CZASOPISMO BEZPŁATNE ISSN: 1505-2419 DWUMIESIĘCZNIK NR 3(73)/2010

ZABEZPIECZENIA

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

CNB - Nowe spojrzenie na kamery CCTV

CNB TECHNOLOGY Inc

GDE POLSKA
ul. Świątnicka 88, Włosań
32-031 Mogilany

www.gde.pl

W NUMERZE:

ambient SYSTEM

PRODUCENT I DOSTAWCA DŹWIĘKOWEGO SYSTEMU OSTRZEGAWCZEGO ABT-Venas.

INSTYTUT TECHNIKI BUDOWLANEJ
ZAKŁAD CERTYFIKACJI
ul. FILTROWA 1, 00-611 WARSZAWA
tel.: (22) 57 96 167, (22) 57 96 168, fax: (22) 57 96 295

AC 020

CERTYFIKAT ZGODNOŚCI WE
1488-CPD-0132/W

Zgodnie z Dyrektywą Rady Wspólnot Europejskich nr 89/106/EWG z dnia 21 grudnia 1988 roku w sprawie zbliżenia ustaw, rozporządzeń i przepisów administracyjnych państw członkowskich, dotyczących wyrobów budowlanych, zgodnie ze zmianami dokonanymi przez Dyrektywę nr 93/68/EWG Rady Wspólnot Europejskich z dnia 22 lipca 1993 roku potwierdza się, że wyrób budowlany:

Centrala Dźwiękowego Systemu Ostrzegawczego
ABT-Venas
w wersji skupionej i rozproszonej z wyniesionym mikrofonem strażaka

o parametrach wg ZAŁĄCZNIKA nr Z-1488-CPD-0132/W
będącego integralną częścią certyfikatu 1488-CPD-0132/W

wprowadzony do obrotu przez:

Ambient System Sp. z o.o.
ul.Sucha 25
80-531 Gdańsk

produkowany jest w zakładzie produkcyjnym:

Ambient System Sp. z o.o.
ul.Sucha 25
80-531 Gdańsk

w którym Producent wdrożył zakładową kontrolę produkcji i prowadzi badania próbek pobranych w tym zakładzie zgodnie z planem badań. Jednostka notyfikowana – *Instytut Techniki Budowlanej* – przeprowadziła wstępne badania typu w celu określenia właściwości wyrobu oraz wstępną inspekcję zakładu i zakładowej kontroli produkcji, a także prowadzi stały nadzór, ocenę i akceptację zakładowej kontroli produkcji.

Niniejszy certyfikat potwierdza, że Producent spełnia wszystkie wymagania dotyczące oceny zgodności i wyrób posiada właściwości użytkowe opisane w załączniku ZA normy:

EN 54-16:2008

(odpowiednik krajowy: PN-EN 54-16:2008)

Niniejszy certyfikat, wydany po raz pierwszy 23.04.2010, jest ważny dopóki wyrób spełnia wymagania zharmonizowanego dokumentu odniesienia i warunki produkcji oraz system zakładowej kontroli produkcji nie uległy istotnym zmianom.

KIEROWNIK
Zakładu Certyfikacji
Barbara Dobosz

DYREKTOR
Instytutu Techniki Budowlanej
Marek Kaproń

Warszawa, 23.04.2010

Certyfikat zgodności WE dla dźwiękowego systemu ostrzegawczego ABT-Venas.

Ambient System jako pierwszy polski dostawca dźwiękowych systemów ostrzegawczych uzyskał prawo do posługiwania się oznakowaniem CE i wprowadzania do obrotu dźwiękowego systemu ostrzegawczego ABT-Venas zarówno na terenie całego kraju jak i całej Unii Europejskiej. Certyfikat wydany przez Instytut Techniki Budowlanej, zgodnie z zasadą nadrzędnego traktowania norm zharmonizowanych, zastępuje wszelkie krajowe techniczne specyfikacje odniesienia.

ambientsystem.pl

Spis treści

CZASOPISMO ZABEZPIECZENIA 3/2010

Twoja firma
też może stracić dane **42**

Kopie bezpieczeństwa **62**

Oświetlenie światłem podczerwonym
a wymagania dotyczące
przepływności w sieci IP **74**

Bezpieczny łańcuch dostaw **84**

Certyfikat zgodności WE dla DSO ABT-Venas

Firma **Ambient System** informuje, że w związku z ustanowieniem w Polsce normy zharmonizowanej EN 54-16 „Systemy sygnalizacji pożarowej – Część 16: Dźwiękowe systemy ostrzegawcze – Centrale" Ambient System, jako **pierwszy polski dostawca**, uzyskał prawo do wprowadzania do obrotu na terenie kraju i całej Unii Europejskiej, oraz do oznaczania oznakowaniem CE, wyrobu budowlanego **ABT-Venas** służącego do ochrony przeciwpożarowej, jednego z najchętniej kupowanych i instalowanych systemów DSO.

Certyfikat zgodności nr CPD-1488-0132/W został wydany przez Instytut Techniki Budowlanej, posiadający jedno z najlepiej wyposażonych laboratoriów w Europie i dysponujący uznaną kadrą fachowców.

Na mocy **dyrektywy** o wyrobach budowlanych, która została wprowadzona do polskiego prawa w ustawie **z dnia 16 kwietnia 2004 roku o wyrobach budowlanych** (Dz. U. nr 92, poz. 881), norma zharmonizowana **EN 54-16**, dotycząca dźwiękowych systemów ostrzegawczych, określa wymogi funkcjonalne i techniczne, a także sposoby badania oraz oznakowania central DSO.

Zgodnie z przyjętą zasadą nadrzędnego traktowania norm zharmonizowanych norma EN 54-16 zastępuje aprobaty techniczne wydawane przez CNBOP na okres pięciu lat.

W kilku ostatnich latach system **ABT-Venas został zainstalowany w ponad dwustu obiektach** o różnorodnym charakterze użytkowym – od wysokościowych biurowców poprzez hotele i centra handlowe do obiektów sportowych włącznie.

Zainstalowaliśmy nasz system między innymi w hotelu Hilton w Gdańsku, w wysokościowcu Intraco II, na stadionie Lecha w Poznaniu, na stadionie Legii w Warszawie, a także w tunelu w Lalikach.

Więcej informacji znajdą Państwo na stronie *www.ambientsystem.pl*.

Bezpośr. inf. Ambient System

Nowe kamery AXIS M11

Firma **Axis Communications** ogłosiła premierę **AXIS M11** – serii stałopozycyjnych kamer IP obsługujących standard HDTV oraz najnowszy format kompresji obrazu H.264. Ze względu na kompaktowe rozmiary kamery AXIS M11 znajdą zastosowanie przede wszystkim w systemach monitoringu w magazynach, szkołach i placówkach publicznych. – *Ze względu na znakomitą jakość rejestrowanego obrazu, łatwą instalację i korzystną cenę kamery sieciowe AXIS M11 znajdą zastosowanie w wielu systemach monitoringu* – powiedział **Edwin Roobol**, dyrektor zarządzający Axis Communications na obszar krajów niemieckojęzycznych, Holandii i Europy Środkowo-Wschodniej. – *AXIS M11 to także kolejny krok na drodze do upowszechnienia technologii cyfrowego obrazowania w sektorze nadzoru wizyjnego* – dodał Edwin Roobol.

Seria kamer AXIS M11 obejmuje następujące modele:

– **AXIS M1103** z przysłoną stałą oraz **AXIS M1113** z przysłoną DC (kamery wytwarzają obraz o rozdzielczości SVGA);
– **AXIS M1104** z przysłoną stałą oraz **AXIS M1114** z przysłoną DC (kamery wytwarzają obraz o rozdzielczości HDTV 720 skanowanie progresywne/1 Mpx).

Wyposażenie modeli AXIS M1113 i AXIS M1114 w obiektywy o zmiennej ogniskowej z przysłoną DC pozwala wykorzystywać je zarówno w mocno, jak i słabo oświetlonych miejscach. Instalacja kamer AXIS M11 jest niezwykle prosta, a ich obsługę dodatkowo ułatwia zastosowanie przelicznika pikseli, który umożliwia sprawdzenie i dostosowanie rozdzielczości rejestrowanego obrazu do wymagań konkretnej instalacji i potrzeb użytkownika. Niewielkie rozmiary kamer powodują, że urządzenia te można łatwo dopasować do każdej obudowy.

Dzięki funkcji Power over Ethernet (IEEE 802.3af) ten sam kabel służy zarówno do zasilania kamery, jak i przesyłania materiału wizyjnego. Cyfrowa funkcja PTZ (obracania w dwóch płaszczyznach i przybliżania obrazu) pozwala na dokładne skadrowanie konkretnego obszaru. Wszystkie kamery z serii AXIS M11 mogą przesyłać wiele indywidualnie konfigurowanych strumieni wideo o wysokiej jakości, skompresowanych w formacie H.264 i Motion JPEG, z prędkością sięgającą 30 klatek na sekundę.

Kamery sieciowe AXIS M11 współpracują z oprogramowaniem AXIS Camera Station oraz największymi aplikacjami do zarządzania materiałem wizyjnym, stworzonymi w ramach programu Axis Application Development Partner.

Bezpośr. inf. Kamila Wierzbicka
Grayling Poland

Firma Videotec wprowadza na rynek
nową obudowę do kamer PUNTO

Firma **Videotec** stworzyła nową obudowę do kamer **PUNTO**, będącą rezultatem 25 lat doświadczeń w projektowaniu i produkcji urządzeń do systemów CCTV. Celem firmy Videotec jest oferowanie wysoce konkurencyjnych rozwiązań cechujących się niezawodnością oraz wysoką jakością, typową dla produktów tej firmy.

Aerodynamiczny i opływowy kształt nowych obudów PUNTO wskazuje, że wygląd zewnętrzny jest zoptymalizowany pod względem dostępnej wewnętrznej przestrzeni oraz wielkości całej obudowy. Rozmiary obudowy są dopasowane do różnych typów kamer i obiektywów bez uszczerbku dla jakości i łatwości montażu.

Zwarta konstrukcja i prawidłowy dobór materiałów zapewniają wysoki poziom ochrony przed skutkami zmiennych warunków atmosferycznych i wnikaniem pyłów. Obudowa wykonana z odpornych tworzyw polimerowych zapewnia możliwość otwierania bocznej części i tym samym pozwala na łatwy dostęp do kamery i obiektywu. Przednia część obudowy została zaprojektowana tak, aby chronić przed promieniami słonecznymi i deszczem. Typ zasilania kamery jest dobierany w zależności od potrzeb użytkownika.

Nowa obudowa może być montowana na różne sposoby, również z uchwytem z przepustem kablowym. Obudowę można instalować zarówno na zewnątrz, jak i wewnątrz budynków.

Bezpośr. inf. Martina Panighel
Videotec
Tłumaczenie: Redakcja

Axis wprowadza do swojej oferty
modułową tablicę sterującą AXIS T8310

Firma **Axis Communications** wprowadza na rynek nową modułową tablicę sterującą wyposażoną w joystick, klawiaturę oraz pokrętło Jog Dial. Tablica umożliwia precyzyjne sterowanie funkcją obracania w dwóch płaszczyznach i przybliżania obrazu (*pan/tilt/zoom*) w kamerach zainstalowanych w sieci, a także zarządzanie zarejestrowanymi materiałami wizyjnymi. Tablica sterująca AXIS T8310 składa się z trzech elementów:

– joysticka (AXIS T8311) – trzyosiowego, z pokrętłem służącym do obracania w dwóch płaszczyznach i przybliżania obrazu (pan/tilt/zoom), wyposażonego w sześć przycisków;
– klawiatury (AXIS T8312) – stosowanej do szybkiego przełączania się między obszarami roboczymi, kamerami, widokami oraz ustawieniami (*pan/tilt/zoom*);
– pokrętła Jog Dial (AXIS T8313) – używanego do przeszukiwania zarejestrowanego materiału wizyjnego.

Każdy z powyższych elementów można nabyć i stosować osobno. Można też wykorzystywać wszystkie razem jako kompletne rozwiązanie.

– Modułowa tablica sterująca upraszcza proces zarządzania materiałem wizyjnym, umożliwiając wygodne sterowanie funkcją obracania w dwóch płaszczyznach i przybliżania obrazu (pan/tilt/zoom), a także szybkie wybieranie różnych widoków z kamer oraz przeszukiwanie zarejestrowanego materiału – powiedział **Edwin Roobol**, dyrektor zarządzający Axis Communications na obszar krajów niemieckojęzycznych, Holandii i Europy Środkowo-Wschodniej. – *Zaletą tego rozwiązania jest jego elastyczność, gdyż poszczególne elementy można stosować oddzielnie lub wykorzystywać razem. Modułowa tablica sterująca znakomicie uzupełnia ofertę sieciowych rozwiązań do nadzoru wizyjnego Axis* – dodał Edwin Roobol.

Wszystkie trzy elementy są łatwe w instalacji dzięki interfejsowi USB. W przypadku stosowania kompletnej tablicy AXIS T8310 moduły te są połączone ze sobą poprzez interfejs USB, a klawiatura AXIS T8312 pełni rolę koncentratora USB.

Bezpośr. inf. Kamila Wierzbicka
Grayling Poland

Nowa kamera AXIS M1054

Firma **Axis Communications** wprowadziła do sprzedaży niewielką kamerę sieciową **AXIS M1054**, zaprojektowaną do dyskretnego nadzoru w małych firmach, butikach, restauracjach, hotelach i budynkach mieszkalnych.

– Kamera AXIS M1054 uzupełnia niezwykle popularną serię AXIS M10, wprowadzoną do sprzedaży w ubiegłym roku. Na życzenie klientów kamera AXIS M1054 może być zasilana w systemie Power over Ethernet i ma rozdzielczość HDTV, dzięki czemu stanowi dobre jakościowo i niedrogie rozwiązanie do nadzoru wizyjnego – powiedział **Erik Frännlid**, dyrektor ds. zarządzania produktami w Axis Communications.

Najnowsza kamera z serii AXIS M10 zapewnia znakomitą jakość obrazu w rozdzielczości HDTV 720p przy częstotliwości wyświetlania 30 klatek na sekundę. Zasilanie Power over Ethernet (IEEE 802.3af) wpływa na zmniejszenie kosztów instalacji, gdyż do zasilania i przesyłu danych wykorzystany jest jeden kabel.

AXIS M1054 oferuje funkcje znane już z modelu AXIS M1031-W (z wyjątkiem interfejsu bezprzewodowego), w tym pasywny czujnik podczerwieni (PIR) do wykrywania ruchu w ciemności oraz białą lampę LED do oświetlania monitorowanego miejsca w razie wykrycia ruchu lub na żądanie użytkownika. Dzięki wbudowanemu mikrofonowi i głośnikowi kamera przesyła dwukierunkowo dźwięk, umożliwiając użytkownikom komunikowanie się z gośćmi lub intruzami. W sytuacji wywołania alarmu kamera może też odtwarzać przesłane przez sieć lub zapisane w pamieci klipy audio. Ponadto model AXIS M1054 jest wyposażony w jedno gniazdo wejściowe i jedno wyjściowe, umożliwiające podłączenie takich urządzeń, jak czujniki i zdalne przekaźniki, które mogą aktywować światła albo otwierać i zamykać drzwi.

AXIS M1054 może przesyłać wiele strumieni wizyjnych z kompresją H.264 i Motion JPEG, co pozwala na optymalizację wykorzystania pamięci masowej i przepustowości sieci. Dzięki technologii progresywnego skanowania kamera wytwarza obrazy o rozdzielczości HD, wolne od efektu rozmycia krawędzi ruchomych obiektów.

Kamera sieciowa AXIS M1054 jest obsługiwana przez liczne, znane w branży aplikacje, służące do zarządzania systemami dozoru wizyjnego, opracowane w ramach programu partnerskiego Axis Application Development, a także przez oprogramowanie AXIS Camera Station.

Bezpośr. inf. Kamila Wierzbicka
Grayling Poland

Videotec
członkiem sojuszu PSIA

Firma **Videotec** przystąpiła do **PSIA** (*Physical Security Interoperability Alliance*) w 2009 roku i przez kilka ostatnich miesięcy aktywnie pracowała nad tym, aby uzyskać pełną wiedzę na temat protokołu. Teraz ten wspólny język został pomyślnie zintegrowany w ramach zespołu **ALBERT** do analityki wideo. Prototyp został pokazany na wystawie ISC WEST w Las Vegas.

Wszyscy odwiedzający stoisko firmy Videotec będą mogli zobaczyć i wypróbować system do zdalnego sterowania telemetrią PTZ poprzez protokół PSIA. Docenią również zaskakujący, nowy sposób, w jaki system ALBERT pomaga operatorom monitorować określoną przestrzeń. Jest on oparty na inteligentnej współpracy pomiędzy zespołami, na zaawansowanym wykrywaniu zdarzeń na zewnątrz obiektu, na łatwości konfigurowania i użytkowania.

Standardy dla sieciowych urządzeń bezpieczeństwa zwiększą rynkowe możliwości rozwiązań wykorzystujących IP jako produktów, które można łatwo zintegrować z innymi, niezależnie od marki. Te standardy umożliwią producentom podkreślenie właściwości i zalet produktów, niezależnie od kosztów.

– Jeśli systemy mówią tym samym językiem, opracowywanie i integracja nowych wyrobów będą łatwiejsze, a jednocześnie użytkownicy uzyskają dostęp do większej liczby produktów kompatybilnych, gwarantujących wizyjnemu systemowi zabezpieczeń dłuższy żywot – twierdzi **Ottavio Campana** z Videotec R&D Albert Group.

Bezpośr. inf. Martina Panighel
Videotec
Tłumaczenie: Redakcja

Rozwiąż test i wybierz kamerę

Firma **Axis Communications** zamieściła na swojej stronie internetowej narzędzie do porównywania i wybierania produktów, dostępne również w postaci aplikacji do iPhone'ów. Nowe narzędzie pozwala instalatorom i klientom na sprawne odszukanie kamer sieciowych, które najlepiej odpowiadają ich potrzebom, dostosowanych do różnych zastosowań. Oferując obecnie ponad 50 modeli kamer sieciowych, firma Axis Communications dysponuje najszerszą na rynku ofertą rozwiązań do nadzoru wizyjnego. Firma zapowiedziała, że planuje wprowadzać nowości w 2010 roku tak szybko, jak w roku 2009.

– Bogata oferta produktów Axis (od urządzeń odpornych na akty wandalizmu poprzez systemy wykrywania ruchu wyposażone w mechanizm wzbudzania alarmu, aż po łączność bezprzewodową i rozdzielczość HDTV) odzwierciedla szeroki zakres zastosowań i środowisk, w których wykorzystywane są nasze kamery. Wprowadzając internetowe narzędzie do wyszukiwania i porównywania produktów Axis, chcemy ułatwić klientom zapoznanie się z naszymi rozwiązaniami i wybór tych, które najbardziej odpowiadają ich konkretnym potrzebom – powiedział **Lars Berg**, wiceprezes ds. marketingu Axis Communications.

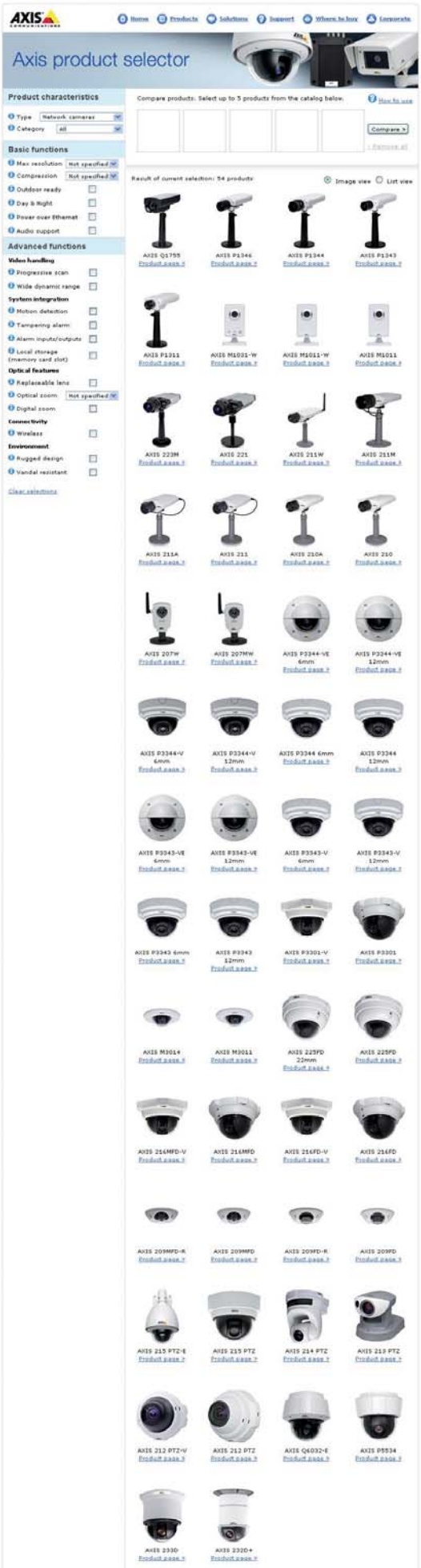
Narzędzie, za pomocą którego można dokonać wyboru optymalnego produktu Axis Communications, jest dostępne pod adresem *www.axis.com*.

– Na podstawie analizy potrzeb klientów wiem, w jakie funkcje musi być wyposażony system sieciowego nadzoru wizyjnego. Jednak nawet z taką wiedzą nierzadko trudno jest dokonać wyboru pomiędzy ofertami różnych dostawców. Moim zdaniem narzędzie do wyboru produktów na stronie internetowej Axis to strzał w dziesiątkę. Pozwoliło mi ono szybko i łatwo znaleźć produkty najlepiej spełniające potrzeby mojego klienta – powiedział **Anders Anell**, dyrektor zarządzający i właściciel Manison Security.

Axis Guide dla iPhone'a – dostęp do zawsze aktualnej oferty produktów Axis w kieszeni

Axis Communications udostępnia dodatkową aplikację dla iPhone'a, dzięki której przebywający w terenie instalatorzy i klienci mogą zapoznać się ze wszystkimi kamerami sieciowymi i enkoderami wizyjnymi, które są dostępne w ofercie firmy Axis, zawęzić wybór produktów za pomocą filtrów, a także bezpośrednio porównać nawet trzy produkty na wyświetlaczu telefonu iPhone. Aplikację Axis Guide można bezpłatnie pobrać ze sklepu Apple App Store *www.apple.com/itunes/*.

Bezpośr. inf. Kamila Wierzbicka
Grayling Poland



Identyfikatory i czytniki w ofercie firmy HID

HID Global oferuje **identyfikatory i czytniki** przeznaczone dla instytucji i organizacji zarządzających i gospodarujących odpadami. Oferowane rozwiązania są przewidziane zarówno dla instytucji gminnych i samorządowych, jak i przedsiębiorstw prywatnych, komunalnych oraz osób prywatnych.

System polega na wykorzystaniu techniki RFID (bezprzewodowej identyfikacji radiowej). HID dysponuje identyfikatorami nadającymi się do zastosowania na pojemnikach, samochodach, w składowiskach itd.

Bezpośr. inf. Jeremy Hyatt
Global Public Relations
Tłumaczenie: Redakcja

Integracja produktów firmy Samsung

z oprogramowaniem Immix firmy Sureview

Dział profesjonalnego bezpieczeństwa grupy **Samsung** poinformował, że wiele kamer CCTV i cyfrowych rejestratorów obrazu DVR z powodzeniem zintegrowano z oprogramowaniem dla alarmowych centrów odbiorczych Sureview Immix.

– Duże nakłady pracy włożone w celu osiągnięcia tego wysokiego poziomu integracji przez ekspertów firm Samsung i Sureview są wiecej niż uzasadnione – twierdzi **Peter Ainsworth**, europejski menedżer produktu w Samsung Techwin Europe. *– Instalatorzy i integratorzy systemów mogą teraz z przekonaniem polecać swoim klientom produkty Samsung CCTV, wiedząc, że alarmowe centra odbiorcze wyposażone w oprogramowanie Immix będą w stanie w pełni wykorzystać właściwości i funkcje naszych nowoczesnych produktów.*

Firmy Samsung i Sureview uzgodniły program bieżącej integracji, w efekcie którego firma Samsung wprowadzi w 2010 roku 170 nowych produktów, w tym bogaty asortyment produktów sieciowych (IP).

– Sformalizowanie naszego partnerstwa z firmą Samsung ma miejsce w szczególnym dla obu stron czasie i zaoferuje zarówno końcowym użytkownikom, jak i integratorom elastyczność i możliwość wyboru urządzeń do zdalnego monitoringu, ponieważ liczba centrów monitorowania korzystających z oprogramowania Immix stale rośnie – twierdzi **Chris Eckersley**, dyrektor sprzedaży Sureview Systems International.

Immix jest oprogramowaniem dla alarmowego centrum odbiorczego, posiadającym atest UL i zaprojektowanym do odbierania sygnałów alarmowych ze standardowych odbiorników alarmów, kamer przemysłowych, urządzeń do analizy sygnałów wizyjnych oraz systemów kontroli dostępu. Immix koreluje zdarzenia alarmowe z materiałami wizyjnymi i fonicznymi z obiektu i przedstawia je operatorowi alarmowego centrum odbiorczego w sposób zapewniający wysoki stopień automatyzacji i łatwość obsługi.

Bezpośr. inf. David Solomons
DRS Marketing
Opracowanie: Redakcja

Megapikselowe kamery IP w standardzie ONVIF

Firma **Eneo** poszerza swoją ofertę produktów telewizji dozorowej IP. Wprowadza **megapiselowe kamery serii NT**, które cechują się bardzo dobrą jakością i przystępną ceną. W ofercie firmy można znaleźć zarówno wersje kopułkowe, jak i klasyczne. W zależności od urządzenia oferowane rozdzielczości mieszczą się w zakresie od 704×576 do 1600×1200 pikseli. Kamery są wyposażone w przetworniki CCD lub CMOS. Dostarczają obraz z maksymalną prędkością 25 kl./s. Dzięki filtrowi IR odcinającemu promieniowanie podczerwone mogą pracować zarówno w dzień i w nocy.

Bogata funkcjonalność

Kamery kopułkowe NLD oraz NXD posiadają zintegrowane obiektywy zmiennoogniskowe 2.8–12 mm ze sterowaniem DC. Aby skompensować silne źródło światła znajdujące się w tle obrazu, niektóre modele wykorzystują funkcję BLC, natomiast w sytuacji, gdy oświetlenie sceny nie jest równomierne, z pomocą przychodzi wydajny algorytm WDR, który rozjaśnia ciemne obszary oraz przyciemnia obszary prześwietlone. Wszystkie kamery są wyposażone także w detektor ruchu oraz cyfrową funkcję PTZ, opartą na predefiniowanych obszarach zainteresowania (ROI – *Region of Interest*). Dostępne są wejścia/wyjścia audio. Niektóre modele posiadają gniazdo na kartę SD, na którą można nagrywać sekwencje wizyjne w sytuacjach alarmowych (30-sekundowe klipy). Wraz z kamerą Eneo IP dostarczane jest bezpłatne oprogramowanie NT-Manager. Można je stosować w instalacjach z maksymalnie 16 kamerami. Oprogramowanie umożliwia podgląd obrazów i definiowanie warunków rejestracji (np. przez kalendarz, w sytuacji alarmowej, w przypadku detekcji ruchu itd.).

Megapikselowe kamery Eneo pozwalają na dokonanie wyboru pomiędzy kopułkami a rozwiązaniami klasycznymi. W pierwszym przypadku są wyposażone w zintegrowany obiektyw oraz zewnętrzną aluminiową obudowę o klasie szczelności IP66.

Standardy i protokoły (ONVIF, PoE)

Przedstawione kamery wykorzystują wiele protokołów sieciowych (IPv4, SMTP, DDNS, HTTP, HTTPS, FTP, DHCP, DSCP, UPnP, RTSP, RTP, TCP, UDP, NTP). Warto wspomnieć, że firma Videor, która jest członkiem ONVIF – forum ds. standaryzacji komunikacji sieciowej urządzeń CCTV, które zostało założone przez firmy Sony, Axis oraz Bosch – kładzie duży nacisk na zintegrowanie produktów Eneo z tym standardem. Obecna, stosowana w kamerach Eneo wersja ONVIF to 1.01. Stosowane w nowych urządzeniach metody kompresji to H.264, MPEG-4 i MJPEG. Dwa strumienie wideo mogą być wysyłane jednocześnie w dwóch różnych formatach (H.264/MJPEG).

Ponadto, aby ułatwić montaż, kamery Eneo IP mogą być zasilane przez sieć, w systemie PoE. Przewidziano także możliwość wykorzystania zasilaczy 12 V_{DC} i 24 V_{AC}.

Bezpieczeństwo

Megapikselowe kamery Eneo pozwalają na jednoczesne zalogowanie dziesięciu osób. Udostępniają bezpieczny, kodowany standard połączenia sieciowego HTTPS. Takie połączenie może być nawiązywane przez przeglądarkę lub przez dostępne oprogramowanie, które pozwala nie tylko na podgląd obrazu, ale również zdalną konfigurację ustawień.

Bezpośr. inf. Krzysztof Krasowski
Videor Oddział w Polsce

Nowy oświetlacz LED
o wysokiej wydajności w ofercie firmy Bosch

Firma **Bosch Security Systems** informuje o wprowadzeniu do sprzedaży nowych, wysokowydajnych oświetlaczy LED **AEGIS SuperLED**, które odznaczają się zarówno wytrzymałą konstrukcją o klasie szczelności IP66, jak również eleganckim wzornictwem. Oświetlacze AEGIS SuperLED, dostępne w wersji promieniowania podczerwonego 850 nm oraz 940 nm, są przeznaczone do zastosowania w najbardziej wymagających systemach bezpieczeństwa. Oświetlacze mogą współpracować z kamerami Dinion firmy Bosch.

Zastosowana w oświetlaczach technologia Constant Light automatycznie reguluje wyjściowy strumień światła w celu kompensacji degradacji diod LED, która ma niekorzystny wpływ na skuteczność urządzenia. Poziom oświetlenia emitowanego przez typowy oświetlacz LED ulega zmniejszeniu nawet o 10% w ciągu kilku pierwszych miesięcy pracy i pogarsza się w czasie całej jego eksploatacji. W praktyce degradacja oświetlacza LED oznacza zmniejszenie zasięgu oraz gorszą jakość obrazu nocą. Są to niedogodności, na które zwracają uwagę zarówno specjaliści z dziedziny ochrony, instalatorzy, jak i użytkownicy końcowi urządzenia. Unikatowa technologia Constant Light, w którą zostały wyposażone wszystkie oświetlacze AEGIS firmy Bosch, rozwiązuje ten problem. Technologia ta zapewnia niezmiennie wysoką jakość i wysoką czytelność obrazów zarejestrowanych nocą przez cały okres eksploatacji, czego potwierdzeniem jest pięcioletni okres gwarancji udzielanej na te oświetlacze.

Cechą wyróżniającą oświetlacze AEGIS SuperLED spośród innych tego typu urządzeń jest innowacyjna technologia produkcji dyfuzora 3D (Black Diamond), który kieruje światło z pierwszego na dalszy plan pola widzenia kamery, dzięki czemu obrazy nocne są oświetlone równomiernie, bez szczególnie jasnych punktów, prześwietleń czy zaciemnionych miejsc.

Wbudowana regulacja mocy pozwala na zasilanie oświetlacza z dowolnego źródła niskonapięciowego, co ułatwia instalację urządzenia i znacznie obniża koszty eksploatacji. W urządzeniu znajduje się specjalny zasilacz impulsowy, bardzo dobrze sprawdzający się w miejscach, w których dostępne jest tylko zasilanie sieciowe.

Oświetlacze AEGIS SuperLED optymalizują warunki pracy zarówno kamer analogowych, jak i cyfrowych, z którymi współpracują. Pozwalają na tworzenie obrazów o wysokim kontraście i niskim zaszumieniu, dzięki czemu zwiększają wydajność platform IP oraz funkcji inteligentnej analizy obrazu. Pozwala to zmniejszyć wymagania dotyczące wielkości dysków twardych i przepustowości sieci, a także znacznie redukuje liczbę fałszywych alarmów.

Daleki zasięg działania (ponad 300 m), wytrzymała konstrukcja o klasie szczelności IP66, niezawodność, niskie koszty utrzymania, powierzchniowo montowane diody LED – wszystkie te cechy sprawiają, że oświetlacze AEGIS SuperLED są najlepszym rozwiązaniem w przypadku krytycznych zastosowań zewnętrznych, takich jak wszelkiego rodzaju ochrona obwodowa czy miejsca użyteczności publicznej. Dzięki atrakcyjnemu wzornictwu oświetlacze AEGIS nadają się również do wykorzystania w miejscach publicznych, w obiektach handlowych, a nawet w przestrzeniach mieszkalnych, a więc tam, gdzie wygląd i estetyka urządzenia dozorowego nabierają szczególnego znaczenia.

Bezpośr. inf. Bosch Security Systems

Klasyczna kamera kompaktowa i minikamery kopułkowe Samsung

z wbudowanymi konwerterami UTP

Kamera kompaktowa **SUB-2000**, przeznaczona do montażu w suficie podwieszanym, kopułkowa **SUD-2080F** i kopułkowa **SUD-2080** do montażu na płaskiej powierzchni posiadają wbudowane konwertery UTP do transmisji sygnału wizji po skrętce na odległość do jednego kilometra.

Firma **Samsung** wprowadziła także nadajnik **SPU-400T UTP**, odbiornik **SPU-400R UTP** oraz urządzenie o nazwie **SPU-100TR**, które zapewnia kompatybilność kamer UTP z istniejącymi urządzeniami łączonymi kablami koncentrycznymi.

Peter Ainsworth, kierownik produktu na Europę w dziale profesjonalnych urządzeń zabezpieczających grupy Samsung, wyjaśnia przyczyny wprowadzenia nowego asortymentu urządzeń z wbudowanymi konwerterami UTP przez firmę Samsung.

– *Coraz częściej architekci wymagają, aby okablowanie UTP było instalowane jako część infrastruktury sieciowej. Wykorzystanie tej infrastruktury w monitoringu zapewni klientom maksymalną korzyść, ponieważ jeden nieekranowany kabel UTP, zwany „skrętką", można nie tylko wykorzystać do przesyłania sygnału wizyjnego i danych sterujących, ale także użyć do zasilania* – powiedział Ainsworth.

Wszystkie trzy kamery są wyposażone w chipset W-5 DSP firmy Samsung oraz wiele funkcji, w tym dodatkowy interfejs BNC do lokalnej konfiguracji lub monitoringu, osiem stref wykrywania ruchu, 12 stref maskowania obszarów prywatności oraz menu ekranowe z wyborem jednego z czternastu języków.

Kamera kompaktowa SUB-2000 jest kamerą kolorową z elektronicznie realizowaną funkcją dzień/noc, natomiast dwie kamery kopułkowe mają funkcję dzień/noc i mechaniczny filtr podczerwieni. Powyższe kamery generują wysokiej jakości kolorowe obrazy o rozdzielczości 600 linii TV przy natężeniu oświetlenia wynoszącym zaledwie 0,05 lx. Ponadto funkcja Sens-up (integracji obrazów) umożliwia generowanie wysokiej jakości obrazów przy bardzo słabym oświetleniu, przy którym inne kamery przełączają się w tryb monochromatyczny.

Stosowana przez firmę Samsung technologia kompensacji tylnego oświetlenia Samsung Super Dynamic Range (SSDR) automatycznie rozjaśnia ciemne obszary obserwowanej sceny, utrzymując jednocześnie ten sam poziom jaskrawości obrazu dla dobrze wyeksponowanych obszarów. Dzięki temu obszary ciemne stają się lepiej widoczne, co umożliwia operatorowi obserwację obiektów ukrytych w cieniu. Kamery są wyposażone także w układ cyfrowej stabilizacji obrazu DIS (*Digital Image Stabilization*), który niweluje drgania kamery podczas silnych wiatrów, oraz technologię redukcji szumów Samsung Super Noise Reduction (SSNRIII).

Dostępny u wszystkich dystrybutorów produktów firmy Samsung nowy asortyment kamer z konwerterem UTP jest oferowany razem z bezpłatnym projektem instalacji, bezpłatną pomocą techniczną i pełną, trzyletnią gwarancją.

Bezpośr. inf. David Solomons
DRS Marketing
Opracowanie: Redakcja

Nowe macierze dyskowe iSCSI

zapewniają najlepszą ochronę nagrań wizyjnych

Firma **Bosch Security Systems** wprowadza na rynek wizyjne **macierze dyskowe iSCSI** z serii **DSA-N2B40**. Charakteryzują się one wyjątkową niezawodnością i skalowalnością, dostosowaną do nawet najbardziej zaawansowanych zastosowań związanych z monitoringiem wizyjnym. Seria DSA stanowi drugą generację wizyjnych macierzy dyskowych firmy Bosch, zaprojektowaną w ramach globalnej współpracy partnerskiej z firmą NetApp.

Macierz DSA-N2B40 zapewnia maksymalny poziom ochrony zapisanych danych wizyjnych dzięki technologii RAID-4 lub RAID-DP. Technologia RAID-DP gwarantuje nieprzerwaną dostępność systemu nawet w przypadku awarii dwóch dysków. Ponadto przed awariami dysków chronią zasilacze oraz wentylatory, których wymiana jest możliwa podczas pracy urządzenia. System zawiera również funkcje raportowania stanu poprawności oraz wczesnego ostrzegania o potencjalnych problemach.

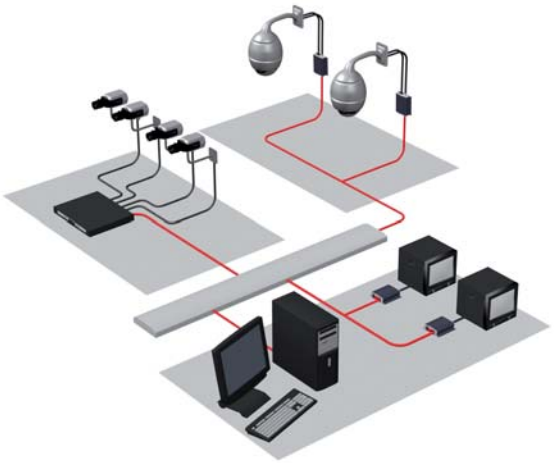
Skalowalne, łatwe do zarządzania sieciowe rozwiązanie pozwala użytkownikom w prosty sposób zwiększać pojemność pamięci, jeśli jest to niezbędne – nawet do 96 TB. Jedna jednostka podstawowa może być podłączona do maksymalnie sześciu jednostek rozszerzeń (półek na dyski), tworząc stos pamięci masowej. Każdy stos to osobny system, który podlega monitorowaniu i zarządzaniu. Wymagany jest dla niego tylko jeden adres IP.

Wydajne produkty z serii DSA-N2B40 charakteryzują się niższymi kosztami użytkowania niż rozwiązania działające w technologii RAID-5. Zawierają cztery porty Gigabit Ethernet, umożliwiające utworzenie nawet 256 szybkich połączeń iSCSI. Podobnie jak wszystkie macierze dyskowe firm Bosch i NetApp, produkty z serii DSA-N2B40 są w pełni zintegrowane z aplikacją Bosch Video Recording Manager 2.0, co umożliwia ich szybką konfigurację. Wizyjne macierze dyskowe są również zgodne z oprogramowaniem Bosch Video Management System 2.x.

Seria DSA-N2B40 wizyjnych macierzy dyskowych iSCSI Video Storage jest częścią bogatej oferty firmy Bosch związanej z rejestrowaniem obrazu CCTV i zarządzaniem nagraniami. Obejmuje ona zarówno bardzo proste czterokanałowe rejestratory CCTV oraz hybrydowe systemy monitoringu, jak i zaawansowane wizyjne macierze dyskowe przeznaczone do najbardziej skomplikowanych zastosowań CCTV.

Bezpośr. inf. Bosch Security Systems

Sprawdź kompatybilność
wizyjnych urządzeń sieciowych



Bosch Security Systems informuje o uruchomieniu interaktywnego serwisu internetowego z informacjami o wizyjnych urządzeniach IP, wersjach wbudowanego oprogramowania oraz funkcjach różnych programów firmy Bosch i innych producentów. Nowy serwis **IP Video Compatibility Zone** udostępnia klientom informacje umożliwiające projektowanie niezawodnych systemów monitoringu z wykorzystaniem najlepszych urządzeń telewizji dozorowej, które można łatwo integrować ze sobą.

Klienci odwiedzający serwis znajdą w nim informacje o produktach i ich funkcjach – takich jak wykrywanie prób ingerencji z zewnątrz, transmisja strumieniowa i powiadamianie o alarmach – realizowanych przez 12 najlepszych systemów firmy Bosch i innych producentów. Klient może wybrać wiele produktów i systemów jednocześnie, a następnie sprawdzić ich zgodność w ramach określonego zbioru producentów i urządzeń.

– *Bezproblemowa integracja to tylko część działań firmy Bosch, które mają na celu rozwój badań w dziedzinie monitoringu, skoncentrowanych na użyteczności obrazu* – powiedział **Dieter Jöcker**, kierownik ds. produktów IP w firmie Bosch Security Systems. – *Efektem tych działań są rozwiązania, które charakteryzują się kompleksową integracją i wyjątkową jakością obrazu* – dodał.

Nowy serwis oferuje także dwa efektywne narzędzia służące do planowania. Tabela zgodności wbudowanego oprogramowania (*Firmware Compatibility*) określa, które jego wersje pasują do kamer IP, koderów, cyfrowych rejestratorów wizyjnych oraz oprogramowania firmy Bosch. Ponadto tabela zgodności koderów i dekoderów (*Encoder-Decoder Compatibility*) określa zgodność pomiędzy konfiguracjami kamera/koder i dekoderami dla kompresji H.264 i MPEG-4. Klienci mogą pobierać tabele zgodności wbudowanego oprogramowania oraz koderów i dekoderów, a następnie korzystać z nich wygodnie w trybie offline.

Bezpośr. inf. Bosch Security Systems

Samsung wprowadza **nowe kamery kopułkowe**
z obiektywami o stałej ogniskowej

Nowe kamery kopułkowe **Samsung** z obiektywami o stałej ogniskowej **SCD-2020**, **SCD-2021** i **SCD-2040** zostały zaprojektowane z myślą o zastąpieniu cieszących się wielkim powodzeniem kamer kopułowych SID-47, SID-48 i SID-49.

Trzy nowe kamery kopułowe, dostępne w konkurencyjnych cenach, zawierają chipset **Samsung W-5 DSP** i dysponują wieloma funkcjami, m.in. wejściem koncentrycznym BNC do lokalnej konfiguracji i lokalnego monitoringu, ośmioma strefami wykrywania ruchu, dwunastoma strefami maskowania prywatności oraz menu ekranowym w czternastu językach.

Kamera SCD-2020 jest dostarczana z obiektywem o ogniskowej 3,7 mm, SCD-2040 – z obiektywem o ogniskowej 8 mm, a SCD-2021 – z obydwiema wersjami obiektywów w celu uzyskania większej elastyczności podczas instalacji. Wszystkie trzy kopułkowe obudowy są wyposażone w kolorowe/monochromatyczne kamery, umieszczone na wsporniku pozwalającym na trójosiową regulację położenia, i tworzą wysokiej jakości barwne obrazy o rozdzielczości 600 linii TV przy minimalnym oświetleniu wynoszącym zaledwie 0,15 lx. Można je montować na ścianie, suficie lub w narożniku.

Dodatkowe funkcje to m.in. technologia redukcji szumów (*Samsung Super Noise Reduction* – SSNRIII) oraz technologia rozszerzająca zakres dynamiki (*Samsung Super Dynamic Range* – SSDR), dzięki której następuje automatyczne rozjaśnianie ciemnych obszarów w całej obserwowanej scenie przy utrzymywaniu tego samego poziomu jasności jaśniejszych obszarów. W ten sposób ciemne obszary stają się lepiej widoczne, umożliwiając operatorowi oglądanie obiektów ukrytych w cieniach.

Kamery SCD-2020, SCD-2021 i SCD-2040 są dostępne u wszystkich dystrybutorów produktów firmy Samsung i są oferowane wraz z możliwością bezpłatnego zaprojektowania systemu, bezpłatną pomocą techniczną i pełną, trzyletnią gwarancją.

Bezpośr. inf. David Solomons
DRS Marketing

Nowa linia kamer firmy Aper

Firma **SPS Trading** wprowadziła do oferty nowe modele kamer z promiennikami podczerwieni, wykorzystujące czterokońcówkowe diody LED. Pozwalają one na budowę promienników o wyższej niezawodności. Diody charakteryzują się większą mocą, przez co ich liczba w układzie może być mniejsza. Cztery wyprowadzenia zapewniają lepszy rozpływ ładunku i szybsze odprowadzanie ciepła z emitera. Zdublowanie ścieżek zasilania pozwoliło zredukować ryzyko wyłączania się poszczególnych sekcji promiennika. Wszystko to sprawia, że zbudowane w ten sposób oświetlacze charakteryzują się bardzo wysoką trwałością i mogą pracować bezawaryjnie przez wiele lat. Ponadto zamiast zwykłego czujnika światła wykorzystano panel słoneczny nieczuły na podczerwień. Dzięki temu promienniki wyłączają się dopiero przy naturalnym słonecznym oświetleniu, a ich pracy nie można zakłócić, kierując na nie wiązkę podczerwieni z innych źródeł.

Do znanej i cenionej przez instalatorów linii VCIR-1652H zostały dodane kolejne produkty o symbolach **VCIR-1782H** i **VCIR-1792H**. Oba modele zamknięto w tulejowych obudowach o klasie szczelności IP66 z pierścieniem separującym elementy optyczne obiektywu od promiennika i tym samym eliminującym wewnętrzne refleksy.

Model VCIR-1782H wyposażono w promiennik o zasięgu 25 metrów, pracujący na standardowej długości fali 850 nm. Model VCIR-1792H zapewnia oświetlenie na odległość dochodzącą do 15 metrów, ale pracuje w zakresie 940 nm, co czyni go niewidzialnym dla ludzkiego oka.

W obu kamerach zastosowano przetwornik Sony generujący obraz o rozdzielczości 520 linii telewizyjnych. W komplecie znajduje się uchwyt montażowy pozwalający na instalację zarówno ścienną, jak i sufitową. Obie wersje są zasilane napięciem 12 V_{DC}.

Bezpośr. inf. Rafał Zieliński
SPS Trading

Kamery o rozszerzonym zakresie dynamiki
Aper VADN-196xH

Firma **SPS Trading** wprowadziła do swojej oferty nową linię kamer marki **APER** o **rozszerzonym zakresie dynamiki**, wykorzystujących przetwornik XDi. **Aper VADN-196xH** to produkt przeznaczony do obiektów, w których występują duże różnice w poziomie oświetlenia obserwowanej sceny. Technologia WDR pozwala bowiem na prawidłową ekspozycję miejsc zarówno słabo, jak i silnie oświetlonych, umożliwiając prawidłową identyfikację osób czy zdarzeń. Tego typu kamery znajdują zastosowanie m.in. w monitoringu wnętrz budynków z przeszklonym lobby. Właściwości użytkowe funkcji WDR są porównywalne z obecnie najbardziej zaawansowanym rozwiązaniem dostępnym na rynku, zastosowanym w kamerach Sanyo Retina.

Kamery charakteryzują się wysoką rozdzielczością 560 TVL (w trybie kolorowym).

Wyposażono je w zaawansowany system cyfrowej stabilizacji obrazu, funkcję cyfrowej redukcji szumów, kompensacji jasnego tła (BLC) oraz detekcji ruchu. Wszystkie posiadają mechanicznie przesuwany filtr podczerwieni i – w przeciwieństwie do tradycyjnych kamer WDR – zapewniają wysoką jakość obrazu także w warunkach słabego oświetlenia.

Od połowy marca dostępne są modele VADN-1960H (zasilany napięciem sieciowym 230 V_{AC}) oraz VADN-1965H (wersja zasilana napięciem niskim 12 V_{DC} / 24 V_{AC}).

Bezpośr. inf. Rafał Zieliński
SPS Trading

Integratorzy systemów bezpieczeństwa

koncentrują się na analizach i projektach w celu zwiększenia swoich przychodów

Według badań **IMS Research** rynek integracji systemów bezpieczeństwa był w roku 2009 oceniany na prawie 5 mld euro. Najszybciej rosnącym typem usługi okazało się analizowanie i projektowanie. W jej przypadku obroty podwoją się w latach 2009–2013.

Analizowanie i projektowanie obejmuje szeroki zakres usług, łącznie z analizą ryzyka, oceną wrażliwości, audytami systemów, analizą polityki bezpieczeństwa, specyfikacją systemów i wymaganiami projektowymi. Historycznie te usługi były trudne do wycenienia, gdyż zwykle są wykonywane na etapie przetargowym, a powinny być traktowane tak, jak instalacja i serwis. Mimo to wielu integratorów systemowych zamierza przesunąć się z rynku instalacyjnego o małej zyskowności w kierunku analizowania i projektowania jako nowego źródła przychodów.

– *Wielu wielkich integratorów definitywnie wycofało się z rynku instalacyjnego. Instalacja jest najmniej zyskownym typem usługi, którą realizuje wielu lokalnych graczy na rynku silnie podzielonym, o wielkiej konkurencji. W wielu przypadkach podwykonawcami są lokalni instalatorzy* – twierdzi **Niall Jenkins**, analityk rynkowy. – Integratorzy twierdzą, że przychód z analizy i projektu daje większe zyski. IMS przewiduje, że integratorzy zwiększą swój portfel usług analizowania i projektowania w ciągu najbliższych kilku lat.

Ostatni zakończony raport IMS – Europejski rynek integracji systemów bezpieczeństwa – wydanie 2010 – omawia ten i inne tematy szczegółowo.

Bezpośr. inf. Alastair Hayfield
IMS Research
Tłumaczenie: Redakcja

Firma Samsung wprowadza 4-kanałowy DVR

z kompresją H.264 i wbudowanym monitorem LCD

Rodzina rejestratorów firmy **Samsung** została uzupełniona o **model SVR-470** z systemem kompresji H.264 pozwalającym zminimalizować wymagania dotyczące przestrzeni dyskowej i szerokości pasma dla obrazów transmitowanych poprzez sieć. Rejestrator umożliwia jednoczesny zapis sygnału wizyjnego w czasie rzeczywistym dla wszystkich czterech kanałów.

Wbudowany w przedni panel rejestratora 3,5-calowy wyświetlacz LCD umożliwia instalatorowi systemu szybki podgląd obrazów. Rejestrator SVR-470 zyska popularność wśród użytkowników poszukujących systemu telewizji dozorowej z niewielką liczbą kamer, ale z najwyższą jakością rejestracji.

SVR-470 posiada wewnętrzny dysk o pojemności 1 TB oraz port USB umożliwiający łatwe kopiowanie materiału wizyjnego. Rejestrator, który jest wyposażony w bezpłatne oprogramowanie zarządzające CMS (*Centralised Management Software*) firmy Samsung, oferuje szeroki wybór innych przyjaznych dla użytkownika funkcji, w tym menu ekranowe w 14 językach, możliwość współpracy z interfejsem sieci Fast Ethernet oraz opcje zapisu tekstów generowanych przez urządzenia ATM-POS. Za pomocą wbudowanych portów RS232C i RS485 rejestrator może sterować kamerami typu PTZ. Urządzenie ma wbudowany ciekłokrystaliczny monitor, ale można podłączyć do niego dodatkowo dwa monitory zewnętrzne, umożliwiając tym samym podgląd na żywo i odtwarzanie zapisanego materiału równocześnie.

Możliwy jest zapis dźwięku we wszystkich czterech kanałach z opcją wykrywania sygnału audio. Dzięki tej funkcji dźwięk zostaje zapisany dopiero po przekroczeniu określonej wartości progowej poziomu dźwięku lub aktywacji alarmu innego typu.

Bezpośr. inf. David Solomons
DRS Marketing
Opracowanie: Redakcja

Międzynarodowa Wystawa Zabezpieczeń

securex 2010

podsumowanie

W dniach od 26 do 29 kwietnia 2010 r. na terenie poznańskich targów odbyła się **Międzynarodowa Wystawa Zabezpieczeń „Securex”**, największa impreza branży zabezpieczeń w Polsce i Europie Środkowej. Targi okazały się rekordowe pod względem wynajętej powierzchni wystawienniczej, liczby prezentowanych nowości oraz odwiedzających targi profesjonalistów.

Tegoroczna, 18. już edycja targów Securex zgromadziła w Poznaniu 260 producentów i dystrybutorów prezentujących kompleksową ofertę z dziedziny systemów wykrywania i zwalczania przestępczości, mechanicznych i elektronicznych systemów zabezpieczeń, systemów nadzoru wizyjnego (CCTV) i ochrony mienia. Na przestrzeni ponad 10000 m^2, w nowoczesnym kompleksie pawilonów 7, 7A, 8, 8A, swoją ofertę zaprezentowali wystawcy z Polski oraz Austrii, Chin, Czech, Danii, Francji, Holandii, Litwy, Niemiec, Polski, Słowacji, Szwecji, Tajwanu, Ukrainy i Wielkiej Brytanii. Podczas targów swoje premiery rynkowe miało ponad 260 nowych produktów i usług. Najliczniej reprezentowane były najnowsze rozwiązania z dziedziny systemów monitoringu wizyjnego i elektronicznych systemów zabezpieczeń, w tym urządzeń do kontroli dostępu i sprzętu zabezpieczająco-alarmowego. Przez cztery dni targi Securex, jak również odbywające się równolegle Międzynarodowe Targi Instalacyjne „Instalacje”, Międzynarodowe Targi Ochrony Pracy, Pożarnictwa i Ratownictwa „Sawo”, Międzynarodowe Targi Branży Wodno-Kanalizacyjnej „Wodociągi” oraz Międzynarodowe Targi Kominkowe „Kominki” odwiedziło blisko 30000 profesjonalistów z branży.


ATLINE
www.atline.pl


SONY


VIVOTEK
Sumo


Genway
SYSTEMY DOMOFONOWE I WIDEODOMOFONOWE


nedap


PS trading
JANEX


ALTRAM


Witamy w
nowym świecie
nadzoru wizyjnego
AXIS


TELENOT


AMPAK
Obiektowy CCTV


ARPOL
MARCH


KONKURS
xtralis


TELENOT


www.janexint.com.pl
INTROX

Najnowsza wiedza z dziedziny zabezpieczeń

Targom Securex towarzyszył bogaty program wydarzeń – konferencji, seminariów, wykładów i pokazów. Patronat nad wydarzeniami objęli Minister Gospodarki, Minister Spraw Wewnętrznych i Administracji, Prezes Związku Banków Polskich oraz Wielkopolski Komendant Wojewódzki Policji w Poznaniu.

Pierwszego dnia targów odbyło się rozstrzygnięcie niezwykle ważnego dla branży konkursu **Polski Mistrz Techniki Alarmowej** zorganizowanego przez Ogólnopolskie Stowarzyszenie Inżynierów i Techników Zabezpieczeń Technicznych i Zarządzania Bezpieczeństwem **„Polalarm"**. W konkursie uhonorowano 13 firm, których produkty uznano za najbardziej postępowe w dziedzinie ochrony mienia. **Laureatem głównej nagrody – Złotej Zbroi w konkursie Polski Mistrz Techniki Alarmowej została firma Linc z Poznania**, która zaprezentowała autonomiczny system nadzoru wideo/audio i rejestracji **Mobotix Q24M-Sec**.

Drugiego dnia targów wielu emocji dostarczył **finał Mistrzostw Polski Instalatorów Systemów Alarmowych** organizowanych przez **PISA**. W rywalizacji wzięło udział sześć zespołów, które zakwalifikowały się do finału po niezwykle trudnych eliminacjach wymagających ogromnej wiedzy i precyzyjnych umiejętności z zakresu instalowania, konserwacji i serwisowania urządzeń systemów alarmowych. Prestiżowy tytuł **Mistrza Polski Instalatorów Systemów Alarmowych 2010** wywalczyli ostatecznie **Michał Bogusz i Zbigniew Fiłkowski z agencji Solid Security ze Szczecina.**

Drugie miejsce i tytuł I Wicemistrza Polski Instalatorów Systemów Alarmowych 2010 zdobył Zespół MR System z Warszawy, który reprezentowali Mariusz Joachimczuk oraz Mariusz Rakowski, natomiast 3. miejsce i tytuł II Wicemistrza Polski Instalatorów Systemów Alarmowych 2010 zdobył zespół Uniwersum z Warszawy (Jakub Dziedzic i Andrzej Sypuła).

Dużą popularnością cieszyła się **I Konferencja Zarządzania Bezpieczeństwem Obiektów** (m.in. obiektów publicznych, szczególnego znaczenia społecznego, sportowych, turystycznych, przemysłowych oraz militarnych). Organizatorzy to MTP i Polalarm. Tematyka konferencji okazała się niezwykle atrakcyjna u progu Mistrzostw EURO 2012. Zorganizowana przez MTP i PISA **konferencja „Wymagania i wytyczne stosowania nowych polskich norm w praktyce projektowania i budowy systemów alarmowych"** zgromadziła liczne grono inwestorów, administratorów i projektantów odpowiedzialnych za organizowanie ochrony ważnych obiektów i zarządzanie systemami bezpieczeństwa fizycznego.

Policja na targach SECUREX

Przez cztery dni targowe Poznań był najbezpieczniejszym miejscem w kraju. Targi Securex przyciągnęły mundurowych z całej Polski. Na targach Securex można było zobaczyć nowoczesne urządzenia i sprzęt policyjny. Wielkopolska Policja oraz Wielkopolski Urząd Wojewódzki przygotowały cykl konferencji propagujących najnowszą wiedzę z dziedziny zabezpieczeń. **Konferencja „Razem bezpieczniej - bezpieczeństwo w miejscach publicznych i miejscu zamieszkania”**, skierowana do służb mundurowych i pracowników samorządów zaangażowanych w zapewnienie bezpieczeństwa i porządku publicznego, pokazała nowatorskie rozwiązania, których przeznaczeniem jest zwiększenie skuteczności działań policji oraz straży miejskiej. Konferencje **„Bezpieczeństwo handlu”** oraz **„Bezpieczeństwo instytucji finansowych”** zgromadziły tymczasem szerokie grono przedstawicieli i pracowników urzędów, instytucji, banków, jak również sieci handlowych i sklepów zainteresowanych przeciwdziałaniem napadom oraz odpowiednim zabezpieczeniem placówki, usług i towarów.

Niezwykle widowiskowe okazały się **pokazy akcji ratowniczej związanej z wypadkiem drogowym**, podczas których zademonstrowane zostały m.in. eksplozje samochodowych poduszek powietrznych. Pokazy były zwieńczeniem konferencji poświęconej bezpieczeństwu na drogach województwa wielkopolskiego, w ramach której zaprezentowane zostały rozwiązania mające na celu ograniczenie liczby wypadków drogowych oraz zmniejszenie liczby ofiar na drogach.


DŹWIĘKOWY SYSTEM
OSTRZEGAWCZY
ABT-Venas


GUNNEBO
For a safer world
Metalkas


AXIS
COMMUNICATIONS


INTEGRAL IP


GŁOŚNIKI POŻAROWE


alarmnet
y3k


DEDICATED MICROS
NetVu
CONNECTED
SAVVO HD


BOSCH
ARPOL
TAMRON
MARCH

Nagrody Międzynarodowych Targów Poznańskich

Poznańskim targom tradycyjnie towarzyszyły **uroczysta gala wręczenia Złotych Medali MTP** oraz **rozstrzygnięcie konkursu Acanthus Aureus**. Złotym Medalem, najcenniejszym trofeum, jakie można zdobyć na poznańskich targach, nagrodzone zostały produkty i usługi, które według Sądu Konkursowego odznaczają się najwyższą jakością i najnowocześniejszymi rozwiązaniami technologicznymi. Są to:

– czytnik kart zbliżeniowych Xpass (Xpass XPM-E Cardco, Łódź),
– sejf Kopenhagen (Inter-Sicherheits-Service, Gorzów Wlkp.),
– stacja interkomowa WS 800F D MD (C&C Partners Telecom, Leszno),
– system sygnalizacji pożarowej i sterowania gaszeniem Integral IP (Schrack Seconet Polska, Warszawa),
– przenośny system ogrodzenia rozwijanego Fencebox (Geobrugg, partner w Polsce, Kraków),
– czujka laserowa Redscan RLS-3060 (SPS Trading, Warszawa),
– system monitoringu CCTV serii HX900 (Zakład Mechaniki i Elektroniki Zamel, J.W. Dzida, K. Łodzińska, Pszczyna),
– seria reflektorów podczerwieni IR Redbeam (Dipol, Kraków),
– lampa kasjerska Decoba 1085 (DCB, Olsztyn),
– kamera MTC-WD 113EF Sony Effio (PHU Merx, D. Migacz, K. Poręba, A. Strózik, Nowy Sącz),
– lekkie kasy pancerne KPL (Konsmetal, Warszawa),
– sejfy LS Laser System (Konsmetal, Warszawa),
– konsola dotykowa Kronos Net 2.0 Revolution (Next!, S. Piela, B. Dryja),
– moduł liniowy 4G2R 808623 (Honeywell Life Safety Austria, przedstawicielstwo w Polsce, Warszawa),
– liniowa czujka dymu Fireray 5000 (Honeywell Life Safety Austria, przedstawicielstwo w Polsce, Warszawa).

Ponadto na targach wyróżniono stoiska najlepiej realizujące założenia strategii marketingowej firmy. Wystawcy zaprezentowali w tym roku imponującą ekspozycję, prześcigając się w pomysłach architektonicznych i graficznych.

Ostatecznie Złotymi Akantami nagrodzono stoiska firm:

– Ambient System,
– Gunnebo Polska,
– MKJ,
– Schrack Seconet Polska,
– SPS Trading.

Bezpośr. inf. Monika Nawrocka
MTP

Zespół targów SECUREX dziękuje...

Za nami osiemnasta już edycja Międzynarodowej Wystawy Zabezpieczeń „Securex", największej imprezy branży zabezpieczeń w Polsce i Europie Środkowej.

Z zadowoleniem informujemy, iż okazała się ona rekordowa pod względem rozmiaru wynajętej powierzchni wystawienniczej, jak również liczby odwiedzających targi profesjonalistów. Przez cztery dni targi Securex, jak również odbywające się równolegle Instalacje, Wodociągi, Kominki i Sawo, odwiedziło blisko 30000 gości poszukujących najnowszych rozwiązań i usług. Na Securexie zaprezentowana została rekordowa liczba 260 nowości debiutujących w ofercie lub po raz pierwszy prezentowanych na targach.

Poziom tegorocznej wystawy był bardzo wysoki, a ekspozycja wystawców zaskoczyła oryginalnością i pomysłowością. Dzięki współpracy i zaangażowaniu wielu firm wspólnie zorganizowaliśmy w Poznaniu niezwykle wartościowe targi przeznaczone dla całej branży zabezpieczeń.

Dziękujemy Państwu za czas zainwestowany w Poznaniu. Mamy nadzieję, że nowe kontakty oraz przeprowadzone podczas czterech dni targowych rozmowy handlowe przyniosą Państwu korzyści i zaprocentują w przyszłości.

Zespół targów SECUREX

Nagrody rozdane

Rozstrzygnięta została **XIII edycja Konkursu Polski Mistrz Techniki Alarmowej**. 11-osobowa komisja konkursowa przyznała następujące nagrody i wyróżnienia w poszczególnych kategoriach:

1. Urządzenia i systemy sygnalizacji włamania i napadu

– I miejsce oraz tytuł Polski Mistrz Techniki Alarmowej 2010 firmie Robert Bosch z Warszawy za centralę alarmową MAP 5000
– wyróżnienie firmie ESAProjekt z Katowic za System Dyskretnego Powiadamiania o Zagrożeniu PORTOS
– wyróżnienie firmie Kabe z Mikołowa za grupę zasilaczy buforowych spełniających wymagania normy PN-EN-50131-6

Firma I.C.S. Polska Hubert Durlik z Warszawy otrzymała podziękowanie za udział w konkursie i prezentację systemu Imperial.

2. Urządzenia i systemy sygnalizacji pożarowej

– I miejsce oraz tytuł Polski Mistrz Techniki Alarmowej 2010 firmie Stekop z Warszawy za System Transmisji Alarmów Pożarowych STAP2009
– wyróżnienie firmie Hortplant – Techniki w Metalu z Nekli za przeciwpożarową kasetkę na klucze Kruse typ 2003

Podziękowanie za udział w Konkursie i prezentację centrali sygnalizacji pożarowej FPA-1200 otrzymała firma Robert Bosch z Warszawy.

3. Urządzenia i systemy nadzoru telewizyjnego i rejestracji obrazów

– I miejsce oraz tytuł Polski Mistrz Techniki Alarmowej 2010 firmie Linc z Poznania za autonomiczny system nadzoru wideo/audio i rejestracji Mobotix Q24M-Sec
– wyróżnienie firmie Axis Communications (Szwecja) za AXIS P1346

– wyróżnienie firmie Axis Communications za AXIS P3344-VE
– wyróżnienie firmie Axis Communications za AXIS Q1755
– wyróżnienie firmie Axis Communications za AXIS Q1910

Podziękowanie za udział w konkursie i prezentację systemu wideonadzoru HD Avigilon otrzymała firma ISM EuroCenter z Warszawy.

Podziękowanie za udział w konkursie i prezentację nowej wersji oprogramowania do inteligentnej analizy obrazu (*Intelligent Video Analysis* – IVA) z funkcją Forensic Search otrzymała firma Robert Bosch z Warszawy.

4. Urządzenia i systemy kontroli dostępu

– wyróżnienie firmie Robert Bosch z Warszawy za oprogramowanie do kontroli dostępu Access Professional Edition z funkcją weryfikacji wideo za pomocą kamery IP NBC-255

Podziękowanie za udział w konkursie i prezentację systemu Vision Expert otrzymała firma APA z Gliwic.

5. Zintegrowane systemy sygnalizacji zagrożeń

– I miejsce oraz tytuł Polski Mistrz Techniki Alarmowej 2010 firmie APA z Gliwic za System Vision Expert

6. Urządzenia i systemy transmisji alarmu oraz monitoringu

– I miejsce oraz tytuł Polski Mistrz Techniki Alarmowej 2010 firmie EBS z Warszawy za system transmisji alarmu wykorzystujący nadajnik PX200N z redundantnym Odbiornikiem Systemu Monitoringu OSM.2007
– wyróżnienie firmie APA z Gliwic za system Vision Expert
– wyróżnienie firmie Robert Bosch z Warszawy za aktywne matryce zmiennokierunkowe Vari-Directional Array

7. Systemy zabezpieczenia przeciwkradzieżowego pojazdów

– I miejsce oraz tytuł Polski Mistrz Techniki Alarmowej 2010 firmie ProSafe z Warszawy za profesjonalny system zabezpieczenia antykradzieżowego pojazdów SAT-DOG ProSafe VIP

8. Inne urządzenia i systemy technicznej ochrony oraz wspomagające ochronę fizyczną

– I miejsce oraz tytuł Polski Mistrz Techniki Alarmowej 2010 firmie System 7 z Bielska-Białej za miniaturową plombę elektroniczną SGSL w wersji przewlekanej i z czujnikiem magnetycznym

Spośród zdobywców I miejsc w poszczególnych kategoriach komisja wyłoniła **zwycięzcę konkursu**. Główną nagrodę w konkursie **Polski Mistrz Techniki Alarmowej 2010 – Złotą Zbroję** – otrzymała firma **Linc z Poznania** za **autonomiczny system nadzoru wideo/audio i rejestracji Mobotix Q24M-Sec**.

Uroczystość ogłoszenia wyników i wręczenia nagród laureatom XIII edycji Konkursu Polski Mistrz Techniki Alarmowej odbyła się w dniu 26 kwietnia 2010 roku, pierwszego dnia Międzynarodowej Wystawy Zabezpieczeń „Securex", na terenie Międzynarodowych Targów Poznańskich.

Bezpośr. inf. Polalarm

Agencja Solid Security zwycięzcą

Mistrzostw Polski Instalatorów Systemów Alarmowych 2010

W finale **II Mistrzostw Polski Instalatorów Systemów Alarmowych**, który miał miejsce w dniu 27 kwietnia 2010 r. podczas Międzynarodowej Wystawy Zabezpieczeń „Securex", zwyciężył zespół **Agencji Solid Security** ze Szczecina w składzie **Michał Bogusz i Zbigniew Fiłkowski**. Mistrzostwa są organizowane przez Międzynarodowe Targi Poznańskie i Polską Izbę Systemów Alarmowych (PISA) pod honorowym patronatem Ministra Spraw Wewnętrznych i Administracji.

Kilka dni przed finałami zespół Securus-Servis z Poznania, zwycięzca eliminacji, wycofał się z udziału w finałach w związku z koniecznością wykonania pilnych zadań zawodowych. W tej sytuacji, zgodnie z regulaminem, finalistą został pierwszy w kolejności zespół rezerwowy – U.S. Uniwersum z Warszawy w składzie Jakub Dziedzic i Andrzej Sypuła. W rezerwie pozostał zespół Agencji Solid Security z Olsztyna, który w pełnym składzie przybył do Poznania.

W finale zmierzyły się ostatecznie: Grupa Solid Security Częstochowa (Krzysztof Kwaśniak i Maksymilian Pęczak), Agencja Solid Security Szczecin (Michał Bogusz i Zbigniew Fiłkowski), Microsystem Sopot (Mariusz Waś i Jacek Zieliński), MR System Warszawa (Mariusz Joachimczuk i Mariusz Rakowski), Dyskam Kraków (Czesław Boroń i Paweł Knap), Uniwersum Warszawa (Jakub Dziedzic i Andrzej Sypuła).

Sześciu finalistów – sześć dwuosobowych zespołów wyłonionych z kilkudziesięciu zgłoszonych do eliminacji – zmierzyło się z zadaniami sześciu konkurencji związanych z systemami telewizji dozorowej, sygnalizacji włamania i napadu oraz kontroli dostępu, które przygotowali partnerzy techniczni mistrzostw, a także konkurencji siódmej, nieznanej zespołom przed finałami, przygotowanej przez PISA.

Konkurencja nr 1 (Robert Bosch) – samodzielny montaż i konfiguracja kamery sieciowej NBC255 na stanowisku roboczym, uzyskanie poprawnej jakości obrazu (zogniskowanie sceny – Rotakin – i jej prezentacja w oprogramowaniu Viewer), rejestracja zdarzenia alarmowego zaistniałego w wyniku detekcji ruchu.

Konkurencja nr 2 (Risco Group Poland) – modyfikacja zintegrowanego systemu alarmowego ProSYS w sposób umożliwiający sygnalizację sabotażu.

Konkurencja nr 3 (Risco Group Poland) – modyfikacja bezprzewodowego systemu alarmowego AGILITY w sposób umożliwiający uzyskanie sygnalizacji odłączenia akumulatora stanowiącego źródło awaryjnego zasilania centrali.

Konkurencja nr 4 (GE Security Polska) – podłączenie czujek i zaprogramowanie linii centrali Advisor Advanced oraz pobudzenie czujek w celu demonstracji prawidłowego podłączenia i działania.

Konkurencja nr 5 (GE Security Polska) – podłączenie modułu radiowego i zaprogramowanie 4-przyciskowego pilota w centrali Advisor Advanced, demonstracja prawidłowego uzbrojenia i rozbrojenia systemu.

Konkurencja nr 6 (C&C Partners Telecom) – wysterowanie sygnalizatora optycznego oraz uzyskanie dostępu do szafy serwerowej.

Czas na wykonanie każdego z sześciu zadań – maksymalnie 15 minut.

Konkurencja nr 7 (PISA) – udzielenie w czasie 30 sekund ustnej odpowiedzi na pytanie, do którego przypisano trzy odpowiedzi (z których prawidłowa mogła być jedna lub więcej niż jedna), a następnie uzasadnienie wyboru w ciągu 90 sekund. Uznanie odpowiedzi za w pełni poprawną wymagało wskazania wszystkich właściwych odpowiedzi. Zestaw pytań i możliwych odpowiedzi w tej konkurencji został zamieszczony po treści komunikatu.

Oficjalnego otwarcia finału II Mistrzostw Polski Instalatorów Systemów Alarmowych dokonali Andrzej Byrt, prezes zarządu MTP, i Mirosław Krasnowski, prezes zarządu PISA.

Miejsca dla VIP-ów w Parku Mistrzostw zajęli oficjalni reprezentanci sponsorów i partnerów technicznych: Agata Majkucińska (Axis Communications), Janusz Grodzki (Siemens), Józef Bycul (Robert Bosch), Kazimierz Kacprzyk (Risco Group Poland), Sławomir Makowski (GE Security Polska), Marek Katarzyński (C&C Partners Telecom), Wiktor Hajduk (Microsystem).

Zmagania zawodników, które trwały 2,5 godziny, omawiał i komentował dla publiczności Georgis Bogdanis z PISA.

Wykonanie zadań konkursowych oceniali sędziowie techniczni będący jednocześnie opiekunami poszczególnych konkurencji: Arkadiusz Gmitrzak (Robert Bosch), Włodzimierz Garwacki (Risco Group Poland), Artur Beta (Risco Group Poland), Rafał Bierniukiewicz (GE Security Polska), Zbigniew Morawski (GE Security Polska), Marek Katarzyński (C&C Partners Telecom), Maksymilian Majerski (PISA).

Nadzór nad prawidłowym przebiegiem finałów sprawowała Komisja Konkursowa Mistrzostw w składzie: Włodzimierz Cieślak (przewodniczący), Maksymilian Majerski, Włodzimierz Matlak, Stefan Jerzy Siudalski.

Oficjalne wyniki finałów:

1) 62 pkt, **1. miejsce i tytuł Mistrza Polski Instalatorów Systemów Alarmowych 2010** zdobył zespół **Agencja Solid Security** Szczecin (**Michał Bogusz** i **Zbigniew Fiłkowski**).
2) 61 pkt, 2. miejsce i tytuł I Wicemistrza Polski Instalatorów Systemów Alarmowych 2010 zdobył zespół MR System Warszawa (Mariusz Joachimczuk i Mariusz Rakowski).

3) 59 pkt, 3. miejsce i tytuł II Wicemistrza Polski Instalatorów Systemów Alarmowych 2010 zdobył zespół Uniwersum Warszawa (Jakub Dziedzic i Andrzej Sypuła).
4) 56 pkt i 4. miejsce zdobył zespół Dyskam Kraków (Czesław Boroń i Paweł Knap).
5) 54 pkt i 5. miejsce zdobył zespół Microsystem Sopot (Mariusz Waś i Jacek Zieliński).
6) 49 pkt i 6. miejsce zdobył zespół Grupa Solid Security Częstochowa (Krzysztof Kwaśniak i Maksymilian Pęczak).

W klasyfikacji nieoficjalnej najlepszymi w poszczególnych konkurencjach okazały się zespoły:

1) konkurencja nr 1 – Dyskam Kraków,
2) konkurencja nr 2 – MR System Warszawa,
3) konkurencja nr 3 – MR System Warszawa,
4) konkurencja nr 4 – Microsystem Sopot,
5) konkurencja nr 5 – Uniwersum Warszawa,
6) konkurencja nr 6 – Agencja Solid Security Szczecin,
7) konkurencja nr 7 – Uniwersum Warszawa, Grupa Solid Security Częstochowa.

Zdobywcy tytułów mistrzowskich otrzymali od organizatorów kryształowe statuetki, dyplomy i nagrody rzeczowe. Mistrzowie Polski otrzymali notebooki Samsung NP-R580-JSO6PL, zdobywcy tytułu I Wicemistrza – aparaty fotograficzne Canon EOS 1000D, a zdobywcy tytułu II Wicemistrza – urządzenia nawigacyjne 7" BLOW GPS70RBT. Pozostali finaliści otrzymali dyplomy uznania i urządzenia nawigacyjne GPS BLOW GPS35V II.

Sponsorzy i partnerzy techniczni Mistrzostw wręczyli finalistom firmowe upominki.

Oficjalnie zamykając II Mistrzostwa Polski Instalatorów Systemów Alarmowych, Przemysław Trawa, wiceprezes zarządu MTP, i Mirosław Krasnowski, prezes zarządu PISA, złożyli gratulacje zwycięzcom i finalistom, a także podziękowali sponsorom, partnerom technicznym, sędziom i wszystkim organizatorom.

Zespół Mistrza Polski Instalatorów Systemów Alarmowych 2010 odebrał zaproszenie na uroczystą Galę Nagród MTP, na której – w gronie laureatów Złotych Medali MTP – został uhonorowany specjalną statuetką prezesa zarządu MTP.

Sponsorami II Mistrzostw Polski Instalatorów Systemów Alarmowych były firmy Axis Communications i Siemens, a partnerami technicznymi – Robert Bosch, C&C Partners Telecom, GE Security Polska, Microsystem, Risco Group Poland. Patronat medialny nad mistrzostwami sprawowały czasopisma *Ochrona Mienia i Informacji*, *Systemy Alarmowe*, *Twierdza*, *Zabezpieczenia* oraz portale branżowe *4safe.pl*, *alarmy.org*, *portal-ochrony.pl*.

Organizatorzy raz jeszcze przekazują słowa podziękowania, uznania i szacunku wszystkim firmom, które zgłosiły zespoły do udziału w eliminacjach II MPISA. Gratulujemy Mistrzowi Polski i zdobywcom pozostałych tytułów mistrzowskich. Gratulujemy zespołom, które – mimo niewielkiej różnicy w wynikach – zakończyły rywalizację w finałach na dalszych miejscach. Gratulujemy wszystkim za wykazaną gotowość sprawdzenia swojej wiedzy i poddania jej ocenie. Dziękujemy sponsorom i partnerom technicznym, którym zawdzięczamy możliwość zrealizowania tego przedsięwzięcia. Dziękujemy Adrianowi Grodzickiemu z firmy Microsystem za przygotowanie, inwencję i realizację wizyjną przebiegu finałów. Dziękujemy patronom medialnym za ich aktywność w popularyzowaniu Mistrzostw.

Bezpośr. inf. Henryk Dąbrowski
PISA

IFSEC 2010
dobre praktyki

Za nami kolejna edycja międzynarodowych targów **IFSEC**, na których, jak wiadomo, pojawiają się wystawcy z całego świata. Wprawdzie w 2009 roku targi w Birmingham były większe od tegorocznych, zarówno pod względem liczby wystawców, jak i zwiedzających, ale i tak trzy ogromne pawilony pełne stoisk zrobiły na odwiedzających duże wrażenie. Widać jednak, że kryzys dotknął także naszą branżę.

Na IFSEC obecni byli przedstawiciele praktycznie wszystkich liczących się na rynku firm z branży ochrony. Poza indywidualnymi stoiskami były także pawilony skupiające przedstawicieli firm z konkretnych krajów, np. USA, Francji, Tajwanu, Chin. Uwidacznia to prężność organizacji branżowych z tych krajów i ich aktywne wspieranie swoich członków za granicą. Niestety polskiego pawilonu nie było. Obecne były stoiska rodzimych firm **Satel, EBS i Next!**

Wśród zwiedzających byli nie tylko Anglicy i Irlandczycy, ale przyjezdni z praktycznie każdego rejonu świata. Osobiście nawiązaliśmy kontakty z firmami z Izraela, Południowej Afryki, Ghany, Angoli, Islandii, Kanady, Serbii, Grecji, Emiratów Arabskich i wielu innych. To duży plus dla targów w Birmingham, ponieważ organizatorzy potrafią ściągnąć odwiedzających z tak wielu krajów.

Sama organizacja i lokalizacja targów też są godne pozazdroszczenia. Tereny targowe są połączone kolejką napowietrzną bezpośrednio z lotniskiem. Przejazd kolejką jest darmowy i zajmuje nie więcej niż pięć minut. W przypadku przedstawicieli firm z południa Polski, takich jak Next!, dojazd na targi Securex do Poznania zajmuje więcej czasu niż dostanie się na lotnisko w Katowicach lub Krakowie i bezpośredni przelot do Birmingham. Teoretycznie, rezerwując poranny lot do Anglii i wieczorny – powrotny – do Polski, można odwiedzić targi i wrócić tego samego dnia. W przypadku skorzystania z tanich linii lotniczych same koszty przelotu też są niewielkie.

Warto wspomnieć o pewnych ciekawostkach. Wszyscy odwiedzający są rejestrowani elektronicznie i dostają kod kreskowy, zaś wystawcy mają czytniki i, zamiast zbierać wizytówki, po prostu odczytują plakietki klientów, dzięki czemu otrzymują listę osób zainteresowanych ich produktami. Jest to wyjątkowo wygodne i praktyczne. Przy wejściu można nawet otrzymać darmową torbę na ulotki, a zwiedzający mogą skorzystać ze stanowisk masażu. Myślę, że jest wiele elementów wartych do przeniesienia na nasz rodzimy grunt. Godne zauważenia są także pozatargowe akcenty polskie – od dużej liczby ekip montujących stoiska, które rozmawiają głównie po polsku, kelnerów i kucharzy z Polski do możliwości wybrania języka polskiego w automatach sprzedających bilety kolejowe. Nawet Brytyjczycy uczą się podstawowych zwrotów w języku polskim. Obecność Polaków jest dostrzegalna praktycznie wszędzie.

Wszystkich, którzy do tej pory skupiali się na regionalnych imprezach targowych, zachęcam do odwiedzania targów IFSEC w celu zapoznania się z międzynarodową ofertą firm z naszej branży.

Bezpośr. inf. Bartłomiej Dryja
Next!

Nagrody IFSEC Security przyznane

Nagrody **IFSEC Security Industry 2010**, honorujące ludzi, wyroby i postęp techniczny, zostały wręczone 10 maja na uroczystym przyjęciu w hotelu Hilton Birmingham Metropole.

Nagrody są przyznawane wspólnie z Brytyjskim Stowarzyszeniem Przemysłu Zabezpieczeń (BSIA). – *Przyznanie nagród IFSEC Security Industry jest idealną okazją do uznania ważnych osiągnięć w przemyśle w ostatnim roku. Nagrody nie tylko promują najlepsze innowacje wśród wyrobów i usług. Dają również przemysłowi okazję do integracji wokół osiągnięć. BSIA jest zobowiązane do promowania jakości i honorowania sukcesów w celu pobudzania postępów w przemyśle* – stwierdził **James Kelly**, dyrektor BSIA.

Finaliści 2010 roku:

Kamery CCTV

– Axis Communications – termiczna kamera sieciowa AXIS Q1910/-E
– IndigoVision – kamera HD PTZ IP
– Panasonic System Networks Europe – kamera WV-CP500
– RayTec – zasilacze serii PRO
– STP Ltd – megapikselowa kamera Logipix dzień/noc 9.1 IP
– Trajet GmbH – Everec 240 3G

System obserwacyjny CCTV (z wyłączeniem kamer i obiektywów)

– Briefcam – BriefCam VS Online
– Duevi – EzyDriveCam
– Genie CCTV – konsola zarządzania systemem wizyjnym Genieus Hybrid 4.0
– IndigoVision – oprogramowanie Video Wall
– Infinova – system zarządzania Invfinova V2216
– Optex Europe – bezprzewodowy system Redwall V SIP

Urządzenia alarmowe – antywłamaniowe lub do ochrony zewnętrznej

– AVS Electronics – BM60HP-BM120HP-BM200HP
– GSM Secure – GSM-VFTA
– Hymatom – Moviwall
– Optex Europe – BoundaryGard-AX-TFR
– Shenzhen Longhorn Security – ePIR
– Sorhea – Solaris

Urządzenia do ochrony fizycznej

– Access Management Solutions – schowek na klucze CyberKey
– APT Controls Ltd – bramki obrotowe
– Centurion Systems – sterownik bramy przesuwnej D10
– Eagle Automation – szybka brama dwuskrzydłowa Eagle
– FAAC – pachołki serii J
– Frontier Pitts – montowana w ziemi blokada Terra Mount

Urządzenia do systemów kontroli dostępu (także biometryczne)

– Access Management Solutions – CyberKey Blue
– Borer Data Systems – system inteligentnej kontroli dostępu Fusion
– Gallagher Security – kontroler Cardax FT 6000
– HID Global – czytnik Omnikey 2061 Bluetooth
– Sagem Securite – MorphoAccess J Series
– Tab Systems – Smarti Guardeon

Łączność

– Cable Vision Electronics – EOC-IN&EOC-AN
– ComNet Europe – samonaprawiający się system transmisji pierścieniowej ComNet Video & Data
– Dedicated Micros – ICR
– Romad – Romad RSP-100
– SafelinQ UK – QlinQ
– WebWayOne – inteligentny system raportowania i serwisowania WebWay

System zintegrowany

– AverMedia Information Inc. – AVerDiGi IWH3216 Touch
– Dedicated Micros – zamknięta TV IP
– Genetec – centrum bezpieczeństwa
– Milestone Systems A/S – Milestone Xprotect Smart Client 5.0
– Urmet Domus Communication & Security UK – system Ipervoice
– Yuan High – SC310.3D N16

Projekt lub instalacja roku

– AD Mobile – GMPTE
– Concept Smoke Screen – System wyświetlania okna antynapadowego
– DVTel – południowoafrykańskie porty lotnicze
– iOmniscient Pty – chiński projekt szybkiego pociągu
– Siemens – Epos-Scan retail shrinkage
– WebWayOne – The Co-Operative Group&WebWay 2424

Usługi ochroniarskie dla Klienta

– FGH Security – Morecambe Bay NHS Trust
– PCL Whitehall – Freshfields Bruckhaus Deringer
– Reliance Security Services – University of Hertfordshire
– Securitas Security Services – Marks and Spencer Plc
– VSG Security – Westfield Derby
– VSG Security – Chiswich Park Estates

Najlepsze partnerstwo policyjne

– schemat zabezpieczeń gminy miejskiej Calderdale (rada miejska Calderdale/zaawansowane bezpieczeństwo/policja West Yorkshire)
– centralny system rejestracji Ipswich (Ipswich Central/policja Suffolk/strażnicy uliczni)
– Operation SISKIN/Challenge 21 Cumbria (FGH Security/policja Cumbria)
– partnerstwo przeciwkryminalne Westfield CastleCourt i Belfast (Westfield Shoppingtowns Ltd./VSG/policja północnoirlandzka)

Źródło: www.securityworldhotel.com
Tłumaczenie: Redakcja

WDR (Szeroki zakres dynamiki)

Funkcja WDR selektywnie rozjaśnia obszary sceny o różnym natężeniu światła w celu prawidłowego wyeksponowania szczegółów w tle obrazu, jak i w pierwszym planie.

WDR wyłączone

WDR włączone

Funkcje zaawansowanej analizy obrazu:

- Wykrywanie przekroczenia zdefiniowanej wirtualnej granicy
- Pojawienie się/ zniknięcie obiektu
- Śledzenie obiektu
- Detekcja ruchu

Funkcja VPS (Wirtualne Progresywne Skanowanie)

Działanie funkcji VPS zapewnia ostre, wyraźne wyodrębnienie krawędzi poruszających się obiektów i tym samym prawidłową reprodukcję detali obrazu.

Skanowanie międzyliniowe (Interlace)

Funkcja VPS

Dedykowane ustawienia

Kamera posiada ułatwiające konfigurację predefiniowane profile ustawień dla szerokiego zakresu warunków pracy.

Wieloboczne strefy prywatności

W pełni skalowalne strefy prywatności wyłączają obszary wrażliwe z podglądu i rejestracji.

Strefy prywatności wyłączone

Strefy prywatności włączone

SSNRIII

Trzecia generacja filtru SSNRIII (Samsung Super Noise Reduction). W warunkach niskiego poziomu oświetlenia eliminuje szumy nie powodując rozmazania obrazu. Funkcja znacznie poprawia jakość obrazu i redukuje rozmiary generowanych plików.

Wyłączone

Włączone

Sterowanie po kablu koncentrycznym

Sterowanie kamerą i realizacja ustawień menu po kablu koncentrycznym gwarantują komfort pracy operatora w centrum monitoringu.

Charakterystyka procesora DSP SV-5 DSP marki Samsung

SV-5 DSP jest ostatnim i najbardziej zaawansowanym procesorem DSP marki Samsung. Możliwość między innymi generacji obrazu o rozdzielczości 650 linii telewizyjnych oraz zaawansowane funkcje jego analizy gwarantują niespotykaną jakość obrazu dla wielu bardzo trudnych warunków pracy.

Procesor SV-5 DSP jest sercem szerokiej gamy kamer klasycznych i kopułowych marki Samsung pozwalając użytkownikom w pełni wykorzystać jego wysoką wydajność i funkcjonalność w różnych instalacjach.

Kamery kopułowe

Kamery kopułowe wandaloodporne

Kamery klasyczne

SV V

T +44 (0)1932 455 308
E STEsecurity@samsung.com
W www.samsungsecurity.com

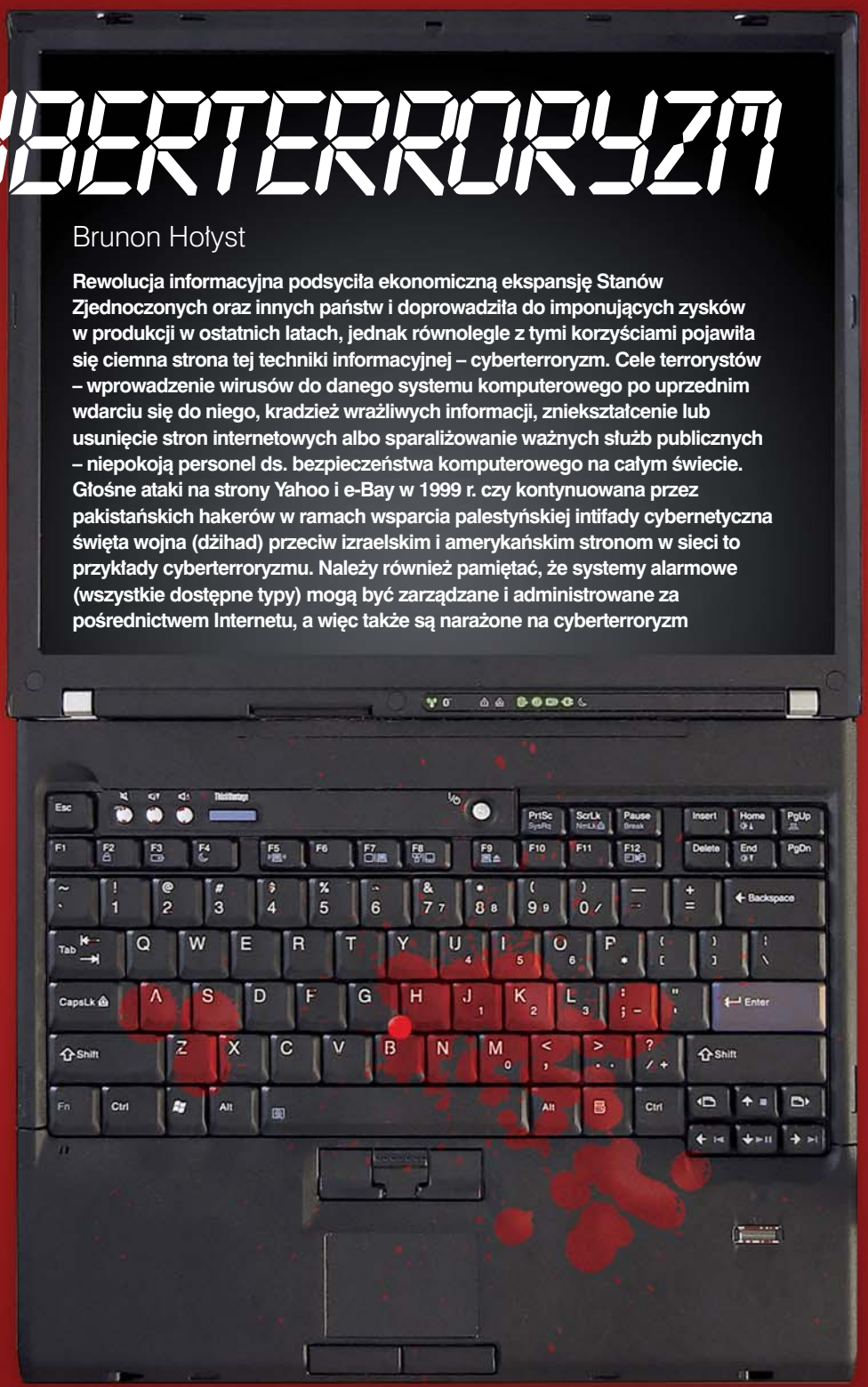
Samsung Techwin Europe Ltd. Samsung House.
1000 Hillswood Drive. Chertsey. Surrey. KT16 0PS. UK

SAMSUNG

CYBERTERRORYZM

Brunon Hołyst

Rewolucja informacyjna podsyciła ekonomiczną ekspansję Stanów Zjednoczonych oraz innych państw i doprowadziła do imponujących zysków w produkcji w ostatnich latach, jednak równolegle z tymi korzyściami pojawiła się ciemna strona tej techniki informacyjnej – cyberterroryzm. Cele terrorystów – wprowadzenie wirusów do danego systemu komputerowego po uprzednim wdarciu się do niego, kradzież wrażliwych informacji, zniekształcenie lub usunięcie stron internetowych albo sparaliżowanie ważnych służb publicznych – niepokoją personel ds. bezpieczeństwa komputerowego na całym świecie. Głośne ataki na strony Yahoo i e-Bay w 1999 r. czy kontynuowana przez pakistańskich hakerów w ramach wsparcia palestyńskiej intifady cybernetyczna święta wojna (dżihad) przeciw izraelskim i amerykańskim stronom w sieci to przykłady cyberterroryzmu. Należy również pamiętać, że systemy alarmowe (wszystkie dostępne typy) mogą być zarządzane i administrowane za pośrednictwem Internetu, a więc także są narażone na cyberterroryzm



Cyberterroryzm jako zagrożenie bezpieczeństwa

Wiele informacji sieciowych ma wpływ nie tylko na rodzaje celów i broni wybieranych przez terrorystów, ale również na metody działania ugrupowań terrorystycznych i strukturę ich organizacji. Kilka spośród najbardziej niebezpiecznych organizacji wykorzystuje technikę informacyjną: komputery, oprogramowanie, urządzenia telekomunikacyjne i Internet w celu lepszej organizacji i koordynacji rozproszonych działań. Podobnie jak wiele korporacji wykorzystujących Internet do skuteczniejszych i bardziej elastycznych działań, terroryści wprzęgają siłę informacji technicznej (IT) do tworzenia nowych doktryn operacyjnych i form organizacyjnych. Podobnie jak firmy prywatne tworzą sojusznicze sieci dla zaopatrzenia klientów w komplet usług, tak ugrupowania terrorystyczne odchodzą od hierarchicznej biurokracji, stają się zdecentralizowane i często zmieniają sieć ugrupowań złączonych wspólnymi celami.

Powstanie powiązanych sieciowo ugrupowań terrorystycznych stanowi część szerszej koncepcji, określanej przez Arquillę i Ronfeldta jako „wojna sieciowa" (*netwar*)[1]. Pojęcie to odnosi się do wyłaniającego się modelu konfliktów i przestępczości na płaszczyźnie społecznej, obejmującego przedsięwzięcia niewystępujące w tradycyjnej wojnie; w modelu tym uczestnicy działają w małych rozproszonych grupach, które komunikują się i koordynują akcje oraz prowadzą kampanie bez centralnego dowództwa.

Organizacje terrorystyczne, korzystające z sieci, mają trzy główne cechy:

– komunikacja i koordynacja są budowane i zmieniane stosownie do zadań; powiązania są często nieformalne i o różnym stopniu intensywności, zależnie od potrzeb;
– wewnętrzne sieci są zwykle uzupełniane przez łączność z osobami spoza organizacji, wychodząc też poza granice państwowe;
– wewnętrzne i zewnętrzne więzy umożliwiają nie biurokratyczne zarządzanie, lecz podzielane wspólnie normy i wartości oraz wzajemne zaufanie.

Powstanie sieciowych układów w organizacjach terrorystycznych stanowi część szerszego ruchu poza formalnymi, sponsorowanymi przez państwo grupami w kierunku prywatnie finansowanych, luźnych sieci osób i podgrup, które mogą mieć strategiczne kierownictwo, ale cieszą się taktyczną niezależnością.

Na Bliskim Wschodzie organizacje terrorystyczne mają różne pochodzenie i ideologię, a większość tradycyjnych organizacji wiąże się z Organizacją Wyzwolenia Palestyny (PLO). Nowsze organizacje, mniej hierarchiczne, takie jak Hamas, Palestyński Islamski Dżihad, Hezbollah, Zbrojna Islamska Grupa Algierska (GIA), Egipska Grupa Islamska i sieć Al-Kaidy, stały się najbardziej aktywne. Na przykład w Egipcie Grupa Islamska, zwana też al-Gamat al-Islamiya, przeprowadziła w 1997 r. atak na turystów w Luksorze, zabijając 58 z nich oraz czterech Egipcjan.

Najbardziej interesującym przykładem terrorystycznej wojny sieciowej jest działalność Usamy Ibn Ladina, mającego wpływ na sieć względnie autonomicznych grup finansowanych przez niego. Jego „święta wojna", wypowiedziana Stanom Zjednoczonym, Izraelowi i całemu Zachodowi, jest prowadzona przy pomocy nieregularnych, lecz bardzo mobilnych sił. Ibn Ladin utrzymuje związki nie tylko z organizacjami na Bliskim Wschodzie (Egipską Grupą Islamską, Narodowym Frontem w Sudanie, Hezbollahem w Libanie), ale też na Filipinach (z Grupą Abu Sayyafa) oraz na Kaukazie (w Czeczenii).

Nowe techniki komunikacji i komputeryzacji nadają sieci trojakie cechy[2]:

– zredukowanie czasu transmisji, które umożliwia rozproszonym organizacjom (grupom) porozumiewanie się i koordynowanie zadań;
– znaczne zmniejszenie kosztów komunikacji, które sprzyja rozproszeniu organizacji przez decentralizację;
– zwiększenie zakresu i kompleksowości informacji.

Takie innowacje, jak telekonferencje czy czaty internetowe, pozwalają uczestnikom na szeroką wymianę informacji bez względu na odległość. Posługiwanie się Internetem przyspiesza mobilizację członków grup terrorystycznych, umożliwia dialog między nimi i zwiększa elastyczność organizacji przez możliwość zmiany taktyki w razie potrzeby. Członkowie grup terrorystycznych mogą dzielić się na podgrupy, ustalać miejsca spotkania, przeprowadzać operacje terrorystyczne, po czym szybko przerywać swoje powiązania i rozpraszać się.

Zgodnie z raportami osób, które były w górskiej kwaterze Ibn Ladina w Afganistanie, ten koordynator i finansista terroryzmu dysponuje nowoczesnym komputerem i sprzętem telekomunikacyjnym, a nawet wykorzystuje telefonię satelitarną do koordynacji działań rozproszonych grup. Dysponuje też urządzeniami dającymi mu bezpieczeństwo, gdy korzysta z systemów komunikacji. Najczęściej dyktuje on polecenia asystentowi, który przekazuje je telefonicznie z różnych miejsc. Funkcjonariusze Ibn Ladina używają dysków CD-ROM do zapisu i rozpowszechniania informacji dotyczących rekrutacji członków, produkcji bomb, ciężkiej broni i operacji terrorystycznych. Amerykańskie agencje wywiadowcze otrzymały ostatnio kopie dysków komputerowych zawierających podręczniki szkoleniowe używane przez Ibn Ladina podczas szkolenia rekrutów[3].

Egipscy eksperci komputerowi, którzy walczyli w Afganistanie, opracowali dla Ibn Ladina sieć komunikacyjną na bazie internetowej i e-mailowej. W latach 90., w operacjach antyterrorystycznych przeciw bazom algierskiej GIA, skonfiskowano komputery i dyskietki z instrukcjami dotyczącymi konstrukcji bomb.

Bojowa grupa islamska Hamas również posługuje się Internetem w przekazywaniu operacyjnych informacji. W Stanach Zjednoczonych aktywiści Hamasu wykorzystują kanały dyskusyjne (*chatrooms*) podczas planowania i realizacji operacji. Agenci Hamasu posługują się także pocztą elektroniczną w koordynowaniu akcji w Gazie, na Zachodnim Brzegu Jordanu i w Libanie. Zauważyli oni, że informacje mogą być przekazywane względnie bezpiecznie przez Internet, gdyż wywiad kontrterrorystyczny nie jest w stanie ściśle monitorować całego ich przepływu i treści.

1) J. Arquilla, D. F. Ronfeldt, The Advent of Netwar, Santa Monica, Calif., 1996.

2) P. Monge, F. Janet, Communication technology for global network organizations, w: Shaping Organizational Form: Communication, Connection and Community, red. G. Desanctis, J. Fulk, Thousand Oaks, Calif., 1999.

3) J. Kelly, US acquires reputed terrorism guide, „USA Today" z 18 września 2000.

Ponadto sieci terrorystyczne mogą chronić przepływ informacji dostępnymi technikami, np. programami kodującymi. Nowe programy kodujące są tak wyrafinowane, że kody zabezpieczające pocztę elektroniczną niezwykle trudno jest złamać. Prawdopodobnie izraelskim siłom nie udało się złamać kodów używanych przez Hamas do przesyłania przez Internet instrukcji terrorystycznych ataków[4]. Terroryści mogą posługiwać się też steganografią, tj. metodą ukrywania tajnych danych w innych informacjach, w tym w plikach graficznych. Mogą też kodować transmisje realizowane przez telefony komórkowe, kraść numery takich telefonów i przeprogramowywać je albo używać opłaconych z góry kart telefonicznych sprzedawanych anonimowo. Te ostatnie techniki komunikowania się umożliwiają terrorystom operowanie z prawie każdego zakątka świata przy dostępie do niezbędnej infrastruktury IT. Analitycy twierdzą, że terroryści mający możność kodowania informacji są niezależni od sponsorów i pomocy państwa i mogą zapewnić sobie większy stopień bezpieczeństwa. Inni wskazują, że grupy terrorystyczne mogą zdobywać pieniądze, wykorzystując sieć. Z Pakistanu jest znany przypadek podjęcia tak dużych sum z kont wahhabitów z Arabii Saudyjskiej, że terroryści planowali utworzenie na ich bazie własnego banku[5].

Komunikacja przez kanały elektroniczne może jednak doprowadzić do wykrycia działalności terrorystycznej i odpowiedzialności za nią, ponieważ pozostawia „ślady" cyfrowe. Na przykład kilka lat temu agenci FBI donieśli, że zastosowali internetowy program podsłuchowy, określany jako „mięsożerca" (*carnivore*), do kontroli korespondencji elektronicznej terrorystów. Jednak program ten nie umożliwił śledzenia poczty e-mailowej Ibn Ladina i został oceniony krytycznie.

Sprawa Ramziego Yousefa, który zorganizował pierwszy zamach bombowy na World Trade Center, dowodzi, że technika wieku informacji może być obosiecznym mieczem. Wielokrotne połączenia telefoniczne, które Yousef nawiązywał w czasie przygotowywania zamachu, zostały zarejestrowane w komputerowej bazie danych i umożliwiły wykrycie jego powiązań z terrorystami z Bliskiego Wschodu. Zgubiony przez niego laptop dostarczył agentom wielu informacji, m.in. ujawnił plany przyszłych ataków, czas detonacji ładunków itd[6]. Jest więcej przykładów przechwytywania elektronicznej informacji będącej w posiadaniu terrorystów przez organa policji i bezpieczeństwa. W 1995 r. został aresztowany jeden z przywódców Hamasu, Abd-al-Rahman Zaydan, a jego skonfiskowany komputer zawierał informacje, które pozwoliły na aresztowanie wielu innych podejrzanych o terroryzm. W grudniu 1999 r. w Jordanii aresztowano 15 terrorystów powiązanych z Al-Kaidą i skonfiskowano wiele materiałów do produkcji bomb, karabiny oraz radiowo kontrolowane detonatory. W czerwcu 2000 r. na dyskach komputerów w domu kontrolowanym przez Hezbollah znaleziono nazwiska 19 podejrzanych o dokonywanie zamachów.

Poza umożliwianiem sieciowych form organizacji IT może służyć ulepszeniu zbierania i analizy materiałów terrorystycznego wywiadu – potencjalne cele mogą być wyszukiwane przez Internet. Technologia wieku informacji pozwala terrorystom na prowadzenie trzech rodzajów ofensywnych operacji informacyjnych: pomaga im w zarządzaniu i działaniach propagandowych, może być użyta do zaatakowania celów wirtualnych i w końcu wykorzystana w atakach fizycznych.

Ze względu na znaczenie wiedzy dla prowadzenia wojny sieciowej nie jest dziwne, że terroryści internetowi zaczęli wykorzystywać IT do zarządzania percepcją i propagandy, by wpływać na opinię publiczną, prowadzić rekrutację nowych członków i zdobywać fundusze. Wysyłanie wiadomości i osiąganie intensywnego wsparcia mediów to ważne komponenty strategii terrorystów. Po tradycyjnej telewizji i druku Internet oferuje terrorystycznym ugrupowaniom alternatywne możliwości docierania do opinii publicznej. Zdaniem Hoffmana terroryści tak ulepszyli techniki zarządzania mediami, że stosują je jako taktykę rzeczników prasowych (*spin doctoring tactics*)[7]. Bojówki Hezbollahu mają nawet własnych kamerzystów, którzy filmują izraelskie ofiary. Filmy te docierają później do izraelskiej telewizji.

Dzięki Internetowi informacje o zamachach bombowych mogą małym kosztem przedostać się bezpośrednio ze stron internetowych do prasy – o ile życzą sobie tego terroryści. Terroryści mający bezpośrednią kontrolę treści informacyjnych mogą dokonywać manipulacji obrazami, stosować specjalne efekty i oszustwa.

Internet jest korzystny także ze względu na możliwość mobilizacji czasowej cyberterrorystów (*parttime cyberterrorists*), tj. osób niezwiązanych bezpośrednio i na stałe z ugrupowaniami terrorystycznymi, ale wspierających ich działania. Na przykład zarówno rząd Palestyny, jak i rząd Izraela zachęcały prywatne osoby do przesyłania danych z komputerów w związku z konfliktem dotyczącym świątyni Al-Aksa i późniejszą intifadą.

Terroryści Internetowi mogą wykorzystywać IT do ataków elektronicznych, które wpływają negatywnie na wolę walki przeciwników. Destrukcyjne ataki obejmują także dławienie systemów komputerowych (*choking*) za pomocą takich metod i narzędzi, jak e-bomby, masowe rozsyłanie wiadomości elektronicznych (*fax-spamming*) i włamania hakerów w celu zniekształcenia stron internetowych. Liczba tych destrukcyjnych ataków ma tendencję wzrostową.

Przykładem ataku z wykorzystaniem bomby e-mailowej jest użycie jej przez organizację Tamilskich Tygrysów przeciw misjom dyplomatycznym Sri Lanki w 1996 r. – ta organizacja partyzancka zalała ambasady tego kraju tysiącami informacji, powodując blokadę wirtualną (*virtual blockade*). Z kolei japońskie grupy terrorystyczne zaatakowały komputerowy system kontrolny pociągów podmiejskich, paraliżując wiele miast przez wiele godzin[8].

Złośliwe wirusy i robaki internetowe (*worms*) mogą być stosowane permanentnie do niszczenia bądź fałszowania danych

4) M. Whine, Islamist organizations on the Internet, „Terrorism and Political Violence", 1999, t. 11, nr 1.

5) J. Stern, Pakistan's Jihad Culture, „Foreign Affairs", listopad/grudzień 2000, s. 115–126.

6) S. Reeve, The New Jackals: Ramzi Yousef, Osama Ben Laden and the Future of Terrorism, Boston, Mass, 1999.

7) B. Hoffman, Inside Terrorism, New York 1998, s. 131–134.

8) M. G. Devost, K. H. Brian, A. P. Neal, Information terrorism: Can you trust your toaster?, w: San Tzu and Information Warfare, Washington, DC, 1997.

i powodować szkody gospodarcze. W najgorszym przypadku narzędzia oprogramowania mogą być użyte do zniszczenia ważnych infrastruktur, takich jak kontrola ruchu lotniczego, systemy elektroniczne i wodne kraju.

Jedynie wysoki poziom ochrony istniejących infrastruktur może stanowić dla terrorystów trudną techniczną przeszkodę do pokonania. Jednak rozwój i coraz większe przywiązywanie wagi do elektronicznych ataków ze strony terrorystycznych organizacji mogą uwzględniać również ryzyko i koszty nowych technik. Terroryści zmierzający do rozszerzania zakresu działań ofensywnych będą badać i udoskonalać techniki, by sprostać zabezpieczeniom komputerowym stworzonym przez ekspertów i administratorów. Ten technologiczny„kierat" wymaga ciągłej uwagi.

Wielu ekspertów w dziedzinie bezpieczeństwa komputerów sądzi, że ataki destrukcyjne pozostaną wyzwaniem dla większości grup terrorystycznych i będą zbyt niedoceniane przez media, aby stać się atrakcyjnymi dla terrorystów. W tej sytuacji także terroryści internetowi będą stosować raczej tradycyjną broń i konwencjonalne bomby do fizycznej przemocy i powodowania jak największej liczby ofiar.

Istnieje jednak obawa, że w toku swojej ewolucji sieciowe grupy terrorystyczne zwrócą się ku wykorzystaniu IT do celów ofensywnych i że powstaną nowe, całkowicie wirtualne grupy, które będą operować wyłącznie w cyberprzestrzeni (*cyberspace*). Sugeruje się, że grupy terrorystyczne zaczną bardziej agresywnie eksperymentować techniką wieku informacji. Do ich ofensywności przyczyni się wyższy stopień kooperacji i wymiany informacji wśród terrorystów gotowych do wojny sieciowej.

Taka kooperacja już się rozpoczęła i radykalni islamiści zorganizowali w tym celu nawet „konferencję terrorystyczną"[9]. Nowym grupom mogą przewodzić osoby technicznie Uzdolnione i przygotowane, co sugeruje powstanie hybrydy terrorysty-hakera (*terrorist-cum-hacker*). Takie grupy starałyby się uderzać w sposób zarówno destrukcyjny, jak i zabójczy dla ludności w celu wsparcia działań politycznych i religijnych.

Polityka i taktyka antyterrorystyczna mogą powstrzymać te niebezpieczeństwa tylko wtedy, silne gdy intensywne zwalczanie terroryzmu pozostawi terrorystom mniej czasu na zdobycie nowych technologii. Dlatego politycy i stratedzy walki z terroryzmem powinni przestrzegać poniższych zaleceń:

1) Należy monitorować zmiany w wykorzystaniu IT przez grupy terrorystyczne, odróżniając możliwości organizacyjne od ofensywnych. Ocena, jak IT kształtuje procesy organizacyjne grup i działania ofensywne, stanie się krytycznym elementem oceny zagrożenia. Najbardziej znaczące trendy, wymagające ścisłej kontroli, to powstawanie nowych, potencjalnie niebezpiecznych grup terrorystycznych, wysoce zinformatyzowanych pod względem organizacyjnym i ofensywnym. Należy zidentyfikować te grupy i śledzić je (m.in. rekrutację hakerów).
2) Należy śledzić przepływ informacji w internetowych grupach terrorystycznych. Priorytetem powinno być przechwytywanie wymiany informacji dokonywanej przez terrorystów i realizacja programu Project Trailblazer (pionierów, pomysłodawców) agencji National Security Agency, reprezentującej możliwości wywiadowcze Stanów Zjednoczonych[10]. Nie można też lekceważyć wysiłków zbierania informacji wywiadowczych drogą nieelektroniczną. Gdy Usama Ibn Ladin zauważył, że jego łączność satelitarno-telefoniczna nie jest bezpieczna, zaczął posługiwać się kurierami w przekazywaniu informacji i instrukcji.
3) Należy utrudniać oparte na IT ofensywne operacje informacyjne (przez należy rozumieć oddziaływanie na informacje i systemy informacyjne przeciwnika oraz obronę własnych) terrorystów poprzez lepszą ochronę infrastruktury. Stany Zjednoczone powinny dostrzec szczególne narażenie tych struktur i opracować techniki zabezpieczania się przed oczekiwanymi zagrożeniami. Użyteczne działania w tym zakresie prowadzą National Infrastructure Protection Center i inne powołane w tym celu organizacje. Agencje kontrterrorystyczne powinny też rozważyć opcje zatrudnienia większej liczby hakerów i wykorzystać ich wiedzę w celach defensywnych, a także odwetowych.
4) Należy pokonać terrorystów sieciowych ich własnym sposobem: chodzi o użycie sieci do walki z sieciami. Rządy chcące zwalczać terroryzm sieciowy powinny przyjąć organizacyjne wzorce i strategie podobne do tych, które są stosowane przez przeciwnika. Przykładem może być organizacja Technical Support Working Group (TSWG), zrzeszająca ponad 100 organizacji z 13 agencji federalnych oraz lokalnych i stanowych agencji, których liczba rośnie. Celem TSWG jest opracowywanie technik zwalczania terroryzmu (w 2000 r. grupa otrzymała na ten cel 48 mln dolarów). Inny przykład to plan kontrwywiadowczy Counter-intelligence 21, mający zwiększyć kooperację personelu kontrwywiadowczego CIA, FBI i Pentagonu.

Zwolennicy tych inicjatyw słusznie uznali, że wiek informacji i w konsekwencji nadejście wojen sieciowych zatarły granice między zagrożeniami krajowymi i zagranicznymi. Społeczności kontrterrorystyczne muszą spełniać wymogi lepszej koordynacji działań interagencyjnych[11].

W latach osiemdziesiątych XX wieku Barry Collin z Institute for Security and Intelligence w Kalifornii ukuł termin „cyberterroryzm" jako pojęcie zbieżne dla przestrzeni cybernetycznej i terroryzmu[12], natomiast Mark Pollit, agent FBI, zaproponował definicję roboczą: „Cyberterroryzm to zamierzony, motywowany politycznie atak na informację, system komputerowy, programy komputerowe i dane, którego skutkiem jest użycie przemocy wobec celów niewalczących przez grupy ponadnarodowe bądź tajnych agentów".

9) H. W. Kushner, Terrorism in America: A Structural Approach to Understanding the Terrorist Threat, Springfield, Ill. 1998, s. 41.

10) J. Kitfleld, Covert counterattack, „National Journal" z 16 września 2000 r.

11) M. Zanini, S. J. A. Edwards, The networking of terror in the information age, w: J. Arquilla, D. Ronfeldt, Networks and Netwars, Santa Monica, 2001, s. 29–60.

12) B. Collin, The future of cyberterrorism, „Crime and Justice International", marzec 1997, s. 15–18.

Politycznie motywowane ataki powodujące poważne szkody, takie jak duże straty ekonomiczne, trwała utrata dostępu do energii elektrycznej lub problemy z zaopatrzeniem w wodę, także mogą być określane jako akty cyberterroryzmu. Również polscy autorzy opracowali roboczą definicję cyberterroryzmu: „Cyberterroryzm jest to politycznie motywowany atak lub groźba ataku na komputery, sieci lub systemy informacyjne w celu zniszczenia infrastruktury oraz zastraszenia bądź wymuszenia na rządach i ludziach daleko idących politycznych i społecznych celów”[13].

Z pojęciem cyberterroryzmu ściśle wiąże się pojęcie wojny sieciowej (*netwar*), która polega na zakłócaniu bądź niszczeniu systemów informacyjnych przeciwnika oraz zdobywaniu jego strategicznych danych dotyczących środków walki i ich rozmieszczenia. Taką wojnę informacyjną zastosowano podczas obu operacji wojskowych przeciw Irakowi, przy czym należy pamiętać również o przewadze militarnej wojsk amerykańskich i sojuszniczych. W wojnie sieciowej główną rolę odgrywają hakerzy-specjaliści z obu stron konfliktu, tak jak w starciu hakerów Chin i Tajwanu w 1999 r i w trwającym nadal konflikcie izraelsko-palestyńskim, w ramach którego armia izraelska systematycznie niszczy infrastrukturę palestyńskich sieci komputerowych i central operatorów internetowych.

W wojnach sieciowych wykorzystuje się wiedzę techniczną i narzędzia używane w atakach cyberterrorystycznych i innych przestępstwach komputerowych. Stąd też określenie, czy mamy do czynienia z cyberterroryzmem, czy tylko z walką internetową, nie jest łatwe. W tej sytuacji Rada Europy przychyla się do opisowej formy zagrożeń, które mają cechy cyberterroryzmu[14]. Chociaż cyberterroryzm przejawia się głównie w atakowaniu systemu i informacji, wykorzystywany jest również w klasycznych postaciach terroryzmu. Atak na system jest uwarunkowany znajomością sposobu funkcjonowania danego systemu i nie zawsze jest natychmiast skuteczny.

Atak na informacje przechowywane w systemie komputerowym może mieć dwojaki cel – chęć podważenia wiarygodności systemu albo kradzież informacji. W pierwszym przypadku sprawca wprowadza własne dane bądź manipuluje danymi zapisanymi w systemie – zazwyczaj dzieje się to tak, by operator nie zauważył zmiany. Ataki na systemy komputerowe mają na celu dezorganizację ich funkcjonowania, co zawsze jest ze szkodą dla społeczeństwa. Działania skierowane na infrastrukturę mogą mieć różnorakie groźne skutki, np. dla ruchu pociągów, zaopatrzenia w energię elektryczną lub wodę. Wywarcie wpływu na przetwarzanie danych w systemach może też prowadzić do zniszczeń materialnych i ofiar w ludziach, a także do wywołania paniki. Działania cyberterrorystów są szczególnie groźne dla krajów wysoko uprzemysłowionych i zinformatyzowanych, a więc, w praktyce, dla państw Europy Zachodniej, Stanów Zjednoczonych i Japonii, które muszą się skutecznie zabezpieczać. Nie mniej groźna jest kradzież danych z systemów komputerowych, które mogą być dla terrorystów przydatne w planowaniu zamachów. Dane te mogą być różnego typu – od projektów architektonicznych obiektów do rozkładu pracy służb ochrony, a nawet zdjęć pracowników. W największym jednak zakresie sieci komputerowe wykorzystywane są do komunikowania się terrorystów przed dokonaniem zamachów, szybkiego i trudno uchwytnego dla organów ścigania.

Grupy terrorystyczne często posługują się Internetem w celu rozpowszechniania swych komunikatów i koordynacji działań. Jak dotąd koordynacja nie była zbyt częsta. Nie było zbyt wielu ataków na sieci komputerowe, które spełniałyby kryteria cyberterroryzmu. Takim atakiem było wyżej wspomniane użycie w 1998 r. „bomby e-mailowej” przeciw ambasadom Sri Lanki przez terrorystyczne ugrupowanie Tamilskich Tygrysów. Wydarzenie to blednie w porównaniu ze skutkami zamachów terrorystycznych, w których zginęły setki osób, takich jak uderzenie samolotami w wieże WTC w 2001 r. (około 3 tys. ofiar), zamachy w Madrycie w 2004 r. (192 ofiary), w Londynie w 2005 r. (54 ofiary) czy wcześniejsze – na ambasady amerykańskie w Nairobi i Dar-es-Salaam (240 ofiar śmiertelnych).

Czy cyberterroryzm ma szanse na przyszłość? Dla terrorystów jest on korzystniejszy od fizycznych zamachów bombowych, ponieważ akty tego typu terroryzmu mogą być dokonywane zdalnie i anonimowo. Ponadto korzystanie z Internetu jest tanie, nie wymaga umiejętności obchodzenia się z materiałami wybuchowymi czy poświęcania się terrorystów w zamachach samobójczych. Grupy terrorystyczne zdobywają rozgłos dzięki mediom publicznym. Wszelki rodzaj ataku komputerowego wywołuje echo wśród dziennikarzy i publiczności, a najczęściej o to chodzi terrorystom. Znane jest stwierdzenie, że jutrzejsi terroryści mogą zrobić więcej za pomocą klawiatury komputera niż dzisiejsi, używając bomb[15].Jednakże są również ujemne strony wykorzystania broni cybernetycznej przez terrorystów. Ze względu na skomplikowanie systemów trudniej jest kontrolować atak i osiągać zamierzone szkody. Jeżeli w zamachu nie giną ludzie, to jest on mniej dramatyczny i nie wywołuje silnych emocji i pożądanego szoku. Z drugiej strony terroryści niechętnie wypróbowują nowe metody destrukcji, jeśli widzą, że dotychczasowe są skuteczne.

W 1997 r. B. Collin opisał kilka przypuszczalnych scenariuszy cyberterroryzmu. W jednym z nich cyberterrorysta wdziera się jako haker do systemu kontrolnego zakładów produktów zbożowych i zmienia poziom dawkowania żelaza. Skutek: dzieci chorują i umierają. W drugim atakuje nowy system kontroli w ruchu lotniczym, co doprowadza do zderzenia dwóch samolotów. W trzecim scenariuszu jego celami są system bankowy, międzynarodowe transakcje i giełda, powoduje zaburzenia systemu ekonomicznego, wskutek czego instytucje tracą zaufanie i następuje czasowa destabilizacja.

Analiza tych hipotetycznych przypadków prowadzi do konkluzji, że jednak istnieje ludzkie zaangażowanie w procesy kontrolne, nie pozwalające na powstanie większego zagrożenia ze strony cyberterroryzmu. Na przykład w scenariuszu zanieczyszczania produktów zbożowych ilość żelaza lub innych toksycznych składników musiałaby być tak duża, że łatwa do zauważenia przez pracowników. Również w scenariuszu kontroli ruchu lotniczego pracownicy szybko zauważyliby

13) A. Bogdół-Brzezińska, M. F. Gawrycki, Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie, Warszawa 2003, s. 73.

14) Organised Crime Situation Report 2004, Focus on the Threat of Cybercrime, Council of Europe, Strasburg, 23.12.2003, s. 125.

15) National Research Council, Computer at Risk, Washington, DC, 1991.

zakłócenia i dokonaliby korekty. Sami piloci są w stanie spostrzec błąd kontrolerów ruchu i postępować samodzielnie.

W 1998 r. Clark Staten, dyrektor Emergency Response and Research Institute w Chicago, potwierdził opinie, iż członkowie niektórych radykalnych organizacji islamskich usiłowali tworzyć „sieć hakerów", aby wesprzeć działania tych organizacji w systemach komputerowych oraz angażować się w ofensywę informacyjną związaną z atakami w wojnie sieciowej w przyszłości[16].

Wobec nielicznych dotychczas przypadków cyberterroryzmu trudno jest ocenić skutki takich ataków. Podobne trudności sprawia ocena potencjalnych szkód – częściowo dlatego, że nie da się przewidzieć, jak silny może być atak na sieć komputerową, zadany w celu oddziałania na politykę krajową lub międzynarodową.

W każdym razie próby ataków na sieci komputerowe skłoniły władze amerykańskie do przygotowania obrony obiektów krytycznej infrastruktury.

Na płaszczyźnie międzynarodowej kilka państw, ze Stanami Zjednoczonymi, zajęło się tą problematyką, w tym układami o pomocy prawnej, ekstradycją, współpracą wywiadów i koniecznością ujednolicenia prawa dotyczącego przestępczości komputerowej. Dzięki temu cyberterroryści mogą być ścigani, nawet wtedy, gdy ich czyny wykraczają poza granice państwowe. Wysiłki te nie koncentrują się na samym cyberterroryzmie (czy hakerstwie), lecz odnoszą się do wszelkich form włamań i ataków na sieci komputerowe, oszustw komputerowych, pornografii dziecięcej w sieci i piractwa elektronicznego (dotyczącego oprogramowania i muzyki). Obejmują one również sponsorowane przez państwo operacje w ramach wojny cybernetycznej, w której wykorzystują ataki hakerów na sieć komputerową jako broń wojskową.

W grudniu 1998 r. z inicjatywy Federacji Rosyjskiej Zgromadzenie Ogólne ONZ przyjęło rezolucję 53/70 dotyczącą przestępczości cybernetycznej, cyberterroryzmu i wojen cybernetycznych. Rezolucja ta, zatytułowana *Developments in the Field of Information and Telecommunication in the Context of International Security* (Rozwój w dziedzinie informacji i telekomunikacji w kontekście międzynarodowego bezpieczeństwa) wzywa państwa członkowskie do informowania Sekretariatu Generalnego o wynikach ich obserwacji i ocenach w sprawach: bezpieczeństwa informacji, określenia koncepcji związanych z tym bezpieczeństwem i opracowania międzynarodowych zasad wzmacniających globalne systemy informacji i telekomunikacji oraz pomagających w zwalczaniu terroryzmu i przestępczości.

Już w 1996 r. Stany Zjednoczone podjęły kilka działań mających na celu lepszą ochronę obiektów krytycznej infrastruktury i powołały w tym celu prezydencką komisję (*President's Commission on Critical Infrastructure Protection*), która miała zbadać struktury istotne dla narodu, określić ich wrażliwość na wiele zagrożeń i zaproponować strategie ich ochrony na przyszłość. Takich infrastruktur jest osiem: telekomunikacja, bankowość i finanse, energia elektryczna, dystrybucja i składowanie paliw i gazu, zaopatrzenie w wodę, transport, służby pomocy w nagłych wypadkach, służby rządowe.

16) J. Staten, Testimony before the Subcommittee on Technology, Terrorism and Government Information, US Senate Judiciary Committee, 24 lutego 1998 r.

Komisja prezydencka stwierdziła, że zagrożenia terroryzmem cybernetycznym zmieniły krajobraz Stanów Zjednoczonych. W przestrzeni cybernetycznej granice nie odgrywają żadnej roli. Potencjalnie poważne ataki cyberterrorystów mogą być planowane bez wykrywalnego logistycznego przygotowania. Przed atakiem sprawca i jego miejsce działania pozostają nieznane. Dlatego ochrona obiektów krytycznej infrastruktury przed atakami cyberterrorystów powinna być zapewniona wcześniej – przed powstaniem szkód. Zalecenia komisji zawarte w Prezydenckiej Dyrektywie 63 doprowadziły do utworzenia takich organizacji prewencyjnych, jak National Infrastructure Protection Center (NIPC), Critical Infrastructure Assurance Office (CIAO), a w prywatnym sektorze – Information Sharing and Assessment Center (ISAC). Oddzielnie Departament Obrony powołał połączone Siły Zadaniowe (Task Forces) jako Computer Network Defense. W 2001 r. placówka National Security Council opracowała *National Plan for Information System Protection* dla wykorzystania najnowszych osiągnięć w tej dziedzinie[17].

Już w 1997 r. National Security Agency (NSA) przeprowadziła symulację ataku cyberterrorystów w celu sprawdzenia wrażliwości amerykańskich komputerów wojskowych, a także niektórych infrastruktur cywilnych na taki atak. Dzięki hakerom z Internetu hakerzy NSA uzyskali uprzywilejowany dostęp do systemów. Wniosek z próby był taki, że wojskowe infrastruktury mogły być zakłócone w stopniu, który utrudniłby rozmieszczanie wojsk. Nie ma dowodów na to, że pozarządowe systemy są narażone mniej albo bardziej niż systemy rządowe i że sytuacja polepsza się – mimo wzrastającego zaopatrzenia w narzędzia bezpieczeństwa informacji.

Haktywiści (*hacktivists*), jak ich określa D.E. Denning[18], mogą mieć poczucie siły, bowiem mogą kontrolować komputery rządowe i zyskiwać rozgłos w mediach, chociaż to nie znaczy, że mogą zmieniać politykę. Odnośnie cyberterroryzmu można wyciągnąć niewiele wniosków dotyczących potencjalnego wpływu na politykę zagraniczną, gdyż dotychczas brak większej liczby wypadków spełniających kryteria. Można tylko powiedzieć, że cyberterroryzm połączony z groźbą działań hakerów wpływa na decyzje polityczne związane z obroną przed tym terroryzmem zarówno na płaszczyźnie krajowej, jak i międzynarodowej. W szczególności terroryzm biologiczny, chemiczny i nuklearny mogą wywierać silny wpływ na narodową politykę obronną. Cyberterroryzm może stać się niebezpieczny, jeśli uzyska lepsze narzędzia, techniki i metody organizacyjne, a działania obronne i prewencyjne nie dotrzymają im kroku.

Internet jest wykorzystywany przez terrorystów także do celów propagandowych, w tym do wzniecania niepokojów, szerzenia nienawiści i – ogólnie – do prowadzenia wojny psychologicznej. Powszechnie znane są groźby terrorystów, a nawet pokazywane przez nich akty egzekucji dziennikarzy i innych osób, w tym członków akcji humanitarnych.

17) Protecting America's Critical Infrastructures: PDD63 the White House, 22 maja 1998 r., National Infrastructure Assurance Council, Executive Order, the White House, 14 lipca 1999 r.

18) D. E. Denning, Activism, hacktivism and cyberterrorism: The Internet as a tool for influencing foreign policy, w: J. Arquilla, D. Ronfeldt, Networks and Netwars, Santa Monica 2001, s. 239–262.

Nie można pominąć również tego, że organizacje terrorystyczne wykorzystują Internet do zdobywania środków finansowych – tą drogą uzyskują one ogromne sumy. Według informacji FBI już w latach dziewięćdziesiątych dokonywano za pośrednictwem komputerów kradzieży kwot rzędu 3–7,5 mld dolarów. Ponadto organizacje te czerpią olbrzymie środki ze skradzionych kart kredytowych, sfingowanych przelewów elektronicznych czy wymuszeń na bankach, do których banki te nawet się nie przyznają.

Na ataki cyberterrorystów szczególnie wrażliwe są sieci energetyczne oraz infrastruktury telekomunikacyjne. Jak wykazały przeprowadzone w 1997 r. ćwiczenia, cała państwowa infrastruktura przemysłowa Stanów Zjednoczonych jest słabo chroniona. Wykazała to NSA w eksperymencie o nazwie Eligible Receiver, którego przedmiotem było Dowództwo Sił Zbrojnych na Hawajach, któremu podlega 100 tys. żołnierzy. Wykrycie przez FBI i Pentagon przygotowania ataków cyberterrorystycznych nie pozwoliło jednak na wczesne przeciwdziałanie ani ustalenie źródeł. Wrażliwość systemów telekomunikacyjnych wiąże się z techniką komputerowego przetwarzania danych i odnosi się do systemów telefonii stacjonarnej, komórkowej i satelitarnej. Przykładem ataku terrorystycznego na tego typu system było włamanie się do brytyjskiego satelity wojskowego i częściowe przejęcie nad nim kontroli w 1999 r.[19]

Szczególnie groźne mogłyby okazać się ataki dokonane przez (D) DOS (*Distributed Denial of Service*), powodujące zablokowanie podstawowych serwerów DNS i mogące wyłączyć Internet w całości. Miałoby to skutki fatalne dla całych sektorów gospodarki, dla świata nauki itd. Nie można nie wspomnieć o skutkach ataków cyberterrorystycznych na systemy zaopatrzenia w wodę i jej uzdatniania. Chroni je wprawdzie profesjonalnie opracowane i zabezpieczone oprogramowanie oraz ciągły monitoring, ale pokonanie tych przeszkód i zatrucie wody np. nadmiarem chloru wcale nie jest wykluczone. W Stanach Zjednoczonych systemy wodne chronione są dodatkowo przez gwardię narodową (National Guard).

Współczesny terroryzm ma różne oblicza, a zagrożenie nim nasila się wraz z postępem technicznym[20]. Obecnie można mówić o terroryzmie katastroficznym (*catastrophic terrorism*) albo terroryzmie masowego zniszczenia (*terrorism of mass destruction*), którego przykładami są zamachy na wieże WTC z 11 września 2001 r. Oprócz superterroryzmu i megaterroryzmu istnieją rodzaje terroryzmu, których nazwy pochodzą od nazw rodzajów wykorzystywanych broni – bioterroryzm, terroryzm nuklearny, terroryzm chemiczny, cyberterroryzm. Coraz silniejsze są obawy, że w wyniku zamachów terrorystycznych zniszczeniu mogą ulec całe miasta, a destabilizacji – duże obszary. Atak na elektrownię atomową mógłby doprowadzić do ogromnej liczby ofiar oraz skażenia wielkich obszarów. Po dokonanym przez sektę Aum Shinrikiyo zamachu na tokijskie metro, podczas którego użyto sarinu, terroryści tureccy z ugrupowania Kalifatstaat planowali atak na mauzoleum Atatürka, twórcy republiki tureckiej, w dzień obchodów 75-lecia państwa, chcąc wykorzystać do zamachu samolot wypełniony trotylem. Ogromna liczba ofiar, w tym zlikwidowanie całego rządu, miała otworzyć drogę do przywrócenia islamskiego państwa wyznaniowego. Z kolei cyberterroryzm wiąże się z wykorzystaniem sieci komputerowych do działań terrorystycznych w skali globalnej, jako że Internet jest siecią ogólnoświatową. Postęp techniczny i cywilizacyjny sprawił, że współczesny terroryzm znalazł się w nowej epoce określanej mianem terroryzmu ponowoczesnego (*postmodern terrorism*)[21]. W tej epoce państwa i społeczeństwa są zagrożone przez ugrupowania terrorystyczne stosujące niekonwencjonalne, tzw. asymetryczne metody walki zgodnie z którymi nie ma kontaktu z przeciwnikiem, a przywódcy pozostają w ukryciu, podobnie jak ich niejasne cele[22].

W przypadku wielu grup islamskich terroryzm początków XXI wieku przybrał formy zorganizowane, umożliwiające atakowanie wszystkich państw, a więc stał się zjawiskiem globalnym[23]. Podstawowe cechy takiego terroryzmu to inspiracja religijna, pozostawanie sprawców w ukryciu, bardziej niszczycielskie i śmiercionośne niż dotychczas skutki oraz międzynarodowy charakter.

Podsumowanie

Każde państwo może być zagrożone atakiem cyberterrorystów ze szkodami tym większymi, im bardziej skomputeryzowana jest jego gospodarka. Z drugiej strony każde państwo może dokonać ataku cybernetycznego, jeżeli tylko znajdą się w nim profesjonalni hakerzy, zdolni i gotowi do jego przeprowadzenia[24]. Podpisana w 2001 r. przez Polskę konwencja o cyberprzestępczości zobowiązuje również nasz kraj do utworzenia ośrodków współpracy i pomocy międzynarodowej w tym zakresie.

prof. dr hab. Brunon Hołyst
Wyższa Szkoła Menedżerska w Warszawie

Bibliografia:

1. B. Hołyst, Terroryzm, tom 1 i 2, LexisNexis, Warszawa 2009.

Prof. dr hab. Brunon Hołyst – polski prawnik, prof. zw. dr hab. nauk prawnych o specjalności kryminalistyka, kryminologia, profilaktyka społeczna, suicydologia, wiktymologia, terroryzm. Autor bardzo wielu podręczników, książek, opracowań naukowych i artykułów dotyczących kryminalistyki i terroryzmu, wydanych zarówno w kraju, jak i zagranicą.

19) S. M. Lawson, Information Warfare: An Analysis of the Threat of Cyberterrorism Towards the US Critical Infrastructure, SANS Institute 2002, s. 6.

20) R. Borkowski, Terroryzm ponowoczesny, Toruń 2006, s. 37–67.

21) W. Laqueur, Postmodern terrorism, „Foreign Affairs" 1996, nr 5, s. 24–36.

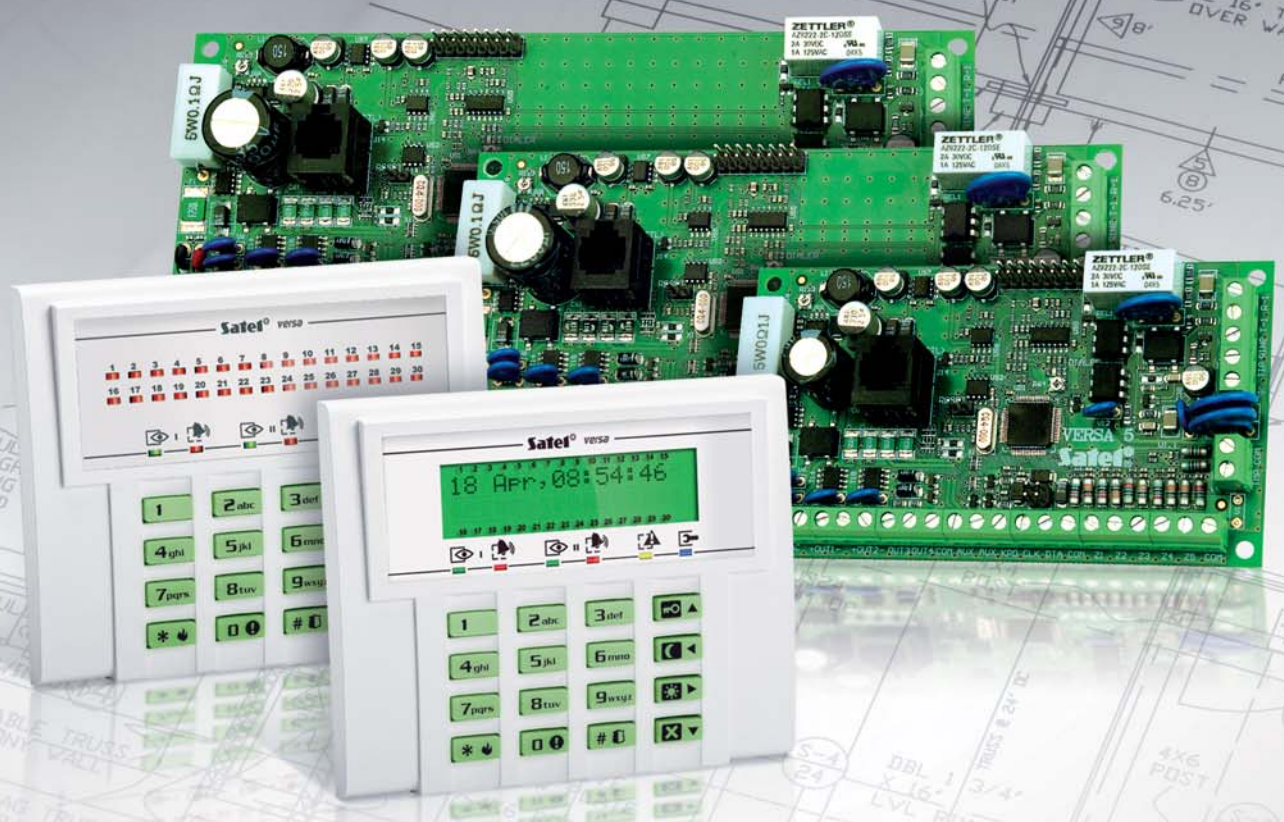
22) H. Münkler, Terrorismus heute. Die Asymmetrisierung des Krieges, „Internationale Politik" 2004, nr 2, s. 1–11.

23) B. Hołyst, Terroryzm – nowe zagrożenie XXI wieku, Polska 2000 plus „Biuletyn" 2003 nr 2, s. 49–60.

24) S. Serwiak, Cyberprzestrzeń jako źródło zagrożenia terroryzmem, w: E. Pływaczewski, Przestępczość zorganizowana, Kraków 2005, s. 589–613.

Versa
wszechstronne centrale alarmowe

Nowoczesne centrale VERSA to połączenie intuicyjnej i prostej obsługi z zaawansowanymi możliwościami rozbudowy i wszechstronnymi funkcjami komunikacyjnymi. Dzięki temu są idealnym rozwiązaniem dla zabezpieczania mieszkań, domów i małych obiektów handlowo-biurowych.



Satel®

ul. Franciszka Schuberta 79, 80-172 Gdańsk, tel.: (0 58) 320 94 00, fax: (0 58) 320 94 01
e-mail: satel@satel.pl, www.satel.pl

Twoja firma też może stracić dane

Paweł Odor, Piotr Dembiński

Niemal 70 procent dokumentów, jakie powstają obecnie w firmach lub są tworzone przez użytkowników prywatnych w Polsce i na świecie, ma postać cyfrową. Niemal 90 procent z nich nigdy nie zostanie jednak wydrukowanych i pozostaną one jedynie w pamięci naszych dysków komputerowych, kart pamięci i innych nośników, których nowsze wersje pojawiają się każdego roku na rynku. Choć ich oprogramowanie i budowa są coraz lepiej przygotowane na ochronę zapisanych na nich danych, eksperci z największej firmy odzyskiwania danych w branży wciąż mają do czynienia z ponad pięćdziesięcioma tysiącami przypadków utraty danych z wszystkich możliwych rodzajów nośników rocznie. W głównej mierze, szczególnie w Polsce, dotyczą one nie użytkowników prywatnych, a firm. W jaki więc sposób tracimy dane i jak zabezpieczyć się przed ich utratą?

Polskie firmy a ochrona danych, czyli czego nie wiedzą polscy przedsiębiorcy

Niewielu menedżerów i członków kadry zarządzającej polskich firm jest świadomych tego, że w przypadku utraty danych duże polskie przedsiębiorstwa narażone są na straty w wysokości nawet 500 tysięcy złotych dziennie. Dotyczy to głównie tych firm, których produkcja bądź działalność oparta jest na systemach informatycznych przetwarzających i magazynujących ogromne ilości danych. Na świecie kwoty te nierzadko przekraczają milion dolarów.

Zdecydowanie największym problemem jest wciąż niska świadomość szefów firm co do potencjalnych problemów związanych z utratą danych. Ponadto panuje również powszechne przekonanie, że tworzenie kopii zapasowych, tzw. backupów, stanowi panaceum na wszystkie problemy. Gdy to panaceum zawodzi, wiele firm oraz użytkowników prywatnych nie widzi już zwykle szans na odzyskanie danych. Założenie to nie musi być prawdziwe, o czym świadczą światowe oraz polskie statystyki skuteczności odzyskiwania danych. Według danych specjalistów z branży, na całym świecie specjaliści odzyskują utracone dane w ośmiu na dziesięć przypadków.

Na polskim rynku wiele firm obawia się wysokich kosztów związanych z odzyskiwaniem danych. Tymczasem koszt utraty danych i braku dostępu do informacji jest bardzo często kilkanaście lub nawet kilkadziesiąt razy większy od kosztu ich przywrócenia. W przypadku najważniejszych danych, kluczowych dla danej organizacji, nawet dziesięć dni bez dostępu do nich może zdecydować o tym, czy firma przetrwa na rynku czy też nie, nie wspominając o poniesieniu dotkliwych strat finansowych i wizerunkowych.

W przypadku firm najwięcej próśb o odzyskanie plików dotyczy danych księgowych, w tym głównie baz danych, a w następnej kolejności dokumentów zapisanych w programach Word i Excel. W przypadku użytkowników prywatnych najczęściej są to zdjęcia i filmy, które uwieczniły ważne chwile, takie jak na przykład narodziny dziecka, uroczystości rodzinne czy dokumentacja wyjazdów wakacyjnych.

Dlaczego tracimy dane?

Obecnie wiemy, że główne przyczyny utraty danych to awaria sprzętu (44 proc. przypadków) oraz błąd człowieka (32 proc. przypadków). Inne przyczyny to między innymi działanie wirusów (7 proc.), błędy aplikacji (4 proc.) i klęski żywiołowe (3 proc.) – np. powodzie.

Analizując najpoważniejszą statystycznie przyczynę utraty danych – awarię sprzętu – możemy mówić o tzw. logicznych i fizycznych uszkodzeniach nośników. W tym pierwszym przypadku mamy do czynienia z awarią układów elektronicznych, które są częścią m.in. dysku twardego. Przypadki uszkodzeń fizycznych występują wtedy, gdy nośnik jest uszkodzony mechanicznie, np. zgniecenie nośnika uniemożliwia jego prawidłowa pracę.

Najpopularniejszym nośnikiem trafiającym do laboratoriów odzyskiwania danych w Polsce i na świecie jest wciąż dysk twardy. Coraz więcej danych tracimy jednak także z coraz popularniejszych dysków SSD i innych urządzeń wykorzystujących technologię flash, np. pamięci przenośnych czy pendrive'ów. Powodem jest przede wszystkim lawinowy wzrost ilości informacji cyfrowych przechowywanych w urządzeniach innych niż komputery, takich jak telefony komórkowe czy cyfrowe aparaty fotograficzne.

Bardziej złożone uszkodzenia, szczególnie fizyczne uszkodzenia nośników, np. spalenie czy zalanie, wymagają ingerencji ekspertów. Wynika to głównie z tego, że nie wszystkie informacje mogą być odtworzone przez automatyczne algorytmy odzyskujące dane, stosowane w programach ogólnie dostępnych dla użytkowników. Duże znaczenie mają tu także takie czynniki, jak konfiguracja komputera, używane oprogramowanie czy możliwość częściowego lub całkowitego nadpisania danych przez nowo tworzone pliki.

Wśród głównych typów nośników, z jakich obecnie odzyskiwane są dane, są m.in. dyski (IDE, EIDE, magistrale: ATA (SATA) SCSI, SAS, Fibre Channel), nośniki w dowolnej konfiguracji (pojedynczy dysk twardy lub złożony dysk RAID), karty pamięci, pendrive'y, a także urządzenia magazynujące zdjęcia, takie jak np. fotobanki.

Nie każdy przypadek utraty danych wymaga wizyty w specjalistycznej „klinice dysków twardych", jaką jest laboratorium. Gdy mamy do czynienia z uszkodzeniem logicznym, a więc takim, w którym nośnik danych nie uległ uszkodzeniu mechanicznemu, użytkownik komputera często może pomóc sobie samodzielnie. W jaki sposób?

Samodzielne odzyskanie danych jest możliwe dzięki wykorzystaniu specjalistycznych programów. Aplikacje te pozwalają na odzyskiwanie utraconych danych zapisanych w różnych programach oraz na odzyskiwanie wiadomości z poczty elektronicznej.

Sezonowość utraty danych

Branża odzyskiwania danych rządzi się pewnymi prawidłowościami. Jedną z nich jest wspomniane wcześniej zjawisko sezonowości utraty danych. Dotyczy ono pewnych okresów roku, w których tracimy dane częściej niż zwykle. Wzrost liczby przypadków utraty danych zauważalny jest głównie latem, lecz również okres zimowych mrozów nie jest tutaj wyjątkiem. Sytuacja ta w szczególności dotyczy laptopów, które w drodze do naszych biur i domów nieustannie poddawane są drastycznym zmianom temperatur.

W lecie komputery, a w szczególności firmowe serwerownie, narażone są na utratę danych. Wśród najważniejszych powodów specjaliści wymieniają zalanie, spalenie dysków komputerowych na skutek spięć w gniazdkach elektrycznych podczas burz czy przegrzanie komputerów przy zbyt wysokich temperaturach. W celu uniknięcia tego typu zdarzeń zalecane jest przede wszystkim stosowanie specjalnych listew zabezpieczających przed uderzeniem pioruna i spięciem, a także właściwe chłodzenie komputerów i zwrócenie szczególnej uwagi na umiejscowienie serwerowni (należy umieścić ją w miejscu dobrze wentylowanym i takim, w które nie dotrze woda).

Nagła zmiana temperatury, powstająca w jej wyniku wilgoć lub naprężenia układów elektronicznych to jedne z najczęstszych przyczyn utraty danych, jakie obserwują eksperci w swoich laboratoriach na całym świecie w okresie nasilenia silnych mrozów. Włączenie „schłodzonego" komputera

w biurze lub mieszkaniu może spowodować skrócenie żywotności twardego dysku lub nawet jego natychmiastową awarię, a stąd już tylko krok do utraty danych. Dlatego każdy użytkownik przenośnego komputera, a w szczególności pracownicy posiadający na swych dyskach kluczowe dla ich firm dane, powinien pamiętać o zagrożeniu elektronicznych informacji, jakie niesie ze sobą mroźna zima. Warto pamiętać, że przypadki utraty danych podczas mrozów dotyczą także innych urządzeń, np. bardzo popularnych odtwarzaczy MP3.

Proces odzyskiwania danych

Jak więc szczegółowo wygląda proces odzyskiwania danych? W pierwszym etapie tego procesu specjaliści telefonicznie zapoznają się z konkretnym przypadkiem i pomagają dopasować najlepsze pod względem czasu reakcji i kosztów rozwiązanie. Po dostarczeniu nośnika do laboratorium (osoba, która straciła dane, może dostarczyć go osobiście bądź kurierem) eksperci przeprowadzają szczegółową analizę uszkodzenia, co pozwala określić stan danych, zakres uszkodzenia oraz szacowany czas przywrócenia informacji. Najczęściej wynikiem ekspertyzy jest raport Verifile, który pozwala klientowi na zapoznanie się z możliwą do odtworzenia strukturą plików i danych jeszcze przed rozpoczęciem procesu odzyskiwania danych. Na tym etapie specjaliści w laboratorium sporządzają także kalkulację odzyskiwania danych. Następnie komplet informacji jest przekazywany klientowi.

Proces odzyskiwania danych rozpoczyna się niezwłocznie po akceptacji wyników ekspertyzy. Specjaliści dokonują odzyskania i naprawy struktur logicznych danych, wykorzystując ponad 120 różnego rodzaju specjalistycznych urządzeń oraz różnorakie oprogramowanie. Po odzyskaniu dane są zwracane klientowi na wybranym przez niego nośniku (zewnętrzny dysk twardy, CD, DVD itd.). Kopia bezpieczeństwa danych

Co zrobić, by nie utracić danych
porady specjalistów

Archiwizuj swoje dane

Nie istnieją idealne zabezpieczenia przed utratą danych. Nawet uchodzące za niezawodne systemy macierzowe dają co najwyżej 99,9 procent pewności bezpieczeństwa danych. Używając na co dzień zwykłego komputera PC, regularnie zachowuj swoje dane na wydzielonej partycji dysku (rozwiązanie najprostsze, choć najmniej bezpieczne), na innych nośnikach (na przykład na drugim dysku).

Sprawdzaj swój backup

Kopia bezpieczeństwa (backup) jest najprostszą metodą ochrony danych przed utratą. Musi być jednak tworzona regularnie i w prawidłowy sposób. Po wykonaniu kopii zapasowej sprawdź, czy jesteś w stanie ją odczytać. Wiele osób tworzy kopie danych, nie sprawdzając, czy w razie potrzeby można ich użyć. Często kopia zawiera błąd, co prowadzi do bezpowrotnej utraty informacji.

Uważaj na wysokie temperatury

Szczególnie w miesiącach letnich komputery narażone są na działanie wysokich temperatur. By uchronić się przed utratą danych związaną z przegrzaniem urządzenia, należy przede wszystkim zapewnić mu dostęp do chłodzenia i nie pozostawiać włączonych urządzeń w pomieszczeniach, w których panują bardzo wysokie temperatury. Należy pamiętać, że w lecie przegrzaniu ulega także wiele źle wentylowanych serwerowni, co powoduje awarię i w rezultacie brak dostępu do danych firm czy tak istotnych instytucji, jak szpitale bądź administracja rządowa.

Uważaj na niskie temperatury

Zmiany temperatur nie służą dyskom twardym. Podstawową zasadą w przypadku narażenia komputera na działanie niskich temperatur jest jego niewłączanie do momentu, kiedy jego temperatura będzie równa temperaturze pokojowej lub zbliżona do niej. Układ smarowania dysku twardego jest wrażliwy na różnice temperatur. Włączenie „schłodzonego" komputera w biurze lub mieszkaniu spowoduje skrócenie żywotności twardego dysku lub jego awarię, a stąd już tylko krok do utraty danych.

Gdy dane zaleje woda

Kontakt nośnika danych z wodą to sytuacja krytyczna, w której użytkownicy komputerów w sposób szczególny narażeni są na utratę danych. Prawidłowe zachowanie się w takiej sytuacji gwarantuje odzyskanie nawet 99 proc. utraconych informacji. Optymalnym rozwiązaniem w takim przypadku jest zwrócenie się o pomoc do specjalistycznej firmy posiadającej laboratorium odzyskiwania danych. Należy pamiętać, że ważny jest czas reakcji, ponieważ elementy nośników ulegają korozji wskutek działania wody. Zanim zwrócimy się do specjalistycznej firmy, sami musimy zadbać o prawidłowy stan zalanego nośnika, z którego chcemy odzyskać dane. Istnieje kilka podstawowych zasad, których trzeba przestrzegać w momencie utraty danych wskutek zalania komputera:

1) Nie wolno podłączać dysku do zasilania! Wskutek zawilgocenia elektroniki dysku podłączenie zasilania spowoduje dodatkowe problemy: od spalenia elektroniki dysku (zewnętrznej i/lub wewnętrznej) po całkowite zniszczenie nośnika.
2) Nie należy osuszać nośnika danych ani dopuścić do jego samoistnego wyschnięcia. Osuszenie i uruchomienie tego elementu może spowodować bezpowrotną utratę zapisanych na nim informacji.

jest przetrzymywana przez 30 dni na firmowym serwerze, następnie bezpowrotnie usuwana, zgodnie z procedurą bezpieczeństwa.

Najciekawsze, najdziwniejsze, najpoważniejsze…

Jednym z najbardziej spektakularnych przypadków odzyskiwania danych przeprowadzonego przez międzynarodowy zespół ekspertów było przywrócenie danych po katastrofie promu kosmicznego Columbia. Choć zniszczenia dysku były wyjątkowo poważne (w trakcie spadania nośnik spalał się w atmosferze), udało się odzyskać aż 99 procent kluczowych dla misji danych. Wśród pozostałych przypadków można wyróżnić także odzyskanie danych z komputera, który wypadł z lecącego helikoptera, z dysku, w którym mrówki utworzyły gniazdo, czy też z komputera przypadkowo upieczonego w piekarniku. Również w Polsce specjaliści z największego i najbardziej zaawansowanego technologicznie w Europie Środkowo-Wschodniej laboratorium zmierzyli się z nietypowymi przypadkami.

Odzyskane wspomnienia z jednej z wypraw Krzysztofa Wielickiego

Jednym z najbardziej spektakularnych przypadków, jakie przydarzyły się w Polsce, było odzyskanie fotografii utraconych podczas jednej z wypraw Krzysztofa Wielickiego, jednego z najwybitniejszych światowych himalaistów. Fotobank (urządzenie, które umożliwia przechowywanie dużej liczby cyfrowych zdjęć o znakomitych parametrach) uległ uszkodzeniu, gdy jeden z Sherpów zgniótł go, siadając podczas postoju. Choć zwykle przypadki utraty zdjęć z aparatów cyfrowych należą do najłatwiejszych, tym razem uszkodzenia były znaczne i bez odpowiedniej wiedzy i doświadczenia fachowców zapewne nie udałoby się odzyskać straconych materiałów.

– Kiedy zobaczyłem urządzenie, na którym były zarchiwizowane zdjęcia z całej wyprawy, załamałem się. Nasz fotobank był

3) Mokry nośnik powinien zostać zawinięty w wilgotny ręcznik, włożony do worka antyelektrostatycznego i bezzwłocznie dostarczony, np. pocztą kurierską, do najbliższego laboratorium odzyskiwania danych.
4) Zabrudzone nośniki wymagają natychmiastowego, gruntownego czyszczenia w sterylnych warunkach. Niedokładne oczyszczenie, dopuszczenie do wyschnięcia i uruchomienie zalanego wcześniej nośnika może spowodować bezpowrotną utratę danych.
5) Prawdopodobieństwo utraty informacji wzrasta w przypadku kontaktu nośnika ze słoną lub silnie zabrudzoną wodą. Dla zwiększenia szans odzyskania danych należy zanurzyć nośnik w wodzie destylowanej, po czym zawinąć ten element w wilgotny ręcznik, włożyć go do worka antyelektrostatycznego i wysłać do laboratorium odzyskiwania danych.
6) W przypadku zalania nośnika danych nie należy stosować oprogramowania służącego do samodzielnego odzyskiwania danych.

Zwróć uwagę na zasilacz

Podczas kupna komputera stacjonarnego warto zwrócić uwagę na zasilacz. Dobry zasilacz kosztuje więcej niż tania obudowa, ale warto w niego zainwestować, nawet jeśli nasz zestaw komputerowy nie jest specjalnie „prądożerny". Dlaczego? Z co najmniej dwóch powodów. Po pierwsze – niewłaściwe (zbyt niskie lub zbyt wysokie) napięcia podawane przez wadliwie działające zasilacze mogą destabilizować pracę komputera i ujemnie wpływać na żywotność komponentów. Po drugie – tanie zasilacze przeważnie nie mają dobrych układów zabezpieczających przed przepięciami. Często rozmawiamy z osobami, którym, na skutek przepięcia, zasilacz spalił większość elementów komputera – w tym dysk twardy.

Zamykaj poprawnie system

Nie wychodź ze swojego systemu, nie zamknąwszy go poprawnie. Wyłączenie komputera przez wyjęcie wtyczki, popularne „zresetowanie" komputera lub naciśnięcie przycisku wyłączającego komputer w czasie pracy systemu może prowadzić do uszkodzenia systemu plików, a co za tym idzie – do utraty danych.

Dbaj o laptopa

Bardzo dużo przypadków utraty danych dotyczy laptopów, które pracują w niestabilnym środowisku, np. na kolanach ich właściciela lub na pościeli. Należy pamiętać, że w takich przypadkach źle ustawiony laptop może nie mieć odpowiedniej wentylacji i wskutek tego może się przegrzać. Istotne jest także to, aby nie poruszać laptopem w trakcie jego pracy i transportować go w przeznaczonych do tego celu ochronnych futerałach.

Nie otwieraj dysku

Zdjęcie obudowy dysku twardego w pomieszczeniu, które nie jest do tego przystosowane, grozi bezpowrotną utratą danych lub drastycznym zmniejszeniem żywotności nośnika (nawet stukrotnym!). Dyski twarde produkowane są w warunkach laboratoryjnych. Pojedynczy pyłek kurzu może mieć szerokość kilku lub kilkudziesięciu ścieżek dysku, na których zapisane są dane. Na każdej ścieżce może być zapisanych kilka plików. Wyobraźmy sobie więc straty, jakie może spowodować kurz dostający się do wnętrza dysku twardego. Możemy bezpiecznie ściągnąć obudowę naszego HDD tylko w przystosowanych do tego celu miejscach, takich jak hale technologiczne producentów dysków twardych czy laboratoria odzyskiwania danych.

Piotr Dembiński
Kroll Ontrack

poobijany i zgnieciony. Nie miałem wątpliwości, że straciłem wszystko. Dopiero znajomy uświadomił mnie, że istnieją specjaliści, którzy są w stanie odzyskać dane nawet z tak zniszczonych urządzeń – powiedział Krzysztof Wielicki.

Specjaliści odzyskiwania danych dla Polskiej Akcji Humanitarnej

W roku 2007 prowadząca projekt pomocy mieszkańcom jednego z najuboższych rejonów Czeczenii Polska Akcja Humanitarna utraciła dane dotyczące akcji. Realizowany przez PAH projekt dotyczył odbudowy domów zniszczonych w wyniku działań wojennych. Dane zostały utracone w biurze PAH w Groznym, gdzie podczas włączania laptopa spalił się dysk zawierający istotne dla Fundacji informacje. Najważniejsze w tej sytuacji było odzyskanie dokumentacji zdjęciowej. Bez jej przywrócenia PAH nie byłaby w stanie przygotować projektu pomocy mieszkańcom rejonu szarojskiego, który należał do najuboższych i najbardziej niebezpiecznych w Czeczenii.

– 70 rodzin z rejonu szarojskiego żyje w skrajnych warunkach, w domach, które zostały zniszczone podczas dwóch wojen. Są to głównie dzieci, wdowy i osoby starsze. Nie mają dostępu do wody, sanitariatów oraz ogrzewania. Co roku poważnym problemem dla nich jest przetrwanie ostrej, mroźnej zimy – tłumaczyła wówczas Janina Ochojska z Polskiej Akcji Humanitarnej.

Cała operacja odzyskiwania danych trwała jedynie dwa dni.

Na ratunek szpitalowi

Wskutek burz i upałów, jakie nawiedziły Polskę w roku 2007, wiele instytucji stanęło przed groźbą utraty swoich najważniejszych danych. Jedną z nich był Szpital im. Rydygiera w Łodzi. Utracenie danych mogło doprowadzić do zakłócenia funkcjonowania szpitala, a tym samym zagrozić zdrowiu jego pacjentów. W tym przypadku podczas gwałtownych burz i deszczów została zalana serwerownia, co uniemożliwiło dotarcie do najistotniejszych danych. W podobnych sytuacjach bardzo istotny jest czas, w jakim możliwe jest odzyskanie straconych danych. Na szczęście specjalistom udało się w porę odzyskać utraconą dokumentację, a tym samym umożliwić szpitalowi normalne funkcjonowanie.

Utracony „Scyzoryk”

Liroy – pionier polskiej sceny rap, autor jednej z najpopularniejszych piosenek rap lat 90, utworu „Scyzoryk”, stracił nagrania ze swojej najnowszej płyty „L-Niño, Vol.1” na dwa tygodnie przed oficjalną premierą. Zawiódł komputer w studio nagrań. Utwory na najnowszy krążek muzyka były nagrywane wspólnie z wykonawcami z kraju i z zagranicy. Ich odtworzenie nie było możliwe. Dane udało się odzyskać w dwa dni i 27 listopada, tak jak planowano, ukazał się nowy album Liroya. To nie pierwsze kłopoty muzyka z danymi. Siedem lat wcześniej, podczas nagrywania płyty „Dzień Szaka-L´a”, w studio nagrań uderzył piorun. Utwory zostały wtedy bezpowrotnie stracone.

Kolejny artykuł z cyklu o ochronie danych będzie dotyczyć informatyki śledczej. Opowiemy w nim o nieuczciwych praktykach przestępców internetowych oraz o tym, jak mogą bronić się przed nimi polskie firmy.

Paweł Odor

Autor jest głównym specjalistą firmy Kroll Ontrack w Polsce

RACS 4

System Kontroli Dostępu

- Do 250 podsystemów w jednym systemie.
- Do 32 kontrolerów dostępu w jednym podsystemie.
- Do 1000 kontrolerów w całym systemie.
- Bezpłatne oprogramowanie do zarządzania systemem KD.

RCP Master *PR602LCD*

roger®

www.roger.pl

Rozwiązania Kontroli Dostępu i Rejestracji Czasu Pracy

Rozszerzono funkcjonalność zaawansowanych kontrolerów dostępu (seria PRxx2) o możliwość losowej kontroli użytkowników.

Prosty przegląd technologii zabezpieczeń sieciowych

Jacek Gawrych

Historia ochrony sieci komputerowych jest historią walki producentów zabezpieczeń z nieposkromioną pasją i nowatorskimi pomysłami domorosłych miłośników ich łamania. Co gorsza, twórcy zabezpieczeń niemal zawsze są o krok w tyle za swoimi przeciwnikami. Metody ochrony sieci powstały przede wszystkim w odpowiedzi na nowe metody włamań. Zapewne jest to najlepsze wytłumaczenie faktu, że na rynku powstało aż tak dużo rozwiązań zabezpieczających sieć. Z niniejszego artykułu można będzie dowiedzieć się, jak wstępnie oszacować, które rozwiązania są odpowiednie dla firmy, a które nie są konieczne

Aby ułatwić zrozumienie zagadnienia, podajmy kilka przykładów. Wyobraźmy sobie, że wynajęto płatnego mordercę do zabicia prezesa naszej firmy w jego własnym gabinecie w godzinach pracy biura. Zobaczmy, jak poradzą sobie z nim wdrożone przez nas zabezpieczenia. Płatny morderca będzie symbolem techniki ataku na naszą sieć.

Firewall – filtr pakietów

Firewall – filtr pakietów to jakby ogrodzenie wokół siedziby naszej firmy. W ogrodzeniu tym są otwarte furtki, ale tylko w zaplanowanych wcześniej miejscach, które są objęte dodatkową ochroną. Zabójca nie podejdzie więc do okna prezesa w budynku i nie wystrzeli z pistoletu. Nie pozwoli mu na to ogrodzenie. Może wejść tylko przez furtkę, gdzie przy okazji zostanie sprawdzony – będzie wiadomo, do kogo idzie, skąd pochodzi, czy prezes się go spodziewa itd. Dalej będzie musiał iść wyznaczonymi szlakami dla gości. Tak działa firewall – filtr pakietów. Sprawdza on, z jakiego adresu przychodzą dane z sieci oraz na jaki adres i jaki port są kierowane. Jeżeli dany pakiet w sieci pasuje do zakazanych kryteriów, jest odrzucany. Dzięki temu możemy odseparować od świata zewnętrznego nasze prywatne aplikacje sieciowe albo określić, z jakich konkretnych adresów mogą być dostępne. Jak to się robi? Po prostu w firewallu określamy konkretne reguły, na przykład:

– zezwól na odwiedzenie naszej strony WWW wszystkim możliwym użytkownikom Internetu (reguła ta w systemie typu UNIX wyglądałaby tak: *pass in quick on eth0 from any to 216.153.191.138 port = 80 tcp keep state*),
– zezwól pracownikom naszej firmy na odwiedzanie dowolnych stron WWW dostępnych w Internecie poprzez protokół HTTPS (*pass out quick on eth1 from $local_users to any port = 443 tcp keep state*).

Firewall jest niemal konieczny dla wszystkich firm korzystających z Internetu. Na szczęście jest zaimplementowany w niemal każdym prostym ruterze (również bezprzewodowym). Nawet jeśli nie mamy wewnątrz firmy aplikacji, które chcemy udostępniać przez Internet (WWW, e-mail), warto skorzystać z tego firewalla, gdyż całkowicie odetnie on dostęp do nas z zewnątrz (nawet dostęp do rutera), a ponadto pozwoli pracownikom na korzystanie tylko z konkretnych usług w Internecie.

Firewall aplikacyjny

Bardziej skomplikowane jest wykorzystanie firewalli aplikacyjnych. Staną one na drodze naszemu mordercy, jeżeli udało mu się przejść przez ogrodzenie (bo faktycznie był umówiony z prezesem). Firewall aplikacyjny to jakby sekretarka, która sprawdzi, czy morderca potrafi porozumiewać się tym samym językiem, co prezes. Jeśli nie potrafi, zostanie zawrócony i nie przedostanie się dalej. Jak to działa w rzeczywistości? Firewalle aplikacyjne realizują ideę FPI (*Full Packet Inspection*) – analizują przychodzące pakiety na poziomie znacznie głębszym niż poziom adresów IP i numerów portów, czyli na poziomie warstwy aplikacji. Dzięki temu do naszego serwera WWW dostaną się tylko pakiety zgodne z protokołem HTTP. Atakujący nie będzie miał pełnej swobody podczas atakowania naszego serwera. Będzie musiał wysłać do niego pakiet zgodny z protokołem HTTP, a to już nie jest takie proste. Na pewno warto zastosować firewall aplikacyjny, jeśli udostępniamy publiczne usługi z sieci, którą sami zarządzamy (jeśli w naszej sieci znajduje się publiczny serwer WWW). Jeżeli nie ma dostępu do naszej sieci z Internetu, w zupełności wystarczy nam prosty firewall – filtr pakietów.

VPN

To zagadnienie zostało poruszone w poprzednim numerze *Zabezpieczeń*, zatem wystarczy telegraficzny skrót. Po pierwsze VPN (*Virtual Private Network*) wspomaga firewalla w umożliwianiu dostępu tylko wyselekcjonowanym pracownikom, po drugie pozwala na szyfrowanie zdalnej komunikacji. Jest to technologia, której zastosowanie na pewno powinny rozważyć te firmy, które chcą umożliwić swoim pracownikom zdalny dostęp do prywatnych zasobów przedsiębiorstwa.

IPS (*Intrusion Prevention System*)

Powiedzmy, że wspomniany potencjalny morderca legalnie przedostał się przez ogrodzenie i mówi tym samym językiem, co nasz prezes. Czy zrobiliśmy wszystko, co było w naszej mocy, by zagwarantować prezesowi bezpieczeństwo? Absolutnie nie! Zlecamy więc zadanie kontrolowania gościa ochroniarzowi. Każdy niewłaściwy ruch skończy się powaleniem napastnika na podłogę, a następnie doprowadzeniem go przed wymiar sprawiedliwości. Zgodnie z taką zasadą działają rozwiązania IPS (*Intrusion Prevention System*), które wychwytują w przychodzących pakietach złośliwy kod. Oczywiście urządzenia IPS mogą zawierać w sobie moduł firewalla aplikacyjnego. W dzisiejszych czasach bardzo silnie dąży się do integracji wielu funkcji w jednym urządzeniu (czego owocem jest duży asortyment produktów UTM – *Unified Threat Management*). Z urządzenia IPS skorzystamy w bardzo podobnych sytuacjach, co z firewalla aplikacyjnego. Oczywiście musi to wiązać się z większymi kosztami ochrony informacji, a więc służyć do ochrony bardziej wrażliwych danych. Ochroniarz także może być lepszy (i z reguły droższy) albo gorszy (z reguły tańszy), ale czy na pewno taki ochroniarz wystarczy w każdym przypadku? Przecież morderca może być szybszy od ochroniarza. Może też najpierw powalić (lub oszukać) ochroniarza, a potem bez problemu zabrać się za prezesa. Z tego powodu często potrzebny jest szereg innych zabezpieczeń, które będą wzajemnie wspierać się i razem obniżać ryzyko utraty prezesa.

NAC (*Network Access Control*)

A co by było, gdybyśmy każdego gościa w naszej firmie prosili o przedstawienie swojego świadectwa niekaralności albo wręcz o jakiś certyfikat potwierdzający uczciwość? Z pewnością mogłoby to odsiać część przestępców, którzy chcieliby odwiedzić naszego prezesa. Mniej więcej tak działają rozwiązania typu Network Access Control. Zanim ktoś zostanie wpuszczony do naszej sieci, będzie najpierw dokładnie sprawdzony – dostęp do niej będzie wiązał się z koniecznością zainstalowania najnowszych aktualizacji oprogramowania, łatek, zaktualizowania bazy wirusów itp. Rozwiązania NAS nie są tak popularne jak wspomniane wcześniej technologie, ale ich popularność ciągle rośnie. Ich wdrożenie powinno wynikać z analizy ryzyka przeprowadzonej w firmie. Większość administratorów sieci musi nauczyć się zastosowania tych rozwiązań – początki mogą być trudne.

Kontrola użytkowników

Załóżmy, że wejście dla gości mamy już tak obwarowane, że tylko najlepsi na świecie mordercy będą w stanie dostać się do prezesa i zlikwidować go. Na tych najlepszych mało kogo stać, więc ryzyko utraty naszego prezesa maleje. Znacznie prostsze wydaje się włożenie bomby do nesesera wiceprezesa i zdetonowanie jej w czasie spotkania zarządu. Żadna z wcześniej omówionych technologii nie jest w stanie temu zapobiec. Nie rozkładajmy jednak rąk. Zainstalujmy przy wejściu do firmy detektor materiałów wybuchowych, który będą mijać również wszyscy nasi pracownicy. O jakim rozwiązaniu teraz mówimy? Oczywiście o systemach antywirusowych, które regularnie muszą przeczesywać zasoby informacyjne w naszej firmie. Jest duża szansa na to, że coś wykryją, zdezaktywują i zapobiegną stratom.

Zostaje jeszcze cały szereg produktów służących do kontroli pracowników, dzięki którym:

- znacznie zmniejsza się prawdopodobieństwo, że zarażą oni swoje komputery, buszując w Internecie,
- bardziej poświęcą się swojej pracy, bo nie będą mieli dostępu do portali społecznościowych, z pornografią, z grami, do komunikatorów, sieci P2P itp.

Kwestie te rozwiązują takie technologie, jak Web Filtering, Anti-P2P, Anti-IM, Anti-VoIP, które przeważnie są dostępne dzięki jednemu urządzeniu. Rozwiązania te na pewno warto wdrażać równolegle z typowymi zabezpieczeniami przed atakami z zewnątrz. W przeciwnym wypadku duża dysproporcja skłoni atakujących do wybrania znacznie prostszych rozwiązań.

Podsumowanie

Istnieje wiele różnych sposobów na zabezpieczenie naszej sieci zarówno przed atakami z zewnątrz, jak i przed tymi z komputerów naszych pracowników. Niech zwykły rozsądek poparty znajomością tych rozwiązań zadecyduje o tym, które z nich należy wybrać w danym przypadku.

Jacek Gawrych

Studium

audytów bezpieczeństwa informacji, czyli obnażenie nieprawidłowości w ochronie informacji

Krzysztof Sierota

Straty spowodowane utratą informacji

Do wytworzenia, przetworzenia i sprzedania dowolnego produktu oprócz materiałów i narzędzi konieczna jest również informacja w postaci wiedzy, jak to zrobić. Najczęściej to właśnie ta informacja jest kluczem do sukcesu. Dzięki niej można wytworzyć lub przetworzyć, a także sprzedać produkt z zyskiem. Jej utrata lub przekazanie komuś niepowołanemu (kradzież informacji) automatycznie wiąże się ze stratami finansowymi. Przeciek informacji dotyczących cen w przetargu może spowodować, że atrakcyjny kontrakt nie zostanie podpisany, gdyż konkurencja poznała ofertę i zaoferowała cenę mniejszą o przysłowiową złotówkę.

Odchodzący z firmy handlowiec lub menedżer, który zabiera ze sobą bazę danych klientów i kontaktów, to częsty przypadek w polskich firmach. Podobnie dzieje się, gdy pracownicy, którzy odeszli z jakiejś firmy, zakładają własną, konkurencyjną działalność i nieuczciwie korzystają z informacji, technologii, *know-how* wypracowanych w macierzystej firmie.

Problemów mogą nastręczyć sytuacje, w których na skutek incydentu związanego z naruszeniem bezpieczeństwa informacji następuje naruszenie reputacji firmy. Utrata zaufania klientów do banku wplątanego w aferę związaną z nieszczelnymi systemami internetowej bankowości czy wyrzucenie na śmietnik ważnych firmowych dokumentów to częste przypadki, zwykle z upodobaniem nagłaśniane przez media.

Ochrona informacji ma również związek z problemem konkurencyjności i postrzegania firmy przez klientów. Każdy jest odbiorcą oraz dostawcą informacji. Każdy chce zapewnienia, że proces wzajemnej wymiany informacji będzie odbywał się zgodnie z ustaleniami i będzie kontrolowany. Firmy świadomie zarządzające informacją i jej bezpieczeństwem poszukują partnerów będących na podobnym poziomie rozwoju. Eliminuje to z rynku tych, którzy pozostali w tyle i nie wprowadzili zarządzania informacją i jej bezpieczeństwem.

Wymagania prawne

Organizacje coraz lepiej uświadamiają sobie, że informacja jest bardzo ważnym, często kluczowym **zasobem** i musi być chroniona adekwatnie do swojej wartości. To chyba najsilniejszy i bezdyskusyjny argument za zarządzaniem bezpieczeństwem informacji. W naszym kraju obowiązuje co najmniej kilkanaście aktów prawnych związanych z ochroną pewnych informacji, do których musi stosować się każda, nawet mała firma. Brak takiej ochrony może skutkować ciężkimi sankcjami finansowymi i karnymi – czy to w stosunku do organizacji, czy do osób – i może doprowadzić nawet do zamknięcia działalności. W tym przypadku ochrona określonych informacji to nie wybór organizacji, tylko wymóg prawny.

Jak dbamy o bezpieczeństwo informacji?

Polskie firmy i instytucje coraz wyraźniej identyfikują wymagania ochrony informacji, zarówno biznesowe, jak i prawne. Deklarują, że muszą coś zrobić. Niektóre spośród nich – te bardziej zaangażowane – nawet usiłują coś zrobić.

Nie jest to proste zadanie. Skuteczna a zarazem efektywna (pod względem kosztów i efektów) ochrona wymaga zaangażowania się w wielu dziedzinach. W wielu przypadkach wymaga zmian organizacyjnych w firmie, większej lub mniejszej reorganizacji „codziennych" czynności pracownika i co najważniejsze – zmian w świadomości wszystkich pracowników, począwszy od najwyższego kierownictwa, a skończywszy na pracownikach wykonujących najprostsze czynności.

Jak to w życiu bywa, skutki działań nie zawsze są takie, jakich się spodziewano. Patrząc z perspektywy doświadczeń audytowych, kontaktów z zainteresowanymi organizacjami, można by pokusić się o pewnego rodzaju wykaz błędów i wypaczeń. Są one dosyć powtarzalne i łatwo je wskazać.

W celu uporządkowania błędy te można przyporządkować do następujących obszarów:

– organizacja bezpieczeństwa informacji,
– realizacja,
– czynnik ludzki.

Poniżej zaprezentowano najbardziej typowe i zarazem najczęściej popełniane błędy. Są one o tyle ciekawe, że, zdaniem autora, wcale nie wynikają z ograniczeń finansowych, a raczej z braku pomysłu na to, jak zapewnić bezpieczeństwo.

Działania doraźne – taktyka strusia, czyli jakoś to będzie...

Tak możemy określić zarządzanie bezpieczeństwem informacji polegające na podejmowaniu jednorazowych, nieskoordynowanych działań, doraźnie usuwających skutki incydentów, czyli funkcjonowanie na zasadzie „jakoś to będzie". Praktyka pokazuje, że najprawdopodobniej dojdzie do incydentu, po którym to „będzie" zamieni się w „już nie będzie ". W tym przypadku trudno mówić o jakiejkolwiek ochronie. Audytor może żartobliwie stwierdzić: „tu nie ma co audytować". Jest to jakiś sposób na przetrwanie, ale tylko przetrwanie i nic więcej.

Zróbmy to szybko i tanio!

Proponowany system najczęściej opiera się na kupionym od byle kogo i byle jak wdrożonym zestawie procedur. Pozornie wydaje się, że wszyscy powinni być zadowoleni – wdrożeniowiec, bo szybko sprzedał i się nie narobił, organizacja, bo ma system ochrony danych i wygrała przetarg – ale tak nie jest z prostej przyczyny – wydano wcale nie tak małe pieniądze, wykorzystano (mimo ofertowych zapewnień) całkiem spore zasoby (czas, ludzi, pieniądze), a efekty są żałośnie mizerne, bo zakupiony zestaw procedur nie pasuje do rodzaju biznesu i realiów organizacji. Całość działań i nakładów na „system" ochrony informacji okazuje się zwykłym marnotrawstwem sił i środków, co skruszeni menedżerowie po jakimś czasie sami przyznają. Jest to niestety częsty grzech. Zazwyczaj jest on konsekwencją przyjętej „polityki bezpieczeństwa", którą organizacja stworzyła samodzielnie albo kupiła od firmy konsultingowej.

Polityka ochrony informacji

Nikt nie aktualizuje procedur, nikt nie zajrzał do dokumentów od czasu ich wdrożenia. Większość pracowników dawno o nich zapomniała, a nowi w ogóle ich nie widzieli, ale wszędzie głośno i wyraźnie mówi się; „mamy przyjętą i zatwierdzoną politykę bezpieczeństwa".

Zwykle jeden audyt pozwala wykazać faktyczny brak zabezpieczenia informacji. Na czym polega problem? Skupiono się na stworzeniu zasad, procedur i instrukcji. Ci, którzy mieli więcej determinacji (i zasobów), wdrożyli opisane i zdefiniowane procedury. Zabrakło jednak czegoś istotnego – ciągłego monitorowania i oceniania procesów związanych z bezpieczeństwem informacji. Tylko ciągła ocena (wręcz „pomiar") bezpieczeństwa pozwala stwierdzić, jak ta ochrona jest realizowana.

Ale pomiar to nie wszystko. Trzeba jeszcze z wyników pomiaru korzystać i na ich podstawie podejmować decyzje, gdzie i co trzeba poprawić. A przede wszystkim należy robić to ciągle!

Warto zainteresować się normą ISO 27001, prezentującą skuteczny model zarządzania bezpieczeństwem informacji. Według tej normy jedną z fundamentalnych zasad postępowania jest wymuszanie na każdym kroku działań według koła Deminga, czyli „Planuj-Wykonuj-Sprawdzaj-Popraw" (cykl PDCA).

Etap „Planuj-Wykonuj" to, wbrew pozorom, coś, co najłatwiej zrealizować. Za to etap „Sprawdzaj-Popraw" to prawdziwe wyzwanie.

Czy bezpieczeństwo jest zapewnione przez sześć haseł i dziesięć podpisów?

Jest to przypadłość trapiąca różnego rodzaju departamenty bezpieczeństwa i urzędników tych departamentów, wynikająca z braku integracji zarządzania bezpieczeństwem informacji z resztą działań w organizacji. Krótko mówiąc, to bezpieczeństwo zamknięte za pancernymi drzwiami i w związku z tym mające określony, czyli żaden, kontakt z rzeczywistością.

W konsekwencji codzienne wymagania w działalności firmy i wymagania departamentu bezpieczeństwa coraz bardziej się rozmijają. Specyfika funkcjonowania firmy wymaga szybkich reakcji, często działań improwizowanych *ad hoc*, a tymczasem „spece" od bezpieczeństwa próbują na siłę wcisnąć wszystkich w jakieś ciasne ramy swoich procedur.

To jest błąd! Bezpieczeństwo musi być kompromisem pomiędzy tym, co jest wymagane, a tym, co jest wykonalne. Rozwiązania muszą być wspólnie wypracowane, a nie narzucone. Procedury muszą być nie tylko dobre dla organizacji, ale także akceptowane przez pracowników (niekoniecznie dobre, bo to nie zawsze się udaje, ale przynajmniej akceptowane).

Skoro dzisiaj jest wtorek, to jestem menedżerem bezpieczeństwa

Jedne z najczęstszych problemów zgłaszanych przez odpowiadających za bezpieczeństwo to stwierdzenia typu „nikt mnie nie słucha" albo „nie mam na to czasu". Szczególnie narzekają ci, których „poproszono" o przejęcie obowiązków urzędnika odpowiedzialnego za bezpieczeństwo informacji, bo ktoś musi nim być. Jest to zrozumiałe. Osobami odpowiedzialnymi za bezpieczeństwo zostają menedżerowie działów IT, administratorzy, informatycy. W konsekwencji ludzie ci, jako odpowiedzialni za realizację ochrony informacji, nadzorują samych siebie. Takie rozwiązanie mogłoby być zaakceptowane, jeśli nie ma innych możliwości. Problem polega na tym, że nie ma kontroli nad osobą zarządzającą.

Z drugiej strony wyżej wymienione osoby są często mocno obciążone pracą i jawnie deklarują, że dbanie o bezpieczeństwo informacji to dla nich dodatkowe obciążenie i zadanie, które będą realizować w miarę możliwości, a więc na ogół niedostatecznie. Podobnie jest w przypadku innych dodatkowo obciążonych pracowników, np. trenerów i wewnętrznych audytorów. Brak czasu na to, by zrealizować te dodatkowe działania, skutkuje zawsze tym samym – kiepskim bezpieczeństwem.

Istotną kwestią jest również pozycja i siła przebicia. Zaleca się, aby osoby odpowiedzialne za koordynację zarządzania jakością (pełnomocnicy) miały odpowiednie upoważnienia najwyższego kierownictwa, a równocześnie były niezależne od struktur wewnętrznych po to, by móc skutecznie działać, a przede wszystkim interweniować w razie stwierdzenia błędów czy nieprawidłowości. W dobrze zorganizowanych strukturach taki menedżer ma prawo wydawać polecenia służbowe wszystkim pracownikom i żądać wykonania tych poleceń. Obarczony odpowiedzialnością za bezpieczeństwo i ochronę informacji pracownik działu IT, który kontroluje swojego przełożonego, szefa działu IT, to wcale nierzadki przypadek.

W następnej części artykułu zostaną opisane inne błędy i kolejne problemy z bezpieczeństwem informacji.

Krzysztof Sierota
TÜV Nord Polska

Puszki instalacyjne PIP-1A i PIP-2A

światło i dźwięk dla bezpieczeństwa

PIP-1A

- Charakteryzuje się przelotowym prostym i kątowym (90°) sposobem prowadzenia linii sygnalizacyjnej.
- Umożliwia poprowadzenie do dwóch przewodów ze ściany
- Występuje w wersji Rozgałęźnej

PIP-2A

- Charakteryzuje się przelotowym prostym sposobem prowadzenia linii sygnalizacyjnej
- Występuje w wersji Przelotowej i Rozgałęźnej – dwu i trzyżyłowej
- Dwa rodzaje przekroju przewodu: 2,5 mm² i 6,0 mm²

W2 lider w produkcji sygnalizatorów do systemów sygnalizacji pożaru.

Dane adresowe:
W2 Włodzimierz Wyrzykowski
ul. Czajcza 6
86-005 Białe Błota
tel./fax (052) 584 01 92
tel. (052) 345 45 00
biuro@w2.com.pl

Puszki instalacyjne PIP-1A i PIP-2A firmy W2 przeznaczone są do podłączenia sygnalizatorów, głośników systemów rozgłaszania przewodowego DSO, klap dymnych, itd. Oba modele uzyskały **orzeczenie CNBOP** Nr 022/BA/2003. Odporność puszek instalacyjnych PIP-1A i PIP-2A na działanie wysokiej temperatury **E90** potwierdza **rekomendacja techniczna CNBOP** Nr RT CNBOP-0015/2008.

Więcej informacji na stronie **www.w2.com.pl**

Stacjonarne monitory promieniowania jonizującego

Mariusz Radoszewski

Promieniowanie jonizujące towarzyszy człowiekowi praktycznie każdego dnia. Jest ono emitowane przez różne źródła zlokalizowane w ziemi, przedmiotach czy też w przestrzeni kosmicznej. W zależności od rodzaju może być ono mniej lub bardziej przenikliwe. Przy dużej intensywności może być szkodliwe, dlatego należy podjąć wszelkie możliwe działania, aby ustrzec się przed nim w takiej sytuacji. Jednym ze sposobów jest monitorowanie i wykrywanie skażeń radioaktywnych, którym mogą ulec różnego rodzaju materiały przenoszone przez ludzi czy też przewożone w różnego rodzaju środkach transportu

Promieniowanie jądrowe jest promieniowaniem, które może powstać w układach ulegających przemianom jądrowym, w akceleratorach cząstek oraz – jak już wcześniej wspomniano – w otaczającej nas przestrzeni (promieniowanie kosmiczne). Charakter oddziaływania promieniowania z materią jest różny dla różnego rodzaju promieniowania.

Rodzaje promieniowania

Promieniowanie alfa (α) jako promieniowanie podstawowe

Jądra atomów różnych materiałów składają się z protonów i neutronów. W zależności od tego, ile protonów znajduje się w danym jądrze, mamy do czynienia z konkretnym pierwiastkiem (liczba neutronów nie ma w tym przypadku większego znaczenia, ponieważ może ona ulegać zmianom). Atomy jednego pierwiastka, które różnią się między sobą liczbą neutronów, to **izotopy**. Z powodu swojej „niestabilnej natury" niektóre z nich ulegają rozpadowi – emitują promieniowanie. Promieniowanie to, przechodząc przez materię, może – dzięki swojej dużej energii – wytrącać z jej atomów elektrony – jonizować ją, dlatego promieniowanie takie nazywa się jonizującym.

Podstawowym rodzajem promieniowania – najmniej przenikliwym – jest promieniowanie alfa (α). Powstaje ono na skutek wytrącenia z jądra atomu cząstki składającej się z dwóch protonów i dwóch neutronów. Jednym z bardziej znanych pierwiastków, emitującym właśnie ten rodzaj promieniowania, jest ameryk 241 (Am-241). Źródło to jest obecnie szeroko stosowane w produkcji jonizacyjnych czujek dymu, będących elementem systemów sygnalizacji pożarowej.

Promieniowanie alfa jest promieniowaniem na tyle mało przenikliwym, że może być zatrzymane przez kartkę papieru. W powietrzu rozchodzi się na odległość zaledwie 10 cm.

Promieniowanie beta (β)

Promieniowanie beta pojawia się na skutek przemiany neutronu w proton w jądrze atomu. Cząsteczki beta, które są przy tym emitowane, to po prostu elektrony. Istnieją również przypadki, gdy w wyniku przemiany jądrowej emitowana jest cząsteczka o ładunku dodatnim i masie równej masie elektronu – pozyton.

Przykładem takiego rozpadu może być przemiana trytu – w którego jądrze znajdują się jeden proton i dwa neutrony – w hel-3 (dwa protony i jeden neutron).

Promieniowanie β jest zdecydowanie bardziej przenikliwe niż promieniowanie typu α. W powietrzu może rozchodzić się na odległość nawet do 10 m. Z tego powodu źródła takiego promieniowania bardzo często są osłonięte. Jako osłony można użyć blachy aluminiowej, szkła organicznego, tworzywa sztucznego itp.

Promieniowanie gamma (γ) oraz X

Mechanizm emisji promieniowania gamma polega na wyzwoleniu energii powstałej w wyniku wzbudzenia jądra atomowego. Stany wzbudzenia jądra mogą towarzyszyć rozpadowi promieniotwórczych izotopów lub są następstwem przemian jądrowych.

Promieniowanie γ (jako jeden – obok promieniowania X – z rodzajów promieniowania elektromagnetycznego) powstaje więc w reakcjach jądrowych. Promieniowanie X jest natomiast efektem wzbudzenia lub wybicia elektronów orbitalnych bądź też wyhamowania elektronów.

Przenikliwość promieniowania typu γ jest tak duża, że źródła tego promieniowania (np. kobaltowe) muszą być osłonięte ze względów bezpieczeństwa. Jako osłonę stosuje się najczęściej kilkunastocentymetrową warstwę ołowiu, stali lub zubożonego uranu o grubości od kilku milimetrów do kilkudziesięciu centymetrów, w zależności od rodzaju i aktywności źródła.

Promieniowanie neutronowe (n)

Neutrony są cząstkami obojętnymi elektrycznie. Wolne neutrony powstają tylko na skutek reakcji jądrowych.

Najczęściej stosowane źródła wytwarzają tzw. elektrony prędkie, które są bardzo przenikliwe (przy jednoczesnej małej zdolności jonizacji). Rozmaitość oddziaływań i powstających przy tym rodzajów promieniowania wtórnego, jak również zależność oddziaływania od energii neutronów, powoduje, że trudno jest zbudować skuteczną osłonę chroniącą przed neutronami prędkimi.

Łatwo jest zatrzymać tzw. powolne neutrony, np. za pomocą cienkiej warstwy kadmu. Należy najpierw spowolnić neutrony za pomocą materiałów lekkich, zawierających dużo węgla lub wodoru (parafina, grafit, woda, polietylen), po czym użyć drugiej warstwy pochłaniającej neutrony termiczne. Spowolnienie neutronów jest również jednym z warunków wykrycia ich przez przeznaczone do tego detektory.

Rodzaje detektorów promieniowania jonizującego

Do detekcji promieniowania jonizującego służą różne przyrządy.

Detektory napełnione gazem to grupa detektorów, z której komora jonizacyjna, liczniki proporcjonalne oraz licznik Geigera-Müllera są najstarszymi i bardzo użytecznymi typami detektorów.

Obecnie najczęściej wykorzystywanym licznikiem omawianego rodzaju jest licznik Geigera-Müllera. Detektor ten może być wykorzystywany do pomiaru wszystkich rodzajów cząstek jądrowych, które chociaż w najmniejszym stopniu są w stanie zjonizować gaz znajdujący się w liczniku. Nadaje się on zwłaszcza do pomiarów promieniowania beta, gamma oraz X.

Detektory scyntylacyjne to urządzenia, które wykorzystują zjawisko powstawania błysków świetlnych zwanych scyntylacjami. Scyntylacje powstają na skutek przejścia cząstek lub kwantów jonizujących przez pewne kryształy. Licznik scyntylacyjny okazał się bardzo uniwersalny (jest wykorzystywany do detekcji wszystkich rodzajach promieniowania – przy zastosowaniu różnych scyntylatorów) i jest obecnie najbardziej wszechstronnym detektorem promieniowania jądrowego, powszechnie wykorzystywanym do wykrywania przede wszystkim promieniowania gamma przez stacjonarne monitory promieniowania.

Oprócz wyżej wymienionych rodzajów detektorów do pomiarów promieniowania jonizującego w różnych dziedzinach

Fot. 1. PM703AGN

Fot. 2. Układ detektorów PM703AGN (kolumna MASTER)

działalności gospodarczej powszechnie stosuje się detektory półprzewodnikowe, termoluminescencyjne, chemiczne i fotometryczne. Istnieje jeszcze wiele innych metod detekcji, które mają zastosowanie w badaniach naukowych.

Uregulowania prawne

Podstawowe regulacje dotyczące promieniowania jonizującego są zawarte w ustawie *Prawo atomowe* z dnia 29 listopada 2000 r. oraz w rozporządzeniach do ustawy, w tym w rozporządzeniu Rady Ministrów w sprawie odpadów promieniotwórczych i wypalonego paliwa jądrowego z dnia 3 grudnia 2002 r.

Dokumenty te zawierają podstawowe informacje dotyczące promieniowania jonizującego, wyszczególniają poziomy aktywności, na których poszczególne rodzaje pierwiastków są uznane za źródło promieniotwórcze, określają sposoby dystrybucji, przechowywania, ewidencjonowania, unieszkodliwiania różnego rodzaju odpadów oraz wskazują osoby odpowiedzialne za egzekwowanie poszczególnych zapisów regulacji.

Główną instytucją zajmującą się sprawami energii atomowej w Polsce jest Państwowa Agencja Atomistyki w Warszawie.

W związku z bardzo rozwiniętą wymianą handlową w Europie i na świecie powołano do życia różne organizacje, które zajmują się kwestiami związanymi z energią atomową. Organizacją o charakterze globalnym jest Międzynarodowa Agencja Energii Atomowej z siedzibą w Wiedniu.

W 2000 roku w Europie powołano specjalną komisję, której zadaniem jest praca nad uregulowaniami dotyczącymi problemu skażeń radioaktywnych złomu, odpadów poprodukcyjnych etc. Planowane jest opracowanie wspólnych procedur pomiarów, ewidencji i dokumentowania skażeń. Podstawowe procedury już istnieją, jednak na razie są tylko zalecane do stosowania (nie mają statusu obowiązujących).

Urządzenia do wykrywania i monitorowania radioaktywnych skażeń

Wykrywanie bardzo niskich poziomów radioaktywnych skażeń materiałów i produktów wymaga zastosowania nowoczesnych i niezawodnych przyrządów pomiarowych. Wykorzystują one wymienione wcześniej detektory (największy udział mają detektory scyntylacyjne, Geigera-Müllera oraz detektory neutronów).

Urządzenia te występują głównie w dwóch konfiguracjach – jako urządzenia stacjonarne oraz urządzenia przenośne.

Wśród stacjonarnych monitorów promieniowania można wyróżnić kilka podstawowych grup urządzeń:

Fot. 3. PM703AGN do kontroli osób na przejściu granicznym

Fot. 4. PM703AGN do kontroli bagaży

– urządzenia do kontroli ruchu osób i (lub) bagażu (**PM703AGN**),
– urządzenia do kontroli ruchu pojazdów, zarówno tych poruszających się po drogach, jak i szynowych (**VM250AGN**),
– urządzenia do kontroli przewożonego złomu metali w transporcie drogowym i kolejowym (**VM250AG/09Z**) oraz na składowiskach odpadów.

PM703AGN

Stacjonarny monitor promieniowania gamma i promieniowania neutronowego PM703AGN (fot. 1) jest przeznaczony do wykrywania materiałów radioaktywnych i jądrowych, znajdujących się w kontrolowanych obiektach (np. w samochodach osobowych, na wózkach bagażowych, na taśmociągach) lub przenoszonych przez osoby przechodzące przez strefę kontrolną. Wymiary strefy kontrolnej oraz poziomy aktywności wykrywanego w niej promieniowania odpowiadają wymaganiom Międzynarodowej Agencji Energii Atomowej (IAEA) w Wiedniu oraz normom międzynarodowym.

Kontrola odbywa się automatycznie, podczas przejazdu obiektu lub przejścia osób przez strefę kontrolną (detekcyjną). Przekroczenie ustalonego progu alarmowego powoduje uruchomienie sygnalizacji optycznej i akustycznej (odpowiednich sygnalizatorów umieszczonych na obudowie monitora).

Urządzenia mogą być wykorzystywane m.in.:
– na przejściach granicznych drogowych, morskich i lotniczych,
– w punktach kontrolnych elektrowni jądrowych, w przedsiębiorstwach przemysłu jądrowego, zakładach i magazynach produkcji zbrojeniowej,
– przy wejściach do instytucji państwowych, banków, urzędów pocztowych itp.

Stacjonarny monitor promieniowania gamma i promieniowania neutronowego typu PM703AGN może być wykonany w dwóch wersjach:

1) PM703AGN-1 – zawiera jedną kolumnę detekcyjną (MASTER) dozorującą strefę kontrolną w odległości do jednego metra od tej kolumny i o wysokości do dwóch metrów. Kolumna zawiera jeden detektor promieniowania gamma i jeden detektor promieniowania neutronowego (fot. 2).
2) PM703AGN-2 – zawiera dwie kolumny detekcyjne (MASTER i SLAVE) usytuowane naprzeciw siebie i dozorujące strefę kontrolną o szerokości do sześciu metrów i wysokości do dwóch metrów. Każda kolumna zawiera jeden detektor promieniowania gamma i jeden detektor promieniowania neutronowego.

Urządzenia są przystosowane do pracy w pomieszczeniach zamkniętych i otwartej przestrzeni.

Informacje o stanie systemu (o przekroczonych progach alarmowania, uszkodzeniach etc.) mogą być sygnalizowane za pośrednictwem wyniesionego terminala kontrolnego stacjonarnych monitorów promieniowania TK-1 (fot. 5). Terminal kontrolny stacjonarnych monitorów promieniowania TK-1 jest niezależnym urządzeniem przeznaczonym do zdalnej

Fot. 5. Terminal kontrolny stacjonarnych monitorów promieniowania TK-1

Fot. 6. VM250AGN

współpracy ze stacjonarnym monitorem promieniowania. Do terminala mogą być transmitowane sygnały akustyczne i optyczne o poziomie promieniowania, wysokim i niskim poziomie promieniowania tła, uszkodzeniach oraz niektórych czynnościach obsługowych. Na wyświetlaczu ciekłokrystalicznym (LCD) można obserwować na bieżąco zliczenia (impulsy na sekundę) poszczególnych detektorów oraz ich sumę, a także odczytać wszystkie informacje dotyczące stanu monitora. Wbudowana drukarka termiczna pozwala na drukowanie raportu w przypadku wystąpienia stanów alarmowych oraz w innych sytuacjach określonych przez użytkownika. Terminal jest wyposażony w pamięć pozwalającą na odtworzenie historii zdarzeń. Terminal kontrolny TK-1 może współpracować aż z 16 stacjonarnymi monitorami promieniowania jednocześnie (jeżeli jest taka potrzeba).

W przypadku konieczności nadzorowania kilku (kilkudziesięciu, kilkuset) stacjonarnych monitorów promieniowania (oddalonych od siebie) można wykorzystać komputerowy system rejestracji i przeglądu zdarzeń radiacyjnych, które zostały zaobserwowane w miejscach zainstalowania urządzeń.

System RADIOMETRIA z kanałem wideo umożliwia:

– monitorowanie stanu połączenia z monitorami włączonymi do systemu,
– monitorowanie statusu działania monitorów,
– rejestrowanie wszelkich zdarzeń sygnalizowanych przez monitory, a w szczególności stanów alarmowych,
– gromadzenie danych opisujących wystąpienie alarmu gamma lub neutronowego w postaci formularza,
– gromadzenie danych o działaniu systemu w bazie danych,
– wykonywanie parametryzowanych raportów z danych zgromadzonych w bazie danych,
– podgląd obrazów z kamer z poziomu komputera nadzorującego system,
– rejestrację wideo w czasie trwania alarmu (z przeglądem wstecz),
– przeglądanie zarejestrowanego materiału dotyczącego zdarzenia alarmowego,
– wybór zdjęcia z zarejestrowanego materiału pokazującego obiekt powodujący alarm i wydrukowanie protokołu wraz z tym zdjęciem,
– nadzór działania kamer (sprawdzanie, czy jest z nimi łączność).

System RADIOMETRIA uzyskał akceptację Komendy Głównej Straży Granicznej w Warszawie dotyczącą funkcjonalności, bezpieczeństwa, a także zgodności z ustawą o ochronie danych osobowych (integralność danych, przepływy danych między podsystemami, rozliczalność działań użytkowników, bezpieczeństwo dostępu do danych, uwierzytelnianie, prawa dostępu, konserwacja systemu).

VM250AGN

Stacjonarny monitor promieniowania gamma i promieniowania neutronowego VM250AGN (fot. 6) jest przeznaczony do wykrywania materiałów radioaktywnych i jądrowych, znajdujących się w pojazdach i obiektach (np. samochodach ciężarowych, autobusach, wagonach, kontenerach itp.) przemieszczających się przez strefę kontrolną (detekcyjną). Wymiary strefy kontrolnej oraz poziomy aktywności wykrywanego w niej promieniowania odpowiadają wymaganiom Międzynarodowej Agencji Energii Atomowej (IAEA) w Wiedniu oraz międzynarodowym normom.

Kontrola i sygnalizacja zadziałania odbywa się automatycznie, podobnie jak w przypadku PM703AGN.

Urządzenie może być wykorzystywane m.in.:

– na przejściach granicznych (drogowych, kolejowych, morskich i lotniczych),
– w punktach kontrolnych elektrowni jądrowych,

przedsiębiorstwach przemysłu jądrowego, zakładach i magazynach produkcji zbrojeniowej, instytutach fizyki jądrowej,
– w składowiskach odpadów materiałów promieniotwórczych, odpadów przemysłowych i komunalnych,
– w punktach kontrolnych instytucji państwowych, banków, urzędów pocztowych itp.

Stacjonarny monitor promieniowania gamma i neutronowego typu VM250AGN zawiera dwie kolumny detekcyjne (*MASTER i SLAVE*) usytuowane naprzeciw siebie i dozorujące strefę kontrolną o szerokości do sześciu metrów i wysokości do czterech metrów. Każda kolumna zawiera dwa detektory promieniowania gamma i dwa detektory promieniowania neutronowego (po dwa liczniki helowe). Urządzenie jest przystosowane do pracy w otwartej przestrzeni.

Podobnie jak PM703AGN, stacjonarne monitory promieniowania VM250AGN mogą współpracować z terminalami kontrolnymi stacjonarnych monitorów promieniowania TK-1 oraz komputerowym systemem nadzoru i wizualizacji RADIOMETRIA.

VM250AG/09Z

Stacjonarny monitor promieniowania gamma typu VM250AG/09Z (fot. 7) jest przeznaczony do wykrywania materiałów radioaktywnych w pojazdach ciężarowych oraz wagonach kolejowych przemieszczających się przez strefę kontrolną.

Kontrola odbywa się automatycznie, podczas przejazdu pojazdów przez strefę kontrolną. Przekroczenie ustalonego progu alarmowego powoduje uruchomienie sygnalizacji optycznej i akustycznej.

Urządzenie jest przeznaczone do stosowania:
– w zakładach handlu i przerobu złomu,
– w hutach,
– na składowiskach odpadów.

Stacjonarny monitor promieniowania gamma typu VM250AG/09Z zawiera dwie kolumny detekcyjne (MASTER i SLAVE) usytuowane naprzeciw siebie i dozorujące strefę kontrolną.

Każda z kolumn zawiera po dwa detektory gamma o wielkiej objętości i specjalnej konstrukcji dostosowanej do wykrywania źródeł promieniotwórczych ekranowanych przez złom metali.

Wymagania Międzynarodowej Agencji Energii Atomowej w Wiedniu oraz norm międzynarodowych określają minimalne poziomy aktywności wykrywanych źródeł promieniowania dla strefy kontrolnej o standardowych wymiarach: 6 x 4 [m] (szerokość x wysokość). W strefie kontrolnej o innych wymiarach poziomy aktywności wykrywanych źródeł będą się zmieniały z kwadratem odległości między kolumnami MASTER i SLAVE. Przy odległości 3 m urządzenie może wykryć źródło promieniowania o aktywności 4-krotnie mniejszej, a przy odległości 12 m – 4-krotnie większej od aktywności ustalonej dla szerokości 6 m. Dlatego zaleca się jak najmniejszy odstęp między kolumnami (już od 3 m). Maksymalny odstęp nie powinien przekraczać 7–8 m.

Charakterystyczne dla tego typu monitorów jest to, że zawierają one tylko kanał detekcji promieniowania gamma. Jest on jednak znacznie bardziej czuły niż w przypadku pozostałych typów urządzeń, wymienionych wcześniej. Jest to związane ze znacznie zwiększoną objętością czynną detektorów,

Fot. 7. VM250AG/09Z

Fot. 8. PM-1401M

Fot. 9. PM-1401GN

która dla pojedynczego detektora wynosi 14 100 cm^3 (to niemal trzykrotnie więcej niż w przypadku detektorów monitorów PM703AGN i VM250AGN).

Podobnie jak opisane wcześniej urządzenia, VM250AG/09Z współpracuje z terminalem TK-1 oraz systemem RADIOMETRIA.

Jeżeli nastąpi wykrycie materiałów promieniotwórczych/skażonych izotopami promieniotwórczymi, dotyczyć będzie ono całego pojazdu wraz z transportowanym ładunkiem czy też człowieka oraz jego bagażu.

Aby móc skutecznie wyselekcjonować skażony element lub partię materiału, należy wykorzystać ręczne urządzenia, przeznaczone do poszukiwania, lokalizacji, a także identyfikacji materiałów promieniotwórczych. Najpopularniejszą grupą tego typu urządzeń są ręczne monitory promieniowania gamma lub gamma i neutronowego. Te, które występują w Polsce w największej liczbie to m.in. ręczny monitor promieniowania gamma PM-1401/1401M (fot. 8), ręczny monitor promieniowania gamma i neutronowego PM-1401GN (fot. 9) oraz wielofunkcyjny monitor promieniowania/spektrometr z funkcją identyfikacji izotopów PM-1401K. Każde z tych urządzeń pozwala na dokładne sprawdzenie transportu w celu odseparowania skażonego elementu.

Realizowanie rozbudowanego i kompleksowego systemu kontroli ruchu osób i towarów na granicach Polski oraz na składowiskach złomu czy odpadów znacząco ograniczyło ilość przypadków wwożenia na teren naszego kraju materiałów skażonych promieniotwórczo, czy też, w przypadku hut, przerobu skażonego materiału wsadowego.

Ciągłe prace badawczo-rozwojowe, które prowadzone są w POLON-ALFA, powodują, że poziom techniczny urządzeń, zaimplementowane algorytmy detekcji sytuują opisane powyżej urządzenia w światowej czołówce tego typu rozwiązań.

mgr inż. Mariusz Radoszewski
POLON-ALFA

Literatura:

1. W. J. Price *Detekcja promieniowania jądrowego*. Państwowe Wydawnictwa Techniczne, Warszawa 1960 r.
2. B. Gostkowska, *Wielkości, jednostki i obliczenia stosowane w ochronie radiologiczne*. Centralne Laboratorium Ochrony Radiologicznej, Warszawa 1991 r.
3. Ustawa Prawo atomowe z dnia 29.11.2000 r. z późniejszymi zmianami.
4. Rozporządzenie Rady Ministrów w sprawie odpadów promieniotwórczych i wypalonego paliwa jądrowego z dnia 03.12.2002 r.
5. A. Piliszczuk *Metody detekcji promieniowania jonizującego*, POLON-ALFA, Bydgoszcz, 2005.

POLON-ALFA NAJNOWSZA TECHNOLOGIA. NAJWYŻSZA JAKOŚĆ

POLON 4100

NOWY WYMIAR BEZPIECZEŃSTWA

„POLON-ALFA" Zakład Urządzeń Dozymetrycznych sp. z o.o.

85-861 Bydgoszcz, ul. Glinki 155, www.polon-alfa.pl

Kopie bezpieczeństwa

Krzysztof Białek

Każdy komputer jest składnicą informacji. Na dysku twardym zgromadzona jest duża ilość danych niezbędnych do prawidłowego funkcjonowania samego komputera, systemu operacyjnego i aplikacji w nim zainstalowanych, znajdują się dane w postaci dokumentów (firmowych czy prywatnych), zdjęć, filmów i wiele innych, wytworzonych w czasie pracy na komputerze lub przekopiowanych z innych źródeł. Bez jednych moglibyśmy się bez problemu obejść, inne są dla nas o wiele bardziej cenne. O tym, jak bardzo, niejednokrotnie przekonujemy się dopiero w momencie, gdy z jakichś przyczyn dostęp do nich jest dla przeciętnego użytkownika znacznie utrudniony lub wręcz niemożliwy

W elementarzu każdego administratora systemowego nie może zabraknąć takiego pojęcia, jak „kopia bezpieczeństwa". Osoba, która jest odpowiedzialna i zajmuje się administrowaniem serwerami, bazami danych czy złożonymi aplikacjami, wie, jak ważne jest posiadanie kopii systemowej. Jej wykorzystanie może być jedyną deską ratunku w sytuacji awaryjnej.

Na początek – dla porządku – warto zwrócić uwagę, iż pojęcia „backup" i „kopia danych" bardzo często są ze sobą mylone. I jedno i drugie oznacza tzw. kopię bezpieczeństwa, jednak różnica tkwi w funkcji przedmiotów odnoszących się do tych pojęć. Backup jest zazwyczaj obrazem dysku lub odwzorowaniem środowiska systemowego, umożliwiającym uruchomienie systemu, bazy danych lub aplikacji w sposób umożliwiający dalszą pracę – dzięki „powrotowi" do pewnego momentu w historii, w którym dana kopia środowiska została wytworzona. Na kopię danych zaś składają się konkretne pliki, na których zabezpieczeniu najbardziej nam zależy.

Postaram się wyjaśnić to obrazowo na przykładzie.

Pan Kowalski ma w swoim domowym komputerze dysk twardy o pojemności 40 GB, który jest w całości przydzielony partycji systemowej. System operacyjny wraz z podstawowymi aplikacjami zajmuje około 10 GB, a na pozostałą część składają się dane dla aplikacji, dokumenty i zdjęcia. Nasz pan Kowalski jest osobą zapobiegliwą i raz na tydzień wykonuje backup całego dysku twardego na innym, zewnętrznym dysku twardym. Dzięki temu w sytuacji wystąpienia awarii systemu bądź podstawowego dysku twardego będzie mógł w krótkim czasie wykorzystać backup do odtworzenia nie tylko samych danych, ale także kompletnego środowiska systemowego – bez konieczności żmudnej instalacji wszystkich komponentów systemu i poszczególnych aplikacji. Co prawda w ten sposób może utracić zmiany wprowadzone w systemie oraz dane, które powstały pomiędzy datą utworzenia backupu a dniem awarii, ale jest to stosunkowo niewielka strata – byłoby gorzej, gdyby takiego backupu nie posiadał w ogóle lub wykonywał go z mniejszą częstotliwością.

Kopia danych (która także jest kopią bezpieczeństwa) to zbiór dokumentów i innych plików, które nie umożliwią przywrócenia poprawnej pracy komputera, ale zapewnią możliwość dostępu do konkretnych informacji w przypadku awarii twardego dysku – w przypadku pana Kowalskiego mogą to być np. zdjęcia z wakacji.

W zależności od krytyczności systemu wykorzystuje się różne metody tworzenia kopii bezpieczeństwa.

W przypadku rozwiązań domowych zazwyczaj wystarczy tworzyć je na zewnętrznych dyskach twardych lub dyskach CD/DVD. Te ostatnie są bardziej uciążliwe, gdyż do zabezpieczenia dysku twardego o większej pojemności trzeba użyć dużej liczby CD/DVD. Wygodniejszą metodą jest wykonywanie zabezpieczeń na dodatkowych dyskach twardych podłączanych bezpośrednio do płyty głównej komputera, jak dyski podstawowe, lub poprzez złącze USB. Do wykonania kopii danych nie są potrzebne dodatkowe programy narzędziowe – wystarczy podłączyć dodatkowy dysk do komputera i po prostu przekopiować na niego dane, na których zabezpieczeniu zależy nam najbardziej. Sytuacja jest nieco bardziej skomplikowana, jeżeli chcemy wykonać backup systemu operacyjnego lub całego dysku twardego – wówczas konieczne jest posiadanie odpowiednich narzędzi informatycznych, nie tylko do utworzenia takiej kopii bezpieczeństwa, ale również do ewentualnego odtworzenia środowiska systemowego z backupu. Na rynku jest bardzo wiele tego typu oprogramowania różniącego się zarówno funkcjami, jak i ceną. Przy odrobinie chęci niedrogi albo nawet darmowy program – może nie w najnowszej wersji, ale za to skuteczny – można znaleźć na dobrych stronach z legalnym oprogramowaniem. Bardzo zaawansowane rozwiązania są z reguły płatne, ale do użytku domowego rozbudowane funkcje nie są potrzebne.

W przypadku firm różnorodność stosowanego oprogramowania jest większa. Niewielkim przedsiębiorstwom mogą wystarczyć „domowe" sposoby zabezpieczania się przed utratą danych wynikającą z awarii sprzętu czy systemu operacyjnego. Firmy, których poprawne funkcjonowanie opiera się na posiadaniu możliwości nieprzerwanego dostępu do zasobów informatycznych, stosują bardziej wyrafinowane metody tworzenia kopii bezpieczeństwa. Jedną z najczęściej stosowanych jest posiadanie w sieci komputerowej serwera zasobowego, na którym dla każdego użytkownika skonfigurowane są odpowiednie połączenia, które umożliwiają przekopiowanie danych ze swojego komputera na dysk serwera. Jeśli takie rozwiązanie nie jest zautomatyzowane i jest zależne jedynie od tego, czy użytkownik sam przekopiuje wrażliwe dane, czy tego nie wykona, istnieje duże ryzyko nieskuteczności takiej metody. Jeżeli nieprzerwany dostęp do danych jest sprawą krytyczną, zazwyczaj korzysta się z systemów i aplikacji scentralizowanych, w których komputer użytkownika stanowi jedynie terminal do komunikowania się z serwerami centralnymi, na których znajdują się dane. Taki system informatyczny, oparty na centralnym zarządzaniu, jest o wiele bardziej skuteczny w kontekście efektywności zarządzania, a przy dużej liczbie stacji roboczych tego typu rozwiązanie jest również bardziej efektywne kosztowo. Przy założeniu, że firma posiada 50 stacji roboczych, dla których administratorzy musieliby dokonywać częstych backupów systemów, jest ono znacznie mniej efektywne niż wykonywanie backupu systemu centralnego.

Im większa jest firma, tym bardziej zaawansowane rozwiązania technologiczne są wykorzystywane. Stosowane są backupy systemowe serwerów centralnych oraz kopie baz danych. Jeszcze bezpieczniejsze rozwiązania bazują na redundantnie zbudowanej infrastrukturze informatycznej, która działa we wzajemnym połączeniu fizycznym i systemowym, czyli na tak zwanych klastrach. Takie rozwiązania pozwalają na synchronizację danych pomiędzy różnymi instalacjami w trybie rzeczywistym, a awaria któregoś z komponentów sprzętowych czy systemowych jest dla użytkownika praktycznie niezauważalna, ponieważ system automatycznie przekierowuje go z jednego zasobu do innego. Klaster może być zbudowany lokalnie (w tym samym pomieszczeniu, budynku), jednak duże instytucje posiadają takie rozwiązania funkcjonujące w różnych ośrodkach przetwarzania danych, co minimalizuje ryzyko utraty możliwości prowadzenia działalności biznesowej w przypadku katastrofy budowlanej lub innego zagrożenia uniemożliwiającego korzystanie z infrastruktury w jednej z lokalizacji. Ci, którzy nie posiadają własnych ośrodków przetwarzania danych, mogą posiłkować się usługami kolokacji własnych zasobów do ośrodków dostawcy zewnętrznego, które to usługi stają się coraz bardziej popularne również na polskim rynku. Możliwe jest również wynajęcie całej infrastruktury bądź kompleksowe wyprowadzenie na zewnątrz usług informatycznych. Wszystko zależy od wyceny ryzyka i posiadanych środków przeznaczonych na realizację tego typu przedsięwzięć.

Na temat sposobów zabezpieczania się przed utratą danych można dyskutować przez wiele dni i nocy, a przedstawione powyżej przykłady rozwiązań stanowią zaledwie wierzchołek góry lodowej. Pytanie zasadnicze, które należałoby zadać sobie teraz brzmi: „A w jaki sposób Ty zabezpieczasz się przed utratą swoich danych służbowych i prywatnych na wypadek awarii dysku twardego, systemu operacyjnego czy serwera?".

Krzysztof Białek

ODKRYJ SZYBKOŚĆ INSTALACJI

DSC

WT5500
Bezprzewodowa klawiatura LCD

WT4989
Bezprzewodowy pilot
z wyświetlaczem LCD

WS4904W
Bezprzewodowe czujki PIR

WS4945
Bezprzewodowa
czujka kontaktronowa

Wyłączny dystrybutor produktów DSC w Polsce:

AAT Holding sp. z o.o.
ul. Puławska 431, 02-801 Warszawa, tel. 22 546 05 46, faks 22 546 05 01
e-mail: aat.warszawa@aat.pl, www.aat.pl

ALEXOR PC9155

BEZPRZEWODOWY SYSTEM ALARMOWY
O KOMUNIKACJI DWUKIERUNKOWEJ

- Obsługa maksymalnie 32 urządzeń bezprzewodowych i 16 breloków
- Kompatybilność z urządzeniami o komunikacji jednokierunkowej
- Obsługa do 4 sygnalizatorów i klawiatur bezprzewodowych
- Funkcja automatycznego przypisywania urządzeń bezprzewodowych
- Szablony programowania skracające czas instalacji
- 16 kodów użytkownika, 1 kod główny, 1 kod konserwatora
- Funkcja sprawdzania kodu identyfikacyjnego systemu
- Alternatywna komunikacja przez sieć GSM/GPRS lub TCP/IP
- Wbudowany sygnalizator akustyczny o mocy 85dB
- 2 zaciski I/O, które mogą być zaprogramowane jako wyjścia PGM lub przewodowe linie dozorowe
- 200mA obciążalności prądowej wyjścia AUX
- Rejestr 500 zdarzeń
- Podwójne zabezpieczenie antysabotażowe przed otwarciem obudowy lub oderwaniem od ściany
- 24 godzinne podtrzymanie baterii

Pozostałe urządzenia bezprzewodowe kompatybilne z centralą PC9155:

WS4939, PT4
Bezprzewodowy pilot i brelok zbliżeniowy

TL265GS, GS2065
Komunikatory alarmowe wysyłające kody raportujące przez sieć GSM/GPRS i TCP/IP

WT4901
Bezprzewodowy sygnalizator wewnętrzny

WT4911
Bezprzewodowy sygnalizator zewnętrzny

WS4916
Bezprzewodowa czujka dymu

WS4985
Bezprzewodowa czujka zalania wodą

WLS912L
Bezprzewodowa czujka zbicia szyby

WS4975
Bezprzewodowa czujka kontaktronowa

Nowe spojrzenie
na telewizję dozorową

Paweł Król

Firma GDE Polska, poszerzając swoją ofertę o dział CCTV, nawiązała współpracę z firmą CNB, należącą do grona czołowych producentów kamer CCTV, jednocześnie zostając wyłącznym dystrybutorem tych kamer na polskim rynku

CNB TECHNOLOGY Inc.

Nazwa firmy jest skrótem od *Challenge, New Technology and Best Quality*, co można przetłumaczyć jako „Wyzwania, Nowa Technologia oraz Najlepsza Jakość". Dbając o zachowanie zgodności swojej nazwy ze standardami działania, firma CNB nastawiona jest przede wszystkim na budowanie wizerunku firmy wyspecjalizowanej w dziedzinie technologii zabezpieczeń.

Firma CNB powstała w 1999 roku. Obecnie jest jednym z czołowych producentów kamer na świecie. Jej siedziba znajduje się w Seulu, w Korei Południowej. Od początku istnienia firmy działa oddział w USA, a w zeszłym roku otwarto biuro w Europie. Potwierdzeniem pozycji CNB na światowym rynku jest wzrost sprzedaży o 220% w ciągu sześciu lat.

Co jeszcze przemawia na korzyść firmy CNB? Między innymi wieloletnie doświadczenie, wdrażanie nowych rozwiązań technologicznych, korzystny wizerunek firmy na tle konkurencji, stosowanie własnych procesorów DSP typu Monalisa oraz Blue-I oraz wdrażanie nowej technologii Inteligent IR.

Aż 32% osób zatrudnionych w firmie pracuje w dziale R&D (*Research & Development*), a na badania i rozwój przeznacza się 5% dochodów ze sprzedaży. CNB opatentowało między innymi jedenaście rodzajów obudów, pięć rozwiązań software'owych, system sterownia kamerami z obiektywami motor-zoom, wielokanałowy system zdalnego monitoringu wizyjnego w sieci IP.

Firma CNB wielokrotnie zdobywała nagrody przyznawane eksporterom, a także za osiągnięcia w dziedzinie wzornictwa przemysłowego. Jedna z nagród to *Good Design Prize*, przyznawana przez prestiżowy Korea Institute of Design Promotion. Wszystkie produkowane przez CNB urządzenia posiadają certyfikaty CE oraz FCC, zaś obudowy do zastosowań zewnętrznych mają klasę szczelności IP65 oraz IP66.

Oferta obejmuje wszystkie rodzaje kamer wraz z niezbędnymi akcesoriami (uchwyty, zasilacze itp.). Wdrożenie własnych procesorów DSP pozwala na poprawę jakości obrazu w porównaniu z produktami firm konkurencyjnych, a jednocześnie zachowanie porównywalnego poziomu cenowego.

Obecnie wdrażane są nowe typy kamer, które wyróżniają się procesorem DSP Monalisa. Zastosowanie nowego procesora DSP pozwoliło na poprawę działania kamer przy słabym oświetleniu oraz umożliwiło doskonałe odwzorowanie kolorów przy zmiennym oświetleniu.

Kamery z procesorem Monalisa cechują:
- duża rozdzielczość, wynosząca 600 TVL w trybie kolorowym oraz 650 TVL w trybie czarno-białym,
- zaawansowana redukcja szumów DNR (*Digital Noise Reduction*),
- opcje maskowania stref prywatności oraz funkcje detekcji ruchu,
- ulepszona kompensacja tylnego oświetlenia SBLC (*Super Back Light Compensation*).

W warunkach dobrego oświetlenia pozytywnie zaskakuje wierna reprodukcja barw, znakomita ostrość obrazu oraz dobrze działająca kompensacja tylnego oświetlenia, lecz dopiero w słabym oświetleniu kamery z procesorem Monalisa pokazują swoje zalety – bardzo małe smużenia przy włączonej funkcji redukcji szumów oraz wysoką czułość.

W ciągu najbliższych kilku miesięcy pojawi się także grupa kamer wyposażona w procesor Blue-I.

Najważniejsze cechy odróżniające go od układu Monalisa to:
- funkcja *sens-up* (inaczej DSS – *Digital Slow Shutter*),
- eklipsa (przesłanianie prześwietlonych części obrazu),
- WDR (poszerzony zakres dynamiki),
- redukcja szumów 3D DNR (*3 Dimensional Digital Noise Reduction*).

Fot. 1. Klasyczne podświetlenie - General IR (A,C) oraz podświetlenie adaptacyjne - Intelligent IR (B,D)

Kolejne osiągnięcie to opcja *Intelligent IR* (inteligentne podświetlenie z użyciem podczerwieni). Klasyczne elementy oświetlające załączają się poniżej pewnego progu oświetlania zewnętrznego i święcą światłem o stałym natężeniu, niezależnie od odległości od obserwowanego obiektu. Powoduje to przejaskrawienia obrazu obiektów znajdujących się zbyt blisko, często całkowicie uniemożliwiając obserwację. Podświetlenie inteligentne (*Intelligent IR*) dostosowuje swą jasność do odległości od obserwowanego obiektu. Dzięki temu obiekt jest zawsze optymalnie doświetlony, niezależnie od odległości, a dodatkowo wydłuża się żywotność diod IR LED o ok. 50%. Zalety podświetlenia adaptacyjnego są szczególnie widoczne przy obserwacji człowieka zbliżającego się do kamery.

Jednymi z najpopularniejszych kamer są kamery kopułkowe DFL-21S oraz VCM-21VF.

DFL-21S to podstawowa kamera wewnętrzna z obiektywem o stałej ogniskowej, wyposażona w procesor Monalisa.

W ten sam procesor wyposażona jest wandaloodporna kamera VCM-21VF, która posiada klasę szczelności IP65, dzięki czemu może być stosowana w warunkach zewnętrznych. Kamera ma obiektyw o ogniskowej regulowanej w zakresie 2,8 mm do 10,5 mm, odsuwany filtr IR oraz wiele funkcji obsługiwanych poprzez system OSD.

Poza kamerami analogowymi oferta CNB obejmuje także kamery IP o rozdzielczości VGA oraz 1,3 Mpix. W drugiej połowie roku dostępne będą także nowo opracowywane kamery o rozdzielczości 2 Mpix oraz druga generacja kamer o rozdzielczości 1,3 Mpix. Wraz z kamerami udostępnione będzie darmowe oprogramowanie do podglądu, rejestracji oraz zarządzania kamerami IP.

Fot. 2. Kamera kopułkowa DFL-21S

Fot. 3. Szybkoobrotowa kamera S2965PX z osłoną przeciwsłoneczną

Dostępne są również cztery grupy kamer szybkoobrotowych z rodziny XPEED – kamery Speed Dome w obudowach wewnętrznych i zewnętrznych oraz kamery mini Speed Dome w obudowach wewnętrznych i zewnętrznych.

Zaletami wszystkich kamer szybkoobrotowych jest odsuwany filtr podczerwieni, funkcja DSS (*Digital Slow Shutter*) zwiększająca czułość przy słabym oświetleniu, duża szybkość obrotowa (360°/s), funkcja *Auto Flip*, czyli automatyczne odwrócenie obrazu w trakcie obrotu kamery w pionie, a także funkcja *parking*, czyli automatyczny powrót na zadane położenie w przypadku braku aktywności operatora.

Kamery Speed Dome są wyposażone w zmiennoogniskowy obiektyw o krotności do ×36 oraz cyfrowy zoom o krotności ×10 lub ×12. Obsługa kamery jest łatwa dzięki możliwości zaprogramowania 128 presetów, czyli zapamiętanych położeń kamery wraz z pełnymi ustawieniami parametrów ekspozycji dla każdego presetu. Bardzo użyteczna jest funkcja *pattern*, dzięki której możemy zapamiętać trasę obserwacji wyznaczoną przez operatora. Możliwe jest także grupowanie funkcji pozwalające na sekwencyjne wykonanie 20 różnych komend w zadanych odstępach czasu.

Łatwy montaż, zabezpieczenie przed upadkiem kamery podczas montażu oraz pełny zestaw akcesoriów do montażu ściennego, sufitowego, narożnego oraz na słupie to kolejne zalety kamer szybkoobrotowych CNB.

Oferta koreańskiej firmy CNB pozwala na realizację różnorodnych instalacji służących do monitoringu wizyjnego, niezależnie od ich wielkości czy specyficznych wymagań klienta.

Świadectwem jakości jest 36-miesięczna gwarancja na kamery stałopozycyjne, 24-miesięczna gwarancja na kamery szybkoobrotowe i 12-miesięczna gwarancja na diodowe moduły podświetlające zastosowane w kamerach. Warto pamiętać, że jest to gwarancja typu *door to door* z dostawą sprzętu we wskazane przez klienta miejsce.

Paweł Król
GDE Polska

Czy mogą Państwo zagwarantować taką samą politykę bezpieczeństwa na całym świecie?

Wielkie firmy stają się globalne. Filie wyrastają na całym świecie. Państwa firma może pracować w różnych strefach czasowych, w innych kulturach, według innych standardów i wartości. Ale nie może zaakceptować różnej polityki w zakresie bezpieczeństwa. Jeżeli standardy bezpieczeństwa w Szanghaju są inne od tych w San Diego, ponoszą Państwo ryzyko. Państwa pracownicy pracują w biurach położonych w różnych częściach świata. Dlatego potrzebne są Państwu środki pozwalające określić, kto będzie miał dostęp do budynków i informacji. AEOS Global Enterprise Edition pozwala na całościowe zarządzanie bezpieczeństwem, na całym świecie, poprzez jeden system.

Nie ryzykuj. Nedap AEOS.

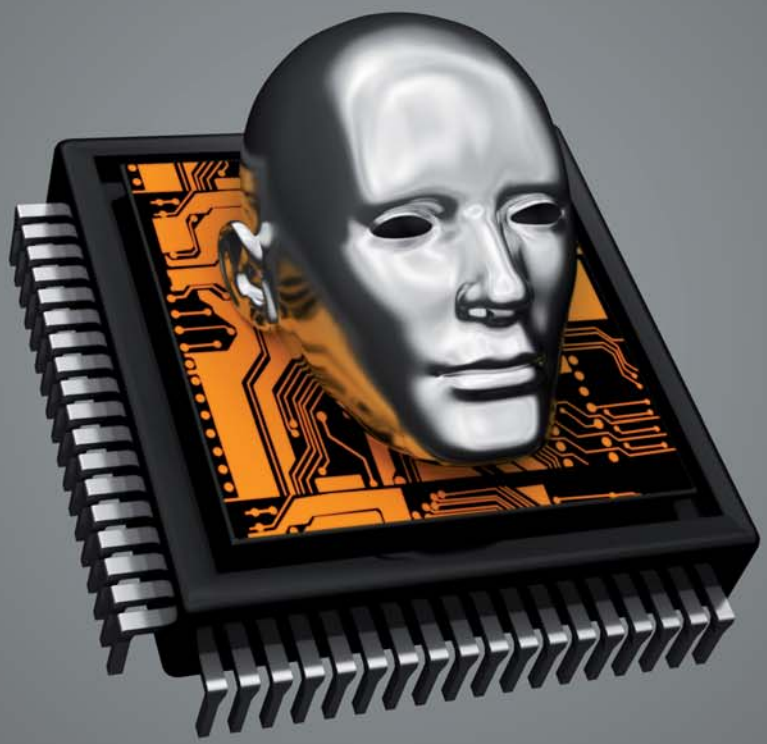
nedap

AEOS

W celu uzyskania bliższych informacji, proszę skontaktować się z działem Nedap Security Management (Zarządzanie Bezpieczeństwem) +48 607 852 699, info@nedap-aeos.com lub odwiedzić naszą stronę internetową www.nedap-securitymanagement.com

Inteligentne kamery marki NOVUS

Patryk Gańko



W kontekście telewizji dozorowej coraz częściej używa się takich pojęć, jak zaawansowane funkcje analizy obrazu, funkcje inteligentne lub funkcje VCA (ang. *Video Content Analysis*). Do tej pory pojęcia te były zarezerwowane dla złożonych systemów cyfrowej obróbki i rejestracji obrazu. Realizacja odnoszących się do tych pojęć funkcji wymagała specjalistycznych algorytmów i wysokowydajnych komputerów, których zasoby procesora i pamięci wykorzystywano do powyższej analizy. Równolegle, w miarę rozwoju i postępującej specjalizacji procesorów DSP, funkcje te zaczęto implementować bezpośrednio w kamerach. Pozwoliło to na upowszechnienie technologii VCA również w niedużych systemach nadzoru wizyjnego oraz łatwą integrację z systemami rejestracji i interakcji z użytkownikiem. Migracja funkcji inteligentnych na krańce sytemu umożliwiła stosowanie ich również w analogowych systemach monitoringu. W niniejszym artykule chciałbym skupić Państwa uwagę na zawansowanych funkcjach analizy i przetwarzania obrazu w analogowych kamerach serii InGenius marki NOVUS

Kamery serii InGenius są klasycznymi kamerami dzień/noc z mechanicznym filtrem podczerwieni i wysoką czułością 0,04 lx/F = 1,2 w trybie monochromatycznym. W warunkach słabego oświetlenia mogą pracować również w trybie wydłużonej migawki (DSS). W trybie kolorowym generowany obraz ma rozdzielczość do 650 linii, natomiast w trybie monochromatycznym – do 700 linii telewizyjnych. Pracującą w trybie dzień/noc kamerą można sterować zewnętrznie, za pomocą wyprowadzonych zacisków na panelu tylnym. Ponadto kamera może wysterować sprzężone z nią promienniki podczerwieni. Kamery InGenius posiadają rozbudowane menu ekranowe, dostępne dzięki przyciskom na panelu tylnym lub zdalnie (standard RS485) – z wykorzystaniem protokołów Novus-C1 oraz Pelco-D i P. Ta druga możliwość jest szczególnie wartościowa dla instalatorów systemów ze względu na złożoność wielu funkcji i ewentualnie ze względu na konieczność korekcji ustawień w trakcie eksploatacji.

Fot. 1. Kamera serii InGenius

Fot. 2. Detekcja ruchu z funkcją zoomu cyfrowego

Strefy prywatności

W obserwowanej scenie można zdefiniować do 15 stref maskowania, tzn. wykluczenia z monitoringu obszarów wrażliwych (np. okien mieszkań prywatnych). Wielkość wszystkich stref może być regulowana. Regulacja ta dotyczy nie tylko długości boków czworokąta, ale również pochylenia tych boków. Tym samym pozwala na bardziej precyzyjne maskowanie stref nieregularnych lub widzianych w perspektywie. Można przyporządkować wybrany kolor maskowanym strefom lub zmniejszyć rozdzielczość danej strefy (pikselizacja). Ponadto maskowane strefy mogą zostać wykluczone z analizy automatyki ekspozycji, zwłaszcza jeśli znacznie różnią się poziomem oświetlenia od pozostałych obszarów.

Detekcja ruchu z funkcją zoomu cyfrowego

W kamerze można zaprogramować do czterech stref detekcji ruchu oraz jedną strefę obejmującą cały ekran. Czułość może być dopasowana do warunków pracy. Uruchomienie funkcji detekcji ruchu powoduje wyświetlenie na ekranie komunikatu *MOTION* oraz aktywację wyjścia alarmowego, które może uruchamiać zewnętrzne sygnalizatory akustyczne i świetlne. Aktywna strefa detekcji może być powiązana z działaniem funkcji zoomu cyfrowego, która automatycznie wykona zbliżenie na tę strefę.

Wykrywanie twarzy

Funkcja ta potrafi wykryć twarz człowieka w obserwowanej scenie i następnie śledzić jej przemieszczanie się. Wykrycie twarzy powoduje aktywację wyjścia alarmowego. Funkcja może być przydatna np. w monitoringu zautomatyzowanych linii produkcyjnych, gdzie tradycyjna detekcja ruchu jest bezużyteczna, a sytuacją nadzwyczajną – wymagającą szczególnego nadzoru ze strony operatora – jest pojawienie się człowieka. Innym zastosowaniem może być monitorowanie wjazdów do garaży w celu zapobieżenia wtargnięciu intruzów. Możliwe jest ustawienie poziomu czułości oraz minimalnego rozmiaru twarzy, przy którym następuje aktywacja wyjścia alarmowego.

Wykrywanie zniknięcia obiektu

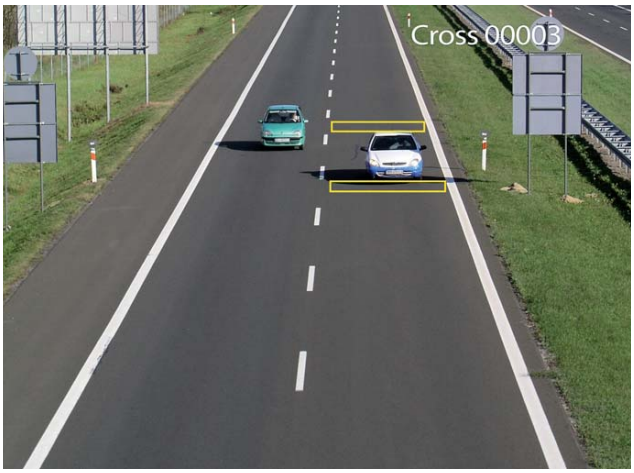
Funkcja wykrywania zmian w obserwowanej scenie, połączona z aktywacją wyjścia alarmowego, pozwala na wykrywanie braku jakiegoś elementu stanowiącego integralny element obrazu, np. brak eksponatu w muzeum.

Zliczanie obiektów wchodzących do pomieszczenia

Funkcja pozwala na zliczanie obiektów, które znalazły się w obszarze zdefiniowanej strefy. Aktualna liczba zarejestrowanych obiektów jest wyświetlana na ekranie, a przekroczenie określonej wartości powoduje aktywację wyjścia alarmowego.

Wykrywanie przekroczenia określonej strefy przez obiekt

Funkcja ta pozwala na zliczanie obiektów przechodzących przez strefy i określenie dozwolonego kierunku przemieszczania się. Jeśli przejście nastąpi zgodnie z kolejnością ustaloną w menu (np. ze strefy 1 do 2), zdarzenie zostanie zaliczone jako detekcja ruchu i dopisane do wewnętrznego licznika. Ruch w stronę przeciwną nie jest uwzględniany. Przekroczenie



Fot. 3. Wykrywanie przekroczenia określonej strefy przez obiekt

wartości uprzednio zdefiniowanej w menu kamery pozwala na aktywację wyjścia alarmowego. Funkcję można wykorzystać m.in. do blokowania szlabanu na parkingu po przejechaniu określonej liczby pojazdów.

Sabotaż kamery

Groźnym zjawiskiem w systemach monitoringu jest sabotaż kamery, czyli przesłonięcie lub zamalowanie obiektywu przez potencjalnych przestępców. Czyni to system całkowicie bezużytecznym na danym obszarze. Dlatego ważna jest natychmiastowa reakcja na tego typu zdarzenie. Kamery serii InGenius reagują na to poprzez aktywację wyjścia alarmowego. Dotyczy to również takich zdarzeń, jak nagła zmiana obserwowanej sceny, np. spowodowana obróceniem kamery lub utratą ostrości.

Fot. 4. Sabotaż kamery

Cyfrowa redukcja szumów (DNR)

Kamera została wyposażona w dwa typy filtrów redukcji szumów – 2D oraz nowej generacji 3D. Celem stosowania powyższej funkcji jest redukcja szumów w warunkach słabego oświetlenia i tym samym wygładzenie oglądanego obrazu. Zwiększa to komfort pracy operatora oraz przyczynia się do znacznej redukcji objętości pamięci dyskowej potrzebnej do zapisu strumienia. Ma to szczególne znaczenie w przypadku najbardziej rozpowszechnionych obecnie rejestratorów systemów kompresji międzyklatkowej – MPEG-4 i H.264. W porównaniu do poprzedniej generacji, filtry 3D pozwalają na redukcję szumów zwłaszcza w przypadku obiektów przemieszczających się. Działanie tej funkcji można łatwo zaobserwować, włączając w kamerze pozycję menu *DNR Demo*, która dzieli ekran na dwa obszary – z włączoną filtracją 3D i bez niej.

WDR, BLC, HLC

Kamera jest przystosowana do pracy w warunkach różnego poziomu oświetlenia obserwowanej sceny, m.in. w warunkach szczególnie trudnych, wymagających od kamery specyficznych funkcji adaptacji. W warunkach typowych, takich jak silne tylne oświetlenie słoneczne w przeszklonych pomieszczeniach, należy użyć funkcji BLC, pozwalającej uwypuklić obiekt znajdujący się na pierwszym planie w obrazie. Znacznie poprawiono parametry funkcji WDR (×512, 54 dB). Funkcja ta jest efektywniejsza niż funkcja BLC i HLC, ponieważ równoważy poziom jasności w całym obrazie, nie rozjaśniając przy tym nadmiernie tła względem obiektu centralnego. Dla scen z silnymi punktowymi źródłami światła, które mogą oślepiać kamerę, należy użyć funkcji HLC (*High Light Compensation*) powodującej maskowanie silnych źródeł światła i tym samym zmniejszanie średniego poziomu oświetlenia sceny. Funkcja ta jest bardzo przydatna w przypadku rozpoznawania tablic rejestracyjnych samochodów.

Kompensacja błędów pikseli matrycy CCD

Według europejskich norm w każdej kamerze pewna ilość pikseli w danym obszarze matrycy może ulec uszkodzeniu. Uszkodzenia te nie implikują uszkodzenia kamery, jako że wada samego piksela może być jedynie chwilowa (tzw. biały piksel). W uruchamianej przez operatora analizie obrazu procesor DSP potrafi wykryć i skompensować do 64 takich pikseli poprzez uśrednienie ich poziomu jasności do poziomu sąsiednich pikseli.

Profile użytkowników i hasła dostępu

Ze względu na złożoność menu istnieje możliwość zapisania do czterech konfiguracji menu. Znacznie ułatwia to testowanie działania wybranych funkcji w zależności od wybranych parametrów. Ponadto dostęp do menu może zostać zabezpieczony hasłem składającym się z czterech znaków alfanumerycznych.

Analiza obrazu będzie jednym z głównych kierunków rozwoju systemów telewizji dozorowej w najbliższym czasie. Tradycyjne systemy monitoringu, przy ciągle rosnącej liczbie kamer, wymagają dodatkowego wsparcia pracujących operatorów. Możliwość maszynowego wyszukiwania pewnych typów scen (np. bijatyk) znacznie poprawiłaby efektywność systemów monitoringu wizyjnego. Analiza obrazu jest procesem wymagającym dużych zasobów obliczeniowych, dlatego rozwój tego segmentu telewizji będzie wymagał specjalizowanych procesorów sygnałowych.

Powyższa charakterystyka kamer serii InGenius nie jest wyczerpująca i ograniczona została do omówienia unikalnych funkcji analizy obrazu, niedostępnych w tradycyjnych kamerach.

Patryk Gańko
AAT Holding

NOVUS®

Profesjonalne rozwiązanie dla systemów zabezpieczeń

Inteligentne kamery o wysoce zaawansowanych funkcjach analizy obrazu!

Wykrywanie twarzy

Funkcja potrafi wykryć twarz człowieka w obserwowanej scenie i następnie śledzić jej przemieszczanie, aktywując wyjście alarmowe. Ma zastosowanie wszędzie tam, gdzie standardowa detekcja ruchu nie zdaje egzaminu, np. może wykrywać pojawienie się ludzi w obszarze, gdzie ruch pieszych jest niepożądany, jednocześnie ignorując ruch innych obiektów (samochodów).

Wykrywanie zniknięcia obiektu

Funkcja wykrywa zmiany w obserwowanej scenie, stale porównując ją ze sceną referencyjną i aktywuje wyjście alarmowe. Pozwala na wykrycie braku jakiegoś elementu, stanowiącego integralną część obrazu, np. brak eksponatu w muzeum, ignorując jednocześnie krótkotrwałe zmiany w obrazie, np. ruch zwiedzających.

Zliczanie obiektów wchodzących do pomieszczenia

Funkcja pozwala na zliczanie obiektów, które znalazły się w obszarze zdefiniowanej strefy. Liczba zarejestrowanych obiektów jest wyświetlana na ekranie. Przekroczenie określonej wartości aktywuje wyjście alarmowe, na ekranie pojawia się stosowny komunikat, a licznik zostaje wyzerowany.

INGENIUS

- Dodatkowe funkcje analizy obrazu: detekcja ruchu, wykrywanie przekroczenia określonej strefy przez obiekt, wykrywanie utraty ostrości bądź próby sabotażu na kamerze, cyfrowa funkcja PTZ
- Mechaniczny filtr podczerwieni
- Rozdzielczość pozioma 650 TVL/700 TVL
- Czułość: od 0.001 lx/F=1.2 (DSS)
- HLC - funkcja redukująca efekt oślepiania kamery
- WDR - Szeroki zakres dynamiki
- DNR - Cyfrowa redukcja szumu
- 30x zoom cyfrowy, 15 stref prywatności
- 1 wyjście alarmowe
- Menu ekranowe
- Sterowanie RS-485 (Novus-C1, Pelco-D, Pelco-P)
- Funkcja kalibracji i kompensacji błędów pikseli matrycy CCD
- Zasilanie: 12 VDC/24 VAC, 230 VAC

AAT Holding sp. z o.o.
ul. Puławska 431, 02-801 Warszawa, tel. 22 546 05 46, faks 22 546 05 01
e-mail: aat.warszawa@aat.pl, www.aat.pl

Oświetlenie światłem podczerwonym

a wymagania dotyczące przepływności w sieci IP - studium przypadku

Bosch Security Systems

Chociaż oświetlenie w podczerwieni jest dojrzałą technologią, która niejednokrotnie udowodniła swoją przydatność w warunkach nocnych, jej użycie w obecnych systemach dozoru wizyjnego obejmuje zaskakującą sferę – zarządzanie przepustowością sieci. Dzięki możliwości zmniejszenia wymagań dotyczących przepływności sieci oświetlenie w podczerwieni może stać się przydatne do lepszego wykorzystania zasobów sieciowych w systemach dozoru wizyjnego. Oświetlenie w podczerwieni może istotnie zmniejszyć wymagania dotyczące przepustowości oraz przestrzeni dyskowej rejestratorów, co sprawia, że staje się czymś więcej niż tylko technologią usprawniającą działanie systemu w warunkach nocnych

Praktycznie wszystkie kamery CCTV – zarówno analogowe, jak i sieciowe – generują użyteczne obrazy dozorowe w dzień, w warunkach dobrego oświetlenia, jednakże dzisiejsze systemy bezpieczeństwa wymagają pracy 24 godziny na dobę przez 7 dni w tygodniu, a to właśnie możliwość pracy w nocy determinuje całkowitą efektywność systemu. W nocy zdarza się większość włamań, kradzieży, napadów oraz ogólnie definiowanych prób wykorzystania słabości systemów dozorowych. Przetworniki CCD i CMOS, stanowiące kluczowy element każdej kamery CCTV, zgodnie ze swoją zasadą działania są zaprojektowane do reagowania na światło i tworzenia w ten sposób użytecznych obrazów. Jeśli nie ma światła, nie może być mowy o jakimkolwiek użytecznym i czytelnym obrazie.

Wiele dostępnych obecnie kamer dysponuje bardzo wysoką czułością, często dochodzącą do 0,1 luksa. Ich dane techniczne sugerują efektywne działanie w warunkach słabego oświetlenia, jednak w branży bezpieczeństwa panuje, skądinąd słuszne, powszechne przekonanie, że złe warunki oświetleniowe przyczyniają się w rezultacie do wytwarzania obrazów o słabej jakości i o wysokim poziomie szumów.

Wraz ze spadkiem poziomu oświetlenia rośnie zapotrzebowanie na przepustowość (przepustowość – albo przepływność – określa, ile bitów danych można przesłać w ciągu sekundy przez dostępną sieć teleinformatyczną, np. Ethernet). Zasadniczo obrazy powstające w dzień wymagają mniejszej przepustowości niż obrazy powstające w nocy – przy założeniu, że pozostałe czynniki (na przykład ruchliwość sceny czy stopień kompresji) są takie same.

Aby zrozumieć nieuchronny wzrost zapotrzebowania na przepływność przy złym oświetleniu, weźmy pod uwagę działanie funkcji automatycznej regulacji wzmocnienia (ARW) w kamerze, która zwiększa wzmocnienie toru wizyjnego w złych warunkach oświetleniowych. Wynikiem wzrostu wzmocnienia jest wzrost zarówno poziomu sygnału wizyjnego, jak i poziomu szumów. Kiedy scena jest słabiej oświetlona, funkcja ARW powoduje wzrost wzmocnienia i zwiększa się poziom szumów w obrazie. Gdy oświetlenie sceny nadal maleje, funkcja ARW jeszcze bardziej zwiększa wzmocnienie, co powoduje dalszy wzrost poziomu szumów. W końcu obraz powstający w kamerze w nocy staje się zaśnieżony oraz ziarnisty. W tych warunkach – nawet w przypadku nieruchomych obrazów – wymagana przepływność sieci może być wiele razy większa niż w dzień.

Co wspólnego mają szumy w obrazie wytwarzanym przez kamerę ze zwiększeniem przepływności łącza sieciowego kamery? Otóż wspólnym elementem łączącym te dwa zjawiska jest zastosowana kompresja. Przy założeniu, że bierzemy pod uwagę stratne algorytmy kompresji obrazu, niezależnie od wyboru konkretnego rozwiązania (M-JPEG, MPEG-4 czy H.264), podstawową zasadą kompresji jest eliminacja nadmiernej ilości danych w celu zmniejszenia rozmiarów plików. Każda kompresja wymaga kompromisu pomiędzy jakością obrazu a rozmiarami uzyskiwanych plików. Wyższy (bardziej stratny) stopień kompresji pozwala w rezultacie na zmniejszenie rozmiarów plików i jednocześnie powoduje pogorszenie jakości obrazu. Mniejszy (mniej stratny) stopień kompresji daje obraz o wyższej jakości, jednak rozmiary plików są większe. Najbardziej popularne, wyżej wymienione algorytmy stosują jeden z dwóch rodzajów redukcji:

– redukcję nieistotnych elementów – usuwającą części sygnału wizyjnego niedostrzegalne dla ludzkiego oka, takie jak nieznaczne zmiany kolorów,
– redukcję nadmiarowości – usuwającą powielone informacje (zarówno z tej samej ramki obrazu, jak i pomiędzy ramkami), takie jak duże, jednolite obszary o jednakowej barwie lub obiekty nieruchome.

Efekt słabszego oświetlenia dostępnego w scenie, a co za tym idzie zwiększonej aktywności funkcji ARW, zakłóca pracę algorytmów kompresji stosowanych w nowoczesnych kamerach sieciowych (IP). Algorytmy kompresji interpretują powodowane przez działanie funkcji ARW zaśnieżenie oraz ziarnistość obrazów jako przydatne informacje (takie jak detale obrazu lub ruch), które nie mogą być potraktowane jako elementy nieistotne lub nadmiarowe. Koder kamery działa więc tak, jak gdyby w scenie pojawiło się więcej ruchu, co w konsekwencji powoduje, że obrazy przesyłane z kamery obserwującej scenę słabiej oświetloną są mniej skompresowane, czyli mają większe rozmiary. Istnieje zatem bezpośredni związek pomiędzy pracą nocną, kompresją i wielkością generowanego strumienia danych.

Pozornie najbardziej oczywistym rozwiązaniem jest wyłączenie funkcji ARW. Rzeczywiście spowodowałoby ono zmniejszenie przepływności, jednak odbyłoby się to kosztem rozróżnialności szczegółów obrazu. Skutkiem byłyby bardzo słabe, jeśli nie bezużyteczne obrazy. Niewątpliwie możliwość pracy systemu dozoru wizyjnego w nocy ma istotne znaczenie dla efektywności zastosowanych zabezpieczeń.

Najlepszym rozwiązaniem do zapewnienia efektywnej pracy sieciowych systemów dozorowych w nocy jest oświetlenie obserwowanej sceny. I tutaj do wyboru mamy dwie drogi. Możemy skorzystać z oświetlenia widzialnym światłem sztucznym (np. halogenowym lub żarowym) albo oświetlenia światłem o długości fali mieszczącej się w zakresie podczerwieni – częściowo lub całkowicie niewidocznym.

Sztuczne oświetlenie w zakresie widzialnym w nocy można chwilowo pominąć ze względu na kilka niekorzystnych z punktu widzenia profesjonalnego systemu monitoringu parametrów (np. zniekształcanie kolorów, krótki zasięg oświetlenia, widoczność promieniowania, czyli również informowanie potencjalnych intruzów o zasięgu widzenia naszych kamer, niska sprawność energetyczna, niższa trwałość i jednolitość źródła światła, brak dokładnego oświetlenia poszczególnych planów czy efekt zanieczyszczenia otoczenia światłem widzialnym). Zajmiemy się oświetleniem w podczerwieni.

Warunkiem wytworzenia pełnowartościowego obrazu w porze nocnej jest właściwy dobór takich elementów, jak kamera, obiektyw i źródło światła. Oczywiście kamera powinna być kamerą dzienno-nocną z mechanicznie usuwanym filtrem podczerwieni i obiektywem przystosowanym do pracy w zakresie podczerwieni, gwarantującą wyraźne, niezaszumione i ostre obrazy przy oświetleniu z wykorzystaniem

podczerwieni. W tych warunkach funkcja ARW staje się zbędna, a kompresja działa stabilnie i wydajnie.

W większości zastosowań częstotliwość odświeżania oraz rozdzielczość są zwykle modyfikowane w celu dostosowania systemu do wymagań użytkowych. Na przykład, jeśli przepustowość sieci lub dostępna przestrzeń dyskowa jest niewystarczająca, powszechną strategią jest redukcja częstotliwości odświeżania, rozdzielczości lub obu tych wielkości. Jednakże takie podejście ma swoje wady. Ograniczenie częstotliwości odświeżania oraz rozdzielczości skutkuje „rwanym" obrazem o słabej jakości, przez co mogą zostać pominięte krytyczne momenty występujące w obserwowanej scenie. Ponadto obniżenie częstotliwości odświeżania i rozdzielczości często uniemożliwia prawidłowe działanie oprogramowania do analizy obrazu. W przypadku projektów mających krytyczne znaczenie dla bezpieczeństwa chronionych obszarów lepszą strategią jest zwiększenie dostępnej przestrzeni dyskowej oraz przepustowości sieci, pozwalające na utrzymanie integralności obrazu.

Zastosowanie aktywnego oświetlenia z wykorzystaniem podczerwieni umożliwia zamianę zaszumionych obrazów na obrazy nocne o znakomitej jakości dzięki emisji „niewidocznego" światła, które kamera może zobaczyć. Funkcja ARW nie jest włączana, a wymagana przepustowość sieci pozostaje taka sama, jak w przypadku pracy w dzień.

Nasze testy miały na celu potwierdzenie oraz ilościowe zobrazowanie wpływu użycia oświetlenia w podczerwieni na wielkość generowanego strumienia danych.

Czym i jak testowaliśmy

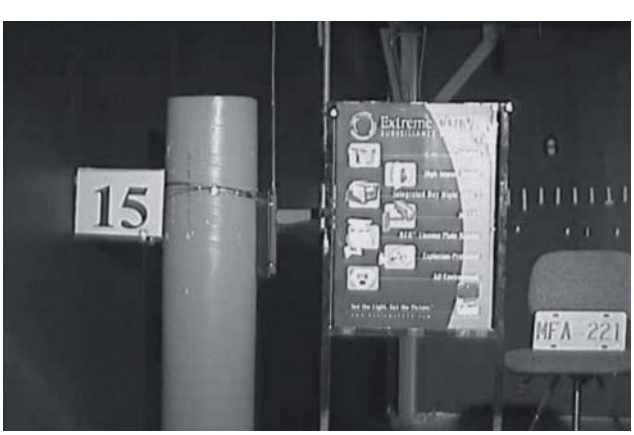
Sprzęt wykorzystany do testów to:

1) Kamera Dinion XF, dzienno-nocna z przetwornikiem o przekątnej 1/3 cala i z 15-bitową, cyfrową obróbką analogowego sygnału wizyjnego. Dlaczego wykorzystaliśmy właśnie tę kamerę? Kamera Dinion XF charakteryzuje się:
   – wysoką dynamiką XF-Dynamic, która gwarantuje znakomitą wierność i optymalne wyświetlanie szczegółów obrazu zarówno w silnie, jak i słabo oświetlonych obszarach sceny;
   – elektroniczną migawką, czyli systemem automatycznej optymalizacji parametrów kamery przy zmianach natężenia światła padającego na przetwornik z obserwowanej sceny – funkcja niezwykle istotna w przypadku potrzeby rejestracji scen przy obniżonym oświetleniu;
   – kompensacją tła – dzięki możliwości pełnego, programowego określenia obszaru działania funkcji kompensacji oświetlenia tła oraz regulowanemu poziomowi kompensacji (konfiguracja kamery może być łatwo dostosowana do pracy nawet w najbardziej wymagających zastosowaniach, takich jak monitoring bram wjazdowych dla podjazdów, czyli wszędzie tam, gdzie w jednej scenie obecne jest równocześnie bardzo silne i bardzo słabe światło);
   – mechanicznie odsuwanym filtrem podczerwieni z wbudowanym inteligentnym czujnikiem światła, który zapobiega przełączaniu kamery w tryb

Fot. 1. Obraz z próby nr 3

Fot. 2. Obraz z próby nr 4

Fot. 3. Obraz z próby nr 11



Fot. 4. Obraz z próby nr 12

kolorowy w przypadku dominującego oświetlenia w zakresie podczerwieni.

2) Obiektyw 2,8–12 mm z korekcją pozwalającą na pracę w zakresie podczerwieni.
3) Oświetlacz podczerwieni AEGIS UFLED (850 nm, kąt świecenia: 60 stopni). Dlaczego wykorzystaliśmy ten oświetlacz? Oświetlacz AEGIS UFLED charakteryzuje się:
   – równomiernym doświetleniem sceny;
   – eliminacją prześwietlenia pierwszego planu i niedoświetlenia tła;
   – funkcją utrzymującą stały poziom natężenia podczerwieni przez cały okres eksploatacji promiennika, pomimo zmienności temperatury otoczenia; dzięki powierzchniowemu montażowi diod ich chłodzenie jest znacznie skuteczniejsze, co powoduje obniżenie temperatury pracy i poprawę parametrów optycznych, a także bezpośrednio wpływa na żywotność oświetlacza.
4) Koder analogowego sygnału wizyjnego na postać IP typu VideoJet X10 z kompresją MPEG-4. Wybraliśmy go ze względu na:
   – jakość i szybkość kodowania,
   – możliwość obciążenia dużym strumieniem danych,
   – obsługę wielostrumieniowości,
   – możliwość elastycznego zarządzania jakością, osobno dla każdego ze strumieni.
5) Profesjonalny luksometr o zakresie pomiarowym od 0,01 do 20 luksów.

Scena, którą wykorzystano do testów przepływności przy różnych poziomach oświetlenia, jest pokazana na fotografiach. Pierwszy plan (słup z lewej strony) znajduje się około pięciu metrów od kamery, najdalszy plan (tło) znajduje się około ośmiu metrów od kamery. W połowie odległości między tymi planami znajduje się tablica informacyjna i krzesło z umieszczoną na nim tablicą rejestracyjną.

Test składał się z dwunastu prób realizowanych przy sześciu różnych poziomach oświetlenia otoczenia, z włączonym i wyłączonym oświetlaczem podczerwieni – na zmianę. Mierzona była przepływność strumienia wizyjnego w obydwu przypadkach. Jakość reprodukowanego obrazu i poziom szumów widocznych na obrazach zostały pokazane na fotografiach.

Wyniki

Tabela 1 prezentuje wyniki z przeprowadzonych pomiarów.

Wnioski

Pozwalając na porównanie wyników uzyskanych podczas obserwacji scen o niskim poziomie oświetlenia światłem widzialnym (1,1 luksa) z wynikami uzyskanymi podczas obserwacji tych samych scen oświetlonych dodatkowo światłem podczerwonym, nasze testy uwidoczniły redukcję wielkości generowanego strumienia danych o 48%, a nawet o 91%, zależnie od warunków. Zmienność wielkości redukcji można przypisać głównie różnicom w poziomie oświetlenia naturalnego. Wyniki pokazują mniejsze poziomy redukcji przepływności, gdy oświetlenie naturalne staje się

Próba	Oświetlenie otoczenia w świetle widzialnym [lx]	Oświetlenie w podczerwieni	Przepływność [Mb/s]	Redukcja przepływności
1	0,04	wyłączone	13,37	91%
2	0,04	włączone	1,21	
3	0,08	wyłączone	13,43	91%
4	0,08	włączone	1,21	
5	0,14	wyłączone	13,12	91%
6	0,14	włączone	1,21	
7	0,62	wyłączone	8,80	86%
8	0,62	włączone	1,21	
9	0,99	wyłączone	7,03	83%
10	0,99	włączone	1,21	
11	1,04	wyłączone	5,27	77%
12	1,04	włączone	1,20	

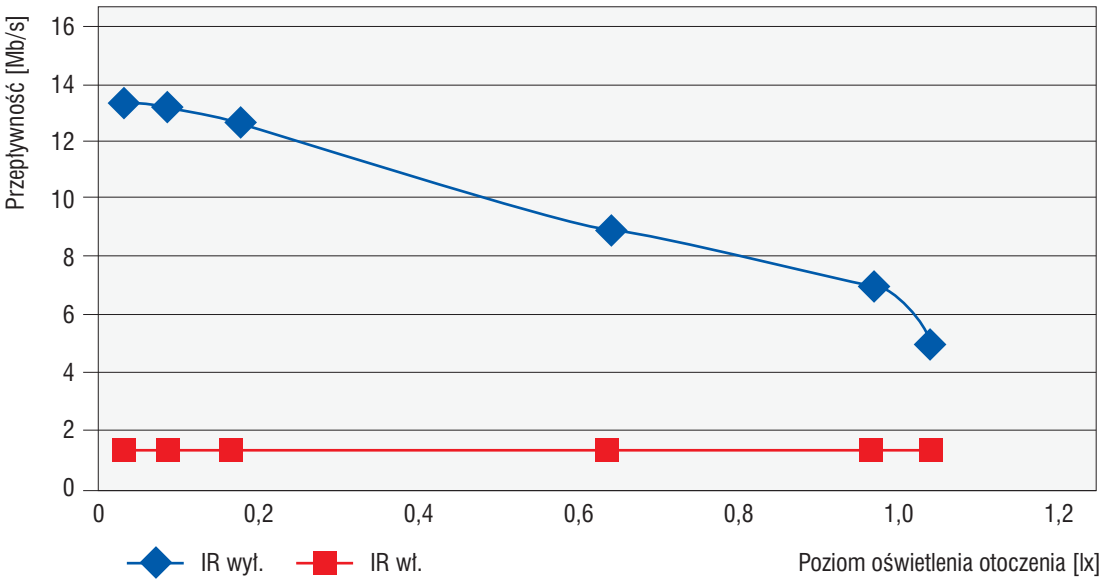
Tab. 1. Wyniki uzyskane w poszczególnych próbach

Próba 3: oświetlenie światłem podczerwonym wyłączone, oświetlenie otoczenia 0,08 lx, przepływność 13,43 Mb/s

Próba 4: oświetlenie światłem podczerwonym włączone, przepływność 1,21 Mb/s, zmniejszenie przepływności o 91%

Próba 11: oświetlenie światłem podczerwonym wyłączone, oświetlenie otoczenia 1,04 lx, przepływność 5,27 Mb/s

Próba 12: oświetlenie światłem podczerwonym włączone, przepływność 1,20 Mb/s, zmniejszenie przepływności o 77%



Wykres 1. Podsumowanie wyników pomiarów

Jaka jest zależność pomiędzy przepustowością a przestrzenią dyskową?

Przepustowość (czy też pasmo przepustowości) i przestrzeń dyskowa, jeden z najbardziej kosztownych elementów systemu dozoru wizyjnego, są bezpośrednio powiązane. Jeśli obraz przeznaczony do zapisu jest przesyłany poprzez sieć z określoną przepływnością, będzie zużywać przestrzeń dyskową z dokładnie tą samą prędkością. Na przykład strumień wizyjny o przepływności 1 Mb/s będzie zużywać 1 megabit przestrzeni dyskowej na sekundę lub około 1/8 = 0,125 MB na sekundę, co odpowiada 0,125 × 3600 = 450 MB na godzinę (czyli około 11 GB dziennie lub około 75 GB tygodniowo).

jaśniejsze, powodując, że oświetlenie w podczerwieni jest mniej istotne dla wielkości strumienia powstałego na skutek kodowania sygnału wizyjnego. Wyniki uzyskane w naszych testach jasno dowodzą, że oświetlenie w podczerwieni jest sposobem obniżenia przepływności w złych warunkach oświetleniowych.

Mówiąc najprościej, promieniowanie w zakresie podczerwieni jest rodzajem światła, tyle że niewidzialnego dla ludzkich oczu, które reagują tak, jak w ciemności. Promieniowanie podczerwone jest formą światła, które nowoczesne kamery wykorzystują do tworzenia obrazów. Oświetlenie w podczerwieni zapobiega tworzeniu się szumów w obrazie, powodując przerwanie łańcucha zdarzeń prowadzących do wzrostu zapotrzebowania na przepływność. Jak pokazują nasze testy, obrazy o niskim poziomie szumów (lub obrazy, które uznalibyśmy za obrazy o wysokiej jakości) wymagają znacznie mniejszej przepustowości niż obrazy zaszumione (o niskiej jakości).

Projektowanie systemów sieciowych zawsze rozpoczyna się od doboru kamer lub obiektywów, który będzie miał wpływ na działanie każdego systemu. Chociaż rynek zmierza w kierunku platform cyfrowych, zasady tworzenia dobrych obrazów pozostają niezmienne i w rzeczywistości, podczas tworzenia systemów CCTV, właśnie te zasady powinny być najważniejsze.

Co prawda przeprowadzone badania skoncentrowały się na zagadnieniach związanych z przepływnością sieci, ale użycie oświetlenia w podczerwieni ma równie istotny wpływ na przestrzeń dyskową. Pomiędzy przepływnością i przestrzenią dyskową istnieje bezpośrednia zależność, dlatego można wywnioskować, że zastosowanie oświetlenia w podczerwieni może być efektywną strategią mającą na celu redukcję zapotrzebowania na przestrzeń dyskową w sieciowych systemach dozoru wizyjnego. To zagadnienie jest szczególnie ważne, gdyż przestrzeń dyskowa stanowi jeden z najbardziej kosztownych elementów systemu CCTV.

Podsumowanie

Sieciowy dozór wizyjny napotyka na problemy związane z jakością obrazu oraz zarządzaniem przepustowością w trudnych warunkach zewnętrznych. Zbadany wpływ oświetlenia w podczerwieni na przepływność w sieci IP miał na celu udowodnienie (z wykorzystaniem danych liczbowych) korzyści wynikających z zastosowania oświetlenia w podczerwieni w sieciowym systemie dozoru wizyjnego. Testy wykazały, że w złych warunkach oświetleniowych oświetlenie w podczerwieni znacznie zmniejszyło wielkość generowanego strumienia danych w zakresie od 70% do 91% (czyli zmniejszyło obciążenie sieci). Wyniki potwierdzają, że oświetlenie w podczerwieni może umożliwić poprawę wykorzystania przepływności sieci przez minimalizowanie efektu wytwarzania dużych strumieni danych podczas kodowania analogowych sygnałów wizyjnych o dużym poziomie szumów. Zmniejszenie strumienia danych przekłada się na redukcję wymaganej wielkości pamięci masowej, co z kolei umożliwia istotną redukcję kosztów uruchomienia oraz utrzymania systemu CCTV IP.

Bosch Security Systems

Sugerowana cena detaliczna netto od 1600 PLN

Optymalna czwórka

Nowy 4-kanałowy rejestrator wizyjny firmy Bosch

Szukasz ekonomicznego i łatwego w instalacji rozwiązania do małych i średnich obiektów?

Dla systemów obejmujących do 4 kamer stworzyliśmy nowy rejestrator wizyjny serii 400. Dzięki niemu zyskasz gwarancję jakości w niespotykanej dotąd cenie. Rodzina rejestratorów serii 400 obejmuje modele: DVR-430-04A050 i DVR-451-04A050

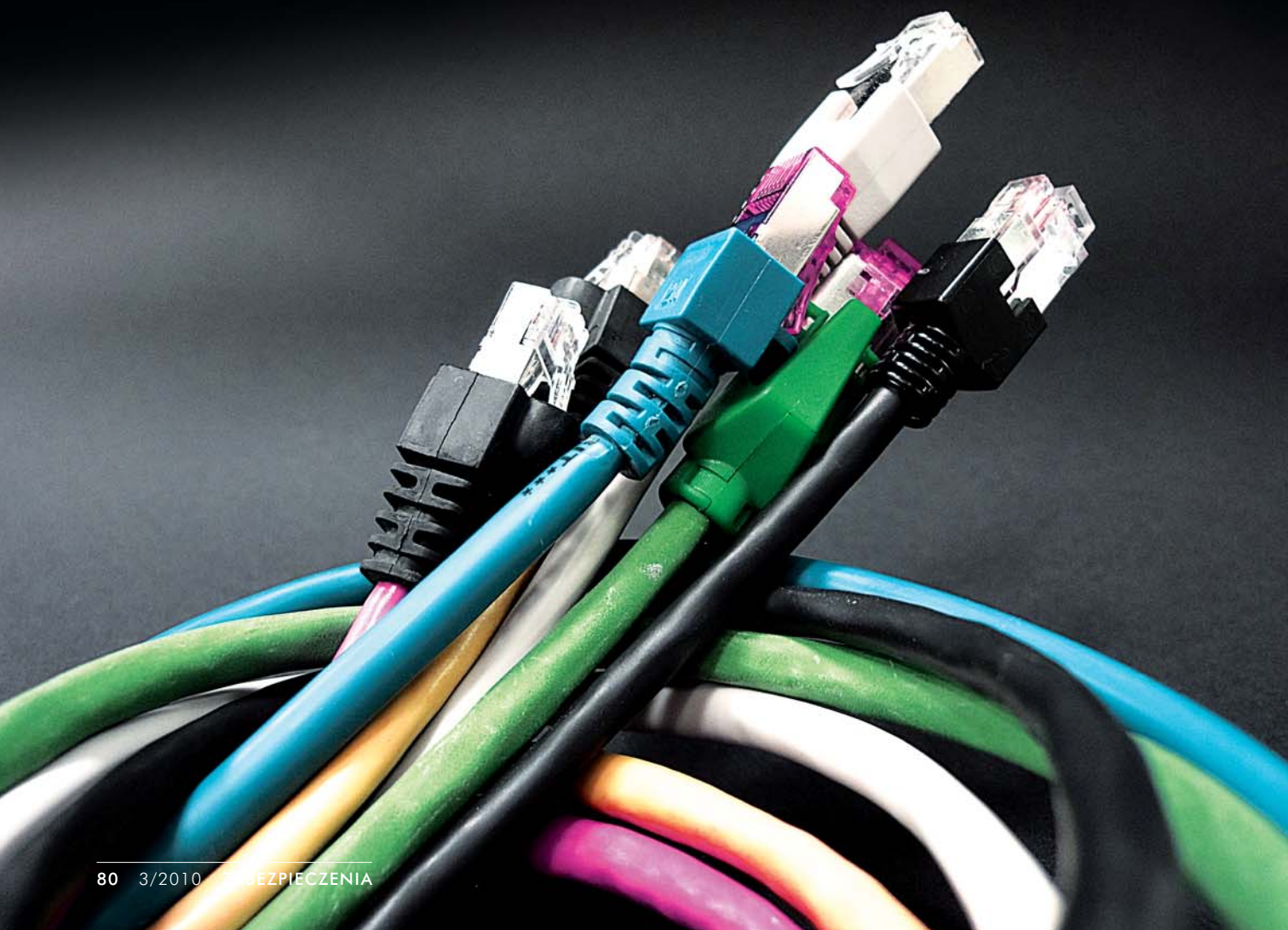
BOSCH
Technologia bliżej nas

Szczegółowe informacje na temat produktów firmy Bosch znajdą Państwo na stronie **www.boschsecurity.pl**

Systemowe rozwiązania w sieciach monitoringu oparte na urządzeniach Dedicated Micros

Karol Fietkiewicz

Dążenie do zapewnienia coraz większego poziomu bezpieczeństwa powoduje, że znaczenie systemów monitoringu ciągle rośnie. Przybywa w nich kamer, rejestratorów, wreszcie – monitorów w centrum obsługi. W rozbudowanych systemach naturalne i praktyczne staje się łączenie poszczególnych ich elementów w bardziej rozległą sieć z jedną lub kilkoma stacjami monitorującymi. Jeżeli mamy na uwadze monitoring przestrzeni publicznej, dróg, ulic, środków komunikacji itp., koniecznością staje się również integracja części CCTV z systemami wykorzystywanymi przez służby publiczne, w szczególności przez policję, straż miejską lub straż pożarną



Wyobraźmy sobie prostą stację monitoringu, w której z biegiem czasu dochodzi do konieczności zwiększenia liczby obsługiwanych rejestratorów i kamer. Zwiększenie liczby kamer wymaga powiększenia liczby monitorów w stacji w celu zapewnienia choćby minimalnego komfortu pracy osobie nadzorującej. Aby przełączać obrazy z kamer, instalowane są kolejne krosownice. System taki szybko przestaje być elastyczny, komplikuje się, a jakakolwiek zmiana jego konfiguracji czy awaria powoduje długotrwałe wyłączenie z eksploatacji. Jeśli stacji monitoringu jest więcej, często istnieje wymóg, aby w różnych z nich można było obserwować obrazy z tych samych kamer i zarządzać tymi samymi kamerami obrotowymi. Do tego dołóżmy konieczność zarządzania systemem za pomocą map synoptycznych i możliwość łączności dźwiękowej pomiędzy operatorem a obsługiwanym obiektem (np. nadanie komunikatu głosowego).

Budowa takich rozległych systemów w technologii analogowej nie jest możliwa. Jedynym sensownym wyjściem zapewniającym dostateczną elastyczność jest skorzystanie z zalet sieci IP.

Idealnymi produktami służącymi do tworzenia takich sieci są urządzenia firmy Dedicated Micros z serii NetVu Connected, do której należy cała gama urządzeń – rejestratory analogowe, rejestratory hybrydowe, kodery i wielowyjściowe dekodery obrazu (m.in. z wyjściami HD), konsole NetVuConsole, cyfrowe krosownice obrazu Pick-a-Point służące do zarządzania systemami.

O jednym z bardziej zaawansowanych rejestratorów Dedicated Micros, DV-IP RT, pisaliśmy w lutowym numerze *Zabezpieczeń*. Urządzenie to może zapisywać obrazy z prędkością dochodzącą do 25 klatek na sekundę w pełnej rozdzielczości 4CIF. Wspiera również obsługę i rejestrację kamer megapikselowych. Szesnaście wejść i dwa wyjścia foniczne umożliwiają nagrywanie dźwięku z każdego kanału oraz dźwiękową komunikację operatora z osobami znajdującymi się w monitorowanym obiekcie. Technologia MultiMode, wraz z możliwością podłączenia zewnętrznych macierzy e-SATA, pozwala na zapis obrazu o wysokiej jakości z zastosowaniem kodowania MPEG4 lub MJPEG, jednocześnie zapewniając bardzo długi okres zapisu. Podobne możliwości ma ośmiowejściowy rejestrator DV-IP HD, zawierający dwa wyjścia HDMI pracujące jako wyjścia główne i pomocnicze. Nieco mniejszą prędkością zapisu dysponują urządzenia DV-IP Server i DV-IP Express. To ostatnie obsługuje tylko kamery analogowe.

Osobną grupą urządzeń są kodery IP, służące do zamiany sygnału wizyjnego z kamery analogowej na strumień danych, oraz dekodery IP, służące do zamiany strumienia danych z sieci IP na postać sygnału wizyjnego. Szczególnie interesujący pod tym względem jest dekoder HDMI DV-IP, wyposażony w osiem analogowych wyjść wizyjnych oraz dwa wyjścia HDMI. Dzięki nim urządzenie jest w stanie dekodować 64 strumienie danych, z czego 32 strumienie mogą reprezentować obrazy o rozdzielczości HD. Dwa dwukierunkowe kanały foniczne pozwolą usłyszeć, co dzieje się w monitorowanym obiekcie, i w razie potrzeby nadać odpowiedni komunikat głosowy. Urządzenie jest wyposażone w port Gigabit Ethernet. Istnieje również wersja dekodera bez wyjść HDMI. Dostępne są także małe, jednokanałowe kodery/dekodery DC-IP-CODEC, mogące zamienić sygnał wizyjny z tradycyjnej kamery analogowej na postać cyfrową lub zdekodować przechwycony strumień danych na postać analogową. O ile zachodzi taka potrzeba, służą one również jako moduł transmisyjny dla pulpitu NetVuConsole.

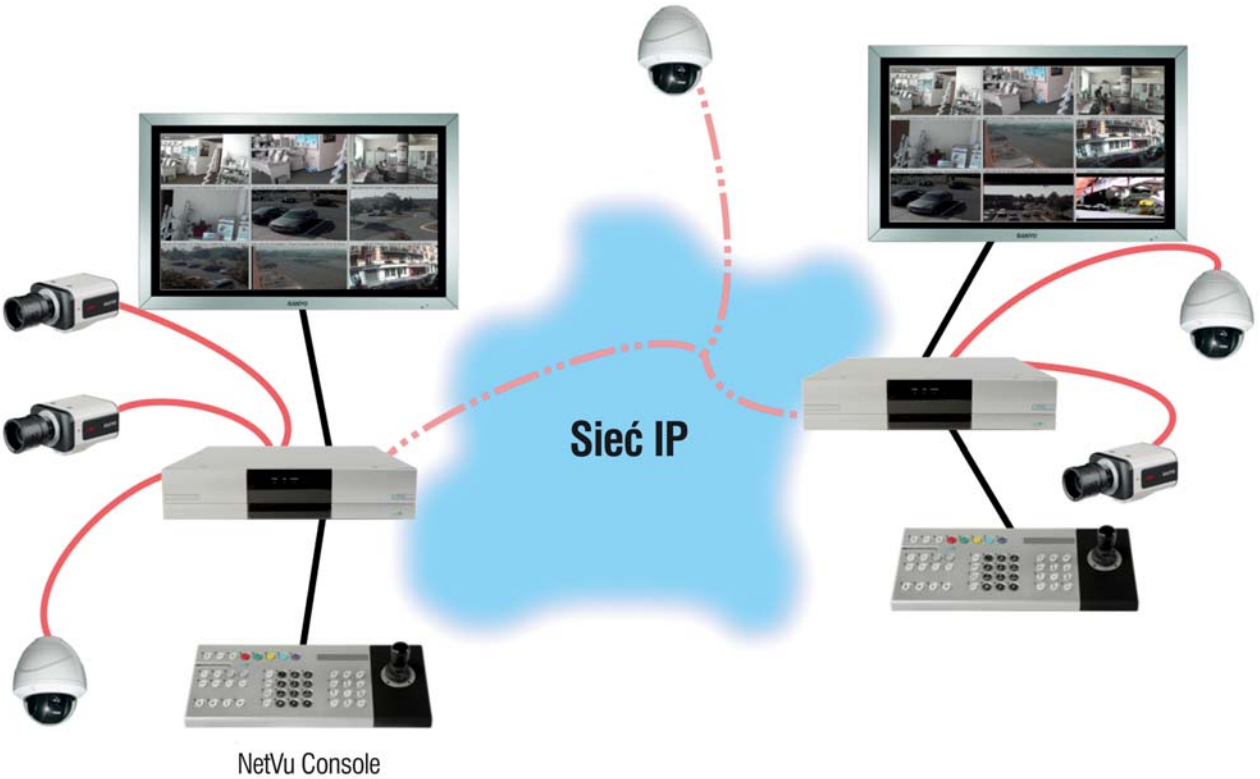
W przypadku wykorzystywania pojedynczego rejestratora nie istnieje problem dostępu do niego z odległych miejsc – wystarczy jeden pulpit sterowniczy, taki jak KBC1 lub KBC2, wyposażony w manipulator. System komplikuje się, jeżeli rejestratorów jest więcej i są one obsługiwane przez wielu operatorów, którzy przebywają w różnych lokalizacjach (na przykład w poszczególnych punktach dozorowych w centrum handlowym) i potrzebują zarządzać wspólnym systemem.

W takiej sytuacji jednym z rozwiązań jest zastosowanie NetVu Console. Jest to specjalny protokół współpracujący z klawiaturami KBC, wbudowany we wszystkie nowoczesne urządzenia Dedicated Micros, dzięki któremu na monitorze podłączonym do dowolnego urządzenia należącego do sieci jesteśmy w stanie wyświetlić i zarządzać obrazem z dowolnej kamery, z dowolnego rejestratora w systemie, włączając w to odtwarzanie, wyszukiwanie, sterowanie kamerą obrotową, czy podziały ekranu. Dzięki temu nie zachodzi potrzeba budowania specjalnych stanowisk kontrolnych, wyposażonych w komputery z oprogramowaniem typu CMS. Każdy z rejestratorów, wyposażonych w klawiaturę KBC, może stać się równoprawnym ośrodkiem zarządzającym naszym systemem. Dużym ułatwieniem w obsłudze systemu jest wyposażenie rejestratorów w mapy synoptyczne (e-mapy), pozwalające na szybki dostęp do obrazu z konkretnej kamery poprzez wybranie ikony znajdującej się na symbolicznej mapie przedstawiającej nasz obiekt. Nie trzeba wówczas pamiętać, która kamera „patrzy" w konkretne miejsce obiektu (jaki ma numer, do którego z rejestratorów jest podłączona).

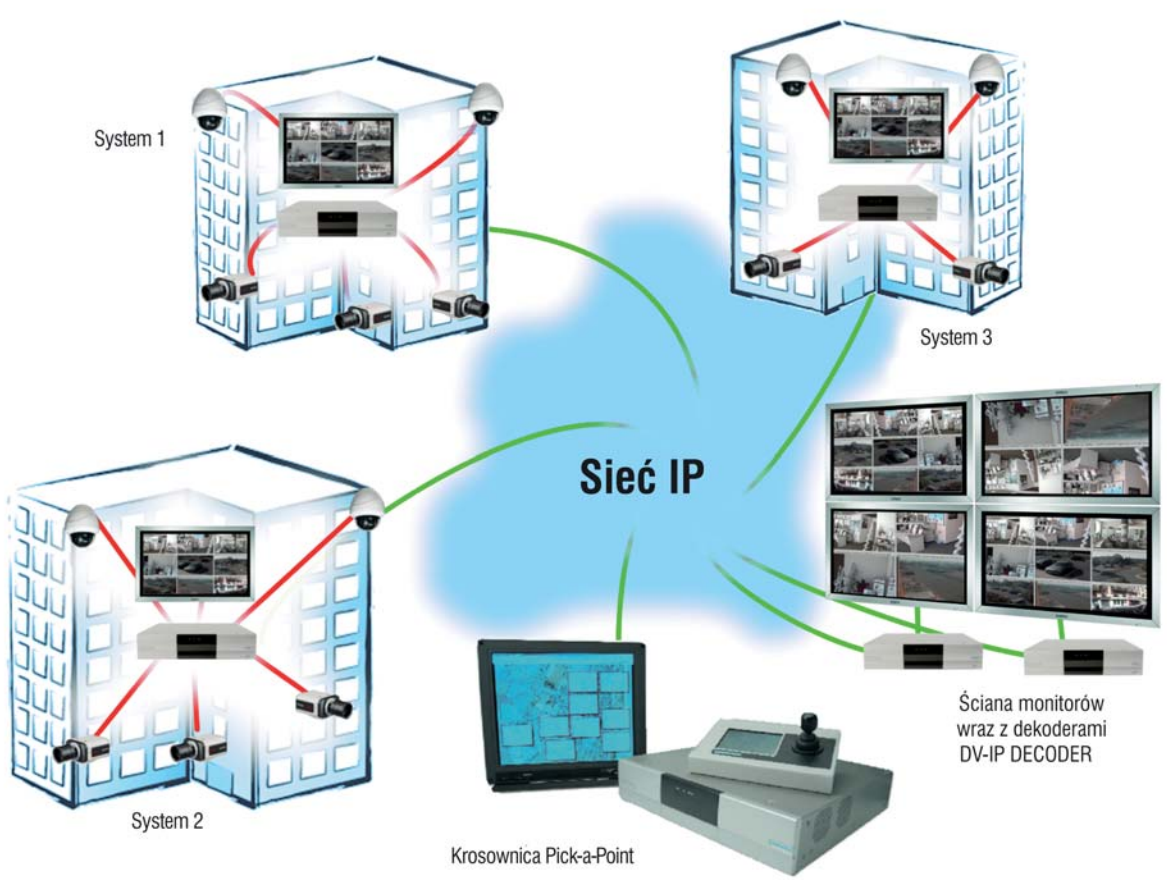
Do zarządzania dużymi i rozległymi systemami CCTV zaprojektowano cyfrową krosownicę wizyjną Pick-A-Point. Łączy ona w sobie system centralnego zarządzania, obsługę wielopoziomowych map synoptycznych, a także stwarza

Fot. 1. Rejestrator serii DM DV-IP-RT

Fot. 2. Konsola DM NetVuConsole



Rys. 1. Schemat prostego systemu obsługiwanego poprzez konsole NetVuConsole



Rys. 2. Przykładowa konfiguracja rozległego systemu zarządzanego jednostanowiskowo, za pomocą krosownicy Pick-a-Point

możliwość zdalnej konfiguracji oraz zarządzania i kontroli stanu urządzeń pracujących w systemie. Umożliwia obsługę dowolnego dekodera w systemie, a w połączeniu z dekoderami DV-IP Decoder HDMI pozwala w prosty sposób budować tak zwaną „ścianę monitorów". Dekodery te potrafią również wyświetlać obrazy z kamer megapikselowych bez straty jakości. Posiadają kilka wejść alarmowych oraz fonicznych, dzięki którym w razie potrzeby można nadać komunikat głosowy. Każde przychodzące do rejestratora zdarzenie alarmowe zostanie zaznaczone na mapie synoptycznej wyświetlanej przez PickAPoint. Możliwość definiowania podziału obrazu, sekwencji czy reakcji na zdarzenie na dowolnym monitorze znajdującym się na „ścianie" monitorów pozwala zaprojektować system, który maksymalnie wspomoże operatora. Obsługa krosownicy odbywa się przy użyciu dodatkowego dotykowego pulpitu sterującego z manipulatorem. Do konfiguracji i obsługi można również wykorzystać mysz i klawiaturę USB.

Dzięki zastosowaniu sieciowej krosownicy Pick-A-Point unikamy konieczności tworzenia kosztownych instalacji analogowych i układania kilometrów kabla koncentrycznego. Cyfrowa krosownica wizyjna zapewnia dużą elastyczność systemu. W każdej chwili, nie ingerując w okablowanie, można dołączyć do systemu dodatkowe kamery i urządzenia oraz odpowiednio je konfigurować. Każdy nadajnik sygnału wizyjnego (rejestrator lub kamera IP) jest w stanie wysłać strumień danych do każdego odbiornika – dekodera IP lub innego rejestratora. Dzięki temu unika się zbędnego obciążenia łącza, a sygnały są przekazywane bez pośrednictwa samej krosownicy Pick-A-Point. Dwustrumieniowość i technologia MultiMode pozwalają na dobranie odpowiednich parametrów transmisji sieciowej pomiędzy urządzeniami generującymi i rejestrującymi obrazy – w przypadku podglądu na żywo możemy zastosować kodowanie MPEG4, a do rejestracji obrazu kodowanie MJPEG. Pozwoli to na uzyskanie płynnych obrazów na monitorach i na zachowanie wysokiej jakości zapisu.

Dla specjalnych systemów o bardzo wysokim stopniu bezpieczeństwa firma Dedicated Micros stworzyła w swoich urządzeniach zestaw funkcji Analytics Capable. Są to funkcje zaawansowanej analizy obrazu, umożliwiające wykrycie przekroczenia wirtualnie zdefiniowanej strefy i określenie liczby osób ją przekraczających, wykrycie ruchu i określenie jego kierunku, analizę i rozpoznawanie numerów tablic rejestracyjnych samochodów lub wykrycie zniknięcia lub pojawienia się jakiegoś przedmiotu.

W dobie nasilonego zagrożenia terrorystycznego szczególnie cenne są wszelkie funkcje pozwalające operatorom systemu CCTV na szybkie wykrycie zdarzenia i ustalenie tożsamości sprawcy. Równie istotne znaczenie mają zaawansowane możliwości analityki, połączone z efektywnym przekazem informacji do operatora. Takie systemy mogą być szybko i elastycznie budowane i rozszerzane. W dziedzinie bezpieczeństwa wszystko powinno być tak dobre, jak to tylko możliwe.

Karol Fietkiewicz
SPS Trading

Bezpieczny łańcuch dostaw

Roman Marszycki

Tematy związane z bezpieczeństwem są jednymi z najistotniejszych dla sprawnego funkcjonowania przedsiębiorstw, niezależnie od branży i obszaru działalności. Zapewnienie bezpieczeństwa aktywności gospodarczej, w tym również logistycznej, stanowi podstawę właściwej działalności firm i ma bezpośrednie przełożenie na jakość świadczonych usług

Ważnym elementem sprawnej i efektywnej realizacji procesu logistycznego jest jego bezpieczeństwo. W ostatnich latach problematyka ta nabrała szczególnego znaczenia, jeżeli bowiem logistykę rozumiemy jako zapewnienie właściwych zasobów w odpowiednim miejscu i czasie, w odpowiedniej ilości i jakości, to możemy zaryzykować stwierdzenie, że w dobie współczesnych procesów globalizacyjnych bezpieczeństwo łańcucha dostaw staje się nadrzędnym celem logistyki.

Jednocześnie powinniśmy mieć świadomość tego, iż bezpieczeństwo łańcuchów dostaw jest kategorią bardzo pojemną i złożoną. Czynników wpływających na bezpieczeństwo logistyki jest wiele. Należą do nich oczywiście zagrożenia kradzieżą, ale również warunki klimatyczne, nieprzewidziane zdarzenia, wypadki itp., które mogą mieć wpływ na bezpieczeństwo realizacji dostaw.

Oferowanie kompleksowych usług logistycznych przez wielu usługodawców wymaga zatem takich ustaleń normatywnych w obszarze bezpieczeństwa, które uwzględniałyby złożoność realizacji procesów oraz liczbę firm logistycznych biorących udział w realizacji danego procesu, ich różnorodność, zakres ich działań itp.

Powstała w 2008 roku norma ISO 28000 została stworzona jako swoista odpowiedź na potrzeby branży. Dotyczy wszystkich organizacji biorących udział w procesie dostaw produktów, na każdym ich etapie (wybór kontrahentów, transport, spedycja, odprawy celne, magazynowanie itp.).

Nadrzędnym celem tej certyfikacji jest zapewnienie odpowiedniego poziomu bezpieczeństwa każdego z ogniw łańcucha w myśl zasady, że system jest tak silny, jak jego najsłabsze ogniwo. Dlatego prewencja w dziedzinie bezpieczeństwa realizacji procesów logistycznych na poziomie pojedynczych podmiotów (grup terminali logistycznych, magazynowych itp.) wydaje się być podstawowym kierunkiem kształtowania odpowiednio wysokiego poziomu bezpieczeństwa łańcucha jako całości.

Powyższy cel może zostać osiągnięty przez podmioty profesjonalnie zajmujące się ochroną mienia dzięki dwóm rodzajom działań. Pierwszy z nich to zewnętrzna ochrona obiektów logistycznych, realizowana przez grupę pracowników ochrony, którzy wykonują zadania określone na podstawie przeprowadzonej wcześniej oceny stanu bezpieczeństwa obiektu.

Zazwyczaj zadania te są ujęte w zestawy odpowiednio przygotowanych procedur postępowania i służą regulacji zachowań pracowników ochrony w sytuacjach przewidywalnych i powtarzalnych, takich jak prewencja, obsługa ruchu towarowego i ruchu osobowego, prowadzenie wymaganej dokumentacji, reakcja w sytuacjach alarmowych.

W tym miejscu należy zaznaczyć, że przygotowanie tych procedur, które stanowią fundament jakości realizowanej usługi, musi odbywać się przy wsparciu i udziale ludzi zajmujących się logistyką – procedury ochrony nie mogą kolidować z procesami logistycznymi. Dla przykładu – drobiazgowa kontrola samochodów wyjeżdżających w tzw. „oknie czasowym" może doprowadzić do załamania terminowości dostaw.

Ponadto ochrona takich obiektów powinna być wspierana przez systemy elektronicznego dozoru mienia, takie jak zewnętrzne systemy telewizji dozorowej, systemy kontroli dostępu, systemy wykrywania włamania czy systemy ppoż.

Druga droga do zapewnienia bezpieczeństwa procesowi logistyki wiedzie przez wewnętrzne wsparcie działań operatora logistycznego. Organizacja logistyczna ma realną szansę na poprawę niektórych wskaźników jakościowych związanych z prowadzeniem procesu dzięki wprowadzeniu firmy ochrony do jej wnętrza.

Powiązanie poprawy wskaźników jakościowych określanych przez operatorów logistycznych z bezpieczeństwem łańcucha logistycznego jest tylko pozornie odległe. Jeżeli założymy, że jednym z ważnych dla firmy logistycznej czynników jakościowych jest poziom strat przedstawianych przy okazji rozmów z nowymi klientami, to zmniejszenie lub ograniczenie tych strat jest elementem przewagi konkurencyjnej.

Odpowiedzią na takie zapotrzebowanie może być program Menedżer Bezpieczeństwa realizowany przez pracowników firmy ochrony, której zadaniem jest nadzór nad przesyłką.

Odpowiednio wybrani i przeszkoleni pracownicy mają realizować zadania w sposób, który w konsekwencji przyniesie zmniejszenie strat na terenie terminali, powstałych w związku z kradzieżami czy uszkodzeniami przesyłek.

Pierwszym krokiem do rozpoczęcia współpracy firmy logistycznej i firmy zapewniającej ochronę jest podpisanie umowy o poufności. Krok ten jest ogromnie istotny ze względu na fakt, że firma ochrony uzyskuje dostęp do bardzo „wrażliwych" danych związanych ze skalą kradzieży i uszkodzeń podczas realizacji bardzo konkretnych projektów logistycznych.

Aby skutecznie przełożyć język prewencji na wymierne wskaźniki opisujące wielkość straty, proponujemy wprowadzenie tzw. współczynnika straty (W_S), który w sposób czytelny i jednoznaczny określa punkt wyjścia (bazę) potencjalnej współpracy.

Współczynnik starty W_S jest stosunkiem wartości zaginięć i (lub) uszkodzeń do wartości sprzedaży w określonym czasie. Na podstawie doświadczeń firma ochrony jest w stanie określić, kiedy i o ile zmniejszy wyznaczony wskaźnik.

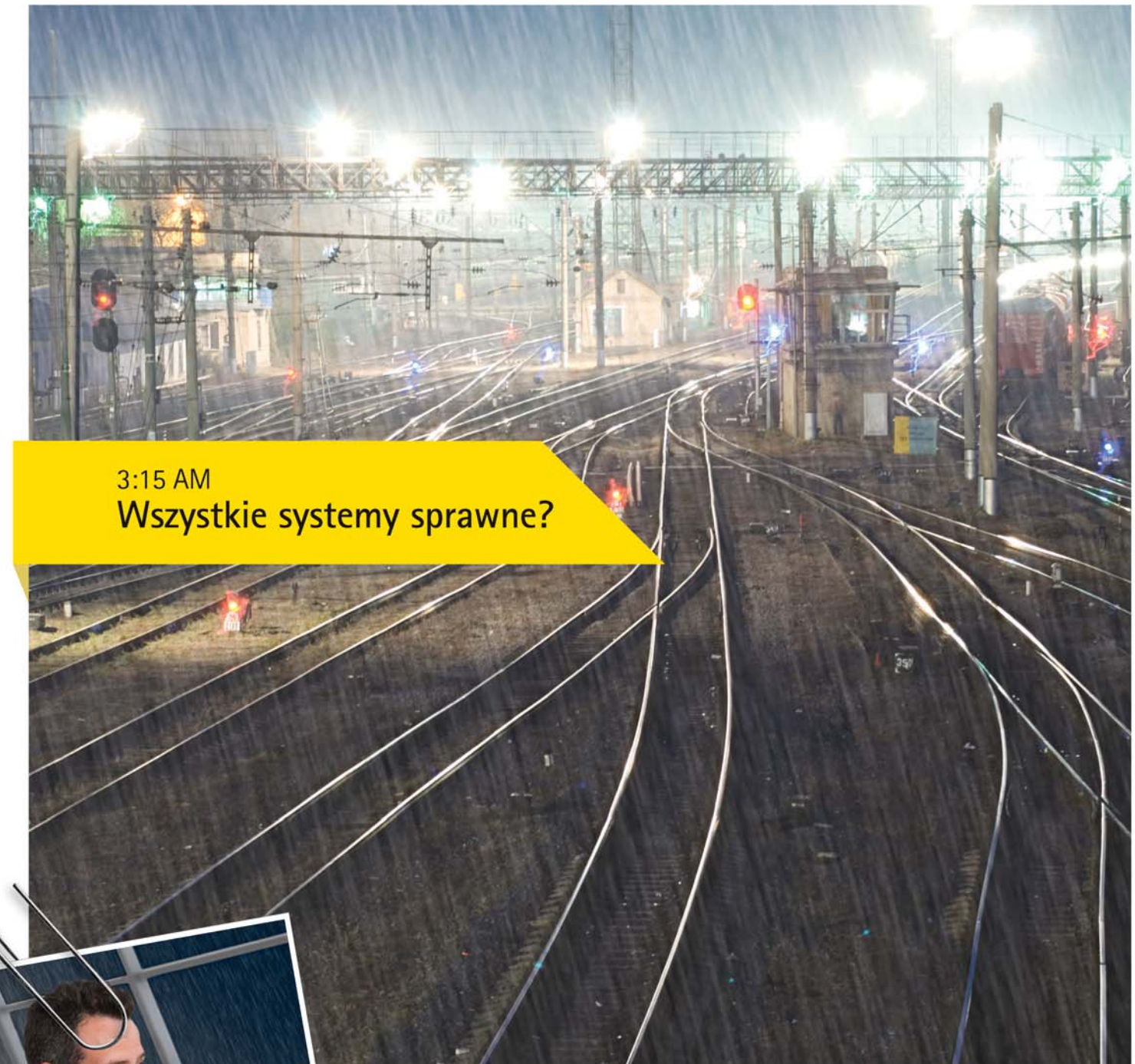
Ten prosty mechanizm pozwala na konkretne, przekładające się na umowne zapisy zobowiązania, do jakich należy dążyć, oraz konsekwencje ich realizacji lub braku realizacji.

Obserwując pracę terminali, staramy się określić miejsca i procesy, które stwarzają potencjalne okazje do kradzieży lub uszkodzeń przesyłek, a następnie proponujemy tak zmienić odpowiednie procedury – czy to bezpieczeństwa, czy to logistyczne – aby wyeliminować powstałe zagrożenie. Praca nad pojedynczymi zdarzeniami w pierwszym etapie po otrzymaniu informacji o reklamacji sprowadza się często do ustalenia drogi, jaką przesyłka przebyła po magazynie. W praktyce oznacza to sprawdzenie, jak przesyłka dotarła do terminalu, kto ją przywiózł, kto ją odebrał, jak wyglądała. Podstawowym narzędziem wykorzystywanym do ustalania tych informacji jest między innymi system telewizji dozorowej. W kolejnym etapie formujemy wnioski i rekomendacje wynikające z zauważonych błędów, które mają poprawić proces logistyczny lub system ochrony.

Praca menedżerów bezpieczeństwa nie ogranicza się jedynie do wyjaśniania powstałych reklamacji – jej ważnym elementem jest tworzenie programów szkoleniowych (na podstawie zdobytego doświadczenia), szkolenie pracowników klienta z zakresu funkcjonowania procedur bezpieczeństwa, wdrażanie nowych procedur oraz doskonalenie procedur istniejących. Korzyści płynące z takiej współpracy to w wymiarze czysto finansowym, zmniejszenie straty, ale również poprawa relacji na linii firma logistyczna – klient.

W naszych rozważaniach nie możemy pominąć kosztów związanych z ubezpieczeniem działalności gospodarczej, gdyż ciągłe zmniejszanie współczynnika szkód przez firmę logistyczną – prowadzi do obniżenia składki ubezpieczeniowej. W konsekwencji wdrożenie programu Menedżer Bezpieczeństwa będzie powodowało zwiększenie konkurencyjności tej drugiej, poprzez świadome działania mające na celu poprawę jakości oferowanej usługi logistycznej.

Roman Marszycki
Securitas Polska



3:15 AM
Wszystkie systemy sprawne?

Efektywny system zewnętrznego nadzoru wizyjnego chroni to co cenimy najbardziej, ostrzega o niespodziewanych zdarzeniach a nawet uaktywnia konkretne działania. Ale kamery, które są w stanie to osiągnąć muszą wytrzymywać ciężkie opady śniegu, intensywne opady deszczu lub silne wiatry i ciągle dostarczać użyteczny obraz.

Kamery do zastosowań zewnętrznych Axis są wyjątkowo proste do zainstalowania, co oszczędza cenny czas i minimalizuje koszty utrzymania.

Wytrzymują one ekstremalne warunki pogodowe i zapewniają wyjątkową jakość obrazu. Ponieważ system nadzoru wizyjnego musi dostarczać niepodważalne dowody w formie przejrzystego, wyraźnego materiału wizyjnego nawet w najcięższych warunkach.

Przyjmij punkt widzenia Axis. Bądź zawsze o krok do przodu.
Odwiedź stronę www.axis.com/outdoor

AXIS Q6032-E Sieciowa Kopułkowa Kamera z mechanizmem PTZ: obudowa klasy IP66, 35xzoom, tryb dzień/noc, wide dynamic range, H.264, Power over Ethernet, Arctic Temperature Control i wiele innych

AXIS COMMUNICATIONS

Wstęp do wirtualizacji

Paweł Duda

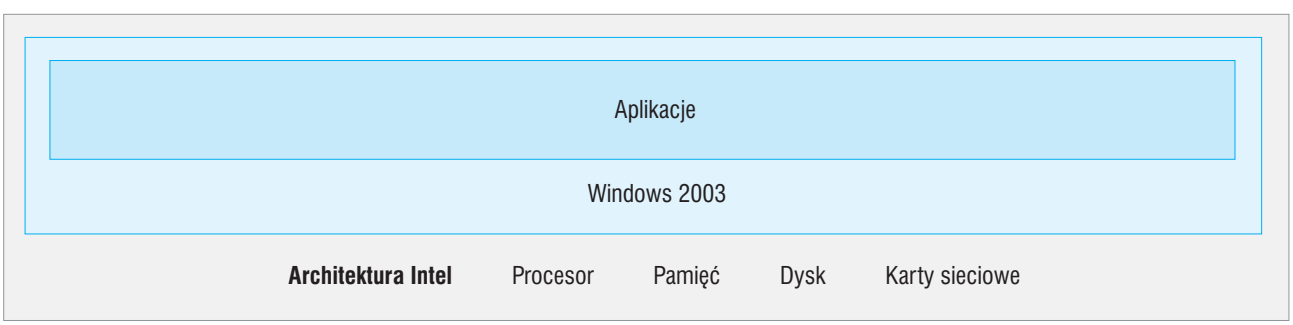
Obecnie szczególną uwagę poświęca się minimalizacji nakładów na infrastrukturę IT. Jednocześnie widać starania mające na celu zwiększenie bezpieczeństwa i dostępności usług oraz ochronę środowiska. Wirtualizacja jest jednym z elementów zabezpieczających zarówno serwery, jak i stacje robocze. Pozwala ona uniezależnić się od platformy sprzętowej, a w związku z tym umożliwia łatwą migrację maszyn wirtualnych pomiędzy fizycznymi serwerami

Zadaniem obecnej infrastruktury IT jest utrzymanie dużej dostępności, zarówno dla aplikacji już działających, jak i nowo wdrażanych. Wiąże się z tym wzrost liczby fizycznych serwerów, wysoka złożoność infrastruktury oraz wzrost kosztów utrzymania związany z zasilaniem, chłodzeniem serwerów, utrzymywaniem administratorów sieci. Na to wszystko ciągle brakuje miejsca w serwerowni. Do tego dochodzi niezbyt optymalne wykorzystywanie serwerów, które nadal mają strukturę x86. Średnie wykorzystanie takiego serwera zawiera się w przedziale od 5 do 15%, co jest związane nie tylko z niewykorzystaniem mocy obliczeniowej serwera, ale również z marnowaniem energii (serwer musi być ciągle zasilany i chłodzony). Jeśli istnieje podział jedna aplikacja – jeden serwer, to zwiększa się liczba serwerów, a to stwarza kolejne problemy z zasilaniem, chłodzeniem i miejscem w serwerowni. Odtworzenie systemu w razie awarii, testowanie aplikacji itp. wymaga kolejnych serwerów (problemy z zasilaniem, chłodzeniem, miejscem w serwerowni). Aby uniknąć tych wszystkich problemów, należy dokonać wirtualizacji serwerów. Umożliwia ona pełne wykorzystanie zasobów.

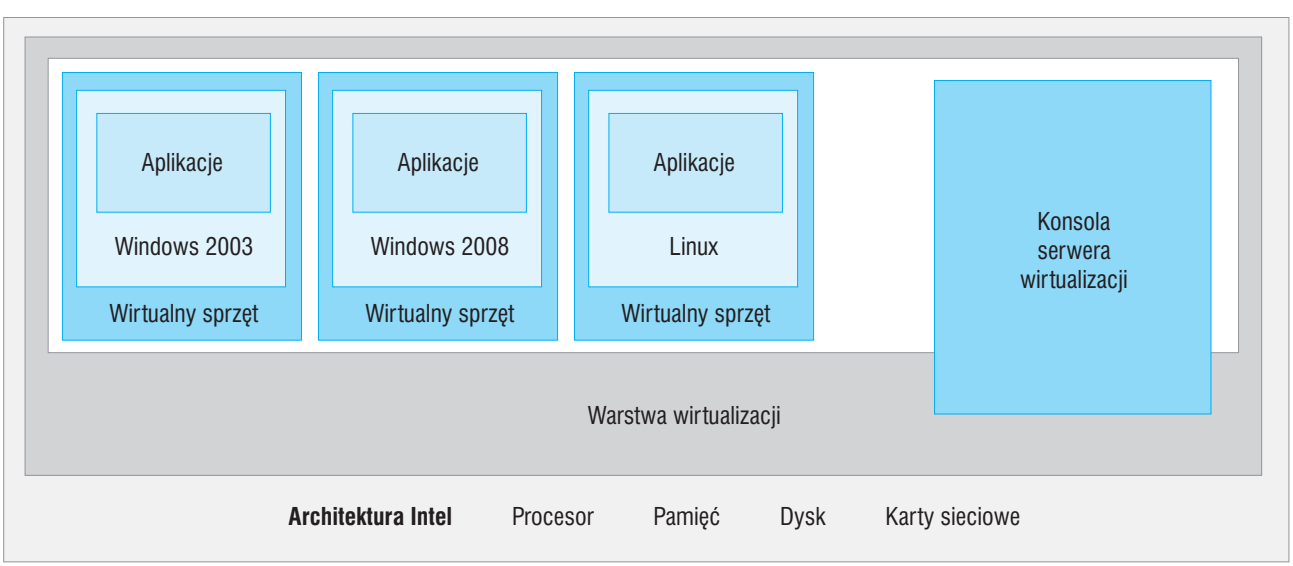
Na początku kilka słów na temat samej wirtualizacji. Generalnie wirtualizacja pozwala uruchomić wiele wirtualnych maszyn posiadających własny (wirtualny) sprzęt i mogących działać w różnych systemach operacyjnych na jednym fizycznym serwerze (tzw. hoście). Na jednym hoście mogą równocześnie pracować różne wirtualne maszyny działające pod kontrolą różnych systemów operacyjnych, np. MS Windows, Linux. Każda z tych wirtualnych maszyn posiada wydzielone zasoby z serwera hosta. Administrator wirtualizacji definiuje wielkość pamięci operacyjnej, liczbę kart sieciowych, pojemność dysków twardych, rodzaj kontrolerów SCSI itp. dla każdej wirtualnej maszyny. Jednym słowem definiujemy wirtualny komputer posiadający te wszystkie elementy, co serwer fizyczny, czyli procesor, pamięć operacyjną, karty sieciowe, kontrolery SCSI, płytę główną, napędy FDD, napędy CD-ROM.

Oczywiście zasoby dla wirtualnych maszyn są wydzielane z zasobów serwera hosta. Z tego wypływa prosty wniosek, iż maszyny fizyczne, które mają być użyte do wirtualizacji, muszą posiadać odpowiednie zasoby odpowiadające potrzebom uruchamianych maszyn wirtualnych.

Biorąc pod uwagę średnie wykorzystanie procesorów serwerów x86 wynoszące od 5 do 15% można przewidzieć, iż na jednym serwerze można uruchomić co najmniej kilka wirtualnych maszyn. Dzięki temu można uzyskać wysoki stopień wykorzystania zasobów, czyli pełnego wykorzystania sprzętu, a jednocześnie zredukować liczbę serwerów fizycznych, np. z dziesięciu do jednego. Weźmy pod uwagę to, że współczesne serwery zazwyczaj mają procesory czterordzeniowe, więc na jednym serwerze można uruchomić około 32 wirtualnych maszyn. Oczywiście jest to wartość przybliżona, gdyż może się zdarzyć, że dana wirtualna maszyna będzie potrzebować więcej niż jednego procesora lub pewne maszyny wirtualne będą mocniej obciążały system hosta niż inne itp. Im wyższy priorytet ma wirtualna maszyna, tym więcej cykli procesora przydziela jej system wirtualizacji – więcej niż innym wirtualnym serwerom, co w konsekwencji skutkuje wydajniejszą pracą maszyny.



Rys. 1. Architektura tradycyjna – system operacyjny uruchamiany bezpośrednio na maszynie fizycznej



Rys. 2. Wirtualizacja tworzy wirtualne maszyny

Uniezależnienie systemu operacyjnego wirtualnej maszyny od fizycznej budowy serwera hosta ułatwia przeniesienie wirtualnej maszyny na serwer fizyczny bez konieczności przeinstalowania systemu operacyjnego i odzyskiwania danych na nowej maszynie. Wymagana jest tylko instalacja warstwy wirtualizacji na sprzęcie fizycznym. Wirtualne maszyny dostają wirtualny sprzęt, który zawsze jest taki sam, niezależnie od tego, jaki jest sprzęt fizyczny (dlatego możliwe jest łatwe przenoszenie wirtualnych maszyn pomiędzy fizycznymi serwerami). Kolejną funkcją umożliwiającą przenoszenie maszyn jest ich hermetyzacja, czyli umieszczenie wirtualnej maszyny w kilku plikach. Cała wirtualna maszyna to jeden katalog, w którym są wszystkie pliki, a w nich wszystkie niezbędne do uruchomienia tej maszyny informacje. Jest m.in. informacja o liczbie procesorów, pamięci, kartach sieciowych, dyskach (o wielkości dysku i ścieżce do pliku dysku), są pliki z zawartością wirtualnych dysków itp. Kopiując te pliki z jednego serwera na drugi, jesteśmy w stanie uruchomić wirtualną maszynę na nowym fizycznym sprzęcie bez konieczności dokonywania zmian na poziomie systemu operacyjnego maszyny wirtualnej.

Wprowadzając wirtualizację osiągamy zwiększenie współczynnika wykorzystania zasobów, zwiększenie ciągłości biznesowej. Bezpieczeństwo eksploatowanych systemów zależy również od testowania i rozwoju aplikacji. Wyobraźmy sobie sytuację, że przez pewien czas administratorowi wyświetla się okno serwisowe. W tym czasie musi zainstalować krytyczną poprawkę do systemu. Co się stanie, jeśli akcja ta nie powiedzie się? W najgorszym przypadku administrator będzie musiał odzyskać konfigurację i zawartość serwera z kopii zapasowej. Dzięki wirtualizacji może zapisać obraz serwera – wykonać zdjęcie migawkowe (*snapshot*) – przed dokonaniem krytycznych instalacji. Jeśli instalacja krytycznej poprawki powiedzie się, obraz serwera może zostać usunięty, a jeśli spowoduje ona nieprawidłowe działanie serwera, administrator może przywrócić jego stan dzięki zapisanemu obrazowi. Ten przykład pokazuje jedną z wielu zalet wirtualizacji.

Kolejne zalety to oszczędności związane ze zmniejszeniem liczby serwerów fizycznych – mniejsze koszty zakupu infrastruktury fizycznej, mniejsze koszty zasilania (mniej fizycznych serwerów – np. zamiast dwudziestu są tylko dwa) i chłodzenia (mniej maszyn generuje mniejszą ilość ciepła), zaoszczędzenie miejsca w serwerowni, uproszczenie infrastruktury fizycznej (podłączone są tylko dwa serwery, a nie 20), a co za tym idzie mniejsza liczba portów na urządzeniach aktywnych. Planowane i nieplanowane przestoje powodują wzrost kosztów operacyjnych. W rozwiązaniach fizycznych (podejście tradycyjne) produkty umożliwiające dużą dostępność są drogie i zazwyczaj stosuje się je tylko w wybranych, krytycznych systemach. Stosując wirtualizację, uzyskujemy dużą dostępność niejako z marszu. Oczywiście także wirtualizacja wymaga określonych nakładów, szczególnie na infrastrukturę zasobów dyskowych, jeżeli chce się uzyskać pełnię jej możliwości, jednak w ostatecznym rozrachunku opłaca się nie tylko ze względu na koszty, ale także utrzymanie infrastruktury.

Paweł Duda
OPTeam

NAJNOWSZE SERIE KAMER TERMOWIZYJNYCH

więcej na: **www.atline.pl**

firma **ATLine®**

kompleksowe zabezpieczanie obiektów

PROJEKTOWANIE KOMPLEKSOWYCH DOKUMENTACJI

- technicznych, architektoniczno - budowlanych wraz z niezbędnymi branżami specjalistycznymi obiektów biurowych i przemysłowych
- innowacyjnych systemów ochrony
- teletechnicznych, elektrycznych i automatyki przemysłowej

WYKONAWSTWO

zaawansowanych technologicznie systemów ochrony i bezpieczeństwa

SPRZEDAŻ

nowoczesnych systemów ochrony

Firma ATLine sp.j. Sławomir Pruski
ul. Franciszkańska 125, 91-845 Łódź
tel. +48 042 657 30 80, fax +48 042 655 20 99
e-mail: info@atline.pl, handel@atline.pl

ZSJZ

AQAP 2110:2006

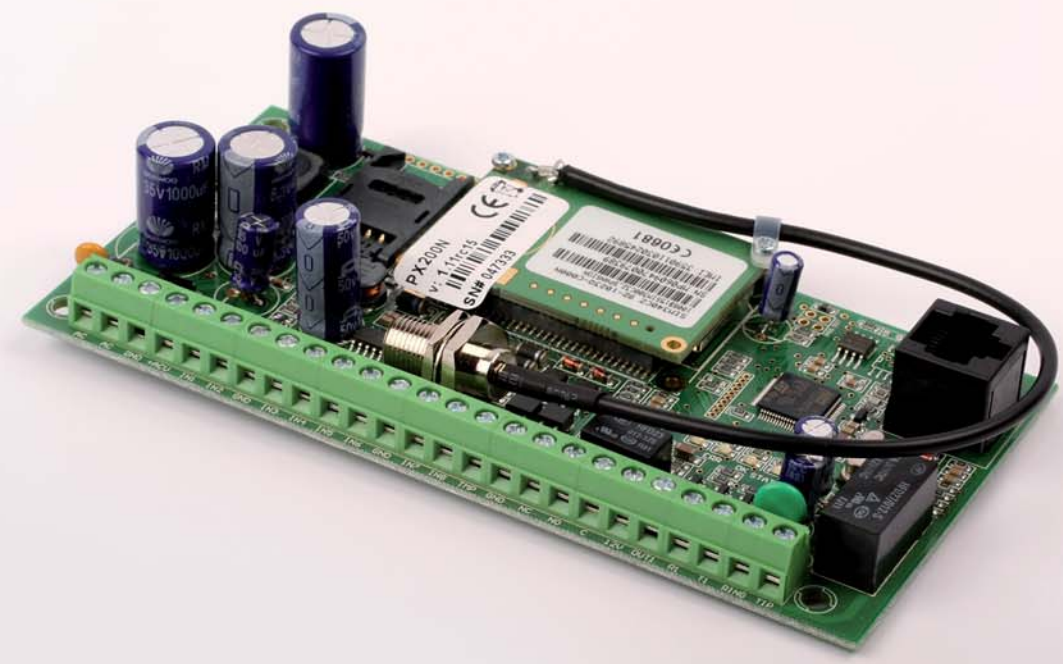
PCBC

Wybrane aspekty bezpieczeństwa systemów ochrony

Bezpieczeństwo transmisji danych

Przemysław Długosz

Systemy ochrony mają za zadanie zapewnić bezpieczeństwo ludziom i obiektom, ale, żeby robić to skutecznie, muszą zadbać o własne bezpieczeństwo. Kluczowym elementem współczesnych systemów ochrony są automatycznie zbierane informacje o chronionych obiektach. Bezpieczeństwo tych danych jest jednym z najistotniejszych aspektów bezpieczeństwa systemów ochrony



Systemy ochrony to zespół środków technicznych, organizacyjnych, prawnych oraz ochrona fizyczna, których zadaniem i celem jest zapewnienie odpowiedniego poziomu bezpieczeństwa ludzi, mienia, danych oraz prawidłowego funkcjonowania chronionego obiektu, przedsiębiorstwa itp. W niniejszym artykule poruszone zostaną te aspekty bezpieczeństwa systemów ochrony, które bezpośrednio wiążą się z niezawodnością przesyłu i szeroko pojętą ochroną danych, zbieranych i analizowanych przez systemy ochrony.

Problemy pojawiające się w związku ze zbieraniem i analizowaniem danych z chronionych obiektów są powszechne. Do ich wyeliminowania prowadzi:

– uświadomienie sobie istnienia pewnych niedoskonałości stosowanych rozwiązań,
– umiejętne zaprojektowanie systemów dostarczania danych (od urządzeń zainstalowanych u użytkownika końcowego systemu do oprogramowania zainstalowanego na komputerze operatora stacji monitorowania),
– wykorzystywanie wszystkich możliwości zaprojektowanego systemu przesyłu danych dzięki jego odpowiedniemu wdrożeniu i konfiguracji.

Należy przy tym pamiętać, że nawet najlepsze rozwiązania techniczne są zależne od pracy ludzi, a opisane metody zabezpieczania przesyłu danych nie zastąpią prawidłowo wypracowanych i wielokrotnie ćwiczonych procedur, dzięki którym każdy pracownik czuwający nad prawidłowym funkcjonowaniem systemu ochrony będzie w stanie poradzić sobie z wszelkimi nietypowymi sytuacjami.

Kategoryzacja

Zdecydowana większość problemów pojawiających się w związku z transmisją i analizą danych przesyłanych z chronionych obiektów pojawia się na skutek popełnionych wcześniej błędów. Ze względu na charakter błędów można je podzielić na:

– błędy projektowe,
– błędy konfiguracyjne,
– błędy ludzkie.

Poszczególne kategorie błędów zostały podane w powyższej kolejności nieprzypadkowo. Jako pierwsze wymieniono błędy projektowe, których skutki powodują największe straty. Eliminacja tych błędów jest najbardziej skomplikowana, czasochłonna i kosztowna. Za najmniej kosztowne uważane są błędy ludzkie. Ich skutki mają najczęściej charakter przejściowy. Poniżej przedstawionych zostanie kilka reprezentatywnych przykładów każdego z typów błędów.

Błędy projektowe

Błędy projektowe pojawiają się wówczas, gdy założenia tworzonego systemu przesyłu danych zostaną oparte na błędnych przesłankach. Na wynikach pracy takiego systemu i integralności przetwarzanych przez niego danych nie można polegać.

Błędy projektowe powstają zazwyczaj na skutek niezrozumienia zasad funkcjonowania sieci transmisyjnych i wykorzystywanych protokołów komunikacyjnych. Typowe błędne przesłanki to założenie, że publicznie dostępne media transmisyjne nie mają luk w zabezpieczeniach, założenie o niezawodności zasilania sieciowego, nieawaryjności środków technicznych systemu, a także o statyczności systemu, tzn. zakładanie, że nie pojawi się potrzeba jego modyfikacji.

Na skutek ww. nieprawidłowych założeń w trakcie projektowania systemu przesyłu danych popełniane są takie błędy, jak niestosowanie zabezpieczeń transmisji, awaryjnego zasilania ani zapasowych urządzeń, a także tworzenie systemów całkowicie nieelastycznych, uniemożliwiających szybkie i tanie dostosowanie ich do zmieniających się warunków zewnętrznych.

Problemy pojawiające się na skutek popełniania tego rodzaju błędów są często trudne do wyeliminowania. Jednym z poważniejszych jest wystąpienie fałszywych alarmów (informacji o zdarzeniach, które nie miały pokrycia w rzeczywistości) w efekcie ingerencji z zewnątrz w niedostatecznie dobrze chroniony system. Na skutek błędów popełnionych podczas projektowania systemu powstają także takie problemy, jak utrata danych lub duże opóźnienia w transmisji spowodowane brakiem zasilania lub awarią jednego z elementów systemu. Kłopotem jest także nieprawidłowe działanie systemu związane z niemożnością jego dostosowania (np. w sytuacji wystąpienia zmian w strukturze transmisji, takich jak zmiana prefiksu sieci telefonicznej).

Istnieje szereg metod pozwalających wyeliminować wymienione powyżej problemy. Ingerencji nieuprawnionych osób w system można zapobiec, stosując szyfrowanie przesyłanych danych za pomocą sprawdzonych, trudnych do złamania algorytmów na każdym etapie transmisji, począwszy od nadajnika, a kończąc na odbiorniku w stacji monitorowania. Zwiększeniu bezpieczeństwa przesyłu służy również zapewnienie dedykowanych łączy, np. w postaci szyfrowanych tuneli od operatorów transmisyjnych (w przypadku GSM – prywatny APN).

Kłopotom powstającym na skutek awarii niektórych elementów systemu można przeciwdziałać, budując system w oparciu o zasady redundancji. Oznacza to m.in. stosowanie nadajników lub par nadajników umożliwiających równoczesny przesył danych do stacji za pomocą wielu metod transmisji oraz zapewnienie dostępu do dwóch niezależnych łączy do operatorów sieci transmisyjnych (np. łączy do Internetu). Redundantne elementy warto również stosować w wewnętrznej sieci komputerowej (rutery, switche itd.). Ważnym sposobem zabezpieczania przesyłu danych jest także stosowanie w stacji monitoringu systemu odbioru danych, który umożliwia odbiornikom pracę w klastrze, dzięki któremu są one w stanie automatycznie lub z niewielkim udziałem człowieka zapewnić ciągłość transmisji w przypadku awarii. Duże znaczenie ma również dywersyfikacja kanałów przesyłu dzięki współpracy z różnymi operatorami telekomunikacyjnymi, szczególnie w przypadku dużych obiektów, w których informacje docierają z wielu nadajników. Dzięki zdywersyfikowaniu operatorów telekomunikacyjnych w przypadku wystąpienia awarii u jednego z operatorów zostajemy pozbawieni tylko części informacji o obiekcie.

Mając na uwadze problemy związane z awariami elementów systemu, podczas tworzenia systemu warto zastosować urządzenia w najwyższym stopniu niezawodne,

np. odbiorniki pozbawione mechaniki (takie urządzenia są pozbawione dysku twardego, a wszelkie informacje są zapisywane na bardziej niezawodnych pamięciach typu flash; są również bardziej odporne na działanie skrajnych temperatur w przypadku uszkodzenia systemu wentylacji). Podstawową i równie istotną kwestią jest także używanie systemów, w których zapewniono ciągłość zasilania (np. dzięki akumulatorom w nadajnikach lub generatorom prądotwórczym w stacjach).

Problemy związane z koniecznością rekonfiguracji elementów systemu można rozwiązać, wybierając takie składniki systemu, które umożliwiają zdalną zmianę konfiguracji. Jest to szczególnie istotne w przypadku nadajników, które są najbardziej oddalonymi fizycznie elementami systemu. Dzięki stosowaniu nadajników umożliwiających pełną zdalną rekonfigurację zapewniamy ciągłość ich pracy w zmieniających się warunkach stosunkowo niskim kosztem.

Spośród wyżej wymienionych elementów za najważniejsze należy uznać projektowanie systemu w oparciu o nadajniki korzystające ze sprawdzonych algorytmów szyfrujących oraz stosowanie automatycznych systemów redundantnych. Bezpieczeństwo takich systemów opiera się na konfigurowalnych kluczach szyfrujących oraz na szybkim powrocie systemu do działania (ang. *recovery*) w przypadku awarii, a tym samym na minimalizacji jej skutków.

Błędy konfiguracyjne

Do kategorii błędów konfiguracyjnych należy zaliczyć wszelkie pomyłki popełniane podczas wdrażania i konfigurowania składników systemów, powstałe na skutek niezrozumienia dokumentacji technicznej (a co za tym idzie – sposobu działania danego elementu systemu), a niekiedy zwykłej niedbałości. Błędy te polegają zazwyczaj na nieprawidłowym ustawieniu parametrów, często powiązanych ze sobą (nagminnym błędem jest złe określenie interwału wysyłania sygnału testu z nadajnika i interwału sprawdzania testu przez odbiornik). Powszechne jest również niewykorzystywanie dostępnych funkcji, co również należy uznać za błąd konfiguracyjny. Użytkownicy często nie włączają modułu nadzorującego pracę (sprzętowego watchdoga) w nadajniku lub odbiorniku, nie stosują metod kontroli ilości przesyłanych danych i wykonywanych połączeń, czy też nie włączają automatycznej archiwizacji bazy danych (ang. *auto backup*) w odbiorniku. Często popełnianym błędem jest także stosowanie domyślnych kodów dostępu, kluczy szyfrujących, list uprawnionych numerów typu „zezwól na wszystko” itd.

Pomyłki lub zaniedbania przy konfiguracji systemu mogą doprowadzić do takich nieprawidłowości, jak uzyskanie dostępu do składników systemu przez osoby nieuprawnione, wielokrotnie powtarzające się błędy transmisji, niedostępność nadajnika lub odbiornika na skutek błędu programowego lub sprzętowego, pojawienie się dużej liczby sygnałów w krótkim czasie (kłopotliwe w odbiorze zarówno dla oprogramowania, jak i obsługi stacji) czy utrata danych w przypadku awarii nośnika danych.

Skutki błędów konfiguracyjnych istotnie wpływają na bezpieczeństwo i niezawodność systemu, jednak można

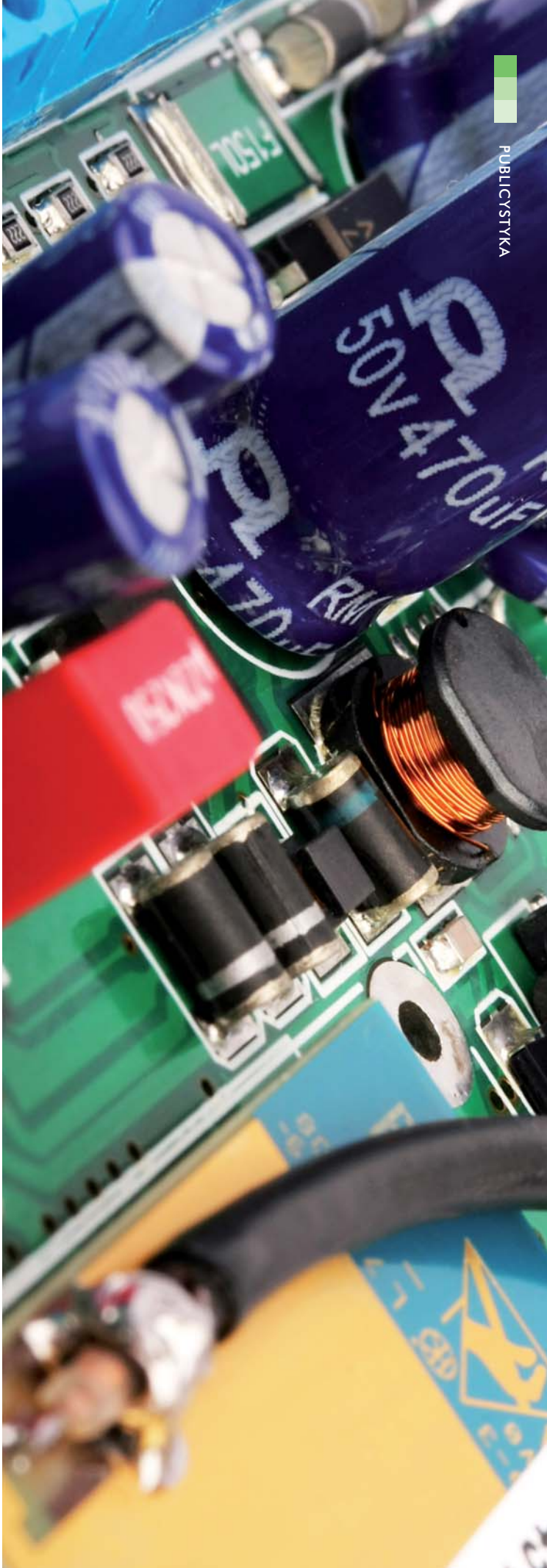
wyeliminować je stosunkowo niewielkim nakładem pracy. Kluczem do unikania tego rodzaju błędów jest staranna analiza dostarczonej dokumentacji projektowej i instrukcji obsługi urządzeń, a także szczegółowa weryfikacja znaczenia określonych parametrów. Jeśli istnieje taka potrzeba, warto dokonać konsultacji u producenta danego urządzenia lub oprogramowania. Dobrą metodą jest przygotowywanie wzorców konfiguracji, jeśli ma ona być powielana dla wielu urządzeń, co minimalizuje liczbę popełnianych błędów. Wszystkie te działania mają na celu pełne wykorzystanie funkcji kontrolujących pracę systemu, takich jak kody dostępowe, klucze szyfrujące, listy dostępowe (w miarę możliwości inne dla każdego ze składników systemu), testy okresowe na każdym etapie transmisji, sprzętowe watchdogi, funkcje zabezpieczające przed przesyłaniem zbyt dużej ilości danych (np. z uszkodzonej czujki alarmowej bądź uszkodzonego nadajnika), czy automatyczne kopie bezpieczeństwa istotnych danych (szczególnie ważne w przypadku zmian konfiguracji nadajnika czy też odbiornika).

Podstawą zapewnienia bezpieczeństwa systemu transmisji danych jest więc skonfigurowanie go w taki sposób, który pozwoli w pełni wykorzystać funkcje zaoferowane przez producentów oprogramowania i sprzętu. Dzięki temu można zminimalizować ewentualne problemy wynikające z naruszania zabezpieczeń lub niepożądanej aktywności nieuprawnionego, jak i uprawnionego użytkownika. Przynosi to szczególnie duże korzyści w przypadku utrzymywania rozległej infrastruktury, z jaką mamy zwykle do czynienia w stacjach monitorowania.

Błędy ludzkie

Błędy ludzkie pojawiają się najczęściej wtedy, kiedy użytkownicy systemu nie rozumieją w pełni zasad działania oprogramowania i systemu transmisji. Zdarza się, że uruchamiają w stosowanym oprogramowaniu nieznane sobie funkcje, ignorują komunikaty ostrzegawcze wyświetlane przez oprogramowanie, przypadkowo zmieniają opcję programu czy gubią nośniki z zapasową kopią danych. Do częstszych błędów należą – uszkodzenie operacyjnej bazy danych niezbędnej do działania systemu transmisyjnego (rejestr urządzeń, zdarzeń, konfiguracja itp.), wysłanie do nadajnika polecenia bez zaznajomienia się z jego możliwymi skutkami, a także zmiana istotnego parametru odbiornika (np. okresu sprawdzania testów) bez wstępnej analizy istniejących danych oraz bez okresowej weryfikacji działania systemu po wprowadzeniu zmiany. Równie powszechne są takie błędy, jak omyłkowe fizyczne przerwanie połączenia (np. odłączenie przewodu Ethernet, RS232 itp.), odłączenie zasilania w odbiorniku lub nadajniku, czy też umieszczanie w okolicy odbiornika lub nadajnika urządzeń elektromagnetycznych zakłócających sygnał przesyłany za pomocą sieci GSM lub drogą radiową.

Skutkiem tych błędów jest pojawienie się okresowych zaburzeń w funkcjonowaniu głównego lub zapasowego toru transmisji danych, takich jak opóźnienia, częste rozłączenia lub utrata części sygnałów. Należy mieć na uwadze to, że w przypadkach zaburzeń działania głównego toru wiele systemów automatycznie podejmuje próbę nawiązania



łączności zapasowymi drogami transmisji (np. przy zaniku połączenia GPRS nadajnik przechodzi na tryb SMS), co może nie tylko wpłynąć na czas dostarczenia wiadomości, ale i pociągać za sobą dodatkowe koszty.

Zaburzenia toru transmisji powstałe na skutek zmiany określonego parametru odbiornika lub nadajnika zwykle można naprawić, przywracając prawidłową wartość parametru. Katastrofalna w skutkach jest natomiast całkowita utrata operacyjnej bazy danych. Jej odtworzenie jest czasochłonne, a czasami w ogóle nie jest możliwe. Utrata zapasowych kopii może więc być bardzo dotkliwa.

Choć błędy ludzkie są rzeczą naturalną, niemożliwą do całkowitego wyeliminowania, można starać się minimalizować ich liczbę i skutki. Służą temu m.in. takie działania, jak stosowanie kontroli uprawnień nie tylko w poszczególnych elementach systemu, lecz również w pomieszczeniach, gdzie znajdują się istotne składniki systemu, regularne tworzenia kopii zapasowych, szkolenia użytkowników i wypracowanie odpowiednich procedur, a także okresowa weryfikacja działania systemu, np. poprzez raporty statystyczne czy bilingi od operatorów (nie tylko w sytuacji celowej zmiany parametrów).

Błędy ludzkie zwykle powodują relatywnie niewielkie straty, lecz w ogólnym rozrachunku mogą okazać się bardzo kosztowne, jeśli występują często. Wdrażając system, warto zatem mieć świadomość, że odpowiednio skonfigurowany system powinien skutecznie zapobiegać potencjalnym stratom wynikającym z niewiedzy użytkowników.

Podsumowanie

Bezpieczeństwo systemu transmisji danych należy traktować jako proces wymagający ciągłego planowania i kontrolowania, a także permanentnej edukacji użytkowników, co w praktyce często jest trudne do zrealizowania.

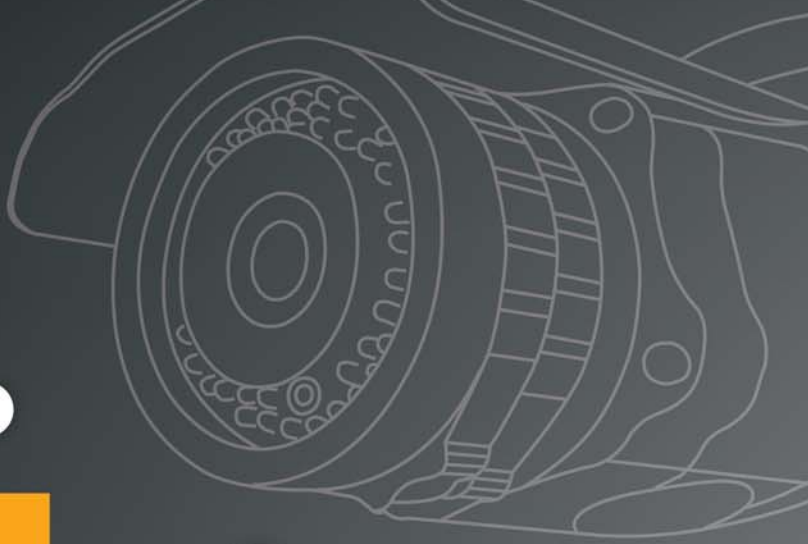
Systemy transmisyjne z pewnością będą podlegać dalszej ewolucji. Zarówno producenci systemów, jak i ich odbiorcy są stawiani przed kolejnymi wymaganiami. W ramach dalszego rozwoju należy spodziewać się maksymalnej automatyzacji wielu prostych czynności (takich jak na przykład konfigurowanie nadajników) w celu wyeliminowania pomyłek ludzkich. Z pewnością rozwinięte zostaną także metody automatycznego nadzoru nad składnikami systemu połączone z zaawansowanymi metodami wznawiania działania po awarii lub zastępowania wadliwego elementu innym.

Warto pamiętać, że pojawiające się na rynku nowe rozwiązania są niekiedy bronią obosieczną. Nowe funkcje mogą istotnie poprawić bezpieczeństwo i niezawodność systemu, ale, użyte niewłaściwie, mogą przynieść również szkody. Dlatego warto rozważyć przeprowadzenie konsultacji lub szkoleń u producenta danego rozwiązania (najczęściej są one bezpłatne), aby zwiększyć świadomość własną i użytkowników.

Przemysław Długosz
EBS

4 POZIOMY BEZPIECZEŃSTWA

Nowe serie kamer marki NOVUS®



seria G

- Czułość od 0.00003 lx
- Do 600 TVL w kolorze
- DSS (wydłużona migawka)
- OSD w języku polskim (menu ekranowe)
- Sterowanie RS-485 (oprócz kamer kopułkowych)
- WDR (szeroki zakres dynamiki)
- HLC (redukcja oślepiania)
- Strefy prywatności
- Zoom cyfrowy
- Detekcja ruchu
- DIS (cyfrowa stabilizacja obrazu)
- Oświetlacz podczerwieni (kamery wandaloodporne)
- Obiektyw f=2.5~12 mm (oprócz kamer kompaktowych)

seria H

- Czułość od 0.00004 lx
- Do 560 TVL w kolorze
- DSS (wydłużona migawka)
- OSD (menu ekranowe)
- WDR (szeroki zakres dynamiki)
- HLC (redukcja oślepiania)
- Strefy prywatności
- Zoom cyfrowy
- Detekcja ruchu

seria B

- Czułość od 0.01 lx
- Do 600 TVL w kolorze
- OSD (menu ekranowe)
- Sterowanie RS-485 (kamery kompaktowe)
- Strefy prywatności
- Detekcja ruchu
- Obiektyw f=2.8~10.5 mm (oprócz kamer kompaktowych)

seria E

- Czułość od 0.05 lx (0 lx przy włączonym oświetlaczu IR)
- Do 540 TVL w kolorze
- Oświetlacz podczerwieni

AAT Holding sp. z o.o.
ul. Puławska 431, 02-801 Warszawa, tel. 22 546 05 46, faks 22 546 05 01
e-mail: aat.warszawa@aat.pl, www.aat.pl

VESDA LaserFOCUS

VESDA LaserFOCUS to detektor do bardzo wczesnej detekcji dymu, zaprojektowany, by chronić niewielkie powierzchnie do 250 m^2 / 500 m^2.

Praca detektora polega na ciągłej analizie zasysanego powietrza poprzez sieć rur ssących. Zasysane powietrze jest filtrowane, a następnie transportowane do komory detekcyjnej, gdzie pod wpływem rozproszonego światła dokonywana jest analiza obecności cząstek dymu w nim zawartych. Wynik analizy jest pokazany na wyświetlaczu detektora.

W przypadku przekroczenie ustalonej wartości zadymienia aktywowane są przekaźniki.

Instalowanie

Detektor VESDA LaserFOCUS może być instalowany bez konieczności używania specjalnego interfejsu czy oprogramowania serwisowego.

Dzięki unikalnemu wyświetlaczowi użytkownik ma dostęp do wszelkich informacji o poziomie zadymienia. Możliwe jest również zastosowanie zdalnego wyświetlacza.

W przypadku sygnalizacji uszkodzenia użytkownik powinien otworzyć panel obsługi i aktywować funkcję poszukiwania uszkodzeń, aby określić jego przyczynę.

Ultradźwiękowy monitoring przepływu powietrza

VESDA LaserFOCUS wykorzystuje opatentowany, ultradźwiękowy system monitoringu przepływu powietrza, który umożliwia bezpośredni odczyt wielkości jego przepływu. System ten jest odporny na zmiany temperatury powietrza, zmiany ciśnienia oraz zanieczyszczenia.

VESDA LaserFOCUS jest pierwszym zasysającym systemem wczesnej detekcji dymu wykorzystującym ultradźwiękowy system monitoringu przepływu powietrza.

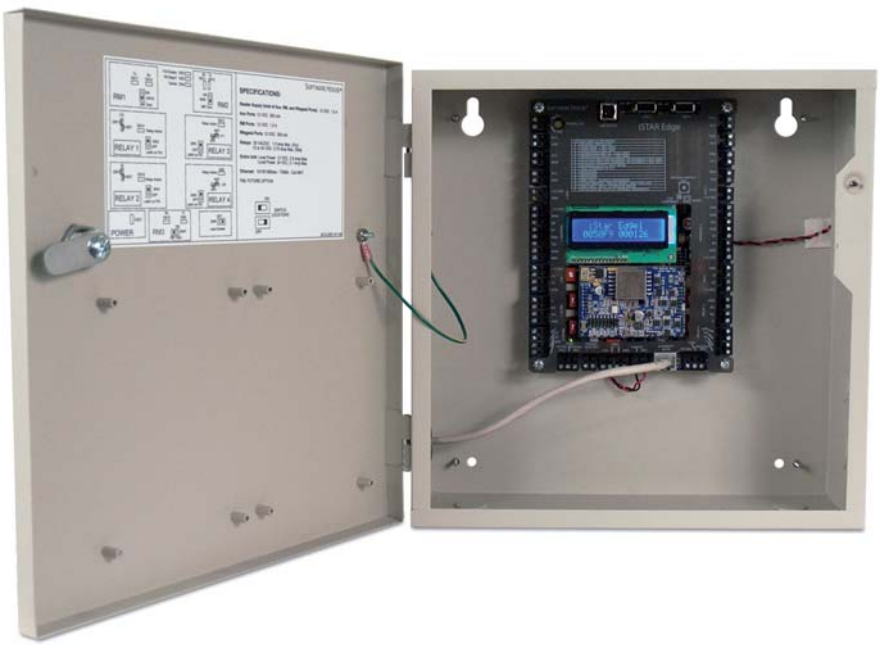
Dane techniczne	
Napięcie zasilania	$24V_{DC}$ (18 ÷ 30 V_{DC})
Pobór prądu	220 mA praca, 295 mA w alarmie
Zabezpieczenie	1,5 A
Wymiary	245 mm × 175 mm × 90 mm
Montaż	pionowy, poziomy, odwrócony
Masa	2 kg
Klasa IP	IP30
Temperatura otoczenia	0°C – 40°C
Temperatura zasysanego powietrza	0°C – 40°C
Wilgotność względna	5 ÷ 95%, bez kondensacji
Maksymalna powierzchnia dozorowana	250 m^2 / 500m^2
Maksymalna długość rury	25m / 50m
Program wspomaganie projektowania	ASPIRE2™
3 przekaźniki o obciążalności styków 2A/30VDC (Pożar1, Akcja, Uszkodzenie)	
Programowanie przekaźników	z zatrzaskiem / bez zatrzasku
Zakres czułości	0,025 do 20% / m
Zakres nastaw progów alarmowych	Alarm, Akcja: 0,025 – 2,0% / m Pożar1, Pożar2: 0,025 – 20,00% / m Opóźnienie: 0 – 60 s
Pamięć zdarzeń	18000 ostatnich zdarzeń
Monitorowanie	wypełnienie filtra, przepływ powietrza
Gwarancja	2 lata

Cechy systemu

- Zredukowane wymiary
- Ultradźwiękowa analiza przepływu powietrza
- Detekcja dymu oparta na technologii laserowej
- Projektowana sieć rur ssących
- Programowalne progi alarmowe
- Wskaźnika stany zadymienia widoczny na wielopoziomowym wyświetlaczu
- Dwustopniowy filtr powietrza
- System wykrywania uszkodzeń Fault Finder™
- Funkcja AutoLearn™ zadymienia
- Funkcja AutoLearn™ przepływu
- Zamykany, serwisowy panel obsługi
- Historia zdarzeń 18000 rekordów
- Możliwość konfiguracji offline/online
- Ochrona powierzchni do 250m^2 / 500m^2

Dystrybucja:
Vision Polska®
Vision Polska Sp. z o.o.
ul. Unii Lubelskiej 1, 61-249 Poznań
tel. (61) 623 23 05, (61) 623 23 05
faks (61) 623 23 17
e-mail: biuro@visionpolska.pl
http://www.vesda.pl/

Kontroler IP iSTAR Edge obsługujący 2 czytniki



iSTAR Edge jest niezawodnym urządzeniem IP obsługującym 2 czytniki, dostarczającym jednocześnie zestaw funkcji, w skład których wchodzą zaawansowane opcje łączenia w klastry, komunikacja peer-to-peer, strefy włamań i polecenia z klawiatury, zaawansowane funkcje monitorowania drzwi i globalny anty-passback. Opcjonalny moduł zasilający Power over Ethernet (PoE) jest w stanie zasilić urządzenia kontroli dostępu w obrębie 2 drzwi i pozwala wykorzystać istniejącą infrastrukturę sieciową, aby zredukować całkowity koszt instalacji systemu.

iSTAR Edge zwiększa ogólną niezawodność i funkcjonalność systemu poprzez umiejscowienie podejmowania decyzji w lokalnej bazie danych, znajdującej się w każdym kontrolerze, obsługę rekordów 400 000 użytkowników, buforowanie lokalnych alarmów i zdarzeń w przypadku, gdy nie jest możliwa komunikacja z komputerem - hostem. iSTAR Edge komunikuje się z oprogramowaniem C•CURE 800 v.10.0, C•CURE 9000 i innymi kontrolerami Software House, zapewniając realizację funkcji stawianych i wykorzystanych przez najbardziej wymagających użytkowników. Nie ma różnicy, czy system zainstalowany jest w głównej siedzibie firmy, gdzie zatrudnionych jest tysiące pracowników, czy też w lokalnych biurach z kilkoma pracownikami. iSTAR Edge zapewnia w każdym miejscu realizację tych samych procedur i zasad bezpieczeństwa.

iSTAR Edge dostarcza rozwiązania stosowvane w systemach bezpieczeństwa nie mające sobie równych w tej branży. Ze względu na swoją wszechstronność i bezpieczeństwo kontrolery iSTAR Edge mogą być używane razem z kontrolerami iSTAR Pro i iSTAR eX stanowiąc doskonałe rozwiązanie korporacyjne.

iSTAR Edge został zaprojektowany, aby radykalnie zmniejszyć koszt instalacji i uruchomienia systemu. Wbudowana funkcja zarządzania zasilaniem, eliminuje potrzebę stosowania dodatkowego zasilacza i zabezpieczeń stosowanych w tradycyjnych instalacjach. Podłączenie przy pomocy wymiennych złącz, wbudowanego wyświetlacza i diod LED wskazujących aktualny stan kontrolera iSTAR Edge, w znacznym stopniu ułatwia instalacje w najtrudniejszych warunkach. Ponadto, zdalna diagnostyka systemu poprzez przeglądarkę internetową, umożliwia zidentyfikowanie i rozwiązanie problemów związanych z wydajnością systemu.

Obudowa iSTAR Edge daje możliwość instalacji dodatkowych modułów I/O i jest zabezpieczona czujnikiem otwarcia w przypadku nieautoryzowanej próby ingerencji w urządzenie. Zagrożenia bezpieczeństwa zostały znacząco zredukowane poprzez szyfrowaną komunikację, zabezpieczenie przed niepożądanym atakiem na system komputerowy czy usługi sieciowe, tworząc kontroler iSTAR Edge urządzeniem o najwyższym poziomie bezpieczeństwa – idealnym rozwiązaniem nawet dla najbardziej sceptycznych managerów IT.

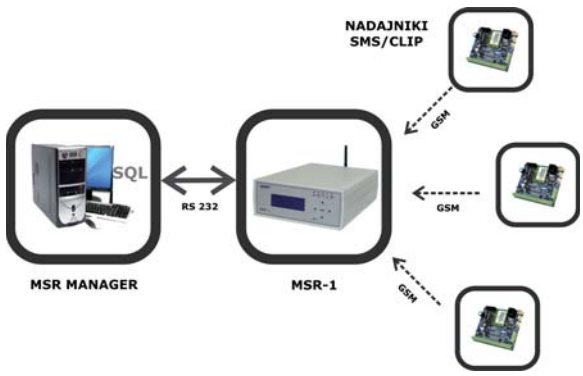
Dystrybucja:

KATON
ACCESS CONTROL & SECURITY SYSTEMS

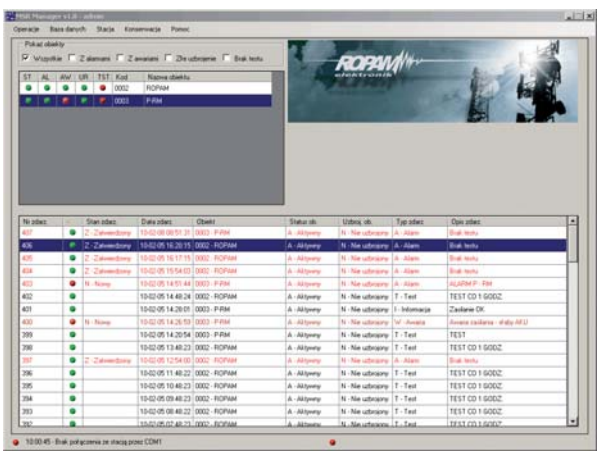
Katon Sp. z o.o.
ul. Bajana 31E
01-904 Warszawa

tel. (22) 869 43 92
e-mail: biuro@katon.eu
http://www.katon.eu

Stacja monitorowania MSR-1 & MSR Manager



Stacja monitorowania MSR-1 wraz z oprogramowaniem MSR Manager to nowoczesne rozwiązanie dedykowane do monitoringu poprzez SMS / CLIP. System składa się z autonomicznego odbiornika MSR-1 w obudowie typu desktop oraz aplikacji bazodanowej do zarządzania sygnałami i obiektami. Odbiornik pozwala na odbiór sygnałów SMS/CLIP (CID CallerID) z modułów GSM marki Ropam lub innych zgodnych. Oprogramowanie to licencyjna aplikacja jednostanowiskowa pracująca w środowisku WINDOWS.



Odbiornik MSR-1

- autonomiczna konstrukcja pozwalająca na okresową pracę off-line
- port RS232 do komunikacji z MSR Manager
- lokalny bufor zdarzeń (500) podczas pracy off-line
- estetyczna obudowa z ABS typu 'desktop'
- duży podświetlany wyświetlacz LCD i klawiatura
- dodatkowa sygnalizacja LED i akustyczna
- zasilanie 230 V_{AC}
- wbudowane zasilanie awaryjne
- wbudowany przemysłowy modem GSM
- przystosowana do odbioru informacji nadawanych przez nadajniki GSM: SMS/CLIP
- możliwość podłączenia dużej ilości obiektów
- funkcja uaktualnienia oprogramowania (firmware)

Oprogramowanie MSR Manager

- licencja dla jednego stanowiska
- aplikacja bazodanowa (SQL)
- praca w środowisku WINDOWS
- łatwa instalacja i konfiguracja
- przyjazna obsługa i prezentacja zdarzeń
- wielopoziomowa struktura dostępu
- rozbudowane funkcje filtracji i przeszukiwania bazy danej
- funkcje eksportu ustawień
- funkcja tworzenia kopii zapasowych bazy danej
- możliwość szybkiej re-instalacji i odtworzenia bazy danej i ustawień
- małe wymagania sprzętowe

Przeznaczenie

System przeznaczony jest do monitoringu sygnałów alarmowych, technicznych, awaryjnych z nadajników GSM pracujących w standardzie SMS /CLIP. Rozwiązanie dedykowane jest do obsługi małych i średnich obiektów (do 1000 obiektów). Dzięki uniwersalnym funkcjom, elastycznemu oprogramowaniu szczególnie zalecane jest do monitoringu:

- systemów alarmowych i kontroli dostępu
- układów automatyki np. przepompownie, studnie
- systemów teletechnicznych
- serwerowni
- systemów awaryjnego zasilania np. USP-y, agregaty prądotwórcze
- sygnałów serwisowych
- ferm hodowlanych itp.

Dystrybucja:

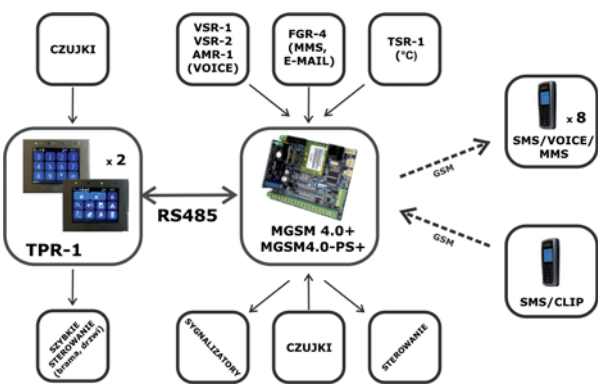
ROPAM elektronik

Ropam Elektronik s.c.
Os.1000-lecia 6A/1
32-400 Myślenice

tel. (12) 379 34 47, tel./faks (12) 272 39 71
e-mail: biuro@ropam.com.pl
http://www.ropam.com.pl

Panel dotykowy TPR-1

Panel dotykowy TPR-1 to nowoczesny element sterowania i kontroli systemu alarmowego. TPR-1 zbudowany jest w oparciu o kolorowy wyświetlacz TFT LCD z panelem dotykowym. Obudowę wykonano z matowej stali nierdzewnej „INOX" co tworzy w całości solidny i estetyczny wygląd, pasujący do większości wnętrz i podkreślający funkcje urządzenia. TPR-1 pozwala na intuicyjne sterowanie i kontrolę systemu alarmowego, dzięki interaktywnemu interfejsowi, który wykorzystuje piktogramy i podpowiedzi tekstowe. Nawigowanie i używanie funkcji jest proste i nie wymaga od użytkownika pamiętania kodu funkcji np. czuwanie nocne, blokowanie czujników. Panel posiada cztery diody LED do sygnalizacji statusu oraz pasek piktogramów na którym na bieżąco prezentuje wszystkie ważne informacje m.in. stan zasilania, zasięg GSM, GPRS, temperaturę.



Cechy charakterystyczne

- kolorowy wyświetlacz 3,5" TFT LCD
- panel dotykowy „Touch Panel", bez mechanicznych styków
- interaktywne graficzne menu z piktogramami (ikony)
- funkcja losowego układu klawiatury numerycznej
- tekstowe podpowiedzi dla danych funkcji
- intuicyjna kontrola i sterowanie systemem
- sterowanie wyjściami modułu
- szybkie sterowanie wyjściem przekaźnikowym w TPR-1
- diody LED statusu systemu
- pasek dodatkowych informacji o stanie systemu
- sygnalizacja akustyczna
- wygaszacz ekranu z funkcją kalendarza i zegara
- wbudowany czujnik temperatury
- dwa wejścia alarmowe
- magistrala RS485 do komunikacji systemowej
- lokalny port RS232TTL
- funkcja uaktualnienia oprogramowania
- estetyczna i solidna obudowa z matowej stali nierdzewnej „INOX"
- zabezpieczenie antysabotażowe obudowy
- rozłączne listwy zaciskowe
- współpraca z modułami MGSM 4.0+, MGSM 4.0-PS+ i przyszłymi produktami

Przeznaczenie

System alarmowy zbudowany w oparciu o TPR-1 i sprawdzone moduły GSM Ropam Elektronik to idealne rozwiązanie dla obiektów mieszkalnych i małych obiektów komercyjnych. Nowoczesna stylistyka, sprawdzona technologia panelu dotykowego z efektownym kolorowym wyświetlaczem LCD doskonale nadaje się do komponowania w większości wnętrz i pomieszczeń. Intuicyjny i przejrzysty interfejs powoduje, że sterowanie systemem alarmowym nigdy nie było tak proste jak z TPR-1. Panel TPR-1 w połączeniu z modułami serii MGSM 4.0+/4.0-PS+ pozwala na zbudowanie w pełni funkcjonalnego systemu alarmowego. Przy wykorzystaniu dwóch paneli otrzymujemy system w konfiguracji: 12 wejść, 8 wyjść, jedna strefa z czuwaniem nocnym oraz z wbudowaną komunikacją i sterowaniem GSM.

Dystrybucja:

ROPAM elektronik

Ropam Elektronik s.c.
Os.1000-lecia 6A/1
32-400 Myślenice

tel. (12) 379 34 47, tel./faks (12) 272 39 71
e-mail: biuro@ropam.com.pl
http://www.ropam.com.pl

Zestawy do programowania kart EM 125 kHz oraz 13.56 MHz Mifare

CPK-1

Zestaw do programowania kart standardu EM 125 kHz z chipem Q5 (karty EMC-4). W skład zestawu wchodzą: czytnik PRT66EM, 10 niezaprogramowanych kart zbliżeniowych, interfejs komunikacyjny RUD-1, CD-ROM z programem RARC oraz kluczem licencyjnym.

CPK-2

Zestaw do programowania kart standardu Mifare 13.56 MHz. W skład zestawu wchodzą: czytnik PRT66MF, 10 kart zbliżeniowych Ultralight, interfejs komunikacyjny RUD-1, CD-ROM z programem RARC oraz kluczem licencyjnym.

PRT66EM

Zewnętrzny czytnik/programator kart EM 125 kHz z układem Q5.

PRT66MF

Zewnętrzny czytnik/programator kart standardu ISO/IEC 14443A i Mifare.

RUD-1

Uniwersalny, przenośny interfejs komunikacyjny USB-RS485, zasilany bezpośrednio z gniazdka USB, posiada wbudowaną przetwornicę impulsową (12V) do zasilania programowanego urządzenia.

RARC

Program RARC służy do obsługi czytników serii PRTxxEM oraz PRTxxMF. Podstawowa wersja programu umożliwia pełne skonfigurowanie czytnika, a także ściąganie zdarzeń zarejestrowanych w jego pamięci i jest bezpłatna.

RARC-LICENSE

Licencja umożliwiająca wykorzystanie czytników PRTxxEM i PRTxxMF do programowania kart zbliżeniowych.

Produkcja: roger®

Roger Sp. j.
Gościszewo 59
82-400 Sztum, woj. pomorskie

tel. (55) 272 01 32, faks (55) 272 01 33
e-mail: roger@roger.pl
http://www.roger.pl

SL2000F & SL2000F-VP
Nowe zamki szyfrowe serii SL2000

Elektroniczne zamki szyfrowe serii SL2000 zostały zaprojektowane jako proste i tanie urządzenia kontroli dostępu bazujące na identyfikacji użytkowników za pomocą kodów PIN. Wszystkie zamki serii SL2000 oferują tą samą funkcjonalność, a różnią się stylistyką obudowy, konstrukcją mechaniczną oraz środowiskiem pracy (praca na zewnątrz lub wewnątrz budynków).

SL2000F

- wewnętrzny zamek szyfrowy
- obudowa z ABS
- zaciski śrubowe
- klawiatura silikonowa z podświetleniem
- możliwość instalacji bezpośrednio na puszce elektroinstalacyjnej 60 mm

SL2000F-VP

- zewnętrzny, wandaloodporny zamek szyfrowy
- górny korpus obudowy oraz klawisze wykonane ze stopu aluminium i pokryte powłoką w kolorze srebrny metalik
- kabel podłączeniowy 0,5 m
- możliwość instalacji bezpośrednio na puszce elektroinstalacyjnej 60 mm

Charakterystyka

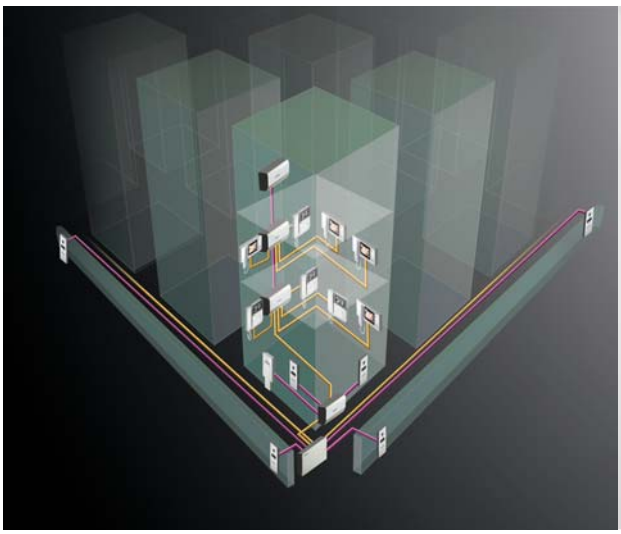
- jedno wyjście przekaźnikowe 1.5A/30V oraz dwa wyjścia tranzystorowe
- sygnalizacja alarmów na wyjściu tranzystorowym ALARM
- współpraca z czujnikiem otwarcia drzwi
- możliwość podłączenia przycisku wyjścia od środka
- kod administratora do celów programowania i zarządzania kodami użytkowników
- kod główny do zmiany aktualnego stanu uzbrojenia zamka
- 55 kodów użytkowników posiadających uprawnienie do otwarcia drzwi
- możliwość czasowej blokady zamka po trzykrotnym wprowadzeniu błędnego kodu
- możliwość blokady dostępu, gdy zamek jest w trybie uzbrojenia
- programowalna długość kodów
- indeksowanie użytkowników
- nieulotna pamięć
- trzy wskaźniki LED oraz Buzzer
- zasilanie 10-15VDC
- ochrona antysabotażowa (tamper)
- znak CE

Produkcja: roger®

Roger Sp. j.
Gościszewo 59
82-400 Sztum, woj. pomorskie

tel. (55) 272 01 32, faks (55) 272 01 33
e-mail: roger@roger.pl
http://www.roger.pl

System wieloabonentowy serii 2400

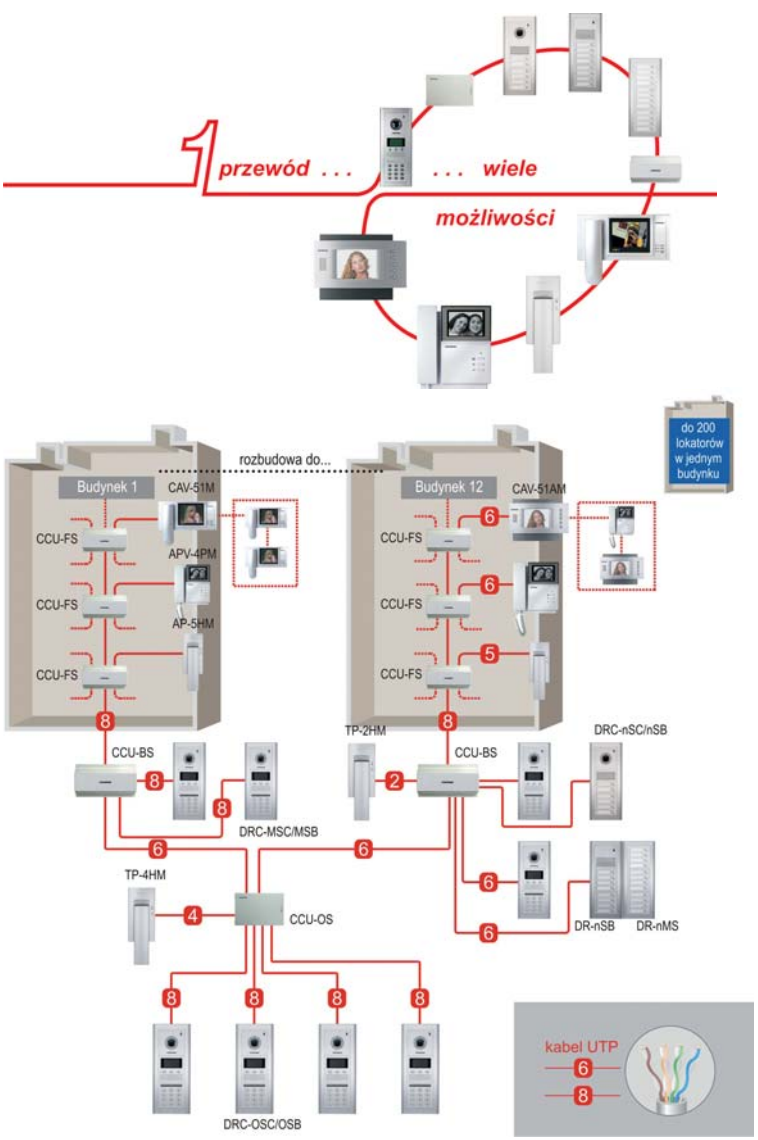


System wieloabonentowy serii 2400 przeznaczony jest do instalacji zarówno w prostych, jak i w bardzo rozbudowanych aplikacjach - maksymalna liczba obsługiwanych przez system abonentów wynosi 2400. U każdego lokatora może być zainstalowane do 3 urządzeń (jedno urządzenie typu Master i dwa urządzenia typu Slave).

Lokator może mieć zainstalowany prosty unifon, umożliwiający kontakt głosowy z osobą odwiedzającą, jak i monitor (czarno-biały lub kolorowy), pozwalający także na obserwację wizualną osoby odwiedzającej.

System umożliwia zastosowanie zarówno paneli zewnętrznych audio, jak wideo - wyposażonych w moduł kamery (czarno-biały lub kolorowy). Panele zewnętrzne występują w wersji przyciskowej lub z klawiaturą numeryczną (umożliwiającą dodatkowo wybór lokatora za pomocą spisu lokatorów oraz otwieranie zamka elektrycznego przy użyciu indywidualnych kodów).

System może być wyposażony w unifon instalowany w portierni, przez co lokatorzy mogą mieć kontakt z osobą dozorującą (portierem). Dzięki dużej elastyczności możliwe jest skonfigurowanie systemu dla małych, pojedynczych bloków, jak i całych osiedli zamkniętych, gdzie ogrodzonych może być klikanaście budynków, a całość jest nadzorowana przez kilku portierów.



Dystrybucja:

GDE POLSKA
Global Distributor of Electronics

GDE POLSKA
Włosań, ul. Świątnicka 88
32-031 Mogilany

tel./faks (12) 256 50 35, 256 50 25
faks (12) 270 56 96
e-mail: biuro@gde.pl

Zwory elektromagnetyczne SCOT

Zwory elektromagnetyczne SCOT są alternatywą dla powszechnie stosowanych w systemach kontroli dostępu elektrozaczepów. Zwora składa się z elementu wykonawczego zawierającego elektromagnes, montowanego na ramie drzwi, oraz metalowej płytki – zwornika, umieszczanej na skrzydle drzwi. Zasilona cewka elektromagnesu przyciąga zwornik, co uniemożliwia otwarcie skrzydła drzwi i zabezpiecza w ten sposób wejście. W zależności od modelu zwory maksymalny nacisk na drzwi przy którym elektromagnes utrzymuje kontakt ze zwornikiem wynosi 180, 280, 350, 540 kg. Wszystkie zwory elektromagnetyczne SCOT przystosowane są do pracy z napięciem 12 lub 24 V_{DC}.

Zwory elektromagnetyczne stosuje się w systemach kontroli dostępu zamiennie z elektrozaczepami rewersyjnymi, wszędzie tam, gdzie przepisy bezpieczeństwa wymagają otwarcia drzwi po zaniku napięcia w systemie kontroli dostępu (np. podczas pożaru instalacji elektrycznej). W obwód zasilania zwory elektromagnetycznej można włączyć również przycisk wyjścia alarmowego, umożliwiając dodatkowo otwarcie drzwi w sytuacjach awaryjnych. Najczęściej tego typu zamki elektryczne instaluje się na wyjściach ewakuacyjnych, przeciwpożarowych i w budynkach użyteczności publicznej.

Zwora elektromagnetyczna nie posiada ruchomych elementów mechanicznych, przez co praktycznie nie występuje zużycie elementów urządzenia. Z tego względu stosowana jest w miejscach o dużym natężeniu ruchu, gdzie kontrolowane drzwi są często otwierane. Zmniejsza to częstotliwość zabiegów konserwacyjnych i serwisowych. Dodatkowe uchwyty montażowe typu „L", „ZL", „UL" pozwalają na montaż zwory praktycznie na każdych drzwiach.

Sygnalizacja

Zwora elektromagnetyczna wyposażona jest w przekaźnik NO/NC, który może być wykorzystany w systemie kontroli dostępu informując o otwarciu / zamknięciu sterowanych drzwi. Dzięki temu możemy przekazać informację np. do systemu alarmowego, informując o stanie drzwi.

Dioda LED

Na obudowie zwory znajduje się dwukolorowa dioda informująca o stanie kontrolowanego przejścia. Jeżeli drzwi są zamknięte i na zworę podane jest napięcie zasilające, jest to sygnalizowane zielonym kolorem świecenia diody – jeżeli drzwi zostaną otwarte lub będą niedomknięte – dioda będzie świecić kolorem czerwonym. Jeżeli cewka zwory elektromagnetycznej nie jest zasilana (np. podczas trwania impulsu sterującego) – dioda jest wygaszona.

Model	Maksymalny nacisk na drzwi	Sygnalizacja	Dioda LED	Zasilanie	Wymiary
EL-350	180 kg	–	–	12V_{DC} / 300mA lub 24V_{DC} / 150mA	170 x 41 x 20 mm
EL-350S	180 kg	NC	–	12V_{DC} / 300mA lub 24V_{DC} / 150mA	183 x 41 x 20 mm
EL-600SL	280 kg	NO/NC	+	12V_{DC} / 480mA lub 24V_{DC} / 240mA	250 x 48 x 26 mm
EL-600TSL	280 kg	NO/NC	+	12V_{DC} / 480mA lub 24V_{DC} / 240mA	250 x 48 x 26 mm
EL-800SL	350 kg	NO/NC	+	12V_{DC} / 500mA lub 24V_{DC} / 250mA	285 x 55 x 29 mm
EL-800WS	350 kg	NC	–	12V_{DC} / 500mA	228 x 52 x 27 mm
EL-800DSL	2 x 350 kg	NO/NC	+	2 x 12V_{DC} / 500mA lub 2 x 24V_{DC} / 250mA	570 x 55 x 29 mm
EL-1200SL	540 kg	NO/NC	+	12V_{DC} / 420mA lub 24V_{DC} / 210mA	265 x 75 x 40 mm
EL-1200DSL	2 x 540 kg	NO/NC	+	2 x 12V_{DC} / 420mA lub 2 x 24V_{DC} / 210mA	530 x 75 x 40 mm

Dystrybucja: GDE POLSKA
Global Distributor of Electronics
GDE POLSKA
Włosań, ul. Świątnicka 88
32-031 Mogilany
tel./faks (12) 256 50 35, 256 50 25
faks (12) 270 56 96
e-mail: biuro@gde.pl

Kamera kopułowa V2810PVR

CNB TECHNOLOGY Inc.

Najważniejsze funkcje wandaloodpornej kamery kopułowej V2810PVR to:

- wysoka rozdzielczość 550 TVL
- funkcja DSS (Digital Slow Shutter) regulowana w zakresie do 32 obrazów
- mechaniczny filtr podczerwieni, tryb kolorowy i czarnobiały
- efektywny zasięg promiennika podczerwieni do 15 m
- wyjście serwisowe sygnału wizji
- trzyosiowa regulacja położenia modułu kamery
- wbudowany obiektyw o zmiennej ogniskowej 3,8÷9,5 mm z automatyczną przysłoną DC
- estetyczna obudowa

Kompaktowe kamery B2810PVF oraz B2310PVF posiadają podobną funkcjonalność do powyższej kamery.

Właściwości:

- kamera dzień/noc
- przetwornik 1/3" Sony Super HAD
- wysoka rozdzielczość 550 TVL
- mechaniczny filtr podczerwieni TDN (ICR)
- czułość: 0,3 lx (kolor), 0,1 lx (B/W), 0,008 lx (DSSx32, kolor), 0,0008 lx (DSSx32, B/W), 0 lx (IR LED włączone)
- obiektyw 3,8 ÷ 9,5 mm
- cyfrowy zoom
- AGC, Flickerless, BLC, D/N, DSS, zoom
- obudowa kopułkowa o średnicy 100 mm

Dane techniczne	
Model	V2810PVR
Standard sygnału wideo	PAL
System skanowania	2:1 z przeplotem
Częstotliwość skanowania w poziomie (H)	15,625 kHz
Częstotliwość skanowania w pionie (V)	50 Hz
Przetwornik	1/3" SONY Super HAD CCD
Rozdzielczość efektywna	752(H) × 582(V) 440K
Liczba linii	550 TVL
Wyjście wideo	1,0V p-p, 75 Ohm
Odstęp sygnał/szum	>50dB
Obiektyw	f=3,8 ÷ 9,5 mm, F1,2
Cyfrowy zoom	2×
Tryb dzień/noc	mechaniczny filtr IR z czujnikiem
Podczerwień	IR LED 20EA (850nm, 30°), czujnik 1EA
Zasięg doświetlenia	max. 15 m
Czułość	0,3 lx / 0,00 lx (IR LED włączone)
Cyfrowa redukcja szumu	automatyczna, SDNR
Balans bieli	automatyczny
Funkcja DSS	do 32 ramek obrazu
Automatyczna regulacja wzmocnienia (AGC)	tak
Kompensacja światła tylnego	BLC, Wł. / Wył.
Redukcja migotania	Wł./Wył.
Odbicie lustrzane obrazu	w poziomie
Elektroniczna migawka	1/50 ~ 1/120 000 sek.
Stopień ochrony IP	IP65
Zasilanie	$12V_{DC}$ / $24V_{AC}$
Pobór prądu	max. 500 mA
Wymiary (Ø x wys.)	montaż natynkowy: 100 x 124,5 mm montaż podtynkowy: 100 x 111 mm
Temperatura pracy / Wilgotność	-10°C~45°C / 30%~80% RH
Masa	1130 g

Kamera kopułowa DFL-21S

CNB TECHNOLOGY Inc.

MONALISA

Kopułowa kamera DFL-21S o wysokiej czułości i bardzo wysokiej rozdzielczości (600 TVL w trybie kolorowym, 650 TVL w trybie B/W) wyróżnia się wierną reprodukcją kolorów. Kamera dedykowana jest do zastosowań wewnętrznych. Powyższe cechy są konsekwencją zastosowania wysokiej jakości procesora DSP „Monalisa".

Kamera wyróżnia się:

- Trzyosiową regulacją położenia modułu kamery: regulacja pionowa, pozioma oraz obrót wokół własnej osi
- SBLC – ulepszona odmiana BLC, czyli kompensacji światła tylnego

Kamera DBM-21VD cechuje się podobną funkcjonalnością, dodatkowo została wzbogacona o ekranowe menu (OSD) i obiektyw ze zmienną ogniskową 4÷9 mm.

Właściwości:

- kamera dzień/noc
- przetwornik 1/3" Sony Super HAD II
- bardzo wysoka rozdzielczość 600 TVL (kolor) / 650 TVL (B/W)
- automatyczny tryb pracy dzień/noc,
- czułość 0,05 lx (tryb kolorowy)
- obiektyw 3,8 mm
- AGC, SBLC, AWB
- zasilanie 12 V DC
- obudowa kopułkowa o średnicy 85 mm

Dane techniczne	
Model	DFL-21S
Standard sygnału wideo	PAL
System skanowania	2:1 z przeplotem
Częstotliwość skanowania w poziomie (H)	15,625 kHz
Częstotliwość skanowania w pionie (V)	50 Hz
Przetwornik	1/3" SONY Super HAD CCD
Rozdzielczość efektywna	752(H) × 582(V) 440K
Liczba linii	600 TVL
Wyjście wideo	1,0V p-p, 75 Ohm
Odstęp sygnał/szum	>50 dB
Obiektyw	f=3,8 mm
Tryb dzień/noc	auto
Czułość	0,05 lx
Balans bieli	automatyczny
Automatyczna regulacja wzmocnienia (AGC)	tak
Kompensacja światła tylnego	SBLC, automatyczna
Elektroniczna migawka	1/50~1/120 000 s
Zasilanie	12 V_{DC}
Pobór prądu	maks. 150 mA
Wymiary (Ø x wys.)	113,2 × 79,15 mm
Temperatura pracy / Wilgotność	-10°C~45°C / 30%~80% RH
Masa	210 g

Dystrybucja: GDE POLSKA Global Distributor of Electronics
GDE POLSKA
Włosań, ul. Świątnicka 88
32-031 Mogilany
tel./faks (12) 256 50 35, 256 50 25
faks (12) 270 56 96
e-mail: biuro@gde.pl

GOLD-PLUS inteligentny tester akumulatorów z ręczną kalibracją

Inteligentny Tester Akumulatorów GOLD-PLUS został zaprojektowany do testowania akumulatorów 6-voltowych o pojemności od 1,2 h do 12 Ah oraz 12-voltowych o pojemności od 1,2 Ah do 100 Ah. Zastosowana technologia symulacji pełnego rozładowania skraca normalny test rozładowania z 20 godzin do 20 sekund. Automatycznie wyświetla napięcie akumulatora i aktualną pojemność. Dzięki funkcji kalibracji testera możliwe jest testowanie szczelnych akumulatorów (SLA) wykonanych w technologii AGM, żelowych do pracy cyklicznej oraz akumulatorów samochodowych. Akumulatory można testować wielokrotnie bez przerw pomiędzy pomiarami. Wbudowana dioda LED ostrzega przed odwróceniem polaryzacji.

Wymiana akumulatora jest zalecana, jeżeli jego współczynnik pojemności spada poniżej 65%. Na obudowie umieszczona jest tabela referencyjna wskazująca, kiedy akumulator powinien zostać doładowany lub wymieniony.

Cechy charakterystyczne

- Testuje w ciągu 20 sekund 6- i 12-voltowe szczelne akumulatory (SLA) - AGM i żelowe oraz akumulatory samochodowe,
- automatycznie wyświetla napięcie akumulatora i aktualną pojemność,
- może być skalibrowany do testowania akumulatorów szczelnych, żelowych i samochodowych o pojemności od 1,2 Ah do 100 Ah,
- zabezpieczony przed odwróceniem polaryzacji,
- testuje akumulatory szybko, dokładnie i jest łatwy w użyciu,
- zastosowanie – akumulatory w systemach alarmowych, zasilaczach UPS, samochodach elektrycznych i spalinowych.

Parametry techniczne	
Model	GOLD- PLUS
Typy akumulatorów	szczelne (SLA) – AGM i żelowe samochodowe akumulatory obsługowe
Pojemność akumulatorów	6 V 1,2 Ah – 12 Ah oraz 12 V 1,2Ah – 100 Ah
Impulsowe obciążenie akumulatora podczas pomiaru	6 A dla akumulatorów 1,2Ah – 9,9Ah, 18 A dla akumulatorów 10Ah – 100Ah
Kalibracja Ah	Kalibrowany w pozycji 0 dla nowego, w pełni naładowanego akumulatora SLA o temperaturze 20-25 °C. Regulacja kalibracji w zakresie 00-99 dla akumulatorów żelowych i samochodowych
Wyświetlacz	podświetlany LCD
Ostrzeżenie o odwróconej polaryzacji	czerwona dioda LED
Ostrzeżenie o zbyt niskim napięciu akumulatora	dla 6V < 5,25 V_{DC}, dla 12 V <12,0 V_{DC}
Tolerancja pomiaru Ah	+/- 10 % (zależy od konstrukcji i parametrów produkcyjnych)
Tolerancja pomiaru VDC	+/- 2 %
Zabezpieczenie odwrócenia polaryzacji	tak
Zdolność wykonania kolejnych testów	natychmiastowa
Obudowa	ABS
Szczelność	IP54
Wymiary	210 mm × 110 mm × 41 mm
Masa	600 g (w opakowaniu)
Wyposażenie	Przewody testowe, futerał, certyfikat zgodności, etykiety na akumulatory
Gwarancja	1 rok

Dystrybucja: alarmnet®

Alarmnet 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
http://www.alarmnet.com.pl

Rejestratory cyfrowe 4-, 8- i 16-kanałowe 4sec serii LCD

Zintegrowane rejestratory serii 4SEC2000LCD posiadają funkcjonalność kompletnego stanowiska nadzoru CCTV. Wysokiej klasy monitory LCD przeznaczone do pracy ciągłej zapewniają doskonały obraz. Przyciski i pokrętła poniżej monitora oraz pilot pozwalają na sterowanie zapisem i podglądem z kamer, podłączenie do sieci Internet pozwala na zdalne sterowanie oraz podgląd obrazu nawet na telefonie komórkowym.

Dzięki zastosowaniu podwójnego kodowania, obraz zapisany w kompresji JPEG2000 ma doskonałą jakość, a dzięki kompresji H.264 transmisja sieciowa nie ma zbyt wygórowanych wymagań przepustowości łącza.

Dane techniczne			
Model	4SEC2004LCD10	4SEC2008LCD19	4SEC2016LCD19
Monitor TFT-LCD	10,2" WVGA	19" SXGA	19" SXGA
Ilość wejść wideo	4	8 przelotowych	16 przelotowych
Audio	4 wejścia 1 wyjście		
Kompresja	JPEG2000 – zapis i odtwarzanie / H.264 – transmisja przez sieć LAN		
Wyjścia wideo	Monitor / spot		
Dyski	1 SATA	2 SATA	
Podział ekranu	1, 4	1, 4, 6, 8, 9	1, 4, 6, 8, 9, 13, 16
Rozdzielczość zapisu	Pełny ekran – 720×288, podział – 360×288		
Prędkość zapisu (PAL)	50 fps (720×288) 100 fps (360×288)	100 fps (720×288) 200 fps (360×288)	
Prędkość podglądu	W czasie rzeczywistym dla wszystkich kanałów		
Wielozadaniowość	Triplex (Odtwarzanie / Zapis / Ethernet)		
PIP / ZOOM	Tak / Tak		
Detekcja ruchu	Strefa 16×12		
Tryby zapisu	Ciągły / Detekcja / Kalendarz / Alarm / Ręczny		
Wyszukiwanie zapisu	Procent zapisu / Data&Czas / Zdarzenia		
Zabezpieczenie	Hasła: Administratora, Managera oraz 8 użytkowników		
Wejścia alarmowe	4 (NO/NC)	8 (NO/NC)	16 (NO/NC)
Wyjścia	1 przekaźnikowe		
Archiwizacja	USB / Zdalne oprogramowanie		
Temperatura pracy	od 5°C do 40°C		
Wilgotność	< 90%		
Wymiary (SxWxG)	282×325×180 mm	418×440×230 mm	
Masa	ok. 6 kg (bez dysków)	ok. 10 kg (bez dysków)	
Zasilanie	12 V_{DC} (zasilacz w komplecie)		

JPEG2000 – najlepsza jakość zapisanego materiału, H.264 – najszybsza transmisja

Podgląd zdalny może być realizowany przez załączone oprogramowanie klienta, przeglądarkę internetową, telefon komórkowy lub w przypadku systemów wielostanowiskowych przez CMS (Centralny System Monitorowania). Dzięki zwartej obudowie rejestrator nie zajmuje więcej miejsca niż standardowy monitor LCD.

Cechy

- Podwójny algorytm kompresji:
  - Zapis i odtwarzanie JPEG2000
  - Transmisja przez Internet H.264
- Wysoka jakość zapisanego materiału
- Tryb pracy – Duplex / Triplex
- Złącze USB do archiwizacji danych
- Sterowanie PTZ
- Wygodne wyszukiwanie i przeglądanie materiału
- Łącze USB do aktualizacji oprogramowania
- Menu w języku polskim
- Zdalne oprogramowanie
- DDNS
- Pilot
- Audio: 4 wejścia, 1 wyjście

Dystrybucja: alarmnet®

Alarmnet 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
http://www.alarmnet.com.pl

Pronto – Drukarka do kart identyfikacyjnych

Pronto

MAGICARD

Mała, kompaktowa drukarka o nowoczesnym wyglądzie do zastosowania w każdej firmie i w każdym miejscu. Do szybkiego drukowania identyfikatorów oraz różnego rodzaju kart plastikowych. Drukarka Pronto jest łatwa w konfiguracji i użytkowaniu, posiada instrukcję i sterowniki w języku polskim do Windows 2000, XP, Vista, 7 i zapewnia niezawodne drukowanie kart przez wiele lat. Drukarka Magicard Pronto umożliwia wykorzystanie HoloKote™ i HoloPatch™ – opatentowanych zabezpieczeń przed nieautoryzowanym kopiowaniem kart.

Dzięki drukarce Pronto samodzielnie wykonasz kolorowe i monochromatyczne nadruki wysokiej jakości.

Specyfikacja techniczna

- Wydruk karty w kolorze od krawędzi do krawędzi w 35 sekund
- Monochromatyczny wydruk karty w 7 sekund
- TRW - Thermal Rewritable (wielokrotny zadruk termiczny)
- Interfejs do PC: USB rev. 1.1. (kompatybilny z USB 2.0)
- Sterowniki w języku polskim: Windows 2000, XP, Vista, 7
- Rozdzielczość wydruku: 300 dpi
- Zasilanie: 90-265 V / 47-63 Hz
- Wymiary / Masa: 270 mm × 215 mm × 233 mm / 4,4 kg
- Temperatura pracy: od 10°C do 30°C
- Gwarancja: 2 lata

Taśmy

- YMCKO 5 paneli nadruk 300 kart (MA300YMCKO)
- YMCKO 5 paneli nadruk 100 kart (MA100YMCKO)
- Monochromatyczna czarna nadruk 1000 kart (MA1000K-BLACK)
- Monochromatyczna czarna plus overlay nadruk 600 kart (MA600KO)
- Monochromatyczna biała nadruk 1000 kart (MA1000K-WHITE)
- Monochromatyczna czerwona nadruk 1000 kart (MA1000K-RED)
- Monochromatyczna niebieska nadruk 1000 kart (MA1000K-BLUE)
- Monochromatyczna zielona nadruk 1000 kart (MA1000K-GREEN)
- Monochromatyczna złota nadruk 1000 kart (MA1000K-GOLD)
- Monochromatyczna srebrna nadruk 1000 kart (MA1000K-SILVER)

Karty

Drukuje na wszystkich standardowych kartach PCV ISO CR-80 (85,6 × 54) oraz CR-79 (84,1 × 52,4) o grubości od 0,51 mm do 1,02 mm, kartach magnetycznych, zbliżeniowych, samoprzylepnych, HoloPatch i kartach do wielokrotnego zadruku TRW.

Zestaw czyszczący

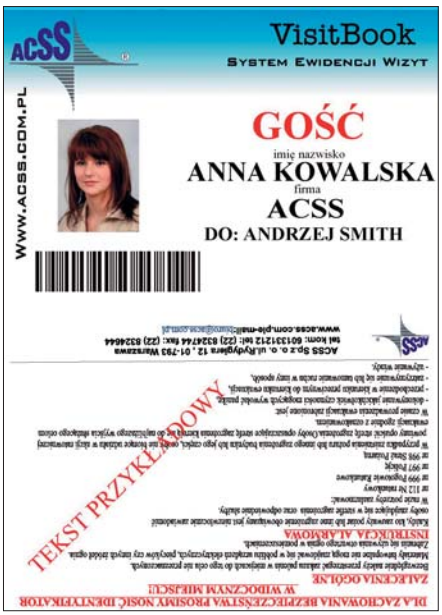
- 1 szt. rolki czyszczącej dostarczanej z każdą taśmą
- 10 szt. kart czyszczących, 1 flamaster (CK1)
- 5 wałków czyszczących plus wymienna oś wałka

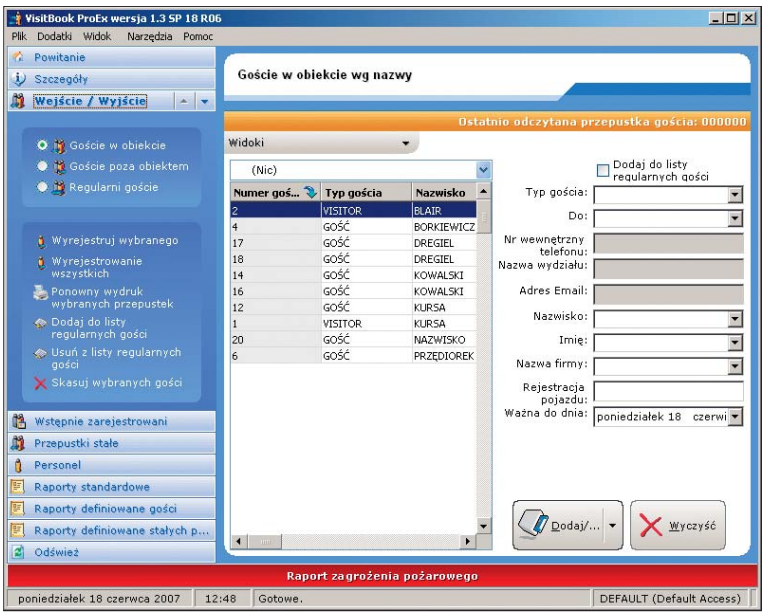
Dystrybucja:

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
http://www.acss.com.pl

System rejestracji gości VisitBook





Wybrane funkcje systemu VisitBook	wersja LITE	wersja PRO	wersja PRO EX	wersja xFR
Kontrola gości, kontrahentów, personelu	tak	tak	tak	tak
Rejestracja wstępna	–	tak	tak	tak
Lista regularnych gości	–	tak	tak	tak
Pobieranie zdjęcia	–	–	tak	tak
Czytnik kodów kreskowych	–	tak	tak	tak
Elektroniczny podpis	–	–	tak	tak
Przepustka pojazdu	–	–	tak	tak
Drukowanie na PVC	–	–	tak	tak
Format bazy danych	Access	Access	Access	MSSQL / MySQL
Dostępność w sieci	–	tak	tak	tak
Administracja konferencji/ wystaw	–	–	tak	tak
Własne wzory przepustek	–	–	tak	tak
Raport standardowy	tak	tak	tak	tak
Raporty definiowane	–	tak	tak	tak
Zabezpieczenie sprzętowe	klucz USB	klucz USB	klucz USB	klucz USB

System rejestracji gości VisitBook jest narzędziem służącym do wspomagania pracy recepcji. Zastępuje papierową księgę gości – jest jej elektronicznym odpowiednikiem. System umożliwia rejestrację danych osób odwiedzających budynek wraz z wydrukiem ich przepustek. Proces wydruku przepustki gościa oraz przechwycenia jego zdjęcia jest płynny i szybki. Rejestrację wejścia i wyjścia gościa można zautomatyzować stosując czytnik kodów kreskowych. Program VisitBook jest dostępny w czterech wersjach: Lite, Pro, ProEx i xFR.

Wersja Lite pozwala na drukowanie przepustek z podstawowymi danymi personalnymi, a rejestracji wejść i wyjść dokonuje pracownik recepcji.

Wersja Pro dodatkowo umożliwia nadruk na przepustce kodu kreskowego wykorzystywanego przy automatycznej rejestracji wejść/wyjść.

ProEx jest wersją bardziej rozbudowaną w porównaniu do wcześniejszych. Umożliwia wydruk przepustki wraz ze zdjęciem i zawiera m.in. funkcję projektowania własnych wzorów przepustek.

Podstawową zaletą różniącą czwartą wersję xFR od pozostałych jest zastosowana w niej platforma SQL zapewniająca szybkość i niezawodność obsługi dużych, ruchliwych obiektów.

Wydruk przepustek jest możliwy na standardowych drukarkach biurowych oraz drukarkach do kart PVC (tylko wersja Pro-Ex i xFR). Główną zaletą użycia systemu jest możliwość raportowania w czasie rzeczywistym, np. raport pożarowy, raport gości w obiekcie, raport ruchów gości itp. Program ponadto zawiera kilka użytecznych funkcji, takich jak: menedżer personelu, menedżer kontrahentów, obsługa konferencji.

Dystrybucja:

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
http://www.acss.com.pl

3D
Wielobranżowe Przedsiębiorstwo Sp. z o.o.
ul. Kościuszki 27C
85-079 Bydgoszcz
tel. (52) 321 02 77
faks (52) 321 15 12
e-mail: biuro@3d.com.pl
www.3d.com.pl

AAT Holding sp. z o.o.
ul. Puławska 431
02-801 Warszawa
tel. (22) 546 05 46
faks (22) 546 05 01
e-mail: aat.warszawa@aat.pl
www.aat.pl

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. 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 32/33
e-mail: aat.kielce@aat.pl

ul. Mieszczańska 18/1, 30-313 **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 60/62
e-mail: aat.poznan@aat.pl

Al. Niepodległości 659, 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

ADT Fire and Security Sp. z o.o.
ul. Palisadowa 20/22
01-940 Warszawa
tel. (22) 430 83 01
faks (22) 430 83 02
e-mail: adtpoland@tycoint.com
www.adt.pl

ALARM SYSTEM
Marek Juszczyński
ul. Kolumba 59
70-035 Szczecin
tel. (91) 433 92 66
faks (91) 489 38 42
e-mail: biuro@bonelli.com.pl
www.bonelli.com.pl

ALARMNET 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

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

ALDOM F.U.H.
ul. Łanowa 63
30-725 Kraków
tel. (12) 411 88 88
faks (12) 294 18 88
e-mail: handel@aldom.pl
www.aldom.pl

ALKAM SYSTEM Sp. z o.o.
ul. Bydgoska 10
59-220 Legnica
tel. (76) 862 34 17, 862 34 19
faks (76) 862 02 38
e-mail: alkam@alkam.pl
www.alkam.pl

ALPOL Sp. z o.o.
ul. Ks. F. Ścigały 10
40-208 Katowice
tel. (32) 790 76 56
Infolinia 0 801 77 77 90
faks (32) 790 76 60
e-mail: katowice@e-alpol.com.pl
www.e-alpol.com.pl

Oddziały:
ul. Warszawska 56, 43-300 **Bielsko-Biała**
tel. (32) 790 76 21
faks (32) 790 76 64
e-mail: bielsko@e-alpol.com.pl

ul. Łęczycka 55, 85-737 **Bydgoszcz**
tel. (32) 720 39 65
faks (32) 790 76 85
e-mail: bydgoszcz@e-alpol.com.pl

ul. Uszczyka 11, 44-100 **Gliwice**
tel. (32) 790 76 23
faks (32) 790 76 65
e-mail: gliwice@e-alpol.com.pl

Al. Solidarności 15b, 25-323 **Kielce**
tel. (32) 720 39 82
faks (32) 790 76 94
e-mail: kielce@e-alpol.com.pl

ul. Pachońskiego 2a, 31-223 **Kraków**
tel. (32) 790 76 46
faks (32) 790 76 73
e-mail: krakow@e-alpol.com.pl

ul. Grenadierów 13, 20-331 **Lublin**
tel. (32) 790 76 50
faks (32) 790 76 74
e-mail: lublin@e-alpol.com.pl

ul. Wigury 21, 90-319 **Łódź**
tel. (32) 790 76 25
faks (32) 790 76 66
e-mail: lodz@e-alpol.com.pl

ul. Kutrzeby 16G, 61-714 **Poznań**
tel. (32) 790 76 37
faks (32) 790 76 70
e-mail: poznan@e-alpol.com.pl

ul. Rzemieślnicza 13, 81-855 **Sopot**
tel. (32) 790 76 43
faks (32) 790 76 72
e-mail: sopot@e-alpol.com.pl

ul. Dąbrowskiego 25, 70-100 **Szczecin**
tel. (32) 790 76 30
faks (32) 790 76 68
e-mail: szczecin@e-alpol.com.pl

ul. Modzelewskiego 35/U9, 02-679 **Warszawa-Mokotów**
tel. (32) 790 76 34
faks (32) 790 76 69
e-mail: warszawa@e-alpol.com.pl

ul. Floriana 3/5, 04-664 **Warszawa-Praga**
tel. (32) 790 76 33
faks (32) 790 76 71
e-mail: warszawa2@e-alpol.com.pl

ul. Stargardzka 7-9, 54-156 **Wrocław**
tel. (32) 790 76 27
faks (32) 790 76 67
e-mail: wroclaw@e-alpol.com.pl

AMBIENT SYSTEM Sp. z o.o.
ul. Sucha 25
80-531 Gdańsk
tel. (58) 345 51 95
faks (58) 344 45 95
e-mail: sekretariat@ambientsystem.pl
www.ambientsystem.pl

Zakład Produkcyjno-Usługowo-Handlowy
ANMA s.c. Tomaszewscy
ul. Ostrowskiego 9
53-238 Wrocław
tel. (71) 363 17 53, faks wew. 7
e-mail: anma@anma-pl.eu
www.anma-pl.eu

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.pl
www.assaabloy.com.pl

ATLine Sp. J.
Sławomir Pruski
ul. Franciszkańska 125
91-845 Łódź
tel. (42) 657 30 80
faks (42) 655 20 99
e-mail: info@atline.pl
www.atline.pl

ROBERT BOSCH Sp. z o.o.
ul. Jutrzenki 105
02-231 Warszawa
tel. (22) 715 41 00/01
faks (22) 715 41 05/06
e-mail: securitysystems@pl.bosch.com
www.boschsecurity.pl

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

bt electronics sp. z o.o.
ul. Dukatów 10
31-431 Kraków
tel. (12) 410 85 10
faks (12) 410 85 11
e-mail: saik@saik.pl
www.saik.pl

LEGRAND POLSKA Sp. z o.o.
ul. Domaniewska 50
Tulipan Hause
02-672 Warszawa
Infolinia 0 801 133 084
faks (22) 843 94 51
e-mail: info@legrand.com.pl
www.legrandgroup.pl

CAMSAT
ul. Garbary 5
86-050 Solec Kujawski
tel. (52) 387 36 58
tel. (52) 387 54 66, faks wew. 24
e-mail: camsat@camsat.com.pl
www.camsat.com.pl

CBC (Poland) Sp. z o.o.
ul. Krasińskiego 41A
01-755 Warszawa
tel. (22) 633 90 90
faks (22) 633 90 60
e-mail: handlowy@cbcpoland.pl
www.cbcpoland.pl

Centrum Monitorowania Alarmów
ul. Puławska 359
02-801 Warszawa
tel. (22) 546 0 888
faks (22) 546 0 619
e-mail: warszawa@cma.com.pl
www.cma.com.pl

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) 340 0 209
faks (71) 341 16 26
e-mail: wroclaw@cma.com.pl

Biura handlowe:
ul. Mieszczańska 18/1, 30-313 **Kraków**
tel. (12) 260 1 395
faks (12) 260 1 396

ul. Racławicka 82, 60-302 **Poznań**
tel./faks (61) 861 40 51
tel. kom. (0) 601 203 664
e-mail: poznan@cma.com.pl

Al. Niepodległości 659, 81-855 **Sopot**
tel. (58) 345 23 24
tel. kom. (0) 693 694 339
e-mail: sopot@cma.com.pl

CONTROL SYSTEM FMN Sp. z o.o.
Al. Komisji Edukacji Narodowej 96 lok. U15
02-777 Warszawa
tel. (22) 855 00 17
faks (22) 855 00 19
e-mail: biuro@cs.pl
www.cs.pl

Przedsiębiorstwo Usług Technicznych D-2 s.c.
K. Kolin, B. Czechowska
ul. Bukowa 1
40-108 Katowice
tel. (32) 253 99 10
faks (32) 253 70 85
e-mail: dravisdravis@neostrada.pl
www.dravis.pl

D-MAX Polska Sp. z o.o.
ul. Obornicka 276
60-693 Poznań
tel. (61) 822 60 52
faks (61) 822 60 52
e-mail: biuro@dmaxpolska.pl
www.dmaxpolska.pl

D+H Polska Sp. z o.o.
ul. Polanowicka 54
51-180 Wrocław
tel. (71) 323 52 50
faks (71) 323 52 40
e-mail: dh-polska@dh-partner.com
www.dhpolska.pl

Oddziały:
ul. Hagera 41, 41-800 **Zabrze**
tel. (32) 375 05 70
faks (32) 375 05 71

ul. Płochocińska 19 lok. 44-45, 03-191 **Warszawa**
tel. (22) 614 39 52
faks (22) 614 39 64

ul. Kielnieńska 134 A, 80-299 **Gdańsk**
tel. (58) 554 47 46
faks (58) 552 45 24

ul. Narutowicza 59, 90-130 **Łódź**
tel. (42) 678 01 32
faks (42) 678 09 20

ul. J. Bema 5A, 73-110 **Stargard Szczeciński**
tel. (91) 561 32 02
faks (91) 561 32 29

ul. Wołczyńska 18, 60-003 **Poznań**
tel. (61) 863 82 08
faks (61) 866 64 16

DANTOM s.c.
ul. Popiełuszki 6
01-501 Warszawa
tel./faks (22) 869 42 70
e-mail: biuro@dantom.com.pl
www.dantom.com.pl

DG ELPRO Sp. J.
ul. Wadowicka 6
30-415 Kraków
tel. (12) 263 93 85
faks (12) 263 93 86
e-mail: biuro@dgelpro.pl
www.dgelpro.pl

DOM Polska Sp. z o.o.
ul. Krótka 7/9
42-200 Częstochowa
tel. (34) 360 53 64
faks (34) 360 53 67
e-mail: dom@dom-polska.pl
www.dom-polska.pl

JABLOTRON Ltd.
Generalny dystrybutor:
DPK System
ul. Piłsudskiego 41
32-020 Wieliczka
tel. (12) 288 23 75, 288 14 26, 278 18 86
faks (12) 278 48 91
e-mail: jablotron@jablotron.pl
www.jablotron.pl

Przedsiębiorstwo DYSKAM Sp. z o.o.
ul. Reymonta 22
30-059 Kraków
tel. (12) 637 80 20
faks (12) 637 80 20 wew. 23
e-mail: dyskam@dyskam.com.pl
www.dyskam.com.pl

DYSKRET Sp. z o.o.
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

EBS Sp. z o.o.
ul. Bronisława Czecha 59
04-555 Warszawa
tel. (22) 518 84 00
faks (22) 812 62 12
e-mail: sales@ebs.pl
www.ebs.pl

ela-compil sp. z o.o.
ul. Słoneczna 15A
60-286 Poznań
tel. (61) 869 38 50-60
faks (61) 861 47 40
e-mail: office@ela.pl
www.ela-compil.pl

EL-MONT A. Piotrowski
ul. Wyzwolenia 15
44-200 Rybnik
tel. (32) 42 23 889
faks (32) 42 30 729
e-mail: el-mont@el-mont.com
www.el-mont.com

Przedsiębiorstwo Handlowo-Usługowe
ELPROMA Sp. z o.o.
ul. Syta 177
02-987 Warszawa
tel./faks (22) 312 06 00 ÷ 02
e-mail: elproma@elproma.pl
www.elproma.pl

ELTCRAC
Mirosław Gabzdyl, Marek Miękina Sp. J.
ul. Ruciana 3
30-803 Kraków
tel. (12) 292 48 60
faks (12) 292 48 65
e-mail: biuro@eltcrac.com.pl
www.eltcrac.com.pl

ELZA ELEKTROSYSTEMY
ul. Ogrodowa 13
34-400 Nowy Targ
tel. (18) 264 04 60
faks (18) 264 92 71
e-mail: elza@ceti.pl
www.elza.com.pl

EMU Sp. z o.o.
ul. Twarda 12
80-871 Gdańsk
tel. (58) 344 04 01÷03
faks (58) 344 88 77
e-mail: gdansk@emu.com.pl
www.emu.com.pl

Oddział:
ul. Jana Kazimierza 61, 01-267 **Warszawa**
tel. (22) 836 54 05, 837 75 93
tel. kom. 0 602 222 516
e-mail: warszawa@emu.com.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

FACTOR SECURITY Sp. z o.o.
ul. Garbary 14B
61-867 Poznań
tel. (61) 850 08 00
faks (61) 850 08 04
e-mail: factor@factor.pl
www.factor.pl

Oddziały:
ul. Morelowa 11A, 65-434 **Zielona Góra**
tel. (68) 452 03 00
tel./faks (68) 452 03 01
e-mail: factor.zg@factor.pl

ul. Grabiszyńska 66e, 53-504 **Wrocław**
tel. (71) 78 74 741
faks (71) 78 74 742
e-mail: factor.wr@factor.pl

FES 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
Leszek Mitusiński
ul. Świątnicka 88
Włosań
32-031 Mogilany
tel. (12) 256 50 35
faks (12) 270 56 96
e-mail: biuro@gde.pl
www.gde.pl

HSA SYSTEMY ALARMOWE
Leopold Rudziński
ul. Langiewicza 1
70-263 Szczecin
tel. (91) 489 41 81
faks (91) 489 41 84
e-mail: biuro@hsa.pl
www.hsa.pl

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

NUUXE – RADIOTON Sp. z o.o.
ul. Olszańska 5
31-513 Kraków
tel. (12) 393 58 00
faks (12) 393 58 02
e-mail: cctv@jvcpro.pl
www.jvcpro.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

P.P.U.H. LASKOMEX
ul. Dąbrowskiego 249
93-231 Łódź
tel. (42) 671 88 00
faks (42) 671 88 88
e-mail: handel@laskomex.com.pl
www.laskomex.com.pl
www.elektrozaczepy.pl
www.edomofon.pl

OBIS CICHOCKI ŚLĄZAK Sp. J.
ul. Rybnicka 64
52-016 Wrocław
tel. (71) 343 16 76, 341 98 54, 340 01 25
faks (71) 343 16 76
e-mail: obis@obis.com.pl
www.obis.com.pl

ISM EuroCenter S.A.
ul. Wyczółki 71
02-820 Warszawa
tel. (22) 548 92 40
faks (22) 548 92 82
e-mail: ism@ismeurocenter.com
www.ismeurocenter.com

MAXBAT Sp. J.
ul. Nadbrzeżna 34A
58-500 Jelenia Góra
tel. (75) 764 83 53
faks (75) 764 81 53
e-mail: info@maxbat.pl
www.maxbat.pl

OMC INDUSTRIAL Sp. z o.o.
ul. Rzymowskiego 30
02-697 Warszawa
tel. (22) 651 88 61
faks (22) 651 88 76
e-mail: sprzedaz@omc.com.pl
www.omc.com.pl

Przedstawicielstwo:
ul. Markiefki 32, 40-213 **Katowice**
tel./faks (32) 202 55 82
e-mail: katowice@omc.com.pl

ul. Murawa 37B/L-6, 61-655 **Poznań**
tel./faks (61) 657 93 60
e-mail: poznan@omc.com.pl

ul. Różyckiego 1c, 51-608 **Wrocław**
tel./faks (71) 347 91 91
e-mail: wroclaw@omc.com.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

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

P.P.H. PETROSIN Sp. z o.o.
ul. Rysi Stok 8/2
30-237 Kraków
tel. (12) 266 87 92
faks (12) 266 99 26
e-mail: office@petrosin.pl
www.petrosin.pl

Oddziały:
ul. Fabryczna 22, 32-540 **Trzebinia**
tel./faks (32) 618 02 00, 618 02 02

ul. Chemików 1, 32-600 **Oświęcim**
tel. (33) 847 30 83
faks (33) 847 29 52

KABE Systemy Alarmowe Sp. z o.o.
ul. Waryńskiego 63
43-190 Mikołów
tel. (32) 324 89 46
faks (32) 324 89 01
e-mail: systemy@kabe.pl
www.kabe.pl/1

MICRONIX Sp. z o.o.
ul. Spółdzielcza 10
58-500 Jelenia Góra
tel. (75) 755 78 78
faks wew. 28
e-mail: info@micronix.pl
www.micronix.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

NAPCO POLSKA
ul. Pszona 2
31-462 Kraków
tel. (12) 412 13 12
faks (12) 410 05 10
e-mail: napco@napco.pl
www.napco.pl

POINTEL Sp. z o.o.
ul. Fordońska 199
85-739 Bydgoszcz
tel. (52) 371 81 16
faks (52) 342 35 83
e-mail: biuro@pointel.pl
www.pointel.pl

POL-ITAL Sp. z o.o.
ul. Irysowa 11
02-660 Warszawa
tel. (22) 831 15 35
faks (22) 831 73 36
e-mail: biuro@polital.pl
www.polital.pl

POLON-ALFA
Zakład Urządzeń Dozymetrycznych Sp. z o.o.
ul. Glinki 155
85-861 Bydgoszcz
tel. (52) 363 92 61
faks (52) 363 92 64
e-mail: polonalfa@polon-alfa.com.pl
www.polon-alfa.pl

PROFICCTV Sp. z o.o.
ul. Obornicka 276
60-693 Poznań
tel. (61) 842 29 62
faks (61) 842 29 62
e-mail: biuro@proficctv.pl
www.proficctv.pl

PULSAR K. Bogusz Sp. J.
Siedlec 150
32-744 Łapczyca
tel. (14) 610 19 40
faks (14) 610 19 50
e-mail: norbert@pulsarspj.com.pl
www.pulsarspj.com.pl

RAMAR s.c.
U. Drogosz-Niemojewska, W. Niemojewska, M. Niemojewski
ul. Modlińska 237
03-120 Warszawa
tel./faks (22) 676 77 37, 676 82 87
e-mail: ramar@ramar.com.pl
www.ramar.com.pl

RISCO GROUP POLAND Sp. z o.o.
ul. 17 Stycznia 56
02-146 Warszawa
tel. (22) 500 28 40
faks (22) 500 28 41
e-mail: poland@riscogroup.com
www.riscogroup.com

ROPAM Elektronik s.c.
Os. 1000-lecia 6A/1
32-400 Myślenice
tel. (12) 379 34 47
tel./faks (12) 272 39 71
e-mail: biuro@ropam.com.pl
www.ropam.com.pl

SATEL Sp. z o.o.
ul. Schuberta 79
80-172 Gdańsk
tel. (58) 320 94 00
faks (58) 320 94 01
e-mail: satel@satel.pl
www.satel.pl

SATIE
Czytniki dalekiego zasięgu
ul. Łączyny 3
02-820 Warszawa
tel. (22) 462 30 86
faks (22) 314 69 50
e-mail: info@satie.pl
www.satie.pl

SAWEL
Elektroniczne Systemy Zabezpieczeń
ul. Lwowska 83
35-301 Rzeszów
tel. (17) 857 80 60
faks (17) 857 79 99
e-mail: sawel@sawel.com.pl
www.sawel.com.pl

SCHRACK SECONET POLSKA Sp. z o.o.
ul. Wołoska 9
02-583 Warszawa
tel. (22) 33 00 620 ÷ 623
faks (22) 33 00 624
e-mail: warszawa@schrack-seconet.pl
www.schrack-seconet.pl

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

ul. Mydlana 1, 51-520 **Wrocław**
tel./faks (71) 345 00 95
e-mail: wroclaw@schrack-seconet.pl

P.T.H. SECURAL
ul. Gen. K. Pułaskiego 4
41-205 Sosnowiec
tel. (32) 291 86 17
tel./faks (32) 291 88 10
e-mail: info@secural.com.pl
www.secural.com.pl

S.M.A.
System Monitorowania Alarmów Sp. z o.o.
ul. Rzymowskiego 30
02-697 Warszawa
tel. (22) 651 88 61
faks (22) 651 88 76
e-mail: sma@sma.biz.pl
www.sma.biz.pl

Oddziały:
ul. Markiefki 32, 40-213 **Katowice**
tel./faks (32) 202 55 82
e-mail: katowice@sma.biz.pl

ul. Murawa 37B/L-6, 61-655 **Poznań**
tel./faks (61) 657 93 60
e-mail: poznan@sma.biz.pl

ul. Różyckiego 1C, 51-608 **Wrocław**
tel. (71) 347 91 91
tel./faks (71) 348 04 19
e-mail: sma@sma.wroclaw.pl

SCHNEIDER ELECTRIC BUILDINGS POLSKA Sp. z o.o.
ul. Rzymowskiego 53
02-697 Warszawa
tel. (22) 313 24 10
faks (22) 313 24 11
e-mail:
SEPLBuildings.Poland@buildings.schneider-electric.com
www.schneider-electric.com/buildings

ul. Arkońska 6 bud. A2
80-387 **Gdańsk**
tel. (58) 782 00 00
faks (58) 782 00 04

ul. Rysia 1A
53-656 **Wrocław**
tel. (71) 711 09 19
faks (71) 711 09 20

ul. Krakowska 280
32-080 **Zabierzów k. Krakowa**
tel. (12) 257 60 80
faks (12) 257 60 81

SONY POLAND Sp. z o.o.
ul. Ogrodowa 58
00-876 Warszawa
tel. (22) 520 25 73
tel. kom. (0) 600 206 117
faks (22) 520 25 77
e-mail: marcin.witkowski@eu.sony.com
www.sonybiz.net/nvm

SPRINT Sp. z o.o.
ul. Jagiellończyka 26
10-062 Olsztyn
tel. (89) 522 11 00
faks (89) 522 11 25
e-mail: sprint@sprint.pl
www.sprint.pl

Oddziały:
ul. Przemysłowa 15, 85-758 **Bydgoszcz**
tel. (52) 365 01 01
faks (52) 365 01 11

ul. Budowlanych 64E, 80-298 **Gdańsk**
tel. (58) 340 77 00
faks (58) 340 77 01

ul. Heyki 27C, 70-631 **Szczecin**
tel. (91) 485 50 00
faks (91) 485 50 12

ul. Canaletta 4, 00-099 **Warszawa**
tel. (22) 826 62 77
faks (22) 827 61 21

S.P.S. Trading Sp. z o.o.
ul. Wał Miedzeszyński 630
03-994 Warszawa
tel. (22) 518 31 50
faks (22) 518 31 70
e-mail: warszawa@spstrading.pl
www.aper.com.pl

Biura Handlowe:
ul. Drożyny 6, 80-302 **Gdańsk**
tel. (58) 624 83 04
faks (58) 668 59 20
e-mail: gdansk@spstrading.pl

ul. Kościuszki 227, 40-600 **Katowice**
tel. (32) 255 64 27
faks (32) 255 64 52
e-mail: katowice@spstrading.pl

ul. Inflancka 6, 91-857 **Łódź**
tel. (42) 617 00 32
faks (42) 659 85 23
e-mail: lodz@spstrading.pl

ul. Polska 60, 60-595 **Poznań**
tel. (61) 852 19 02
faks (61) 825 09 03
e-mail: poznan@spstrading.pl

ul. Grudziądzka 176, 87-100 **Toruń**
tel. (56) 653 99 43
faks (56) 653 90 81
e-mail: torun@spstrading.pl

ul. Inowrocławska 39 C, 53-649 **Wrocław**
tel. (71) 348 44 64
faks (71) 348 36 35
e-mail: wroclaw@spstrading.pl

STRATUS
ul. Nowy Świat 38
20-419 Lublin
tel./faks (81) 743 87 72
e-mail: stratus@stratus.lublin.pl
www.stratus.lublin.pl

SYSTEM 7
ul. Krakowska 33
43-300 Bielsko-Biała
tel. (33) 821 87 77
Infolinia 801 000 307
faks (33) 816 91 88
e-mail: biuro@s7.pl
www.system7.pl
Internetowa Hurtownia Zabezpieczeń:
www.system7.biz

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

Biuro Handlowe:
ul. Rzymowskiego 30, 02-697 **Warszawa**
tel. (22) 843 83 95
faks (22) 843 79 12
e-mail: tap5@tap.com.pl

TAYAMA POLSKA Sp. J.
ul. Słoneczna 4
40-135 Katowice
tel. (32) 258 22 89, 357 19 10, 357 19 20
faks (32) 357 19 11, 357 19 21
e-mail: biuro@tayama.com.pl
www.tayama.com.pl

TECHNOKABEL S.A.
ul. Nasielska 55
04-343 Warszawa
tel. (22) 516 97 97
faks (22) 516 97 91
e-mail: sprzedaz@technokabel.com.pl
www.technokabel.com.pl

TP TELTECH Sp. z o.o.
ul. Tuwima 36
90-941 Łódź
tel. (42) 639 83 60
faks (42) 639 89 85
e-mail: teltechinfo@tpteltech.pl
www.tpteltech.pl

Oddziały:
al. Wyzwolenia 70, 71-510 **Szczecin**
tel./faks (91) 423 70 55
e-mail: witold.brzozowski@telekomunikacja.pl

ul. Rzeczypospolitej 5, 59-220 **Legnica**
tel. (76) 856 60 71
faks (76) 856 60 71
e-mail: marian.sitko@telekomunikacja.pl

ul. Nasypowa 12, 40-551 **Katowice**
tel. (32) 202 30 50
faks (32) 201 13 17
e-mail: dariusz.gawor@telekomunikacja.pl

ul. Rakowicka 51, 31-510 **Kraków**
tel. (12) 431 59 01
faks (12) 423 97 65
e-mail: marek.zembaty@telekomunikacja.pl

ul. Kosmonautów 82, 20-358 **Lublin**
tel. (81) 745 39 83
faks (81) 745 39 78
e-mail: zbigniew.chodkiewicz@telekomunikacja.pl

UNICARD S.A.
ul. Wadowicka 12
30-415 Kraków
tel. (12) 39 89 900
faks (12) 39 89 901
e-mail: biuro@unicard.pl
www.unicard.pl

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

VISION POLSKA Sp. z o.o.
ul. Unii Lubelskiej 1
61-249 Poznań
tel. (61) 623 23 05
faks (61) 623 23 17
e-mail: biuro@visionpolska.pl
www.visionpolska.pl

Nazwa firmy	produkcja	projektowanie	dystrybucja	instalacja	szkolenia
3D	TAK	TAK	–	–	TAK
AAT Holding	–	TAK	TAK	–	TAK
ACSS ID Systems	–	–	TAK	–	–
ADT Fire and Security	TAK	TAK	TAK	TAK	TAK
Alarm System	TAK	TAK	TAK	TAK	–
Alarmnet	–	TAK	TAK	–	TAK
Alarmtech Polska	TAK	TAK	–	–	TAK
Aldom	–	TAK	TAK	TAK	TAK
Alkam System	TAK	TAK	TAK	TAK	–
Alpol	–	–	TAK	–	TAK
Ambient System	TAK	TAK	TAK	TAK	TAK
Anma	–	TAK	–	TAK	TAK
ASSA ABLOY	–	–	TAK	–	–
Atline	–	TAK	TAK	TAK	TAK
BOSCH	TAK	–	TAK	–	TAK
P.W.H. Brabork - Laboratorium	–	TAK	TAK	TAK	–
bt electronics	TAK	TAK	TAK	TAK	TAK
CAMSAT	TAK	TAK	–	–	TAK
CBC Poland	TAK	–	TAK	–	TAK
CMA	TAK	TAK	TAK	TAK	–
CONTROL SYSTEM FMN	–	TAK	TAK	TAK	TAK
D-2	–	TAK	TAK	TAK	–
D-MAX	–	TAK	TAK	–	TAK
D+H Polska	–	TAK	TAK	TAK	TAK
DANTOM	TAK	–	TAK	–	–
DG Elpro	–	TAK	TAK	TAK	–
DOM Polska	TAK	TAK	TAK	–	–
DPK System	–	–	TAK	TAK	TAK
Dyskam	TAK	TAK	–	TAK	TAK
Dyskret	–	TAK	TAK	TAK	TAK
EBS	TAK	TAK	TAK	–	–
ela-compil	TAK	–	TAK	–	TAK
El-Mont	–	TAK	–	TAK	–
Elproma	–	TAK	–	TAK	–
Eltcrac	TAK	TAK	TAK	TAK	TAK
Elza Elektrosystemy	–	TAK	–	TAK	TAK
Emu	–	–	TAK	–	–
Eureka	–	TAK	–	TAK	–
Factor Polska	–	–	TAK	–	TAK
FES	–	TAK	TAK	TAK	–
GDE Polska	–	–	TAK	–	TAK
HSA	–	–	TAK	–	–
Insap	–	TAK	TAK	TAK	TAK

Nazwa firmy	produkcja	projektowanie	dystrybucja	instalacja	szkolenia
ISM EuroCenter	–	–	TAK	–	–
Janex International	–	TAK	TAK	–	TAK
KABE	–	TAK	TAK	TAK	TAK
KATON	–	–	TAK	–	TAK
Kolektor MR	–	TAK	TAK	TAK	–
Laskomex	TAK	TAK	TAK	–	TAK
Legrand Polska	TAK	TAK	TAK	–	TAK
MAXBAT	TAK	TAK	TAK	TAK	TAK
MicroMade	TAK	–	–	–	–
Micronix	–	TAK	TAK	TAK	–
NAPCO	–	–	TAK	TAK	TAK
Nuuxe – Radioton	–	–	TAK	–	–
OBIS	–	TAK	–	TAK	–
OMC INDUSTRIAL	–	–	TAK	–	TAK
Petrosin	–	TAK	–	TAK	–
Pointel	–	TAK	–	TAK	–
POL-ITAL	–	TAK	TAK	TAK	TAK
Polon-Alfa	TAK	–	–	–	–
ProfiCCTV	–	TAK	TAK	–	TAK
Pulsar	TAK	–	–	–	–
Ramar	–	–	TAK	TAK	TAK
RISCO	TAK	–	TAK	–	TAK
ROPAM Elektronik	TAK	–	TAK	–	–
Satel	TAK	–	–	–	–
SATIE	TAK	–	TAK	TAK	–
Sawel	–	TAK	TAK	TAK	TAK
Schrack Seconet Polska	TAK	–	–	–	TAK
Secural	TAK	TAK	TAK	–	TAK
S.M.A.	–	TAK	–	TAK	–
Schneider Electric Buildings Polska	TAK	TAK	TAK	TAK	TAK
Sony	TAK	–	–	–	–
Sprint	–	TAK	TAK	TAK	–
S.P.S. Trading	TAK	–	TAK	–	TAK
STRATUS	–	TAK	TAK	–	TAK
SYSTEM 7	TAK	–	TAK	–	–
Tap – Systemy Alarmowe	–	–	TAK	–	TAK
Tayama	–	–	TAK	–	–
Technokabel	TAK	TAK	–	–	–
TP TELTECH	–	TAK	TAK	TAK	–
UNICARD	TAK	TAK	TAK	TAK	TAK
W2	TAK	TAK	TAK	–	–
Vision Polska	–	TAK	TAK	–	TAK

Nazwa firmy	systemy sygnalizacji włamania i napadu	systemy telewizji dozorowej	systemy kontroli dostępu	systemy sygnalizacji pożarowej	systemy ochrony peryferyjnej	integracja systemów	monitoring	zabezpieczenia mechaniczne	systemy nagłośnień
3D	–	TAK	–	–	–	–	–	–	–
AAT Holding	TAK	TAK	TAK	TAK	–	TAK	TAK	–	–
ACSS ID Systems	drukarki do identyfikatorów, akcesoria do kart, systemy rejestracji gości, karty magnetyczne i zbliżeniowe								
ADT Fire and Security	TAK	TAK	TAK	TAK	–	TAK	TAK	–	TAK
Alarm System	TAK	TAK	TAK	–	–	–	–	–	–
Alarmnet	TAK	TAK	TAK	–	–	TAK	–	TAK	–
Alarmtech Polska	TAK	–	–	–	–	–	–	–	–
Aldom	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
Alkam System	TAK	TAK	TAK	TAK	–	TAK	–	–	TAK
Alpol	TAK	TAK	TAK	TAK	–	–	–	–	TAK
Ambient System	TAK	TAK	–	TAK	–	–	–	–	TAK
Anma	TAK	TAK	TAK	TAK	–	TAK	–	–	–
ASSA ABLOY	–	–	TAK	–	–	–	–	TAK	–
ATLine	–	TAK	–	–	TAK	–	TAK	–	–
BOSCH	TAK	TAK	TAK	TAK	–	TAK	–	–	TAK
P.W.H. Brabork-Laboratorium	TAK	TAK	TAK	TAK	–	TAK	–	–	TAK
bt electronics	–	–	TAK	–	–	–	–	TAK	–
CAMSAT	–	TAK	–	–	–	–	TAK	–	–
CBC Poland	–	TAK	–	–	–	–	–	–	–
CMA	TAK	–	–	–	–	–	TAK	–	–
Control System FMN	TAK	TAK	TAK	–	–	TAK	–	TAK	–
D-2	TAK	TAK	TAK	TAK	–	TAK	TAK	–	TAK
D-MAX	–	TAK	–	–	–	–	–	–	–
D+H Polska	–	–	–	TAK	–	–	–	TAK	TAK
DANTOM	TAK	TAK	TAK	TAK	–	–	–	TAK	–
DG Elpro	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
DOM Polska	–	–	TAK	–	–	–	–	TAK	–
DPK System	TAK	–	–	–	–	–	–	–	–
Dyskam	TAK	TAK	TAK	TAK	–	TAK	TAK	–	–
Dyskret	TAK	TAK	TAK	TAK	–	TAK	–	TAK	TAK
EBS	TAK	–	TAK	–	–	–	–	–	–
ela-compil	–	–	–	–	–	TAK	–	–	–
El-Mont	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
Elproma	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
Eltcrac	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
Elza Elektrosystemy	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
Emu	akumulatory bezobsługowe do zasilania awaryjnego urządzeń alarmowych								
Eureka	TAK	TAK	TAK	TAK	TAK	TAK	TAK	–	–
Factor Polska	TAK	TAK	TAK	TAK	TAK	–	–	–	–
FES	TAK	TAK	TAK	TAK	–	TAK	–	–	TAK
GDE Polska	–	TAK	TAK	–	–	–	TAK	–	–
HSA	TAK	TAK	TAK	TAK	–	–	–	TAK	–
Insap	TAK	TAK	TAK	TAK	–	TAK	TAK	–	TAK

Nazwa firmy	systemy sygnalizacji włamania i napadu	systemy telewizji dozorowej	systemy kontroli dostępu	systemy sygnalizacji pożarowej	systemy ochrony peryferyjnej	integracja systemów	monitoring	zabezpieczenia mechaniczne	systemy nagłośnień
ISM EuroCenter	–	TAK	–	–	–	–	TAK	–	–
Janex International	TAK	TAK	TAK	TAK	–	TAK	–	–	TAK
KABE	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
KATON	–	TAK	TAK	–	–	TAK	–	–	–
Kolektor MR	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
Laskomex	–	TAK	TAK	–	–	–	–	TAK	–
Legrand Polska	–	–	TAK	–	–	–	–	–	–
MAXBAT	TAK	TAK	TAK	TAK	TAK	TAK	–	TAK	TAK
MicroMade	–	–	TAK	–	–	–	–	–	–
Micronix	TAK	TAK	TAK	–	–	–	–	TAK	–
NAPCO	TAK	TAK	TAK	TAK	–	–	–	–	–
Nuuxe – Radioton	–	TAK	–	–	–	TAK	–	–	–
OBIS	TAK	TAK	TAK	TAK	–	–	–	–	TAK
OMC INDUSTRIAL	TAK	TAK	TAK	TAK	–	–	–	TAK	–
Petrosin	TAK	TAK	TAK	–	–	–	–	–	–
Pointel	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
POL-ITAL	konserwacja i serwis zabezpieczeń mechanicznych								
Polon-Alfa	–	–	–	TAK	–	–	–	–	–
ProfiCCTV	TAK	TAK	TAK	TAK	–	–	–	–	–
Pulsar	TAK	TAK	TAK	–	–	–	–	TAK	–
Ramar	TAK	TAK	TAK	TAK	TAK	–	–	–	–
RISCO	TAK	–	TAK	–	–	TAK	TAK	–	–
ROPAM Elektronik	TAK	TAK	TAK	TAK	–	–	TAK	–	–
Satel	TAK	–	TAK	–	–	–	TAK	–	–
SATIE	–	–	TAK	–	–	–	–	–	–
Sawel	TAK	TAK	TAK	TAK	TAK	TAK	–	–	–
Schrack Seconet Polska	–	–	–	TAK	–	–	–	–	–
Secural	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
S.M.A.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
Schneider Electric Buildings Polska	TAK	TAK	TAK	TAK	–	TAK	TAK	–	–
Sony	–	TAK	–	–	–	–	TAK	–	–
Sprint	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
S.P.S. Trading	TAK	TAK	TAK	TAK	–	TAK	TAK	TAK	TAK
STRATUS	TAK	TAK	TAK	TAK	TAK	TAK	–	–	TAK
SYSTEM 7	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
Tap – Systemy Alarmowe	TAK	–	TAK	–	–	–	–	–	–
Tayama	TAK	TAK	TAK	TAK	–	–	–	–	TAK
Technokabel	TAK	TAK	TAK	TAK	TAK	–	TAK	–	TAK
TP TELTECH	TAK	TAK	TAK	TAK	TAK	–	TAK	–	–
UNICARD	TAK	TAK	TAK	–	–	TAK	–	TAK	–
W2	TAK	–	–	TAK	–	–	–	–	–
Vision Polska	–	–	–	TAK	–	–	–	–	–

ZABEZPIECZENIA
dwumiesięcznik

Redaktor naczelny
Teresa Karczmarzyk

Redaktorzy merytoryczni
Stanisław Banaszewski
Andrzej Walczyk

Dział marketingu i reklamy
Ela Końka

Redaguje zespół
Krzysztof Białek
Marek Blim
Patryk Gańko
Norbert Góra
Paweł Karczmarzyk
Ryszard Sobierski
Waldemar Szulc
Adam Wojcinowicz
Marek Życzkowski

Współpraca zagraniczna
Rafał Niedzielski

Współpraca
Marcin Buczaj
Adam Bułaciński
Piotr Czernoch
Marcin Pyclik
Adam Rosiński
Sławomir Wagner
Andrzej Wójcik

Skład i łamanie
Marek Bladoszewski

Korekta
Paweł Karczmarzyk

Adres redakcji
ul. Puławska 359, 02-801 Warszawa
tel. (22) 546 0 951, 953
faks (22) 546 0 959
www.zabezpieczenia.com.pl

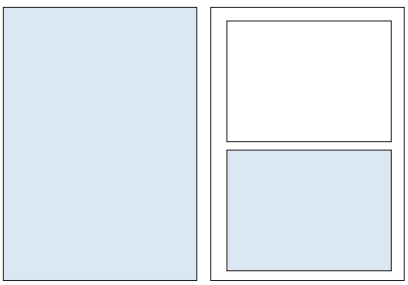
Wydawca
AAT Holding sp. z o.o.
ul. Puławska 431, 02-801 Warszawa
tel. (22) 546 0 546
faks (22) 546 0 501

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

Cennik reklam

Reklama wewnątrz czasopisma:

cała strona, pełny kolor	4200 zł
cała strona, czarno-biała	2200 zł
1/2 strony, pełny kolor	2700 zł
1/2 strony, czarno-biała	1500 zł
1/3 strony, pełny kolor	1900 zł
1/3 strony, czarno-biała	1000 zł
1/4 strony, pełny kolor	1400 zł
1/4 strony, czarno-biała	800 zł
karta katalogowa, 1 strona	900 zł



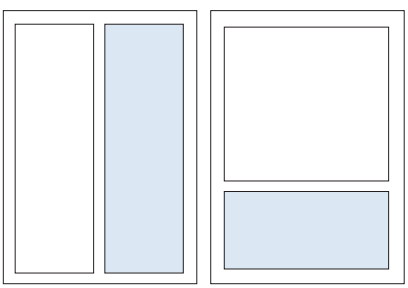
cała strona (200 x 282 mm + 3mm spad)

1/2 strony (170 x 125 mm)

Artykuł sponsorowany:
indywidualne negocjacje (forma graficzna artykułu sponsorowanego podlega zasadom jednolitym dla wszystkich materiałów zamieszczonych w czasopiśmie)

Reklama na okładkach:

pierwsza strona	indywidualne negocjacje
druga strona	5000 zł
przedostatnia strona	5000 zł
ostatnia strona	5000 zł

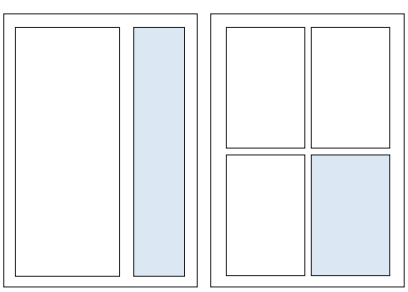


1/2 strony (83 x 260 mm)

1/3 strony (170 x 80 mm)

Spis teleadresowy:

jednorazowy wpis	70 zł



1/3 strony (54 x 260 mm)

1/4 strony (83 x 125 mm)

Redakcja przyjmuje zamówienia na 6 kolejnych emisji

Podane ceny nie uwzględniają podatku VAT (22%)

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

Spis reklam

SONY

Sony robi MEGA dobrze!

Kamery megapikselowe

- Full HD i HD ready
- Lider technologii przetworników optycznych
- XDNR – doskonała dynamiczna redukcja szumów
- View DR – szeroki zakres dynamiki
- Standardy kodowania: H.264, MPEG-4, JPEG

IPELA

GO CAPTURE

ANALOGUE

HD

IP SOLUTIONS

Potrzebuję.....

mieć moje własne ID,
teraz, od razu, kiedy jest
mi potrzebne.

HID stwarza ci możliwość...

wyprodukowania kart ID w twoim własnym przedsiębiorstwie.

Technologie HID znacznie zmniejszają czas i koszt produkcji i umożliwiają większą kontrolę. Bez komplikacji, bez czekania... Najwyższej jakości karty, szeroki zakres technologii dostosowanych do indywidualnych potrzeb. Funcjonalność i bezpieczeństwo. Fargo umożliwia Ci kontrolowanie Twojego bezpieczeństwa dostarczając ekonomiczne i nowoczesne rozwiązania technologiczne.

HID

Chcąc stworzyć swój identyfikator, skontaktuj się z **hidglobal.com/cardissuance/Zab**