

BIULETYN

STOWARZYSZENIA POLALARM



**Ogólnopolskie Stowarzyszenie Inżynierów
i Techników Zabezpieczeń Technicznych
i Zarządzania Bezpieczeństwem**

- Od redakcji - słowo Redaktora Biuletynu;
- O Targach SECURECH 2018, Marta Rybko;
- Przegląd prasy branżowej, Artur Bogusz;
- Analiza budowy elementów infrastruktury zarządzania kryzysowego w Polsce, Mariusz Furmanek;
- Ochrona danych osobowych w nowych warunkach, Artur Bogusz;
- Reklamy;

Szanowne Koleżanki i Koledzy,

Mija czas nieubłagane i efekty pracy wykonywanej nie zawsze nas zadawalają. Niestety nie zawsze udaje się nam zrobić tyle i tak abyśmy byli z tego zadowoleni czy dumni.

Oczywiście dobrze jest tak realizować zadania jakie są przed nami stawiane w stopniu co najmniej zadawalającym. A jeszcze lepiej kiedy udaje nam się robić wszystko tak abyśmy mogli być z tego dumni.

Praca na rzecz Stowarzyszenia to praca społeczna i wynikająca z naszej wewnętrznej potrzeby zrobienia czegoś ważnego dla branży bezpieczeństwa w Polsce.

Pozostaje więc pytanie, które powinniśmy sobie postawić: czy jest w nas chęć do robienia czegoś społecznie, czegoś co może przynieść korzyść innym?

W mojej ocenie wszyscy powinniśmy pracować na rzecz Naszego Stowarzyszenia po to aby poprawiać stan branży bezpieczeństwa w Polsce. Poprawiać jest oczywiście ciągle co. Pytanie stałe tylko czy chcemy coś zmienić?

Zapraszam do współpracy w ramach Stowarzyszenia!

Kilka słów o Targach SECUREX 2018;

SECUREX 2018 – najszybciej rosnąca edycja w historii;

Międzynarodowe Targi Zabezpieczeń SECUREX odbędą się w dniach 23-26.04.2018 i widnieją w kalendarzach branżowców, którzy termin przeznaczają na wielkie spotkanie biznesowo – marketingowe w Poznaniu. Przygotowania do wydarzenia trwają w tempie, które nadała ubiegła edycja.

Niemal cała powierzchnia terenów targowych tętniła rozmowami profesjonalistów, którzy wzięli udział w bloku targów, na który złożyły się Międzynarodowe Targi Zabezpieczeń SECUREX wraz z Forum Technologii Cyfrowych POZNAŃ MEDIA EXPO, Międzynarodowe Targi Ochrony Pracy, Pożarnictwa i Ratownictwa SAWO oraz Międzynarodowe Targi Instalacyjne INSTALACJE.

Ubiegłoroczne targi SECUREX współtworzyło niemal 300 wystawców, którzy zaprezentowali 150 nowości ze swojej oferty. Wszystkie wydarzenia ubiegłej edycji przyciągnęły blisko 30 000 profesjonalistów.

Kilka słów o Targach SECUREX 2018;

Targi spełniają potrzeby branży;

Pierwszy termin zgłoszeń zaowocował znaczną sprzedażą powierzchni ekspozycyjnej, która pomieści firmy m.in. z sektorów elektronicznych systemów zabezpieczeń, CCTV, systemów ochrony danych – ochrony informacji (SECUREX IT), zabezpieczeń PPOŻ, a także z sektora inteligentnego budynku, ochrony i nadzoru, systemów łączności i zarządzania w stanach kryzysowych – wyposażenia i sprzętu dla służb mundurowych. Słowem – zakres tematyczny ponownie okazał się być dokładnie dopasowanym do potrzeb poszczególnych sektorów branży. Procent zamawianej przez firmy powierzchni przyrasta szybko, jak nigdy dotąd.



securex[®]
P O L A N D
Międzynarodowe Targi Zabezpieczeń

Kilka słów o Targach SECUREX 2018;

SECUREX z nową energią;

Po raz pierwszy w historii nastąpi włączenie do bloku targów wydarzenia EXPOPOWER – Międzynarodowych Targów Energetyki. Branża zabezpieczeń z pewnością doceni fakt, że swoją ofertę na targi będzie mogła poszerzyć o rozwiązania dedykowane zakładom energetycznym, czy elektrowniom. Wciąż aktualny i ważny temat dotyczący zabezpieczeń informatycznych i ochrony danych osobowych, który podczas ubiegłej edycji odbył się pod hasłem SECUREX BeIN – Bezpieczeństwo Informacji, wzbudził duże zainteresowanie, będzie miał swą kolejną odsłonę. Kontynuowane będą cieszące się ogromnym powodzeniem wśród uczestników, jak i zaangażowaniem wystawców, Mistrzostwa Polski Instalatorów Systemów Alarmowych, których VI edycję zorganizuje Polska Izba Systemów Alarmowych wraz z MTP. Drugiego dnia targów przestrzeń MPISA udostępniona zostanie uczniom szkół zawodowych i techników branżowych, którzy będą mogli spróbować swoich sił w lekcjach i warsztatach instalatorskich. To przedsięwzięcie o charakterze edukacyjnym ma na celu zachęcić i wykształcić przyszłych profesjonalistów.

Kilka słów o Targach SECUREX 2018;

Zabezpiecz termin, odbezpiecz zasoby;

Kolejna edycja Międzynarodowych Targów Zabezpieczeń SECUREX odbędzie się w dniach 23-26.04.2018 roku w Poznaniu. To będą dni obfitujące w bogactwo nowości prezentowanych przez wystawców z Europy Środkowo – Wschodniej, jak i wydarzeń merytorycznych. Dlatego warto szczególnie przygotować się do wizyty w Poznaniu: zabezpieczyć termin i logistykę oraz odbezpieczyć magazyn z materiałami reklamowymi, ponieważ będzie to czas intensywnych spotkań i rozmów.

Do zobaczenia na wiosnę w Poznaniu!

Marta Rybko

PR & Marketing
Zespół Promocji Sprzedaży/ Promotion team
tel. +48 61 869 23 85
kom. 691 033 299
e-mail: marta.rybko@mtp.pl



Drodzy Czytelnicy tym razem przegląd prasy będzie trochę inny niż ten do którego przywykliśmy. W tym numerze biuletynu będę chciał Was zabrać na wycieczkę po stronach internetowych znanych publikatorów w branży bezpieczeństwa.

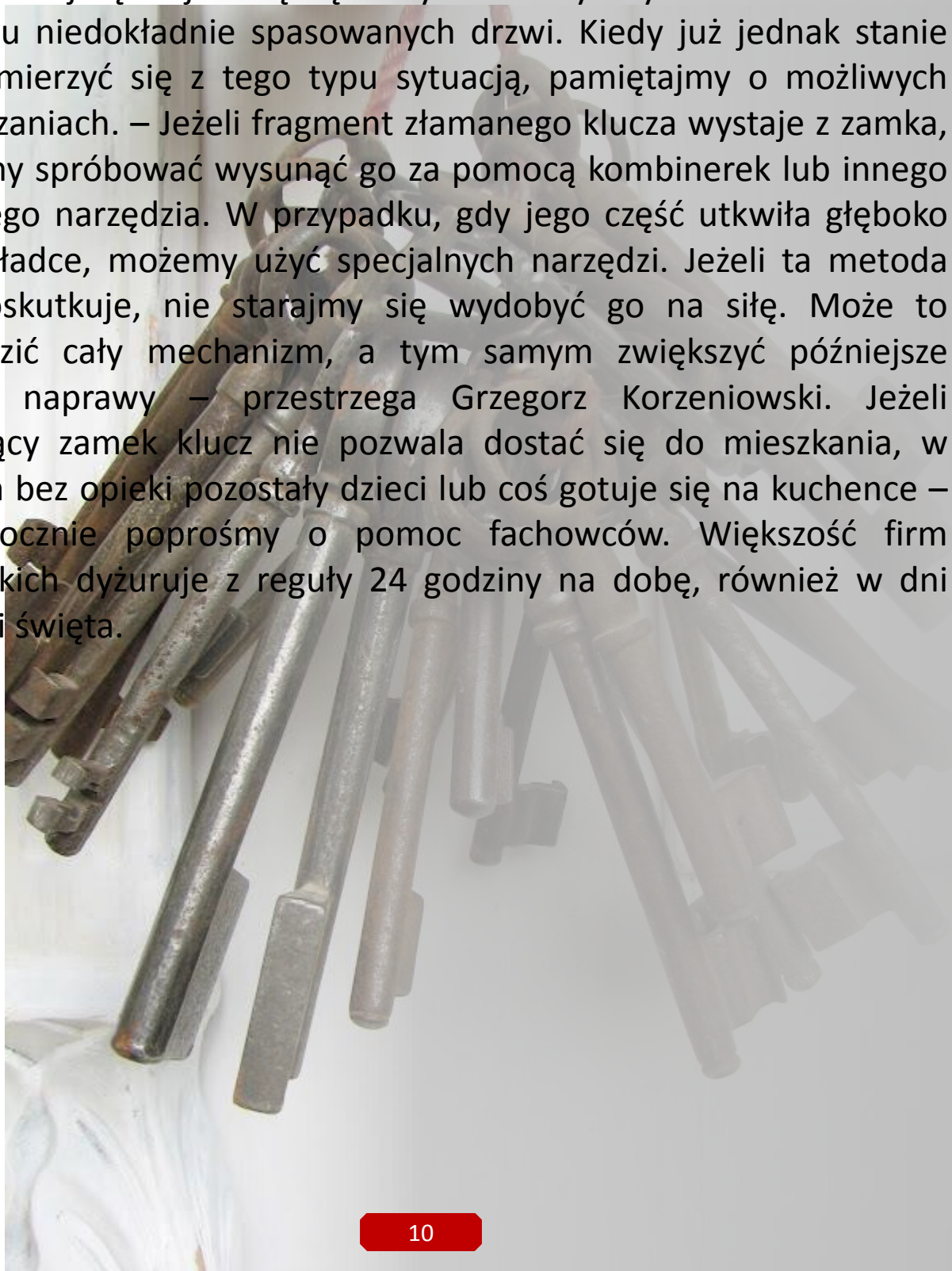
Strona Zabezpieczeń (www.zabezpieczenia.com.pl) to sporo artykułów w dziedzinie bezpieczeństwa i systemów zabezpieczeń. Ciekawe relacje i rekomendacje w zakresie technicznych systemów zabezpieczeń. Wiele ciekawych artykułów i zdjęć z różnych wydarzeń jakie miały miejsce w czasie minionym. Znajdziemy tu ciekawy artykuł firmy Axis Communications, która wprowadziła na rynek nową generację kamer zmiennopozycyjnych z serii AXIS Q86 i AXIS Q87, które umożliwiają operatorom szybsze i bardziej precyzyjne obracanie i pochylanie urządzeń w celu obserwacji dużych obszarów czy ochrony perymetrycznej w czasie rzeczywistym.





Kamery błyskawicznie reagują na wykryte alarmy i zagrożenia. Dzięki rozszerzonym funkcjom umożliwiają stały dozór w zakresie 360 stopni bez zniekształceń obrazu przy aż 135-stopniowym polu widzenia w pionie. Pojawiła się ciekawa informacja na temat współpracy Politechniki Łódzkiej i firmy Bosch Security Systems, które to podmioty zawarły 21 czerwca 2017 roku umowę dotyczącą współpracy. Współpraca ta będzie dotyczyła przede wszystkim dziedziny badawczo-rozwojowej, a także kształcenia studentów w zakresie systemów zabezpieczeń i nowoczesnych, inteligentnych rozwiązań wykorzystywanych w przestrzeni miejskiej. Bardzo ciekawe jakie efekty dla branży bezpieczeństwa przyniesie ta współpraca w przyszłości. Zabezpieczenia to również zabezpieczenia mechaniczne, a wśród nich zamki i klucze. Na stronie zabezpieczeń znajdziemy ciekawy artykuł w tej tematyce. Do złamania klucza w drzwiach nie potrzeba wielkiej siły.

Do tego typu uszkodzeń dochodzi na szczęście coraz rzadziej, a wszystko za sprawą nowoczesnych technologii i materiałów, stosowanych przy produkcji mechanizmów otwierania. Klucze bowiem najczęściej łamią się w wyniku fabrycznych uszkodzeń lub z powodu niedokładnie spasowanych drzwi. Kiedy już jednak stanie nam zmierzyć się z tego typu sytuacją, pamiętajmy o możliwych rozwiązaniach. – Jeżeli fragment złamanego klucza wystaje z zamka, możemy spróbować wysunąć go za pomocą kombinerek lub innego twardego narzędzia. W przypadku, gdy jego część utkwiała głęboko we wkładce, możemy użyć specjalnych narzędzi. Jeżeli ta metoda nie skutkuje, nie starajmy się wydobyć go na siłę. Może to uszkodzić cały mechanizm, a tym samym zwiększyć późniejsze koszty naprawy – przestrzega Grzegorz Korzeniowski. Jeżeli blokujący zamek klucz nie pozwala dostać się do mieszkania, w którym bez opieki pozostały dzieci lub coś gotuje się na kuchence – bezzwłocznie poprośmy o pomoc fachowców. Większość firm ślusarskich dyżuruje z reguły 24 godziny na dobę, również w dni wolne i święta.



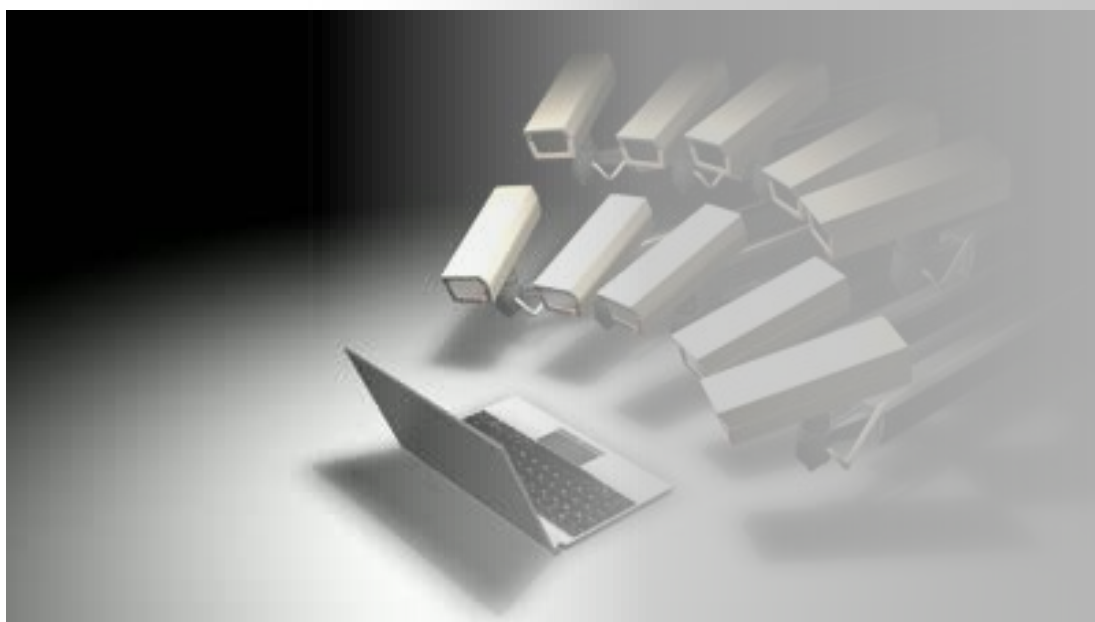
Kolejna strona to ochrona mienia i informacji (www.ochrona-mienia.pl) gdzie również można znaleźć wiele ciekawych artykułów i relacji z wydarzeń jakie w branży miały miejsce. Znajdujemy tu informację o tym, że za nami kolejna edycja Ogólnopolskich Dni Zintegrowanych Systemów Bezpieczeństwa Pożarowego, które od sześciu lat z dużym powodzeniem organizuje firma Schrack Seconet we współpracy z partnerami technologicznymi, merytorycznymi i medialnymi. Tegoroczne dwudniowe szkolenie w Hotelu Windsor w Jachrance zgromadziło ponad 500 osób – ekspertów, niezależnych specjalistów i wszystkich tych, których łączy branża szeroko pojętego bezpieczeństwa pożarowego. Ponadto można znaleźć informację, że 27-28 września 2017 w Resorcie Nosalowy Dwór w Zakopanem odbyła się piętnasta, południowa edycja Spotkania Projektantów Instalacji Niskoprądowych. Wyjątkowa, jubileuszowa edycja zgromadziła ponad 320 uczestników, a stolica Tatr na dwa dni stała się centrum technologii zabezpieczeń elektronicznych, monitoringu, instalacji telekomunikacyjnych, systemów zarządzania budynkiem i rozwiązań Data Center. Podczas 15SPIN na uczestników czekały nowości w programie wydarzenia.



Dotychczasowa, ceniona przez Partnerów i uczestników formuła została wzbogacona w dodatkowy czas poświęcony na nawiązywanie kontaktów i wymianę doświadczeń w strefie stoisk wystawienniczych. Nowością były także indeksy 15SPIN, które spotkały się z entuzjazmem zarówno uczestników jak i Partnerów, a za cel miały aktywizowanie uczestników do odwiedzania stoisk Partnerów. Podczas 15SPIN nie zabrakło atrakcji, które integrowały branżę, a jednocześnie pozwoliły w wyjątkowy sposób uczcić jubileusz podczas aktywnego popołudnia oraz artystycznego wieczoru w pierwszym dniu spotkania. Na prezentowanej stronie można znaleźć ciekawy artykuł o radarach Scan 360. Radary Scan 360 można już znaleźć w ofercie LINC Polska. To innowacyjne rozwiązania wykorzystujące zaawansowaną technologię przetwarzania sygnału, rozwijaną przez producenta od ponad 20 lat. Radary marki Scan 360 mogą działać zarówno samodzielnie – generując alarm w przypadku wykrycia zagrożenia – jak i w połączeniu z kamerą termowizyjną oraz/ lub tradycyjną światła widzialnego. W przypadku wygenerowania alarmu przez radar, kamera zostaje nakierowana na określony cel.



Dodatkowo wykorzystując przejrzysty i intuicyjny graficzny interfejs użytkownika można w łatwy i szybki sposób ustawić, skalibrować i zdefiniować strefy detekcji. Istnieje możliwość stworzenia 36 stref, które mogą być zlokalizowane na dystansie od 0 do 200m. Ze względu na długi zasięg detekcji radary Scan 360 doskonale nadają się do ochrony dużych obszarów, takich jak lotniska, farmy słoneczne, rezydencje VIP itp. Atrakcyjna cena oraz łatwość instalacji, kalibracji i użytkowania czynią je korzystnym elementem szczelnego systemu ochrony. Wysoka wydajność oraz wytrzymałość połączona z wykorzystaniem technologii mikrofalowej to kolejne ich atuty. Kolejny ciekawy artykuł jaki możemy znaleźć dotyczy kwestii obserwacji terenu w nocy. Obserwacja terenu w dzień wymaga sprawnego oka i precyzyjnej lunety lub obiektywu kamery. Jednak ten sam teren w nocy nie jest już tym samym środowiskiem.



Noc stwarza zupełnie inne warunki i wymusza odnalezienie się w nich. Dlatego po zmroku najważniejszą kwestią staje się jakość noktowizji lub termowizji. O ile większość producentów zapewnia dostosowanie się do problematycznych, nocnych warunków, o tyle dla marki Electrooptic takie warunki nie są problemem, a korzyścią. Wszystko za sprawą misji, jaką od 1996 roku, Electrooptic sukcesywnie wdraża w życie – kluczem do najskuteczniejszej nocnej obserwacji jest nieustanne stawianie na innowacyjne rozwiązania. Jednym z nich jest celownik termowizyjny Legat R Smart wyposażony w bardzo czuły sensor mikrobolometryczny, a także jasny obiektyw o ogniskowej 50 mm. Dzięki temu obraz jest klarowny i wyraźny – niezależnie od otoczenia. Co więcej, za sprawą modułu Wi-Fi może on być bezprzewodowo przesyłany na urządzenia mobilne znajdujące się w promieniu 100 metrów.





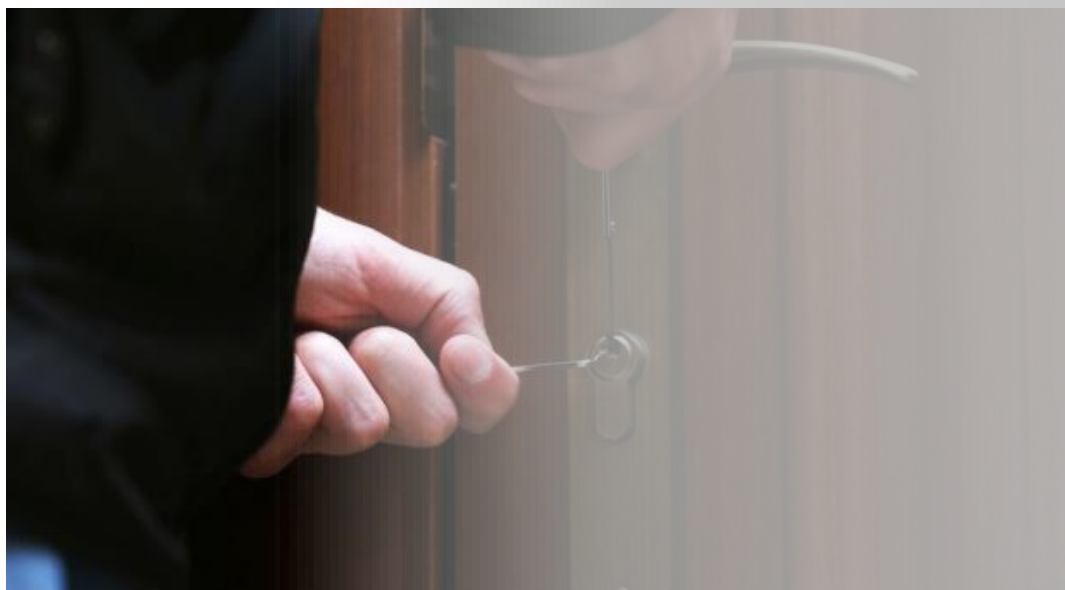
Kolejna odwiedzona strona to strona twierdzy (www.twierdza.info.pl) gdzie w numerze można również zapoznać się z ciekawymi artykułami i wypowiedziami w zakresie bezpieczeństwa technicznego. Artykuł pod tytułem Współczesne systemy monitoringu wideo autorstwa Mariana Mazurskiego. Artykuł stawia pytanie: Czy monitoring wizyjny jest najbardziej uniwersalnym rozwiązaniem spośród wszystkich systemów zabezpieczeń? Autor próbuje odpowiedzieć na to pytanie, przedstawiając możliwości wykorzystania systemów CCTV w różnych zastosowaniach. Czy mu się udaje? Artykuł o tytule Jak czytać parametry? Autorstwa Mariana Mazurskiego, który podejmuje próbę przedstawienia zestawienia parametrów najpopularniejszych w Polsce szybkoobrotowych kamer HD IP, czyli zintegrowanych kamer wysokorozdzielczych z mechanizmem uchylno-obrotowym i zoomem, których medium transmisyjnym jest przewodowa lub bezprzewodowa sieć LAN.

W artykule o tytule Ochrona szyta na miarę obiektu i jego użytkowników, autor Bartek Piotrowski, reprezentujący firmę SATEL podejmuje próbę wykazania, że elektroniczne zabezpieczenia techniczne, w tym systemy alarmowe, aby spełnić swoje zadanie, muszą być jak najlepiej dopasowane do oczekiwań użytkowników i typu chronionego obiektu. Na co należy zwrócić uwagę przy wyborze urządzeń SSWiN? Ciekawa próba wykazania, że kwestia projektowania i doboru urządzeń jest bardzo ważna w efektywności działania określonego systemu zabezpieczeń.

Kolejna odwiedzona strona to ABI EXPERT (www.abi-expert.pl). Ochrona danych osobowych zawsze była istotna i ważna, natomiast ostatnio kiedy to wszyscy wokół straszą karami wynikającymi z wprowadzenia nowych, unijnych przepisów w zakresie ochrony danych osobowych w Polsce kwestia ta nabrzmiewa i staje się tematem wielu rozmów ekspertów w zakresie bezpieczeństwa. Na stronie znajdziemy artykuł o kierunkach zmian przepisów dotyczących danych osobowych.



Jednym z zasadniczych celów rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE L 119 z 04.05.2016) – dalej: *rodo* – jak wynika z motywu 10 preambuły *rodo*, jest zapewnienie równorzędnego we wszystkich państwach członkowskich stopnia ochrony praw i wolności osób fizycznych w związku z przetwarzaniem ich danych. Nie oznacza to jednak całkowitego wyłączenia możliwości państw członkowskich zarówno w doprecyzowaniu stosowania tego aktu w przepisach krajowych, jak i w przyjmowaniu uregulowań sektorowych w dziedzinach wymagających przepisów bardziej szczegółowych, na co wyraźnie wskazuje prawodawca unijny w motywie 10 preambuły *rodo*. Kolejny artykuł dotyczy dopuszczalności stosowania biometrii przez pracodawcę w świetle *rodo*.



Z uwagi na intensywny rozwój technologii biometrycznych należy się spodziewać wzrostu zainteresowania pracodawców wykorzystywaniem biometrii dla realizacji różnych celów związanych z zatrudnianiem pracowników. Zdaje się to dostrzegać prawodawca unijny, ponieważ zdecydował się unormować *explicite* przetwarzanie danych biometrycznych. W nowym akcie prawa UE – *rodo* – prawodawca unijny wprowadza pojęcie danych biometrycznych, jednocześnie kwalifikując je, z pewnym zastrzeżeniem, do kategorii danych szczególnie chronionych. W rezultacie oznacza to, począwszy od 25 maja 2018 r., tj. daty rozpoczęcia stosowania przepisów *rodo*, dopuszczalność korzystania przez pracodawców z narzędzi biometrycznych będą wyznaczały nowe reguły. I kolejny artykuł dotyczący przetwarzania danych osobowych w systemach kontroli dostępu. Dostęp do danych osobowych powinien być ograniczany wyłącznie do osób upoważnionych. Jedną z form ograniczania takiego dostępu jest stosowanie systemów kontroli dostępu. Paradoksalnie, wdrażając taki system, administrator zaczyna przetwarzać dane osobowe specjalnie do tego celu. Kontrola dostępu jest niczym innym jak zarządzaniem: kto, do czego i kiedy ma dostęp. Przedmiotem kontroli dostępu może być informacja w systemie IT, dokumenty czy nośniki z informacjami w obszarze przetwarzania. System takiej kontroli może być kombinacją rozwiązań teleinformatycznych, mechanicznych i organizacyjnych, zapewniających zbieranie informacji kto, kiedy i do czego miał dostęp. Najprostszy, niezautomatyzowany system kontroli dostępu polega na każdorazowym wpisaniu się – zarejestrowaniu w specjalnym rejestrze – każdej osoby wchodzącej do danego pomieszczenia lub dopuszczanej do konkretnych dokumentów. I na koniec artykuł dotyczący danych osobowych w badaniach klinicznych produktów leczniczych.

Podmioty prowadzące badania kliniczne w praktyce napotykają wiele trudności związanych z ochroną i przetwarzaniem danych osobowych uczestników włączanych do badania. Rozbieżności interpretacyjne dotyczą stosowania przepisów uodo w stosunku do badań klinicznych uregulowanych w przepisach prawa farmaceutycznego oraz rozporządzeniach. Generalny Inspektor Ochrony Danych Osobowych (dalej: GIODO) już w 2013 r. za temat przewodni VII Dnia Ochrony Danych Osobowych wybrał „Dane osobowe w ochronie zdrowia i badaniach klinicznych” i podkreślał wielokrotnie, że kwestia przetwarzania danych osobowych na potrzeby prowadzenia badań klinicznych wymaga przemyślenia, jednak dotychczas brakuje jego jednoznacznego stanowiska w tych kwestiach. Dla uczestników biorących udział w danym badaniu istotne jest także to, czy mają oni prawo wiedzieć, czy jest im podawany badany produkt leczniczy czy placebo.





Sponsorzy badań klinicznych oraz osoby lub jednostki organizacyjne prowadzące badania kliniczne na zlecenie, czyli tzw. organizacje CRO (ang. Contract Research Organization) czekają na rozpoczęcie stosowania przepisów rozporządzenia w sprawie badań klinicznych, które ma nastąpić prawdopodobnie 1 lipca 2019 r. Przepisy rozporządzenia w sprawie badań klinicznych w sposób jasny regulują materię przetwarzania danych osobowych oraz odsyłają w art. 56 do mających zastosowanie przepisów dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych oraz rozporządzenia (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych, a więc z mocy art. 94 ust. 2 rodo w istocie do przepisów tego rozporządzenia.

Zanim przejdę do omówienia przedmiotowej analizy, chciałbym zdefiniować podstawowe pojęcia, których używałem w analizie. Opisanie tych pojęć pozwoli na wskazanie i zrozumienie funkcji poszczególnych elementów systemu teleinformatycznego kolokwialnie nazywanego „Telefonem 112”.

Aby zacząć mówić o zarządzaniu kryzysowym musimy cofnąć się do roku 1998. Tego bowiem czasu sięga geneza budowy w Polsce systemu zarządzania kryzysowego, którego elementem stał się w okresie późniejszym system teleinformatyczny nazywany Ogólnopolską Siecią Telefonu 112.

Pierwszą poważną próbą stworzenia takiego systemu podjęto w latach 1998 - 2000. Polegała ona na próbie przekształcenia Obrony Cywilnej w powszechny system ochrony ludności, którego rozwiązania wzorowane były na doświadczeniach podobnych systemów działających w państwach NATO. Siłami wykonawczymi systemu miały być profesjonalne siły ratownicze. Zakładano, że będą je stanowić wydzielone pododdziały Państwowej Straży Pożarnej, Wojska Polskiego, Policji, a także korpusu technicznego Obrony Cywilnej. Siłami wspierającymi miały być organizacje społeczne o charakterze ratowniczym, organizacje pozarządowe i pomocy humanitarnej.



Podjęta próba stworzenia powszechnego systemu zarządzania kryzysowego udała się tylko częściowo w czasie wprowadzania w życie reformy administracyjnej kraju.

Polska nie dysponuje również, zintegrowanym ze wszystkimi służbami rządowym Centrum Zarządzania Kryzysowego, które pozwalało by premierowi na koordynację działań tych służb w sytuacjach kryzysowych. Powyższe od wielu lat skutkuje chaosem prawnym, kompetencyjnym i organizacyjnym powodującym marnotrawstwo środków publicznych na realizację najczęściej nieudanych prób budowy modułów systemu zarządzania kryzysowego. Mimo upływu 15 lat od dyrektywy unijnej nakazującej wdrożenie OST 112 nie jest do dziś w pełni gotowy.





Wskazane powyżej CPR miały zajmować się między innymi przyjmowaniem i selekcją zgłoszeń o nagłym zagrożeniu życia, zdrowia, środowiska i mienia. Ponad to wspomaganiem koordynatora medycznych działań ratowniczych. Koncepcja ta była w założeniu projektem pozwalającym Ministrowi Spraw Wewnętrznych na wywiązanie się z obowiązku nadzoru nad funkcjonowaniem systemu powiadamiania ratunkowego. Do nadzoru takiego Minister Spraw Wewnętrznych zobligowany był treścią artykułu 12 ustawy z dnia 24 sierpnia 1991 roku o ochronie przeciwpożarowej. Powyższe wynikało z porozumienia podpisanego 8 czerwca 2000 roku pomiędzy Ministrem Zdrowia i Ministrem Spraw Wewnętrznych. Stało się jednocześnie podstawą organizacji i standaryzacji CPR.

Mijały lata w, trakcie których podejmowano kolejne nieudane i rozbieżne próby budowy zarówno CPR jak i wdrożenia Dyrektywy 2002/22/WE Parlamentu Europejskiego i Rady z dnia 7 marca 2002 roku w sprawie „Usługi Powszechnej” (Dz.U.E.L2002.108.51).

Po raz pierwszy pojęcie numeru 112 pojawiło się w roku 2005. Połączenia z tego numeru miały być odbierane w każdym powiecie. Fizycznie wywołania z tego numeru odbierane były w stacjach pogotowia ratunkowego i w stacjach kierowania krajowego systemu ratowniczo gaśniczego. Dopiero Ustawa z dnia 8 września 2006 roku o Państwowym Ratownictwie Medycznym (Dz. U numer 191, poz. 1940 ze zm.) z dniem 1 stycznia 2007 założyła, że przyjęcie wywołań alarmowych z numeru 112 spoczywa na powołanych przez wojewodę Centrach Powiadamiania Ratunkowego – CPR. W myśl poprzedniej ustawy o ratownictwie medycznym z 21 lipca 2001 roku CPR stanowiły zintegrowane stanowiska dyspozytorskie służb ratowniczych i usytuowane były na poziomie powiatowym i ponad powiatowym lecz nie na wojewódzkim.

Użycie tej samej nazwy dla CPR funkcjonujących na różnych poziomach administracji i faktycznie realizujących inne zadania spowodowało, z obawy o utratę podstaw prawnych do zaniechania budowy zintegrowanych stanowisk dyspozytorskich na poziomie powiatowym i ponad powiatowym. Powyższe doprowadziło do dezintegracji procesu integracji służb ratowniczych.

We wrześniu 2007 roku w MSW powstał dokument pod nazwą „Koncepcja Systemu 112”. Dokument służył zasadniczo jedynie wypełnieniu unijnej dyrektywy, o której już wcześniej mówiłem. Proponowane w Koncepcji rozwiązania zamiast wprowadzać narzędzia pomocnicze do już istniejących i sprawdzonych rozwiązań takich jak na przykład platforma lokalizacyjna, postulowały tworzenie rozwiązań nowych powiększając jedynie koszty.



Dla prawidłowego działania – zgodnie z wymogami UE, system wymagał usługi lokalizacji abonentów sieci. Podobnie rzecz się ma z konieczną szczegółową analizą wspomnianego dokumentu to jest” Koncepcji Systemu 112 z września 2007 roku”. Powołany dokument wytworzony został w celu określenia jednolitej, praktycznej koncepcji realizacji przepisów dotyczących numeru alarmowego 112, oraz centrum powiadamiania ratunkowego. Koncepcja systemu 112 w Polsce, jak i rozporządzenia z dnia 17 września 2007 r. w sprawie szczegółowej organizacji centrów powiadamiania ratunkowego (Dz. U. Nr 178, poz. 1263) stanowiły we wrześniu 2007 roku dwa główne elementy mające umożliwić optymalną realizację wdrażania systemu powiadamiania ratunkowego na numer alarmowy 112.

Koncepcja zdeterminowana była, jak podnosili autorzy powołanego dokumentu realizacją podstawowego zadania jakim jest stworzenie skutecznego krajowego systemu przeznaczonego do odbioru i obsługi zgłoszeń na numer alarmowy 112 uwzględniającego aktualny stan prawny. Koncepcja w swoim zakresie obejmowała: zasady finansowania budowy i organizacji systemu 112, określał przyjęte definicje i wskazywał ponad to na przyjęte założenia i rozwiązania techniczne. Koncepcja została oparta, jak podnosili wytwórcy dokumentu o rozwiązania przyjęte w obowiązującym w Polsce porządku prawnym ze szczególnym uwzględnieniem ustawy z dnia 8 września 2006r. o Państwowym Ratownictwie Medycznym (Dz.U. Nr 191 poz. 1410 z późn. zm.) oraz zawartej w art. 25 ust.3 delegacji ustawowej do wydania rozporządzenia z dnia 17 września 2007r. w sprawie szczegółowej organizacji centrów powiadamiania ratunkowego (Dz.U. Nr 178 poz. 1263), ustawy z 16 lipca 2004r.- Prawo Telekomunikacyjne (Dz.U. Nr 171 poz. 1800 z późn. zm.) i ustawy z dnia 26 kwietnia 2007r. o zarządzaniu kryzysowym (Dz.U. Nr 89, poz. 589 z późn. zm.).



Autorzy Koncepcji definiowali pojęcie systemu 112 jako jednolity krajowy system odbioru zgłoszeń na numer alarmowy 112. System ten obejmować miał sieć Centrów Powiadamiania Ratunkowego (CPR), których celem było przyjmowanie, przetwarzanie i obsługa zgłoszeń na numer alarmowy 112. W szczególności dotyczyło to przekazywanie szczegółowych informacji o zdarzeniu do właściwych terytorialnie stanowisk kierowania służb. Powyższe w celu umożliwienia podjęcia interwencji, a w razie potrzeby utrzymania ciągłego połączenia osoby zgłaszającej zdarzenie oraz przekierowanie zgłoszenia do dyspozytora medycznego. Z systemem współdziałać miały wedle treści Koncepcji, służby Policji, Państwowej Straży Pożarnej, pogotowia ratunkowego, a także inne podmioty ratownicze, do których przekierowywane są zgłoszenia alarmowe, i które zwrotnie potwierdzają podjęcie akcji ratowniczej lub innej interwencji.

W ramach ww. projektu zgłoszone zostały następujące inwestycje, które miały być realizowane z udziałem środków POIŚ: wykonanie projektu adaptacyjnego budynków, adaptacja obiektów przeznaczonych na centra powiadamiania ratunkowego oraz wyposażenie centrów powiadamiania ratunkowego w sprzęt niezbędny do ich prawidłowego funkcjonowania. Środki, którymi mieli dysponować wojewodowie na budowę CPR miały uwzględniać partycypację w kosztach zamówienia centralnego jak i realizację zadań własnych pojmowanych jako adaptację i przystosowanie budynków na potrzeby CPR.

W okresie 2011 - 2013 Ministra Spraw Wewnętrznych dopuścił do organizowania w większości województw Wojewódzkich Centrów Powiadamiania Ratunkowego z pominięciem powiatowych centrów powiadamiania ratunkowego, mimo że podstawę systemu, zgodnie z prawem miały stanowić powiatowe centra powiadamiania ratunkowego działające lokalnie. Zrezygnowano z tworzenia w organizowanych wojewódzkich centrach wspólnych stanowisk kierowania. Zgodnie z zapisami Ustawy O ochronie przeciwpożarowej (art. 14a ust. 2 pkt 1 i 2) w skład Wojewódzkiego CPR winno wchodzić stanowisko kierowania komendanta wojewódzkiego PSP oraz lekarza koordynatora ratownictwa medycznego (w powiatowych centrach powiadamiania ratunkowego odpowiednio: stanowisko kierowania komendantów powiatowych (miejskich) PSP oraz dyspozytorów medycznych. W roku 2012 Minister Spraw Wewnętrznych zaniechał działań na rzecz stworzenia jednolitego Ogólnokrajowego Cyfrowego Systemu Łączności Radiowej, który miał stanowić ważny element integracji działań poszczególnych służb ratunkowych stosownie do nowych wyzwań i rozwoju cywilizacyjnego. Decyzja ta była prawdziwym ciosem dla osób starających się o poprawę poziomu przygotowania państwa na sytuacje kryzysowe. W wyniku odwołania przetargu na wskazany system łączności nadal, także i dziś służby reagowania kryzysowego w tym Policja, PSP Ratownictwo Medyczne i oddziały WP nie są w stanie komunikować się między sobą za pomocą łączności radiowej dedykowanej tym służbom. Mogą to jedynie uczynić za pośrednictwem otwartych sieci teleinformatycznych komercyjnie działających telekomów.

Od wielu lat interesuję się problematyką bezpieczeństwa, w tym w szczególności zarządzaniem kryzysowym. Staram się na bieżąco zapoznawać z dostępnymi publikacjami na ten temat. Nieocenionym źródłem informacji w przedmiotowych kwestiach są raporty Ośrodka Studiów Wschodnich oraz Najwyższej Izby Kontroli. Jeśli chodzi o tę ostatnią instytucję na szczególną uwagę zasługują Informacja o wynikach kontroli „Przygotowanie Systemu Ochrony Ludności Przed Klęskami Żywiotowymi oraz Sytuacjami Kryzysowymi” Informacja została zatwierdzona przez Prezesa NIK w dniu 20 czerwca 2013 roku.

Analizując postępy w budowie systemu zarządzania kryzysowego w Polsce, w tym OST 112 korzystałem z tego i kilku innych źródeł informacji na temat zarówno systemu powiadamiania ratunkowego, zarządzania kryzysowego, ratownictwa medycznego, ratownictwa PSP oraz na bieżąco śledziłem losy próby zbudowania w Polsce nowoczesnego cyfrowego systemu łączności radiowej dedykowanego służbom ratowniczym i porządku publicznego zwanego kolokwialnie systemem w standardzie TETRA.

Mariusz Furmanek



Praktycznie we wszystkich jednostkach organizacyjnych dla właściwego ich funkcjonowania muszą być i są przetwarzane dane osobowe. Co oczywiste dane te są przetwarzane w różnym zakresie, różnym dla różnych jednostek organizacyjnych. Trudno wyobrazić sobie dwie jednostki organizacyjne, które będą przetwarzały dokładnie te same dane osobowe. Oczywiście jest, że różne dane będą przetwarzane w różnych uwarunkowaniach organizacyjnych, technicznych, fizycznych czy informatycznych. Te kwestie będą zależały od świadomości najwyższego kierownictwa danej jednostki organizacyjnej, ale również od zasobności portfela i możliwości przeznaczenia określonych środków finansowych na zabezpieczenie danych osobowych. Chcąc właściwie zrozumieć sytuację ochroną danych osobowych w nowych uwarunkowaniach prawnych należy zrozumieć i zaakceptować nowe mechanizmy i najważniejsze zmiany jakie wprowadzi rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, dalej zwane rodo, w stosunku do rozwiązań obowiązujących na gruncie ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, zwanej uodo. Podstawową różnicą między rodo a poprzedzającą je dyrektywą 95/46/WE jest brak potrzeby implementacji nowych przepisów do krajowego porządku prawnego. Nowe przepisy będą obowiązywały wprost. Nie oznacza to oczywiście, że nie będzie czy nie może być krajowych przepisów w zakresie ochrony danych osobowych.



Aby podjąć odpowiednie decyzje, konieczne jest znalezienie odpowiedzi na pytanie: jak właściwie zrównoważyć w organizacji bezpieczeństwo, technologię i finanse? Każdy podmiot przetwarzający informacje musi dokonać wyboru, jakie rozwiązania techniczne i organizacyjne będzie stosował. Porównując koszty i uzyskiwane korzyści dotyczące wydajności, bezpieczeństwa, dostępności oraz zarządzania infrastrukturą, należy podjąć decyzję o optymalnie dobranych środkach, które będą wchodziły w skład systemu przetwarzania danych osobowych. Zgodnie z obowiązującymi uwarunkowaniami prawnymi to na administratorze danych osobowych ciąży obowiązek wykazania, że sposób, w jaki przetwarza dane, odpowiada wymaganiom stawianym przez przepisy, normy, dobre praktyki i regulacje branżowe.

Za kilka miesięcy zaczną obowiązywać wymagania stawiane przez rodo (tu podać pełną nazwę dokumentu), które niestety przy swojej złożoności i dużej objętości, nie wskazują, w jaki konkretny sposób należy wypełniać obowiązki w zakresie organizacyjnym, technicznym, a nawet formalnym, gdy dotyczy to realizacji zagadnień związanych z funkcjonowaniem procesów informatycznych. Administrator ma sam podejmować decyzje, bazując na prowadzonej analizie ryzyka przetwarzanych danych i jego wpływu na prawa i wolności podmiotów danych.

Działania przygotowujące do stosowania rodo są następujące:

- Analiza formularzy służących gromadzeniu danych i ocena ich zgodności z wymogami dotyczącymi zgody na przetwarzanie danych oraz dopełnienia obowiązku informacyjnego wynikającego z przepisów rodo;
- Analiza dokumentacji ochrony danych oraz dostosowanie jej do nowych wymogów, zwłaszcza utworzenie rejestru czynności przetwarzania danych, co jak się wydaje może być dokonane w oparciu o politykę bezpieczeństwa;
- Przejrzenie umów powierzenia przetwarzania danych pod kątem zgodności z wymogami zawartymi w rodo i dostosowanie umów do nowych wymogów;
- Przygotowanie się do spełnienia obowiązków związanych z informowaniem o naruszeniu ochrony danych osobowych. ABI powinien także rozważyć, czy nie zachodzi potrzeba przeprowadzenia oceny skutków dla ochrony danych, o której mowa w art. 35 rodo;
- Przygotowanie się przez osobę mającą pełnić funkcję inspektora ochrony danych osobowych do realizacji nowych zadań. Przepisy krajowe powinny dookreślić, w jaki sposób powinny być realizowane niektóre obowiązki np. poinformowanie organu nadzorczego o danych kontaktowych inspektora;



Ustawodawca w rodo zawiera szereg przepisów określających pozycję i zadania inspektora ochrony danych, który ma zastąpić urzędnika do spraw ochrony danych, w polskich przepisach nazywanego administratorem bezpieczeństwa informacji (ABI). Wyznaczenie inspektora będzie obowiązkowe we wskazanych przypadkach. Dotyczy to całego sektora publicznego oraz podmiotów prywatnych, które przetwarzają na dużą skalę dane wrażliwe, bądź ich główna działalność polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą. Użyte we wskazanym przepisie sformułowania są nieostre i mogą być różnie interpretowane. Przepisy przewidują możliwość powołanie jednego inspektora dla wielu administratorów, Ustawodawca w rodo nakłada na administratora, a także na podmiot przetwarzający dane na zlecenie administratora, obowiązek publikacji danych kontaktowych inspektora ochrony danych i zawiadomienia o nich organu nadzorczego. Inspektor w odróżnieniu od ABI będzie reprezentował administratora w kontaktach zewnętrznych, a nie tylko wewnętrznych jednostki organizacyjnej, będzie podejmował działania mające na celu realizację uprawnień podmiotów danych.



Artur Bogusz

KOMPLEKSOWE **R**OZWIĄZANIA **O**CHRONY **N**IEJAWNEJ

KRON SP. Z O.O.

UL. TADEUSZA KOŚCIUSZKI 21

05-500 PIASECZNO

KONTAKT TEL. 605-67-47-14, 601-377-431

EMAIL: INFO@NIEJAWNY24.PL

- RZECZOZNAWSTWO W ZAKRESIE BEZPIECZEŃSTWA TECHNICZNEGO I FIZYCZNEGO
- AUDYTY, WDROŻENIA, NADZÓR, DORADZTWO
- PROJEKTOWANIE, OBSŁUGA SYSTEMÓW BEZPIECZEŃSTWA TECHNICZNEGO W PEŁNYM ZAKRESIE
- INTEGRACJA SYSTEMÓW, OPTIMALIZACJA
- KOMPLEKSOWA BUDOWA KANCELARII TAJNYCH, POMIESZCZEŃ SPECJALNYCH, MAGAZYNÓW BRONI
- BEZPIECZEŃSTWO PRZEMYSŁOWE (ANALIZA ROZWIĄZAŃ, DOKUMENTACJI)

WWW.NIEJAWNY24.PL

**Miejsce na Twoją
reklamę**



Międzynarodowe Targi Poznańskie



securex[®]
P O L A N D

Międzynarodowe Targi Zabezpieczeń

23-26.04.2018
POZNAŃ

Zabezpiecz
swój sukces!

www.securex.pl

Biuro Usług Rzeczoznawczych i Konsultingowych

W ramach Ogólnopolskie Stowarzyszenia Inżynierów i Techników Zabezpieczeń Technicznych i Zarządzania Bezpieczeństwem **POLALARM**, które jest organizacją o charakterze naukowo-technicznym, zrzeszającą osoby zajmujące się w sposób profesjonalny zagadnieniami związanymi z technicznym zabezpieczeniem osób i mienia, kwestiami bezpieczeństwa informacji i zabezpieczania danych oraz problematyką zarządzania bezpieczeństwem funkcjonuje Biuro Usług Rzeczoznawczych i Konsultingowych (BURiK).

W dyspozycji Biura pozostaje ponad 100 przeszkolonych rzeczoznawców systemów zabezpieczających na terenie całej Polski. Rzeczoznawcy posiadają niezbędną wiedzę i uprawnienia w zakresie technicznych systemów zabezpieczeń, która pozwala realizować wszelkie prace, które swoim zakresem obejmują systemy bezpieczeństwa. Rzeczoznawcy ci działają według zasad zawartych w Uchwale Nr 20/98 Rady Krajowej Federacji Stowarzyszeń Naukowo-Technicznych w sprawie statusu rzeczoznawców oraz zasad organizacji rzeczoznawstwa stowarzyszeń naukowo-technicznych zrzeszonych w Federacji SNT NOT.



Biuro Usług Rzeczoznawczych i Konsultingowych

Specjalizacja Biura Usług Rzeczoznawczych i Konsultingowych Stowarzyszenia obejmuje zagadnienia z zakresu:

- wykonywanie audytów systemów bezpieczeństwa wskazanych obiektów;
- przeprowadzanie działań audytowych w zakresie bezpieczeństwa obiektów w ujęciu normy 27001,
- opracowywanie raportów i zaleceń do udoskonalania i przebudowywania technicznych systemów zabezpieczeń, po przeprowadzeniu odpowiedniego audytu bezpieczeństwa,
- opiniowaniu projektów systemów zarządzania bezpieczeństwem,
- opiniowaniu systemów i urządzeń technicznych służących ochronie osób i mienia,
- opracowywanie koncepcji i projektów wykonawczych ochrony obiektów i obszarów z wykorzystaniem systemów technicznego zabezpieczenia osób i mienia oraz uwzględniających aspekty organizacyjne, prawne, obowiązujące procedury i instrukcje wewnętrzne,
- reprezentowania osób prawnych i instytucji państwowych w charakterze inwestora zastępczego w obszarze bezpieczeństwa technicznego,
- upowszechnianiu informacji technicznej w zakresie pozytywnie zweryfikowanych systemów i urządzeń służących ochronie osób i mienia,
- rekomendowaniu produktów i usług w dziedzinie systemów technicznej ochrony.

Zapraszamy do współpracy z Biurem. Kontakt:
artur.bogusz@polalarm.org.

SZKOLENIA W STOWARZYSZENIU POLALARM

W związku z rosnącym zainteresowaniem stosowaniem praktycznym w pracy instalatorów i projektantów elektronicznych systemów zabezpieczeń obowiązujących Norm Obronnych, Nasze Stowarzyszenie organizuje szkolenia w zakresie posługiwania się Normą Obronną, Obiekty Wojskowe, Systemy Alarmowe, NO-04-A004 arkusze od 1 do 9.

Szkolenie będzie miało na celu zapoznanie z uwarunkowaniami prawnymi, organizacyjnymi, technicznymi i praktycznymi wynikającymi z zapisów poszczególnych arkuszy Normy Obronnej. Celem szkolenia jest jak najlepsze przygotowanie osób zainteresowanych do posługiwania się zapisami Normy Obronnej w praktyce projektowej czy instalatorskiej.

W POLALARMIE prowadzone są bardzo intensywne prace mające na celu przygotowanie *„Poradnika stosowania praktycznego Norm Obronnych, Obiekty wojskowe, Systemy alarmowe serii NO-04-A004 arkusze od 1 do 9”*. Publikacja ta ma być pomocna instalatorom i projektantom w praktycznym poruszaniu się w obszarze Norm Obronnych.

Wszystkich zainteresowanych odbyciem takiego szkolenia zapraszamy do zgłaszania się do Biura Stowarzyszenia pod numer telefonu +48 503 828 424 lub pod adres email: polalarm@polalarm.com.pl.

Ogólnopolskie Stowarzyszenia Inżynierów i Techników Zabezpieczeń Technicznych i Zarządzania Bezpieczeństwem



POLALARM

Redaktor Naczelny Biuletynu Informacyjnego: Artur Bogusz
Redakcja: Artur Bogusz;
Stowarzyszenie POLALARM
ul. Poleczki 40, 02-822 Warszawa
tel. +48 503 828 424, 22 626 90 31;
e-mail: polalarm@polalarm.com.pl, www.polalarm.org
Konto bankowe:
ALIOR BANK 70 2490 0005 0000 4520 4686 4115

Redakcja nie odpowiada za treść zamieszczonych artykułów, reklam i ogłoszeń.
Wszelkie prawa zastrzeżone. Nakład jednorazowy 150 egz.

Warszawa, październik 2017 r.