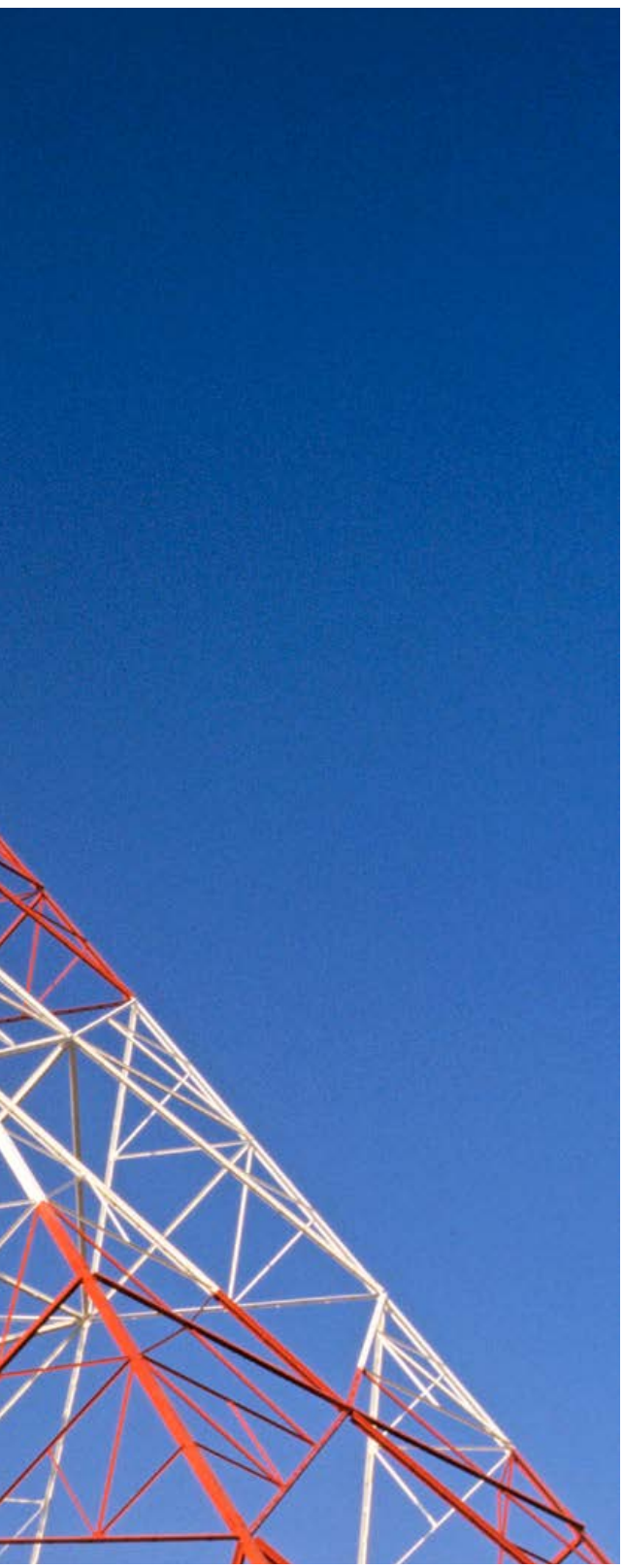
Bezpieczeństwo infrastruktury telekomunikacyjnej

Maciej Flis

Obiekty infrastrukturalne sieci telekomunikacyjnych są szczególnie narażone na niepożądane działania ze strony osób trzecich. Jednym z powodów jest oddalenie telekomunikacyjnych węzłów sieciowych od innych budynków, które znacznie zmniejsza prawdopodobieństwo zaobserwowania intruza przez osoby postronne. Istotne jest również to, że w obiektach infrastruktury sieciowej zazwyczaj nie przebywają pracownicy lokalnie monitorujący działanie systemów zabezpieczających. Ponadto znaczna wartość zainstalowanych w chronionych obiektach urządzeń telekomunikacyjnych zachęca intruzów do prób włamania. Poprawne działanie sieci telekomunikacyjnych jest jednym z warunków bezpieczeństwa narodowego, dlatego wszystkie obiekty infrastruktury telekomunikacyjnej powinny być w maksymalnym stopniu chronione przed dostępem osób nieuprawnionych

System zarządzania bezpieczeństwem obiektów rozproszonych

Rozwiązaniem gwarantującym pełne zabezpieczenie rozproszonych sieci telekomunikacyjnych jest zastosowanie zintegrowanego systemu zarządzania bezpieczeństwem iProtect. W ramach kompleksowego systemu zabezpieczeń ochronie podlegają zarówno węzły dystrybucyjne i szkieletowe, jak i centra zarządzania siecią. W poszczególnych obiektach instalowane są elementy systemów kontroli dostępu, sygnalizacji włamania i napadu, dozoru wizyjnego, sygnalizacji pożarowej oraz monitoringu środowiskowego. Platforma umożliwia również integrację innych systemów, m.in. rejestracji czasu pracy czy automatyki budynkowej. Zainstalowane w obiekcie elementy wykonawcze poszczególnych systemów komunikują się w czasie rzeczywistym z centrum zarządzania. Elementy systemu komunikują się ze sobą za pośrednictwem sieci TCP/IP. Dzięki wykorzystaniu wysokiej klasy algorytmów szyfrujących dane przesyłane w systemie zabezpieczeń przez łącza transmisyjne operatora mogą być współdzielone z innymi aplikacjami. Istotną cechą platformy jest autonomiczne działanie systemów zabezpieczeń w każdym z obiektów. W momencie przerwania połączenia między poszczególnymi węzłami sieci systemy lokalne działają autonomicznie. Po ponownym nawiązaniu połączenia z centrum zarządzania lokalne i centralne rejestry zdarzeń i praw dostępowych wzajemnie się synchronizują.



W ramach części szkieletowej i dystrybucyjnej infrastruktury sieciowej ochronie podlegają obiekty węzłowe, które mają postać zewnętrznych szaf, kontenerów czy murowanych budynków, w zależności od potrzeb i możliwości inwestora. Bogaty asortyment oferowanych przez C&C Partners systemów zabezpieczeń umożliwia zastosowanie urządzeń dopasowanych do konkretnej konstrukcji obiektu.

Efektywne zarządzanie systemami zabezpieczeń i monitoringu środowiskowego

Kluczowymi elementami instalowanymi lokalnie w każdym z obiektów są kontrolery sieciowe Apollo. Innowacyjny sterownik sieciowy Apollo, wprowadzony na rynek przez firmę Keyprocessor, umożliwia efektywne zarządzanie elementami systemów zabezpieczeń i monitoringu środowiskowego zlokalizowanymi w newralgicznych obiektach infrastrukturalnych.

Sterownik Apollo jest dostępny w wersji dostosowanej do montażu w szafie typu RACK. Dzięki kompaktowym rozmiarom (wysokość – 1U, głębokość – 22,5 cm) można go łatwo zainstalować w szafie dowolnego typu.

Sterownik Apollo umożliwia pełne zarządzanie dostępem do obiektu dzięki obsłudze dwóch czytników pracujących w systemie kontroli dostępu oraz ośmiu elementów wykonawczych (zwory, elektrozaczepy, przyciski wyjścia itp.). Sterownik ma wbudowany moduł ośmiu wejść i ośmiu wyjść umożliwiających podłączenie elementów detekcyjnych i sygnalizacyjnych pracujących w systemie sygnalizacji włamania i napadu (detektory ruchu, kontaktrony, sygnalizatory optyczno-akustyczne itp.), systemie sygnalizacji pożarowej (detektory dymu/ciepła, ręczne ostrzegacze pożarowe itp.), systemie monitoringu środowiskowego i automatyki (detektory zalania, mierniki parametrów zasilania, UPS itp.). W sterowniku Apollo znajdują się również dwa wejścia analogowe, które umożliwiają pomiar wartości parametrów środowiskowych – temperatury i wilgotności.

Wyposażony we wbudowany interfejs TCP/IP Apollo komunikuje się z centrum zarządzania poprzez sieć Ethernet. Urządzenie może być zarządzane centralnie, z poziomu platformy iProtect, i komunikować się z innymi systemami nadzorczymi z wykorzystaniem protokołu SNMP.

Fot. 1. Sterownik sieciowy Apollo umożliwia efektywne zarządzanie elementami systemów zabezpieczeń

Fot. 2. Szafa teleinformatyczna 19" z zamknięciem sterowanym przez system kontroli dostępu

W momencie utraty połączenia z systemem nadzorczym sterownik pracuje autonomicznie, zapisując w pamięci wszystkie zdarzenia zachodzące w obiekcie.

Sterownik Apollo jest przełomowym rozwiązaniem przeznaczonym do zarządzania elementami systemów zabezpieczeń i monitoringu środowiskowego w ramach jednej platformy sprzętowej. Dzięki obsłudze wielu różnych urządzeń może być elementem wyposażenia zarówno pojedynczych szaf serwerowych, jak i obiektów infrastrukturalnych rozbudowanych sieci telekomunikacyjnych.

Inteligentny monitoring wizyjny IP

Istotną rolę w weryfikacji zdarzeń alarmowych pełni system dozoru wizyjnego. W zależności od rodzaju obiektu i miejsca instalacji możliwe jest zastosowanie kamer kopułkowych, tulejowych lub obrotowych. Obraz z kamer może być zapisywany lokalnie lub centralnie, w centrum zarządzania. Idealnym rozwiązaniem do przechowywania materiałów wizyjnych i zarządzania nimi w systemach telewizji dozorowej jest platforma VMS VDG DIVA.

Kluczowym atutem współczesnych systemów dozoru wizyjnego IP jest wykorzystywanie funkcji inteligentnej analizy treści obrazu, np. w celu automatycznej detekcji pojawienia się osób w pobliżu chronionego obiektu czy wykrycia sabotażu któregoś z punktów kamerowych. Funkcja inteligentnej analizy treści obrazu zwiększa efektywność i ergonomię pracy operatorów, zarazem optymalizując wymagane pasmo potrzebne do przesyłu strumieni wizyjnych. Wykorzystanie funkcji analizy treści obrazu sprawia, że operator reaguje na zdarzenia z zachowaniem najwyższego poziomu skupienia.

W zabezpieczaniu sieci telekomunikacyjnych znakomicie sprawdzą się kamery z wbudowanym modułem SFP Siqura, który umożliwia podłączenie światłowodu bezpośrednio do kamery. Zapewnia to galwaniczne odseparowanie punktu kamerowego od innych elementów systemu oraz uwalnia od konieczności stosowania dodatkowych konwerterów i zasilaczy po stronie punktu kamerowego.

Komunikacja głosowa i rozgłoszeniowa

Aby serwisowanie obiektów wyniesionych było efektywne, należy zapewnić bezproblemową komunikację serwisantów z centrum nadzoru. W tym celu w poszczególnych obiektach infrastrukturalnych montuje się interkomy umożliwiające nawiązanie komunikacji z centrum zarządzania lub jakimkolwiek innym obiektem infrastrukturalnym. Nowoczesne technologie zapewniają bardzo wysoką jakość i czystość dźwięku, niezależnie od poziomu hałasu dochodzącego z otoczenia. Funkcja ciągłej kontroli stanu połączenia z interkomem zapewnia pełną dostępność urządzeń bez żadnych ograniczeń czasowych.

W ochronie obiektów wyniesionych ważna jest możliwość odtwarzania komunikatów głosowych za pomocą systemu rozgłoszeniowego. System składa się z głośnika i wzmacniacza o dużej mocy, a także z modułu interkomowego, który może być podłączony bezpośrednio do sieci TCP/IP. Osoba obsługująca stanowisko operatorskie w centrum zarządzania obserwuje dany węzeł za pomocą kamer i może zareagować prewencyjnie, emitując komunikat głosowy odstraszający potencjalnego intruza. Komunikat może być również odtwarzany automatycznie, w reakcji na zadziałanie czujki pracującej w SSWiN lub wykrycie ruchu w polu widzenia kamery.

Tworząc rozproszony, sieciowy system interkomowy z wykorzystaniem serwera centralnego, interkomu nadzorczego oraz modułów lokalnych zainstalowanych w obiektach rozproszonych, można zbudować sieć umożliwiającą połączenia głosowe w ramach wszystkich obiektów, które zostaną nią połączone. W rozproszonych systemach komunikacji głosowej doskonale sprawdzi się system interkomowy Commend.

Centrum nadzoru – serce systemu zabezpieczeń

Sercem sieci telekomunikacyjnej jest centrum zarządzania siecią. Zlokalizowane są w nim serwery centralne poszczególnych systemów oraz stacje operatorskie. Platforma iProtect umożliwia wizualizację oraz pełne zarządzanie urządzeniami zabezpieczającymi znajdującymi się w każdym z węzłów. Operator posiadający odpowiednie uprawnienia może m.in. zdalnie kontrolować przejścia przez poszczególne drzwi, włączać w dozór i wyłączać z dozoru wybrane strefy SSWiN, przeglądać obrazy z kamer czy weryfikować parametry środowiskowe. Dodatkowo administrator systemu może centralnie zmieniać konfigurację i parametry urządzeń rozproszonych, dzięki czemu nie jest wymagana ingerencja pracowników serwisu w obiektach. Dzięki scentralizowaniu systemu inwestor może znacznie obniżyć koszty obsługi i serwisu, a także skrócić czas reakcji w przypadku wystąpienia zdarzenia alarmowego.

Aby zwiększyć niezawodność systemu zabezpieczeń, platforma zapewnia pełną redundancję systemów. Dzięki temu możliwe jest stworzenie głównego i zapasowego centrum zarządzania. Jeżeli centrum główne ulegnie zniszczeniu, pełne zarządzanie systemem będzie możliwe w centrum zapasowym.

Dostarczane przez C&C Partners systemy zabezpieczeń, w tym system zarządzania bezpieczeństwem iProtect, gwarantują pełne zabezpieczenie rozproszonej infrastruktury telekomunikacyjnej. Są wykorzystywane w Polsce i za granicą, a ich wysoka jakość i niezawodność zostały potwierdzone podczas wieloletniej eksploatacji.

Maciej Flis
kierownik ds. produktu
C&C Partners
m.flis@ccpartners.pl