OCHRONA i BEZPIECZEŃSTWO OBIEKTÓW I BIZNESU

Nr 1/2024 styczeń/luty
Cena 17,50 (w tym 8% VAT), ISSN 2658-1779, nr ind. 381756

ZINTEGROWANA PLATFORMA BRIVO DO KONTROLI DOSTĘPU

ŚWIATOWY LIDER I PIONIER W ZAKRESIE KONTROLI DOSTĘPU I PLATFORM OCHRONY OPARTYCH W CHMURZE

Kontrola dostępu
Zautomatyzuj kontrolę dostępu budynku oraz raportowanie

Monitoring wizyjny
Wyświetlaj obrazy w czasie rzeczywistym i przeglądaj zapisy

Zdalne zarządzanie
Zarządzaj zabezpieczeniami z dowolnego urządzenia mobilnego

Zarządzanie użytkownikami
Nadawaj uprawnienia użytkownikom w systemie

Kontrola odwiedzających
Bezpieczne warunki dla odwiedzających i pracowników

Analiza danych
Przetwarzaj informacje na temat bezpieczeństwa fizycznego

Dzień dobry,

Pierwszy numer naszego czasopisma w 2024 roku poświęcamy przede wszystkim bezpieczeństwu obiektów użyteczności publicznej, ze szczególnym uwzględnieniem budynków sądów. Powodem tego są przede wszystkim zmiany przepisów prawa, które weszły w tym zakresie jesienią ubiegłego roku.

Omówienie nowych zasad ochrony budynków sądów znajdziecie Państwo w artykule mojego autorstwa. Cezary Mecwaldowski prezentuje tematykę i dokonuje przeglądu urządzeń do kontroli i zapobiegania przemytom na terenie zakładów karnych. W tym kontekście należy także czytać artykuły Roberta Gabrysiaka dotyczące depozytorów kluczy i innych przedmiotów oraz integracji systemów PSIM i SMS.

Wielkimi krokami zbliża się także „konferencyjna wiosna". Już dzisiaj zapraszamy Państwa do uczestnictwa w III Międzynarodowych Targach POLSECURE w Kielcach, które według zapowiedzi organizatorów wydają się jeszcze ciekawsze niż poprzednie edycje. W nowej odsłonie odbędą się także organizowane w cyklu dwuletnim targi SECUREX w Poznaniu. Wiemy, że wielu naszych czytelników nie może się doczekać kolejnego Spotkania Projektantów Instalacji Niskoprądowych, którego wiosenna edycja odbędzie się w malowniczej Ostródzie.

Do zobaczenia!

Sergiusz Parszowski
Redaktor programowy

Dwumiesięcznik Ochrona i Bezpieczeństwo powstaje we współpracy z

Forum Służby Więziennej

Instytut Bezpieczeństwa Pożarowego NODEX Niezależny Ośrodek Doradców i Ekspertów

PISA

polsecure

Targi Kielce
exhibition & congress centre

III Międzynarodowe Targi POLSECURE

23-25.04.2024
Targi Kielce

Budujemy bezpieczną przyszłość

polsecure.targikielce.pl

#PublicSecurity #UniformedForces #Cybersecurity #Safety

TARGI SECUREX – PROFESJONALNIE O BEZPIECZEŃSTWIE

W ostatnich miesiącach słowo „bezpieczeństwo” odmieniane jest przez wszystkie przypadki, w najróżniejszych kontekstach. Umiejętność dostrzegania i usuwania zagrożeń to podstawa działania każdego podmiotu, niezależnie od skali i zasięgu funkcjonowania. W dniach 23–25 kwietnia 2024 roku na Międzynarodowych Targach Poznańskich odbędą się Targi Zabezpieczeń SECUREX, skupiające się na zagadnieniu bezpieczeństwa budynków, osób, mienia i cyberprzestrzeni.

Najbliższa edycja tego odbywającego się w cyklu dwuletnim wydarzenia przyjmie odświeżoną formułę, jeszcze lepiej trafiając w oczekiwania i potrzeby profesjonalistów zajmujących się zabezpieczeniami. Wydarzenie zostanie wzbogacone o spotkania z największymi autorytetami branży, bezprecedensową możliwość wymiany wiedzy oraz prezentację innowacyjnych rozwiązań na międzynarodową skalę. To tutaj swój asortyment prezentują liderzy rynku oraz firmy wyspecjalizowane w tworzeniu systemów zabezpieczeń dla poszczególnych sektorów. Program wydarzeń odpowiada na aktualne wyzwania branży.

Tematem przewodnim nadchodzącej edycji Targów SECUREX będzie „Bezpieczna przyszłość. Niekonwencjonalne rozwiązania w branży security”. W oparciu o dotychczasową tradycję Targów SECUREX zbudujemy wydarzenie w nowej formule, które jeszcze lepiej trafi w oczekiwania i potrzeby branży zabezpieczeń oraz odpowie na najważniejsze pytania dotyczące innowacji i trendów na najbliższe lata.

Ubiegłoroczne Targi SECUREX przyciągnęły praktyków wielu branż, w tym projektantów, inżynierów budownictwa i pożarnictwa, rzeczoznawców ds. zabezpieczeń, funkcjonariuszy służb, a także właścicieli i zarządzających obiektami. Mając na uwadze duże zainteresowanie tematyką szeroko rozumianego bezpieczeństwa organizatorzy przygotowują atrakcyjną propozycję na kolejną edycję – *Naszym nadrzędnym celem, jako Zespołu Targów SECUREX, jest stworzenie spotkania, z którego jego uczestnicy wyjdą usatysfakcjonowani najświeższą wiedzą i nowymi perspektywami, które przyjmą dzięki konfrontacji z szerokim wachlarzem produktów i ekspertów dostępnymi na Targach. Mówienie o zagrożeniach i przedstawianie sprawdzonych rozwiązań, jeszcze zanim wystąpi problem, to sedno naszego działania. Pragniemy zwiększać świadomość branżową, dlatego do współpracy zapraszamy wybitnych ekspertów i rynkowych liderów* – mówi Paulina Maniecka, dyrektor projektu SECUREX.

Targi SECUREX to możliwość spotkania z czołowymi dostawcami produktów i usług z zakresu ochrony mienia i osób, informacji, systemów alarmowych, urządzeń i systemów sygnalizacji, monitoringu wizyjnego, zabezpieczeń technicznych i systemowych oraz cyberbezpieczeństwa, a także sprawdzenia na żywo najnowszych rozwiązań i usług. Program wydarzeń towarzyszących zapewni uczestnikom dostęp nie tylko do najświeższej wiedzy branżowej, możliwość wymiany informacji z ekspertami, ale także wysłuchania najbardziej doświadczonych i charyzmatycznych postaci branży zabezpieczeń.

Ważnym punktem przyszłorocznego programu będzie I Międzynarodowy Kongres Zabezpieczeń Technicznych „W poszukiwaniu innowacji i dobrych praktyk”, zainicjowany dzięki współpracy Targów SECUREX, firmy Safety Project, Wyższej Szkoły Bezpieczeństwa Publicznego i Indywidualnego APEIRON oraz wsparciu współorganizatorów strategicznych: Polskiej Izby Systemów Alarmowych (PISA), Polskiej Izby Ochrony (PIO), Wojskowej Akademii Technicznej, Wydziału Bezpieczeństwa, Logistyki i Zarządzania oraz Centrum Ratownictwa.

Kolejną wartą uwagi przestrzenią będzie „walk of ideas” – specjalnie przygotowana strefa pokazowa zawierająca produkty z zakresu zabezpieczeń, które należą do kategorii: AI (sztuczna inteligencja), cloud computing (chmura danych), Internet of Things oraz cyberbezpieczeństwo.

Międzynarodowe Targi Zabezpieczeń SECUREX to od lat jedno z najważniejszych wydarzeń biznesowych skierowanych dla branży zabezpieczeń w Europie. Jego kolejna edycja odbędzie się w bloku targów biznesowych, wspólnie z Targami Energii Odnawianej greenPOWER, Targami Energetyki EXPOPOWER, Targami Ochrony Pracy, Pożarnictwa i Ratownictwa SAWO oraz Targami Branży Instalacyjnej INSTALACJE.

www.securex.pl

SPIN EXTRA 2024 – WIOSENNA EDYCJA WYDARZENIA JUŻ W MARCU!

W dniach **21–22 marca 2024** w **Hotelu Radisson Blu Resort & Conference Center, Ostróda Mazury** odbędzie się wiosenna edycja wydarzenia SPIN Extra 2024. Tradycyjnie podczas spotkania Partnerzy zaprezentują swoje rozwiązania podczas prelekcji. Do dyspozycji uczestników będzie część ekspozycyjna, w ramach której prowadzone będą prezentacje sprzętu i indywidualne doradztwo. Nie zabraknie konsultacji z ekspertami oraz czasu na rozmowy kuluarowe i integrację.

Edycja wiosenna dedykowana jest dla projektantów z północnej i centralnej Polski. Rejestracja na wydarzenie odbywa się za pośrednictwem formularza zamieszczonego na stronie: https://spin.lockus.pl/rejestracja/

Wśród Partnerów, którzy zaprezentują swoje rozwiązania podczas SPIN Extra 2024 znajdują się następujące firmy:

- **Złoci Partnerzy**: AAT Systemy Bezpieczeństwa, Bosch Building Technologies, Eltrox wraz z firmą Seagate i Pelco, Hanwha Vision, Konica Minolta wraz z Mobotix, Megavision Technology, Miwi Urmet, Reichle&De-Massari Polska, Roger wraz z firmą Sensor – Online, TP-Link
- **Srebrni Partnerzy**: Assa Abloy, Cloud Electronics, Eltcrac System, Emiter, Ewimar, IP&S, Optex, Promitel, ZKTeco
- **Brązowi Partnerzy**: 2N, ACO, Asbis Poland, BT Electronics, Elmark Automatyka, Faac, Novet

Tematyka SPIN obejmuje szeroki wachlarz specjalizacji z branży niskich prądów: od systemów sygnalizacji pożarowej, nowoczesnych systemów CCTV, systemów kontroli dostępu, systemów DSO, systemów zarządzania budynkiem, poprzez systemy zasilania gwarantowanego, rozwiązania Data Center, systemy parkingowe, po profesjonalne rozwiązania sieciowe, multimedialne i integrację systemów.

Szczegółowe informacje na temat nadchodzącej edycji można znaleźć na stronie internetowej: https://spin.lockus.pl/ oraz w mediach społecznościowych: FB: www.facebook.com/SPINiSPINExtra oraz LinkedIn: https://bit.ly/3IBOrcc

spin.lockus.pl/rejestracja/

ROGER

PREZENTACJA OPROGRAMOWANIA VISO 2.0.8 DO SYSTEMU RACS 5

roger
Intelligence for Building

Wersja 2.0.8 oprogramowania VISO polskiej platformy zarządzania bezpieczeństwem, kontroli dostępu oraz automatyki budynkowej wprowadza szereg nowych funkcji i udoskonaleń, wśród których najważniejsze to:

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

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

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

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

www.roger.pl

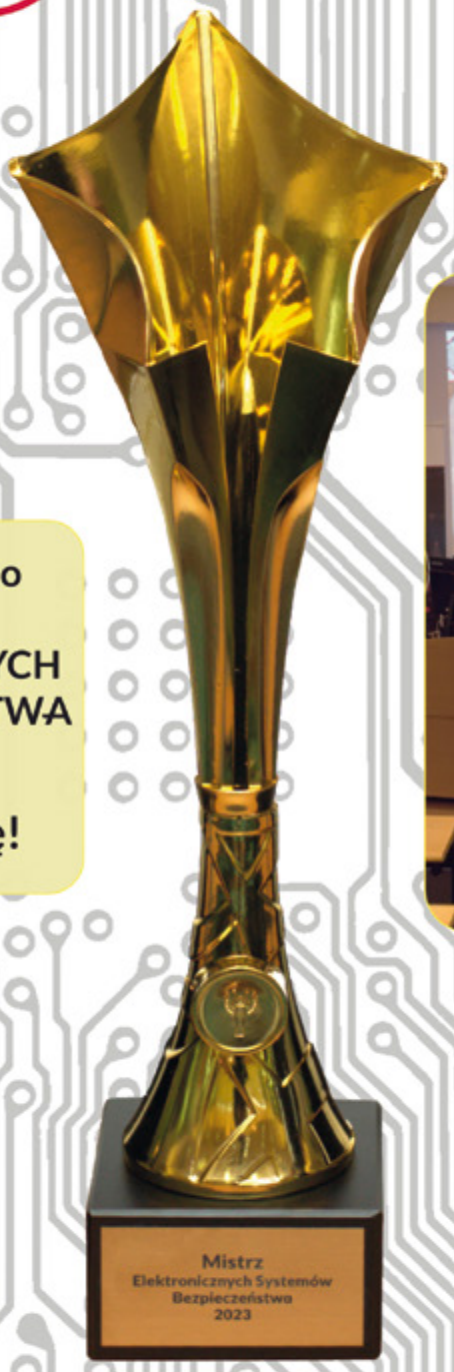
Wojskowa Akademia Techniczna

SEMINARIUM BRANŻY ELEKTRONICZNYCH SYSTEMÓW BEZPIECZEŃSTWA

IX EDYCJA

Wydział Elektroniki

Serdecznie zapraszamy na seminarium prowadzonego przez przedstawicieli firm wiodących w branży



W programie przewidziano konkurs o tytuł MISTRZA ELEKTRONICZNYCH SYSTEMÓW BEZPIECZEŃSTWA z cennymi nagrodami!

Sprawdź swoją wiedzę!

12 III 2024
godzina 8:30
aula E/100
ZAPRASZAMY

www.wel.wat.edu.pl

Adres:

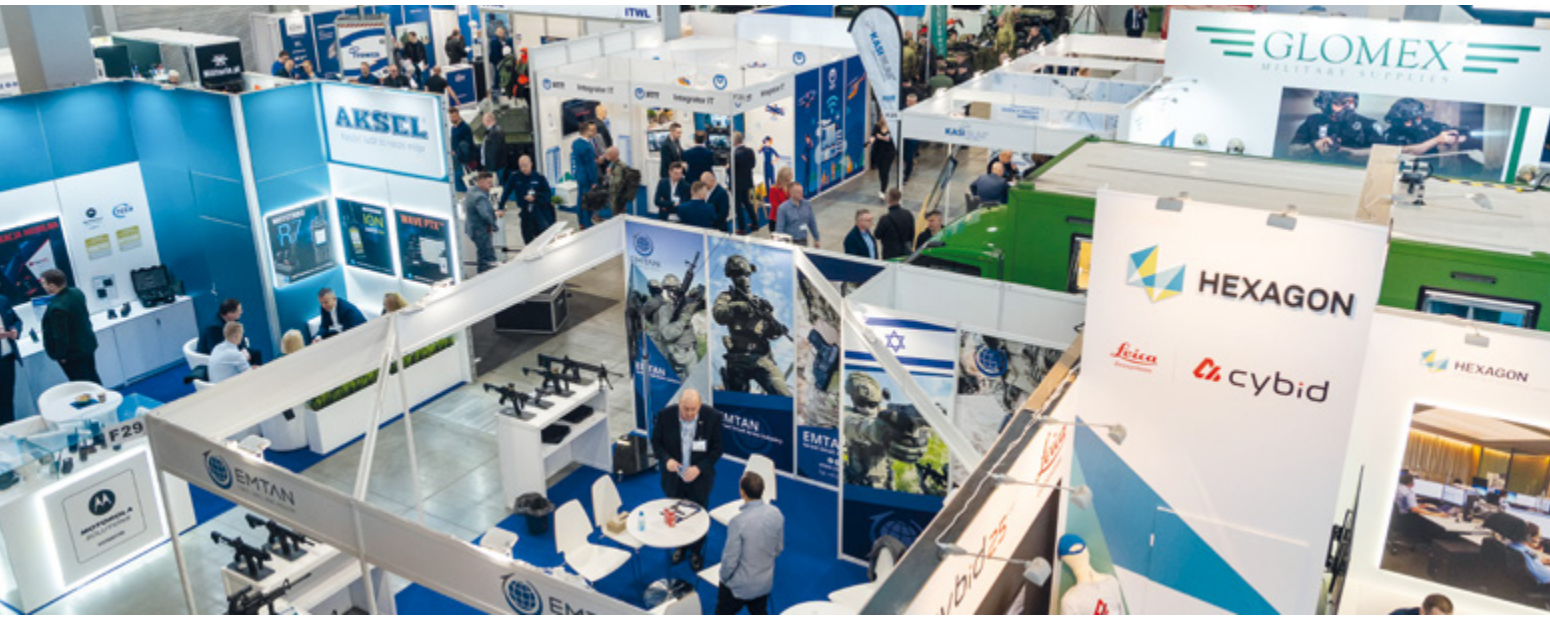
Wydział Elektroniki
Wojskowa Akademia Techniczna
ul. gen. Sylwestra Kaliskiego 2
00-908 Warszawa
bud. 45

Patron merytoryczny:

PISA
Polska Izba Systemów Alarmowych

Partner akademicki:

Szkoła Główna Służby Pożarniczej



TARGI DLA BEZPIECZEŃSTWA – CZYLI POLSECURE W 2024 ROKU!

Nowoczesny sprzęt, bieżące tematy konferencji – szeroko pojęte bezpieczeństwo wciąż jest tematem ważnym i aktualnym. Kolejna edycja wydarzenia, poświęconego tej tematyce, która odbędzie się w 2024 roku w Targach Kielce zapowiada się interesująco. Obok ważnego wsparcia Komendy Głównej Policji, organizatorzy kieleckich targów mogą również liczyć na zaangażowanie innych służb.

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

Odbiorcami targów są służby podległe Ministrowi Spraw Wewnętrznych i Administracji. Targi Polsecure dedykowane są więc Policji, Straży Granicznej, Państwowej Straży Pożarnej oraz Służbie Ochrony Państwa. Ofertą mogą też być zainteresowane służby specjalne, Krajowa Administracja Skarbowa oraz organizacje ratownicze GOPR, TOPR, WOPR.

– Myślę, że tego typu targi są bardzo potrzebne, zwłaszcza gdy mamy do czynienia z nowym sprzętem. Tu mamy możliwość zaprezentowania go bezpośredniemu użytkownikowi – tak POLSECURE 2023 podsumowywała Anna Makowska z firmy IBKOL. Czasem jest po prostu trudno dotrzeć ze sprzętem właśnie do tego użytkownika. Po tym evencie mamy bardzo pozytywny feedback. Mam nadzieję, że wrócimy tu w przyszłym roku.

Polsecure dołączyło w 2022 roku do portfolio Targów Kielce obok wystaw skierowanych do służb mundurowych, jak znany na całym świecie Międzynarodowy Salon Przemysłu Obronnego czy Międzynarodowe Targi Sprzętu i Wyposażenia Straży Pożarnej i Służb Ratowniczych IFRE-EXPO.

Miniona edycja targów dla bezpieczeństwa zajęła blisko 6 500 metrów kwadratowych. Wystawę odwiedziło przeszło 5 000 zwiedzających. Targi zostały także docenione poza granicami naszego kraju. Wystawę odwiedziło 36 delegacji z 27 krajów takich jak: Bułgaria, Chorwacja, Czechy, Estonia, Gruzja, Hiszpania, Izrael, Korea Południowa, Litwa, Łotwa, Malta, Mołdawia, Niemcy, Norwegia, Portugalia, Rumunia, Rwanda, Słowacja, Słowenia, Ukraina, USA, Węgry, Wielka Brytania, Włochy oraz przedstawiciele Europol-u i FRONTEX-u.

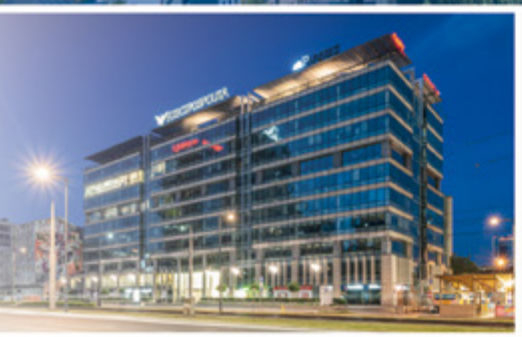
www.targikielce.pl

System kontroli dostępu RACS 5 w sektorze komercyjnym

roger
Intelligence for Building

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

Wybrane realizacje






TECHNOLOGICZNA REWOLUCJA W BRANŻY OCHRONY. TRENDY, KTÓRE ZMIENIĄ TEN SEKTOR W 2024 ROKU

System, który sam koordynuje dostawy, wykrywa ryzyko podczas zgromadzeń czy dba o przestrzeganie zasad BHP w zakładzie – rozwój technologiczny to trend, który w najbliższych miesiącach zdominuje branżę ochrony osób i mienia. I mocno wpłynie na formułę jej działania, zmieniając profil pracowników, powodując konsolidację firm i umożliwiając im maksymalną personalizację usług.

Główną rolę w rozwoju technologicznym branży odegra sztuczna inteligencja (AI), która ułatwia przekształcenie usług ochrony fizycznej na rozwiązania techniczne.

– *Istotnym elementem napędzającym ten postęp jest zwiększona dynamika wzrostu płacy minimalnej w Polsce, a co za tym idzie – średniej płacy w ochronie. Rozwiązania techniczne są natomiast mniej podatne na te zmiany legislacyjne, które powodują wzrost kosztów pracy. Dzięki AI firmy z branży będą mogły automatyzować procesy coraz częściej i coraz bardziej skutecznie* – podkreśla **Paweł Korzybski, prezes Polskiego Związku Pracodawców Ochrona**.

Do czego można wykorzystać AI w ochronie? Sztuczna inteligencja świetnie sprawdzi się choćby w analityce wideo. Potrafi bowiem bardzo skutecznie rozpoznawać określone zdarzenia, dotychczas identyfikowane przez pracowników ochrony. AI potrafi wykryć wtargnięcie na chroniony obszar, ale też bardziej skomplikowane incydenty, np. zablokowanie drogi pożarowej czy gromadzenie się osób w niedozwolonym miejscu. Nowoczesne rozwiązania zawierają już systemy analityczne wbudowane w kamerach, a nie w oprogramowaniu zewnętrznym. Dzięki temu np. na terenie zakładów przemysłowych zwiększa się poziom bezpieczeństwa. W jaki sposób? System potrafi wykryć pożar w początkowym stadium, a tam, gdzie nie wolno używać smartfonów w ciągach komunikacyjnych, alarmuje, gdy pracownik na korytarzu wpatruje się w ekran podczas przechodzenia.

System zaczyna myśleć

W tym roku firmy ochrony będą jeszcze mocniej wykorzystywać tzw. internet rzeczy (IoT). – *Przykładowo kiedyś, aby wykryć wyciek wody w obiekcie, trzeba było montować czujki zalania w miejscach potencjalnego wycieku. Potrzebny był też duży system spinający te czujki, a na przyłączu – zawór odcinający wodę w razie alarmu. Dzięki IoT czujki są montowane na rurach i uczą się rytmu przepływu wody, obliczając trend dzienny czy tygodniowy. I gdy np. wieczorem nagle pojawi się ciągły pobór wody, to czujka zaczyna myśleć, co mogło się stać. Jeśli wydedukuje, że wystąpiła awaria, zamyka zawór wody* – wyjaśnia **Krzysztof Bereza, ekspert Polskiego Związku Pracodawców Ochrona**.

Tego typu usługi automatyzacji będą coraz bardziej skomplikowane. To już nie tylko zdalne otwieranie szlabanu czy autoryzacja wideo osób wchodzących do obiektu. Coraz częściej firmy ochrony mogą na odległość – ze stacji monitorowania – nadzorować nocne dostawy towarów do sklepów czy przyjmować i wydawać pojazdy w warsztatach samochodowych. Z kolei na budowach zdalnie kontrolują, czy wchodzące osoby mają założony kask i okulary ochronne.

Sztuczna inteligencja coraz mocniej wzmocni też „zaplecze" działań związanych z bezpieczeństwem. Firmy ochrony wykorzystują algorytmy, które badają np. liczbę fałszywych alarmów lub same – jako chatboty – komunikują się z klientem. Dzięki temu fizyczni operatorzy angażują się tylko w te akcje alarmowe, których nie da rady obsłużyć silnik sztucznej inteligencji.

Sektor ochrony będzie też intensywnie wykorzystywał programy do automatyzacji procesów. Dotąd firmy z branży likwidowały sporo posterunków ochrony fizycznej, przede wszystkim te patrolowe, które działały prewencyjnie na potencjalnych przestępców. Zostały natomiast te posterunki, których pracownicy bezpośrednio obsługują procesy, czyli np. sprawdzają na bramach listy awizacyjne czy kierują pojazdy do doków. Teraz jednak obserwujemy duży rozwój programów wspierających te działania – po to, by kierowcy mogli samodzielnie zgłaszać swój wjazd. Firmy ochrony często też wdrażają systemy automatycznego ważenia dużych pojazdów

wpuszczanych na teren dużych zakładach przemysłowych. I jeżeli różnica zadeklarowanej masy pojazdu i towaru, który ma zostawić w zakładzie, jest znacząco wyższa, system wstrzymuje taki samochód do kontroli.

Takie nowoczesne technologie powodują, że ochrona fizyczna służy obecnie głównie do tego, by interpretować dane, które przychodzą z systemu, i ewentualnie na nie reagować.

Prestiż zawodu wbrew stereotypom

W związku z postępem technologicznym skala zatrudnienia w sektorze ochrony będzie się zauważalnie kurczyć w kolejnych latach. Tam, gdzie wcześniej było trzech pracowników ochrony i mały system wizyjny, teraz będzie duży system z analityką, obsługiwany przez jedną osobę. Ale przede wszystkim zmieni się profil pracowników, jeśli hybrydowy system ochrony ma zostać skutecznie wdrożony.

Pracownik ochrony jest coraz częściej operatorem systemów. Musi umieć zebrać i przetworzyć generowane przez nie informacje, a następnie przygotować na ten temat raport.

– *Będziemy więc potrzebować osób, które nie boją się technologii i znają języki obce. Idziemy więc w kierunku połączenia kompetencji technicznych i interpersonalnych* – zauważa Paweł Korzybski.

Dotąd zawód pracownika ochrony był postrzegany jako mało atrakcyjny – średnio płatny i nie dający możliwości rozwoju. Teraz to się zmieni właśnie dzięki modyfikacji profilu pracowników. Bo coraz częściej w ochronie będzie poszukiwany operator systemów wizyjnych czy systemów bezpieczeństwa. Poza tym pracownicy ochrony realizują nie tylko zadania związane z kontrolą ruchu osobowego czy kołowego, ale też weryfikują alarmy instalacji systemu pożarowego czy funkcjonowanie pieców w kotłowni. Przyszłością tej branży są więc wykształceni specjaliści z jasno określoną ścieżką rozwoju i potwierdzonymi umiejętnościami.

Kto nie inwestuje, ten został w tyle

Aby wdrażać zmiany technologiczne, agencje ochrony muszą wydawać więcej środków na ten cel.

– *Nie da się przejść z ochrony fizycznej w stronę technicznej z dnia na dzień ani nawet z roku na rok. To proces, który rozpoczął się kilkanaście lat temu, z powodu pierwszej znaczącej podwyżki płacy minimalnej. Już wtedy rozsądne firmy ochrony zrozumiały, że muszą zmienić strategię, optymalizować koszty pracy i budować swój kapitał na technologii. Dzięki temu dziś są w zupełnie innym miejscu. A firmy, które nie wyczuły takiej konieczności, mają teraz przeogromny problem* – podkreśla Krzysztof Bereza.

Rynek zaczyna się konsolidować i firmy ochrony, które nie inwestowały w technologię, teraz są wchłaniane przez inne przedsiębiorstwa z branży, które mają takie zaplecze i potrafią z niego korzystać.

Klient już nie chce pudełek

Coraz więcej firm ochrony tworzy zespoły inżynierów, którzy mają wysokie kompetencje techniczne i technologiczne, a ich zadaniem jest szukanie rozwiązań, jak usprawnić procesy klientów, np. produkcyjne. Przedsiębiorstwa z branży będą też intensywnie rozwijać oprogramowanie dziedzinowe do zarządzania procesami, by mieć ofertę idealnie wpisującą się w potrzeby klienta.

– *Te oprogramowania są w 90 procentach szyte na miarę. Klient już nie chce „pudełek", bo nie chce zmieniać swojego sposobu działania. Oczekuje natomiast, by to firma projektująca nowy system ochrony dopasowała go do specyfiki zleceniodawcy. Powstają więc programy takie jak e-recepcja, która potrafi zweryfikować, czy nowo zatrudniony pracownik przeszedł szkolenie BHP, i na tej podstawie generować przepustki* – mówi Krzysztof Bereza.

Duże podmioty gospodarcze, szczególnie z zagranicznym kapitałem, zmieniają też sposób kupowania usług. Nie chcą już zamawiać osobno ochrony, sprzątania czy utrzymania nieruchomości. Takie przedsiębiorstwa oczekują kompleksowego zarządzania obiektami (ang. facility management). Kontrakty zdobędą więc firmy, które mają w swoim portfolio te wszystkie usługi. Ten kierunek będzie zyskiwać na znaczeniu, bo w przetargach, zarówno publicznych, jak i komercyjnych, usługi ochrony fizycznej są coraz częściej na stałe połączone z usługą ochrony technicznej, czyli czuwaniem nad infrastrukturą budynku oraz zarządzaniem w przypadku awarii. Na rynku wygrają więc firmy, które będą mieć możliwość synergii tych wszystkich usług.

www.pzpochrona.pl

SELFIE Z EKSPONATEM

Jakub Sobek

Muzea, to miejsca, gdzie historia z teraźniejszością siada przy kawie, a obie razem snują opowieści o jutrze. Lecz w tej kawiarnianej scenie jest haczyk – trzeba uważać, by nikt nie dosypał trucizny do filiżanki. Z jednej strony mamy systemy, czujne niczym rodzic na placu zabaw, lecz wystarczy moment nieuwagi i już – dziecko ląduje na piasku. Technologia, jak rycerska tarcza, ma ochraniać skarby, ale co, gdy zaczyna ona przesłaniać widok? Tu zaczyna się ta gra, gdzie bezpieczeństwo z dostępnością siadają po przeciwnych stronach szachownicy. Mały ruch, jedno potknięcie i partia może zmienić swój rezultat.

Dylemat pomiędzy bezpieczeństwem a dostępnością muzeów jest tematem, który od dawna rodzi kontrowersje w środowiskach zarządzających muzeami, ekspertów ds. bezpieczeństwa, a także wśród samych odwiedzających. Z jednej strony, wzrost zagrożeń takich jak kradzież, wandalizm, a nawet terroryzm wymusza na muzeach wprowadzenie rygorystycznych środków bezpieczeństwa. Z drugiej strony, zbyt restrykcyjne procedury mogą odstraszyć odwiedzających, tworząc barierę pomiędzy eksponatami a ich odbiorcami. Zatem, jak można pogodzić te dwa pozornie sprzeczne cele: maksymalizację bezpieczeństwa przy jednoczesnym zachowaniu otwartości i dostępności muzeów? Konieczne jest zrozumienie, że bezpieczeństwo i dostępność nie są wzajemnie wykluczającymi się koncepcjami. Wręcz przeciwnie, mogą one współistnieć, jeśli zostaną odpowiednio zintegrowane i zbalansowane przez świadome, przemyślane strategie zarządzania i projektowania. Nowoczesne rozwiązania techniczne sprawiają, że system może być skuteczny oraz zarazem dyskretny. Zatem trzeba pamiętać o balansowaniu pomiędzy aspektami bezpieczeństwa, a psychologicznymi odczuciami i oczekiwaniami odwiedzających. Należy zatem poszukiwać różnorodnych strategii, praktyki i rozwiązań, które mogą pomóc w znalezieniu złotego środka.

Wyzwania

Podczas zwiedzania muzeów, można czasem odnieść wrażenie, że najtrudniejszym zadaniem pracowników jest powstrzymanie zwiedzających przed robieniem selfie z eksponatami. Zmieniający się świat wpływa także na ewolucję sposobu, w jaki doświadczamy kultury. W rezultacie, w muzeach, do których udajemy się, by podziwiać dzieła, tradycyjne eksponaty stopniowo ustępują miejsca treściom multimedialnym. Coraz częściej to właśnie one zajmują centralne miejsce, przyciągając uwagę i zainteresowanie publiczności. Jednak wyzwania, przed jakimi stoją muzea, są znacznie bardziej złożone i wielowymiarowe. Zagrożenia, takie jak kradzież i wandalizm, nadal stanowią poważne ryzyko. Cenne artefakty przyciągają nie tylko pasjonatów sztuki, ale również tych, którzy widzą w nich potencjalny łup. W związku z tym, muzea muszą inwestować w zaawansowane systemy zabezpieczeń. Nie zawsze jednak środki finansowe, jakie są do dyspozycji pozwalają na wdrażanie najlepszych rozwiązań.

Instytucje muzealne stoją obecnie przed imperatywem adaptacyjnym, wymuszającym inkorporację nowatorskich metod prezentacji swoich kolekcji. Taki proces transformacyjny nakłada na te instytucje obowiązek inwestycji znaczących środków finansowych w zaawansowaną technologię, taką jak specjalistyczne ekrany, projektory oraz inne urządzenia elektroniczne, które są nieodzowne do kreowania interaktywnych ekspozycji. Paradoksalnie, niekiedy to właśnie ten wysokospecjalistyczny sprzęt elektroniczny, wykorzystywany przez muzea, reprezentuje wartość finansową przewyższającą wartość eksponatów zgromadzonych w danej sali wystawienniczej. W związku z tym, konieczność właściwej ochrony rozciąga się nie tylko na same zbiory muzealne, ale także na infrastrukturę technologiczną.

Debaty dotyczące restytucji artefaktów do ich pierwotnych krajów pochodzenia oraz zmagania z problematyką praw autorskich stanowią jedynie fragment szerokiego spektrum komplikacji, z którymi konfrontują się współczesne instytucje muzealne. Roszczenia restytucyjne wobec zbiorów muzealnych generują złożoną dynamikę społeczno-polityczną, która w przypadku eskalacji może manifestować się poprzez demonstracje protestacyjne, nierzadko eskalujące do aktów wandalizmu skierowanych bezpośrednio przeciwko dziełom sztuki. Ponadto, należy uwzględnić napięcia na płaszczyźnie międzynarodowej, gdzie fluktuacje w sferze geopolitycznej mogą instygować antagonizm wobec instytucji muzealnych, które prezentują materiały o kontrowersyjnym lub dyskusyjnym charakterze. Szczególnie dotkliwie problem ten dotyka muzea zajmujące się tematyką żydowską, które są często celami dla ekstremistycznych ugrupowań o antysemickim charakterze. Takie ugrupowania, przekraczając granice retoryki, nie tylko formułują groźby wobec personelu muzeów, lecz również stanowią bezpośrednie zagrożenie dla muzealnych kolekcji oraz bezpieczeństwa odwiedzających i pracowników instytucji. W kontekście tych wyzwań, zarządzanie ryzykiem oraz rozwijanie strategii ochrony dziedzictwa kulturowego staje się nie tylko kwestią administracyjną, lecz także istotnym elementem ochrony tożsamości kulturowej i historycznej.

Jedno znaczące zdarzenie rozegrało się w prestiżowym Muzeum Prado w Madrycie, gdzie aktywiści z grupy Futuro Vegetal przykleili swoje ręce do ram dwóch znanych obrazów Francisco Goi: „La maja vestida" i „La maja desnuda". Aktywiści zaznaczyli również na ścianie muzeum napis „+1.5°C", podkreślając swoje wezwanie do przestrzegania celu Porozumienia Paryskiego, dotyczącego ograniczenia globalnego ocieplenia. Mimo dramatycznej natury protestu, doniesiono, że same dzieła sztuki nie poniosły uszczerbku. Jednakże akt ten był częścią szerszego wzorca incydentów przypisywanych aktywistom klimatycznym na terenie Hiszpanii, które łącznie spowodowały szkody przekraczające 500 000 euro.

Podobnie, londyńska Galeria Courtauld stała się świadkiem protestu grupy Just Stop Oil, gdzie dwóch aktywistów przykleiło się do obrazu Vincenta van Gogha „Kwitnące drzewa brzoskwiniowe". Ten akt miał na celu nie tylko przyciągnięcie uwagi, ale również zmuszenie rządu i instytucji do działania. Wybór obrazu van Gogha był symboliczny, odzwierciedlając podatność klimatyczną jego lokalizacji, Arles, w Prowansji — regionu, który przewiduje się, doświadczy ciężkich susz i ekstremalnych warunków pogodowych. Ten protest, jak i inne podobne, m.in. w Kelvingrove Art Gallery and Museum w Glasgow, podkreślają rosnący trend wykorzystywania prestiżowych przestrzeni kulturowych i artefaktów do amplifikacji przesłania aktywizmu klimatycznego.

Precyzja, skupienie i planowanie

Znalezienie równowagi między bezpieczeństwem a dostępnością w muzeach to zadanie przypominające żonglerkę na linie – wymaga precyzji, skupienia i strategicznego planowania. Proces ten, oparty na adaptacji, charakteryzuje się ciągłością i wymaga elastyczności, aby efektywnie reagować na dynamiczne zmiany w środowisku

Zdjęcie 1. Przestrzeń muzealna powinna być dostępna i bezpieczna
Autor: Jakub Sobek

Zdjęcie 2. Systemy zabezpieczenia technicznego mogą pozostawać dyskretne nie zaburzając odbioru ekspozycji
Autor: Jakub Sobek

Zdjęcie 3. Niejednokrotnie muzea stają przed wyzwaniem zabezpieczenia wyjątkowo trudnych eksponatów
Autor: Jakub Sobek

kulturowym, technologicznym i społecznym. Bezpieczeństwo, rozumiane jako ochrona przed potencjalnym uszkodzeniem lub utratą, wymaga zaimplementowania zaawansowanych systemów zabezpieczeń oraz procedur konserwacyjnych, które są jednak często percepcyjnie i fizycznie ograniczające dla odwiedzających. Z drugiej strony, dostępność – jako demokratyczna wartość muzeów – nakłada na te instytucje konieczność stworzenia przestrzeni inkluzywnej i edukacyjnej, dostosowanej do różnorodności odbiorców i ich potrzeb. Wymaga to od decydentów muzealnych nie tylko dogłębnej znajomości aktualnych trendów w technologii i zarządzaniu zbiorami, ale także empatycznego i proaktywnego podejścia do potrzeb społecznych, kulturowych i edukacyjnych ich publiczności.

Planowanie strategiczne to kluczowy element już na samym starcie tworzenia muzeów. Już na etapie kreowania pierwszych koncepcji, niezwykle ważne jest, aby mieć na uwadze aspekty związane z ochroną miejsca. Właśnie w tym momencie architekci oraz projektanci powinni ściśle współdziałać z ekspertami od bezpieczeństwa. Cel? Zintegrować systemy ochronne tak, aby były one niemalże niewidoczne, nie naruszając przy tym ani estetyki, ani funkcjonalności przestrzeni przeznaczonej na muzeum. Weźmy na przykład systemy monitoringu – mogą one być wkomponowane tak dyskretnie, aby harmonijnie współgrały z całokształtem aranżacji muzealnej. Nawet oświetlenie, zaprojektowane przede wszystkim z myślą o podkreślaniu eksponatów, może również pełnić funkcję wspomagającą – pozwalać dostarczać wysokiej jakości obraz z kamer. Co więcej, oświetlenie zewnętrzne może zostać zaplanowane w taki sposób, aby nie tylko pięknie eksponować architekturę budowli, ale i odstraszać potencjalnych intruzów. Okazuje się więc, że istnieje możliwość zgrabnego połączenia w jedną całość – i to w sposób bardzo subtelny – zarówno aspektów bezpieczeństwa, jak i wystawienniczych.

Stosowanie systemów zabezpieczenia technicznego w muzeach nie tylko pełni kluczową rolę w ochronie cennych eksponatów, ale jest także ściśle uregulowane prawem. To zobowiązanie wynika z przepisów zawartych w Rozporządzeniu Ministra Kultury i Dziedzictwa Narodowego z dnia 2 września 2014 roku, które szczegółowo reguluje kwestie zabezpieczania zbiorów muzeum przed szeregiem zagrożeń, takich jak pożar, kradzież, czy inne niebezpieczeństwa, które mogą prowadzić do ich zniszczenia lub utraty. Dokument ten nie tylko precyzuje minimalne wymagania, ale również wyszczególnia konkretne systemy zabezpieczeń, które powinny być zainstalowane na terenie muzeów. Warto podkreślić, że choć rozporządzenie nakłada na muzea obowiązek instalacji wskazanych systemów, to jednak określa ono jedynie pewne minimalne standardy

Zdjęcie 4. Przykład organizacji wejścia do muzeum: namiot do kontroli osobistej oraz bloki najazdowe chroniące oczekujących na wejście
Autor: Jakub Sobek

bezpieczeństwa. Dlatego instytucje często decydują się na wdrażanie dodatkowych, bardziej zaawansowanych rozwiązań, mając na uwadze bezcenną wartość przechowywanych zbiorów.

Najważniejsze aby w tym wszystkim pamiętać, żeby zabezpieczenia techniczne były zawsze uzupełniane o odpowiednie procedury bezpieczeństwa oraz szkolenia personelu, co dopiero razem tworzy kompleksową strategię ochrony dziedzictwa kulturowego. Personel muzeum powinien być regularnie szkolony z zakresu procedur bezpieczeństwa, obsługi systemów alarmowych, a także umiejętności komunikacji w sytuacjach kryzysowych. Pracownicy powinni być świadomi potencjalnych zagrożeń i wiedzieć, jak reagować w przypadku incydentu.

Szczególną uwagę należy zwrócić na rozwijanie umiejętności komunikacyjnych, które są kluczowe w zarządzaniu sytuacjami kryzysowymi. Efektywna komunikacja może znacząco ograniczyć skutki nieoczekiwanych zdarzeń, uspokajać publiczność oraz wspierać koordynację działań zespołu. Pracownicy powinni umieć szybko i jasno przekazywać informację w obrębie wewnętrznego zespołu muzeum. Zrozumienie hierarchii komunikacyjnej i posiadanie jasno określonych protokołów może przyczynić się do szybkiego i skutecznego reagowania na kryzys. Kluczowe jest także, aby personel potrafił uspokoić odwiedzających, przekazać im jasne i zrozumiałe instrukcje oraz utrzymać porządek. To wymaga nie tylko znajomości procedur, ale również umiejętności empatycznego i asertywnego komunikowania się. W stresujących sytuacjach, niewerbalne sygnały takie jak mowa ciała i ton głosu mogą mieć równie duże znaczenie, co przekazywane słowa. Systematycznie organizowane ćwiczenia oraz symulacje różnych scenariuszy awaryjnych mogą istotnie wpłynąć na poziom przygotowania pracowników. To właśnie praktyczne treningi, przeprowadzane w warunkach jak najbardziej zbliżonych do realnych, umożliwiają zespołowi dogłębne przyswojenie procedur. Takie ćwiczenia pozwalają także na doskonalenie umiejętności komunikacyjnych oraz szlifowanie zdolności do błyskawicznego, a zarazem skutecznego reagowania, kiedy sytuacja nabierze naprawdę dużej dynamiki.

W obliczu tych licznych wyzwań, muzea – te skarbnice ludzkiej historii i kultury – muszą znaleźć równowagę między konserwatyzmem a innowacyjnością, między ochroną a dostępnością. To właśnie w tym wyjątkowym miejscu, gdzie krzyżują się liczne sprzeczności, rodzi się niepowtarzalna magia, która stanowi istotę każdego muzeum. Ważne jest, aby pamiętać, że każda strategia ochrony, każda wprowadzona procedura musi być nie tylko skuteczna, ale także elastyczna. Świat nieustannie się zmienia, ewoluują zagrożenia, ale zmieniamy się również my sami oraz nasze oczekiwania, sposób postrzegania i interakcja z przestrzenią muzealną. Dlatego muzea muszą być gotowe na nieustanne przekształcanie się, adaptowanie i poszukiwanie nowych rozwiązań. Rozwiązania te muszą nie tylko zabezpieczać cenne eksponaty, ale również otwierać je na świat, na ludzi, na nas wszystkich. Zatem droga, którą muszą przebyć muzea, jest wyboista i pełna niespodzianek. To ścieżka wymagająca odwagi, wytrwałości i ciągłego poszukiwania. Ale to również ścieżka, która może prowadzić do niezwykłych odkryć, do nowych horyzontów myślenia i do głębszego zrozumienia siebie oraz świata, który nas otacza. ■

Źródła:
1. https://www.dw.com/en/spain-climate-activists-glue-hands-to-goya-paintings/a-63660380
2. https://www.spainenglish.com/2024/01/14/spanish-police-arrest-climate-activists-who-glued-themselves-goya-paintings/
3. https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20140001240

Jakub Sobek

DEPOZYTORY KLUCZY I INNYCH PRZEDMIOTÓW

Robert Gabrysiak

Do szeroko rozumianego pojęcia bezpieczeństwa oprócz różnego rodzaju systemów alarmowych czy monitoringu należą także depozytory kluczy. Są to urządzenia czysto mechaniczne bądź, jak przystało na dzisiejsze czasy, elektromechaniczne, które mają za zadanie zarządzać kluczami w obiekcie. W budynkach, organizacjach, instytucjach państwowych, urzędach centralnych, firmach prywatnych potrzebny jest sprawny, bezpieczny, zautomatyzowany i łatwy sposób przechowywania, wydawania wszelkiego rodzaju kluczy. Korzystając z depozytorów kluczy można całkowicie wyeliminować błędy spowodowane tzw. czynnikiem ludzkim i sprawnie zarządzać kluczami oraz ich obiegiem. Pozwala to uniknąć przypadków dostępu do kluczy przez osoby nieuprawnione.

Depozytory mogą być zainstalowane w różnych lokalizacjach, o różnej konfiguracji i zarządzane w ramach jednej aplikacji dzięki której mamy możliwość nadawania uprawnień, raportowania kto, gdzie i kiedy pobrał oraz zwrócił klucze. Depozytory kluczy są zaawansowanymi urządzeniami o stosunkowo prostej idei konstrukcyjnej. W większości przypadków składają się z wielu współpracujących ze sobą elementów o różnej funkcjonalności. Poniżej przedstawiono podstawowe funkcje i możliwości depozytora kluczy:

- Umożliwia bezpieczne pobieranie, przechowywanie i rozliczanie kluczy.
- Rejestruje wszystkie operacje jak np. dokładną datę, godzinę i operacje wykonywane w urządzeniu.
- Umożliwia przeglądanie zdarzeń na konsoli depozytora lub online poprzez sieć z depozytorem.
- Spełnia funkcje wyszukiwania obecnego posiadacza kluczy.
- Umożliwia drukowanie raportów bądź ich export do plików csv lub xls.
- W razie awarii układu elektrycznego bądź zaniku zasilania depozytor posiada system podtrzymujący zasilanie (minimum 24h i większe).
- Depozytor posiada możliwość mechanicznego zwolnienia blokad kluczy i awaryjnego otwarcia urządzenia.
- Potrafi identyfikować miejsca, w których dokonano błędnego wsadzenia kluczy.
- Generuje alarm zbyt długo otwartych drzwi.
- Posiada alarm sabotażowy.
- Generuje alarm zbyt długo przetrzymanych kluczy.
- Posiada możliwość rozbudowy o dodatkowe depozytory rozszerzające.
- Umożliwia późniejszą rozbudowę o dodatkowe miejsca na klucze.
- Umożliwia zainstalowanie elementów dodatkowych: kamera, alkomat, inne.

Obecnie spora część produktów tego typu, możliwych do nabycia na rynku, jest wyposażana w coraz bardziej zaawansowane układy elektroniczne podnoszące własności użytkowe. Przykładowo depozytory wyposaża się w czytniki biometryczne, czytniki RFID czy też oznaczenia zajętości skrytek (np. za pomocą diod LED).

Depozytor kluczy ma realnie wpływać na poziom bezpieczeństwa w obiekcie, dlatego też musi być odpowiednio dobrany do jego potrzeb, prawidłowo zainstalowany oraz skonfigurowany. Wszystkie te czynności powinny być poprzedzone odpowiednim rozpoznaniem obiektu, panującym w nim obiegu kluczy, liczbie osób mających do nich dostęp itp. Dlatego warto tę część pracy pozostawić fachowcom z firm oferujących depozytory kluczy. Należy jednak zawsze pamiętać o tym, że nawet najbardziej zaawansowane technicznie urządzenia mogą nie dać zamierzonego efektu, jeśli będzie zawodzić czynnik ludzki, a więc brak konsekwentnego stosowania wypracowanych dla obiektu procedur związanych z pobieraniem i deponowaniem kluczy w elektromechanicznym depozytorze kluczy.

Miejsce montażu depozytora kluczy powinno umożliwiać łatwe doprowadzenie okablowania, np. w pobliżu tras kablowych lub punktów dystrybucyjnych. Ponadto powinno ono również zapewniać pracownikom swobodny dostęp do depozytora oraz spełniać wymagania przepisów ppoż. a także zapewniać swobodne przejście za plecami osób korzystających z depozytora.

Od nowoczesnych deopozytorów kluczy wymaga się tez pełnej integracji z systemami bezpieczeństwa czy zabezpieczeń technicznych takich jak: kontrola dostępu, systemy CCTV, systemy alarmowe SSWiN czy tez systemy ppoż. Dla systemów kontroli dostępu sygnał z dyspozytora kluczy może być jednocześnie sygnałem rozpoczęcia pracy przez osobę identyfikującą się danym pinem, czy biometrią a zarejestrowana godzina zwrotu kluczy może być wyznacznikiem czasu pracy tej osoby.

System depozytorów powinien posiadać własne, dedykowane oprogramowanie do zarządzania całością systemu. Należy zwrócić uwagę, aby licencja na oprogramowanie nie była ograniczona czasowo albo ilościowo np. przez ograniczenie ilości stanowisk administracyjnych, ilości użytkowników lub ilości urządzeń w systemie.

W depozytorach najczęściej przechowywane są klucze, jednak coraz bardziej popularne są urządzenia do przechowywania przedmiotów takich jak: telefony komórkowe, laptopy, korespondencja (listy, paczki), dyski twarde, dokumenty pojazdów (w tym książki pojazdów), jak również specjalistyczne urządzenia do przechowywania broni krótkiej i długiej.

Największe wymagania stawiane są tam gdzie przechowywana jest broń. Broń jest jedną z nielicznych grup przedmiotów, których

przechowywanie jest uregulowane prawnie (ustawa z dnia 21 maja 1999r oraz Rozporządzenie Ministra Spraw Wewnętrznych z dnia 26 sierpnia 2014r w sprawie przechowywania, noszenia oraz ewidencjonowania broni i amunicji). Niezależnie od tego, jaki rodzaj depozytorów broni jest potrzebny, powinniśmy mieć informacje o stanie zajętości skrytki z bronią. W tym celu skrytki wyposaża się w rozmaite urządzenia do automatycznej identyfikacji statusu skrytek, które mogą być użytkowane razem lub osobno w zależności od potrzeb. Przykładowo w depozytorach mogą być zamontowane czujnik optyczne pozwalające identyfikować kto i kiedy zapełnił skrytkę, czy skrytka jest pełna czy pusta i co jest w środku. Innym rodzajem czujki montowanym w depozytorach broni może być czujka wagi. Szczególnie przydatne jest to w depozytorach w których przechowywana jest ciągle ta sama broń a identyfikacja jej wagi pozwala stwierdzić czy w skrytce znajduje się właściwa broń. Kolejnym przykładem czujek mogą być czujniki zbliżeniowe oraz kodów QR, które pozwalają na najdokładniejszy sposób rozpoznawania broni, jednak wiąże się to z koniecznością oznaczenia broni identyfikatorem odczytywanym elektronicznie (np. zatopienie w rękojeści broni kodu RFID).

Kolejnym rodzajem depozytorów są urządzenia służące do inteligentnego przechowywania przedmiotów osobistych takich jak telefony komórkowe, laptopy czy tablety. Charakteryzują się tym, że posiadają wymiary pozwalające przyjąć wszelkie przedmioty, których osoba nie chce lub nie może wnieść na określony teren lub do strefy bezpieczeństwa. Zasadnicza różnica w stosunku do depozytorów kluczy polega na tym, że depozytory kluczy wykorzystywane są z reguły przez pracowników danej organizacji, natomiast depozytory na telefony mogą być wykorzystywane przez różne osoby, które często mają z nimi kontakt po raz pierwszy. Przykładem mogą tu być osoby np. odwiedzające skazanych w zakładach karnych lub wchodzące na teren obiektu wojskowego czy produkcyjnego jako gość. W celu obsługi osób z zewnątrz konieczne jest umożliwienie pozostawienia przedmiotu przez każdą osobę, która będzie chciała to uczynić.

Depozytor na telefony komórkowe powinien umożliwić ustawienie indywidualnego kodu PIN, który służyć będzie do ponownego otwarcia skrytki. Podstawowe wyposażenie depozytora powinno zawierać czujki zajętości skrytki oraz czujniki optyczne pozwalające rozpoznać jej zawartość. W bardzo szczególnych sytuacjach, gdzie bezpieczeństwo i przede wszystkim poufność są na pierwszym miejscu, warto wprowadzić np. maskowanie dźwięków tła, które mogłyby być nagrane przez zdeponowany telefon lub inne urządzenie posiadające funkcję dyktafonu. Zadanie to można osiągnąć poprzez automatyczne uruchomienie głośnika emitującego tzw. biały szum, czyli jednostajny dźwięk. Umiejscowienie głośnika w bezpośrednim sąsiedztwie telefonu dodatkowo zamkniętego w niewielkiej przestrzeni skrytki, która ponadto odbija emitowany szum, sprawia, że każda próba nagrania prowadzonej rozmowy w bezpośrednim sąsiedztwie depozytora skończy się niepowodzeniem. Takie rozwiązania często wybierane jest przez duże firmy prywatne i instytucje państwowe, które chcą ograniczyć niebezpieczeństwo wypływania w ten sposób informacji przekazywanych na poufnych spotkaniach. Drugim zagadnieniem jest blokada sygnału GSM zdeponowanych telefonów. Może to być istotne, jeśli nie chcemy, by niewyciszony telefon przeszkadzał przez sygnał dzwonka przychodzących wiadomości.

Fajną funkcją jest wyposażenie deopozytorów telefonów komórkowych w odpowiednie urządzenia pozwalające na ich ładowanie. W tym celu często w skrytkach montuje się kable USB-C, micro-USB czy Lightning (dla telefonów Apple). Innym rozwiązaniem jest też zamontowanie gniazd 230V, do których użytkownicy skrytki będą mogli podpiąć ładowarki swoich telefonów a nawet laptopów czy tabletów.

Ponieważ telefony komórkowe jak i inne urządzenia wyposażone w akumulatory zagrożone są tzw. samoistnym zapłonem, to depozytory do ich przechowywania powinny posiadać odporność pożarową. Odpowiednią opinię dotyczącą tego aspektu wystawia zawsze niezależny instytut do spraw ochrony p.poż., którym w Polsce jest CNBOP.

Każdy – NIEZALEŻNIE od przeznaczenia – depozytor musi mieć możliwość awaryjnego otwarcia za pomocą mechanicznego rozwiązania, jakim są klucze serwisowe. Takie rozwiązanie jest zawsze dostępne i odporne na uszkodzenia elektroniczne. Dobre depozytory posiadają wbudowane wkładki zamków mechanicznych w 6. klasie odporności i otwierane są kluczami patentowymi. No i w tym momencie pojawią się pytanie: gdzie takie klucze patentowe przechowywać? Na pewno nie wolno tego robić w samym depozytorze, gdyż całkowicie będą one niedostępne w przypadku awarii. Nie wolno ich także przechowywać w pomieszczeniach do których dostęp stanie się niemożliwy w wyniku awarii. Pozostaje zatem trzymanie ich przez zaufaną osobę lub przez pracownika ochrony, jeśli takowy obsługuje obiekt. Jednakże najlepszym rozwiązaniem wydaje się wyposażenie wybranego depozytora w specjalną skrytkę z mechanicznym zamkiem szyfrowym – analogicznie jak w sejfach. Zamek taki powinien być wykonany w klasie A lub wyższej wg normy PN-EN 1300. Każda osoba znająca odpowiednią kombinację może otworzyć skrytkę, w której zdeponowano klucze serwisowe.

Rynek depozytorów kluczy jak innych przedmiotów jest bardzo bogaty i różnorodny. Pamiętajmy jednak, że tylko prawidłowo dobrany (wg specyfiki i wymagń obiektu) i skonfigurowany będzie poprawnie służył w miejscu zainstalowania. Dlatego zawsze poleca się zlecić wykonanie audytu budynku i określenia potrzeb wykwalifikowanej osobie, która po odpowiednim rozpoznaniu funkcjonowania budynku i jego pracowników optymalnie dobierze właściwe depozytory, wyposaży je w odpowiednie funkcje i podłączy do istniejących systemów alarmowych czy kontroli dostępu. ■

Robert Gabrysiak

NOWE ZASADY OCHRONY BUDYNKÓW SĄDÓW

Budynki sądów powszechnych są tymi obiektami użyteczności publicznej, w których wymagania i standardy bezpieczeństwa powinny być jednymi z najwyższych. Jesienią ubiegłego roku weszły w życie nowe przepisy dotyczące bezpieczeństwa w sądach i – chociaż nie są one pozbawione wad – przez wielu były długo oczekiwane i zostały przyjęte z zadowoleniem.

Sergiusz Parszowski

„Dawno, dawno temu…”

Właśnie w taki oto sposób można rozpocząć omawianie nowych przepisów. Wszystko bowiem zaczęło się już w 2014 roku, kiedy to Irena Lipowicz, pełniąca wówczas funkcję Rzecznika Praw Obywatelskich, wskazywała na konieczność uregulowania na poziomie ustawowym podstawy prawnej przeglądania zawartości bagażu i odzieży osób wchodzących do budynku sądu.

Za niedopuszczalne uznawała, aby kwestie te były regulowane np. w regulaminach sądów. Zwracała uwagę, że nawet pobieżne przeglądanie bagażu czy odzieży wiąże się z koniecznością ograniczenia konstytucyjnych praw i wolności (m.in. gwarantowanego prawa do prywatności). Wszelkie tego typu ograniczenia mogą być wprowadzane jedynie wówczas, kiedy zachodzą ku temu konstytucyjne przesłanki. Jednocześnie musi być to dokonywane na podstawie ustawy[1].

W latach 2014, 2015 i 2018 kolejni Rzecznicy Praw Obywatelskich występowali do Ministrów Sprawiedliwości w sprawie potrzeby ustawowego określenia uprawnień pracowników ochrony w budynkach sądowych. Nowelizacja ustawy z 7 lipca 2023 roku Prawo o ustroju sądów powszechnych uczyniła wreszcie zadość temu oczekiwaniu[2].

Kontrola osób wchodzących do budynku

Obowiązujące przepisy prawa zabraniają wnosić do budynków sądów: broni, amunicji, materiałów

[1] Biuletyn Informacji Publicznej RPO, https://bip.brpo.gov.pl/pl/content/od-4-lat-rzecznik-upomina-sie-o-ustawowe-uregulowanie-kontroli-bagazy-osob-wchodzacych-do-sadow [31.01.2024].

[2] Ustawa z dnia 7 lipca 2023 r. o zmianie ustawy – Kodeks postępowania cywilnego, ustawy – Prawo o ustroju sądów powszechnych, ustawy – Kodeks postępowania karnego oraz niektórych innych ustaw (Dz.U. 2023 poz. 1860).

wybuchowych ani innych środków niebezpiecznych. Ograniczenie wnoszenia wymienionych przedmiotów dotyczy wszystkich z wyjątkiem osób wykonujących w budynkach sądów obowiązki służbowe wymagające posiadania broni (np. funkcjonariuszy służb).

Budzącym wiele kontrowersji jest nieprecyzyjne sformułowanie „inne środki niebezpieczne", które zarówno prezesom i dyrektorom sądów, jak również pracownikom ochrony pozostawiają bardzo dużą swobodę w określaniu przedmiotów, których wniesienie do sądu jest niedozwolone. Nawet pobieżna analiza regulaminów bezpieczeństwa i porządku sądów powszechnych prowadzi do wniosku, że zakres niedozwolonych przedmiotów czasem bardzo różni się w poszczególnych obiektach.

Kontrolę osób wchodzących do budynków na podstawie charakteryzowanych przepisów przeprowadzają kwalifikowani pracownicy ochrony, przy czym warto uzupełnić, że na podstawie odrębnych przepisów ochrona bezpieczeństwa i porządku publicznego w budynkach sądów należy także do zadań policji sądowej[3]. Informację o przysługujących osobom wchodzącym do budynku sądu prawach i obowiązkach związanych z czynnościami pracowników ochrony podejmowanymi przy wykonywaniu zadań ochrony osób i mienia w budynkach sądu umieszcza się w widocznym miejscu przy wejściu do budynku sądu.

Uprawnienia pracowników ochrony

W celu zapewnienia bezpieczeństwa w budynkach sądów oraz zapobiegania wnoszenia zabronionych środków stosuje się przepisy o ochronie osób i mienia z zastrzeżeniem, że uprawnienia kwalifikowanych pracowników ochrony wykonujących swoje zadania w budynkach sądów zostały rozszerzone dodatkowo o prawo do:

- przeglądania zawartości bagażu lub odzieży osób wchodzących do budynku sądu;
- odmowy zezwolenia na wejście do budynku sądu osobie odmawiającej poddania się przeglądaniu zawartości bagażu lub odzieży;
- odmowy zezwolenia na wejście do budynku sądu osobie posiadającej przy sobie: broń, amunicję, materiały wybuchowe lub inne środki niebezpieczne;
- żądania usunięcia innych przedmiotów i urządzeń, które mogą stanowić zagrożenie dla życia lub zdrowia ludzkiego, lub mienia albo oddania ich do depozytu.

Pracownik ochrony, który odmówił zezwolenia na wejście do budynku sądu osobie wezwanej na rozprawę lub posiedzenie sądu, ma obowiązek poinformować o tym sekretariat właściwego wydziału sądu.

Kontrola bagażu

Pracownik ochrony ma prawo żądania udostępnienia bagażu, w tym otwarcia i pokazania jego zawartości. Przeglądanie zawartości bagażu polega na:

- wzrokowej i manualnej kontroli zawartości bagażu, w tym manualnym sprawdzeniu znajdujących się w nim przedmiotów;
- sprawdzeniu bagażu z wykorzystaniem środków technicznych niezbędnych do wykrywania materiałów i urządzeń zabronionych, w szczególności broni, materiałów wybuchowych oraz substancji mogących stanowić zagrożenie dla życia lub zdrowia.

Czynności kontrolne muszą być wykonywane w obecności posiadacza bagażu oraz w miarę możliwości nie powinny powodować uszkodzenia bagażu i znajdujących się w nim przedmiotów.

Kontrola osób

Pracownik ochrony ma prawo do żądania zdjęcia przez osobę wchodzącą do budynku sądu

[3] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 16 sierpnia 2007 r. w sprawie szczegółowego zakresu zadań i zasad organizacji policji sądowej (Dz.U. 2007 nr 155 poz. 1093).

zewnętrznych warstw odzieży, pokazania zawartości kieszeni, innych części odzieży lub przedmiotów znajdujących się na ciele tej osoby, lub przez nią posiadanych. Przeglądanie odzieży polega na:

- manualnym sprawdzeniu zawartości odzieży oraz przedmiotów znajdujących się na ciele osoby wchodzącej do budynku sądu lub przez nią posiadanych bez odsłaniania przykrytej odzieżą powierzchni ciała;
- sprawdzeniu za pomocą środków technicznych niezbędnych do wykrywania materiałów i urządzeń zabronionych, w szczególności broni, materiałów wybuchowych oraz substancji mogących stanowić zagrożenie dla życia lub zdrowia.

Kontrolę osób wykonuje się w sposób możliwie najmniej naruszający dobra osobiste osoby, wobec której są wykonywane oraz w niezbędnym zakresie do zrealizowania celu wykonywanej czynności. Czynności wykonuje w miarę możliwości pracownik ochrony tej samej płci, co osoba poddana przeglądaniu odzieży.

Protokół z kontroli

Wszystkim osobom, które zostały poddane przeglądaniu zawartości bagażu lub odzieży, przysługuje prawo żądania sporządzenia przez pracownika ochrony protokołu z wykonania tych czynności. Wzór protokołu określa stosowne rozporządzenie[4] i zawiera on:

- oznaczenie czynności, podstawy prawnej i przyczyny jej podjęcia, miejsca jej dokonania oraz dane osoby poddanej przeglądaniu zawartości bagażu lub odzieży obejmujące imię, nazwisko oraz numer ewidencyjny PESEL lub datę urodzenia oraz serię i numer dowodu osobistego lub innego dokumentu stwierdzającego tożsamość osoby;
- datę i godzinę rozpoczęcia i zakończenia czynności;
- dane pracownika ochrony dokonującego czynności obejmujące imię, nazwisko oraz nazwę przedsiębiorcy, na rzecz którego wykonuje zadania ochrony albo nazwę jednostki organizacyjnej lub przedsiębiorcy w przypadku, gdy pracownik ochrony wykonuje zadania ochrony w ramach wewnętrznej służby ochrony;

[4] Rozporządzenie Ministra Sprawiedliwości z dnia 27 września 2023 r. w sprawie dokumentowania czynności przeglądania zawartości bagażu lub odzieży osób wchodzących do budynków sądów (Dz.U. 2023 poz. 2030).

- przebieg czynności, oświadczenia i wnioski jej uczestników;
- spis znalezionych i odebranych przedmiotów oraz w miarę potrzeby ich opis;
- pouczenie osoby poddanej przeglądaniu zawartości bagażu lub odzieży o jej prawach, w szczególności o prawie do złożenia skargi;
- podpis osoby dokonującej czynności oraz osoby poddanej przeglądaniu zawartości bagażu lub odzieży albo wzmiankę o odmowie złożenia podpisu.

W przypadku zaś, gdy w trakcie kontroli znaleziono przedmioty mogące stworzyć niebezpieczeństwo dla życia, zdrowia ludzkiego lub mienia, a osoba poddana tym czynnościom nie zgłosiła żądania sporządzenia protokołu z dokonanej czynności, pracownik ochrony niezwłocznie dokumentuje dokonanie czynności w notatce służbowej, odnotowując rodzaj, czas, miejsce i wynik czynności, dane pracownika ochrony oraz sporządzając spis znalezionych i odebranych przedmiotów, a także – w miarę potrzeby – ich opis.

Wyłączenia z kontroli

Jakkolwiek zakaz wnoszenia wymienionych wcześniej przedmiotów dotyczy wszystkich z wyjątkiem osób wykonujących w budynkach sądów obowiązki służbowe wymagające posiadania broni, to jednak nie wszystkie osoby wchodzące do budynku sądu poddawane są kontroli. Nie przeprowadza się kontroli w stosunku do:

- Prezydenta Rzeczypospolitej Polskiej;
- Prezesa Rady Ministrów;
- członków Rady Ministrów;
- Rzecznika Praw Obywatelskich;
- Rzecznika Praw Dziecka;
- Rzecznika Finansowego;
- Prezesa Urzędu Ochrony Danych Osobowych;
- osób korzystających z immunitetu parlamentarnego, sędziowskiego lub prokuratorskiego, ławników danego sądu oraz referendarzy sądowych;
- osób korzystających z immunitetów dyplomatycznych lub konsularnych na mocy ustaw, umów międzynarodowych albo powszechnie uznanych zwyczajów międzynarodowych;
- adwokatów, radców prawnych, notariuszy, komorników sądowych, prezesa, wiceprezesów, radców i referendarzy Prokuratorii Generalnej Rzeczypospolitej Polskiej;
- kuratorów sądowych, rzeczników patentowych, biegłych sądowych, doradców restrukturyzacyjnych – w trakcie pełnienia czynności służbowych;
- funkcjonariuszy Policji, Straży Granicznej, Służby Ochrony Państwa, w tym inspektorów Biura Nadzoru Wewnętrznego oraz funkcjonariuszy Służby Więziennej, Centralnego Biura Antykorupcyjnego, Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służby Wywiadu Wojskowego, Służby Kontrwywiadu Wojskowego, Służby Celno-Skarbowej, Straży Ochrony Kolei, żołnierzy Żandarmerii Wojskowej i pracowników Krajowej Administracji Skarbowej – w trakcie pełnienia czynności służbowych;
- innych osób, w stosunku do których dyrektor sądu albo prezes sądu wyrazili zgodę na ich wejście

– po uprzednim okazaniu legitymacji służbowej lub dokumentu umożliwiającego ustalenie tożsamości i zajmowanego stanowiska lub pełnionej funkcji.

Stosowanie środków bezpieczeństwa

Prezes sądu w regulaminie bezpieczeństwa i porządku sądu decyduje o rodzajach stosowanych środków bezpieczeństwa mających na celu zapewnienie bezpieczeństwa w budynkach sądów oraz zapobieganie wnoszeniu zabronionych przedmiotów. W zakresie urządzeń technicznych najczęściej użytkowanych w sądach znajdują się: urządzenia służące do identyfikacji dokumentów, bramowe i ręczne wykrywacze metalu i ceramiki, ręczne detektory, urządzenie do prześwietlania bagaży oraz skanery rentgenowskie (RTG). Więcej na temat urządzeń do przeglądania odzieży i bagażu przeczytacie w kolejnym artykule Cezarego Mecwaldowskiego znajdującego się w tym wydaniu naszego czasopisma. ■

Sergiusz Parszowski
Lider zespołu eksperckiego Instin.pl
Prezes think tanku ObserwatoriumBezpieczeństwa.pl

BEZPIECZEŃSTWO SIECI: PRÓBA PRZEDSTAWIENIA DOBRYCH PRAKTYK ORAZ KLUCZOWYCH KONCEPCJI

Grzegorz Data

W obecnych czasach gospodarki opartej na przesyłaniu oraz przetwarzaniu danych, kwestia zabezpieczenia sieci nabiera fundamentalnego znaczenia. W miarę jak codzienne operacje przedsiębiorstw oraz ludzi stają się coraz bardziej uzależnione od infrastruktury komputerowej, potrzeba pewnych i solidnych środków bezpieczeństwa sieci staje się bardziej paląca niż kiedykolwiek wcześniej.

Niniejszy artykuł jest próbą analizy najlepszych praktyk związanych z bezpieczeństwem sieci komputerowej. Omówimy kluczowe koncepcje bezpieczeństwa sieci, spróbujemy zidentyfikować potencjalne zagrożenia, omówimy środki bezpieczeństwa zarówno podstawowe, jak i zaawansowane, oraz podkreślimy potrzebę opracowania kompleksowej polityki bezpieczeństwa sieci.

Zrozumienie bezpieczeństwa sieci komputerowej

Pojęcie bezpieczeństwa sieci odnosi się do kompleksowej ochrony infrastruktury komputerowej przed nieautoryzowanym dostępem, niewłaściwym wykorzystaniem, modyfikacją lub odmową usług. Obejmuje ono szereg praktyk, technologii i zasad mających na celu zabezpieczenie danych oraz zapobieganie ewentualnym atakom na sieć. Zrozumienie istoty bezpieczeństwa sieci stanowi pierwszy krok ku skutecznej implementacji środków ochrony.

Znaczenie bezpieczeństwa sieci

Bezpieczeństwo sieci gwarantuje poufność, integralność i dostępność danych. Dzięki wdrożeniu solidnych środków bezpieczeństwa możliwe jest zabezpieczenie wrażliwych informacji przed dostępem osób niepowołanych, zapobieżenie nieautoryzowanym modyfikacjom danych oraz utrzymanie dostępności sieci i usług dla autoryzowanych użytkowników.

Ochrona reputacji i zaufania organizacji w dzisiejszej erze cyfrowej związana jest z zagadnieniem bezpieczeństwa danych. Ataki cybernetyczne są powszechne, a organizacje, które nie skupiają się na zabezpieczeniu swoich sieci, narażają się na poważne konsekwencje. Priorytetowe traktowanie bezpieczeństwa sieci świadczy o zaangażowaniu w ochronę danych klientów, co przekłada się na budowanie zaufania i wiarygodności.

Bezpieczeństwo sieci pełni również kluczową rolę w zapewnianiu zgodności z przepisami i normami branżowymi. W wielu sektorach, takich jak opieka zdrowotna czy finanse, istnieją konkretne wymagania dotyczące bezpieczeństwa, których organizacje muszą przestrzegać. Dzięki solidnym

środkom bezpieczeństwa sieci można osiągnąć zgodność z regulacjami, unikając potencjalnych konsekwencji prawnych i finansowych.

Kluczowe terminy i koncepcje bezpieczeństwa sieci

Przed zagłębieniem się w praktyki bezpieczeństwa sieci, istotne jest poznanie kluczowych terminów i koncepcji stanowiących fundament tego obszaru. Niektóre z kluczowych terminów obejmują zapory ogniowe, systemy wykrywania włamań (IDS), szyfrowanie, wirtualne sieci prywatne (VPN) oraz mechanizmy uwierzytelniania.

- **Zapory Ogniowe** stanowią barierę pomiędzy siecią wewnętrzną a światem zewnętrznym, monitorując oraz kontrolując ruch przychodzący i wychodzący. Pełnią one kluczową rolę w zapobieganiu nieautoryzowanemu dostępowi oraz ochronie sieci przed złośliwymi działaniami.
- **Systemy Wykrywania Włamań (IDS)** zostały zaprojektowane w celu wykrywania potencjalnych zagrożeń bezpieczeństwa i skutecznego reagowania na nie. Monitorują one ruch sieciowy, analizując go pod kątem podejrzanych działań lub wzorców.
- **Szyfrowanie** to proces konwersji danych do formy nieczytelnej dla osób nieupoważnionych. Zabezpiecza ono poufność danych, sprawiając, że stają się one niezrozumiałe dla osób nieposiadających klucza deszyfrującego. Szyfrowanie znajduje powszechne zastosowanie w ochronie poufnych informacji, takich jak hasła, dane kart kredytowych czy dane osobowe.
- **Wirtualne sieci prywatne (VPN)** zapewniają bezpieczne i zaszyfrowane połączenia przez Internet, umożliwiając zdalny dostęp do sieci prywatnej. Są one powszechnie stosowane do ustanawiania bezpiecznych połączeń dla pracowników zdalnych lub do bezpiecznego łączenia oddziałów. Zapewniają one, że dane przesyłane przez Internet są chronione przed podsłuchem oraz nieuprawnionym dostępem.
- **Mechanizmy uwierzytelniania** odgrywają kluczową rolę w procesie przyznawania dostępu do sieci poprzez weryfikację tożsamości użytkowników lub urządzeń. Standardowe metody uwierzytelniania obejmują hasła, dane biometryczne oraz uwierzytelnianie dwuskładnikowe."

Identyfikacja potencjalnych zagrożeń dla infrastruktury sieciowej

W kontekście zabezpieczania sieci, kluczowym etapem jest identyfikacja potencjalnych zagrożeń, które mogą zagrażać integralności struktury. W dziedzinie ataków sieciowych pojawia się różnorodność form, zatem świadomość tych zagrożeń oraz podjęcie adekwatnych środków zaradczych jest niezwykle istotne.

Podstawowe typy ataków sieciowych

Ataki na sieć obejmują zarówno te o charakterze prostym, jak choćby próby złamania hasła, jak i zaawansowane ataki, takie jak rozproszone ataki typu „odmowa usługi" (DDoS) czy infiltrowanie złośliwego oprogramowania. Każdy rodzaj ataku niesie ze sobą unikalne zagrożenia dla infrastruktury sieciowej, dlatego zrozumienie ich charakterystyki jest kluczowe dla skutecznej obrony.

Przykłady ataków obejmują:

- Ataki typu phishing: polegające na zwodzeniu użytkowników do ujawniania poufnych informacji poprzez podszywanie się pod godne zaufania podmioty. Ataki te często przybierają formę fałszywych wiadomości e-mail lub stron internetowych imitujących legalne źródła.
- Ataki typu spoofing: polegające na podszywaniu się pod legalne urządzenia lub użytkowników w celu uzyskania nieautoryzowanego dostępu do sieci. Osoby przeprowadzające atak mogą manipulować pakietami sieciowymi, aby sprawiały wrażenie, jakby pochodziły z zaufanych źródeł.
- Ataki typu man-in-the-middle: w których atakujący przechwytują komunikację między dwiema stronami, umożliwiając podsłuchiwanie lub nawet zmianę przesyłanych wiadomości. Ten rodzaj ataku stanowi szczególne zagrożenie, gdyż może działać niezauważalnie, naruszając poufność i integralność danych sieciowych.

Rozpoznawanie luk w zabezpieczeniach infrastruktury sieciowej

Oprócz zrozumienia typów ataków, równie kluczowe jest identyfikowanie luk w zabezpieczeniach sieci. Te luki mogą wynikać z nieaktualnego oprogramowania, błędnie skonfigurowanych urządzeń, słabych haseł czy też niewystarczającej kontroli dostępu.

Typowe luki zabezpieczeń obejmują:

- Nieaktualne oprogramowanie: atakujący wykorzystują to jako punkt wejścia do nieautoryzowanego dostępu do sieci. Regularna aktualizacja oprogramowania stanowi skuteczną metodę minimalizowania ryzyka korzystania z potencjalnych luk.
- Błędnie skonfigurowane urządzenia: nieprawidłowo skonfigurowane zapory sieciowe, routery czy przełączniki mogą tworzyć luki w zabezpieczeniach, które stają się podatne na wykorzystanie przez atakujących. Regularne monitorowanie konfiguracji urządzeń sieciowych i ich zgodność z najlepszymi praktykami w dziedzinie bezpieczeństwa może skutecznie zapobiec potencjalnym zagrożeniom.
- Słabe hasła: wielu użytkowników nadal stosuje łatwe do odgadnięcia hasła lub używa tego samego hasła na wielu kontach. Wdrożenie rygorystycznych zasad dotyczących haseł, takich jak wymóg używania kombinacji wielkich i małych liter, cyfr oraz znaków specjalnych, zdecydowanie podnosi poziom bezpieczeństwa sieci.
- Niewystarczająca kontrola dostępu: nadanie użytkownikom nadmiernych uprawnień lub brak deaktywacji dostępu, gdy nie jest on już konieczny, może znacząco zwiększyć ryzyko działań nieautoryzowanych. Regularna rewizja i aktualizacja zasad kontroli dostępu stanowi skuteczną strategię zapewniania, że tylko uprawnione osoby mają dostęp do zasobów sieciowych."

Wdrożenie podstawowych Środków Bezpieczeństwa Sieci

Egzekwowanie podstawowych środków bezpieczeństwa sieci jest niezbędne dla ustanowienia solidnych fundamentów w ochronie przed potencjalnymi zagrożeniami. W tym kontekście, kluczowym krokiem jest skonfigurowanie zapór ogniowych oraz systemów wykrywania włamań, które stanowią pierwszą linię obrony przed próbami nieautoryzowanego dostępu. Systemy wykrywania włamań (IDS/IPS) pełnią istotną rolę, uzupełniając działanie zapór ogniowych poprzez aktywne monitorowanie ruchu sieciowego i generowanie alertów w przypadku wykrycia podejrzanej aktywności.

Kolejnym krokiem jest regularne aktualizowanie infrastruktury sieciowej poprzez stosowanie łatek i aktualizacji zabezpieczeń, eliminujących potencjalne luki w zabezpieczeniach. Dalsze działania obejmują wdrażanie silnej kontroli dostępu oraz mechanizmów uwierzytelniania użytkowników, wykorzystujących silne hasła, uwierzytelnianie wieloskładnikowe i kontrolę dostępu opartą na rolach.

Zapobieganie utracie danych (DLP) to jedna z metod cyberbezpieczeństwa, która łączy technologię i najlepsze praktyki, aby zapobiec ujawnieniu wrażliwych informacji poza organizacją, w szczególności danych regulowanych, takich jak dane osobowe i dane związane ze zgodnością wieloma normami bezpieczeństwa: ISO 27001, NIST, itp.

Sandboxing, stanowiący element strategii zapewnienia bezpieczeństwa w cyberprzestrzeni, to procedura polegająca na uruchamianiu kodu lub otwieraniu plików w kontrolowanym, izolowanym środowisku na komputerze hosta, które symuluje środowisko operacyjne użytkownika końcowego. Celem sandboxingu jest monitorowanie otwieranych plików lub kodu w celu wykrywania potencjalnie złośliwego zachowania, mającego na celu zapobieganie przedostawaniu się zagrożeń do sieci. Przykładowo, zastosowa-

nie tej praktyki pozwala bezpiecznie identyfikować i blokować złośliwe oprogramowanie w plikach takich jak PDF, Word, Excel i PowerPoint, zanim te pliki dotrą do użytkownika końcowego, który nieświadomie może stanowić potencjalne źródło ryzyka.

Uwierzytelnianie dwuskładnikowe (2FA): W dzisiejszym środowisku opanowanym przez ransomware, uwierzytelnianie dwuskładnikowe powinno być również uważane za minimalny wymóg dla wszystkich form zdalnego dostępu. SMS nie jest uważany za optymalne rozwiązanie, ale często może być najwygodniejszy i najprostszy do wdrożenia. Aby zwiększyć bezpieczeństwo przy użyciu telefonów komórkowych, dostępne są bezpłatne aplikacje uwierzytelniające od Google, Microsoft i innych.

Następnie, zaleca się przeszkolenie personelu w zakresie najlepszych praktyk bezpiecznego korzystania z Internetu, zwracając uwagę na rozpoznawanie prób phishingu oraz prawidłowe postępowanie z poufnymi informacjami. Implementacja protokołów szyfrowania, takich jak Secure Sockets Layer (SSL) czy Transport Layer Security (TLS), stanowi kolejny kluczowy element zabezpieczania przesyłanych danych.

Aby kompleksowo odpowiadać na potencjalne incydenty, niezbędne jest opracowanie planu reagowania na incydenty, obejmującego kroki od wykrywania incydentów, przez ich powstrzymywanie, eliminowanie, aż po odzyskiwanie. Mimo że powyższe podstawowe środki są niezwykle ważne, kolejne zaawansowane działania mogą dalsze wzmocnić ochronę sieci.

Lepsza kontrola zasobów

Większe organizacje muszą wdrożyć bardziej zaawansowane zasoby, aby wykrywać i blokować nieautoryzowane urządzenia w dużych sieciach.

- Blokowanie lub poddawanie kwarantannie urządzeń: Rozwiązania kontroli dostępu do sieci (Network Access Control NAC) testują nieaktualne lub podatne na ataki oprogramowanie na punktach końcowych i przekierowują urządzenia do kwarantanny do czasu ich usunięcia. Nieautoryzowane urządzenia mogą być blokowane lub poddawane kwarantannie. Niektóre funkcje NAC można uzyskać, dodając filtrowanie adresów MAC lub białe listy do zapór ogniowych i serwerów, ale utrzymanie białych list może być czasochłonne.
- Ciągłe skanowanie zasobów: Narzędzia IT Asset Management (ITAM) mogą skanować urządzenia podłączone do sieci i wysyłać alerty lub blokować niezarejestrowane urządzenia. Organizacje muszą zweryfikować typy zasobów, które będą wykrywane. Niektóre aplikacje, infrastruktura chmurowa, sprzęt sieciowy lub urządzenia Internetu rzeczy (IoT) mogą wymagać bardziej zaawansowanego ITAM lub dodatkowych narzędzi do ich wykrywania.
- Wyłączenie niepotrzebnych funkcji: Wszelkie nieużywane porty dostępu w zaporze sieciowej, niepotrzebny dostęp zdalny (pamięć masowa, drukarka, routery itp.) i podobne funkcje często nie będą monitorowane. Hakerzy będą starali się znaleźć i wykorzystać

te możliwości. Lepiej po prostu je wyłączyć, jeśli są niepotrzebne. Z tego powodu organizacje powinny również wyłączyć funkcje Universal Plug and Play (UPnP) po zakończeniu konfiguracji, ponieważ hakerzy znaleźli sposoby na wykorzystanie funkcji automatyzacji do ładowania złośliwego oprogramowania.

- Uwierzytelnianie wieloskładnikowe (MFA): Rozwijające się organizacje stoją w obliczu zwiększonego ryzyka naruszenia, ponieważ potencjalne szkody wynikające z kradzieży danych uwierzytelniających rosną wraz z wielkością i reputacją firmy. Aby zmniejszyć to ryzyko, wiele z nich stosuje uwierzytelnianie wieloskładnikowe, aby zapewnić lepsze bezpieczeństwo niż 2FA, zwłaszcza gdy aplikacje lub tokeny zastępują wrażliwy tekst SMS jako czynnik. Rozwiązania biometryczne i bezhasłowe mogą być droższe, ale trudne do sfałszowania.
- Segmentacja i izolacja sieci to zaawansowana strategia, polegająca na podziale sieci na mniejsze podsieci w celu ograniczenia przepływu danych i minimalizowania skutków potencjalnego naruszenia. Wdrożenie kontroli dostępu gwarantuje, że tylko upoważnione osoby i urządzenia mają dostęp do konkretnych segmentów, co skutecznie redukuje ryzyko bocznego ruchu atakujących.
- Model bezpieczeństwa zerowego zaufania (Zero Trust Network Access) definiuje, że użytkownik powinien posiadać dostęp i uprawnienia jedynie w zakresie niezbędnym do skutecznego pełnienia swojej roli. Jest to podejście diametralnie różne od klasycznych rozwiązań bezpieczeństwa, takich jak Virtual Private Network (VPN), które nadają użytkownikowi pełny dostęp do sieci docelowej. Pomysł dostępu do sieci o zerowym zaufaniu, często określany również jako Software-Defined Perimeter (SDP), umożliwia precyzyjny dostęp do aplikacji organizacji dla użytkowników, którym ten dostęp jest niezbędny w celu efektywnego wykonywania ich obowiązków.
- Kluczowym elementem jest ustanowienie kompleksowej polityki bezpieczeństwa sieci, która precyzyjnie określa cele związane z bezpieczeństwem, zasady korzystania z sieci oraz procedury, a także przewiduje odpowiedzi na potencjalne naruszenia. Przestrzeganie tych wytycznych stanowi fundament w utrzymaniu bezpiecznego środowiska sieciowego.

Zabezpieczanie sieci to ciągły proces

Sieci tworzą pomost pomiędzy użytkownikami i ich komputerami z jednej strony, a zasobami, do których muszą dotrzeć, z drugiej. Bezpieczeństwo sieci chroni ten most, ale aby zapewnić bezpieczeństwo, jednak każdy koniec tego mostu musi być również chroniony przez zabezpieczenia użytkowników, aplikacji, danych i zasobów (punktów końcowych, serwerów, kontenerów itp.). idąc dalej ta analogią, most i jego fundamenty muszą być konserwowane i stale monitorowane, aby mieć pewność, że wszystko działa prawidłowo i bez błędów. Każdy element strategii bezpieczeństwa wzmacnia i chroni organizację jako całość przed awarią któregokolwiek konkretnego elementu.

Jednak sieci, tak jak mosty, działają dobrze tylko w przypadku określonego zakresu użytkowników, ruchu i zasobów. W miarę rozwoju i kurczenia się organizacji sieć i chroniące ją zabezpieczenia będą musiały ewoluować, aby dotrzymać kroku ciągłemu postępowi technologii.

Zespoły ds. bezpieczeństwa IT muszą nie tylko zachować świadomość swoich obecnych i przyszłych potrzeb, ale także muszą jasno komunikować te potrzeby interesariuszom nietechnicznym, aby uzyskać budżety oraz inne wsparcie. ■

mjr Grzegorz Data
specjalista ds. informatyki i łączności
OISW w Rzeszowie

Linc Polska Sp. z o.o.

BEZPIECZNE FARMY FOTOWOLTAICZNE

Od kilku lat zauważamy dynamiczny rozwój rynku farm fotowoltaicznych, będący rezultatem intensywnych działań na rzecz zrównoważonej gospodarki energetycznej. Coraz większa świadomość ekologiczna społeczeństwa oraz wsparcie rządu dla odnawialnych źródeł energii skutkują znaczącym wzrostem liczby i mocy farm fotowoltaicznych na polskim rynku. W zeszłym roku w Polsce za pomocą prawie 17GW elektrowni fotowoltaicznych zaspokojono 7,5% całkowitego zapotrzebowania na energie elektryczną.

Rok 2024 zapowiada dalszy rozwój tego rynku. Nowością są duże magazyny energii, które mają zapewnić lepsze bilansowanie wyprodukowanej energii. Potrzeba współdziałania tych systemów sprawia, że pojawia się dodatkowa opcja inwestycji i modernizacji również istniejących obiektów. Spodziewamy się rozwoju zarówno małych instalacji pojedynczych megawatów, jak również tych dużych przekraczających 30 MW.

Budowa farmy fotowoltaicznej jest procesem kosztownym, ale przynosi też relatywne zyski. Jednakże, aby je wypracować należy zadbać zarówno o stan techniczny urządzeń, jak i o zabezpieczenie obiektu przed wandalami i możliwymi kradzieżami.

Tanie, czy skuteczne? Masz wybór!

Często systemy zabezpieczeń wybierane są wg kryterium najniższej ceny – niestety efektem takiego doboru rozwiązań jest duża ilość fałszywych alarmów lub brak tych istotnych. W wielu przypadkach istniejące systemy stwarzają jedynie wrażenie działania i zabezpieczania farmy fotowoltaicznej. Przeciętna stacja monitorująca ma do obsłużenia stosunkowo dużo fałszywych alarmów, co skutkuje tym, iż w dłuższej perspektywie operator po prostu nie jest w stanie trafnie ocenić sytuacji.

Jednocześnie na przestrzeni ostatnich lat technologia niezwykle się rozwinęła i pojawiają się coraz to nowsze i skuteczniejsze systemy detekcji intruzów. Trudno nie wspomnieć o rozwoju AI w wielu sektorach biznesu – również w branży zabezpieczeń, gdzie powszechnie stosowane są kamery korzystające z algorytmów AI.

Wykorzystaj algorytmy AI

Aby skutecznie zabezpieczyć nie tylko farmę fotowoltaiczną, ale każdy obiekt, należy wybrać rozwiązanie nowoczesne, oparte na najnowszych zdobyczach technologii. Takim rozwiązaniem zdecydowanie jest CAMECT hub do monitoringu wideo, który wykrywa intruzów z wykorzystaniem algorytmów AI. Ten inteligentny system jest w stanie zidentyfikować ponad 30 różnych obiektów, dzięki czemu z powodzeniem odróżni człowieka od zwierzęcia i wyśle tylko ten alarm, który dotyczy faktycznego zagrożenia. Skuteczność w eliminowaniu fałszywych alarmów w przypadku CAMECT wynosi aż 99,7 proc.

CAMECT bardzo dobrze współpracuje z najnowszymi kamerami takimi, jak Honeywell Serii 35, które doskonale sprawdzają się przy zabezpieczaniu farm fotowoltaicznych, ale również innych obiektów infrastruktury krytycznej. Co ważne spełniają wymogi cyberbezpeiczeństwa stawiane przez dyrektywę NIS2, która niebawem zacznie obowiązywać w Polsce. Są one również wypełni zgodne z NDAA.

CAMECT jest dobrym rozwiązaniem w przypadku modernizacji istniejących już instalacji zabezpieczających, ponieważ z powodzeniem może pracować z kamerami IP starszego typu lub nawet zostać podłączonym bezpośrednio do rejestratorów stanowiąc doskonałe uzupełnienie o system analizy wideo.

Niezależnie od tego, czy mówimy o nowych, czy istniejących obiektach, ważnym jest, aby osiągnąć cel jakim jest minimalna ilość fałszywych alarmów przy jednoczesnym zapewnieniu wykrycia tych pożądanych. Odpowiedzią na tę potrzebę jest właśnie CAMECT, inteligentny HUB do wideo monitoringu. ■

Artykuł firmy **Linc Polska**

camect

CAMECT SMART HUB

- MNIEJ NIŻ 1% **FAŁSZYWYCH ALARMÓW**
- NAJLEPSZA W SWOJEJ KLASIE **ANALIZA AI**

NIEUZASADNIONE ALARMY GENERUJĄ ZBYT DUŻE KOSZTY?

Wyobraź sobie system, który **eliminuje fałszywe alarmy**, bo rozróżnia **ludzi, owady i deszcz**.

Taki właśnie jest **Camect** Smart Hub - **rejestrator z Analizą AI** do wykrywania **intruzów** w oparciu o sieci neuronowe.

- Szybka powtórka - zobacz 1 dzień w 24 h
- Zapis ciągły
- Bezpieczny dostęp zdalny bez dodatkowego VPN
- Szybkie wyszukiwanie zdarzeń
- Mniej niż 1% fałszywych alarmów
- Rozróżnianie ponad 30 różnych obiektów

OFICJALNY DYSTRYBUTOR:

LINC POLSKA SP. Z O.O.
ul. Czarnkowska 22, 60-415 Poznań
tel.: +48 61 839 19 00, www.linc.pl

Linc Polska Sp. z o.o.

IFTER EQU
– KOMPLEKSOWE ZARZĄDZANIE BEZPIECZEŃSTWEM OBIEKTÓW BIUROWYCH

Firma IFTER od blisko 25 lat produkuje rozwiązania dedykowane do systemów bezpieczeństwa. Główne produkty naszej firmy to system do integracji i wizualizacji IFTER EQU2 oraz kontrola dostępu EQU ACC. Znajdują one zastosowanie na obiektach wymagających najwyższej jakości przy bardzo dużych możliwościach. Jednym z takich obiektów jest siedziba Urzędu Marszałkowskiego Województwa Zachodniopomorskiego, gdzie wdrożono nasze produkty uzyskując bardzo ciekawe rozwiązanie.

Na tym obiekcie zostały wykorzystane kompleksowo nasze rozwiązania zarówno w zakresie systemów integrujących, zarządzających i wizualizujących, jak i kontroli dostępu (SKD) rozbudowane o elementy rejestracji czasu pracy (RCP). Mimo tak szerokiego zakresu systemu, zarządzanie nim jest proste i zautomatyzowane poprzez wykorzystanie jednej bazy danych dla wszystkich podsystemów.

Wizualizacja systemów bezpieczeństwa

Wizualizacja i integracja obejmuje system sygnalizacji pożaru, kontrolę dostępu, sygnalizację włamania i napadu oraz telewizję dozorową.

Sama wizualizacja została wykonana w sposób intuicyjny z mechanizmami prowadzenia od planu ogólnego do szczegółowego oraz w przypadkach ochrony obszarów wysokiego ryzyka: automatycznej prezentacji miejsca zagrożonego. Wszystkie integrowane systemy prezentowane są na wspólnych podkładach architektonicznych obiektu, dzięki czemu w przypadku np. alarmu pożarowego, operator może łatwo

IFTER®

AND SEE MORE

OCHRONA

System EQU ACC 400 wykonany jest w klasie 4 zgonie z normą PN-EN60839-11, zapewniając najwyższy poziom bezpieczeństwa w zakresie kontroli dostępu. System jest dedykowany dla obiektów wojskowych, przemysłowych i infrastruktury krytycznej.

EFEKTYWNY KOSZTOWO

Dzięki swojej modułowości zarówno w zakresie sprzętu jak i oprogramowania, może być efektywnie dostosowany do potrzeb klienta. Cały system produkowany jest na terenie Unii Europejskiej więc nie ma problemów z ciągłością dostaw.

INTERAKTYWNY

Rozbudowany pakiet oprogramowania zapewnia nie tylko wizualizację w trzech technologiach, (raster, wektor, web) która jest zintegrowana z innymi systemami bezpieczeństwa, ale mamy do dyspozycji również recepcję, awizację czy RCP.

TECHNOLOGIA

Dbałość o szczegóły podczas projektowania EQU ACC 400 zapewnia wysoką ochronę przed przepięciami i uszkodzeniami mechanicznymi, szeroki zakres temperatury pracy, wykrywanie sabotaży i antymaskingu wejść. Dzięki temu sprzęt ma 5 lat gwarancji.

OTWARTOŚĆ

Obsługa OSDPv2 pozwala przy zachowaniu wysokiego poziomu bezpieczeństwa na podłączenie czytników dowolnego producenta. Uproszczona konfiguracja wyłącznie z oprogramowania, przyspiesza i upraszcza proces uruchomienia

ELASTYCZNOŚĆ

Kontroler przechowuje w pamięci pełną konfigurację i do 1mln kart i 0,5mln zdarzeń. Każdy komunikuje się z systemem nadzorczym po TCP/IP, więć nie ma znaczenia czy wszystkie kontrolery znajdują się w tym samym budynku czy są rozproszone po całym świecie.

IFTER® EQU VER. 2

Wola Niemiecka 78C, 21-025 Niemce
http://www.ifter.eu/index.php/pl/
Tel.+48 81 473 53 17

zweryfikować miejsce pożaru klikając w ikony kamer znajdujących się w pobliżu pobudzonego czujnika. Prezentowany obraz z kamer dodatkowo wyświetlany jest automatycznie po przyjściu alarmu wraz z obrazem archiwalnym na 10s przed powstaniem zagrożenia. Dzięki wbudowanej obsłudze kontroli dostępu, operator może śledzić przemieszczanie się osób z ich weryfikacją dzięki kamerom. Na bieżąco widzi również ile osób znajduje się na poszczególnych kondygnacjach. Operator dzięki wysokiej intuicyjności IFTER EQU2 nie ma problemów ze skutecznym nadzorowaniem bezpieczeństwa nad ponad 5tys. czujników i przejść. Dodatkowo należy pamiętać, że w każdej chwili system można rozszerzyć o monitorowanie wszystkich urządzeń aktywnych sieci szkieletowej oraz parametrów środowiskowych serwerowni takich jak zasilanie, temperatura i wilgotność.

W celu skutecznego zarządzania dwoma budynkami, ochrona monitoruje system w dwóch oddzielnych centrach monitorowania obsługiwanych przez dwa serwery integracyjne.

Kontrola dostępu

Budynki mają strukturę organizacyjną typową dla obiektów biurowych, dlatego też jest tutaj ponad 800 przejść objętych kontrolą dostępu IFTER EQU ACC. Każdy z kontrolerów ma połączenie z systemem nadzorczym poprzez sieć Ethernet, dlatego rozbudowa systemu o kolejne przejścia jest uproszczona do uzbrojenia przejścia w czytniki i czujniki oraz kontroler, który podpina się do najbliższego switch-a. Każdy z kontrolerów zgodnie z normą PN-EN-60839 montowany jest w wytrzymałej obudowie wyposażonej w zasilacz buforowy wraz z akumulatorem podtrzymującym działanie SKD na danym przejściu. Dzięki temu nawet podczas braku zasilania głównego, obiekt jest w pełni chroniony i monitorowany. Taka struktura systemu pozwala na bardzo szybkie działanie i wykazuje się wysoką niezawodnością.

Dzięki rozbudowanym funkcjonalnościom IFTER EQU ACC kontrola dostępu została dostosowana do indywidualnych potrzeb każdego przejścia, np. drzwi wejściowe, aby umożliwić wejście interesantom są automatycznie odblokowywane w godzinach ich przyjmowania, niektóre pomieszczenia biurowe są sterowane na zasadzie pierwsze zbliżenie karty do czytnika zezwala na swobodne przechodzenie przez te drzwi, kolejne zbliżenie przywraca działanie SKD. Pomieszczenia o najbardziej restrykcyjnych obostrzeniach zabezpieczane są kartą z PIN lub poprzez zbliżenie karty dwóch osób. Ochrona korzysta również z kart modyfikujących pracę przejścia jak stałe otwarcie czy też jego blokadę. Pozwala to ochronie na szybką reakcję w zaistniałej sytuacji. Do dyspozycji jest również kontroler globalnego anti-passback, który kontroluje, aby osoba, która np. nie opuściła budynku „A" nie mogła wejść do budynku „B". Kontroler zarządza pracą wszystkich przejść w systemie.

Rejestracja czasu pracy

Zamontowanie w licznych wejściach do budynków dotykowych, kolorowych wyświetlaczy pozwoliło na rejestrację zdarzeń rozpoczęcia i zakończenia pracy, wyjść służbowych i wielu innych typów przejść pracowniczych, które są swobodnie definiowane. Dzięki temu rozwiązaniu uprościły się zadania monitorowania czasu pracy stawiane księgowości, ponieważ wyliczanie czasu pracy jest realizowane automatycznie. Systemem RCP zostały objęte nie tylko obiekty znajdujące się w Szczecinie, ale również zamiejscowe. Dlatego w przypadku oddelegowania pracownika do oddziału, nie ma problemu z rozliczeniem jego przepracowanych dni. Moduł RCP pozwala na definiowanie harmonogramów pracy pracowników oraz rozliczanie ich względem wybranych punktów kontroli, które mogą być zarówno terminalami RCP jak i standardowymi przejściami kontroli dostępu. Standardowo jest wiele typów absencji z ewentualnymi limitami, które będą brane pod uwagę podczas wyliczania podstawy do wypłacenia pensji. Podczas analizy spójności danych, system sugeruje brakujące dane z oczekiwaną datą wystąpienia.

Liczne raporty i zestawienia analityczne pozwalają w łatwy sposób na obliczanie przepracowanych godzin oraz przeprowadzają optymalizację pracy.

Oprogramowanie do zarządzania SKD

Na szczególną uwagę zasługuje oprogramowanie do konfigurowania i zarządzania kontrolą dostępu w formie aplikacji pod system Windows. Jego rozbudowane możliwości pozwalają na sprawne zarządzanie systemami nawet na 800 przejść. Do głównych zalet należy możliwość grupowania sprzętu (kontrolerów i przejść) np. względem kondygnacji, budynków, miejscowości. Drugim ułatwieniem jest możliwość tworzenia grup organizacyjnych typu pracownicy działu HR, informatycy czy pracownicy fizyczni. Każdej grupie możemy przypisać restrykcje dotyczące osób w grupie (jakie wymagania będziemy mieli względem danych, ważność karty, do jakich grup dostępowych można przypisać taką osobę). Następstwem przypisania osoby do wybranej grupy będzie automatyczne filtrowanie tej osoby względem wybranej grupy, co w sposób wydatny usprawnia zarządzanie wieloma tysiącami użytkowników. Nie ma ograniczeń w tworzeniu ilości grup dostępowych, które są przypisywane do kart. Każdej grupie przypisywany jest harmonogram oraz wybrane przejścia. W takiej grupie

mogą być zarówno pojedyncze przejścia jak i np. wszystkie wejścia do budynku.

Do jednej osoby możemy przypisać wiele kart, które będą reprezentowały np. różne technologie transmisji danych (Unique, Mifare DESFire, UHF), jak również zmiana karty nie powoduje braku ciągłości zdarzeń dla danej osoby. Dzięki czemu po danych gościa przychodzącego wielokrotnie na obiekt można filtrować jakie karty były mu wydawane i jak się poruszał po obiekcie. Mechanizm ten pozwala również w przypadku zgubienia lub zapomnienia karty przez pracownika, wydanie jednodniowego duplikatu karty przez ochronę. W przypadku wykrycia użycia oryginalnej karty, duplikat jest automatycznie blokowany. Osobie dodatkowo można przypisać samochód, który będzie automatycznie rozpoznawany po tablicach rejestracyjnych lub po karcie UHF.

W celu ułatwienia zarządzania użytkownikami SKD system pozwala na import danych z pliku, import automatyczny z systemu kadrowego, synchronizację danych poprzez usługi katalogowe korzystające z protokołu LDAP. Do ułatwień możemy również zaliczyć automatyczne filtrowanie kart względem ważności, usunięcia, ważności badań/szkoleń. Jeżeli w przejściu zamontowany jest terminal to na nim mogą być wyświetlane informacje dodatkowe postaci: zbliżającej się daty wygaśnięcia uprawnień, ważności badań/szkoleń. Uproszczenie pracy zapewnia również moduł personalizacji kart, który automatycznie pobiera zdjęcie z aparatu fotograficznego, wkleja go do wcześniej przygotowanego szablonu, który pobiera dane z systemu typu imię i nazwisko, grafikę karty. Po korekcie wizualnej, karta jest drukowana.

W przypadku przeprowadzania ewakuacji nie wynikającej z wykrycia pożaru, ochrona może klikając na jeden przycisk odblokować wszystkie przejścia ewakuacyjne. Pracownicy zbierają się w punkcie ewakuacyjnym dokąd kieruje ich ochrona, przy okazji zczytując dzięki czytnikom bezprzewodowym ich karty. Pozwala to ochronie bieżąco monitorować ilość osób, która pozostała w budynku. W podobny sposób, grupowo można zablokować wszystkie przejścia znajdujące się w danej grupie sterowań, klikając na przycisk w oprogramowaniu.

Aplikacje Web

Dla ułatwienia obsługi osobom, które mają wprowadzać dane w sposób ograniczony i wykonywać raporty oraz analizy wcześniej przewidziane dla danego stanowiska najlepszym rozwiązaniem jest aplikacja Web, która pozwala na uruchomienie na dowolnym urządzeniu. W ten sposób na obiekcie wykorzystywanych jest 35 dostępów do systemu poprzez przeglądarkę Web w sekretariatach działów do wprowadzania

informacji o delegacji pracowników (gdzie się udaje, w jakim zakresie czasowym, jakim środkiem lokomocji) oraz liczne raporty dotyczące obecności, spóźnień itp.

Z aplikacji Web można dodawać i zarządzać pracownikami. Dla wybranego profilu można zdefiniować najbliższy czytnik, który w chwili zbliżenia karty wprowadzi niezbędne dane do aplikacji. Istotną cechą jest bardzo skuteczne zarządzanie dostępem do danych, pozwalające na ograniczanie tego dostępu wyłącznie osobom, które się tym zajmują. Dlatego sekretarka z działu „1" nie widzi pracowników z działu „2" i nie może modyfikować ich danych ani wykonywać raportów.

Należy zauważyć, że na innych obiektach dodatkowo poprzez aplikację WEB prowadzona jest awizacja gości łącznie z automatycznym generowaniem kodu QR pozwalającego na wejście na obiekt oraz liczne raporty i analityczne zestawienia. Dostępny jest również na bieżąco podgląd osób przebywających w poszczególnych obszarach bezpieczeństwa. W przypadku zerwania połączenia między urządzeniem, a głównym serwerem, zestawienie jest zamrażane, aby umożliwić dalszą prezentację.

Kompleksowe rozwiązanie IFTER EQU2 wraz z wbudowaną kontrolą dostępu EQU ACC zaliczane jest do najbardziej rozbudowanych systemów bezpieczeństwa dostępnych na rynku. Przewagą tego systemu jest elastyczność, intuicyjność oraz możliwość dostosowania do potrzeb klienta. ■

Jerzy Taczalski

REWIZJA *ROZPORZĄDZENIA PARLAMENTU EUROPEJSKIEGO I RADY (UE) USTANAWIAJĄCEGO WARUNKI WPROWADZANIA WYROBÓW BUDOWLANYCH DO OBROTU*


Marta Iwańska


Ewa Sobór


Michał Chmiel


Michał Pietrzak

Wstęp

Obszar wyrobów budowlanych na terenie Unii Europejskiej regulowany jest obecnie rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 305/2011 ustanawiającym zharmonizowane warunki wprowadzania do obrotu wyrobów budowlanych (nazywane również „rozporządzeniem w sprawie wyrobów budowlanych" lub „CPR"), które zostało przyjęte w 2011 r. Jego głównym celem jest usprawnienie funkcjonowania jednolitego rynku i poprawa swobodnego przepływu wyrobów budowlanych w UE, poprzez ustanowienie zharmonizowanych warunków wprowadzania ich do obrotu. W praktyce oznacza to umożliwienie wprowadzenia wyrobów budowlanych legalnie do obrotu w jednym państwie członkowskim. Jednakże, jak większość przepisów, tak i przedmiotowe rozporządzenie było poddawane dalszej analizie i dyskusji w ramach Komisji Europejskiej. W konsekwencji przeprowadzonych prac opracowany został projekt nowego rozporządzenia ustanawiającego zharmonizowane warunki wprowadzania do obrotu wyrobów budowlanych, zmieniające rozporządzenie (UE) 2019/1020 i uchylające rozporządzenie (UE) 305/2011 mający na celu rozwiązanie znaczącej liczby problemów związanych m.in. z normalizacją, uproszczeniem dla mikroprzedsiębiorstw, nadzorem rynku i egzekwowaniem przepisów.

Obecny stan rozporządzenia „CPR”

Nadrzędnym celem prawodawstwa UE w zakresie wyrobów budowlanych jest „osiągnięcie właściwego funkcjonowania rynku wewnętrznego wyrobów budowlanych”. Jednakże, przepisy UE dotyczące wyrobów budowlanych często nie są zgodne ze wspólnym „nowym podejściem do harmonizacji technicznej” mającym zastosowanie do większości przepisów dotyczących rynku wewnętrznego wspólnoty i poszczególnych państw członkowskich. Sytuacja ta wynika z połączenia dwóch istotnych czynników: charakteru tych wyrobów oraz faktu, że obiekty budowlane i zezwolenia na ich eksploatację należą do kompetencji państw członkowskich. W rzeczywistości rozporządzenie w sprawie wspólnych przepisów nie określa żadnych wymagań dotyczących wyrobów, które musiałyby spełniać wyroby budowlane. Zamiast tego ustanawia zharmonizowane zasady dotyczące sposobu wyrażania ich właściwości użytkowych w odniesieniu do ich zasadniczych charakterystyk (np. reakcja na ogień, przewodność cieplna lub izolacyjność akustyczna) oraz zapewnia zharmonizowane zasady dotyczące oznakowania CE tych wyrobów. Państwa członkowskie pozostają w pełni odpowiedzialne za wymagania dotyczące bezpieczeństwa, środowiska i energii mające zastosowanie do budynków i obiektów inżynierii lądowej i wodnej.

System ustanowiony najpierw przez CPD („Construction Product Directive”), a następnie przez CPR („Construction Product Regulation”), miał na celu stworzenie warunków dla właściwego funkcjonowania rynku wewnętrznego wyrobów budowlanych. W praktyce oznaczało to umożliwienie wprowadzenia wyrobów budowlanych legalnie do obrotu, tj. udostępnienie wyrobu na rynku UE po raz pierwszy. Nie gwarantowało jednak, że wyrób opatrzony oznakowaniem CE może być systematycznie stosowany (tj. włączany do obiektów budowlanych) w każdym państwie członkowskim. Działo się tak dlatego, że przepisy dotyczące obiektów budowlanych oraz obiektów inżynierii lądowej i wodnej pozostają w szerokim zakresie kompetencji państw członkowskich, realizowanych na szczeblu krajowym, regionalnym, a nawet lokalnym, zgodnie z odpowiednim prawem wtórnym UE oraz Traktatem o funkcjonowaniu Unii Europejskiej (TFEU). Obecnie stosowane rozporządzenie ma na celu zapewnienie odpowiednich warunków dla swobodnego przepływu wyrobów budowlanych we wszystkich krajach członkowskich UE. Cel ten osiągany jest poprzez zapewnienie, że wyroby budowlane oznakowane oznakowaniem CE przechodzą jednolite badania i wymagają sporządzenia jednolitej deklaracji właściwości użytkowych (DoP), niezależnie od tego, gdzie są udostępniane na rynku UE. Wprowadzając wspólny język techniczny wyrażający właściwości użytkowe wyrobów budowlanych, CPR określa zharmonizowane warunki wprowadzania wyrobów budowlanych do obrotu.

Rozporządzenie CPR zapewnia zatem krajowym organom publicznym środki do określania ich wymagań dotyczących właściwości użytkowych budynków i obiektów budowlanych oraz do sprawdzania zgodności w zakresie ich kompetencji krajowych. CPR miał umożliwić państwom członkowskim realizację celów związanych z „bezpieczeństwem pożarowym”, „gospodarką energetyczną” i „zrównoważonym wykorzystaniem zasobów naturalnych” (które należą do siedmiu podstawowych wymagań dotyczących obiektów budowlanych określonych w załączniku I do CPR). Jednakże w sprawozdaniu Komisji opublikowanym w 2016 roku z realizacji i funkcjonowania CPR wskazano pewne uchybienia w jego wdrażaniu oraz znaczącą liczbę problemów związanych m. in. z normalizacją, uproszczeniem dla mikroprzedsiębiorstw, nadzorem rynku i egzekwowaniem przepisów, co w konsekwencji wymagało dalszej analizy i dyskusji. Komisja doszła do wniosku, że udało się sprostać pewnym wyzwaniom związanym z trudnościami we wdrażaniu i opóźnionym dostosowaniem przez zainteresowane strony oraz że konieczne są dalsze prace w celu poprawy wdrożenia CPR. W omawianym sprawozdaniu wskazano również znaczną liczbę kwestii wykraczających poza samo wdrożenie i zasługujących na dalszą poważną analizę i dyskusję. Wśród nich można wymienić:

- potrzebę szybszego i sprawniejszego procesu normalizacji z uwagi na wymagane stosowanie norm w procesach oceny i weryfikacji stałości właściwości użytkowych wyrobu budowlanego;
- konieczność wprowadzenia nadzoru rynku dla poszczególnych sektorów i egzekwowania przepisów;
- konieczność ustanowienia szczegółowych przepisów dotyczących jednostek notyfikowanych oraz
- usprawnienie zasad proceduralnych dotyczących finalizowania europejskich dokumentów oceny przez Europejską Organizację Oceny Technicznej (EOTA).

Rewizja CPR

Celem rewizji CPR jest poprawa rynku wewnętrznego wyrobów budowlanych poprzez ułatwienie ich swobodnego obrotu. Podczas rewizji większy nacisk został położony na zwiększenie poziomu ochrony środowiska, co powiązane będzie z regulacjami dotyczącymi trwałości wyrobów budowlanych i zrównoważonego wykorzystywania zasobów naturalnych. Dodatkowo, identyfikując problemy utrudniające funkcjonowanie jednolitego rynku wyrobów budowlanych, a tym samym

uniemożliwiające osiągnięcie pierwotnych celów CPR, Komisja Europejska wskazała dwa ogólne cele rewizji CPR:

1. stworzenie sprawnie funkcjonującego jednolitego rynku wyrobów budowlanych;
2. przyczynienie się do realizacji celów ekologicznej i cyfrowej transformacji, w szczególności nowoczesnej, zasobooszczędnej i konkurencyjnej gospodarki.

Natomiast jako cele szczegółowe Komisja Europejska wskazała:

1. odblokowanie systemu harmonizacji technicznej;
2. zmniejszenie krajowych barier w handlu wyrobami objętymi CPR;
3. poprawę egzekwowania przepisów i nadzoru rynku;
4. zapewnienie większej jasności (bardziej wyczerpujące definicje, ograniczenie nakładania się przepisów, kolizję przepisów z innymi aktami prawnymi) i uproszczenie;
5. zmniejszenie obciążeń administracyjnych, w tym poprzez uproszczenie procedur i cyfryzację;
6. zapewnienie bezpiecznych wyrobów budowlanych;
7. przyczynianie się do zmniejszenia ogólnego wpływu wyrobów budowlanych na klimat i środowisko, w tym dzięki stosowaniu narzędzi cyfrowych (cyfrowego paszportu).

Podsumowanie

Analizując projekt nowego rozporządzenia CPR dotyczącego oceny wyrobów budowlanych należy zwrócić uwagę na jego mocne strony oraz możliwości wynikające z rewizji. Wśród mocnych stron należy wymienić fakt, iż nowe rozporządzenie spowoduje zastąpienie starych mandatów nowymi wnioskami standaryzacyjnymi zgodnie z rozporządzeniem UE 1025/2012, a co za tym idzie daje szansę na wyjście z obecnego impasu normalizacyjnego, który powoduje brak harmonizacji norm i cytowań w Dzienniku Urzędowym UE. Zauważyć można również, iż rewizja umożliwi opracowywanie dobrowolnych norm zharmonizowanych obejmujących specyficzne wymagania dotyczące wyrobów (np. środowiskowe, bezpieczeństwa i funkcjonalne), co może bezpośrednio prowadzić do zwiększenia ilości norm zharmonizowanych opracowanych przez CEN i CENELEC w obszarze wyrobów budowlanych. Rewizja umożliwia ponadto poprawę zrównoważenia środowiskowego wyrobów budowlanych.

Należy jednak pamiętać, że każde nowe przedsięwzięcie niesie ze sobą, oprócz mocnych stron i możliwości, również pewne słabe strony oraz zagrożenia, bądź nowe wyzwania. Jedną z takich słabych stron analizowanego projektu są przypisane Komisji Europejskiej uprawnienia do ustanowienia w drodze aktu delegowanego przepisu technicznego w przypadku opóźnień w normalizacji. Nie rozwiąże to pewnych podstawowych kwestii prawnych związanych z cytowaniem obowiązkowych norm zharmonizowanych (np. brak tłumaczenia hEN na wszystkie języki urzędowe UE, brak cytowań lub odniesień normatywnych itp.). Wyzwaniem może również okazać się proponowane wyłączenie nielicznych wyrobów budowlanych, które są obecnie objęte normami hEN wspierającymi CPR, co może doprowadzić do braku harmonizacji na jednolitym rynku w odniesieniu do tych wyrobów.

Na uwadze należy mieć fakt, iż do czasu wejścia w życie nowego rozporządzenia wszelkie rozważania mają jedynie wymiar teoretyczny, niemniej wdrożenie nowych wymagań będzie na pewno wyzwaniem zarówno dla jednostek notyfikowanych, jak i producentów wyrobów budowlanych. ■

Marta Iwańska
Ewa Sobór
Michał Chmiel
Michał Pietrzak

securex®
POLAND
Międzynarodowe Targi Zabezpieczeń

ZAPRASZA
mtp
GRUPA

23-25 kwietnia 2024

Lokalizacja: Międzynarodowe Targi Poznańskie

NOWA ODSŁONA TARGÓW SECUREX

Hasło przewodnie:
Bezpieczna przyszłość.
Niekonwencjonalne rozwiązania w branży security.

- *premiery rynkowe i prezentacje na żywo*
- *szansa na nowe kontakty biznesowe*
- *nowatorskie eventy merytoryczne*
- *autorytety branży i najbardziej charyzmatyczne postaci*

W tym samym czasie: Poznań MediaExpo

securex.pl /TargiSecurex

URZĄDZENIA DO KONTROLI I ZAPOBIEGANIA PRZEMYTOM

Cezary Mecwaldowski

W polskich więzieniach dobre relacje funkcjonariuszy z osadzonymi traktuje się jako niewłaściwe i konsekwentnie eliminuje. Tymczasem, te dobre relacje to jeden z filarów ochrony dynamicznej, współcześnie najskuteczniejszej formy ochrony[1]. W więzieniach Norwegii, Niemczech, Portugali traktowanie osadzonych z godnością, humanitaryzmem z jednoczesnym ograniczaniem nadzoru i kontroli, przynosi niepodważalne korzyści w postaci mniejszej liczby zdarzeń i utrzymania wyższego poziomu bezpieczeństwa.

Funkcjonariusz Służby Więziennej musi posiadać wysoki poziom kultury osobistej, etyki zawodowej, rozumienia swojej roli w procesie przywracania osadzonych do społeczeństwa, swoją postawą stanowić dobry przykład dla osadzonych. Ochrona dynamiczna wymaga od kadry dużych kompetencji w zakresie umiejętności komunikacyjnych, wychowawczych, negocjacyjnych i mediacyjnych. Niestety, funkcjonariusz który posiada braki kompetencyjne, w sytuacjach konfliktowych bardzo często przyjmuje postawy konfrontacyjne, siłowe co eskaluje zdarzenia zamiast im zapobiegać.

W polskich więzieniach jednym z podstawowych przedsięwzięć ochronnych są kontrole. Przeprowadza się następujące rodzaje kontroli[2]:

- osobistą lub pobieżną osadzonego;
- cel i innych pomieszczeń w oddziałach mieszkalnych;
- pomieszczeń poza oddziałami mieszkalnymi;
- paczek i przedmiotów
- pojazdów;
- generalną.

Ponadto, przy wejściu do jednostki penitencjarnej realizowane są następujące kontrole[3]:

- legitymowania w celu ustalenia tożsamości;
- sprawdzenia pojazdów;
- przy pomocy urządzeń technicznych lub psa specjalnego – odzieży i ubrania osób ubiegających się o wstęp oraz przeglądania zawartości ich bagaży i innych przedmiotów, które posiadają;
- manualnej – odzieży i ubrania osób ubiegających się o wstęp oraz przeglądania zawartości ich bagaży i innych przedmiotów, które posiadają;
- osobistej – osób ubiegających się o wstęp.

[1] C. Mecwaldowski, R. Poklek, „Technika w ochronie dynamicznej obiektu na przykładzie systemu penitencjarnego", OiB 2/2020

[2] Rozporządzenie Ministra Sprawiedliwości z dnia 17 października 2016 r. w sprawie sposobów ochrony jednostek organizacyjnych Służby Więziennej, § 67.

[3] Rozporządzenie Rady Ministrów z dnia 23 grudnia 2019 r. w sprawie szczegółowego trybu działań funkcjonariuszy Służby Więziennej podczas wykonywania czynności służbowych

Zdj. 1. Przykłady ręcznych wykrywaczy metali
Źródło: materiały własne autora.

Każda z wymienionych powyżej kontroli realizowana jest wg procedur i praktyki penitencjarno-ochronnej. Część kontroli realizowanych w polskich więzieniach jest obligatoryjna a część fakultatywna. Ta fakultatywność kontroli, pozwala na jej nadmiarowe stosowanie, co przekłada się na zniechęcenie i rutynę kadry. Ponadto, kiedy wystąpi zdarzenie, to funkcjonariusz z pierwszej linii (bezpośredniego kontaktu z osadzonym) ponosi konsekwencje w postaci odpowiedzialności dyscyplinarnej lub karnej.

Do wymienionych wyżej kontroli mogą być wykorzystane następujące, przykładowe urządzenia:

- Ręczne wykrywacze metali;
- Bramkowe wykrywacze metali;
- Detektory narkotyków i materiałów wybuchowych;
- Alkomaty;
- Kamery inspekcyjne;
- Detektory telefonów komórkowych;
- Detektory elektroniki;
- Skanery rentgenowskie bagażu i przesyłek.

Ręczne wykrywacze metali – wykrywają metale żelazne i nieżelazne jak złoto, srebro, aluminium. Nie wszystkie modele służą do kontroli osób. Ze względów bezpieczeństwa, funkcjonariusz powinien wybierać detektor pozwalający na zachowanie dystansu do kontrolowanej osoby. Pozwala to dokonać kontroli osoby bez niebezpiecznego pochylania się np. do kontroli okolic obuwia. Należy okresowo sprawdzać wielkość wykrywanych przedmiotów metalowych, czy ktoś nie zmienił ustawień detekcji lub nie doszło do uszkodzenia detektora. Z reguły duże przedmioty są wykrywane, problem występuje przy mniejszych jak żyletki, nożyki od jednorazowej maszynki do golenia lub igieł. Urządzenia spełniające amerykańskie standardy produkowane są do detekcji przedmiotów metalowych zgodnych z kategoriami wielkości wykrywanych przedmiotów od MD-1 do MD-4. Niestety, dostępnych jest coraz więcej przedmiotów niedozwolonych, które nie są wykrywane przez detektory metali np. noże wykonane z ceramiki, szkła, drewna, plastiku czy włókien węglowych

i ukryte w innych przedmiotach, jak grzebienie do włosów czy klamry od pasków. Instrukcja od danego modelu detektora powinna być dołączona do instrukcji stanowiskowej tak, aby funkcjonariusz mógł zapoznać się z zasadami obsługi i możliwości kontroli osób tj. kobiet w ciąży, osób z rozrusznikiem serca, implantami słuchu czy bionicznymi kończynami[4]. Producent musi dopuszczać kontrolę takich osób z jednocześnie spełnionym warunkiem braku przeciwskazań lekarskich (brak zagrożenia życia i zdrowia osoby).

Bramkowe wykrywacze metali – wykrywają metale żelazne i nieżelazne jak złoto, srebro, aluminium. Występują one w wielu rozwiązaniach konstrukcyjnych: przenośne, stacjonarne, do zabudowy w przejściu, odporne na warunki atmosferyczne. Mogą posiadać wiele stref detekcyjnych, pozwalających na dokładną lokalizację wykrytego przedmiotu metalowego. Posiadają dodatkowe funkcjonalności jak interfejs sieciowy do zdalnych aplikacji lub integracji z systemami zabezpieczeń elektronicznych. Można wybrać modele z rozpoznawaniem kierunku ruchu osób, funkcją zliczania osób, dodatkowymi detektorami np. telefonów komórkowych, małej elektroniki, temperatury przechodzących osób czy substancji promieniotwórczych[5]. Ze względu na wiele stref i programów detekcji, natężenie pola elektromagnetycznego, urządzenia te wrażliwe są na pobliskie (do 2 m) ruchome przedmioty metalowe i zmiany pola elektromagnetycznego. Podczas instalacji należy spełnić wymagania producenta co do lokalizacji bramkowego detektora metali, odległości od wspomnianych przedmiotów i pól. Urządzenia te podczas uruchomienia dokonują adaptacji do występujących zakłóceń. W związku z częstym posiadaniem przez osoby poddawane kontroli, małych przedmiotów metalowych jak klucze, monety, zegarki, przedmioty jubilerskie, klamry od pasków przy bramkowych detektorach metali należy stosować dedykowane korytka do takich przedmiotów, wykonane z metalu stanowią ekran eliminujący detekcję tych przedmiotów w pobliżu bramki.

[4] C. Mecwaldowski, „Ręczne wykrywacze metali", OMiI 3/2016

[5] C. Mecwaldowski, „Bramkowe wykrywacze metali", OMiI 2/2016

Zdj. 2. Przykład bramkowego wykrywacza metali
Źródło: materiały własne autora.

Zdj. 3. Przykłady detektorów narkotyków i materiałów wybuchowych
Źródło: materiały własne autora.

Detektory narkotyków i materiałów wybuchowych – najczęściej chromatografy gazowe, urządzenia przenośne bądź stacjonarne, działają na zasadzie spektrometrii lotnych jonów. Urządzenia wykrywające śladowe ilości substancji. Wymagają dokonywania systematycznych pomiarów tak, aby można było stwierdzić czy nastąpił wzrost obecności substancji, utrzymanie czy spadek.

Alkomaty – urządzenia służące do pomiaru zawartości alkoholu w wydychanym powietrzu. Te prostsze pokazują wynik mieszczący się w ustalonych zakresach, a dokładniejsze często z drukarką, pozwalają na uzyskanie dokładnego pomiaru ilości promili w wydychanym powietrzu. Zasada wykonywania pomiaru polega na wykonaniu co najmniej dwukrotnego pomiaru wydmuchiwanego powietrza, drugi pomiar po 15 minutach (ma to na celu wyeliminowanie pozytywnych wyników pomiaru spowodowanych np. lekami, cukierkami z alkoholem itp.). Wymagają okresowej kalibracji, związane jest to ze skutkiem dyscyplinarnym, jaki niesie pozytywny wynik testu dla kontrolowanego osadzonego. Urządzenia pozwalające także dokonać pomiaru z otoczenia (bez wymuszonego obiegu powietrza) służą do szybkiego rozpoznawania płynów znalezionych w butelkach.

Kamery inspekcyjne – kamery te służą do kontroli przedmiotów, pomieszczeń i pojazdów. Nie wolno ich stosować do kontroli osób lub „ukrytego" monitoringu. Doskonale nadają się do kontroli kratek wentylacyjnych, kaloryferów, rur wodno-kanalizacyjnych (wodoodporne), wąskich przestrzeni za szafkami, półkami, konstrukcji sprzętu kwaterunkowego. W zależności od technologii wykonania różnią się średnicą głowicy i przewodu giętkiego[6].

[6] C. Mecwaldowski, „Kamery inspekcyjne", OMiI 5/2016

Zdj. 4. Przykłady alkomatów
Źródło: materiały własne autora.

Zdj. 5. Przykłady kamer inspekcyjnych
Źródło: materiały własne autora.

Zdj. 6. Przykłady detektorów telefonów komórkowych
Źródło: materiały własne autora.

Detektory telefonów komórkowych – Są to odbiorniki radiowe w zakresie częstotliwości i systemów komórkowych, ale także innych rodzajów komunikacji radiowej jak Wi-Fi czy Bluetooth. Często jest to skaner w szerokim zakresie częstotliwości, z anteną dookólną lub kierunkową, wbudowaną lub zewnętrzną. Umożliwiający detekcję, realizację nasłuchu sygnałów i alarmowania w czasie rzeczywistym. Paleta dostępnych urządzeń jest duża, można spotkać urządzenia: od najprostszych przypominających pager-y, umożliwiających detekcję pojedynczych systemów GSM, po profesjonalne analizatory widma i szerokopasmowe skanery częstotliwości z antenami kierunkowymi. Bywają urządzenia wbudowane w bramkowe detektory metali, przenośne, stacjonarne czy systemowe zainstalowane w obiekcie, połączone w sieć i wizualizowane w specjalnym oprogramowaniu[7]. Detektory te wykrywają włączone telefony komórkowe, które nadają sygnały np. techniczne do stacji BTS, wysyłanie SMS i MMS, rozmowę telefoniczną lub sygnały Wi-Fi i Bluetooth. Coraz trudniej stosować proste metody detekcji telefonów komórkowych, ponieważ Służba Więzienna korzysta z innych urządzeń pracujących w zakresie częstotliwości detektorów np. radiowe liczniki ciepła, energii, kamery inspekcyjne z bezprzewodowymi ekranami, tablety do podpisu elektronicznego, radiotelefony z modułami Wi-Fi i Bluetooth, kuchenki mikrofalowe itp.

Detektory elektroniki – do takich urządzeń zaliczane są detektory złącz nieliniowych (ang. non-linear junction detectors – NLJD). Służą one do detekcji elektroniki zawierającej półprzewodniki. Pozwalają na wykrycie przedmiotów zawierających elektronikę już od wielkości 1 cm^2, zarówno elektroniki aktywnej – włączonej/zasilanej jak i pasywnej – wyłączonej lub nieposiadającej zasilania[8].

Mogą być stosowane do detekcji ukrytej elektroniki w: pomieszczeniach, ich ścianach, sufitach oraz podłogach, meblach, przedmiotach (np. półkach, odzieży), przesyłkach i paczkach, samochodach oraz ich ładunkach, innych miejscach, przedmiotach i obszarach.

Detektory elektroniki umożliwiają wykrycie: wszelkiej elektroniki zawierającej półprzewodniki, telefonów komórkowych (włączonych, jak i wyłączonych), kart SIM, nośników danych jak pendrive, kart pamięci, ukrytych kamer, podsłuchów, dyktafonów, rejestratorów video itp.

Ze względu na zastosowanie mikrofal dużej mocy, anten tych urządzeń nie wolno kierować w stronę osób (poza rozwiązaniami dedykowanymi do kontroli osób np. bramek zdj. 7).

[7] C. Mecwaldowski, „Detektory telefonów komórkowych", OMiI 3/2015

[8] C. Mecwaldowski, „Detektory elektroniki NLJD", OMiI 6/2016

Zdj. 7. Przykłady detektorów elektroniki
Źródło: materiały własne autora.

Skanery rentgenowskie bagażu i przesyłek – poprzez emisję i przenikanie promieniowania rentgenowskiego przez przedmioty, pozwalają zidentyfikować kontrabandę. Obecnie jedno z najnowszych rozwiązań to skanery X-Ray dające obraz 3D tzw. MVCTC (Multi-View and Computed Tomography Capable). Stosowanie urządzeń wytwarzających promieniowanie jonizujące usankcjonowane jest przepisami ustawy prawo atomowe[9] i wymaga zezwolenia wydawanego przez prezesa Państwowej Agencji Atomistyki (PAA). Szczegółowe regulacje określają: wydanie zezwolenia, zasady stosowania, wymagane prawem pomiary dozymetryczne, procedury eksploatacyjne, wymagane dokumentacje i zasady kontroli[10]. Uruchomienie jak i naprawy skanera rentgenowskiego dokonuje firma posiadająca stosowne zezwolenie PAA. Funkcjonariusze przystępując do pracy z tymi urządzeniami muszą zostać skierowani do lekarza medycyny pracy, z zamieszczoną informacją na skierowaniu o pracy z urządzeniem wytwarzającym promieniowanie jonizacyjne. Ponadto muszą ukończyć szkolenie z ochrony radiologicznej i obsługi danego modelu urządzenia. Coraz nowocześniejsze techniki obrazowania pozwalają uzyskiwać wysoką rozdzielczość obrazów z funkcją rozpoznawania przedmiotów i substancji. Doskonale nadają się do rozpoznawania elektroniki, przedmiotów z ceramiki i wielu innych. Należy prowadzić kwartalną dozymetrię z protokołami z pomiarów, za pomocą dozymetrów indywidualnych, środowiskowych (miejsca pracy) lub pomiary realizowane przez uprawnioną osobę (inspektora ochrony radiologicznej).

Poza przywołanymi wyżej urządzeniami, do realizacji kontroli w więzieniach stosuje się także:

- Chemiczne testy substancji psychoaktywnych;
- Młotki drewniane, gumowe, stalowe do kontroli zabezpieczeń mechanicznych;
- Pręty do kontroli załadunku pojazdu;
  Lustra inspekcyjne;
- Psy specjalne wykrywające narkotyki i materiały wybuchowe.

Aby uniknąć konfliktów lub niepotrzebnych czynności wykonywanych przez funkcjonariuszy, przed wejściem do jednostki penitencjarnej, na tablicy informacyjnej (a także na stronie www jednostki) powinny być zamieszczone informacje o stosowanych urządzeniach do kontroli oraz psach specjalnych.

Funkcjonariusz wyposażony w urządzenia mechaniczne lub elektroniczne ma obowiązek wykorzystywania ich do kontroli[11]. Obowiązujące przepisy nie różnicują urządzeń i narzędzi oraz nie dają funkcjonariuszowi możliwości decydowania o ich zastosowaniu lub niezastosowaniu. Co było jedną z przyczyn wstrzymania przez Służbę Więzienną kontroli osób za pomocą alkomatu przy wejściu do jednostki penitencjarnej.

Każdy funkcjonariusz posługujący się urządzeniami do kontroli powinien zostać zapoznany z instrukcją danego urządzenia, zasadami realizacji kontroli, odstępstwami oraz zasadami BHP. Niestety, systematycznie skracane szkolenia zawodowe oraz specjalistyczne nie sprzyjają przygotowaniu kadry do realizacji zadań.

Zdj. 8. Przykład skanera rentgenowskiego do bagażu i przesyłek
Źródło: materiały własne autora.

Podział kompetencji i odpowiedzialności w stosowaniu urządzeń do kontroli:

- Funkcjonariusz i pracownik, jako użytkownik: eksploatacja bieżąca – dbanie o dobry stan urządzenia, czyszczenie w ramach bieżącej obsługi, wizualne sprawdzenie stanu przy każdorazowym użyciu oraz informowanie przełożonych w przypadku stwierdzenia nieprawidłowości w funkcjonowaniu lub widocznych uszkodzeń;
- Funkcjonariusz i pracownik, jako przełożony/kierownik ochrony: odpowiedzialność za prawidłowy dobór urządzeń do wykonywanych zadań, założenia konfiguracyjne i ustawienia urządzeń, kontrola prawidłowości ich wykorzystania, zapewnienie szkoleń użytkownikom;
- Funkcjonariusz i pracownik obsługi technicznej/administrator systemów: przeglądy kresowe, naprawy i wysyłka do serwisu, czyszczenie w ramach przeglądu okresowego w zakresie niemożliwym do zrealizowania przez użytkownika, konfiguracja i ustawienia urządzeń zgodnie z zaleceniami kierownika ochrony, realizacja szkoleń użytkowników.

Właściwie wyszkolony funkcjonariusz wyposażony jest w kompetencje i umiejętności niezbędne do skutecznej realizacji zadań. Z kolei brak wiedzy o zasadach działania, metodach detekcji, słabych i mocnych stronach urządzeń do kontroli, jest przyczyną udanych przemytów kontrabandy na teren zakładów karnych i związanych z nią innych zdarzeń. Mimo prób, w polskich więzieniach, nie udało się wdrożyć zasad ochrony dynamicznej. Wymaga to przede wszystkim zmiany relacji funkcjonariusz-osadzony. To w efekcie skutecznie realizowanej ochrony dynamicznej uzyskuje się zmniejszenie nadzoru i liczby kontroli, przy jednoczesnym zwiększeniu poziomu bezpieczeństwa jednostki penitencjarnej (zmniejszenie liczby zdarzeń). ■

[9] Ustawa Prawo Atomowe z 29 listopada 2000 r.

[10] C. Mecwaldowski, „Skanery XRay i MMW", OMiI 4/2016

[11] Rozporządzenie Ministra Sprawiedliwości z dnia 17 października 2016 r. w sprawie sposobów ochrony jednostek organizacyjnych Służby Więziennej. § 41. Funkcjonariusz (…) pkt. 2 wyposażony w urządzenia mechaniczne lub elektroniczne ma obowiązek wykorzystywania ich do kontroli, o których mowa w § 67

mjr mgr inż. Cezary Mecwaldowski
Komendant Centralnego Ośrodka Szkolenia Służby Więziennej w Kulach. Wykładowca Ośrodka Szkolenia Polskiej Izby Systemów Alarmowych. Ekspert think tanku ObserwatoriumBezpieczeństwa.pl

INTEGRACJA SYSTEMÓW PSIM I SMS

PSIM to skrót od angielskiej nazwy Physical Security Information Managment i dotyczy platformy umożliwiającej kompleksowe zarządzanie wszystkimi systemami zainstalowanymi w danym obiekcie lub na danym terenie. Oprogramowanie klasy PSIM pozwala na jednoczesne zarządzanie tak zróżnicowanymi systemami jak systemy bezpieczeństwa, łączności, transportu czy automatyki budynkowej. Natomiast platforma SMS (Security Managment System) umożliwia zarządzanie tylko systemami bezpieczeństwa. Zatem za jej pomocą możemy zarządzać np. systemami CCTV, PPOŻ, Kontroli Dostępu, Systemami Sygnalizacji Włamania i Napadu itp. Systemy SMS instaluje się aby umożliwić zarządzanie bezpieczeństwem obiektu z jednego miejsca i z poziomu jednej aplikacji.

Robert Gabrysiak

Obecnie nadzór i sterowanie systemami różnych producentów z aplikacji jednego, konkretnego producenta nie jest możliwe. Dlatego właśnie powstały systemy SMS pozwalające scentralizować zarządzanie i nadzór na poziomie jednej aplikacji a wspólny interfejs oraz możliwość powiązania różnych systemów pozwala na uzyskanie wysokiego poziomu bezpieczeństwa obiektu. Systemy SMS nie pozwalają na „ukrywanie" usterek w poszczególnych systemach bezpieczeństwa. Przykładowo system SMS nie pozwoli na wprowadzenie blokady na niesprawnych elementach tym samym nie pozwoli np. zablokować czujek PPOŻ, które aktualnie są niesprawne i zakłócają prace systemu PPOŻ. Dzięki temu obsługa systemu PPOŻ zmuszona jest wymienić taką czujkę na nową i przywrócić tym samym system PPOŻ do pełnej sprawności. Oczywiście mniejsze znaczenie miałoby to w przypadku awarii elementów systemu np. kontroli dostępu jednakże w przypadku kluczowych systemów mających bezpośredni wpływ na nasze bezpieczeństwo ta cecha systemów SMS jest bardzo potrzebna i pożądana. Zamiast wielu systemów działających obok siebie, są one teraz zintegrowane w jednym centralnym rozwiązaniu. W ten sposób codzienna obsługa systemów bezpieczeństwa staje się jasnym i spójnym zadaniem dla operatorów ochrony. Muszą teraz tylko nauczyć się obsługi SMS-a zamiast wielu różnych aplikacji, które często znajdują się w centrum kontroli bezpieczeństwa. Jednym słowem, SMS umożliwia centralne zarządzanie systemami bezpieczeństwa, zwiększenie poziomu bezpieczeństwa i świadomości sytuacyjnej, zapewniając jednocześnie lepszy sposób oceny zagrożeń bezpieczeństwa. Zaletą systemów SMS, o której nie zawsze się pamięta, są niższe koszty szkolenia operatorów systemu, którzy muszą nauczyć się obsługiwać tylko SMS'a a nie kilku systemów składowych.

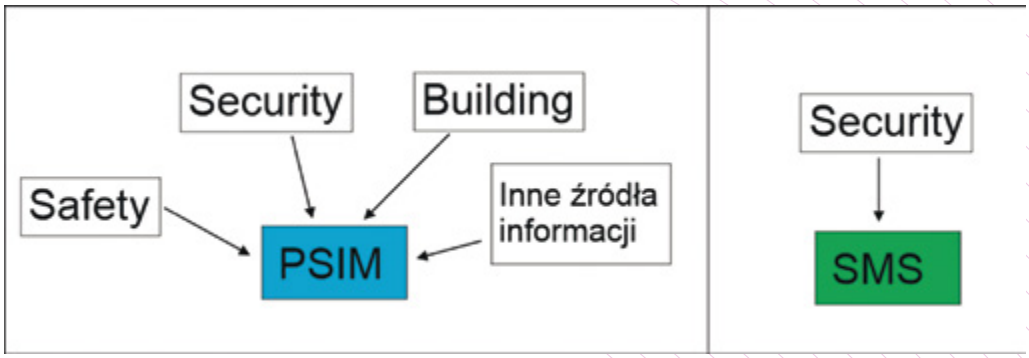
Integracja danych z wielu źródeł sprawia, że systemy stają się inteligentniejsze, a tym samym bardziej efektywne. SMS ma jednak pewne ograniczenia, dlatego też powstała platforma PSIM, która okazuje się zdecydowanie bardziej skuteczna dla obiektów z wieloma złożonymi systemami.

Platforma oprogramowania PSIM to platforma, która integruje wszystkie systemy związane z bezpieczeństwem budynku lub obszaru wielostanowiskowego w jednym, intuicyjnym interfejsie. Podobnie jest z SMS-em. Ale tam, gdzie SMS jest w większości zdolny jedynie do integracji systemów bezpieczeństwa i alarmów, platforma PSIM może pójść znacznie dalej łącząc ze sobą nie tylko systemy bezpieczeństwa ale także inne systemy budynkowe. Takie zintegrowanie wszystkich systemów za pomocą platformy PSIM ma na celu obniżyć koszty oraz poprawić wydajność i bezpieczeństwo. Zastosowanie integracji systemów za pomocą platformy PSIM zapewnia:

- nieprzerwane działanie systemów różnych producentów lub integratorów,
- wysoki poziom bezpieczeństwa we wszystkich obiektach,
- możliwość pracy w rozległej i różnorodnej strukturze,
- czytelny i intuicyjny graficzny interfejs użytkownika.

Można powiedzieć, że system PSIM jest tzw. hipernadzorcą budynku – czyli jest systemem nadrzędnym nad wszystkimi innymi systemami. PSIM jako hipernadzorca łączy i zarządza wszystkimi systemami w budynku, podczas gdy nadzorca zarządza tylko określonym systemem – czyli tak naprawdę fragmentem całego systemu PSIM. Przykładowym

Różnice pomiędzy systemami SMS i PSIM trafnie obrazują poniższe rysunki oraz tabela



Cecha	PSIM	SMS
Wspólny interfejs	TAK	TAK
Możliwość integracji	Nielimitowana	Tylko systemy ochrony
Niezależność od producenta systemu	Wysoka	Wysoka
Zarządzanie i kontrola	TAK	Głównie monitoring
Konfiguracja	Skomplikowana	Stosunkowo prosta
Obsługa incydentów	Bardzo wysoka	Niska
Świadomość sytuacyjna	Bardzo wysoka	Średnia/Niska
Kontrola ryzyka	Bardzo wysoka	Średnia

nadzorcą może być system zarządzający tylko kontrolą dostępu czy systemami CCTV.

Dziś szybkie i skuteczne lokalizowanie i rozwiązywanie problemów powstałych w budynku ma niezwykle duże znaczenie. Operatorzy PSIM mogą skutecznie podejmować działania w przypadku wyzwolenia alarmu w dowolnym podsystemie – jak np. CCTV czy wykrycia pożaru. Ponadto operatorzy mogą generować raporty w celu oceny wydajności podsystemów oraz tworzyć szczegółowe statystyki zdarzeń.

Korzystanie z oprogramowania PSIM wymaga zaangażowania wielu podmiotów, którzy odgrywają kluczową rolę w zapewnieniu sukcesu platformy. Każdy z nich ma do odegrania określoną rolę w zarządzaniu systemami budynkowymi i ich optymalizacji, a ich współpraca jest niezbędna do osiągnięcia pełnego potencjału oprogramowania PSIM. Głównym celem oprogramowania PSIM jest operator, który będzie codziennie korzystał z platformy. Interfejs powinien być atrakcyjny, przejrzysty i intuicyjny. Jeśli operator musi wyszukać określone przyciski w sytuacji kryzysowej, oznacza to, że oprogramowanie PSIM nie wykonuje poprawnie swojej pracy. Każda platforma PSIM powinna być w stanie zapewnić narzędzie do zarządzania dla menedżerów ds. bezpieczeństwa.

Do podstawowych korzyści wynikających ze stosowania platformy PSIM należą:

- możliwość kontroli ryzyka – polega to na szybkim wykrywaniu i obsłudze alarmów i zdarzeń zgodnie ze zdefiniowanym przepływem pracy,
- redukcja kosztów – poprzez ograniczenie kosztów ochrony, których zdecydowaną większość pochłaniała dotychczas stała obecność w obiektach wyspecjalizowanych pracowników ochrony,
- zwiększenie świadomości sytuacyjnej u operatorów systemu – operatorzy są uruchamiani za pomocą powiadomień, błysków i dźwięków. Korzystając z predefiniowanego przepływu pracy, mogą szybko obsłużyć wszystkie alarmy i zdarzenia,
- skalowalność systemu – system PSIM może rozwijać się zgodnie z oczekiwaniami i możliwościami budżetowymi jednostki. Skalowalność systemu PSIM pozwala rozbudować go później o kolejne systemy lub obszary do zabezpieczenia.

Systemy klasy PSIM znalazły zastosowanie również w obiektach infrastruktury krytycznej. W więzieniach, elektrowniach gazowych, wiatrowych czy farmach fotowoltaicznych wymagane są najwyższej jakości systemy podnoszące efektywność procesów, dające wysoki poziom bezpieczeństwa, umożliwiające natychmiastową reakcję w sytuacjach awaryjnych oraz dostarczające jednoznaczne informacje pozwalające ocenić sytuację o zagrożeniu – a takie właśnie są systemy klasy PSIM. ■

Robert Gabrysiak

OCHRONA i BEZPIECZEŃSTWO OBIEKTÓW I BIZNESU
www.ochrona-bezpieczenstwo.pl

Czasopismo z branży ochrony pełni rolę doradczą, informacyjną, publicystyczną, propagującą wiedzę w obszarze ochrony i bezpieczeństwa obiektów oraz biznesu.

PRENUMERATA

Dział prenumeraty

Tel. kom. +48 535 085 030
prenumerata@mediafachowe.pl

Zamówienie prenumeraty przyjmujemy

- Telefonicznie **+48 535 085 030**
- e-mailem **prenumerata@euro-media.pl**

Prenumerata

Roczna	**69 zł**
Roczna studencka	**50 zł**

Prenumerata dostępna także przez

- **RUCH S.A.**
- **Kolporter Sp. z o.o. S.K.A.**
- **Garmond Press S.A.**
- **G.L.M. Sp. z o.o.**
- **AS Press Andrzej Szlachciuk**

Wejdź na nasz profil i polub nas!

Lubię to!

www.facebook.com/**ochronaibezpieczenstwo**

KONTAKT

Wydawca

Euro-Media sp. z o. o.
ul. Wąski Jar 9
02-786 Warszawa

Prezes zarządu: **Katarzyna Polesińska**

Redakcja:

ul. Wąski Jar 9, 02-786 Warszawa
redakcja@ochrona-bezpieczenstwo.pl
www.ochrona-bezpieczenstwo.pl

Sergiusz Parszowski
Redaktor programowy

redakcja@ochrona-bezpieczenstwo.pl
tel. +48 737 393 280

Lidia Tuchowska
Redaktor/Marketing i PR

tel. 604 995 466
l.tuchowska@ochrona-bezpieczenstwo.pl

Katarzyna Kalata-Kieblesz
Kierownik Działu Reklamy

tel. 604 588 851
k.kalata@ochrona-bezpieczenstwo.pl

Stała współpraca:
Jerzy Ciszewski, Urszula Garlińska, Mateusz Gosk, Sebastian Hładun, Dariusz Knapek, Waldemar Kubik, Marek Kustra, Krzysztof Łangowski, Paweł Łuszcz, Dobrosław Mąka, Cezary Mecwaldowski, Krzysztof Młudzik, Radosław Monia, Sergiusz Parszowski, Michał Pietrzak, Robert Poklek, Adam Radomyski, Janusz Sawicki, Jakub Sobek, Tomasz Sowa, Stanisław Sulenta, Jerzy Taczalski, Norbert Tuśnio, Damian Żabicki, Małgorzata Żmigrodzka.

Zdjęcia: zespół redakcyjny, materiały promocyjne, www.stock.adobe.com/pl/

Łamanie i opracowanie graficzne: WAŻKA Łukasz Piotrowski

SPIN 2024 extra.

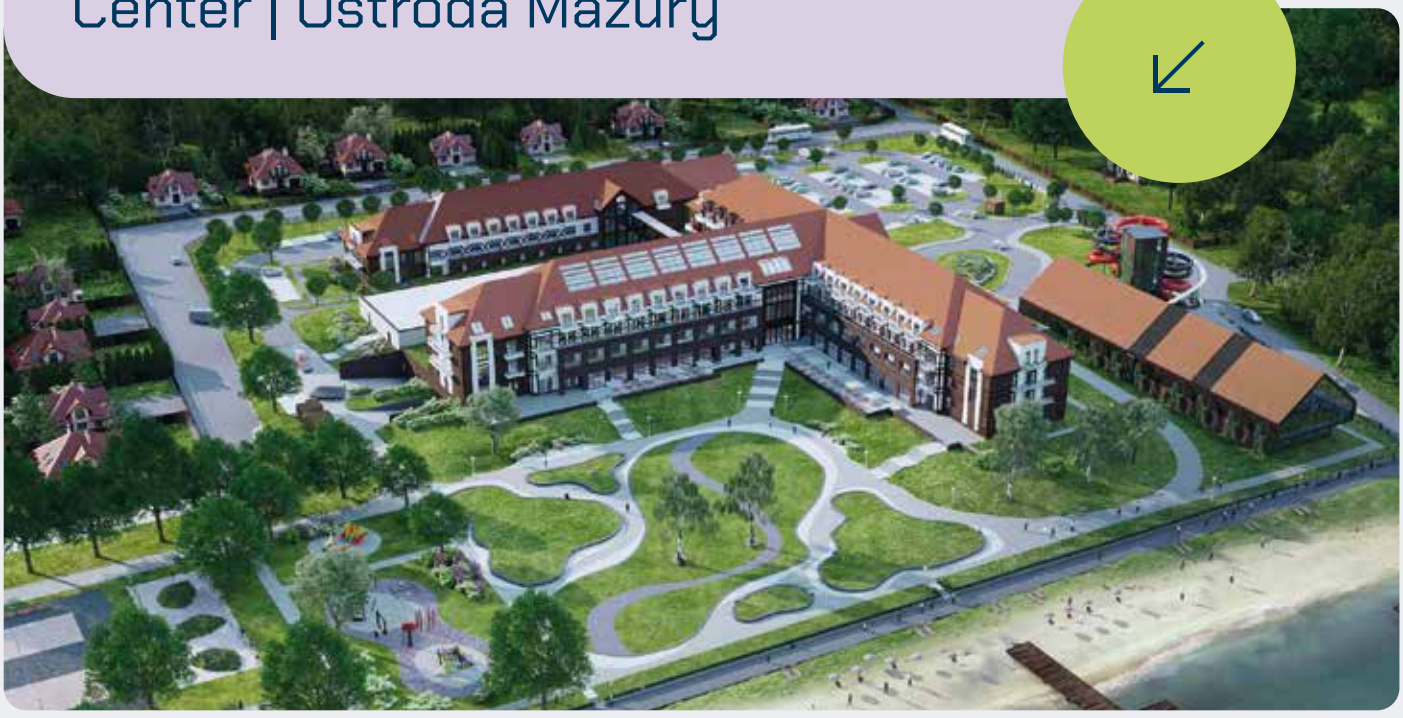
spin.lockus.pl ↗

SPOTKANIE PROJEKTANTÓW INSTALACJI NISKOPRĄDOWYCH.

EDYCJA WIOSENNA

21 – 22 marca 2024

Radisson Blu Resort & Conference Center | Ostróda Mazury



Nowa seria sygnalizatorów pożarowych P8

PRODUCENT SYGNALIZATORÓW I OSPRZĘTU INSTALACYJNEGO

SO-P8 (optyczny)

- Występuje w 6 odmianach
- Dokumenty CNBOP-PIB
- Funkcja synchronizacji
- Ogranicznik prądu rozruchowego
- Obudowa o wytrzymałości mechanicznej IK07
- Do stosowania na zewnątrz budynków (Typ B)
- Możliwość wyboru 1 z 4 częstotliwości błysków
- Możliwość wyboru 1 z 4 brył optycznych (3, 6, 9, 12m) w jednym urządzeniu

SA-P8 (akustyczny)

- Występuje w obudowie białej lub czerwonej
- Dokumenty CNBOP-PIB
- Funkcja synchronizacji
- Ogranicznik prądu rozruchowego
- Obudowa o wytrzymałości mechanicznej IK07
- 16 wzorów dźwięku
- Potencjometr regulacji poziomu dźwięku
- Opcja stopniowego narastania poziomu dźwięku

SAO-P8 (akustyczno-optyczny)

- Występuje w 6 odmianach
- Dokumenty CNBOP-PIB
- Funkcja synchronizacji
- Ogranicznik prądu rozruchowego
- Obudowa o wytrzymałości mechanicznej IK07
- 16 wzorów dźwięku
- Potencjometr regulacji poziomu dźwięku
- Opcja stopniowego narastania poziomu dźwięku
- Możliwość wyboru 1 z 4 brył optycznych (3, 6, 9, 12m) w jednym urządzeniu

W2 Poland sp. z o.o., ul. Ceramiczna 1A, 86-005 Kruszyn Krajeński
tel. +48 52 522 32 38, www.w2.com.pl, NIP: 5543009367