrznej. Gdy monitor zostanie dodatkowo wyposażony w opcjonalną kartę micro SD, osoby dzwoniące będą mogły zostawić wiadomość głosową i wizyjną.

Oba urządzenia, tzn. stacja bramowa oraz monitor, mogą być zasilane metodą PoE przez złącze sieciowe.

W sumie dostajemy system prosty w konfiguracji i instalacji, łatwy w obsłudze, a co najważniejsze spełniający oczekiwania wymagającego użytkownika.

Więcej informacji znajduje się na stronie:
www.dahuasecurity.com.

Bezpośr. inf. Wojciech Pawlica
Dahua Technology Poland

Dwuprzewodowe wideodomofony Dahua

Firma Dahua Technology, światowy lider w dziedzinie systemów bezpieczeństwa, wprowadziła na polski rynek nowatorskie **wideodomofony IP**, w których do zasilania i transmisji danych służy jedna para przewodów.

Jednostka bramowa **VTO2000A-2** umożliwia komunikację z monitorem **VTH1550CHW-2** bez potrzeby stosowania dodatkowych urządzeń. Zastosowano w niej kamerę HD o rozdzielczości 1,3 MP z obiektywem o ogniskowej 2,8 mm, dzięki czemu obraz odznacza się bardzo dobrą jakością, a kąt widzenia jest szeroki. Wandaloodporna obudowa wykonana z nierdzewnej stali może być montowana zarówno natynkowo jak i podtynkowo. Zastosowany monitor VTH1550CHW-2 ma ekran dotykowy o przekątnej 7" i rozdzielczości 800×480 pikseli. Do jednostki można włożyć kartę micro SD, na której osoba dzwoniąca za pomocą panelu bramowego może pozostawiać wiadomości głosowe lub wizyjne. Monitor może również pełnić funkcję małej centrali alarmowej z sześcioma wejściami i jednym wyjściem. Intuicyjne menu umożliwia łatwe skonfigurowanie centrali alarmowej zgodnie z potrzebami użytkownika. Dodatkowy moduł **VTNC3000A** daje możliwość podłączenia czterech urządzeń (do wyboru są bramofony lub monitory) z użyciem pojedynczych par przewodów oraz zapewnia zdalny dostęp do systemu poprzez Internet. Mobilna aplikacja umożliwia obserwację obrazu z kamery umieszczonej w bramofonie, połączenie głosowe i wizyjne z bramofonem, zdalne otwarcie drzwi i wysyła powiadomienia o próbach dzwonienia. Na monitorze wideodomofonu można obserwować także obrazy z kamer IP dostępnych w wewnętrznej sieci. Podsumowując – poza standardowymi funkcjami wideodomofonu użytkownik otrzymuje system alarmowy oraz sieciowy system dozoru wizyjnego. Możliwość zdanego odbierania połączeń, kontroli stanu drzwi oraz ich odryglowania sprawia, że zaproponowane rozwiązanie jest bardzo funkcjonalne.

Więcej informacji znajduje się na stronie:
www.dahuasecurity.com.

Bezpośr. inf. Wojciech Pawlica
Dahua Technology Poland

Zestawy do instalacji systemów
kontroli dostępu RACS 5

Firma **ROGER** wprowadziła do swojej oferty zestawy złożone z metalowej obudowy, zasilaczy oraz modułów elektronicznych, które są potrzebne podczas instalacji systemów kontroli dostępu w najpopularniejszych konfiguracjach.

Dostępność tych zestawów upraszcza zarówno zaprojektowanie, jak i zainstalowanie systemu. Minimalizuje prawdopodobieństwo popełnienia błędów wynikających z nieprawidłowego doboru sprzętu.

Do oferty wchodzą zestawy z kontrolerem dostępu przeznaczone do obsługi od 1 do 4 przejść, a także zestawy rozszerzeń, które umożliwiają dodanie kolejnych przejść do systemu. Zestawy przystosowano zarówno do systemów współpracujących z czytnikami serii MCT, oryginalnie przeznaczonymi do pracy w systemie RACS 5, jak i do systemów współpracujących z czytnikami Wieganda. Zestawy zostały zoptymalizowane pod kątem ekonomicznego doboru obudów oraz zasilaczy. W ich skład wchodzą powszechnie dostępne obudowy firmy

Pulsar oraz zasilacze impulsowe firmy Mean Well. Instalatorzy mogą również dobrać elementy zestawu samodzielnie.

Bezpośr. inf. ROGER

Winkhaus zarządza dostępem w fabryce okien

Firma Domel, producent okien i drzwi z Łomży, dołączyła w tym roku do grona użytkowników innowacyjnego systemu dostępowego **Winkhaus blueSmart**. Rozwój firmy, inwestycja w nowy zakład i związane z tym zmiany organizacyjne wymogły zakup systemu, który w znacznym stopniu ułatwia zarządzanie firmą. Rozwiązania techniczne oferowane przez firmę **Winkhaus** spełniły wymagania inwestora, ponieważ umożliwiły dalszy rozwój i optymalizację procesów produkcyjnych. W obiekcie zainstalowano 38 wkładek elektronicznych, dwa czytniki online i 220 kluczy blueSmart.

Elektroniczne wkładki i klucze Winkhaus blueSmart działają w tzw. sieci wirtualnej – komunikują się ze sobą w momencie włożenia klucza do wkładki. Ten krótkotrwały kontakt wystarcza, by przekazać dane z wkładki, czyli informacje o wejściach do danego pomieszczenia, do klucza. Z kolei z klucza do wkładki przesyłane są aktualne, dotyczące uprawnień do dostępu dane pobrane z czytnika, który znajduje się przy wejściu do budynku. Czytnik jest połączony z komputerem administratora, na którym zainstalowane jest oprogramowanie do zarządzania systemem kontroli dostępu w obiekcie. W nim wprowadzane są wszelkie zmiany w strukturze uprawnień do dostępu do pomieszczeń.

– Poszukiwaliśmy rozwiązania, które umożliwi wygodne administrowanie złożonym systemem kontroli dostępu – powiedział Paweł Kicun, dyrektor zarządzający i prokurent firmy Domel. – *System blueSmart spełnił nasze oczekiwania dzięki możliwości łatwego administrowania za pomocą oprogramowania blueControl. Nie ma konieczności ręcznego programowania każdej wkładki z osobna, za to jest możliwość nadawania indywidualnych uprawnień do dostępu do określonych pomieszczeń na określony czas. Chcieliśmy, żeby wybrany system był wystarczająco innowacyjny i spełnił wymagania użytkowe w naszej nowej siedzibie. Istotne okazały się takie cechy systemu jak bezprzewodowy sposób wymiany danych w trakcie użytkowania kluczy wyposażonych w elektroniczne chipy, w których, oprócz praw dostępu, zapisywane są dane sczytane z wkładek elektronicznych. Te dane są przekazywane innym wkładkom oraz wprowadzane do oprogramowania. Oczywiście nie bez znaczenia jest możliwość natychmiastowej blokady dostępu w przypadku zgubienia klucza. Ważna dla nas była także elastyczność systemu, który w przyszłości pozwoli na integrację z siecią komputerową, urządzeniami biurowymi i systemem rejestracji czasu pracy.*

Bezpośr. inf. Kamilla Los-Marszałek
Winkhaus Polska

Elementy automatyki budynkowej
w systemie kontroli dostępu RACS 5

Podstawowym przeznaczeniem systemu **RACS 5** jest kontrola dostępu, ale ma on także funkcje automatyki budynkowej. Do realizacji tych funkcji mogą służyć standardowe kontrolery z serii **MC16-PAC** służące do fizycznej kontroli dostępu, a także specjalnie przystosowane kontrolery automatyki budynkowej z serii **MC16-BAC**.

W obu wersjach kontrolerów funkcje automatyki budynkowej realizuje się za pośrednictwem tzw. węzłów automatyki. Węzeł automatyki to stan logiczny w pamięci kontrolera, który może być sterowany przez użytkownika i wpływać na stan kontrolera, w szczególności na stan innego węzła automatyki. Stan węzła automatyki może być replikowany na liniach wyjściowych i w ten sposób służyć do sterowania systemami lub urządzeniami wykorzystywanymi w budynku (sterownikami rolet, oświetleniem, klimatyzacją, ogrzewaniem, wentylacją i innymi). Dzięki wielofunkcyjności zarówno każdej z linii wejściowych, jak i każdej z linii wyjściowych można przypisać kilka lub nawet kilkanaście różnych funkcji, co umożliwia realizację własnych, złożonych funkcji logicznych. Stanem węzła automatyki można sterować ręcznie (za pomocą przycisku funkcyjnego, przycisku podłączonego do linii wejściowej lub przez wydanie zdalnej komendy po zalogowaniu się za pomocą czytnika) lub automatycznie, wykorzystując harmonogramy czasowe.

Do sterowania węzłami automatyki, jak również do prezentacji ich stanów posłużyć może graficzny panel dotykowy **MD70** lub terminal z wbudowanym wyświetlaczem **MCT88M-IO**. Uruchomienie i wyłączenie węzła automatyki może nastąpić po włożeniu lub wyjęciu uprawnionej karty do czytnika **MCT82M-IOCH**. Dzięki dostępności bezprzewodowych ekspanderów wejść/wyjść (RACS 5 AIR) możliwe jest sterowanie automatyką w miejscach nie mających połączenia przewodowego z kontrolerem.

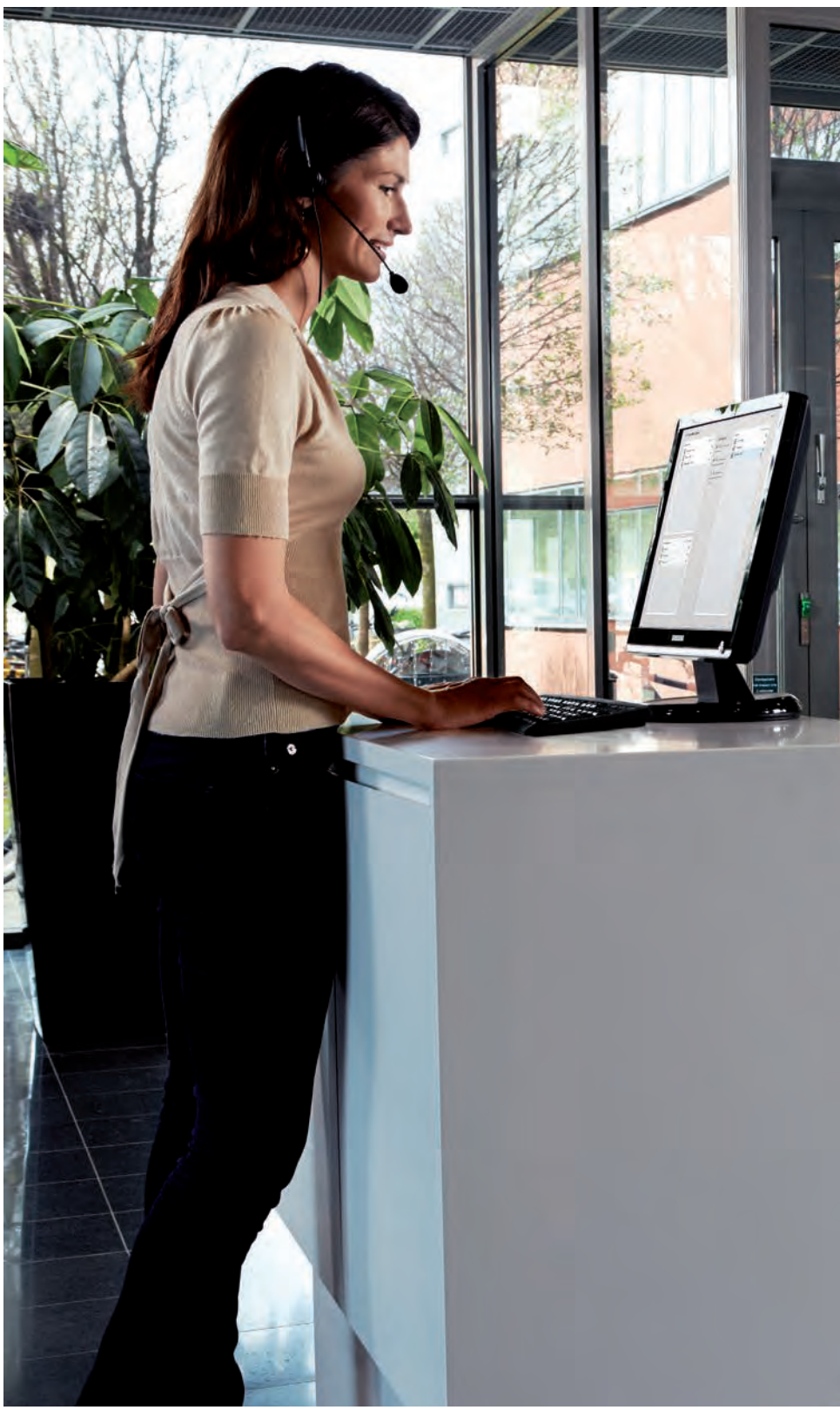
Elementy automatyki systemu RACS 5 mogą być zintegrowane z innymi systemami (np. BMS) za pomocą tzw. serwera integracji, który udostępnia programowe metody sterowania węzłami automatyki oraz sprawdzenia ich aktualnego stanu.

Bezpośr. inf. ROGER

Axis Communications proponuje przyszłościowe rozwiązania do kontroli dostępu

Axis Communications

W 1996 roku firma Axis, lider na rynku sieciowych systemów wizyjnych, wprowadziła na rynek pierwszą na świecie kamerę sieciową. Od tego czasu stale tworzy innowacyjne produkty, przyczyniając się do podniesienia poziomu bezpieczeństwa milionów osób na całym świecie. Dbając o nieprzerwany rozwój, opracowaliśmy bazujące na protokole IP rozwiązania z dziedziny kontroli dostępu, które cechują się otwartością i elastycznością oraz stanowią alternatywę dla systemów tradycyjnych



Produkty firmy Axis Communications przeznaczone do systemów kontroli dostępu sprawdzają się w wielu różnych zastosowaniach – od identyfikacji osób i kontroli wejść po zaawansowane zarządzanie dostępem i integrację z innymi systemami zarządzania bezpieczeństwem. Obecnie posiadamy w naszej ofercie takie urządzenia sieciowe jak kontrolery drzwi, domofony, czytniki kart oraz moduły przekaźnikowe wejścia i wyjścia.

Tradycyjne systemy kontroli dostępu mają scentralizowane moduły sterujące, które są połączone kablami z urządzeniami peryferyjnymi. Mają zamkniętą strukturę i nie można ich łatwo rozbudowywać. Wraz z sieciowym kontrolerem drzwiowym AXIS A1001 pojawiły się alternatywne, skalowalne rozwiązania do systemów kontroli dostępu.

Sieciowy kontroler drzwi AXIS A1001 umożliwia zastosowanie dowolnie wybranego rodzaju systemu kontroli dostępu. Ta dowolność wynika z zasady działania sieci IP. Podobną drogę rozwoju przeszły niegdyś wizyjne systemy dozorowe firmy Axis. Otwarty interfejs API Axis ułatwia dobór sprzętu oraz oprogramowania pochodzącego od firm partnerskich.

Fot. 1. Oznaczenia kolorami ułatwiają uruchomienie systemu z kontrolerem AXIS A1001

Co równie istotne, umożliwia też integrację z innymi sieciowymi systemami bezpieczeństwa oraz aplikacjami pochodzącymi od różnych producentów bez konieczności stosowania kosztownych urządzeń pełniących funkcję mostu łączącego systemy.

AXIS A1001 jest produktem umożliwiającym stworzenie systemu kontroli dostępu z wykorzystaniem rozwiązań innych producentów. Sprawdzi się zarówno w małych instalacjach, jak i w zaawansowanych systemach bezpieczeństwa.

Konwencjonalne produkty i systemy kontroli dostępu są zwykle projektowane i optymalizowane pod kątem dużych instalacji, obsługujących setki drzwi i tysiące uwierzytelnień, a oprogramowanie bywa trudne w obsłudze. Z drugiej strony na rynku jest popyt na produkty do instalacji małych, zwykle obejmujących nie więcej niż kilkanaście drzwi. Mając to na uwadze, opracowaliśmy platformę Entry Manager, która powstała, aby umożliwić sprawne zarządzanie dostępem właśnie w niewielkich instalacjach. Jest to gotowe do użycia rozwiązanie dla małych i średnich przedsiębiorstw. Można je zastosować w miejscach, w których potrzebne są tylko podstawowe funkcje związane z kontrolą dostępu, np. w biurach i sklepach. W przypadku większych systemów wymagających kompleksowego programowania otwarty interfejs aplikacji AXIS A1001 umożliwia partnerom firmy Axis (*Application Development Partners*) tworzenie systemów kontroli dostępu dostosowanych do specyficznych wymagań konkretnych użytkowników.

Fot. 2. Sieciowy kontroler drzwi AXIS A1001

Dzięki okablowaniu strukturalnemu oraz oznakowaniu poszczególnych połączeń kolorami urządzenia Axis można łatwo zainstalować. Wykorzystanie zasilania metodą PoE upraszcza okablowanie i zmniejsza koszty instalacji systemu.

Uruchomienie systemu kontroli dostępu, którego elementem jest kontroler drzwiowy AXIS A1001, jest proste dzięki asystentowi konfiguracji i wcześniej wspomnianym złączom z oznaczeniami barwnymi. Sieciowy kontroler drzwiowy AXIS A1001 jest przystosowany do instalacji nad sufitem podwieszanym. Obudowa urządzenia jest wykonana z materiału spełniającego wymogi normy UL2043 dotyczącej testów pożarowych, określającej warunki wydzielania ciepła oraz dymu dla produktów zainstalowanych w zamkniętych przestrzeniach. W czasie pożaru następuje stopienie obudowy, a nie jej spalenie.

Inteligentne rozwiązania IP pozwalają na decentralizację systemu, która ułatwia jego instalację oraz późniejszą rozbudowę. Zastosowanie platformy AXIS Entry Manager eliminuje konieczność użycia centralnego modułu sterującego bądź serwera. Każdy sieciowy kontroler drzwiowy AXIS A1001 jest wyposażony w pamięć i procesor. Nadmiarowe dane systemowe, a także dane dotyczące uwierzytelnień oraz konfiguracji podlegają automatycznej synchronizacji we wszystkich urządzeniach w systemie.

Umożliwiamy całkowicie swobodną rozbudowę systemu. Czynności tak proste jak objęcie kontrolą kolejnych drzwi w małej firmie lub tak zawiłe jak integracja z wizyjnym systemem dozorowym w rozległym obiekcie są możliwe do zrealizowania z użyciem kontrolera AXIS A1001.

Axis Communications

@saltosystems

Nowy XS4 One:

INSPIRUJĄCA INNOWACJA

Witamy w nowym wymiarze kontroli dostępu!

Technologia – Zamek elektroniczny z wbudowaną najnowszą technologią bezprzewodowej kontroli dostępu.

Dostęp mobliny – Wbudowana technologia Wireless oraz klucz mobilny JustIN Mobile.

Wszechstronność – Nieskończone możliwości w dopasowaniu do wszelkiego typu drzwi.

Funkcjonalność – Bezpieczny i łatwy w użytkowaniu system bez klucza mechanicznego.

Design – Nowoczesny styl, który podkreśla estetykę całego obiektu.

Niezawodność – Gwarancja jakości SALTO Systems.

SALTO SYSTEMS
Tel.: +48 609 01 7777
Email: info.pl@saltosystems.com
www.saltosystems.pl

SALTO
inspiredaccess

Pięciogwiazdkowy standard bezpieczeństwa w pięciogwiazdkowym hotelu

Bosch Security Systems

Bezpieczeństwo gości i pracowników to priorytet w każdym hotelu. Hotelarstwo to jednak bardzo konkurencyjna branża, więc systemy zabezpieczeń powinny wyróżniać się nie tylko funkcjonalnością, ale też prostą obsługą i atrakcyjną ceną. Modułowe i skalowalne systemy wykorzystujące standardowe techniki sieciowe umożliwiają integrację, która poprawia bezpieczeństwo, a jednocześnie obniża koszty instalacji, wdrożenia i eksploatacji

Fot. Hotel Sheraton (fot. Bosch)

W celu zapewnienia wyższego standardu bezpieczeństwa swoim gościom oraz pracownikom hotel Sheraton w Warszawie postanowił wymienić dotychczasowy system sygnalizacji pożarowej na system firmy Bosch. Dodatkowo partner Boscha, firma ASD, zainstalowała dźwiękowy system ostrzegawczy zintegrowany z nowymi centralami sygnalizacji pożarowej.

Pięciogwiazdkowy Sheraton Warsaw Hotel jest jednym z najbardziej prestiżowych hoteli w stolicy Polski. Jest usytuowany przy Placu Trzech Krzyży i dzieli go zaledwie kilka kroków od Łazienek Królewskich, zabytkowej ulicy Nowy Świat oraz budynku Sejmu. Hotel był także tymczasową siedzibą kilku zagranicznych ambasad.

Po wielu latach eksploatacji dotychczasowego systemu sygnalizacji pożarowej dyrektor ds. technicznych i menedżer ds. bezpieczeństwa hotelu podjęli decyzję o jego wymianie oraz zainstalowaniu innowacyjnego i modułowego systemu łączącego w sobie najwyższej klasy system sygnalizacji pożarowej z inteligentnym dźwiękowym systemem ostrzegawczym. Biuro projektowe Instel MM, ściśle współpracujące przy tym projekcie z firmą instalacyjną ASD, zaprojektowało system sieciowy z dwiema centralami sygnalizacji pożarowej Bosch Modular Fire Panel Series 5000 obsługiwanymi za pomocą zdalnych klawiatur Remote Keypad Series 5000. W pokojach gości, salach, biurach i częściach ogólnodostępnych zainstalowano ponad 1600 automatycznych optycznych i termicznych czujek dymu oraz prawie 200 ręcznych przycisków alarmowych. System Bosch BIS (Building Integration System) zapewnia wizualizację pożaru i umożliwia płynną integrację oraz centralne sterowanie centralami sygnalizacji pożarowej oraz dźwiękowym systemem ostrzegawczym.

W celu zapewnienia szybkiej i bezpiecznej ewakuacji w razie alarmu firma ASD, integrator systemu, zainstalowała cyfrowy dźwiękowy system nagłośnieniowo-ostrzegawczy PRAESIDEO z 29 wzmacniaczami. Obsługuje on ponad 1500 głośników i umożliwia przekaz doskonale zrozumiałych instrukcji ewakuacyjnych w różnych częściach budynku.

W warszawskim hotelu Sheraton działa teraz zintegrowany system zabezpieczeń wykorzystujący system BIS oraz otwartą, modułową architekturę, zapewniający ekonomiczną eksploatację i umożliwiający rozbudowę w przypadku konieczności dostosowania go do nowych wymagań w przyszłości.

Zintegrowane systemy zabezpieczeń są teraz znacznie łatwiejsze do wdrożenia niż kiedykolwiek dotąd. Po raz pierwszy w historii rosnąca liczba technik sieciowych, takich jak Ethernet czy IP, pozwala stworzyć wspólną, ekonomiczną platformę techniczną dla wszystkich rodzajów zabezpieczeń. Informacje z kamer, czujek pożarowych lub kontrolerów drzwi można łączyć za pomocą popularnych protokołów, takich jak TCP/IP, oraz standardowych interfejsów, np. OPC. Ponadto ten rodzaj integracji umożliwia obsługiwanie kilku aplikacji za pomocą współdzielonego, uniwersalnego i indywidualnie konfigurowanego interfejsu użytkownika – najczęściej w systemach działających pod kontrolą Windows i w standardowych przeglądarkach internetowych. Wykorzystanie standardowych technik sieciowych jako bazy dla wszystkich systemów zabezpieczeń umożliwia operatorowi korzystanie z aplikacji w obrębie istniejącej infrastruktury IT, bez konieczności tworzenia dwóch oddzielnych infrastruktur. W oczywisty sposób przyczynia się to do zmniejszenia wydatków – zarówno inwestycyjnych, jak i eksploatacyjnych.

Bosch Security Systems

Bramki uchylne SpeedStile FL^{S} w budynkach biurowych

Anna Sadłowska

Czy możliwe jest odpowiednie zabezpieczenie budynku bez negatywnego wpływu na jego wygląd?

Fot. 1. Bramki uchylne SpeedStile FL^{S} zapewniają wysoki poziom bezpieczeństwa przy przepustowości wynoszącej 40 osób na minutę

Wdrożenie systemu kontroli dostępu w budynku biurowym nie sprowadza się tylko do montażu bramek oraz przepuszczania osób z identyfikatorami. Inwestorzy oczekują nie tylko walorów użytkowych, ale także wizualnych, a więc rozwiązań pasujących do architektury danego budynku. Firma Gunnebo jako dostawca urządzeń zabezpieczających mienie oferuje duży wybór bramek SpeedStile, których wygląd jest dostosowany do nowoczesnych i eleganckich obiektów. Urządzenia do kontroli dostępu dopasowuje się już na etapie projektowania budynku biurowego, gdyż stanowią integralne części lobby, recepcji oraz wejść.

Podobnie było w przypadku firmy IMMOFINANZ – największego inwestora na stołecznym rynku biurowym. Instalacja nowych bramek w budynkach IMMOFINANZ była powiązana z wprowadzeniem nowej marki biurowej – myhive. Warto podkreślić, że dla osób odpowiedzialnych za promocję tej marki bardzo ważny był wygląd lobby, który ma istotny wpływ na postrzeganie obiektu biurowego jako całości.

Aby spełnić wymagania estetyczne i zarazem zapewnić najwyższy poziom bezpieczeństwa w lobby czterech warszawskich obiektów myhive (myhive Brama Zachodnia, myhive Park Postępu, myhive Crown Point oraz myhive Equator) wykorzystano nowoczesne bramki Gunnebo SpeedStile. Analizowanie natężenia ruchu osób oraz ustalanie, kiedy uprawnione osoby wchodziły do danych pomieszczeń i kiedy z nich wychodziły, pomogło określić zachowania użytkowników. Miało to decydujący wpływ na wybór odpowiednich bramek uchylnych. Wybrano bramki FL^{s}, które umożliwiają przejście uprawnionych osób bez opóźnień, więc można uniknąć niezadowolenia użytkowników powodowanego koniecznością oczekiwania w kolejce. Wspomniana analiza obejmowała dwie pory dnia: godziny poranne oraz popołudniowe, gdyż wtedy odnotowywanych jest najwięcej przejść przez bramki.

Zastosowane bramki uchylne SpeedStile FL^{s} mają zarówno walory użytkowe, jak i walory estetyczne. Dodatkowym atutem bramek jest ich przepustowość, która pozwala na kontrolowane przejście 40 osób na minutę przy zapewnieniu najwyższego poziomu bezpieczeństwa. Bramki wykrywają próby nieuprawnionego przejścia za osobą uprawnioną i próby przejścia w przeciwną stronę.

Fot. 2. Bramki uchylne SpeedStile FL^{s} w budynku myhive Crown Point w Warszawie

Anna Sadłowska
Gunnebo Polska

Bezpieczeństwo w hotelach

Piotr Rogalewski

Dla niektórych z nas hotel to drugi dom. Dla mnie również. W hotelu chcemy czuć się komfortowo i bezpiecznie, podobnie jak w domu. Przekonaj się, w jaki sposób można skutecznie zadbać o bezpieczeństwo hoteli i innych obiektów noclegowych, wykorzystując rozwiązania firmy Hanwha Techwin

Monitorowanie

Bogata oferta kamer Hanwha Techwin umożliwia budowę wizyjnych systemów dozorowych, w których uzyskuje się obraz o rozdzielczości od 2 do 12 megapikseli. Najnowsze kamery z serii X z procesorem DSP WiseNet 5 gwarantują najwyższą jakość obrazu. Dzięki funkcji WDR pozwalającej uzyskać obraz o dynamice 150 dB obserwacja mocno oświetlonych wejść do zacienionych obiektów czy przeszklonych przestrzeni nie stanowi problemu. Dzięki bardzo wysokiej czułości matrycy można instalować kamery na zewnątrz obiektów bez konieczności dodatkowego doświetlania. Stabilizacja żyroskopowa gwarantuje obraz o doskonałej stabilności, np. w przypadku kamer zamontowanych na wysokich słupach oświetleniowych. Kompresja metodą H.265 oraz transmisja WiseStream II powoduje redukcję wymaganego pasma o 75% w porównaniu z kompresją H.264 i umożliwia ograniczenie potrzebnej przestrzeni dyskowej.

Fot. 1. Kamera kopułkowa QND-7080R z kompresją H.265

Miejsca, które trzeba obserwować na obrazie o bardzo dużej rozdzielczości, to np. recepcja czy hotelowy bar. To zadania dla kamer serii P. Określenie liczby i rodzaju banknotów przy kasie jest warunkiem właściwej obsługi zgłoszeń reklamacyjnych klienta, a identyfikacja twarzy jest podstawą działań odpowiednich służb, jeśli dojdzie do incydentu wymagającego śledztwa. Funkcja Hallway View (obrót obrazu o 90 lub 270 stopni) gwarantuje efektywną obserwację korytarzy i ciągów komunikacyjnych. Kamery z serii Q sprawdzą się tam, gdzie nie jest wymagana analiza treści obrazu. Niewielkie wymiary, estetyczny wygląd i atrakcyjna cena to ich cechy szczególne.

Kamery należące do serii P, m.in. hemisferyczny model PNF-9010R i czteroobiektywowy, panoramiczny PNM-9020V, nadają się do obserwacji dużych przestrzeni, takich jak hol główny, restauracja czy patio.

Windy także wymagają nadzoru. W nich doskonale sprawdzą się kamery SNV-6012, SNV-L6013 i SNV-L6014RM, z których każda ma małe rozmiary, jest wyposażona w wandaloodporną obudowę (certyfikat IK-10) i szerokokątny obiektyw, a ponadto charakteryzuje się szczególnie dużą odpornością na zakłócenia elektromagnetyczne.

Fot. 2. Kamera XNO-6080R z procesorem DSP serii WiseNet 5

Dzięki analizie treści obrazu kamery z serii X i P wykryją niedozwoloną próbę zmiany pola widzenia, pozostawienie podejrzanego obiektu lub zabranie obiektu chronionego, zbyt długie przebywanie w chronionym miejscu, jazdę pod prąd na parkingu itp. Dzięki analizie dźwięku w kamerach z serii X obsługa zostanie zaalarmowana w przypadku wykrycia dźwięku zgodnego z określonym wzorcem, np. odgłosów tłuczenia szkła, krzyku, eksplozji czy strzałów z broni palnej.

Zapis obrazu zapewniają rejestratory sieciowe. Mogą to być tanie rejestratory 4- i 8-kanałowe (np. QRN-410S), rejestratory 16-kanałowe z wbudowanym przełącznikiem sieciowym i z portami PoE (np. XRN-1610S), a także najbardziej zaawansowane modele 32- i 64-kanałowe (np. XRN-2011 czy PRN-4011). Stabilność i niezawodność, zapis awaryjny, kompresja H.265, długi czas rejestracji i analiza treści odtwarzanego materiału wizyjnego to tylko niektóre ich właściwości i funkcje.

Do komfortowego zarządzania systemem służy oprogramowanie Smart Security Manager (SSM), które w najprostszej wersji jest oferowane całkowicie bezpłatnie. Wykorzystuje ono najnowsze dostępne techniki, m.in. równoległe przetwarzanie obrazu CUDA.

Statystyki

W przypadku takiego obiektu jak hotel istotne są informacje o tym, ile w poszczególnych okresach znajduje się w nim ludzi i w których miejscach przebywają. Funkcja analizy treści obrazu, która jest dostępna w kamerach z serii X i P, pomoże w zdobyciu potrzebnych danych. Funkcja zliczania osób pozwoli łatwo sprawdzić liczbę gości korzystających z baru czy restauracji w określonych godzinach, dzięki czemu można skuteczniej zarządzać dostępnym personelem. Na mapach ciepła (czyli dzięki mapowaniu ruchu) będzie widać, gdzie i w jakich okresach gromadzi się najwięcej osób. Taka wiedza może okazać się bezcenna np. podczas ewakuacji obiektu. Przetworzone dane mogą być automatycznie wysyłane, np. raz dziennie, na podany adres e-mail. Wszystkie funkcje analizy

Fot. 3. Zliczanie osób i mapowanie ruchu w kamerach serii P

treści obrazu są dostępne bez dodatkowych licencji i związanych z nimi kosztów – opłata jest już zawarta w cenie kamer.

Integracje

Obiekt hotelowy jest chroniony także przez systemy ppoż., kontroli dostępu czy SSWiN. Każdy z nich można łatwo zintegrować z wizyjnym systemem dozorowym Hanwha Techwin. Dzięki temu próba nieuprawnionego użycia karty w systemie kontroli dostępu może automatycznie spowodować wyświetlenie obrazu korytarza, na którym ktoś takiej próby dokonuje. Inny przykład to wyświetlenie obrazów z ciągów ewakuacyjnych w momencie wykrycia pożaru przez system ppoż.

Integracja rejestratorów sieciowych Hanwha Techwin z terminalami POS i kasami fiskalnymi umożliwia powiązanie treści paragonów z zarejestrowanymi obrazami. Dzięki temu można np. błyskawicznie wyszukać nagranie na podstawie nazwy sprzedanego towaru, jego ceny, numeru paragonu czy fragmentu numeru karty kredytowej. Ułatwia to rozpatrywanie reklamacji i rozstrzyganie konfliktów.

Możliwa jest także współpraca kamer z systemem parkingowym. Dwa modele kamer z funkcją rozpoznawania tablic rejestracyjnych (SNO-6084R oraz SNO-60985RH) mogą współpracować z rejestratorami sieciowymi i oprogramowaniem SSM. Wyszukanie nagrania z momentu wjazdu albo wyjazdu poszukiwanego auta sprowadza się do wpisania jego numeru rejestracyjnego. Wprowadzenie uprzywilejowanych numerów rejestracyjnych do systemu umożliwia automatyczne otwieranie szlabanu, np. dla pojazdów dostawczych lub obsługi hotelowej.

Informacja, reklama, film

Goście hotelowi docenią poinformowanie o lokalizacji wyjść ewakuacyjnych, godzinach otwarcia poszczególnych stref hotelowych i określonych usługach. Podniesie ono ogólny komfort, a także poziom bezpieczeństwa. Dzięki funkcji MagicInfo Player S3, dostępnej m.in. w 32-calowych modelach SMT-3232A, monitory Hanwha Techwin mogą zapewnić takie informacje, gdyż łączą cechy urządzeń do telewizji dozorowej i nośników informacyjno-reklamowych. Na monitorze mogą być wyświetlane obrazy z kamer dozorowych, ale również informacje i reklamy, a także filmy. Tryb pracy monitora można zmienić zdalnie, przez sieć. Obraz może być wyświetlany w poziomie lub w pionie.

Fot. 4. Monitor SMT-3232A z funkcją MagicInfo Player S3

Obecnie Hanwha Techwin przygotowuje opracowanie dotyczące bezpieczeństwa obiektów hotelowych. Dokument będzie dostępny już wkrótce u naszych autoryzowanych dystrybutorów. Zapraszamy do kontaktu!

Piotr Rogalewski
Hanwha Techwin Europe

WISENET
SAMSUNG

WISENET X

eXtremalna wydajność

- 2**X** szybsze przetwarzanie wideo
- 3**X** więcej pamięci
- dodatkowe gniazdo pamięci SD
- e**X**plozja dynamiki obrazu 150 dB dzięki funkcji WDR
- efektywna kompresja wideo H.265 i technologia WiseStream II

Odkryj więcej na www.WisenetX.com

Hanwha Techwin

System bezprzewodowy RACS 5 AIR w hotelach, biurach i domach

Maciej Kubicki

Komunikacja bezprzewodowa stała się funkcją wielu systemów. Istnieje zapotrzebowanie również na bezprzewodowe systemy kontroli dostępu. W związku z tym firma ROGER przygotowała serię urządzeń bezprzewodowych RACS 5 AIR będących integralnymi częściami systemu kontroli dostępu i automatyki budynkowej RACS 5. Do oferty firmy wprowadzone zostały zamki i okucia bezprzewodowe, zamek szafkowy oraz bezprzewodowe ekspandery wejść i wyjść. Obszar potencjalnych zastosowań urządzeń bezprzewodowych RACS 5 AIR obejmuje m.in. kontrolę dostępu w obiektach hotelowych i biurowych, kontrolę dostępu do szafek pracowniczych oraz bezprzewodową automatykę budynkową

Zastosowanie zamków bezprzewodowych w obiektach hotelowych i biurowych

Zamki RWL-1 i RWL-2 działają w systemie RACS 5 i umożliwiają bezprzewodową kontrolę dostępu. Urządzenia te znajdują zastosowanie głównie w miejscach, w których instalacja okablowania jest kłopotliwa lub konstrukcja drzwi utrudnia montaż zamków przewodowych.

Zamki RWL przygotowano głównie z myślą o obiektach hotelowych oraz biurowych, co nie wyklucza wykorzystania ich w obiektach innych typów. Obydwa zamki umożliwiają kontrolę wejścia do pomieszczenia, natomiast wyjście jest zawsze możliwe dzięki użyciu klamki wewnętrznej. W przypadku modelu RWL-1 sterowanie dostępem odbywa się za pomocą trybem „nie przeszkadzać". Zarówno w przypadku zamka bezprzewodowego RWL-1, jak i okucia RWL-2 istnieje możliwość podłączenia zewnętrznego czujnika otwarcia drzwi. Zamki RWL zasilane są powszechnie dostępnymi bateriami alkalicznymi. Dostęp do baterii jest możliwy jedynie od wewnętrznej strony drzwi. Zamek RWL-1 jest zasilany czterema bateriami AA, które umożliwiają jego pracę przez ok. dwa lata. Zamek RWL-2 jest zasilany czterema bateriami AAA umożliwiającymi pracę przez około jeden rok. Niski stan baterii jest sygnalizowany na zamku oraz w oprogramowaniu zarządzającym systemem. W sytuacjach awaryjnych przejścia kontrolowane przez zamki RWL mogą być otwarte za pomocą tradycyjnego klucza mechanicznego.

Fot. 1. Zamki bezprzewodowe RWL-1 i RWL-2

serwomechanizmu umieszczonego w zamku wewnętrznym montowanym w skrzydle drzwi. Taki zamek ma funkcję automatycznego wysuwania rygla po zamknięciu skrzydła i zawiera czujnik położenia rygla. Funkcja automatycznego ryglowania znacznie podnosi poziom odporności przejścia na próby jego sforsowania lub sabotażu i jest wymagana w obiektach hotelowych.

W zamku RWL-2 serwomechanizm jest umieszczony w szyldzie i służy do uaktywniania klamki, która normalnie nie umożliwia otwarcia drzwi. Zamek RWL-2 odpowiada rozmiarami standardowym zamkom wpuszczanym w skrzydło o rozstawie 72 mm.

Obydwa zamki wyposażono w czytnik kart zbliżeniowych obsługujący karty MIFARE Ultralight, Classic, Plus i DESFire oraz komunikację NFC, dzięki czemu możliwe jest wykorzystanie telefonów z systemem Android w zastępstwie kart zbliżeniowych. Zamki RWL mogą być sterowane z użyciem harmonogramów czasowych, dzięki którym zostaną otwarte o ustalonych porach dnia. Funkcja ta znajduje zastosowanie w obiektach biurowych, gdy wymagany jest swobodny ruch osób w ustalonych porach dnia. W szyldzie wewnętrznym zamka RWL-1 znajduje się dwupozycyjne pokrętło, którego funkcja może być zaprogramowana. W zastosowaniach hotelowych pokrętło to może być wykorzystane do sterowania

Bezprzewodowe systemy kontroli dostępu do szafek i schowków

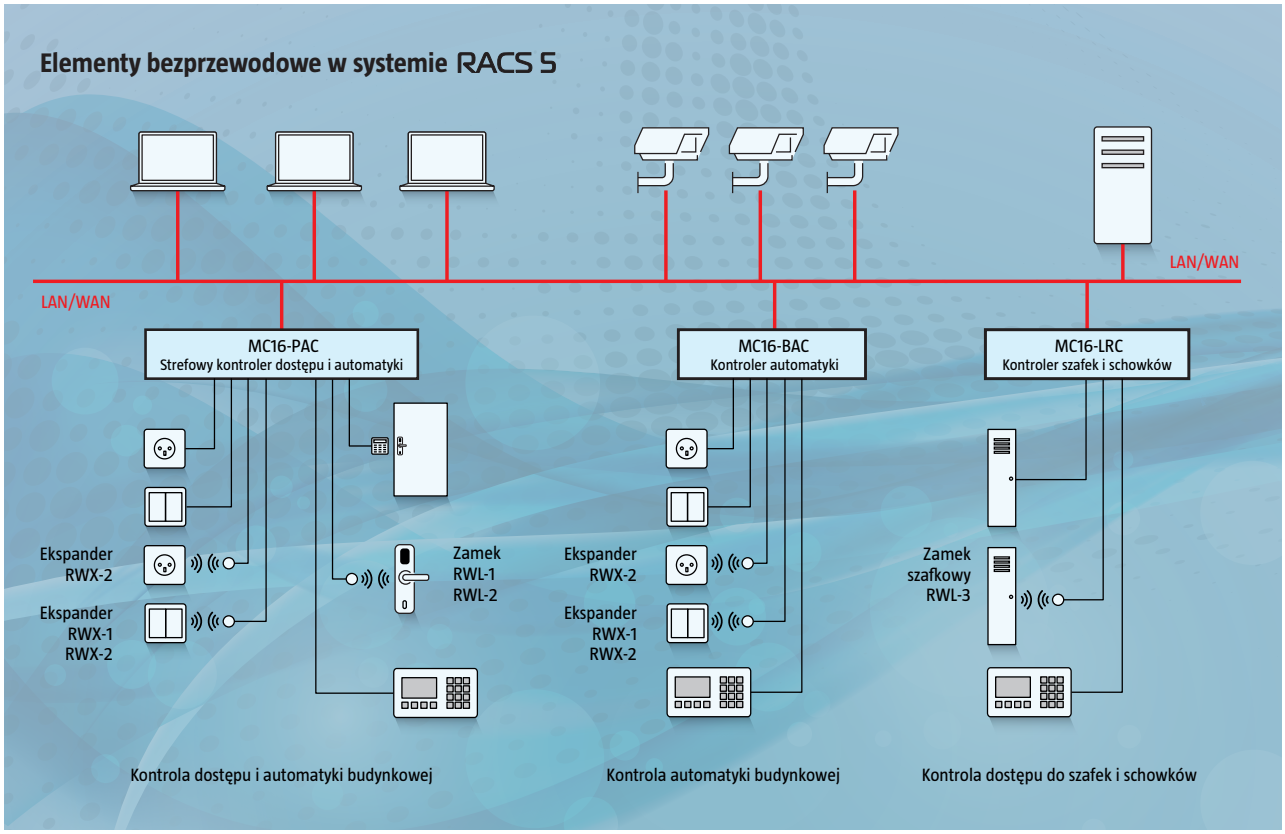
W skład oferowanego systemu RACS 5 AIR wchodzi zamek RWL-3, który umożliwia kontrolę dostępu do wszelakiego rodzaju szafek i schowków. Zamek RWL-3 składa się z panelu przedniego z czytnikiem zbliżeniowym mocowanym na drzwiach szafki lub schowka oraz mechanizmu rygla, który wraz z zasobnikiem na baterie jest instalowany po wewnętrznej stronie drzwi.

Fot. 2. Zamek bezprzewodowy RWL-3

Zamek jest zasilany trzema bateriami AAA, które umożliwiają jego działanie przez jeden rok. Podobnie jak w przypadku zamków RWL-1 i RWL-2, niski stan baterii jest sygnalizowany na czytniku oraz w oprogramowaniu zarządzającym

systemem. Zamek RWL-3 jest wyposażony w czujnik stanu rygla oraz wejście umożliwiające dołączenie czujnika otwarcia. Czytnik kart zbliżeniowych w zamku RWL-3 obsługuje karty MIFARE Ultralight, Classic, Plus i DESFire oraz komunikację NFC.

stując przedstawione ekspandery, pozostałe bezprzewodowe i przewodowe elementy systemu RACS 5 i oprogramowanie systemu kontroli dostępu, można stworzyć system inteligentnego domu o zaawansowanej logice działania.



Rys. 1. Elementy bezprzewodowe systemu RACS 5

Zastosowania w inteligentnym domu

Do zastosowania w inteligentnym domu przeznaczono dwa rodzaje ekspanderów wejść/wyjść, które mają wiele zastosowań i można je zamontować na różne sposoby. Ekspander RWX-1 jest dostosowany do instalacji pracujących pod napięciem 12 V_{DC}. Jest wyposażony w trzy uniwersalne linie wejścia/wyjścia oraz jedną wysokoprądową linię wyjściową przeznaczoną do bezpośredniego sterowania zworą elektromagnetyczną lub elektrozaczepem. Ekspander RWX-2 jest przeznaczony do bezpośredniego sterowania odbiornikami pracującymi pod napięciem 230 V_{AC}. Urządzenie to ma wbudowany zasilacz sieciowy, dwa wejścia sterujące optoizolowane o szerokim zakresie napięć wejściowych (od 5 V_{DC} do 230 V_{AC}) oraz jedno wyjście obsługiwane za pomocą triaka o nominalnej obciążalności 16 A, przeznaczone do sterowania odbiornikiem pracującym pod napięciem 230 V_{AC}. Ekspandery bezprzewodowe mogą być montowane w standardowej puszce elektroinstalacyjnej, na szynie DIN lub na płaskiej powierzchni, np. na obudowie metalowej. Szczególnym przypadkiem montażu ekspandera RWX-2 jest umieszczenie urządzenia w głębokiej puszce elektroinstalacyjnej, bezpośrednio pod gniazdem elektrycznym lub włącznikiem pracującym pod napięciem 230 V_{AC}. Ten sposób montażu umożliwia przekształcenie dowolnego gniazda lub włącznika w element systemu inteligentnego domu. Wykorzy-

Podsumowanie

Bezprzewodowe urządzenia systemu RACS 5 AIR są kolejnymi elementami rozszerzającymi zakres zastosowań systemów kontroli dostępu i automatyki budynkowej RACS 5. Ich dostępność umożliwia instalację systemu również w tych miejscach, gdzie wcześniej, z racji problemów związanych z okablowaniem lub wymaganiami estetycznymi, było to bardzo problematyczne lub wręcz niemożliwe. Urządzenia bezprzewodowe są obsługiwane w systemie RACS 5 na tych samych zasadach logicznych co urządzenia przewodowe i mogą być stosowane razem z nimi nawet w przypadku zastosowania pojedynczego kontrolera dostępu. Choć ceny urządzeń bezprzewodowych są wyższe, brak kosztów okablowania może w wielu przypadkach spowodować, że cała instalacja okaże się tańsza. Zakłada się, że w miarę stopniowego wzrostu kosztów robocizny oraz jednoczesnego spadku cen urządzeń bezprzewodowych coraz częściej będą one wartościową alternatywą dla rozwiązań przewodowych.

Maciej Kubicki
ROGER

Międzynarodowe Targi Poznańskie

Funkcje elektronicznego klucza
Bezprzewodowy system kontroli dostępu Winkhaus

Miron Łukaszczyk

Odpowiednia organizacja i zarządzanie uprawnieniami w systemach kontroli dostępu umożliwia sprawne i bezpieczne funkcjonowanie firm w budynkach. Bez względu na rozmiar obiektu i liczbę korzystających z niego użytkowników kontrola dostępu jest ważna ze względu na ochronę dóbr materialnych oraz bezpieczeństwo pracowników

Mechaniczne systemy z kluczem uniwersalnym (*ang. master key*), które są obecnie stosowane, mają sporo wad. Jedną z nich jest niemożność zachowania odpowiedniego poziomu bezpieczeństwa w przypadku zgubienia klucza. Z reguły klucz używany w takim systemie służy do otwierania wielu pomieszczeń. Mogą być ich dziesiątki, a nawet setki. Jeżeli zostanie zgubiony, trzeba wymienić albo przekodować dużą liczbę wkładek. To kosztowna i czasochłonna operacja, która często okazuje się nieopłacalna. Rozwiązaniem jest zastosowanie elektronicznego systemu kontroli dostępu.

Kontrola dostępu do pomieszczeń

Firma Winkhaus, która od ponad 160 lat jest dostawcą zabezpieczeń mechanicznych, od kilkunastu lat oferuje również innowacyjne i niezawodne elektroniczne systemy kontroli dostępu. Jednym z nich jest blueSmart. W systemie blueSmart

wykorzystane są elektroniczne wkładki, których wymiary są zgodne z wymiarami najczęściej używanych wkładek mechanicznych. Instalacja systemu kontroli dostępu Winkhaus blueSmart sprowadza się do wymiany wkładek we wszystkich drzwiach znajdujących się w obiekcie. Jest to operacja szybka i bezinwazyjna, ponieważ wszystkie wkładki są wyposażone w baterie i nie wymagają kłopotliwego okablowania.

Zaletą wkładek stosowanych w systemie blueSmart jest ich długi czas pracy. Wkładki do drzwi wewnętrznych mogą działać nawet sześć lat, a wkładki do drzwi zewnętrznych nawet dziesięć lat bez konieczności wymiany baterii, w zależności od liczby użyć. System blueSmart to jednak nie tylko wkładki. Dostęp do pomieszczeń uzyskuje się, korzystając z klucza, na którym zapisane są informacje o uprawnieniach dotyczących dostępu. Podobnie jak w systemach mechanicznych, klucz jest wkładany do wkładki i obracany, co powoduje przesunięcie rygla zamkowego. Wkładki blueSmart nadają się więc do każdych drzwi wyposażonych w zamek z klasyczną wkładką profilową.

Klucze blueSmart pełnią w systemie rolę nośników informacji o uprawnieniach dotyczących dostępu. To na podstawie danych zapisanych w kluczu wkładka pozwala bądź nie pozwala na obrót klucza i tym samym odryglowanie lub zaryglowanie zamka. Transmisja danych między kluczem a wkładką jest oparta na technice RFID, w której pasywny klucz korzysta z energii dostarczanej przez zasilaną bateryjnie wkładkę. Klucze użytkowników są więc bezobsługowe.

Sterowanie urządzeniami elektrycznymi

Klucze blueSmart, w założeniu przeznaczone do obsługi wkładek systemowych, mogą pełnić również inne role. Za pomocą swojego klucza użytkownik może obsługiwać także inne systemy i urządzenia. Popularnym uzupełnieniem systemu kontroli dostępu Winkhaus blueSmart są czytniki sterujące urządzeniami elektrycznymi. Za pomocą klucza użytkownik może otwierać szlabany, sterować oświetleniem czy włączyć w dozór system alarmowy.

Elektroniczny klucz blueSmart może być zastosowany również w innych systemach sterowania lub kontroli dostępu, jeżeli potrzebna będzie identyfikacja użytkownika. Wystarczy zadbać o to, by czytnik obcego systemu był zgodny z typem transpondera RFID zastosowanym w kluczu blueSmart. Takim kluczem można np. obsługiwać system rejestracji czasu pracy, sterować windą albo uruchomić jakąś maszynę lub pojazd.

Korzystanie z drukarek

Niezbędnym wyposażeniem każdego biura są urządzenia drukujące. Dostęp do nich również można zabezpieczyć kluczem blueSmart. Aby wydrukować dokument, użytkownik będzie musiał najpierw zalogować się kluczem blueSmart w czytniku umieszczonym przy drukarce. To zapewnia poufność i bezpieczeństwo informacji. Niezależnie od drukowania, również skanowanie dokumentów za pomocą urządzeń kopiujących może

Fot. 1. Aktywny klucz umożliwia otwarcie wkładki, w której rozładowała się bateria. Może także na krótki czas przejąć funkcję klucza użytkownika

być zabezpieczone kluczem blueSmart. Po zalogowaniu pliki zeskanowanych dokumentów zostaną wysłane na wcześniej zapisany adres email właściciela klucza.

Jeśli z jakichś powodów nie jest możliwe wyposażenie obcego systemu w czytnik zgodny z transponderem RFID zastosowanym w kluczu blueSmart, można wyposażyć klucz w dodatkowy, właściwy dla danego systemu transponder. Klucz będzie

Fot. 2. Wkładka elektroniczna Winkhaus blueSmart ma taki sam kształt i wymiary jak najpopularniejsze wkładki mechaniczne dostępne w sprzedaży

więc mógł obsługiwać komponenty systemu blueSmart oraz inne funkcjonujące w obiekcie instalacje, które działają z wykorzystaniem techniki RFID.

Łatwa zmiana praw dostępu

System blueSmart został zaprojektowany z myślą o firmach, instytucjach oraz placówkach oświatowych i medycznych. W takich obiektach naturalna jest częsta zmiana praw dostępu. Oprócz tego możliwe jest zgubienie kluczy. Łatwość i szybkość wprowadzania zmian czy zablokowania kluczy ma zatem decydujące znaczenie. Dzięki wygodnemu i łatwemu w obsłudze oprogramowaniu zarządzanie systemem blueSmart nie sprawia żadnych trudności. Administrator systemu wprowadza na swoim komputerze zmiany, które trafiają do bazy danych na serwerze. Oprogramowanie zapewnia stałą wymianę informacji z czytnikiem aktualizującym klucze. Użytkownicy kluczy mają obowiązek skorzystania z tego czytnika w pewnych odstępach czasu. W ten sposób prawa dostępu są zapisywane na kluczach, a potem przenoszone za ich pomocą do wkładek. Czas ważności klucza, czyli okres, po którym trzeba go ponownie aktywować w czytniku, może być zmieniany.

Aktywowanie klucza za pomocą czytnika polega na zbliżeniu go do tego urządzenia. To wystarcza, by w kolejnym, z góry ustalonym okresie umożliwić użytkownikowi dostęp do wy-

Fot. 3. Czytnik z ekranem dotykowym. Dodatkowe zabezpieczenie wejścia kodem cyfrowym za pomocą czytnika z ekranem dotykowym

branych pomieszczeń. Są jednak sytuacje, w których aktywacja klucza do strategicznych pomieszczeń powinna być dodatkowo zabezpieczona. Można wówczas użyć czytnika z wyświetlaczem, który przy aktywacji określonych kluczy będzie wymagał podania kodu PIN.

Dostęp do mebli i witryn

Kontrola dostępu to nie tylko sterowanie drzwiami i przejściami. Oprócz podstawowych komponentów systemu blueSmart, takich jak wkładki, czytniki i klucze, firma Winkhaus oferuje również zamki elektryczne do wszelkiego rodzaju mebli biurowych. Użytkownik może swoim kluczem obsługiwać np. szafkę odzieżową, kontener z dokumentami czy witrynę z farmaceutykami.

System blueSmart firmy Winkhaus umożliwia komfortowe i elastyczne zarządzanie obiektem, niezależnie od jego wielkości i sposobu funkcjonowania. Bogaty asortyment dostępnych komponentów, możliwość integracji, wysoki poziom bezpieczeństwa i niskie koszty eksploatacji sprawiają, że blueSmart spełnia oczekiwania najbardziej wymagających użytkowników.

Miron Łukaszczyk
Winkhaus Polska

Always precise

Inteligentna kontrola dostępu dla każdego obiektu

Bez kłopotliwej instalacji i remontu

Winkhaus blueSmart to system elektronicznych wkładek z własnym zasilaniem, który pozwala efektywnie zarządzać prawami dostępu w budynku. Za pomocą centralnego czytnika klucze blueSmart komunikują się z oprogramowaniem, tworząc sieć wirtualną. Tu prawa dostępu nadawane użytkownikom są przekazywane do kluczy, które przekazują je dalej do wkładek. Z wkładek klucze przenoszą do oprogramowania historię zdarzeń i dane o stanie baterii. Funkcjonujący w ten sposób system jest niezwykle elastyczny i tani w eksploatacji.

+ system wkładek elektronicznych otwieranych kluczem
+ brak okablowania
+ łatwy i szybki montaż
+ wysoki poziom bezpieczeństwa (IMP klasa 6.2)
+ błyskawiczna, bezkosztowa zmiana dostępu
+ dyskretna stylistyka

Wkładka elektroniczna

Klucz elektroniczny

Danfoss

Program Zarządzania Globalnymi Klientami spółki Nedap pomógł firmie Danfoss wprowadzić spójną politykę bezpieczeństwa dla całej organizacji.

Technologie projektowane przez Danfoss trafiają na szeroki rynek, ponieważ firma zatrudnia ponad 22 500 pracowników oraz zaopatruje przeszło 100 krajów. Uprzednio firma dzieliła się na Danfoss Climate & Energy oraz Danfoss Power Solutions, funkcjonujące w formie kilku niezależnych przedsiębiorstw, podejmujących różne decyzje strategiczne. Dawna strategia ustąpiła miejsca globalnej polityce „jedna firma, jedna droga", którą firma wprowadziła w 2010 r., mając na uwadze takie aspekty jak nieruchomości, bezpieczeństwo fizyczne, a także kontrolę dostępu. Fritz Lorenzen, Senior Security Consultant of Danfoss, oraz Henrik Hansen, Head of Portfolio Management of Danfoss, przedstawiają, jak z powodzeniem zastosowali strategię bezpieczeństwa, a także stworzyli wartościową propozycję poprzez ulepszenie procesów przy mniejszym zużyciu zasobów.

Umożliwienie wprowadzenia strategii globalnej

Zanim spółka Danfoss wprowadziła swoją strategię „jedna firma, jedna droga", decyzje dotyczące nieruchomości, bezpieczeństwa czy też kontroli dostępu podejmowane były niezależnie przez wiele przedsiębiorstw będących częściami składowymi spółki. Dziś jednak obszary te są zcentralizowane i charakteryzują się globalnym podejściem. Poza ustanowieniem nadrzędnego organu, którego zadaniem jest czuwanie nad fizycznym bezpieczeństwem i kontrolą dostępu na całym świecie, firma powołała również menedżera ds. bezpieczeństwa globalnego. Organ ten podejmuje decyzje mające wpływ na całą firmę, dzięki czemu może ona usprawnić fizyczne bezpieczeństwo na globalną skalę.

Potrzeba utworzenia jednego system bezpieczeństwa, który mógłby zagwarantować prosty dostęp do firmy każdemu z jej pracowników stanowiło naturalną kolej rzeczy po uzyskaniu globalnego obrazu w kwestiach takich jak bezpieczeństwo. Oczywistym jest to, że firma potrzebowała nowego dostawcy bezpieczeństwa fizycznego, ponieważ dotychczasowe rozwiązania nie były w stanie tego zapewnić.

W oparciu o trzy kluczowe przesłanki firma przeszła proces starannej selekcji globalnego partnera ds. bezpieczeństwa fizycznego, co zaowocowało wyborem spółki Nedap. Platforma AEOS, oferująca kontrolę dostępu, wykrywanie włamań, nagrania video czy też wykorzystanie przestrzeni na jednej platformie, stanowiła największą atrakcję systemu bezpieczeństwa opartego na oprogramowaniu spółki. Ponadto, sieć partnerów zagranicznych spółki Nedap oraz Program Zarządzania Globalnymi Klientami gwarantują ściśle kontrolowany oraz dostosowany proces wdrażania.

Program Zarządzania Globalnymi Klientami

– Jedną z najistotniejszych przyczyn, dla której wybraliśmy Nedap na swojego partnera ds. systemów bezpieczeństwa jest fakt, że spółka ta wyróżnia się sprawdzonym, ujednoliconym podejściem w kwestii wprowadzenia bezpieczeństwa fizycznego. Chcieliśmy skuteczności, a Program Zarządzania Globalnymi Klientami spółki Nedap nam ją dał – twierdzi Fritz.
– Naszym celem było wprowadzenie szeregu zmian w wewnętrznych strukturach oraz znaczne zwiększenie wydajności. Jednakże poprzez globalne ujednolicenie systemów bezpieczeństwa odkryliśmy zupełnie nową dziedzinę działań, ze względu na co zaczęliśmy poszukiwać takiego partnera, z którym moglibyśmy się konsultować w sprawie całego procesu wdrażania. Jako że Nedap jest firmą o zasięgu globalnym, może nam doradzać oraz zaspokoić nasze potrzeby z dowolnego miejsca na świecie, co wyjaśnia, dlaczego jej model biznesowy jest dla nas tak korzystny. Za każdym razem, gdy mamy projekt do zrealizowania, niezależnie od miejsca, w którym aktualnie się znajdujemy, firma Nedap może bez problemu wyznaczyć partnera instalacyjnego do przejęcia platformy AEOS. Mimo że między nami a spółką Nedap pośredniczą partnerzy instalacyjni, to wciąż spółka Nedap ponosi pełną odpowiedzialność za jakość usług – dodaje Henrik.

Ujednolicone podejście

Program Zarządzania Globalnymi Klientami spółki Nedap był realizowany dla firmy Danfoss przez sztab ekspertów technicznych i ekspertów ds. projektu zatrudnionych w obu firmach. Pozwoliło to na równoczesne wykorzystanie wiedzy Danfoss odnośnie organizacji i strategii firmy oraz doświadczenia spółki Nedap w kontekście bezpieczeństwa i wdrażania projektów globalnych.

Wspólne działania doprowadziły do przekształcenia filozofii bezpieczeństwa, a także ustanowienia globalnej polityki i narzędzi bezpieczeństwa. W głównej fazie programu przygotowano system zarządzania; utworzono centralny serwer i środowisko testowe; sporządzono jasne specyfikacje oraz opracowano środki bezpieczeństwa, a także zarejestrowano nowe obszary w różnych zakątkach świata.

Sprawdzone narzędzia zwiększają wydajność

Program Zarządzania Globalnymi Klientami spółki Nedap polega na dzieleniu się wskazówkami oraz doradzaniu w kwestii wyboru firmy instalacyjnej, a także szablonów ofert – po to, aby w każdym miejscu zapewnić jak najwyższy poziom usług. W związku z tym centralny zespół programowy zawsze może obserwować i spójnie oceniać dostawców. Jednocześnie partnerzy instalacyjni spółki Nedap cenią sobie klarowność w kwestiach ceny, norm branżowych oraz czasu potrzebnego na wykonanie zamówienia.

– Nakreśliliśmy i zebraliśmy wszelkie istotne informacje. Tak więc za każdym razem, gdy będziemy mieli do czynienia z inwestycją realizowaną od podstaw lub będziemy odczuwali potrzebę wprowadzenia jakiejś zmiany w systemie, wystarczy, że wybierzemy model nadający się do powtórzenia, a który będzie zarazem trwały, a 80% pracy będzie już za nami. Dzięki temu rejestracja nowych projektów przebiega o wiele łatwiej i mniej kosztownie. Oczekujemy od sześciu do ośmiu projektów każdego roku i podczas gdy dotychczas spędzałem cztery tygodnie na przygotowanie, teraz zajmie mi to nie więcej jak jeden tydzień - wyjaśnia Fritz.

W pełni zintegrowana platforma

Poza Programem Zarządzania Globalnymi Klientami jednym z najważniejszych powodów, dla którego firma Danfoss zdecydowała się wybrać spółkę Nedap na swojego globalnego partnera ds. bezpieczeństwa fizycznego, jest fakt, że platforma AEOS jest oparta na oprogramowaniu. Powinniśmy w aktywny sposób chronić naszą firmę, pracowników oraz kapitał przed potencjalnym zagrożeniem. Dlatego możliwość połączenia kontroli dostępu, wykrywania włamań oraz zarządzanie nagraniami video w ramach jednej platformy ma dla nas duże znaczenie – podkreśla Fritz.

– Na rynku jest wielu producentów oferujących zintegrowane platformy, ale w rzeczywistości są to osobne systemy, które tylko ze sobą współpracują. Odkryliśmy, że platforma Nedap oparta na oprogramowaniu komputerowym jest naprawdę wyjątkowa i ma nam do zaoferowania całkowitą kontrolę, a także bardzo szybkie odpowiedzi – za każdym razem, gdy tego potrzebujemy. Ponadto, z racji swojego oprogramowania, platforma umożliwia nam wdrożenie polityki globalnej, jednocześnie gwarantując zachowanie lokalnej zgodności. Platforma AEOS pozwoliła nam nawet na zmianę naszego system wykrywania wtargnięć, zachowując równocześnie ten sam sprzęt, co z punktu widzenia wydajności jest dla nas niezwykle cenne – kontynuuje Fritz.

Możliwości zwiększania wartości

Dziś na platformie AEOS zarejestrowanych jest już siedem obszarów firmy Danfoss. Obszary te obejmują takie miejsca jak Ćennaj w Indiach, gdzie po raz pierwszy ujednolicono różne jednostki biznesowe firmy Danfoss, czy też Monterrey w Meksyku, które jest środowiskiem o wysokim poziomie bezpieczeństwa. W planach firmy jest przeniesienie większości pozostałych 80 lokalizacji do platformy AEOS w ciągu najbliższych pięciu lat.

Na początku tej migracji firma Danfoss z powodzeniem wprowadziła spójną politykę bezpieczeństwa dla całej organizacji poprzez ulepszenie procesów przy mniejszym zużyciu zasobów. – Udało nam się to osiągnąć dzięki wprowadzeniu platformy AEOS poprzez Program Zarządzania Globalnymi Klientami spółki Nedap. Oczekujemy, że w przyszłości jeszcze rozwiniemy tę propozycję wartości. Tymczasem możemy rozważyć możliwości centralnych ośrodków monitorowania, które pozwoliłyby nam otworzyć każde drzwi na całym świecie, znajdując się wciąż w jednym miejscu. Już teraz integrujemy platformę AEOS z innymi systemami związanymi z pracownikami, takimi jak transakcje gotówkowe w restauracjach czy rejestracja czasu pracy. Teraz mamy punkt wyjścia do dalszej analizy tego, w jaki sposób możemy dodać jeszcze więcej wartości naszej firmie w przyszłości. Wiemy także, że w spółce Nedap mamy partnera, który będzie nam doradzał w kwestii nowych i korzystnych rozwiązań dla naszej organizacji – tłumaczy Henrik.

Skalowalny system zarządzania i nadzoru wizyjnego

Katarzyna Chabasiewicz

Firma Pelco, jedna z czołowych firm na globalnym rynku CCTV, wprowadziła nowy system zarządzania i nadzoru wizyjnego VideoXpert. Jego najważniejszymi cechami są skalowalność i modularność, które dają możliwość stabilnego rejestrowania, wyświetlania i zarządzania zasobami wizyjnymi niezależnie od tego, czy zastosowano 100 czy 10 000 kamer. Dzięki możliwości modułowego łączenia wielu serwerów obsługujących kolejne urządzenia zyskujemy rozbudowany, niezawodny i wysoce wydajny system

VideoXpert składa się z czterech podstawowych modułów: Core, Media Gateway, Ops Center oraz Storage Manager.

Core (rdzeń) odpowiada za zarządzanie bazą danych dotyczącą kamer i rejestratorów, administrowanie użytkownikami, zapewnia podstawowy dostęp do sygnałów wizyjnych, przechowuje wybrane dane i umożliwia ich eksport.

Media Gateway (bramka mediów) zarządza dostępem do sygnałów wizyjnych oraz pozwala zadbać o to, aby użytkownicy na wszystkich poziomach dostępu, łączący się w różny sposób - za pośrednictwem sieci LAN lub WAN, a nawet korzystający z urządzeń przenośnych, otrzymywali właściwy rodzaj materiału wizyjnego, dopasowany do ich możliwości odbioru.

Ops Center jest aplikacją, z poziomu której użytkownicy mają dostęp do sygnału wizyjnego oraz narzędzi analitycznych. Obsługuje do sześciu monitorów, z których każdy umożliwia wyświetlanie 16 strumieni wizyjnych. Użytkownicy mogą płynnie przełączać się pomiędzy strumieniem wizyjnym emitowanym na żywo, a zarejestrowanym wcześniej. Dzięki opcji współdzielenia bieżącego widoku (układu okien, wybranych kamer itp.) można pracować zespołowo podczas prowadzenia nadzoru. Aplikacja ma opcje umożliwiające sortowanie kamer i ich łatwe wyszukiwanie według wybranych kryteriów. Ops Center obsługuje też dodatkowe rozszerzenia, np. mapowania, nakładania informacji na strumienie wizyjne (eConnect) oraz rozpoznawania tablic rejestracyjnych (PlateSmart).

Storage Manager (VSM) rejestruje sygnały wizyjne i zapewnia dostęp do danych. Za jego pomocą można tworzyć bloki składające się z maksymalnie sześciu serwerów danych, realizujące zabezpieczone oraz redundantne usługi rejestracji sygnałów wizyjnych.

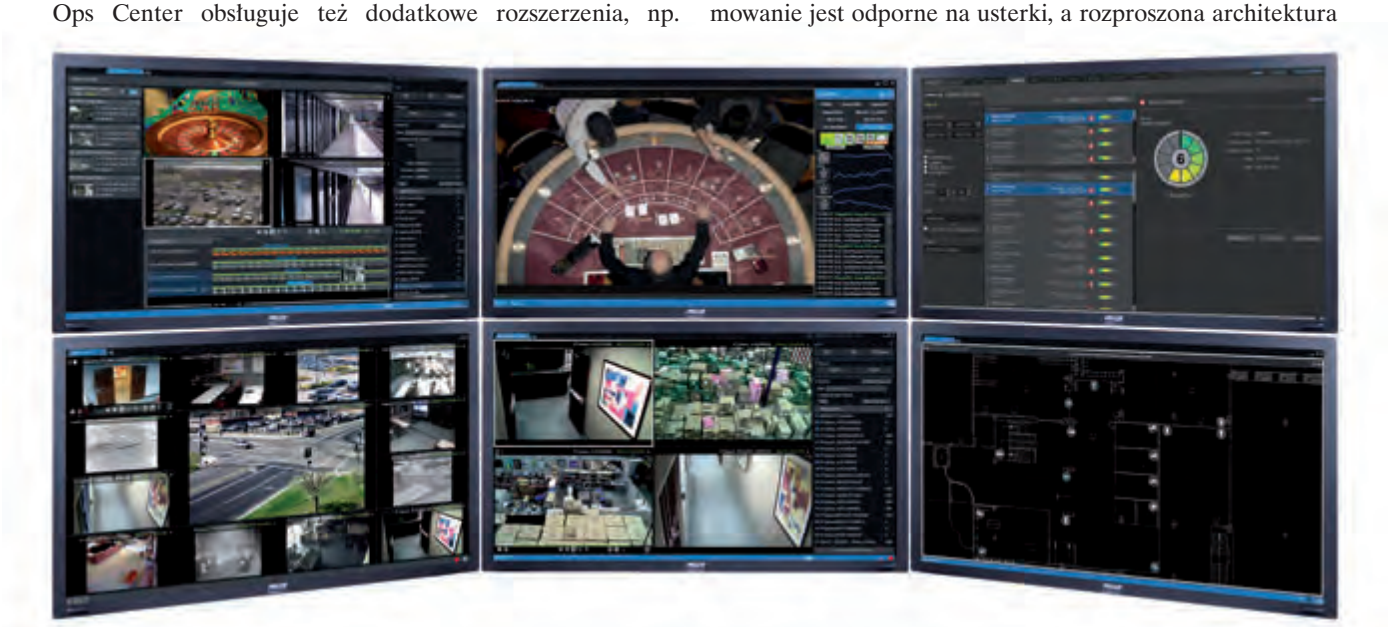
VideoXpert jest łatwy w instalacji i konfiguracji. Współpracuje z systemem Windows. Moduł Core można skonfigurować za pośrednictwem przeglądarki internetowej. Na stronie administracyjnej dostępnych jest wiele funkcji, w tym opcja dodawania znaczników ułatwiających zarządzanie kamerami i innymi urządzeniami systemowymi oraz opcja tworzenia zdarzeń systemowych wraz z procedurami ich obsługi.

System występuje w wersji podstawowej Enterprise i rozszerzonej Ultimate. Ta druga pozwala łączyć wiele systemów nadzoru wizyjnego i obsługiwać je za pomocą wspólnego interfejsu. Dzięki temu zasoby rozproszone w różnych sieciach mogą być eksploatowane przez administratorów w jednym miejscu.

VideoXpert Ultimate i Enterprise jako systemy o architekturze rozproszonej nie mają żadnego pojedynczego elementu, którego awaria unieruchomiłaby cały system lub uniemożliwiłaby rejestrację danych. System ma wielopoziomową redundancję. Specjalistyczne urządzenia i wyrafinowane algorytmy zapewniają jego bezawaryjną pracę.

VideoXpert współdziała i integruje się z innymi systemami. Dostępna jest pełna wersja sprzętowa, ale można też kupić samo oprogramowanie i wykorzystać już posiadane urządzenia (Endura i Digital Sentry) w celu utworzenia nowego systemu. Można również wykorzystywać jednostki pamięciowe NSM5200 lub Digital Sentry jako urządzenia rejestrujące i zarazem zachować zgromadzone w nich nagrania. System obsługuje kamery IP różnych producentów, co pozwala użytkownikom na swobodny wybór sprzętu.

Produkt firmy Pelco stanowi potężne narzędzie do rejestracji obrazów i zarządzania sygnałami wizyjnymi. Oprogramowanie jest odporne na usterki, a rozproszona architektura i zwielokrotnione poziomy redundancji gwarantują niezawodność działania systemu. Intuicyjny interfejs z wieloma użytecznymi funkcjami umożliwia łatwe i wygodne administrowanie dostępnymi zasobami oraz nadzór wizyjny. Więcej informacji na temat nowego systemu oraz całej oferty Pelco znajduje się na stronie *www.pelco.com.pl*.



Fot. 1. Moduł Ops Center obsługuje do sześciu monitorów, z których każdy umożliwia wyświetlanie 16 obrazów

Katarzyna Chabasiewicz
CONNECT Security
Autoryzowany Dystrybutor Pelco
ul. Nektarowa 3
Bielany Wrocławskie
55-040 Kobierzyce
tel. +48 735 742 799
pelco@pelco.com.pl
www.pelco.com.pl

Podstawy przeprowadzania audytu dotyczącego zarządzania bezpieczeństwem obiektów

dr inż. Andrzej Wójcik

Spośród wielu definicji audytu można wybrać i przytoczyć te, które oddają cel, sens i potrzeby biznesowe czy też normatywno-prawne jego realizacji. Audyt ocenia zgodność teraz i w przeszłości. Jego odmianą jest inspekcja, która ocenia zgodność jedynie w przeszłości. Obydwie odmiany są ważną częścią procesu zarządzania. Jest to usystematyzowany, niezależny i udokumentowany proces uzyskiwania dowodu z audytu oraz obiektywnej oceny spełnienia jego kryteriów

Audyt bezpieczeństwa obiektu to całokształt przedsięwzięć, których celem jest uzyskanie pełnych informacji o stanie bezpieczeństwa jednostki organizacyjnej, które w konsekwencji umożliwia podniesienie poziomu bezpieczeństwa we wszystkich sferach działalności organizacji oraz stworzenie warunków skutecznego reagowania na potencjalne zagrożenia i sytuacje kryzysowe.

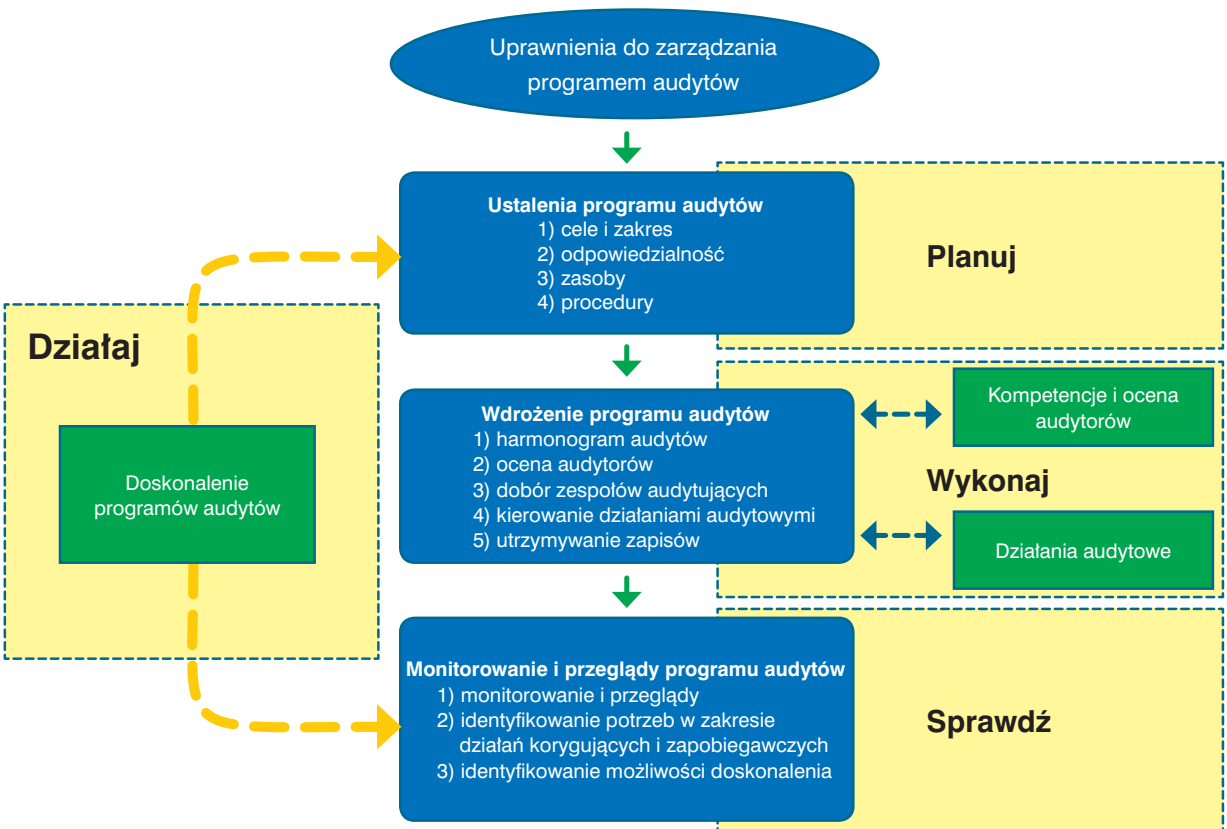
Kto może audytować?

Audytować może ten, kto spełnia warunki odbiorcy audytu. W praktyce są to osoby przeszkolone w zakresie prowadzenia audytu i mające wiedzę dotyczącą przedmiotu audytu, np.

- pierwszej strony (audyt wewnętrzny) – kiedy audytujemy własny system;
- drugiej strony (audyt zewnętrzny) – kiedy audytujemy dostawcę lub jesteśmy audytowani przez odbiorcę;
- trzeciej strony (audyt zewnętrzny) – kiedy jesteśmy audytowani przez niezależną organizację certyfikującą.

Podstawy normatywne audytu

Podstawy prowadzenia audytu zostały opisane w normie PN-EN ISO 19011:2012 *Wytyczne dotyczące audytowania systemów zarządzania*. Norma ta zawiera wskazówki dotyczące dobrych praktyk oraz planowania i prowadzenia audytów systemów zarządzania. Należy wspomnieć także o normie zawierającej wymagania dotyczące jednostek prowadzących audyty certyfikujące systemy zarządzania, tj. o normie PN-ISO/IEC 27006:2014 *Technika informatyczna – Techniki bezpieczeństwa – Wymagania dla jednostek prowadzących audyt i certyfikację systemów zarządzania bezpieczeństwem informacji*.



Rys. 1. Model programu zarządzania audytami

rzeczoznawca, ekspert, audytor oceniający zgodność z normą, prawem, standardem czy dobrymi praktykami.

Audytor to ten, kto ocenia, przeprowadza kontrolę, dokonuje przeglądu, sporządza raporty – również w każdej innej branży, np. energetycznej, informatycznej czy transportowej. Ze względu na wąskie specjalizacje audytorzy branżowi powinni być fachowcami w swoich dziedzinach.

Rzeczoznawca to tytuł przyznawany na podstawie odpowiednich przepisów osobom o wysokich kwalifikacjach i odpowiednio dużym, udokumentowanym doświadczeniu w określonej dziedzinie i specjalizacji zawodowej.

Ekspertem jest specjalista, biegły rzeczoznawca, powoływany do wydania orzeczenia lub opinii w sprawach spornych, wchodzących w zakres jego kompetencji.

Jakie rodzaje audytów można spotkać w praktyce?

Wyróżniamy następujące rodzaje audytów:

Audyt jako przegląd techniczno-eksploatacyjny systemu

Realizacja pojedynczego zadania audytowego ma dostarczyć informacji na temat poprawności przestrzegania zasad i norm dotyczących bezpieczeństwa w trakcie realizowanych procesów objętych audytem. W praktyce należy opracować i wdrożyć długotrwały program zarządzania audytami bazujący na cyklu Deminga i potraktować rezultaty jako informacyjne sprzężenie zwrotne zapewniające stały, obiektywny nadzór nad realizacją procesów bezpieczeństwa.

Wymagania ogólne dotyczące prowadzenia audytu

Zaleca się przeprowadzanie audytów w przedsiębiorstwie w zaplanowanych odstępach czasu w celu ustalenia, czy zastosowane zabezpieczenia organizacyjno-techniczne oraz procesy i procedury z nimi związane są:

a) zgodne z dokumentacją powykonawczą;
b) zgodne z wymaganiami specyfikacji technicznej i z powołanymi normami, odpowiednimi ustawami i przepisami uwzględniającymi nowe ustawy i przepisy;
c) adekwatne do zidentyfikowanych zagrożeń i poziomów ryzyka (należy uwzględnić nowe zagrożenia i nowe rodzaje ryzyka);
d) wykorzystywane lub były wykorzystywane w przypadku wystąpienia incydentów, które miały poważny wpływ na bezpieczeństwo;
e) wynikiem efektywnego wdrożenia i eksploatacji, a systemy są odpowiednio konserwowane i serwisowane;
f) zgodne z oczekiwaniami użytkownika;
g) zgodne z wymaganiami umownymi i biznesowymi.

Program audytu powinien zostać zaplanowany i uwzględniać wyniki poprzednich audytów. Częstotliwość i metody przeprowadzania audytu, przyjęte kryteria i zakres, którego on dotyczy, powinny być z góry ustalone. Wybór audytorów i sposób przeprowadzenia audytu powinny zapewnić obiektywność i bezstronność procesu. Audytorzy nie powinni prowadzić audytów dotyczących ich własnej pracy. Wymagania i odpowiedzialność za planowanie i przeprowadzanie audytów w organizacji oraz za raportowanie ich wyników i utrzymywanie zapisów powinny zostać określone w udokumentowanej procedurze. Audytorzy powinni posiadać udokumentowane uprawnienia potwierdzające wiedzę, doświadczenie oraz umiejętności.

Inicjowanie audytu – wyznaczenie zespołu audytującego

W celu wyznaczenia zespołu audytowego potrzebne są określone działania, w tym:

1. Wyznaczenie audytorów oraz audytora wiodącego (kierownika zespołu) do danego audytu oraz sprawdzenie uprawnień, kompetencji i doświadczenia audytorów.
2. Określenie celów audytu, jego zakresu i kryteriów. Audyt ma sprawdzić zgodność stanu zastanego z wymaganym. Zgodność ta jest oceniana na podstawie przyjętych kryteriów oceny.
3. Określenie wykonalności audytu. Zaleca się określenie wykonalności audytu z uwzględnieniem takich czynników jak:
   – dostępność wystarczających i odpowiednich informacji;
   – możliwość potrzebnej współpracy z audytowanym;
   – adekwatny czas i zasoby (w tym dostępność osób i dostęp do obszarów audytowanych).

   Jeżeli audyt jest niewykonalny, klientowi proponuje się wykonanie audytu alternatywnego.
4. Nawiązanie pierwszego kontaktu z audytowanym. Pierwszy kontakt z audytowanym może być nieformalny lub formalny, ale zaleca się, żeby był nawiązany przez audytorów odpowiedzialnych za zarządzanie programem lub przez audytora wiodącego. Celem pierwszego kontaktu jest:
   – ustalenie sposobów komunikacji z przedstawicielem audytowanego;
   – potwierdzenie uprawnień do przeprowadzenia audytu;
   – dostarczenie informacji dotyczących proponowanego harmonogramu oraz składu zespołu audytującego;
   – wnioskowanie o dostęp do stosownych dokumentów;
   – określenie zasad bezpieczeństwa mających zastosowanie w danym miejscu;
   – dokonanie ustaleń dotyczących audytu;
   – uzgodnienie uczestnictwa obserwatorów oraz przewodników dla zespołu audytującego.

Przebieg procesu audytu został przedstawiony na rysunku 2.

Przegląd dokumentacji

Przed podjęciem działań audytowych zaleca się dokonanie przeglądu dokumentacji w celu określenia zgodności kryteriów audytu z normami, np. technicznymi lub dotyczącymi zarządzania bezpieczeństwem informacji. Dokumentacja ta może obejmować odpowiednie dokumenty i zapisy dotyczące systemu zarządzania, a także raporty z poprzednich audytów. Podczas przeglądu zaleca się wzięcie pod uwagę wielkości, charakteru i złożoności przedsiębiorstwa oraz celów i zakresu audytu. Jeżeli dokumentacja okaże się nieodpowiednia, audytor wiodący powinien poinformować o tym odbiorcę audytu, osoby odpowiedzialne za zarządzanie programem audytów oraz audytowanego. Zaleca się podjęcie decyzji o kontynuacji audytu albo jego zawieszeniu do czasu rozwiązania kwestii związanych z dokumentacją.

Planowanie działań audytowych realizowanych na miejscu

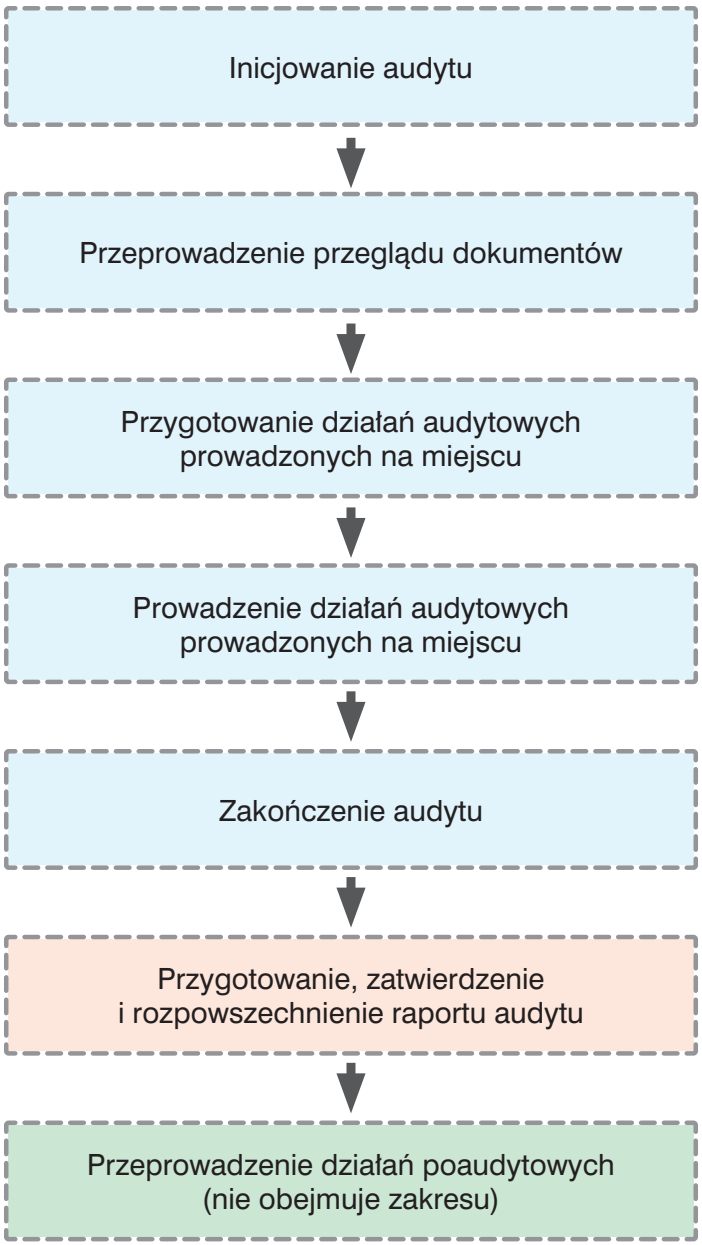
Audytor powinien przygotować plan przeprowadzenia audytu stanowiący podstawę do uzgodnień pomiędzy odbiorcą audytu, zespołem audytującym oraz audytowanym. Zaleca się, żeby plan ułatwiał ustalenie terminów i koordynację działań audytowych. Plan audytu powinien być przejrzany i zaakceptowany przez odbiorcę audytu oraz przedstawiony audytowanemu przed rozpoczęciem działań audytowych. Wszelkie zastrzeżenia audytowanego powinny być rozstrzygnięte wspólnie – przez audytora, audytowanego i odbiorcę audytu. Zaleca się, żeby przed kontynuowaniem audytu każda zmiana planu została uzgodniona pomiędzy stronami, których ona dotyczy.

Przeprowadzanie działań audytowych

Audyt powinien rozpocząć się od spotkania otwierającego, na którym powinien być obecny audytor oraz osoby odpowiedzialne za audytowane dziedziny, np. kierownicy działów.

Celem spotkania otwierającego jest:
– potwierdzenie planu audytu;
– krótkie zaprezentowanie, jak będą wykonywane działania audytowe;
– potwierdzenie metod komunikowania się;
– umożliwienie audytowanemu zadawania pytań.

Podczas audytu audytor wiodący powinien zgłaszać wszelkie zastrzeżenia i okresowo informować audytowanego i odbiorcę audytu o postępach w procesie audytu. Jest to dobra praktyka. Dowody zebrane podczas audytu, które wskazują na bezpośrednie i znaczące uchybienia, audytor powinien bezzwłocznie



Rys. 2. Przykład przebiegu procesu audytu

przekazać audytowanemu i, jeżeli to właściwe, odbiorcy audytu. Każda sprawa dotycząca problemu wybiegającego poza zakres audytu powinna być odnotowana i przedstawiona audytorowi wiodącemu w celu ewentualnego zakomunikowania odbiorcy audytu i audytowanemu. Jeżeli dostępne dowody wskazują na to, że cele audytu są niemożliwe do osiągnięcia, zaleca się, żeby audytor wiodący przedstawił odbiorcy audytu i audytowanemu przyczyny w celu podjęcia określonych działań. Działania te mogą obejmować potwierdzenie audytu lub zmianę jego planu, celów lub zakresu lub jego zakończenie. Każda potrzeba zmiany zakresu, która może pojawić się na skutek realizacji działań audytowych, powinna być omówiona z odbiorcą, przez niego zatwierdzona oraz, jeżeli to właściwe, sprawdzona i zatwierdzona przez audytowanego.

Zbieranie i weryfikowanie informacji

Informacje dotyczące celów, zakresu oraz kryteriów audytu, łącznie z informacją dotyczącą oddziaływania pomiędzy funkcjami, działaniami i procesami, powinny być gromadzone poprzez odpowiednie pobieranie próbek podczas audytu i weryfikowane. Tylko uzyskana podczas audytu informacja, która jest możliwa do zweryfikowania, może stanowić dowód. Taka informacja powinna być zapisana.

Najczęściej spotykane metody zbierania informacji to:
- rozmowy;
- obserwacje działań i procesów;
- przegląd dokumentów;
- przegląd zapisów, rejestrów.

Ustalenia na podstawie audytu

Ustalenia mogą wskazywać na zgodność lub niezgodność z kryteriami, np. normami technicznymi. Jeżeli jej wykazanie było jednym z celów audytu, ustalenia mogą wskazać sposób poprawy.

Wnioski z audytu

Zespół audytujący (audytor) powinien naradzić się przed spotkaniem zamykającym audyt w celu:
- sprawdzenia, co ustalono podczas audytu i jakie informacje zebrano w związku z obranymi celami;
- uzgodnienia wniosków z uwzględnieniem niepewności związanej z audytowaniem,
- przygotowania rekomendacji, jeżeli taki jest jeden z wyznaczonych celów;
- przedyskutowania działań po audycie, jeżeli uwzględniono je w planie.

Spotkanie zamykające

Spotkanie zamykające prowadzone przez audytora powinno odbyć się w celu przedstawienia ustaleń oraz wniosków w taki sposób, aby były one zrozumiałe i potwierdzone przez audytowanego. Zaleca się ustalenie terminu przedstawienia planu działań korygujących i zapobiegawczych przez audytowanego. W spotkaniu zamykającym powinni uczestniczyć wszyscy audytowani, ale może w nim uczestniczyć także odbiorca audytu i inne strony. Jeżeli to konieczne, zaleca się, żeby audytor poinformował audytowanego o sytuacjach zaistniałych w trakcie audytu, które mogą negatywnie wpłynąć na ocenę wniosków z audytu. W niektórych przypadkach, np. po audycie w małym przedsiębiorstwie, spotkanie zamykające może polegać tylko na zakomunikowaniu ustaleń i wniosków. Zazwyczaj jednak powinno mieć charakter formalny i być zgodne ze wszystkimi zasadami, łącznie ze składaniem podpisów na liście obecności. Wszelkie rozbieżne opinie zespołu audytującego i audytowanego dotyczące ustaleń i wniosków powinny być przedyskutowane i, jeśli to możliwe, uzgodnione. W przypadku braku zgodności opinii zaleca się zapisanie obu opinii w raporcie z audytu. Raport powinien zawierać rekomendacje dotyczące sposobu poprawy stanu, jeżeli taki jest jeden z celów audytu.

Zakończenie audytu

Audyt będzie zakończony, gdy zostaną wykonane wszystkie działania opisane w planie i zostanie rozesłany zatwierdzony raport. Dokumenty dotyczące audytu powinny być zachowane lub zniszczone na podstawie uzgodnień pomiędzy stronami uczestniczącymi oraz zgodnie z procedurami, mającymi zastosowanie przepisami oraz wymaganiami wynikającymi z umów. Zespół audytujący oraz osoby odpowiedzialne za zarządzanie programem audytów nie powinny ujawniać osobom trzecim zawartości dokumentów, innych informacji uzyskanych podczas audytu lub raportu z audytu bez jasno wyrażonego pozwolenia odbiorcy audytu i, jeżeli to właściwe, audytowanego, chyba że działanie takie jest nakazane przez prawo. Jeżeli wymagane jest ujawnienie zawartości dokumentu dotyczącego audytu, zaleca się jak najszybsze poinformowanie o tym odbiorcy audytu i audytowanego.

Przygotowanie, zatwierdzenie i rozpowszechnianie raportu dotyczącego audytu

Przygotowanie raportu dotyczącego audytu

Audytor jest odpowiedzialny za przygotowanie i treść raportu dotyczącego audytu. Zaleca się, żeby raport ten zawierał kompletne, dokładne, zwięzłe i jasne informacje dotyczące audytu. Powinien obejmować:
- wskazanie celów audytu;
- podanie czasu trwania audytu;
- określenie zakresu audytu, w szczególności wskazanie audytowanych jednostek organizacyjnych i funkcjonalnych lub audytowanych procesów;
- wskazanie odbiorcy audytu;
- wskazanie audytora wiodącego i członków zespołu audytującego;
- podanie daty i miejsca prowadzenia działań audytowych na miejscu;

Raport powinien powoływać się na:
- kryteria dotyczące audytu;
- ustalenia wynikające z audytu;
- wnioski wypływające z audytu.

Raport dotyczący audytu jest tworzony na podstawie indywidualnego wzoru dostosowanego do potrzeb odbiorcy audytu.

Zatwierdzenie i rozpowszechnianie raportu dotyczącego audytu

Raport dotyczący audytu powinien być przekazany w uzgodnionym terminie. Jeżeli nie jest to możliwe, należy zakomunikować przyczyny opóźnienia odbiorcy audytu oraz uzgodnić nowy termin przesłania raportu. Raport powinien być zatwierdzony, a następnie rozesłany do odbiorców wskazanych przez odbiorcę audytu. Raport dotyczący audytu jest własnością odbiorcy audytu. Członkowie zespołu audytującego (audytor) oraz wszyscy odbiorcy raportu powinni przestrzegać zasad dotyczących poufności raportu.

Działania po audycie

Wnioski wypływające z audytu mogą wskazywać na potrzebę podjęcia działań korygujących, naprawczych lub doskonalących, jeżeli ma to zastosowanie. Takie działania są zwykle określane i podejmowane przez audytowanego w uzgodnionym terminie oraz nie są uważane za część audytu. Zaleca się, żeby audytowany informował odbiorcę audytu o statusie tych działań.

Weryfikacja zakończenia i skuteczności działań korygujących

Weryfikacja ta może być częścią następnego audytu, którego celem będzie także sprawdzenie skuteczności i efektywności działań korygujących. Program audytu może określać udział zespołu audytującego w działaniach po audycie, które przynoszą dodatkową korzyść dzięki już zdobytemu przez ten zespół doświadczeniu. Należy zadbać o bezstronność zespołu, jeżeli będzie on wykonywał dodatkowe działania audytowe.

dr inż. Andrzej Wójcik

Ekspert i rzeczoznawca
ds. bezpieczeństwa technicznego i ochrony informacji
audytor ds. bezpieczeństwa biznesu
andrzejw@esinstal.pl

POLON-ALFA NAJNOWSZA TECHNOLOGIA. NAJWYŻSZA JAKOŚĆ

dobrze zaprojektowane BEZPIECZEŃSTWO

SYSTEMY SYGNALIZACJI POŻAROWEJ

- innowacyjnie rozproszony **POLON 6000**
- interaktywny **POLON 4000**
- konwencjonalny **IGNIS 1000/2000**

oraz

UNIWERSALNE CENTRALE STERUJĄCE UCS 6000

Polon-Alfa Spółka z ograniczoną odpowiedzialnością Sp. k.
85-861 Bydgoszcz, ul. Glinki 155 | www.polon-alfa.pl

Bezpieczeństwo informacji w chmurze (część 1)

dr inż. Marek Blim

Korzystanie z obliczania „w chmurze” zaczęto oferować w latach 2006-2007, kiedy to firma Amazon dysponująca nadwyżkami mocy obliczeniowej własnego sprzętu zaoferowała jej udostępnienie na rynku publicznym. W związanych z tym faktem w publikacjach użyto wówczas – po raz pierwszy (i, jak widać, skuteczny) – określenia *cloud computing*

U podstaw dzisiejszej chmury obliczeniowej leżą elementy zaczerpnięte z różnych obszarów działalności *stricte* informatycznej:

– ekonomii: współużytkowanie (tzn. dzielenie czasu dostępu do komputera typu *mainframe*) mające na celu zmniejszenie kosztów eksploatacji i pełniejsze wykorzystanie możliwości obliczeniowych dostępnego sprzętu (relacja: maszyna-klient);
– architektury systemów: maszyna wirtualna jako sposób przedstawienia użytkownikowi jego czasowego dostępu do użytkowanego systemu;
– praktyk projektantów systemów IT: rysunek chmurki symbolizujący Internet i wszelkie procesy w nim zachodzące; maszyny (komputery typu *mainframe*) są pomijane w odniesieniu do elementów użytkowych i klienckich (urządzeń WE/WY – terminalu, drukarki, plotera).
Rozkład w czasie oraz charakter tych zmian jest zaprezentowany na rysunku 1.

Obliczanie w chmurze jest kolejnym stopniem w ewolucji przetwarzania informacji z jej zmieniającymi się paradygmatami (kolejno mamy więc: samodzielny komputer klasy *mainframe*, model architektury klient-serwer, przetwarzanie wspólnego zadania w udostępnionym systemie rozproszonym – ang. *grid computing*, chmura obliczeniowa jako uniwersalna usługa dostosowana do życzeń i potrzeb klienta) i jest to tylko jeden z wymiarów zmian zachodzących w obszarze I&CT.

Rys. 1. Ewolucja zmian w organizacji dostępu do obszaru I&CT[1] (opracowanie własne)

Zmiany dotyczą również centrów danych z dużymi, zmiennymi, różnorodnymi zbiorami danych określanymi mianem *Big Data*), ich zasobów fizycznych, przechowywania danych, zasilania, utrzymywania oraz modernizacji (centrum danych, instancja wirtualna, farmy serwerów i ich maszynownie, konteneryzacja i unifikacja zasobów).

Ewolucja sprzętowa i systemowa sprowadza korzystanie z systemów IT do powszechnej postaci usługi widzianej w układzie „cienki klient <-> chmura obliczeniowa” opartej na szerokopasmowym, szybkim dostępie potencjalnego użytkownika do jego wynajętego zasobu oczekiwanego od dostawcy (IaaS, PaaS lub SaaS ew. XaaS). Pojęcie „cienkiego” klienta odnosi się do prostego terminalu odbiorczego użytkownika (tzn. smartfonu, iPoda Touch, tabletu itp.) zapewniającego dwie funkcje: zapytanie/zlecenie i odbiór/zobrazowanie w komunikacji z wirtualnym środowiskiem pojedynczej osoby lub grupy uprawnionych osób/urządzeń[2].

Cloud computing to, najprościej rzecz ujmując, usługa polegająca na wynajęciu od dostawcy mocy obliczeniowej procesora, powierzchni pamięci RAM i powierzchni dyskowej zamiast zakupu fizycznej infrastruktury i kłopotów z jej uruchomieniem oraz obsługą. W chmurze obliczeniowej można przechowywać pliki, a także tworzyć aplikacje i strony/portale internetowe. Można też wykorzystywać ją do różnych innych celów. Sama chmura to zbiór serwerów, które zajmują się różnego rodzaju obliczeniami.

Według najnowszych danych GUS-u polskie firmy sektora MŚP oraz korporacje coraz chętniej sięgają po chmurę obliczeniową – korzysta z niej już jedna czwarta przedsiębiorstw klasyfikowanych w tym sektorze. Ten rynek nie zwalnia i z roku na roku wzrasta w tempie dwucyfrowym. Szacuje się (grudzień 2016 r.), że już w 2019 roku rynek chmury obliczeniowej ma być wart w Polsce około 1,5 mld dolarów.

1. Zmiany w dostępie do informacji dzięki rozwojowi teleinformatyki (I&CT)

Nie od dziś wiadomo, że postępu zatrzymać się nie da. Szczególnie uwidacznia się to we wręcz żywiołowym, a więc bardzo trudnym do okiełznania rozwoju technologii i technik szybkiego dostępu i wykorzystania zasobów informacyjnych przechowywanych z wykorzystaniem różnych systemów informacyjnych. Nazwa *cloud computing* jest nadużywana, gdyż nie wszystkie proponowane usługi IT spełniają podstawowe kryteria przynależności do usług z dziedziny *cloud computing*. Kryteria te zostały określone przez National Institute of Standards and Technology (NIST) jako podstawowe, warunkujące sposób wykorzystania (są to: dostępność oczekiwanej usługi na żądanie; szeroki, zróżnicowany dostęp do sieci; dynamiczna pula zasobów; elastyczność na żądanie; mierzalność udostępnionej usługi - czyli opłata za rzeczywiste wykorzystanie).

1.1. Rozwiązania I&CT jako podstawa ewolucji dostępu do zasobów

Na rynku usług I&CT funkcjonuje coraz więcej nowych norm i rozwiązań, ale wiele firm jest uzależnionych od jednego dostawcy, który w efekcie jako jedyny posiada szczegółowe informacje na temat funkcjonowania zastosowanych przez te firmy systemów I&CT. Gdy konieczny jest zakup nowych komponentów

1) I&CT – akronim anglojęzyczny (Information and Communication Technology) określający wykorzystanie łączne technik oraz technologii informatycznych i telekomunikacyjnych.

2) Mamy coraz częściej przypadki przyznawania atrybutów kontroli dostępu elementom nieosobowym (ABAC).

lub licencji, zamówienie może zrealizować tylko ten określony dostawca. Taki brak konkurencji skutkuje wyższymi cenami i w samym tylko sektorze publicznym EOG/EEA odnotowuje się z tego powodu straty wynoszące ok. 1,1 mld € rocznie.

1.2. Krytyczne właściwości dostępu do informacji (czas dostępu, pewność zarządzania, wiarygodność informacji)

Zasoby informacji oraz jej podstawowe atrybuty (PID/CIA)[3] w tym głównie dostęp do nich stały się niekwestionowanymi aktywami biznesowymi, a minimalizacja kosztów przetwarzania tych informacji – celem samym w sobie, zwłaszcza wobec wielości oferowanych usług systemowych (np. ASP czy VPS), odbiegających od zasad „chmury obliczeniowej" (choćby ze względu na ograniczoną skalowalność), ale gwarantujących klientowi pewność zarządzania i dostępu do posiadanych zasobów wiarygodnych informacji. Należy pamiętać, że przewaga rozwiązań z dziedziny *cloud computing* w kontroli bezpieczeństwa technicznego systemu przetwarzania zasobu jest bezsporna – głównie za względu na równoległe stosowanie zapisów migawkowych (snapshotów) i aktywnych kopii bezpieczeństwa (backupów) oraz zapewnienie zrównoważonego obciążenia (load balancingu) urządzeń współpracujących w ramach systemu/klastra co obrazuje tabela.

Rozwiązania „w chmurze" ujawniają tutaj swoją dużą przewagę pod względem kosztów użytkowania. Klient płaci tylko za rzeczywisty czas korzystania z usługi. Nie ma konieczności kupienia i eksploatowania systemu i oprogramowania (IaaS, SaaS lub PaaS lub XaaS).

1.3. „Cienki" i „gruby" klient usług w chmurze obliczeniowej

Możliwość pełnego wykorzystania dobrodziejstw *cloud computing* jest uzależniona od szerokopasmowego, szybkiego dostępu z zewnątrz do wysokowydajnych rozwiązań oferowanych w wirtualnych instancjach chmury i jest decydującym elementem w walce o jej wyższość nad innymi rozwiązaniami.

„Cienki" klient to użytkownik posiadający wysokowydajny terminal indywidualny (smartfon, iPad Touch, tablet itp.) z szerokopasmowym, szybkim dostępem (transmisja G5) do wybranych zasobów danych (filmów, GIS-u[4], wirtualnej grafiki obrazowej itp.). Tacy klienci to na ogół prywatni użytkownicy zasobów lokowanych w sieciach publicznych lub specjalistycznych.

„Gruby klient" to z zasady użytkownik wewnętrzny chmury prywatnej lub hybrydowej wyposażony we własny system dostępowy (nierzadko kodowany/szyfrowany) i wykorzystujący alokowane w nim własne specjalistyczne oprogramowanie użytkowe. Na ogół jest to użytkownik instytucjonalny/wieloosobowy/wielostanowiskowy pomimo pojedynczego łącza, które jest w tym przypadku wykorzystywane sekwencyjnie do współpracy z zasobami w chmurze.

	Chmura	Serwer dedykowany	VPS
		Elastyczność	
Swoboda doboru konfiguracji	✓	×	✓
Zmiana parametrów w czasie rzeczywistym	✓	×	×
Dostępność na żądanie	✓	×	✓
Uruchamianie gotowych rozwiązań	✓	×	✓
Wykorzystanie własnego ISO	✓	✓	×
		Kontrola i bezpieczeństwo	
Snapshoty i backupy	✓	×	✓
Loadbalancing	✓	✓	×
Ciągłość działania podczas modernizacji	✓	×	✓
Dostęp administratora	✓	✓	×
Autoskalowanie zasobów	✓	×	×
		Koszty	
Rozliczenie tylko za rzeczywiste zużycie	✓	×	×
Inwestycja w zakup	×	✓	×

Tab. 1. Tabelaryczne porównanie rozwiązań z zakresu I&CT

2. Definicja chmury obliczeniowej

Zgodnie z powszechnie akceptowaną definicją z 2007 r., podaną przez National Institute of Standards and Technology (NIST), chmura obliczeniowa to model umożliwiający powszechny, wygodny, udzielany na żądanie dostęp za pośrednictwem sieci do wspólnej puli możliwych do konfigurowania zasobów (np. sieci, serwerów, przestrzeni do przechowywania, aplikacji i usług), które można szybko dostarczyć i uwolnić

3) PID/CIA – podstawowe atrybuty informacji zdefiniowane w normie wymagań bezpieczeństwa informacji (ISO/IEC 27001) i przywoływane w szeregu innych to: Poufność, Integralność, Dostępność/Confidential, Integrity, Availability.

4) GIS – akronim anglojęzyczny określający systemy informacji geograficznej „ożenione" z informacjami punktowymi/statystycznymi lub adresowalnymi.

przy minimalnym wysiłku, poprzez oferowane zarządzanie lub działanie dostawcy usługi.

Różni użytkownicy korzystają z chmury na różne sposoby. Konsumenci zwykle wykorzystują ją w ramach poczty elektronicznej, do przechowywania plików, do dzielenia się różnymi treściami i informacjami, korzystając z usług związanych z płatnościami oraz udostępnianiem muzyki i filmów. Przedsiębiorstwa wykorzystują ją przede wszystkim jako podstawowe narzędzie biurowe, do celów związanych ze wzajemną współpracą firm, do zarządzania projektami oraz do projektowania różnych aplikacji. Administracja wykorzystuje chmurę w dużej mierze w taki sam sposób jak przedsiębiorstwa, a ponadto nadaje nową jakość e-administracji.

Dla przedsiębiorstw największą zaletą chmury jest uniknięcie wydatków na IT oraz możliwość dostosowywania wielkości zasobów IT. Oznacza to możliwość szybszego wprowadzania nowych produktów na rynek oraz osiągania innowacyjności przez małe i średnie przedsiębiorstwa. Dzięki chmurze można ograniczyć koszty administracji, wprowadzić innowacje w e-administracji i poprawić jakość dotychczasowych rozwiązań. Istnieją już przykłady jednostek administracji publicznej, zarówno na szczeblu lokalnym, jak i krajowym, które przyjęły lub planują przyjąć usługi bazujące na wykorzystaniu chmury, a coraz więcej rządów rozwija wszechstronne strategie dotyczące chmur obliczeniowych (tak jest również w Polsce).

3. Rodzaje i modele chmury obliczeniowej

Istnieje kilka rodzajów chmury obliczeniowej, które można wyodrębnić w zależności od sposobu przetwarzania oraz umiejscowienia serwerów.

Prywatna chmura (ang. *private cloud*) to rozwiązanie wykorzystujące infrastrukturę i zasoby należące do klienta. Umożliwia ono firmie wprowadzenie wewnętrznego rozliczania z wykorzystania zasobów IT i jednocześnie zapewnia ich dużą elastyczność i efektywność.

Chmura hybrydowa (ang. *hybrid cloud*) to rozwiązanie przeznaczone dla tych klientów, którzy oczekują wykorzystania nadwyżek zapotrzebowania na moc przetwarzania w cyklach operacyjnych. Dotychczas kupowano w tym celu dodatkowe jednostki obliczeniowe i używano ich tylko cyklicznie, zatem mieliśmy do czynienia z zakupionym dodatkowym sprzętem, który nie był w pełni wykorzystywany. Można powiedzieć, że marnowano moc obliczeniową dodatkowego sprzętu, który po prostu nie był potrzebny na co dzień. Dzięki rozwiązaniu hybrydowemu można obecnie wykupić w razie potrzeby wymaganą ilość dodatkowej mocy obliczeniowej na zdalnych serwerach tylko na czas, kiedy rzeczywiście jest ona potrzebna.

Publiczna chmura (ang. *public cloud*) to najciekawsza odmiana chmury obliczeniowej. To rozwiązanie umożliwia dostarczanie całego systemu (mocy obliczeniowej i oprogramowania) przez sieć. Największą zaletą jest w tym przypadku skalowalność, czyli dostosowywanie wielkości chmury do aktualnych potrzeb użytkownika. W przypadku wzrostu zapotrzebowania na moc obliczeniową użytkownik może zwiększyć zakres wykorzystania *cloud computing*, a w przypadku spadku zapotrzebowania można równie łatwo ten zakres zmniejszyć. Ma to ogromne znaczenie z ekonomicznego punktu widzenia, gdyż wiele firm w różnych okresach działalności osiąga różne poziomy sprzedaży swoich usług, więc dotychczas – w przypadku korzystania z tradycyjnych systemów – kiedy dana firma potrzebowała więcej mocy obliczeniowej i więcej licencji na użytkowanie oprogramowania musiała kupić zarówno dodatkowy sprzęt, jak i dodatkowe licencje, by później, kiedy sprzedaż spadała, przechowywać zbyteczną nadwyżkę systemów IT. Ważną cechą publicznej chmury obliczeniowej jest to, że usługa jest dostarczana w ustalonej formie, a ponadto jest specjalnie dostosowana do uwarunkowań związanych z jej świadczeniem i pod względem funkcjonalności. Niezwykle istotne jest również to, że specyfikacja zasobów i konfiguracja infrastruktury IT jest niewidoczna dla klienta końcowego. Takie rozwiązanie jest szczególnie cenne dla małych i średnich przedsiębiorstw oraz różnego rodzaju instytucji o ograniczonych środkach finansowych.

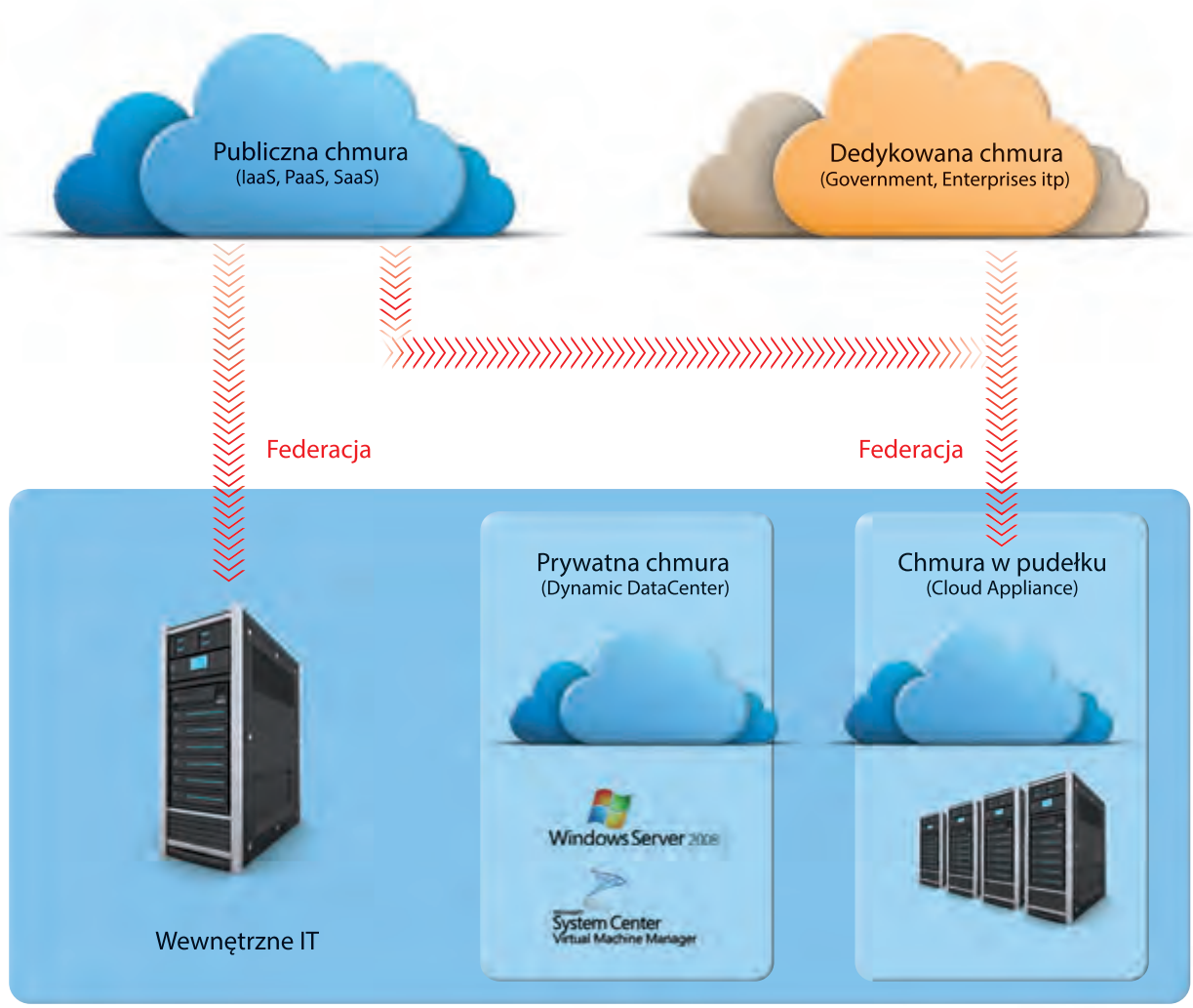
Chmurę obliczeniową możemy zatem przyrównać do wirtualnych komputerów, które są w pełni skalowalne, które jesteśmy w stanie dopasowywać do naszych aktualnych potrzeb, które można zabierać ze sobą w każde miejsce na świecie, gdzie tylko mamy dostęp do Internetu, oraz za których wykorzystanie nie musimy płacić, gdy już nie są nam potrzebne. Dzięki chmurze obliczeniowej znika również problem kompatybilności sprzętowej, gdyż urządzenie, z którego fizycznie korzystamy, tylko pośredniczy pomiędzy użytkownikiem a systemem w chmurze, a zatem może mieć dowolną konfigurację sprzętową i dowolny system operacyjny.

Podstawowe modele chmury obliczeniowej według National Institute of Standards and Technology:

1) IaaS – infrastruktura jako usługa (ang. *Infrastructure as a Service*). Ten model polega na dostarczaniu klientowi infrastruktury informatycznej (sprzętu, oprogramowania oraz serwisowania).
2) PaaS – platforma jako usługa (ang. *Platform as a Service*). Jest to sprzedaż gotowego kompletu aplikacji, dostosowanego do potrzeb użytkownika. Nie jest to związane z koniecznością zakupu sprzętu ani instalacją oprogramowania. Wszystkie potrzebne programy znajdują się na serwerach dostawcy. Interfejs użytkownika jest dostępny poprzez program, np. przeglądarkę internetową.
3) SaaS – oprogramowanie jako usługa (ang. *Software as a Service*). Klient otrzymuje konkretne, potrzebne mu funkcje i korzysta dokładnie z takiego oprogramowania, jakiego potrzebuje. Nie interesuje go ani sprzęt, ani środowisko pracy. Ma jedynie zapewniony dostęp do konkretnych funkcjonalnych narzędzi – niekoniecznie połączonych ze sobą jednolitym interfejsem. Wszelkie programy działają na serwerze dostawcy. Klient nie musi kupować licencji – płaci jedynie za każdorazowe ich użycie, a dostęp do nich uzyskuje na żądanie.

4. Przykładowe usługi bazujące na *cloud computing*

Oprócz podstawowych usług bazujących na *cloud computing*, tzn. IaaS, PaaS i SaaS, które zostały zdefiniowane przez National Institute of Standards and Technology już dekadę temu, istnieje wiele innych, które zaczęto oferować, gdyż pojawiło się na nie zapotrzebowanie. Termin *Anything as a Service* i skrót *XaaS* oznaczają je wszystkie, a więc cokolwiek, co jest usługą w chmurze (litera *X* oznacza cokolwiek).



Rys. 2. Podstawowe rodzaje chmury obliczeniowej[5]

4.1. Anything as a Service (czyli XaaS), do których należą m.in.:

– Desktop as a Service (DaaS), czyli pulpit jako usługa. W takim modelu użytkownik kupuje od usługodawcy hostowaną (czyli zlokalizowaną w jego serwerowni i przez niego obsługiwaną) maszynę wirtualną, w pełni spersonalizowaną i w pełni zgodną ze specyfikacją narzuconą przez klienta. To jest dojście do szczytu wirtualizacji – przeniesienie całego oprogramowania (wraz z systemem operacyjnym) na serwer oraz zainstalowanie u użytkownika „cienkiego" klienta mającego tylko interfejsy do komunikacji z obsługującą go osobą. W przypadku szybkich łączy internetowych taki „cienki" klient mógłby się łączyć z serwerem nie będącym w sieci lokalnej, umiejscowionym gdziekolwiek na świecie;
– Backup as a Service (BaaS), czyli kopiowanie jako usługa – usługodawca zapewnia za pośrednictwem chmury kompleksowe zabezpieczenie funkcji kopiowania zbiorów (na bieżąco oraz z archiwizacją użytkową);
– Communications as a Service (CaaS), czyli komunikacja jako usługa, kiedy to usługodawca zapewnia platformę (specjalizowany zestaw sprzętu wraz z oprogramowaniem) pod telekomunikacyjne środowisko pracy;
– Integration Platform as a Service (IPaaS), czyli platforma integracyjna jako usługa – platforma zapewniająca integrację różnych usług w chmurze dla pojedynczego użytkownika;
– Disaster Recovery as a Service (DRaaS), czyli ochrona przed katastrofą jako usługa, która ma na celu synchronizację i replikację systemu do chmury, a wdrażana jest w ramach już istniejącej infrastruktury sieciowej i fizycznej;
– Unified Communication a as Service (UCaaS), czyli zunifikowana łączność jako usługa, która obejmuje telefonię IP, wideotelefonię VoIP i inne nowoczesne narzędzia komunikacji. Jest to wirtualizacja systemów użytkowych, która bazuje na telekomunikacyjnym środowisku pracy w chmurze.

4.2. Rozwiązania CC z trwałą lokacją – usługi umocowane

Oprócz rozwiązań wirtualnych typu XaaS, dostępne są tzw. usługi umocowane, czyli rozwiązania trwałe technologicznie.

W ostatnich latach pojawiły się nowego rodzaju chmury, a mianowicie chmury przypisane użytkownikowi (dedykowane) i chmury „w pudełku" u użytkownika (instalacje kontenerowe).

Chmura dedykowana to rozwiązanie stworzone dla firm, które chciałyby korzystać z funkcjonalności zapewnianej przez

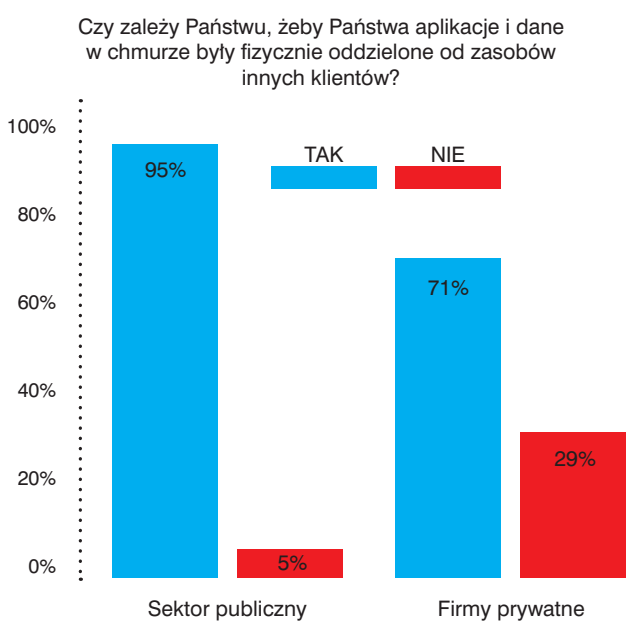
5) Źródło: http://blogs.technet.com/b/mkedziora/archive/2010/05/08/co-jest-chmura-cloud-computing.aspx.

cloud computing, ale nie stać ich na uruchomienie własnej chmury prywatnej, a z publicznej nie mogą bądź z jakichś względów nie chcą korzystać. Niektórzy duzi operatorzy chmur mogą z własnych centrów danych wyizolować część zasobów (sprzętu, usług itp.) na potrzeby konkretnego klienta, tworząc w ten sposób tzw. chmurę przypisaną (dedykowaną). Oczywiście takie rozwiązanie jest droższe od usług w „zwykłej" chmurze publicznej, jednak znacznie tańsze niż utworzenie własnej chmury prywatnej o podobnej funkcjonalności (choćby drogą użyczenia, czyli kolokacji).

Chmura „w pudełku" (instalacja CC w kontenerze ustawionym u użytkownika) to kolejne rozwiązanie limitowane (aktualnie testują je m.in. Dell, eBay i Fujitsu), ale docelowo ma być bardziej dostępne. Potrzebny sprzęt będzie fizycznie dostępny w serwerowni klienta. W skład systemu wchodzi specjalne oprogramowanie Windows Azure. Całe to rozwiązanie bazuje na doświadczeniach Microsoftu związanych z chmurą publiczną i dedykowaną. Niewątpliwą zaletą rozwiązania jest całkowita kontrola nad taką chmurą, ale też pełna odpowiedzialność – zarówno za to, co się stanie w środku, jak i za odpowiednią skalowalność. W tym przypadku dorzucenie kolejnego serwera do kontenera nie jest i nie będzie ani proste, ani tanie.

Podsumowanie

To czego oczekują polscy przedsiębiorcy w odniesieniu do bezpieczeństwa swoich danych w chmurze prezentują wyniki ankiety[6].



Rys. 3. Wyniki ankiety w polskich firmach

Opracował dr inż. Marek Blim

6) Patrz: „Bezpieczeństwo chmur publicznych z perspektywy polskich organizacji", ankieta – styczeń 2016, COMPUTERWORLD from IDG, [White Paper IBM].

Bibliografia

1. *Bezpieczeństwo biznesu w XXI wieku, praca zbiorowa*, wyd. SASMA EUROPE, Warszawa 2014.
2. Handzel Z., *Cloud computing – czyli chmura obliczeniowa i możliwości jej wykorzystania w mediach,* „Problemy Zarządzania" vol. 11, nr 4 (44), wyd. UW, Warszawa 2013.
3. Konarski X., *Komentarz do ustawy o świadczeniu usług drogą elektroniczną*, wyd. Difin, Warszawa 2004.
4. Kępa L., Tomasik P., Dobrzyński S., *Bezpieczeństwo systemu e-commerce*, wyd. Helion, Gliwice 2012.
5. Mateos A., Rosenberg J., *Chmura obliczeniowa. Rozwiązania dla biznesu*, wyd. Helion, Gliwice 2011.
6. Michalak A., *Ochrona tajemnicy przedsiębiorstwa. Zagadnienia cywilnoprawne*, wyd. Kantor Wydawniczy ZAKAMYCZE, Kraków 2006
7. Siwicki M., *Ochrona praw autorskich, bezpieczeństwa systemów informatycznych, danych osobowych i tajemnicy komunikacyjnej w chmurach obliczeniowych*, „Prokuratura i Prawo"nr 5/2015, s. 109–127.
8. Spraul V. A., *Jak działa oprogramowanie*, wyd. Helion, Gliwice 2016.

Netografia

1. http://it-manager.pl/chmura-obliczeniowa-w-polskim-e-biznesie-raport-e24cloud/ (stan z 14.05.2017).
2. www.3s.pl/pl/17,serwery-i-cloud.html (stan z 14.05.2017).
3. www.computerworld.pl/news/Dlaczego-chmura-sie-w-Polsce-nie-udaje,405741.html (stan z 14.05.2017).
4. www.cyberdefence24.pl/526022,jak-chronic-infrastrukture-krytyczna-nowe-rekomendacje-nist (stan z 14.05.2017).
5. www.europarl.europa.eu/RegData/etudes/etudes/join/2012/475104/IPOL-IMCO_ET(2012)475104_PL.pdf (stan z 14.05.2017).
6. www.giodo.gov.pl/259/id_art/6271/j/pl (stan z 14.05.2017).
7. www.hbrp.pl/a/chmura-obliczeniowa-bilans-korzysci-i-zagrozen/36ypu9gW (stan z 14.05.2017).
8. www.piit.org.pl/documents/10181/268830/Definicja_rodzaje_chmur_obliczeniowych_oraz_poziomy_uslug_-_Dorota_Grudzien-Molenda_HP.pdf (stan z 14.05.2017).
9. www.spidersweb.pl/2013/11/tencent-10-tb-za-darmo.html (stan z 14.05.2017).
10. www.spidersweb.pl/2015/11/jaka-chmure-wybrac-dysk-google-mega.html (stan z 14.05.2017).

A ty, jaki masz nadajnik alarmowy?

Daniel Kamiński

Czy zastanawiałeś się kiedykolwiek, Czytelniku, czy w przypadku włamania sygnał alarmowy z Twojego obiektu na pewno dotrze do centrum odbiorczego obsługiwanego przez firmę zajmującą się ochroną? Czy zdarzyło się, że system alarmowy zasygnalizował nieudaną próbę komunikacji z centrum odbiorczym? Czy zostałeś powiadomiony o braku komunikacji przez centrum?

Podobne pytania często zadaję znajomym korzystającym z usług monitorowania, aby sprawdzić, czy są świadomi możliwości oraz ograniczeń rozwiązań dostępnych na rynku. Następnie staram się zachęcać ich do korzystania z funkcji kontroli komunikacji, które niestety często nie są uruchamiane w systemach alarmowych. Powodów niekorzystania z funkcji kontroli komunikacji jest kilka. Czasem powodem jest wybranie najtańszego abonamentu, czasem nadmierna liczba sygnalizowanych usterek, a czasem brak takich funkcji w urządzeniach dostarczanych przez firmy ochrony.

Poznawszy przyczyny braku kontroli komunikacji w konkretnych systemach, rozmawiam na ten temat z właścicielami firm ochrony, którzy zajmują się usługami monitorowania alarmów. To oni decydują, jaki standard usług oferują swoim klientom, jakie systemy alarmowe proponują, które systemy transmisji są wykorzystywane oraz czyje odbiorniki alarmowe obsługują monitorowane systemy.

Okazuje się, że jest wiele mitów oraz nieporozumień, które wymagają wyjaśnień. W artykule podzielę się przemyśleniami na temat wymagań oraz oczekiwań dotyczących usług monitorowania alarmów.

Różne standardy monitorowania

W naszym kraju powielane są trzy sposoby łączenia centrali alarmowej z urządzeniem służącym do transmisji alarmu (nadajnikiem):

1) Najbardziej rozpowszechnione jest podłączenie programowalnych wyjść centrali do wejść nadajnika. Sposób ten wymaga znajomości kodu instalatora centrali alarmowej w celu dodania modułu wyjść centrali i odpowiedniego zaprogramowania tego modułu. W takim układzie każdemu wejściu nadajnika przypisywany jest rodzaj zdarzenia. W zależności od typu nadajnika oraz centrali takie wejścia mogą służyć do przekazywania informacji o pewnych rodzajach zdarzeń alarmowych (od jednego do ośmiu rodzajów) – najczęściej o włamaniu, napadzie, otwarciu, zamknięciu, usterce lub sabotażu.
2) Drugim bardzo częstym sposobem jest przyłączenie nadajnika bezpośrednio do wyjścia sygnalizatora optyczno-akustycznego. Zakłada się, że sygnalizator działa tylko w przypadku alarmu, więc wejście nadajnika podpisuje się *alarm ogólny*. Sposób ten jest popularny z dwóch powodów. Po pierwsze, nie jest potrzebny kod instalatora, co jest bardzo przydatne w przypadku przyłączania nadajnika do systemu przejętego od konkurencji. Po drugie, nie ma skomplikowanych procedur – niezależnie od tego, jakie zdarzenie wywoła alarm, rolą załogi będzie weryfikacja zdarzenia i odpowiednia reakcja.
3) Trzecim sposobem jest przyłączenie nadajnika poprzez dialer telefoniczny lub złącze RS232. Oba rozwiązania pozwalają na przekazywanie do centrum odbiorczego wszystkich zdarzeń generowanych przez centralę alarmową. Najczęściej wykorzystywane są w tym celu formaty ContactID lub SIA. Rozwiązanie to jest najrzadziej wykorzystywane, gdyż wymaga stosowania specjalnych nadajników, liczba transmisji jest „duża” i potrzebna jest praca mająca na celu zaprogramowanie centrali alarmowej. Zaletą jest możliwość dokładnego określenia, która czujka wygenerowała alarm oraz który użytkownik jako ostatni włączał system w dozór.

Nadajniki alarmowe dostępne na rynku

Sposób łączenia nadajników z centralami alarmowymi wynika z technik wykorzystywanych do transmisji alarmów. Firmy ochrony najczęściej oferują dwa rodzaje nadajników – radiowe oraz GSM.

Nadajniki radiowe są dostępne na naszym rynku od ponad 25 lat. Ze względu na częstotliwość transmisji na początku nie

mogły przesyłać zbyt wielu informacji. Ale wówczas wystarczało to, że nadajnik przesyłał jedną informację i wywoływał alarm w centrum odbiorczym. Obecnie nadajniki radiowe przekazują do dziesięciu informacji i nadal stanowią ok. 45% wszystkich sprzedawanych nadajników.

Nadajniki GSM również przeszły sporą ewolucję. Są w sprzedaży od ponad 20 lat. Początkowo wykorzystywały do transmisji alarmu wiadomości SMS oraz identyfikację numeru CLIP. Ze względu na to, że koszty wiadomości SMS były wówczas wysokie (ok. 50 gr), bardzo popularne stało się bezpłatne monitorowanie za pomocą CLIP (dzwonienie na wskazany numer w celu identyfikacji numeru bez nawiązywania połączenia). Nadajniki GSM przekazywały maksymalnie osiem informacji, podobnie jak nadajniki radiowe. Są nadal w sprzedaży i stanowią ok. 20% wszystkich oferowanych nadajników.

Bezprzewodowe nadajniki pracujące w trybie on-line zaczęto stosować ponad 15 lat temu, po powiązaniu transmisji GPRS z publicznym adresem IP oraz udostępnieniu firmom ochrony bezpośredniej łączności z serwerami operatorów telefonii komórkowej. Łączność pakietowa okazała się najtańszym sposobem transmisji, dzięki czemu część nadajników zaczęła przekazywać wszystkie sygnały generowane przez centralę alarmową. Obecnie nadajniki te stanowią ok. 30% wszystkich dostępnych w sprzedaży.

Nadajniki jako urządzenia nadawczo-odbiorcze

Współczesne normy (PN-EN 50131: systemy alarmowe oraz PN-EN 50136: systemy transmisji alarmu) wprowadziły nowe wymagania dotyczące nadajników alarmowych. Dotychczasowe urządzenia transmisji alarmu (UTA) zostały przemianowane na urządzenia nadawczo-odbiorcze (UNO).

Wcześniejsze normy dopuszczały używanie nadajników jednokierunkowych, czyli wysyłających wiadomości do odbiornika, ale nie otrzymujących potwierdzenia dotarcia sygnału alarmowego. Pojawiało się ryzyko, że alarm nie dotrze do centrum odbiorczego. W tym okresie firmy ochrony wprowadziły do umów o świadczenie usług monitorowania zapisy, że nie będą odpowiadać za brak reakcji na sygnały, które nie dotarły do centrum odbiorczego. Niestety użytkownik nie był powiadamiany o nieodebraniu sygnału alarmowego w centrum.

Wprawdzie na rynku były dostępne nadajniki radiowe odbierające potwierdzenie dotarcia sygnału alarmowego do centrum odbiorczego, ale ze względu na małą przepustowość kanałów systemu łączności monitorowania przyjęły się tylko w monitorowaniu pożarowym. Przez pewien czas były opracowywane i stosowane nadajniki otrzymujące potwierdzenie w postaci SMS, ale ze względu na duże koszty transmisji oraz blokowanie odbiorników zostały praktycznie zapomniane.

Do nadajników jednokierunkowych należą przede wszystkim:

– nadajniki radiowe,
– nadajniki GSM wysyłające powiadomienia SMS,
– nadajniki GSM wykorzystujące funkcję CLIP.

Większość nadajników dwukierunkowych wykorzystuje transmisję GPRS. Niskie koszty transmisji umożliwiają stałe zestawienie połączenia (on-line) oraz potwierdzanie przekazywanych wiadomości. Poza tym nadajniki te zwykle przekazują do centrum odbiorczego informację o czasie wystąpienia zdarzenia, co w połączeniu z czasem odbioru tej informacji pozwala w prosty sposób określać dostępność sieci transmisyjnej.

Nadajniki otrzymujące potwierdzenie przekazują do centrali alarmowej abonenta informację dotyczącą odebrania sygnału alarmu w centrum odbiorczym. Jeżeli sygnał nie dotrze do centrum odbiorczego firmy ochrony, użytkownik zostanie o tym poinformowany. Niezależnie od tego urządzenia odbiorczo-nadawcze znajdujące się w centrum odbiorczym mogą wykrywać nadajniki, które przestały nadawać, ale to już temat na oddzielny artykuł.

Zastanawia to, że zmiany wprowadzone przez wymienione normy praktycznie nie zostały zauważone przez operatorów systemów monitorowania. To powoduje, że wielu użytkowników nie zdaje sobie sprawy, że ich nadajniki nie spełniają wymagań obecnych norm. Przy założeniu, że monitorowanych jest ok. miliona nadajników, jest możliwe, że aż 600 000 z nich pracuje bez potwierdzeń dostarczenia alarmu do centrum odbiorczego.

Dodatkowe funkcje współczesnych nadajników

Współczesne nadajniki alarmowe mają kilka przydatnych dla użytkowników końcowych funkcji. Wyposażone są w wyjścia programowalne służące do zdalnego sterowania oświetleniem, otwierania bram czy sterowania podlewaniem ogrodu. Dodatkowo umożliwiają obsługę powiadomień poprzez aplikacje mobilne, w których dostępne są historia zdarzeń, informacja o statusie systemu alarmowego oraz informacja na temat jakości połączenia z centrum odbiorczym.

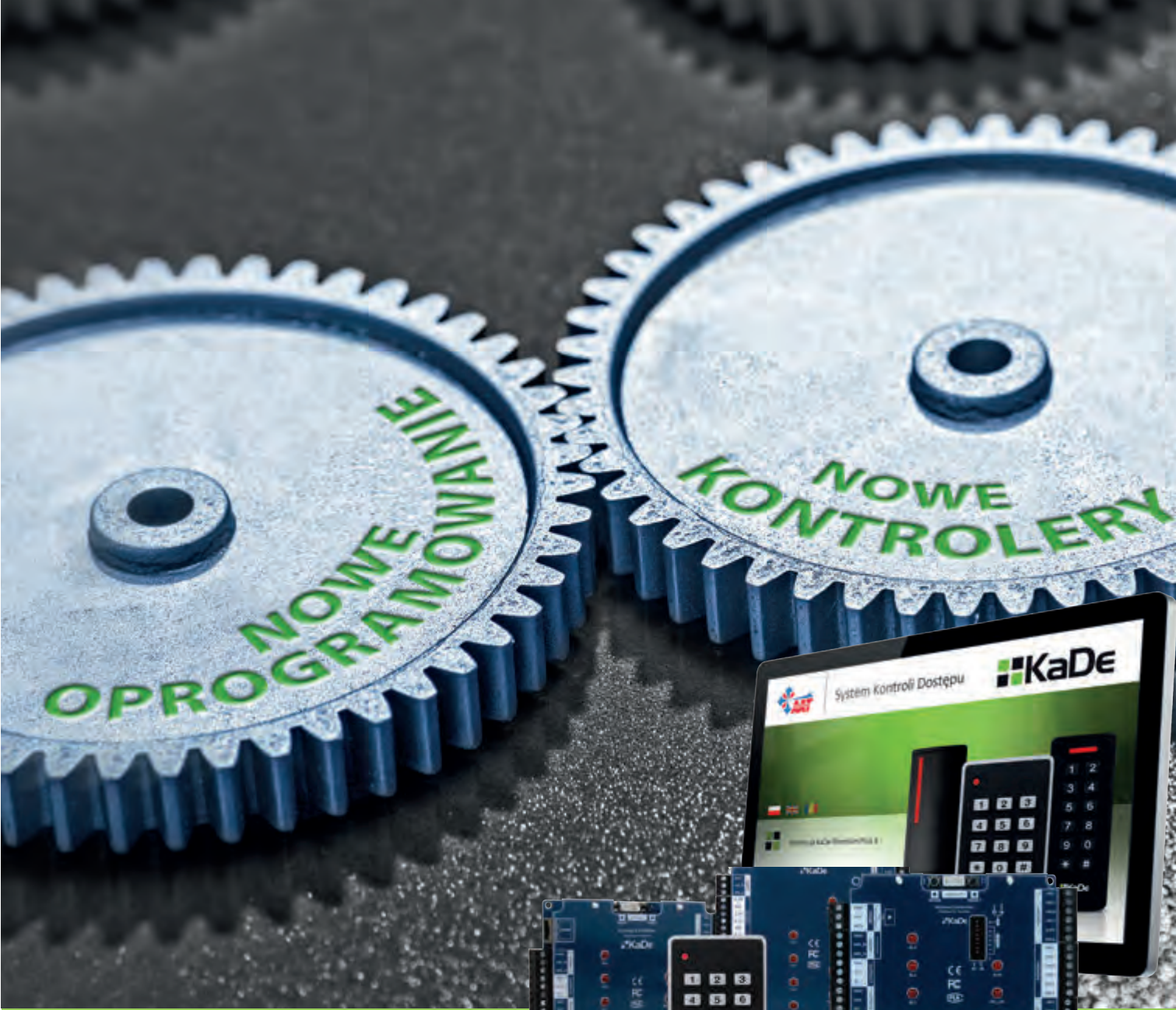
Podsumowanie

Drogi Czytelniku, zachęcam do zainteresowania się tym, jakiego rodzaju urządzenie do transmisji alarmu zostało zainstalowane u Ciebie. Zwłaszcza teraz, w okresie wzrostu cen usług monitorowania, masz prawo wymagać zastosowania nadajnika zgodnego z normami oraz umożliwiającego sprawdzenie, czy chroniąca Cię firma odebrała sygnał alarmu z Twojego systemu alarmowego.

Daniel Kamiński

Alert Control
ALARMY POD KONTROLĄ

ALERTCONTROL Daniel Kamiński
ul. Przyrodnicza 7E
05-126 Michałów-Grabina
alertcontrol@alertcontrol.pl
tel.: (+48) 784 646 386



KaDe

NOWY SYSTEM KADE
IDEALNE DOPASOWANIE

MAPY OBIEKTU Z AKTYWNYMI, ANIMOWANYMI IKONAMI ELEMENTÓW SYSTEMU
GLOBALNY ANTI-PASSBACK

AAT HOLDING S.A.
PRODUCENT I DOSTAWCA ELEKTRONICZNYCH SYSTEMÓW ZABEZPIECZENIA MIENIA
www.aat.pl

System KaDe Premium Plus II
dobra zmiana (część 2)

Ryszard Sobierski

W poprzednim numerze *Zabezpieczeń* przedstawiłem nową serię kontrolerów marki KaDe. W tym numerze zaprezentuję najnowszą wersję oprogramowania KaDe – KaDe Premium Plus II

Nowa wersja programu nadzorczego do obsługi kontrolerów marki KaDe obsługuje więcej niż dotychczas kontrolerów (w tym nowe modele) i ma kilka nowych, ciekawych funkcji. Dotyczy to w szczególności trybów monitorowania systemu oraz zaawansowanych funkcji dostępnych podczas korzystania z kart.

Powiększony asortyment oferowanych kontrolerów

Obecnie, po wprowadzeniu nowych modeli, oferowanych jest w sumie 11 kontrolerów KaDe Premium Plus II. Lista obejmuje zarówno dotychczasowe modele z serii 10XX, jak również nowe wersje z serii 20XX. Dotychczasowe kontrolery z serii 10XX mają w dalszym ciągu te same funkcje związane z monitorowaniem stanu współpracujących z nimi elementów pomimo użycia nowych ikon na mapie. Dlatego nie zaleca się instalowania systemów zbudowanych z wykorzystaniem starych i nowych kontrolerów, jeżeli ma być użyty tryb monitorowania on-line.

KDH-KS2012-IP
KDH-KS2024-IP
KDH-KS2012-RS
KDH-KZ2000-IP-M
KDH-KZ2000-IP-U
KS-1012-IP
KS-1012-RS
KS-1024-IP
KS-1024-RS
KZ-1000-M-IP
KZ-1000-U-IP

Rys. 1. Lista kontrolerów KaDe

Globalny anti-passback

W programie KaDe Premium Plus II została zaimplementowana funkcja globalnego anti-passbacku. Nowa opcja w konfiguracji pozwala tworzyć grupy drzwi objętych kontrolą dwustronną. Dodanie kontrolera do definiowanej grupy anti-passbacku globalnego automatycznie uaktywnia tę funkcję. Oznacza to, że użytkownik musi użyć karty na przemian w czytniku wejściowym i wyjściowym, ale może wejść dowolnym wejściem i wyjść dowolnym wyjściem przypisanym do tej grupy. Grupa może obejmować czytniki podłączone do wielu kontrolerów. Funkcja ta dotyczy tylko kontrolerów z portami IP i działa tylko gdy jest możliwa komunikacja z programem nadzorczym, który podejmuje decyzję o dostępie. Oprócz tego dla każdego kontrolera można uaktywnić funkcję anti-passbacku lokalnego. Dotyczy to wówczas czytników w obrębie jednego kontrolera i decyzje o dostępie podejmuje kontroler, bez konieczności komunikowania się z programem nadzorczym.

Włączanie i wyłączanie funkcji dodawania kart bez udziału programu

To nowa funkcja, bardzo przydatna na etapie instalacji i uruchamiania systemu, umożliwiająca dodawanie kart do pamięci kontrolera bez komunikacji z programem nadzorczym. W trakcie konfiguracji tej opcji konieczne jest zaprogramowanie karty administratora służącej do dodawania i usuwania kart użytkowników. Funkcję tę można wyłączyć w programie (w menu konfiguracji kontrolera) po nawiązaniu komunikacji z kontrolerem. W programie można również usuwać dodane tą metodą karty.

Ustalanie trybu pracy drzwi

W nowej wersji programu można wybrać jeden z czterech trybów działania drzwi. Dotyczy to sposobu odryglowywania. Dostępny jest nowy tryb, w którym odryglowywanie jest automatyczne, zgodne z terminarzem i w którym nie jest potrzebny odczyt ważnej karty w czytniku.

Rys. 2. Tryby pracy kontrolowanych drzwi

Nowe uprawnienia dla użytkowników kart

Użytkownicy kart mogą skorzystać z dwóch nowych funkcji. Pierwsza z nich to wyłączenie albo włączenie monitorowania linii dozorowych w danym kontrolerze. Funkcja ta jest dostępna tylko w czytnikach z klawiaturą. Po wpisaniu specjalnego kodu alarmowego na klawiaturze czytnika i odczycie ważnej karty (uprawnionej do tej operacji) następuje wyłączenie albo włączenie monitorowania linii dozorowych, co skutkuje wyłączeniem albo włączeniem alarmu. Funkcja działa sekwencyjnie. Kod alarmowy ustawia się w oknie konfiguracji kontrolera.

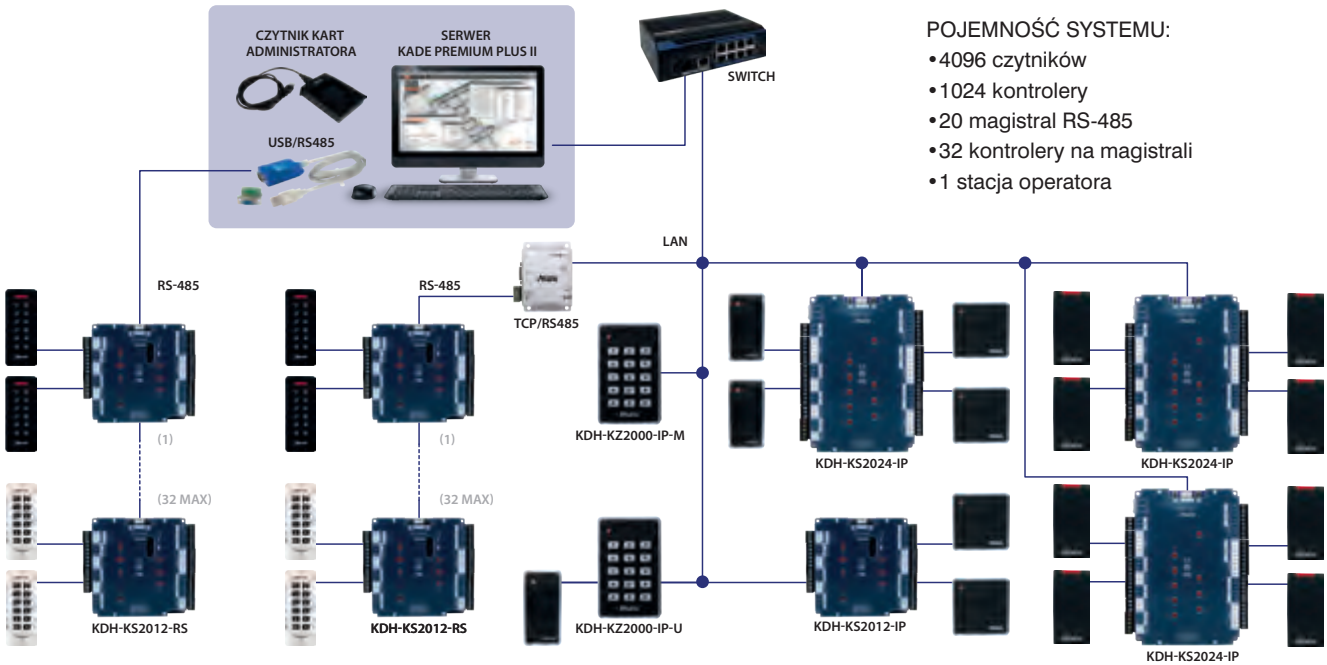
Drugą nową funkcją jest zaryglowanie i ponowne odryglowanie drzwi za pomocą karty, chodzi o drzwi, które – zgodnie z terminarzem – zostały odryglowane automatycznie na stałe lub na pewien czas. Użytkownik uprawniony do tej operacji (i do korzystania z tych drzwi) może po wyjściu z pomieszczenia zaryglować drzwi poprzez dwukrotny odczyt karty na czytniku. Wróciwszy, może je ponownie odryglować na stałe poprzez jednokrotny odczyt.

Trzy okna programu

Program KaDe Premium Plus II jest programem jednostanowiskowym. W stosunku do swojego poprzednika ma rozszerzony zakres funkcji. Trzy kanały komunikacyjne w kontrolerach serii 20XX z portem IP umożliwiają wykonywanie trzech różnych operacji w trzech uruchomionych niezależnie oknach programu. Dogodnym rozwiązaniem w przypadku takiego trybu pracy jest korzystanie z komputera z dwoma lub czterema monitorami. W jednym oknie można uruchomić monitorowanie na żywo, w drugim wykonywać operacje na kartach użytkowników lub modyfikować parametry urządzeń, a w trzecim

można tworzyć raporty. Dane dotyczące zmian można następnie przesyłać do kontrolerów bez konieczności uprzedniego wyjścia z trybu monitorowania on-line systemu.

niało ocenę stanu systemu. Najważniejszą linią dozorową jest linia czujnika stanu drzwi, która pokazuje stan skrzydła drzwi objętych systemem kontroli dostępu. Dzięki możliwości ciągłej kontroli tego stanu możliwe jest prawidłowe wyświetle-



Rys. 3. Schemat blokowy systemu KaDe Premium Plus II

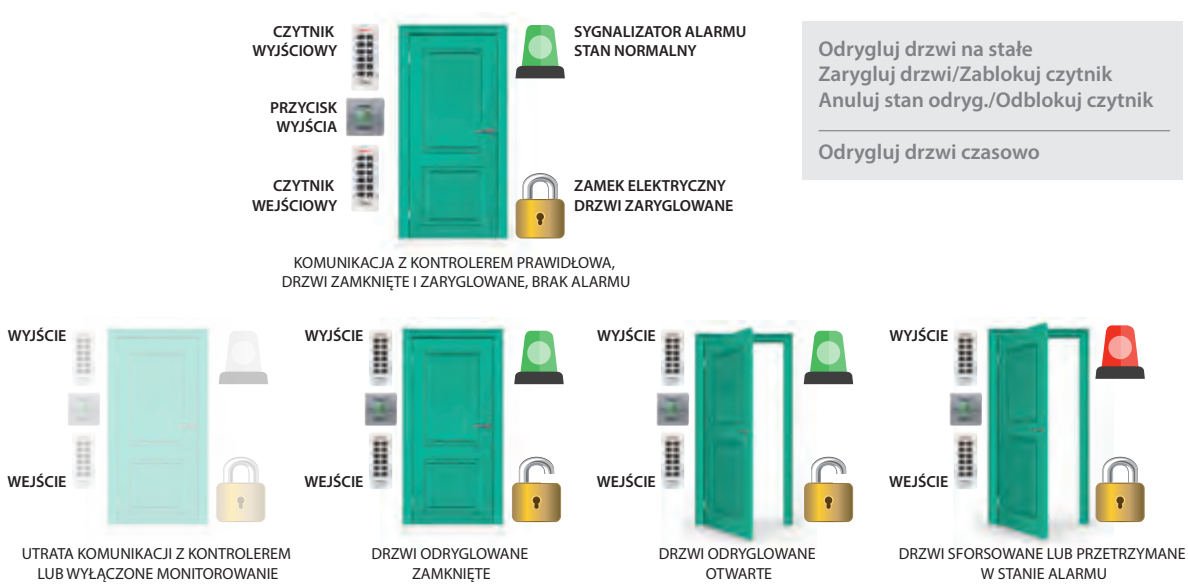
Nowe ikony i menu kontekstowe z wizualizacją elementów na mapie

Najważniejszą cechą nowej serii kontrolerów KaDe jest udostępnianie programowi nadzorczemu informacji o stanie wejść linii dozorowych oraz wyjść sterujących, co umożliwia poprawne wyświetlenie ich stanu na mapie obiektu za pomocą ikon. Poprzednia seria 10XX takich możliwości nie miała, co utrudnie odpowiedniej ikony sygnalizującej status drzwi. Na mapie widzimy teraz dokładnie, czy drzwi są zamknięte czy otwarte, zaryglowane czy odryglowane.

W nowej wersji programu animowana ikona drzwi składa się z kilku elementów, które obrazują:

– stan skrzydła drzwi – zamknięte/otwarte,

– stan zamka – zaryglowany/odryglowany,



Rys. 4. Ikona drzwi w różnych stanach

– stan urządzenia – normalny (kolor zielony)/alarmowy (kolor czerwony),
– użycie przycisku wyjścia (kolor zielony/pulsowanie/kolor czerwony),
– odczyt karty w czytniku (kolor biały/pulsowanie/kolor czerwony),
– menu kontekstowe – odrygluj/zarygluj/odrygluj czasowo/zablokuj/odblokuj.

Szary kolor ikony oznacza utratę lub brak komunikacji z kontrolerem obsługującym dane drzwi. Dodane menu kontekstowe umożliwia wykonywanie na mapie operacji mających związek z drzwiami.

jest pełna kontrola ich aktualnego stanu. Kontrolery należące do serii 2000 są wyposażone w szybkie 32-bitowe procesory, dzięki którym każdy z nich może udostępniać informacje na temat stanu elementów współpracujących – zamka elektrycznego (odryglowany/zaryglowany), skrzydła drzwi (otwarte/zamknięte) – oraz stanu drzwi (dzięki monitorowaniu czujnika stanu drzwi) w przypadku alarmu wywołanego na skutek ich sforsowania. Ponadto platforma VENO monitoruje stan połączenia z poszczególnymi kontrolerami KaDe oraz stan wejść linii dozorowych i wyjść sterujących. Monitorowane są również linie dozorowe i wyjścia sterujące na dodatkowych modułach z liniami dozorowymi i wyjściami przekaźnikowymi. Menu

Rys. 5. Ikona linii dozorowej w różnych stanach

W oknie konfiguracji dodany został terminarz monitorowania, którego włączenie jest sygnalizowane pojawieniem się „okularów" na ikonie. W takim stanie alarmy są aktywne. Poza okresem czuwania wynikającym z terminarza ikona sy-

kontekstowe ikon na panelach graficznych umożliwia wykonywanie określonych operacji na elementach systemu kontroli dostępu KaDe (odryglowanie/zaryglowanie drzwi, zmiana stanu przekaźnika itp.). Wybrane operacje na elementach syste-

Rys. 6. Ikona wyjścia sterującego w różnych stanach

gnalizuje zmianę stanu linii nie wywołującą alarmu. Sygnalizowany jest początek i koniec stanu alarmowego. Ta ikona nie ma menu kontekstowego.

Ikona wyjścia sterującego nie występowała w poprzedniej wersji programu. Ikona ta ma menu kontekstowe, które umożliwia zmianę stanu przekaźników na mapie.

Integracja z oprogramowaniem VENO

Osoby wykorzystujące zaawansowane funkcje systemów zabezpieczeń zainteresuje z pewnością wiadomość, że nowa seria kontrolerów marki KaDe została zintegrowana z oprogramowaniem VENO służącym do wizualizacji i integracji systemów zabezpieczających mienie. Seria ta obejmuje modele standardowe – KDH-KS2012-IP (dwa porty czytników, 1–2 drzwi) i KDH-KS2024-IP (cztery porty czytników, 2–4 drzwi) – oraz modele zintegrowane – KDH-KZ2000-IP-U (wersja na karty Unique) i KDH-KZ2000-IP-M (wersja na karty Mifare). Wszystkie wymienione modele mają wbudowane porty IP do komunikacji z programem nadzorczym. Porty te są wykorzystywane również do bezpośredniej komunikacji z platformą VENO. Kontrolery są konfigurowane w programie KaDe Premium Plus II. Po przesłaniu bazy danych z programu do kontrolerów mogą one zostać dodane jako urządzenia zintegrowane do bazy platformy VENO. Na panelach zawierających plany poszczególnych fragmentów obiektu można dodać ikony drzwi objętych kontrolą dostępu. Dzięki temu możliwa

mu mogą być wykonywane automatycznie, przez operatora lub zgodnie z przypisanym terminarzem. Wymienione powyżej funkcje gwarantują sygnalizowanie prawidłowych stanów elementów systemu kontroli dostępu na panelach graficznych VENO.

Aktualna wersja programu VENO ma także wbudowany interfejs do operacji mających związek z użytkownikami kart systemu KaDe. W oknie określania uprawnień możliwe jest wyświetlenie listy użytkowników kart pobranej z bazy programu KaDe Premium Plus II. Dzięki temu w VENO można dodawać nowych użytkowników, modyfikować ich uprawnienia dotyczące dostępu do poszczególnych pomieszczeń oraz blokować lub usuwać karty.

Program nadzorczy KaDe Premium Plus II jest przeznaczony do małych i średnich systemów kontroli dostępu, od których użytkownicy oczekują prostej, intuicyjnej obsługi oraz realizacji podstawowych funkcji. Możliwość włączenia trybu monitorowania on-line umożliwia personelowi odpowiedzialnemu za ochronę fizyczną skuteczne monitorowanie stanu systemu zarówno w oknie monitorowania w programie KaDe, jak i na platformie integrującej VENO.

Ryszard Sobierski
AAT HOLDING

KDH-KS2012-IP - Kontroler standardowy KaDe serii 2000

Kontroler KDH-KS2012-IP jest przeznaczony do pracy w systemach KD, bazujących na programie nadzorczym **KaDe Premium Plus II.** Model ten może obsłużyć 1 drzwi dwustronnie lub 2 drzwi jednostronnie. Posiada port IP do komunikacji z programem KaDe Premium Plus II oraz port RS485 do podłączenia modułu rozszerzeń KDH-MOD2000INOUT (zawiera 4 wyjścia przekaźnikowe, 4 wejścia linii dozorowych i 4 wyjścia do sterowania sygnalizatorów akustycznych w czytnikach). Współpracujące z kontrolerem czytniki (wyposażone w interfejs Wiegand 26-40 bitów) mogą identyfikować użytkownika poprzez odczyt karty zbliżeniowej, kod dostępu lub skanowanie cechy biometrycznej.

Charakterystyka urządzenia:

- 32-bitowy procesor
- Duża pojemność pamięci dla zdarzeń, alarmów, kart i kodów dostępu
- Płynna praca w trybie monitorowania on-line
- Udostępnianie stanów: drzwi, zamka, linii dozorowych i wyjść sterujących
- Funkcje specjalne: podwójny odczyt karty, dostęp po odczycie 2-4 kart, pierwsza karta otwierająca, dostęp po potwierdzeniu przez operatora

Model	KDH-KS2012-IP
Pamięć kart/kodów dostępu	20 000
Pamięć zdarzeń	50 000 (autom. kasowanie najstarszych)
Pamięć alarmów	20 000 (autom. kasowanie najstarszych)
Napięcie zasilania / pobór prądu	12 V_{DC} / 100 mA
Otoczenie	tylko do instalacji wewnątrz pomieszczeń
Temperatura pracy	-10°C ~ +55°C
Wilgotność względna	10% - 90%
Port do połączenia z komputerem	TCP
Port do podłączenia modułów rozszerzeń	RS485
Porty czytników	2 porty - interfejs Wiegand
Format kart	26-bitowy, 34-bitowy, definiowany format
Typy kart	zgodne z technologią czytnika
Format kodów klawiatury na czytnikach	4-bitowy, bez buforowania
Wejście czujnika stanu drzwi	NO/NC - 2 linie dozorowe
Wejście do przycisku wyjścia	NO/NC - 2 linie dozorowe
Wejście - zastosowanie ogólne	NO/NC - 2 linie dozorowe
Wejście na module - zastosowanie ogólne	NO/NC - 4 linie dozorowe (opcja)
Wyjścia - sterujące zamkiem elektrycznym	przekaźnikowe 12 V_{DC}, 3 A - 2 wyjścia
Wyjście - zastosowanie ogólne	przekaźnikowe 12 V_{DC}, 3 A - 1 wyjście
Wyjścia - zastosowanie ogólne na module	przekaźnikowe 12 V_{DC}, 3 A - 4 wyjścia (opcja)
Tryb identyfikacji	karta, PIN, karta lub PIN, karta + PIN

Producent:

AAT HOLDING S.A.
ul. Puławska 431
02-801 Warszawa

tel. +48 22 546 05 46
e-mail: kontakt@aat.pl
www.aat.pl

WP8010 – Bezprzewodowa kompaktowa centrala alarmowa DSC, działająca w protokole PowerG

DSC with PowerG Technology

Centrala alarmowa **DSC WP8010** to kompaktowe, bezprzewodowe urządzenie przeznaczone do pracy w obiektach trudnych do zabezpieczenia innymi systemami. Umożliwia lokalizację czujek w znacznej odległości, ma wydłużoną żywotność baterii w urządzeniach bezprzewodowych i stabilność na poziomie systemów przewodowych. Komunikacja ze wszystkimi urządzeniami odbywa się dwukierunkowo i bezprzewodowo. Dzięki zastosowaniu rewolucyjnego protokołu **PowerG**, centrala odpowiada w pełni najwyższym wymaganiom branży zabezpieczeń oraz wyzwaniom dnia jutrzejszego.

Charakterystyka urządzenia:

- Wbudowana klawiatura oraz wyświetlacz LCD do obsługi i konfiguracji systemu
- Obsługa ponad 60 urządzeń bezprzewodowych
- Opcjonalne moduły do komunikacji: GSM/GPRS oraz IP
- Szeroka gama urządzeń bezprzewodowych przeznaczonych do różnych zastosowań
- Konfigurowanie ustawień urządzeń bezprzewodowych z poziomu centrali
- SirenNet – czujki dymu jako sygnalizatory alarmowe
- Współpraca z aplikacją mobilną **DSC WP**

Model	WP8010
Zasilanie	wejście 230 V_{AC}, 50 Hz, wyjście 7,5 V_{DC}
Wymagany akumulator	Specjalny 4,8 V 1300 mAh
Czas podtrzymania na akumulatorze	24 godziny
Wbudowany sygnalizator	tak
Pasma częstotliwości	868-869 MHz
Częstotliwości FHSS	4
Typ komunikacji	Dwukierunkowa
Stopień zabezpieczenia	grade 2
Wbudowany dialer telefoniczny	tak
Obsługiwane formaty komunikacji	SIA, Contact ID
Liczba linii dozorowych przewodowych	1
Liczba wyjść programowalnych PGM	1 (+ opcjonalny moduł 5 wyjść: PGM-5)
Liczba podsystemów	3
Liczba kodów użytkownika	8
Maks. liczba breloków zbliżeniowych	8
Maks. liczba pilotów bezprzewodowych	8
Maks. liczba linii bezprzewodowych	30
Maks. liczba klawiatur bezprzewodowych	8
Maks. liczba sygnalizatorów bezprzewodowych	4
Maks. liczba retransmiterów	4
Wyświetlacz	16-znakowy LCD, jednowierszowy
Pojemność rejestru zdarzeń	250 wpisów

Producent:

AAT HOLDING S.A.
ul. Puławska 431
02-801 Warszawa

tel. +48 22 546 05 46
e-mail: kontakt@aat.pl
www.aat.pl

RWL-1
Zamek bezprzewodowy z okuciem

Zamek **RWL-1** umożliwia realizację jednostronnej, bezprzewodowej kontroli przejścia w systemie kontroli dostępu i automatyki budynkowej RACS 5. Zamek składa się z dwóch szyldów zespolonych z klamkami oraz zamka wpuszczanego w skrzydło. Czytnik zbliżeniowy jest umieszczony w szyldzie zewnętrznym natomiast pojemnik na baterie, w szyldzie wewnętrznym. Rygiel zamka jest na stałe sprzęgnięty z klamką wewnętrzną, co powoduje, że drzwi mogą być otwarte w dowolnej chwili od wewnątrz i bez obecności zasilania bateryjnego. Klamka zewnętrzna jest normalnie odseparowana od rygla i porusza się swobodnie. W momencie przyznania dostępu układ elektroniczny sprzęga klamkę zewnętrzną z ryglem, co umożliwia otwarcie drzwi od zewnątrz. W momencie zamknięcia skrzydła rygiel zamka jest automatycznie uwalniany, co powoduje uzyskanie pełnego poziomu zabezpieczenia drzwi przed otwarciem. Zamek może być opcjonalnie wyposażony w wkładkę patentową, która umożliwia awaryjne otwarcie drzwi przy pomocy tradycyjnego klucza mechanicznego. Stany wszystkich czujników oraz stan baterii są raportowane do systemu kontroli dostępu.

Charakterystyka

- zamek wpuszczany w skrzydło z serwomechanizmem
- rygiel uwalniany samoczynnie w momencie zamknięcia drzwi
- czujnik położenia rygla
- czujnik położenia gałki wewnętrznej
- możliwość dołączenia zewnętrznego czujnika stanu drzwi
- komunikacja bezprzewodowa IEEE 802.15.4/ 2,4 GHz
- zasięg komunikacji 50 m w otwartej przestrzeni
- karty ISO/IEC 14443A/MIFARE Ultralight/Classic/Plus/DESFire
- możliwość użycia telefonu (Android/NFC) w zastępstwie kart
- cztery wskaźniki LED oraz głośnik sygnalizacyjny
- zasilanie z czterech baterii AA
- typowy czas pracy zamka na jednym zestawie baterii - 2 lata przy 10 odczytach dziennie
- raportowanie stanu baterii do systemu kontroli dostępu
- lokalna sygnalizacja niskiego poziomu baterii
- konfiguracja poprzez połączenie przewodowe lub bezprzewodowe z poziomu aplikacji RogerVDM
- wymiary szyldu bez klamki (sz. x wys. x gł.): 77x242x20 mm
- mocowanie szyldu: 4 wkręty metryczne 5x60 mm
- rozstaw zamka (dystans klamka-wkładka): 72 mm
- odległość od czoła zamka do osi obrotu: 55 mm
- blacha czołowa zaokrąglona: 235x20 mm
- wkładka patentowa jednostronna wraz z kompletem kluczy
- grubość skrzydła drzwiowego od 38 do 55 mm

Producent: roger®

ROGER Sp. z o.o. Sp. k.
Gościszewo 59
82-400 Sztum, woj. Pomorskie

tel. 55 272 0132, faks 55 272 0133
e-mail: roger@roger.pl
http://www.roger.pl

RWL-2
Okucie bezprzewodowe

Okucie **RWL-2** umożliwia realizację jednostronnej, bezprzewodowej kontroli przejścia w systemie kontroli dostępu i automatyki budynkowej RACS 5. Okucie składa się z dwóch szyldów zespolonych z klamkami współpracujących z oryginalnym mechanicznym zamkiem wpuszczanym. Czytnik zbliżeniowy jest umieszczony w szyldzie zewnętrznym natomiast pojemnik na baterie, w szyldzie wewnętrznym. Klamka wewnętrzna jest na stałe sprzęgnięta z trzpieniem współpracującym z zamkiem wpuszczanym, przez co, drzwi mogą być otwarte w dowolnej chwili od wewnątrz i bez obecności zasilania bateryjnego. Klamka zewnętrzna jest normalnie odseparowana od trzpienia i porusza się swobodnie. W momencie przyznania dostępu układ elektroniczny sprzęga klamkę zewnętrzną z trzpieniem współpracującym z zamkiem wpuszczanym, co umożliwia otwarcie drzwi od zewnątrz. Okucie współpracuje ze standardową wkładką patentową, która umożliwia awaryjne otwarcie drzwi przy pomocy tradycyjnego klucza mechanicznego (w przypadku zastosowania mechanicznego zamka wpuszczanego wyposażonego w dźwignię otwierania bez użycia klamki). Okucie umożliwia dołączenie zewnętrznych czujników otwarcia drzwi oraz położenia rygla. Stany wejść czujnikowych oraz stan baterii są raportowane do systemu kontroli dostępu.

Charakterystyka

- okucie bezprzewodowe z serwomechanizmem
- możliwość dołączenia zewnętrznego czujnika stanu drzwi
- możliwość dołączenia zewnętrznego czujnika stanu rygla
- komunikacja bezprzewodowa IEEE 802.15.4/ 2,4 GHz
- zasięg komunikacji 50 m w otwartej przestrzeni
- karty ISO/IEC 14443A/MIFARE Ultralight/Classic/Plus/DESFire
- możliwość użycia telefonu (Android/NFC) w zastępstwie kart
- cztery wskaźniki LED oraz głośnik sygnalizacyjny
- zasilanie z czterech baterii AAA
- typowy czas pracy 12 miesięcy przy 10 odczytach dziennie
- raportowanie stanu baterii do systemu kontroli dostępu
- lokalna sygnalizacja niskiego poziomu baterii
- konfiguracja niskopoziomowa poprzez połączenie przewodowe lub bezprzewodowe z poziomu aplikacji RogerVDM
- wymiary szyldu przedniego bez klamki (sz. x wys. x gł.): 46x280x27 mm
- wymiary szyldu tylnego bez klamki (sz. x wys. x gł.): 46x280x20 mm
- montaż szyldu na 2 śruby 5x50 mm
- rozstaw zamka (dystans klamka-wkładka): 72 mm
- grubość skrzydła drzwiowego: od 38 do 50 mm

Producent: roger®

ROGER Sp. z o.o. Sp. k.
Gościszewo 59
82-400 Sztum, woj. Pomorskie

tel. 55 272 0132, faks 55 272 0133
e-mail: roger@roger.pl
http://www.roger.pl

AAT HOLDING S.A.
ul. Puławska 431
02-801 Warszawa
tel. 22 546 05 46
faks 22 546 05 01
e-mail: kontakt@aat.pl
www.aat.pl

D PROD S

Oddziały:
ul. Koniczynowa 2A, 03-612 **Warszawa II**
tel./faks 22 743 10 11, 811 13 50
e-mail: aat.warszawa-praga@aat.pl

ul. Antoniuk Fabryczny 22, 15-741 **Białystok**
tel. 85 688 32 33
tel./faks 85 688 32 34
e-mail: aat.bialystok@aat.pl

ul. Łęczycka 37, 85-737 **Bydgoszcz**
tel./faks 52 342 91 24, 342 98 82
e-mail: aat.bydgoszcz@aat.pl

ul. Ks. W. Siwka 17, 40-318 **Katowice**
tel./faks 32 351 48 30, 256 60 34
e-mail: aat.katowice@aat.pl

ul. Prosta 25, 25-371 **Kielce**
tel./faks 41 361 16 32, 361 16 33
e-mail: aat.kielce@aat.pl

ul. Biskupińska 14, 30-732 **Kraków**
tel./faks 12 266 87 95, 266 87 97
e-mail: aat.krakow@aat.pl

ul. Energetyków 13a, 20-468 **Lublin**
tel. 81 744 93 65/66
faks 81 744 91 77
e-mail: aat.lublin@aat.pl

ul. Dowborczyków 25, 90-019 **Łódź**
tel./faks 42 674 25 33, 674 25 48
e-mail: aat.lodz@aat.pl

ul. Racławicka 82, 60-302 **Poznań**
tel./faks 61 662 06 60, 662 06 61
e-mail: aat.poznan@aat.pl

Al. Niepodległości 606/610, 81-855 **Sopot**
tel./faks 58 551 22 63, 551 67 52
e-mail: aat.sopot@aat.pl

ul. Zielona 42, 71-013 **Szczecin**
tel./faks 91 483 38 59, 489 47 24
e-mail: aat.szczecin@aat.pl

ul. Na Niskich Łąkach 26, 50-422 **Wrocław**
tel./faks 71 348 20 61, 348 42 36
e-mail: aat.wroclaw@aat.pl

ACSS ID Systems Sp. z o.o.
ul. Karola Miarki 20C
01-496 Warszawa
tel. 22 832 47 44
faks 22 832 46 44
e-mail: biuro@acss.com.pl
www.acss.com.pl

D PROD PROJ

AGIS FIRE & SECURITY Sp. z o.o.
ul. Palisadowa 20/22
01-940 Warszawa
tel. 22 430 83 01
tel. kom. 604 290 185
faks 22 430 83 02
e-mail: lmarciniak@agisfs.com
www.agisfs.com

B C D I PROD PROJ S

ALARMNET BORKIEWICZ Sp. J.
ul. Karola Miarki 20c
01-496 Warszawa
tel. 22 663 40 85
faks 22 833 87 95
e-mail: biuro@alarmnet.com.pl
www.alarmnet.com.pl

D PROD PROJ S

ALARMTECH POLSKA Sp. z o.o.
Oddział w Gdańsku
ul. Kielnieńska 115
80-299 Gdańsk
tel. 58 340 24 40
faks 58 340 24 49
e-mail: info@alarmtech.pl
www.alarmtech.pl

D PROD PROJ S

ALKAM SYSTEM Sp. z o.o.
ul. Bydgoska 10
59-220 Legnica
tel. 76 862 34 17
e-mail: alkam@alkam.pl
www.alkam.pl

I PROD PROJ

ASSA ABLOY POLAND Sp. z o.o.
ul. Jana Olbrachta 94
01-102 Warszawa
tel. 22 751 53 54
faks 22 751 53 56
e-mail: biuro@assaabloy.com
www.assaabloy.com.pl

D I PROJ S

FIRMA ATLINE SPÓŁKA JAWNA SŁAWOMIR PRUSKI
ul. Franciszkańska 125
91-845 Łódź
tel. 42 236 30 19
faks 42 655 20 99
e-mail: biuro@atline.pl
www.atline.pl

D I PROD PROJ

BOSCH SECURITY SYSTEMS
ul. Jutrzenki 105
02-231 Warszawa
tel. 22 715 40 00
e-mail: securitysystems@pl.bosch.pl
www.boschsecurity.pl

D S

P.W.H. BRABORK LABORATORIUM Sp. z o.o.
ul. Ratuszowa 11
03-450 Warszawa
tel. 22 619 29 49
faks 22 619 25 14
e-mail: brabork@braborklab.pl
www.braborklab.pl

D I PROJ

bt electronics Sp. z o.o.
ul. Dukatów 10
31-431 Kraków
tel. 12 429 36 16, 410 20 33
faks 12 410 85 11
e-mail: bte@bte.pl
www.saik.pl

D I PROD PROJ S

CAMSAT
Gralak Przemysław
ul. Ogrodowa 2a
86-050 Solec Kujawski
tel. 52 387 36 58
faks 52 387 36 58 w. 24
e-mail: camsat@camsat.com.pl
www.camsat.com.pl

D PROD

CBC (Poland) Sp. z o.o.
ul. Anny German 15
01-794 Warszawa
tel. 22 633 90 90
faks 22 633 90 60
e-mail: cbc@cbcpoland.pl
www.cbcpoland.pl

D PROD PROJ S

CMA MONITORING
Spółka z ograniczoną odpowiedzialnością Sp. k.
ul. Puławska 359
02-801 Warszawa
tel. 22 546 0 888
faks 22 546 0 619
e-mail: info@cma.com.pl
www.cma.com.pl

D I PROD PROJ

Oddziały:
ul. Świętochłowicka 3, 41-909 **Bytom**
tel. 32 388 0 950
faks 32 388 0 960
e-mail: bytom@cma.com.pl

ul. Zatorska 36, 51-215 **Wrocław**
tel. 71 342 03 78
tel. kom. 697 972 558
faks 71 341 16 26
e-mail: wroclaw@cma.com.pl

Biura handlowe:
ul. Skośna 12, 30-383 **Kraków**
tel. 12 260 13 96
tel. kom. 882 126 082
faks 12 260 13 95
e-mail: info@cma.com.pl

ul. Nowy rynek 2, 62-002 **Suchy Las k/Poznania**
tel. 61 861 40 51
tel. kom. 601 203 664, 601 410 979
faks 61 861 40 51
e-mail: poznan@cma.com.pl

ul. Hallera 140, lok. 124, 80-416 **Gdańsk**
tel. 58 345 23 24
tel kom. 693 694 339
e-mail: gdansk@cma.com.pl

CONTROL SYSTEM FMN
Al. KEN 96 lok. U-15
02-777 Warszawa
tel. 22 855 00 17/18
faks 22 855 00 19
e-mail: cs@cs.pl
www.cs.pl

D I PROD PROJ S

DAHUA TECHNOLOGY POLAND Sp. z o.o.
ul. Salsy 2, Lisbon Building, Lobby II
02-823 Warszawa
tel. 22 395 74 00
faks 22 395 74 10
e-mail: biuro.pl@global.dahuatech.com
www.dahuasecurity.com/pl

B C D PROD PROJ S

DG ELPRO Sp. J.
ul. Bonarka 21
30-415 Kraków
tel. 12 263 93 85
faks 12 263 93 86
email: biuro@dgelpro.pl
www.dgelpro.pl

D I PROJ

DYSKRET POLSKA
Spółka z ograniczoną odpowiedzialnością Sp. K.
ul. Mazowiecka 131
30-023 Kraków
tel. 12 423 31 00
faks 12 423 44 61
e-mail: office@dyskret.com.pl
www.dyskret.com.pl

D I PROJ

EBS Sp. z o.o.
ul. B. Czecha 59
04-555 Warszawa
tel. 22 518 84 00
faks 22 518 84 99
e-mail: sales@ebs.pl
www.ebs.pl

B C D PROD S

PHU ELPROMA
ul. Syta 177
02-987 Warszawa
tel. 22 396 98 53, 606 270 756
faks 22 396 98 53
e-mail: elproma@elproma.pl
www.elproma.pl

I PROJ

ELSTECH
os. Złota Podkowa 6/4
31-352 Kraków
tel. kom. 570 400 537, 570 400 538
faks 12 350 45 03
e-mail: info@elstech.pl
www.elstech.pl

Eltrox.pl
ul. Główna 23
42-280 Częstochowa
tel. 34 341 14 61
tel. kom. 517 015 471
e-mail: sklep@eltrox.pl
www.eltrox.pl

Oddziały:
ul. Hynka 6/2, 80-465 **Gdańsk**
tel. kom. 517 015 441
e-mail: gdansk@eltrox.pl

ul. 6 sierpnia 14, 90-416 **Łódź**
tel. 42 632 31 24
e-mail: lodz@eltrox.pl

ul. Brynowska 65/4, 40-584 **Katowice**
tel. 32 203 50 73
e-mail: katowice@eltrox.pl

ul. Wybickiego 42A, 31-302 **Kraków**
tel. kom. 501 945 239
e-mail: krakow@eltrox.pl

ul. Dmowskiego 2/1, 45-365 **Opole**
tel. kom. 501 945 246
e-mail: opole@eltrox.pl

ul. Stablewskiego 31/3, 60-223 **Poznań**
tel. kom. 504 904 710
e-mail: poznan@eltrox.pl

ul. Wyszyńskiego 26, 70-203 **Szczecin**
tel. 91 434 78 72
e-mail: szczecin@eltrox.pl

ul. Remiszewska 1/7B, 03-550 **Warszawa**
tel. 22 676 78 40
e-mail: warszawa@eltrox.pl

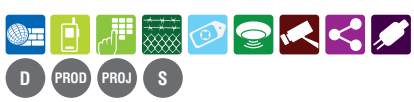
ul. Łopuszańska 22, 02-220 **Warszawa**
tel. kom. 506 601 006
e-mail: warszawa2@eltrox.pl

ul. Komandorska 53R, 50-258 **Wrocław**
tel. kom. 503 127 533
e-mail: wroclaw@eltrox.pl

EUREKA SOFT & HARDWARE
ul. Rynek 13
62-300 Września
tel. 61 437 90 15
e-mail: biuro@eureka.com.pl
www.eureka.com.pl

EUROPEAN SECURITY TRADING POLSKA Sp. z o.o.
ul. Wilcza 54a lok. 1
00-679 Warszawa
tel. 22 629 53 49
e-mail: kontakt@estpolska.pl
http://europeansecuritytrading.com/pl

EWIMAR Sp. z o.o.
ul. Konarskiego 84
01-355 Warszawa
tel. 22 691 90 65
e-mail: handel@ewimar.pl
www.ewimar.pl

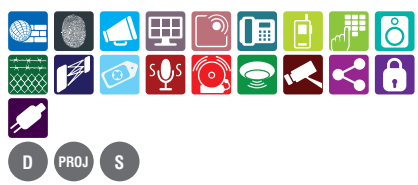


FES Trading Sp. z o.o.
ul. Schuberta 100
80-171 Gdańsk
tel. 58 340 00 41 ÷ 44
faks 58 340 00 45
e-mail: fes@fes.pl
www.fes.pl

GDE POLSKA
Włosań, ul. Świątnicka 88
32-031 Mogilany
tel. 12 256 50 35
faks 12 270 56 96
e-mail: biuro@gde.pl
www.gde.pl

HANWHA TECHWIN EUROPE Ltd.
Baltic Business Park
ul. 1-go Maja 38/39
71-627 Szczecin
e-mail: hte.poland@hanwha.com
www.hanwha-security.eu

ICS POLSKA
ul. Poleczki 82
02-822 Warszawa
tel. 22 646 11 38
faks 22 849 94 83
e-mail: biuro@ics.pl
www.ics.pl



INSAP Sp. z o.o.
ul. Ładna 4-6
31-444 Kraków
tel. 12 411 49 79, 411 57 47
faks 12 411 94 74
e-mail: insap@insap.pl
www.insap.pl

JANEX INTERNATIONAL Sp. z o.o.
ul. Płomyka 2
02-490 Warszawa
tel. 22 863 63 53
faks 22 863 74 23
e-mail: janex@janexint.com.pl
www.janexint.com.pl

KATON Sp. z o.o.
ul. Bajana 31E
01-904 Warszawa
tel. 22 869 43 92
faks 22 869 43 93
e-mail: biuro@katon.eu
www.katon.eu

KOLEKTOR
K. MIKICIUK I R. RUTKOWSKI Sp. J.
ul. Obrońców Westerplatte 31
80-317 Gdańsk
tel. 58 553 67 59
faks 58 553 48 67
e-mail: info@kolektor.pl
www.kolektor.pl

LEGRAND POLSKA Sp. z o.o.
ul. Domaniewska 50
02-672 Warszawa
tel. 22 549 23 30
e-mail: info@legrand.com.pl
www.legrand.pl

MICROMADE
Gałka i Drożdż Sp. J.
ul. Wieniawskiego 16
64-920 Piła
tel./faks 67 213 24 14
e-mail: mm@micromade.pl
www.micromade.pl

MICRONIX Sp. z o.o.
ul. Spółdzielcza 10
58-500 Jelenia Góra
tel. 75 755 78 78
e-mail: info@micronix.pl
www.micronix.pl

NUUXE RADIOTON Sp. z o.o.
ul. Olszańska 5H
31-513 Kraków
tel. 12 393 58 00
faks 12 393 58 02
e-mail: nuuxe@nuuxe.com
www.nuuxe.com

POLON-ALFA
Spółka z ograniczoną odpowiedzialnością Sp. k.
ul. Glinki 155
85-861 Bydgoszcz
tel. 52 363 92 61
faks 52 363 92 64
e-mail: polonalfa@polon-alfa.pl
www.polon-alfa.pl

PROFICCTV Sp. z o.o.
ul. Strzeszyńska 66
60-479 Poznań
tel./faks 61 842 29 62
e-mail: biuro@proficctv.pl
www.profisystems.pl

RAMAR s.c.
ul. Modlińska 237
03-120 Warszawa
Tel. 22 676 77 37, 676 82 87
e-mail: ramar@ramar.com.pl
www.ramar.com.pl

RETT-POL
Bogusław Godlewski
ul. Podmiejska 21
01-498 Warszawa
tel. 22 632 72 22
faks 22 833 09 07
e-mail: biuro@rettpol.pl
www.rettpol.pl

Oddział:
ul. Sportowa 3, 35-111 Rzeszów
tel. 17 785 18 16
faks 22 833 09 07
e-mail: rzeszow@rettpol.pl

ROPAM Elektronik s.c.
Polanka 301
32-400 Myślenice
tel. 12 272 39 71, 341 04 07
faks 12 379 34 10
www.ropam.com.pl

SATEL Sp. z o.o.
ul. Budowlanych 66
80-298 Gdańsk
tel. 58 320 94 00
faks 58 320 94 01
e-mail: satel@satel.pl
www.satel.pl

D I PROD PROJ S

SCHRACK SECONET POLSKA Sp. z o.o.
ul. Domaniewska 44A
02-672 Warszawa
tel. 22 33 00 620
faks 22 33 00 624
e-mail: warszawa@schrack-seconet.pl
www.schrack-seconet.pl

PROD PROJ S

Oddziały:
ul. M. Gomółki 2, 80-279 **Gdańsk**
e-mail: gdansk@schrack-seconet.pl

ul. Jasnogórska 23 lok. 17 (wejście od ul. Stawowej)
31-358 **Kraków**
tel. 12 637 11 74
e-mail: krakow@schrack-seconet.pl

ul. Wierzbięcice 1, 61-569 **Poznań**
tel./faks 61 833 31 53, 833 50 37
e-mail: poznan@schrack-seconet.pl

ul. Mydlana 1, 51-502 **Wrocław**
tel./faks 71 345 00 95
e-mail: wroclaw@schrack-seconet.pl

TAP- Systemy Alarmowe Sp. z o.o.
Os. Armii Krajowej 125
61-381 Poznań
tel. 61 876 70 88
faks 61 875 03 03
e-mail: tap@tap.com.pl
www.tap.com.pl

D PROJ S

Zakład Rozwoju Technicznej Ochrony Mienia TECHOM Sp. z o.o.
Szkoła Elektronicznych Systemów Zabezpieczeń
Al. Wyzwolenia 12
00-570 Warszawa
tel. 22 625 34 00, 622 04 50
Automat zgłoszeniowy 22 625 26 75
e-mail: techom@techom.com
www.techom.com

B C I PROJ S

W2 Włodzimierz Wyrzykowski
ul. Czajcza 6
86-005 Białe Błota
tel. 52 345 45 00
faks 52 584 01 92
e-mail: biuro@w2.com.pl
www.w2.com.pl

B D PROD PROJ

WINKHAUS POLSKA BETEILIGUNGS
Spółka z ograniczoną odpowiedzialnością Sp.K.
ul. Przemysłowa 1
64-130 Rydzyna
tel. 65 525 57 00
faks 65 525 58 00
e-mail: winkhaus@winkhaus.pl
www.winkhaus.pl

D PROD

Legenda

Kategorie*

- bezpieczeństwo IT
- biometria
- DSO
- monitoring
- ochrona fizyczna
- RFID
- systemy domofonowe i wideodomofonowe
- systemy komunikacyjne
- systemy kontroli dostępu
- systemy nagłośnieniowe
- systemy ochrony peryferyjnej
- systemy ochrony zewnętrznej
- systemy przeciwkradzieżowe
- systemy przywoławcze
- systemy sygnalizacji pożarowej
- systemy sygnalizacji włamania i napadu
- systemy telewizji dozorowej
- systemy zintegrowane
- zabezpieczenia mechaniczne
- zasilanie

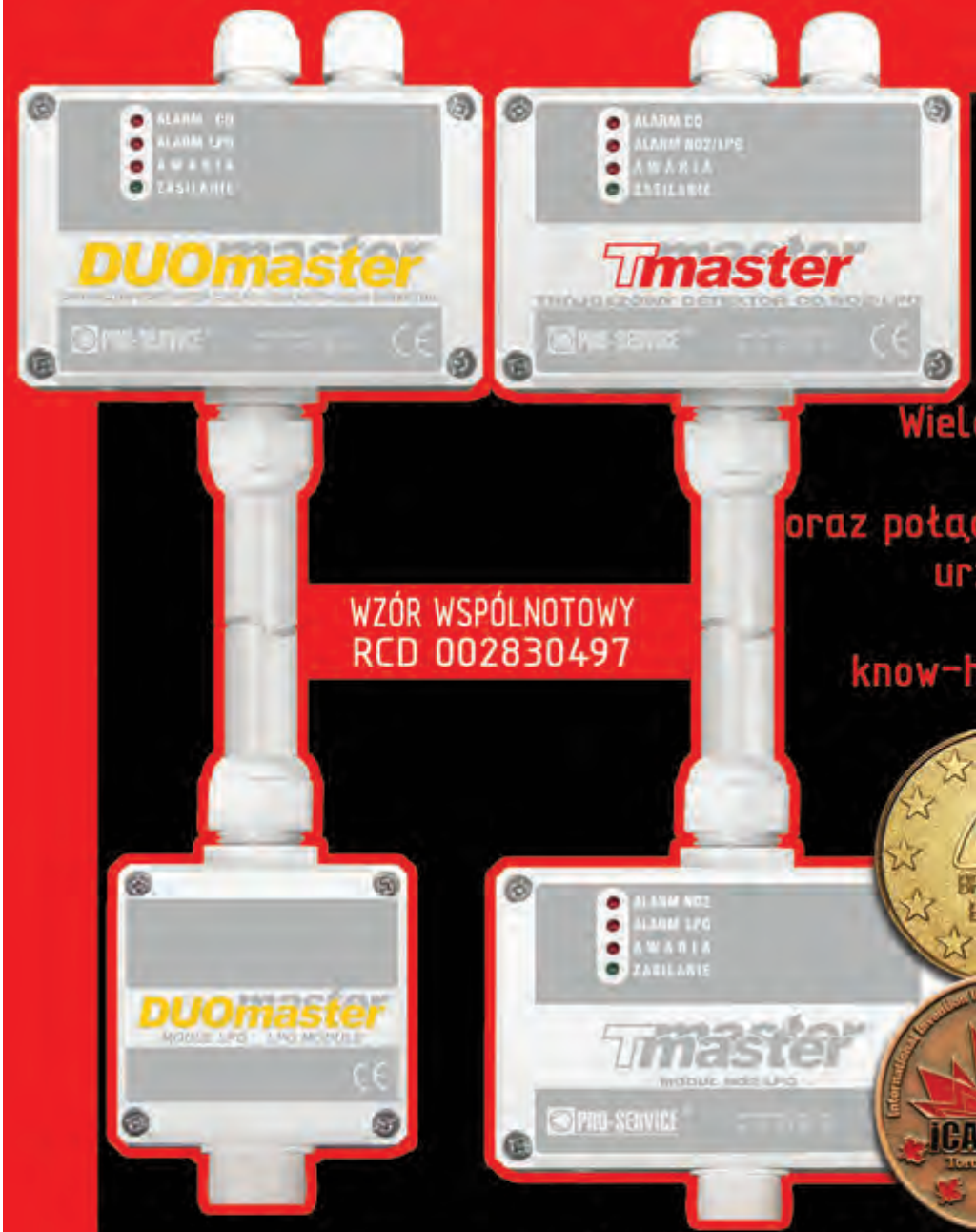
Działalność*

- B badania
- C certyfikacja
- D dystrybucja
- I instalacja
- PROJ projektowanie
- PROD produkcja
- S szkolenia

* Szybkie wyszukiwanie przez filtrowanie na naszej stronie *www.zabezpieczenia.com.pl*

WIELOPUNKTOWY I WIELOGAZOWY SYSTEM DETEKCJI CO/LPG... NO_2... W GARAŻACH I PARKINGACH PODZIEMNYCH

JEŚLI MUSISZ STOSUJ ORYGINALNE



WZÓR WSPÓLNOTOWY
RCD 002830497

Uwaga!

Wielogazowe, stacjonarne detektory gazów oraz połączenie dwóch modułów urządzenia to wyłączne i chronione know-how firmy Pro-Service

PRO-SERVICE®

Przedsiębiorstwo Wdrożeniowe Pro-Service© Sp. z o.o.
Os. Złotej Jesieni 4, 31-826 Kraków, Tel. 12 425 90 90
www.alarmgaz.com

ZABEZPIECZENIA

dwumiesięcznik

Redaktor naczelny
Teresa Karczmarzyk

Redaktorzy merytoryczni
Stanisław Banaszewski
Andrzej Walczyk

Dział marketingu i reklamy
Ela Końka

Redaguje zespół
Marek Blim
Patryk Gańko
Norbert Góra
Daniel Kamiński
Paweł Karczmarzyk
Adam Rosiński
Ryszard Sobierski
Waldemar Szulc
Andrzej Wójcik

Współpraca
Marcin Buczaj
Adam Bułaciński
Piotr Czernoch
Marcin Pyclik
Sławomir Wagner

Skład i łamanie
Piotr Przybylski

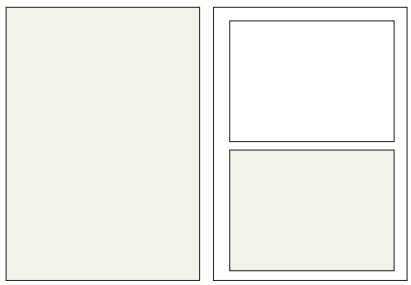
Adres redakcji
ul. Przy Bażantarni 13
02-793 Warszawa
tel. 22 670 09 19
faks 22 649 97 19
www.zabezpieczenia.com.pl

Wydawca
AAT HOLDING S.A.
ul. Puławska 431, 02-801 Warszawa
tel. 22 546 0 546
faks 22 546 0 501

Druk
Regis Sp. z o.o.
ul. Napoleona 4, 05-230 Kobyłka

Dostępne formy reklamy

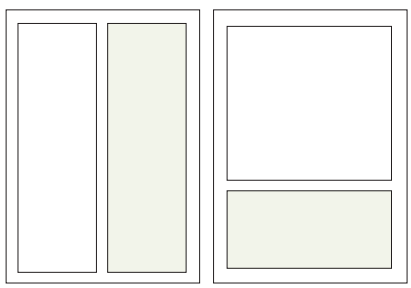
Reklama wewnątrz czasopisma
cała strona, pełny kolor
cała strona, czarno-biała
1/2 strony, pełny kolor
1/2 strony, czarno-biała
1/3 strony, pełny kolor
1/3 strony, czarno-biała
1/4 strony, pełny kolor
1/4 strony, czarno-biała
karta katalogowa, 1 strona



cała strona
(200 x 282 mm + 3mm spad)

1/2 strony
(170 x 125 mm)

Reklama na okładkach
pierwsza strona
druga strona
przedostatnia strona
ostatnia strona



1/2 strony
(83 x 260 mm)

1/3 strony
(170 x 80 mm)

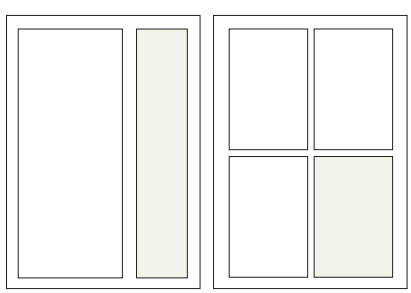
Artykuł sponsorowany
Forma graficzna artykułu sponsorowanego podlega zasadom jednolitym dla wszystkich materiałów zamieszczonych w czasopiśmie)

Spis teleadresowy
Redakcja przyjmuje zamówienia na 6 kolejnych emisji

Ceny negocjujemy indywidualnie

Warunki techniczne przyjmowanych reklam dostępne są na stronie internetowej http://www.zabezpieczenia.com.pl w dziale **Reklama**

Udostępniamy również powierzchnię reklamową na naszej stronie internetowej http://www.zabezpieczenia.com.pl



1/3 strony
(54 x 260 mm)

1/4 strony
(83 x 125 mm)

Spis reklam

DSC

with PowerG Technology

WYKORZYSTAJ DWUKIERUNKOWĄ KOMUNIKACJĘ BEZPRZEWODOWĄ OPARTĄ NA TECHNOLOGII **PowerG**

NOWA KOMPAKTOWA CENTRALA ALARMOWA WP8010

AAT HOLDING S.A.
PRODUCENT I DOSTAWCA ELEKTRONICZNYCH SYSTEMÓW ZABEZPIECZENIA MIENIA
www.aat.pl

BOSCH
Technologia bliżej nas

Oni widzą doskonałą usługę

Zdalny Dostęp

Ty widzisz łatwy i efektywny sposób zarządzania wszystkimi zainstalowanymi systemami.

Bosch umożliwia budowanie bezpieczniejszego świata. Dzięki usłudze zdalnego dostępu oferuje trzy przełomowe rozwiązania. Doświadcz lepszej łączności, stałej dostępności na dowolnym poziomie, oraz pełnej ciągłości działania w każdym miejscu na świecie.