SYSTEMY VMS,

czyli jak podnieść bezpieczeństwo obiektu na najwyższy poziom z wykorzystaniem najnowocześniejszych technologii

System monitoringu wizyjnego pełni kluczową rolę w zapewnieniu bezpieczeństwa osadzonych, pracowników oraz integralności obiektów penitencjarnych. Ze względu na uwarunkowania finansowe, rozwój systemów bezpieczeństwa na przestrzeni lat skutkuje tym, że kolejne elementy, takie jak kamery, rejestratory, enkodery są dokładane sukcesywnie. W związku z tym produkty często różnią się między sobą marką, czy technologią (IP, analog AHD itp.). Różnice funkcjonalności tych produktów wywołują brak optymalizacji zarządzania całym systemem. Administratorzy tracą wiele czasu z powodu uciążliwego i problematycznego zarządzenia, utrzymania i serwisowania produktów pochodzących z wielu źródeł. Natomiast operator ma zaburzony komfort pracy, co bezpośrednio wpływa na poziom bezpieczeństwa osób, czy mienia.

Jak zatem rozwiązać problem, który dotyczy wielu jednostek penitencjarnych?

Wykorzystując nowoczesny system zarządzania wideo VMS otwarty na produkty pochodzące od różnych producentów np. kamery z wykorzystaniem protokołów producenckich, w celu uzyskania kompletnej integracji i wykorzystania wszystkich możliwości produktów. Dzięki temu, pomimo funkcjonowania w obiekcie urządzeń różnych marek, operator oraz administrator zarządzają system wykorzystując jeden spójny, wygodny interfejs.

Jakie cechy powinien zatem posiadać interfejs?

- **Intuicyjność** – powinien działać niemal wyłącznie z wykorzystaniem myszy, zapewniając sprawne poruszanie się w systemie np. umożliwiać uzyskanie obrazu z dowolnego punktu obiektu bez konieczności znajomości nazw kamer, czy skomplikowanego menu.
- **Adaptację do preferencji każdego z operatorów** – każdy indywidualny, zalogowany użytkownik otrzymuje indywidualnie dostosowany układ widoków, który zapewni mu szybki i wygodny sposób działania.
- **Możliwość kooperacji i eskalacji informacji między poszczególnymi operatorami** poprzez wykorzystanie funkcji wideowall oraz opcję dodawania komentarzy do zdarzeń.
- **Możliwość blokowania przed nadpisaniem** materiału wideo w przypadku ważnych zdarzeń.
- **Możliwość zarządzania parametrami kamer** np. strumieniami;
- **Zapewnianie anonimizacji wizerunku osób** np. przy eksporcie materiału video.
- **Możliwość implementowania analizy obrazu** na serwerze dla każdej z kamer, mimo iż kamery analogowe czy starsze IP nie mają jej wbudowanej.
- **Możliwość wykonywania analizy obrazu wstecz** na nagranym już materiale w celu szybkiego odnalezienie zdarzeń.
- **Głęboką i sprawdzoną integrację z systemami nadrzędnymi**, takimi jak system zarządzania bezpieczeństwem (SMS), oprogramowanie do zarządzania bezpieczeństwem fizycznym PSIM, a także popularnymi systemami SSWiN, czy systemami ochrony obwodowej.

Każdy nowoczesny system VMS musi zapewniać także wielopoziomowe bezpieczeństwo i gwarancję zapisu danych w tak newralgicznych obiektach, jakimi są obiekty penitencjarne. Taki cel jest możliwy do osiągnięcia dzięki wykorzystaniu tzw. serwerów redundantnych / Failover 1:1 czy 1:wielu, niezawodnych komponentów, czy modułów odroczonej kopii materiału wideo. Nowoczesny VMS powinien umożliwiać także implementację na serwerach renomowanych marek z usługami serwisowymi tzw. next bussines day, czyli dostawę uszkodzonego komponentu w czasie 24 godzin. Ważne, żeby posiadał możliwość wykorzystania platform wirtualizacyjnych, takich jak VMWare czy Hyper-V oraz pełen pakiet redundancji zapewniany przez te środowiska. Takie rozwiązania nie są możliwe w przypadku klasycznych rozwiązań rejestratorowych.

W dzisiejszych czasach zagrożenie bezpieczeństwa cyfrowego jest coraz większe, dlatego system musi zapewniać cały pakiet ochrony w tym zakresie. Należy zatem stosować pomiędzy elementami systemu rozwiązanie szyfrowania komunikacji na poziomie AES 256, szyfrowanie plików konfiguracji, czy autoryzację lub podwójne potwierdzenie logowania na zasadzie „two-person rule".

W jaki sposób sprawdzać jakość produktu w mnogości dostępnych rozwiązań na rynku?

Należy wymagać przedstawiania certyfikatów potwierdzających jakość np. Grade 3 (3 stopień zabezpieczenia) dla systemu VMS wg normy PN-EN-62676-1-1 2014-06, czy też uczestnictwa producentów w kluczowych stowarzyszeniach standaryzujących, jak np. Onvif na poziomie pełnego członkostwa.

Pełna świadomość niezbędnych wymagań w stosunku do niezawodnego i optymalnego rozwiązania pozwoliła nam stworzyć i dopracować na przestrzeni lat system VMS VDG Sense od TKH Security. Jest to sprawdzone rozwiązanie w obiektach i systemach wymagających najwyższego poziomu bezpieczeństwa, takich jak systemy ochrony granic, lotnisk, zakładów penitencjarnych na całym świecie.

mgr inż. Tomasz Smoczyk
Kierownik ds. produktu w C&C Partners
t.smoczyk@ccpartners.pl
tel. +48 601 299 378

ZARZĄDZANIE KRYZYSOWE W JEDNOSTKACH SŁUŻBY WIĘZIENNEJ WPIERANE SYSTEMAMI INFORMATYCZNYMI KLASY PSIM

Zadania Służby Więziennej to m.in. utrzymanie porządku i bezpieczeństwa na terenie jednostek penitencjarnych. Z tego powodu funkcjonariusze podawani są szkoleniom, a obiekty penitencjarne wyposażane są w coraz to nowsze narzędzia i systemy usprawniające pracę funkcjonariuszy w zakresie transportu, komunikacji elektronicznej, głosowej (wewnętrznej i zewnętrznej), czy w zakresie systemów bezpieczeństwa.

Natomiast w systemie bezpieczeństwa państwa (w tym w SW), zawierają się działania polegające na podejmowaniu właściwych decyzji i koordynowaniu działań sił i środków w zakresie zarządzania kryzysowego. Z tego powodu również zarządzanie kryzysowe jest bardzo istotnym elementem systemu penitencjarnego.

W związku z tym należy zadać sobie pytanie, czy systemy informatyczne integrujące systemy bezpieczeństwa można połączyć z instrukcją ochronną jednostki organizacyjnej?

Czy wykonywanie zadań, takich jak kontrolowanie osadzonego, prześwietlenie celi, patrolowanie oraz kontrolowanie stanu zabezpieczeń techniczno-ochronnych można zlecać systemowo i archiwizować potwierdzenie wykonania tych zadań w systemie IT?

Służba Więzienna, zarządzanie kryzysowe, występujące zdarzenia

Jedną z podstaw prawnych w systemie zarządzanie kryzysowego jest *Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2007 r. Nr 89, poz. 590 z późn zm.)*. Zgodnie z art. 2 ustawy zarządzenie kryzysowe to m.in. działalność, która polega na zapobiegniu sytuacjom kryzysowym, przejmowaniu nad nimi kontroli, w końcu reagowaniu.

Dodatkowo rozporządzenie w art. 4 określa opracowywanie procedur postępowania na wypadek zagrożeń i przygotowywanie planów reagowania kryzysowego, co idealnie pokrywa się z założeniami i architekturą systemów klasy PSIM.

Na podstawie załącznika do zarządzenia Nr 1/2018 Dyrektora Generalnego Służby Więziennej z dnia 03 stycznia 2018 określa się jednoznacznie, jakie zdarzenia mogą wystąpić w Służbie Więziennej. Należą do nich m.in zakłócenie funkcjonowania jednostki, takie jak napaść na jednostkę lub konwój SW, wzięcie zakładnika, bunt, ucieczka, bójka osadzonych, czy napaść na funkcjonariusza. Obsługa tych zdarzeń wymaga każdorazowo innych sił, środków oraz procedur, które można dzisiaj wdrożyć w aplikacjach integrujących, aby usprawnić proces ich obsługi.

Czym jest PSIM i dlaczego to rozwiązanie dla Służby Więziennej?

Z definicji PSIM WinGuard to oprogramowanie do zarządzania bezpieczeństwem fizycznym (Physical Security Information Management), które integruje wiele autonomicznych systemów bezpieczeństwa, pozwalając na ich kontrolowanie za pośrednictwem jednolitego interfejsu użytkownika. WinGuard umożliwia użytkownikowi końcowemu zarządzanie zdarzeniami, które zostają wykryte przez różne systemy tworząc jednolity plan sytuacyjny (instrukcję ochroną) dla całego chronionego obszaru.

Odpowiednie wykrywanie sygnałów przez systemy lub osoby pozwala stwierdzić, czy występuje sytuacja kryzysowa. Bez identyfikacji zdarzeń nie zdajemy sobie sprawy z zaistniałej sytuacji, zatem nie możemy nią zarządzać. Dlatego ważne jest, aby posiadać zbiorczą identyfikację zdarzeń i integrować różne systemy do PSIM w celu zapewniania odpowiedniego transferu sygnałów do odpowiednich funkcjonariuszy. Sygnałami odbieranymi przez PSIM mogą być np. napaść na funkcjonariusza/wychowawcę aktywowany przyciskiem napadowym systemu SSWiN, funkcja „czaty" monitorująca aktywność oddziałowego, próba ucieczki wykryta przez system ochrony obwodowej i system kamer termowizyjnych i VCA.

W takim zintegrowanym rozwiązaniu, informacja ma możliwość najszybszego dotarcia do funkcjonariuszy.

Elektroniczna instrukcja ochronna

Rozporządzenie Ministra Sprawiedliwości z dnia 17 października 2016 r. w sprawie sposobów ochrony jednostek organizacyjnych Służby Więziennej, przewiduje opracowanie planu obrony zawierające opracowaną instrukcję ochronną jednostki organizacyjnej. Według § 13. w/w rozporządzenia instrukcja ochronna składa się z m.in. z: procedur działań ochronnych i alarmowania oraz planu sytuacyjnego, co idealnie pokrywa się z założeniami systemów PSIM.

Za pomocą aplikacji PSIM instrukcję ochrony można przenieść do cyfrowego świata rozwiązań IT, które w następstwie będą aktywnie wspierać operatora w czasie wystąpienia zdarzenia. Dzięki takiemu rozwiązaniu, możemy wielu osobom jednoznacznie zobrazować aktualną sytuację w jednostce, kontrolować ruch osadzonych, osób i pojazdów, zlecać systemowo kontrolę cel, czy bezzwłoczne informować dowódcę zmiany o zagrożeniach.

Zgodnie z § 15 w/w rozporządzenia, w planie sytuacyjnym jednostki zawiera się graficzne przedstawienie m.in. budynków i budowli, ciągów komunikacyjnych i dróg ewakuacyjnych, usytuowania wartowni, magazynu uzbrojenia, wieżyczek, pomieszczenia na sprzęt przeciwpożarowy, ujęć wody znajdujących się na zewnątrz budynków, a także głównych wyłączników prądu i gazu.

W aplikacji PSIM istnieje możliwość wizualizowania i zarządzania wszystkimi w/w elementami.

Proces inwestycyjny

System WinGuard jest rozwiązaniem nie powiązanym z żadnym producentem sprzętu, co umożliwia jego bardzo szybkie wdrożenie w istniejącej infrastrukturze serwerowej. PSIM to aplikacja skalowana, co oznacza, że system może się rozwijać zgodnie z możliwościami budżetowymi jednostki. Przykładowo w pierwszym etapie inwestycji można podłączyć do aplikacji PSIM WinGuard alarmowy system SSWiN, następnie wdrożyć w PSIM procedury obsługi zgłoszeń z przycisków napadowych. W kolejnych etapach, w dowolnym momencie można system rozszerzyć o kolejne systemy, takie jak CCTV, ochrona obwodowa, kontrola dostępu, depozytor kluczy, systemy energetyczne, komunikacyjne (telefonia VoIP, interkomy, rozgłoszenia PA, radiotelefony) oraz systemy IT (switche, UPS, serwery itp.) dowolnych producentów.

Podsumowanie

System PSIM WinGuard bez wątpienia jest rozwiązaniem przyszłościowym, z którego służby mundurowe korzystają na całym świecie. Możliwość przeniesienia procedur obowiązujących w danej jednostce do elektronicznego świata IT jest ogromnym autem zarówno dla osób zarządzających ryzkiem w jednostce, jaki i dla funkcjonariuszy obsługujących system.

WinGuard jest neutralny względem producentów systemów technicznych, co umożliwia wizualizację i kontrolę całej infrastruktury budynku.

WinGuard zapewnia skalowalność rozwiązania od autonomicznego systemu z jedną stacją roboczą, do rozproszonej instalacji z nadrzędnym centrum zarządzania bezpieczeństwem.

Prostota obsługi, możliwość samodzielnej konfiguracji zapewnia użytkownikowi wprowadzenie zmian w systemie na bieżąco. Połączenie możliwości konfiguracji PSIM z analizą i wyciąganiem wniosków z obsługi zdarzeń pozwala udoskonalać system zarządzania tym samym sprawiając, że można działać szybciej, sprawniej i bezpiecznej utrzymywać porządek i bezpieczeństwo na terenie jednostek penitencjarnych.

mgr inż. Leszek Schmidt
Kierownik działu wsparcia technicznego
w C&C Partners
l.schmidt@ccprtners.pl
tel. +48 601 299 378