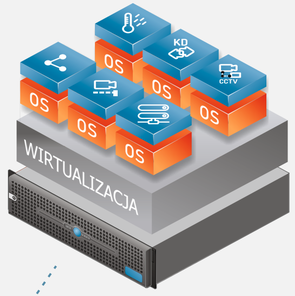
OBIEKTY ROZPROSZONE

zarządzanie komunikacją
i bezpieczeństwem

GCN Główne Centrum Nadzoru

Miejsce nadrzędne, do którego spływają wszystkie informacje z całego systemu (zarówno alarmowe, jak i serwisowe). GCN jest w stanie przejąć kontrolę nad wszystkimi podrzędnymi Lokalnymi Centrami Nadzoru.

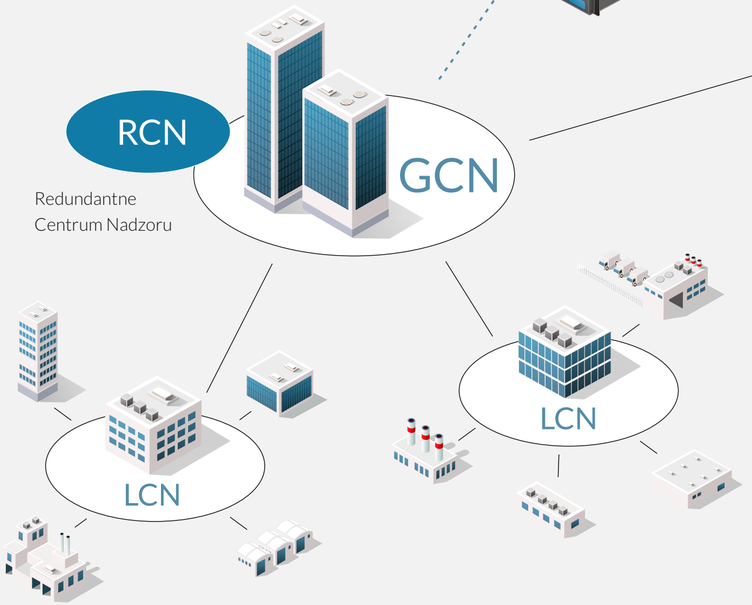


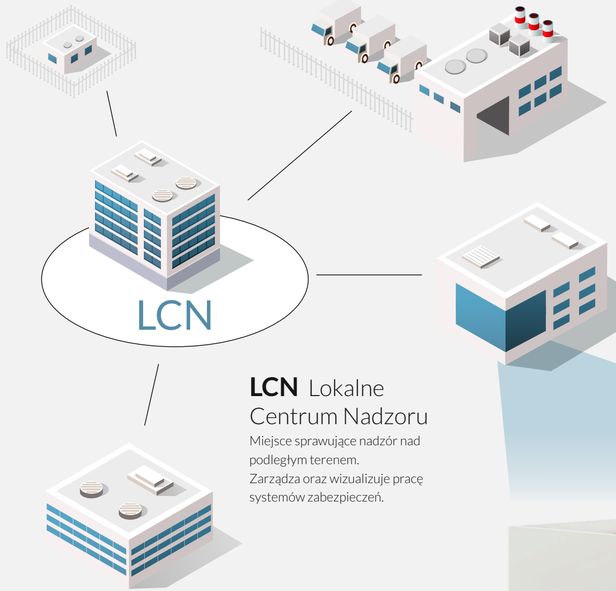
WIRTUALIZACJA

Technologia umożliwiająca działanie wielu systemów operacyjnych, w tym również systemów zabezpieczeń, na jednej odpowiednio przygotowanej do tego celu jednostce serwerowej.

Korzyści:

- możliwość wykorzystania zasobów sprzętowych inwestora
- wysoka dostępność usług świadczonych przez poszczególne systemy
- uproszczony i przyspieszony proces utrzymania systemów





LCN Lokalne Centrum Nadzoru

Miejsce sprawujące nadzór nad podległym terenem. Zarządza oraz wizualizuje pracę systemów zabezpieczeń.

TABLET / SMATRPHONE

Aplikacja zarządzająca dostępna jest zdalnie z poziomu urządzeń mobilnych

KORZYŚCI SYSTEMU

- Ułatwiona obsługa wieloobiektowych systemów za pomocą interaktywnej wizualizacji
- Obniżone koszty eksploatacji oraz serwisu zunifikowanej platformy
- Możliwość dopasowania systemu do procedur bezpieczeństwa obiektu
- RCN zapewniające ciągłość działania systemu poprzez pracę w środowisku wirtualnym
- Uniwersalny moduł raportowania zdarzeń z systemów zabezpieczeń
- Jeden moduł zarządzania alarmami dla wielu różnych podsystemów zabezpieczeń
- Automatyczne interakcje pomiędzy systemami zabezpieczeń

Zarządzanie bezpieczeństwem w OBIEKTACH ROZPROSZONYCH

1. Zarządzanie i integracja rozproszonych systemów zabezpieczeń
2. Kontrola dostępu
3. Monitoring wizyjny
4. Komunikacja interkomowa i rozgłoszeniowa PA
5. Sygnalizacja włamania
6. Rozpoznawanie tablic LPR
7. Ochrona obwodowa
8. Sygnalizacja pożaru
9. Integracja systemów zewnętrznych

1. Zarządzanie i integracja rozproszonych systemów zabezpieczeń

- monitorowanie, zarządzanie i konfiguracja różnych systemów zabezpieczeń z poziomu jednej platformy bezpieczeństwa
- aplikacja zarządzająca dostępna lokalnie i zdalnie z poziomu przeglądarki internetowej oraz urządzeń mobilnych
- wykorzystanie protokołów szyfrujących gwarantujących wysokie bezpieczeństwo przesyłanych danych
- możliwość jednoczesnego zarządzania poszczególnymi obiektami przez wielu operatorów zgodnie z uprawnieniami

2. Kontrola dostępu

- lokalna i zdalna kontrola dostępu do poszczególnych pomieszczeń lub części budynku
- dynamiczna zmiana uprawnień dostępu dla konkretnej strefy w danym okresie czasu
- monitorowanie przepływu osób i mienia wraz z systemem raportowania
- wsparcie zaawansowanych funkcjonalności (m.in. anti-passback, śluzowość, wejście pod przymusem)
- elastyczna rozbudowa systemu kontroli dostępu o kolejne pomieszczenia, czy budynki
- automatyczna obsługa gości i pracowników firm zewnętrznych

3. Monitoring wizyjny

- obserwacja obrazu wysokiej jakości „na żywo" przez pracowników ochrony
- tworzenie własnych widoków ekranowych dopasowanych do indywidualnych potrzeb i preferencji użytkownika lub operatora
- wykorzystanie algorytmów analizy obrazu (m.in. rozpoznawanie twarzy, tablic rejestracyjnych, pozostawionego przedmiotu)
- integracja kamer analogowych za pomocą wielokanałowych koderów IP
- bezpieczeństwo zapisu dzięki redundancji sprzętowej

4. Komunikacja interkomowa i rozgłoszeniowa PA

- komunikacja głosowa oraz wideo punkt-punkt, punkt-wiele punktów
- nadawanie komunikatów zbiorowych oraz indywidualnych, muzyki w tle, wzywanie lub poszukiwanie osób
- stacje interkomowe naścienne i nabiurkowe do różnych zastosowań
- terminale interkomowe dostosowane do środowiska i warunków pracy
- integracja z centralą telefoniczną, urządzeniami mobilnymi oraz systemami przyzywowymi

5. Sygnalizacja włamania

- wykrywanie intruzów za pomocą szerokiej gamy detektorów
- przesyłanie informacji o alarmie do operatora lub firmy zewnętrznej
- pełna wizualizacja statusu detektorów i stref na stanowisku ochrony
- zarządzanie z poziomu wizualizacji

6. Rozpoznawanie tablic LPR

- kontrola dostępu na terenie parkingu realizowana w oparciu o analizę tablic rejestracyjnych lub czytniki dalekiego zasięgu
- możliwość otwarcia szlabanu z poziomu wizualizacji
- komunikacja z portiernią za pomocą systemu interkomowego
- ograniczanie ilości miejsc na parkingu dla konkretnych grup użytkowników
- wyświetlanie ilości wolnych miejsc parkingowych na PYLONIE

7. Ochrona obwodowa

- pełna detekcja wtargnięć intruzów na teren wokół chronionego obiektu
- wykorzystanie barier mikrofalowych, podczerwieni oraz kabli sensorycznych
- inteligentna analiza sygnału niwelująca fałszywe alarmy przy trudnych warunkach środowiskowych
- powiązanie obrazu z kamer z poszczególną strefą systemu ochrony obwodowej

8. Sygnalizacja pożaru

- detekcja pożaru za pomocą szerokiej gamy czujek
- możliwość zastosowania systemu bezprzewodowego
- w pełni cyfrowe i indywidualnie adresowane urządzenia
- oprogramowanie wizualizacyjne w celu zapewnienia szybkiej lokalizacji zagrożenia

9. Integracja systemów zewnętrznych

- systemy zarządzania windami
- systemy zarządzania kluczami
- systemy automatyki budynkowej
- systemy kadrowo-płacowe
- systemy parkingowe

Zarządzanie bezpieczeństwem w obiektach rozproszonych na przykładzie **Politechniki Wrocławskiej**

24.000	3.000	13	8	6
użytkowników	samochodów	punktów weryfikacji	budynków	parkingów

Na terenie Politechniki Wrocławskiej został zainstalowany system zarządzania bezpieczeństwem obejmujący ochroną elektroniczną kompleks budynków oraz zarządzający uczelnianymi parkingami.

W ramach zastosowanego rozwiązania zintegrowane zostały następujące systemy: kontroli dostępu, sygnalizacji włamania i napadu, monitoringu wizyjnego, komunikacji interkomowej oraz depozytora kluczy. Ponadto została zintegrowana baza danych studentów i pracowników. System KD pozwala na kontrolę przepływu niepożądanych osób w strefach administracyjnych, bibliotecznych, archiwalnych, a także zapobiega ich przedostaniu się do miejsc newralgicznych, takich jak np. serwerownie i informatyczne punkty węzłowe. Legitymacja studencka/karta pracownicza stanowi jednocześnie kartę dostępu do różnych miejsc.

System sygnalizacji włamania i napadu aktywowany jest w godzinach nocnych, a alarmy przez niego generowane zbiegają się w jednym centrum nadzoru, gdzie podejmowane są decyzje co do dalszych kroków. System monitoringu wizyjnego weryfikuje niepożądane zdarzenia, a także wspomaga decyzje podejmowane przez pracowników ochrony obiektów. Monitoringowi podlegają miejsca newralgiczne, a także ciągi komunikacyjne i teren zewnętrzny.

Bardzo ciekawym rozwiązaniem jest włączenie do systemu bezpieczeństwa parkingów uczelnianych, które z punktu widzenia systemu stają się strefami chronionymi, a dostęp do nich następuje po weryfikacji uprawnień. Przy wjeździe na parking następuje odczyt tablicy rejestracyjnej pojazdu. Jeżeli dany numer pojazdu znajduje się w bazie i ma uprawnienia do wjazdu na parking, zostaje automatycznie wpuszczony. W przypadku zabrudzenia tablicy, bądź przyjazdu innym samochodem, użytkownik może użyć legitymacji studenckiej/pracowniczej jako karty kontroli dostępu. Kierowcy samochodów nie zarejestrowanych w bazie np. dostawy kurierskie lub goście, mogą użyć interkomu. Ochrona weryfikuje ich uprawnienia wjazdowe. Dodatkowo system ten podaje liczbę dostępnych miejsc parkingowych.
Co najważniejsze, baza systemu wymienia informacje z uczelnianą bazą studentów i pracowników, a także portalem uczelni. Nadanie uprawnień danej osobie w systemie uczelnianym automatycznie umożliwia dostęp do określonych zasobów w systemie bezpieczeństwa.

Przy tak zaprojektowanym i wykonanym systemie oraz zaimplementowanych integracjach, użytkownik uzyskuje benefity w postaci bardzo łatwego zarządzania bezpieczeństwem w obiekcie, przejrzystego i szybkiego sposobu nadawania uprawnień oraz dostępów dla poszczególnych użytkowników.