

CCTV

Dobre Praktyki w Projektowaniu CCTV

Projektowanie efektywnego systemu CCTV wymaga przemyślanego podejścia obejmującego wiele aspektów technicznych, operacyjnych i regulacyjnych. Poniżej przedstawiam kompleksowy przewodnik dotyczący najważniejszych praktyk.

Faza Planowania i Oceny Ryzyka

Zanim przystąpi się do projektowania, konieczne jest przeprowadzenie dokładnej oceny lokalizacji. Proces planowania powinien obejmować identyfikację zagrożeń, ocenę podatności i definicję konkretnych celów bezpieczeństwa. Ocena ryzyka powinna uwzględnić zagrożenia zewnętrzne (kradzież, wandalizm, sabotaż), wewnętrzne (nieupoważniony dostęp, przypadkowe uszkodzenie mienia) oraz czynniki środowiskowe (warunki pogodowe, zasilanie, temperaturę, zalesienie). Na tej podstawie należy ustalić rzeczywiste potrzeby systemu, definiując obszary pod nadzorem, cele obserwacji oraz oczekiwaną wydajność obrazu.

Kluczową część planowania stanowi przeprowadzenie analizy terenu, które powinno obejmować ocenę oświetlenia, identyfikację martwych pól, sprawdzenie tras kablowania i dostępności zasilania. Dokładna mapa terenu umożliwi zidentyfikowanie wszystkich punktów krytycznych i wąskich gardeł w projektowanym systemie.

Wybór i Umieszczenie Kamer

Lokalizacja kamer

Kamery powinny być rozmieszczane strategicznie w celu zapewnienia kompleksowego pokrycia bez martwych pól. Kluczowe obszary do monitorowania obejmują główne wejścia i wyjścia, niebezpieczne strefy, magazyny, parkingi oraz strefy wysokiej aktywności. Kamery należy umieszczać w miejscach trudnych do ominięcia, uszkodzenia lub zasłonięcia. W przypadku zdiagnozowania miejsc, za którymi zlokalizowano układy sterowania, szafy elektryczne lub potencjalnie mógłby się ktoś ukryć, należy to miejsce dodatkowo uzbroić w kamerę.

Wysokość i kąt montażu

Zalecana wysokość montażu wynosi 2,5–3 metry, co zapobiega manipulacjom i zapewnia wyraźny obraz twarzy osób wchodzących. Kamery powinny być zainstalowane pod lekkim kątem opadającym (30–40°), aby zminimalizować martwe pola bezpośrednio pod kamerą. Pozycja kamerą nie powinna być zbyt wysoka, aby zapewnić wyraźne zidentyfikowanie osób – rekomenduje się kąt umożliwiający przechwycenie zarówno zbliżającej się osoby, jak i jej twarzy.

Długość ogniskowej i pole widzenia

Wybór odpowiedniej długości ogniskowej obiektywu jest kluczowy dla efektywności systemu. Krótkie ogniskowe (około 2 mm) zapewniają szerokie pole widzenia (około 101°), idealne do monitorowania dużych przestrzeni na odległości około 6 metrów. Średnie ogniskowe (2,8–6 mm) oferują zbalansowany stosunek między zakresem a szczegółami, nadając się do pomieszczeń biurowych i wejść. Długie ogniskowe (12 mm i więcej) pozwalają na obserwację szczegółów na większych odległościach, ale zawężają pole widzenia – idealne do monitorowania specyficznych punktów wejściowych.

Stopień zjawiska optycznego i pokrycie

W miarę możliwości kamery powinny mieć nakładające/zachodzące się pola widzenia, zapewniające ciągłe monitorowanie obszarów krytycznych i umożliwiające obserwację z różnych perspektyw. Należy zastosować kamery szerokokątne, które zapewniają duże pokrycie i bardzo dobrą jakość obraz z moto- albo auto- zoomem (kopułkowe, tubowe lub obrotowe PTZ z zależności od lokalizacji).

Rozdzielczość i Jakość Obrazu

Minimalna zalecana rozdzielczość to Full HD 1080p (1920×1080 pikseli), która stanowi standard dla większości instalacji biurowych. Dla większych przestrzeni lub aplikacji wymagających identyfikacji szczegółów (np. parkingi, place opałowe, hale kottów i maszyn) zaleca się rozdzielczość 4MP (2560×1440) lub wyższą.

Wybór rozdzielczości bezpośrednio wpływa na wymagania dotyczące przechowywania i przepustowości. Kamery 4K zużywają około 2–3 razy więcej miejsca niż kamery 1080p przy tej samej ilości klatek. Dlatego wybór powinien być zrównoważony między klarownością a dostępnymi zasobami.

Technologie poprawiające jakość obrazu

Kamery powinny obsługiwać technologie takie jak szeroki zakres dynamiczny (WDR) – umożliwiający przechwytywanie kolorowych obrazów w trudnych warunkach oświetlenia z dużymi kontrastami między jasnymi i ciemnymi obszarami. Wszystkie kamery powinny być kompatybilne z normami ONVIF w celu zapewnienia interoperacyjności z innymi produktami bezpieczeństwa fizycznego.

Korzystanie z AI – sztucznej inteligencji wbudowanych w funkcję urządzenia

Urządzenia, kamery i systemy zarządzające nie mogą wykorzystywać usług i serwisów używających sztucznej inteligencji do poprawiania obrazu oraz modyfikowania zawartości danych, w tym metadanych nagrań i innych. Należy unikać wbudowanych funkcji sztucznej inteligencji, a gdy jest możliwość wyłączać ją.

Oświetlenie i tryby “nocne”

Kamery powinny unikać skierowania bezpośrednio na jasne źródła światła, aby zmniejszyć refleks i zniekształcenia obrazu. W obszarach ze słabym oświetleniem konieczne jest stosowanie kamer dostosowanych do nocnych warunków przez wbudowane funkcje, takie jak np. oświetlenie podczerwone (IR), doświetlenie białym światłem LED, filtry czerni/bieli. Termowizja jest wskazana w obszarze składowania biomasy, oleju opałowego oraz ścieżek i instalacji gazowych. Należy ją też zastosować również z rozdzielniach elektrycznych i trafostacjach, halach kottów i urządzeń oraz wzdłuż podajników paliw.

Technologia noktowizyjna

Kamery noktowizyjne wykorzystują diody LED emitujące światło podczerwone (niewidoczne dla ludzkiego oka) do oświetlenia sceny w pełnej ciemności. Filtry IR odcięcia mechanicznie blokują światło podczerwone w jasny dzień, zapewniając prawidłowe odwzorowanie kolorów, a podczas nocy pozwalają światłu IR wejść w celu poprawy widoczności. Kamery powinny posiadać czujnik o niskiej impedancji (low lux rating) i dużą aperturę obiektywu (szybkie obiektywu) dla optymalnej wydajności w warunkach słabego oświetlenia.

Detekcja ruchu

Kamery powinny być wyposażone w czujnik ruchu, który umożliwia szybsze i efektywniejsze przeglądanie archiwum w przypadku wystąpienia zdarzenia. Na osi czasu mamy wskazane obszary z poszczególnych kamer, momenty wykrycia ruchu, znacząco i wizualnie przedstawiając obszar poszukiwań.

Anti-tampering

Kamery muszą być wyposażone w system informowania albo zapisywania w logach zdarzeń związanych z próbą ich otwarcia lub modyfikowania fizycznego ich obrazu, podłączenia innego urządzenia lub systemu do ich architektury. Jeżeli urządzenie na to pozwala, powinna być stosowana redundancja systemów, wysyłając informację w postaci wiadomości email albo/oraz wiadomości sms na telefon osoby wyznaczonej.

Przepustowość i Przechowywanie danych

Obliczenia przepustowości

Przepustowość wymagana dla systemu IP zależy od rozdzielczości, liczby klatek na sekundę (fps), rodzaju kompresji i liczby kamer. Kamera 1080p z kompresją H.264 wymaga około 2–4 Mbps, podczas gdy aparat 4K wymaga 8–15 Mbps.

Wzór na obliczenie przepustowości: $\text{Przepustowość (Mbps)} = \text{Szybkość transmisji (główna)} \times N + \text{Szybkość transmisji (podrzędna)} \times M$, gdzie N i M reprezentują liczbę kamer dla głównego i podrzędnego strumienia.

Pojemność miejsca, niezbędna do przechowywania danych.

Obraz z każdej z kamer musi być przechowywany przez 30 dni. W oparciu o tą informację, dostępną przepustowość oraz DTRki kamer należy dobrać pojemność serwera danych. Przechowywanie danych musi być zaplanowane w taki sposób, aby podzielić kamery na krytyczne, ważne i reszta. Krytycznych zapisy należy trzymać do 120 dni, ważne do 90 dni, reszta do 30 dni. W oparciu o ilość i kluczowość kamer należy ustalić wielkość przestrzeni serwera.

Architektura i zarządzanie łącznością w sieci

Dla instalacji obejmujących duże odległości (ponad 100 metrów) tradycyjne kable miedziane (CAT6) z ograniczeniem 100 metrów mogą być niewystarczające. Światłowód umożliwia transmisję na odległościach do 40 kilometrów, oferując wyższą przepustowość i lepszą przepustowość niż połączenia miedziane.

Standardem powinno być położenie nowego okablowania według wymagań, regulacji oraz dobrej praktyki na bazie standardów zapisanych w ISO 27001 i IEC 62443. Nowa sieć powinna zostać oznaczona i zabezpieczona w odpowiedni sposób, przed możliwością zniszczenia, uszkodzenia, manipulacji, itd. W trakcie instalacji sieć musi zostać oddzielona fizycznie oraz logicznie po stronie urządzeń i systemów. Tego typu sieć nie może łączyć się z innymi sieciami oraz urządzeniami, szczególnie określonymi jako krytyczne i ważne dla infrastruktury IT oraz OT. W infrastrukturze OT i IT należy stworzyć oddzielny punkt zarządzania, kontroli i dystrybucji, do którego wyłącznie ma dostęp określona osoba lub grupa osób w organizacji. Fizyczna struktura musi wykorzystywać dla wewnętrznych i zewnętrznych lokalizacji kable miedziane kategorii 6stej, z wyższym standardem

bezpieczeństwa oraz ochroną przed zewnętrznymi niebezpieczeństwami - manipulacja, gryzienie, uszkodzenia od warunków pogodowych i temperatury, itd.

Okablowanie

Wymaga się profesjonalnego zarządzania kablami z prawidłowym routingiem, zabezpieczeniem przed wilgocią i uszkodzeniami. Dla instalacji zewnętrznych należy stosować obudowy odporne na warunki atmosferyczne i zaciski wodoszczelne oraz zewnętrzne, żelowane kable CAT6.

Segmentacja sieci

System powinien być zaprojektowany z VLAN (Virtual Local Area Networks), implementacją QoS (Quality of Service) oraz konfiguracją zapory sieciowej w celu separacji ruchu CCTV od pozostałych sieci.

Redundancja i utrzymanie ciągłości działania systemu

Systemy krytyczne wymagają implementacji wielopoziomowej redundancji, aby zapewnić ciągłą pracę podczas awarii komponentów.

Standardem w przypadku tego typu systemów jest przyjęcie zasady dualizmu dla urządzeń głównych i redundancji jednego albo dwóch pozostałych urządzeń jak przełączniki, konwertery i kamery. Dla urządzeń, które przechowują nagrania, redundancja polega na wykorzystaniu odpowiedniej ilości dysków pamięci masowej, utrzymanie ich w ustalonej konfiguracji (RAID) tak, aby w przypadku awarii jednego z dysków system nadal pracował, a jednocześnie pozwalał na wymianę uszkodzonego komponentu bez zatrzymywania urządzenia (hotswap).

Zasady redundancji

Redundancję można osiągnąć poprzez: wdrażanie konfiguracji RAID 5 lub RAID 6 dla urządzeń przechowywania, implementację zduplikowanych serwerów w konfiguracji hot standby (każdy serwer główny ma wyznaczony serwer rezerwowy), wykorzystanie systemów UPS (zasilacze awaryjne) dla nieprzerwanego zasilania, oraz tworzenie zdywersyfikowanych rozwiązań magazynowania – kombinacja przechowywania lokalnego i chmurowego.

Architektura sieciowa

Struktura sieci powinna być zaprojektowana z redundancją – sieć siatkowa (mesh network) pozwala na istnienie wielu tras między przełącznikami a urządzeniami CCTV, co gwarantuje dostępność alternatywnych ścieżek w przypadku awarii.

Przełączanie awaryjne kamery

Kamery z wbudowaną pamięcią będą nadal zapisywać dane wideo lokalnie w przypadku problemów z siecią, a następnie synchronizować się z systemem nagrywającym po przywróceniu połączenia.

Serwery Nagrywające – DVR i NVR

Wybór urządzenia

Przy wyborze serwera nagrywającego (DVR – cyfrowy rejestrator wideo, lub NVR – sieciowy rejestrator wideo) należy uwzględnić:

- **Liczba kanałów:** urządzenie powinno obsługiwać obecną liczbę kamer plus możliwość rozszerzenia w przyszłości o 20%.
- **Obsługa rozdzielczości:** nowoczesne NVR-y obsługują 4K i wyższą rozdzielczość.
- **Pojemność magazynu:** powinna spełniać wymagania dotyczące czasu przechowywania nagrań.
- **Łączność sieciowa:** wsparcie dla niezawodnych połączeń sieciowych i kompatybilność z istniejącą infrastrukturą.
- **Dostęp zdalny i monitoring:** możliwość przeglądania obrazu zdalnie i zarządzania systemem (VPN lub wbudowany system w urządzenie).
- **Integracja:** możliwość integracji z systemami kontroli dostępu, alarmu i zarządzania budynkami.
- **Analityka wideo:** wsparcie dla automatycznego wykrywania anomalii i zdarzeń bezpieczeństwa.
- **Kamery z czujnikami ruchu:** montowane w przestrzeniach krytycznych takich jak ogrodzenia, wjazdy/wyjazdy, wejścia/wyjścia, klatki schodowe, rozdzielnie elektryczne, obszar jednostek wytwórczych, przestrzenie niebezpieczne i krytyczne dla eksploatacji. System powinien być tak skonstruowany, aby umożliwiał powiększanie obrazu w dodatkowym oknie z kamery, która wykryła ruch oraz posiadał możliwość wysłania notyfikacji na adres email.

NVR-y oferują wyższy poziom ochrony przed awariami w porównaniu do tradycyjnych DVR-ów, z wbudowanymi konfiguracjami RAID i zduplikowanymi dyskami SSD do mirroring systemu operacyjnego.

Pomieszczenie Kontrolne

Ergonomia stanowisk

Operatorzy spędzają długie okresy obserwując ekrany, dlatego ergonomia jest krytyczna. Stanowiska powinny mieć:

- Regulowane krzesła i biurka, dostosowane do różnych typów ciała.
- Monitory ustawione na poziomie oczu, aby zapobiec napięciu szyi i zmęczeniu oczu.
- Dedykowane ramiona do montażu monitorów, umożliwiające operatorom ustawienie optymalnej wysokości i odległości.

Oświetlenie i akustyka

Oświetlenie powinno być wystarczające, aby zapobiec zmęczeniu oczu, ale nie tak jasne, aby powodować odbicia na ekranach. Materiały pochłaniające dźwięk i projektowanie powinny minimalizować hałas otoczenia, pomagając operatorom utrzymać skupienie.

Wymiary pomieszczeń

Pomieszczenie powinno być wystarczająco przestronne, aby zmieścić całą infrastrukturę sprzętu, konsolę sterowania, monitory i jednostki przechowujące. Otwarta układzie może wspierać komunikację między operatorami.

Bezpieczeństwo Danych i Dostęp

Ochrona danych osobowych

Wszystkie systemy CCTV muszą być zaprojektowane z uwagą na bezpieczeństwo. Wymaga się implementacji właściwych technicznych i organizacyjnych środków ochrony danych przed nieautoryzowanym przetwarzaniem, przypadkową stratą, zniszczeniem lub uszkodzeniem.

Kontrola dostępu

System dostępu powinien być ograniczony za pomocą haseł i szyfrowania. Dostęp zdalny do nagrań powinien być zabezpieczony poprzez szyfrowanie i mechanizmy uwierzytelniania.

Osobą udzielającą dostępu do monitoringu jest najwyższa funkcyjnie osoba, zarządzająca obiektem.

System dostępu musi wykorzystywać podstawowe standardy bezpieczeństwa informacji i ochrony danych. Jednym z głównych elementów jest system tworzenia i zarządzania wieloma kontami, z dodatkowym zabezpieczeniem w postaci szyfrowania oraz aktywacją MFA/2FA dla każdego z kont. W zależności od rodzaju połączenia, niezależnie czy jest to wewnętrzne albo zewnętrzne, system musi filtrować i weryfikować, czy urządzenie łączące się z daną kamerą jest bezpiecznym i potwierdzonym zapisem na białej liście sprzętowej. Lista użytkowników i ich uprawnień musi zostać przygotowana, tak samo w przypadku administratorów. Konta muszą stosować się do polityk haseł stosowanej w organizacji, a same hasła muszą być zmieniane według określonych zasad.

Audyt dostępu

Dzienniki dostępu powinny być regularnie przeglądane w celu zapewnienia, że tylko uprawniony personel miał dostęp do nagrań. Należy unikać używania wspólnych haseł, aby zmniejszyć ryzyko nieuprawnionego użytkownika systemu, które mogłoby pozostać niezauważone. Należy przewidzieć system/urządzenie, które pozwala na nadanie każdemu użytkownikowi jego/jej własnego konta z hasłem + oddzielnie konta administracyjne i serwisowe.

Konserwacja i Testy Systemów

Harmonogram konserwacji

Regularna konserwacja jest niezbędna dla utrzymania niezawodności systemu. Zalecany harmonogram obejmuje:

- **Codziennie:** weryfikacja, że wszystkie kamery nagrywają prawidłowo, sprawdzenie wskaźników statusu systemu - checklista.
- **Tygodniowo:** testowanie procedur kopii zapasowych, weryfikacja odtwarzania wideo z losowo wybranych okresów.
- **Miesięcznie:** czyszczenie sprzętu, sprawdzenie stanu dysków twardych, testowanie systemu zasilania awaryjnego (UPS/bateria).
- **Kwartalnie:** przegląd rozmieszczenia kamer i efektywności pola widzenia, aktualizacja oprogramowania i firmware'u.

Kontrole techniczne

Wszystkie komponenty, w tym kamery, urządzenia nagrywające i połączenia sieciowe, powinny być regularnie testowane. Wymaga się przeprowadzania testów odtwarzania wydajności i weryfikacji, że kopie zapasowe są funkcjonalne.

Czyszczenie obiektywów

Obiektywy kamer powinny być czyszczone dwa razy w roku miękką ściereczką i czyszczącym roztworem nienabłyszczającym. Kamery zewnętrzne mogą wymagać częstszego czyszczenia ze względu na ekspozycję na czynniki środowiskowe, takie jak sól, pył i pajęczyny.

Zgodność Prawna i Prywatność

GDPR i ochrona danych

Systemy CCTV muszą być zaprojektowane zgodnie z Ogólnym Rozporządzeniem o Ochronie Danych (GDPR). Wymaga się przejrzystości, minimalnego zbierania danych i bezpiecznych kontroli dostępu.

Bezpieczeństwo informacji i cyberbezpieczeństwo

Ze względu na przepisy KSC 1 i nowe KSC 2, w których skład wchodzi nowe regulacje Parlamentu EU

Informowanie użytkowników

Muszą być wyświetlone wyraźne znaki informujące osoby, że znajdują się na terenie pod nadzorem wideo. Dostęp do nagrań powinien być ograniczony do uprawnionych pracowników, a nagrania powinny być usuwane po ustalonego okresu przechowywania (zazwyczaj 30 dni).

Integralność i Interoperacyjność

Standardy ONVIF

Wszystkie kamery sieciowe powinny być kompatybilne ze standardami ONVIF (Open Network Video Interface Forum) w celu zapewnienia efektywnej interoperacyjności z produktami bezpieczeństwa fizycznego innych producentów. Umożliwia to przeglądanie i przetwarzanie przechwyconych nagrań CCTV na kompatybilnych platformach.

Testowanie i Walidacja Systemu

Po instalacji, system powinien być gruntownie testowany w warunkach rzeczywistych, zarówno w dzień jak i nocy, w celu weryfikacji prawidłowego funkcjonowania i pokrycia martwych pól. Należy przeprowadzić spacerowe testy (walk tests), poruszając się po terenie podczas sprawdzania transmisji na żywo, aby potwierdzić pokrycie wszystkich obszarów krytycznych.

KD

Systemy kontroli dostępu stanowią pierwszą linię obrony dla organizacji dążących do zapewnienia bezpieczeństwa fizycznego ludzi, mienia i zasobów. Skuteczne projektowanie wymaga strategicznego podejścia uwzględniającego aspekty techniczne, operacyjne, bezpieczeństwa i zgodności z przepisami.

Planowanie i Analiza Wymagań

Ocena potrzeb bezpieczeństwa

Przed rozpoczęciem projektowania konieczne jest przeprowadzenie kompleksowej analizy wymagań bezpieczeństwa organizacji. Należy zidentyfikować konkretne zagrożenia, ocenić podatności oraz zdefiniować cele bezpieczeństwa. Ten proces powinien obejmować szczegółową ocenę lokalizacji, identyfikację obszarów krytycznych, analizę wzorców ruchu i określenie różnych poziomów uprawnień dostępu wymaganych dla różnych grup użytkowników.

Efektywne planowanie wymaga zaangażowania użytkowników końcowych i interesariuszy od samego początku, przeglądu projektów na poziomie koncepcyjnym oraz ustanowienia standardów kontroli dostępu, które będą stanowić solidną podstawę do długoterminowego użytkowania.

Zakres systemu

Określenie zakresu systemu jest kluczowe dla projektu. Należy zdefiniować wszystkie punkty dostępu wymagające kontroli, w tym hale kotłowni i urządzeń, główne wejścia, drzwi boczne, bramy, klatki schodowe, pomieszczenia serwerowe, laboratoria i inne obszary wrażliwe. Dla każdego punktu dostępu należy ustalić wymagany poziom bezpieczeństwa i odpowiednie metody uwierzytelniania.

Architektura Wielowarstwowa

Nowoczesne systemy kontroli dostępu powinny być projektowane z wykorzystaniem podejścia wielowarstwowego, często określanego jako "obrona w głąbi". Architektura ta polega na tworzeniu wielu koncentrycznych pierścieni ochrony wokół najbardziej krytycznych zasobów, gdzie każda warstwa służy jako bariera – jeśli jedna zostanie naruszona, kolejna jest gotowa wykryć i powstrzymać zagrożenie.

Strefy bezpieczeństwa

System powinien być zorganizowany w cztery główne strefy fizyczne, z eskalacją poziomu kontroli w miarę zbliżania się do bardziej wrażliwych obszarów:

Obwód zewnętrzny: Najbardziej zewnętrzna warstwa skupia się na kontroli dostępu na granicy terenu. Obejmuje identyfikację pojazdów na duże odległości (tagi RFID), kontrolę bram, czujniki obwodowe i bariery fizyczne.

Wejście do budynku: Na tym etapie weryfikacja tożsamości jest najważniejsza. Uwierzytelnianie wieloskładnikowe, rozwiązania zarządzania gośćmi zapewniają, że tylko autoryzowany personel uzyskuje dostęp do obiektu.

Strefy wewnętrzne i klatki: Wewnątrz budynku kontrola dostępu oparta na rolach i zarządzanie strefami ograniczają ruch do wyznaczonych obszarów. Funkcje takie jak ochrona przed tailgatingiem i służby osobowe (mantrap) wymuszają ścisłe oddzielenie (kotłowniki).

Szafy i stojaki serwerowe: Najbardziej wewnętrzna warstwa wykorzystuje elektroniczne zamki i czytniki dostępu dla poszczególnych szaf, zapewniając najwyższy poziom pewności i generując szczegółowe dzienniki audytu dla każdego zdarzenia.

Modele Kontroli Dostępu

Role-Based Access Control (RBAC)

Jednym z najbardziej efektywnych sposobów zarządzania uprawnieniami dostępu jest wdrożenie modelu kontroli dostępu opartej na rolach. W ramach RBAC prawa dostępu są przypisywane w oparciu o rolę osoby w organizacji. Minimalizuje to ryzyko nieautoryzowanego dostępu i zapewnia, że pracownicy mają dostęp tylko do zasobów niezbędnych do wykonywania swoich obowiązków.

Uprawnienia należy grupować według funkcji – na przykład grupa IT może potrzebować dostępu do serwerowni, ale nie do magazynu, i tylko w określonych godzinach. Role powinny być regularnie przeglądane i aktualizowane, aby uwzględniać zmiany w obowiązkach zawodowych lub restrukturyzację organizacji.

Zasada Najmniejszych Uprawnień (Principle of Least Privilege)

System powinien być zaprojektowany zgodnie z zasadą najmniejszych uprawnień, co oznacza, że użytkownicy powinni mieć tylko minimalny poziom dostępu niezbędny do wykonywania swoich funkcji zawodowych. Takie podejście ogranicza potencjalne szkody, które mogą wystąpić w przypadku naruszenia konta użytkownika, redukując ryzyko zagrożeń wewnętrznych i przypadkowego naruszenia danych.

Wdrożenie tej zasady wymaga regularnego audytu uprawnień użytkowników i cofania dostępu, gdy nie jest już potrzebny, szczególnie dla pracowników tymczasowych, wykonawców i dostawców zewnętrznych.

Wybór Technologii Uwierzytelniania

Karty dostępu i technologie RFID/NFC

Tradycyjne systemy kart stanowią podstawę większości wdrożeń kontroli dostępu. Dostępne są różne technologie:

Karty zbliżeniowe (Proximity Cards, 125 kHz): Pasywne karty RFID transmitujące stały identyfikator w pobliżu czytnika. Kompatybilne z wieloma istniejącymi systemami, ale oferują podstawowy poziom bezpieczeństwa.

Karty inteligentne (Smart Cards, 13,56 MHz): Wykorzystują zaawansowane szyfrowanie i oferują wyższy poziom bezpieczeństwa niż karty zbliżeniowe. Mogą przechowywać więcej danych i obsługiwać wiele aplikacji.

Technologia NFC: Ewolucja RFID działająca w ekstremalnie bliskiej odległości (maksymalnie 4 cm). Umożliwia dwukierunkową komunikację i jest szeroko wykorzystywana w smartfonach do kontroli dostępu mobilnego.

Kody obiektu na karcie dostępu (Facility code)

Kod obiektu to unikalna wartość liczbowa, która jest programowana na karcie kontroli dostępu lub breloku, wraz z unikalnym indywidualnym kodem dla każdej osoby, która jest upoważniona do dostępu do obiektu. Kody obiektów są zazwyczaj nadawane przez producenta systemu kontroli dostępu lub przez organizację wdrażającą system. Są one zwykle używane w połączeniu z numerem identyfikacyjnym posiadacza karty, aby zapewnić, że dostęp jest przyznawany tylko upoważnionym osobom. Gdy karta lub brelok zostanie przyłożony do czytnika przy określonych drzwiach lub wejściu, czytnik sprawdza kod obiektu i indywidualny kod, aby określić, czy dana osoba jest upoważniona do wejścia.

Uwierzytelnianie wieloskładnikowe (MFA)

Dodanie dodatkowej warstwy bezpieczeństwa poprzez uwierzytelnianie wieloskładnikowe jest kluczowe dla ochrony obszarów wrażliwych. MFA wymaga, aby użytkownicy weryfikowali swoją tożsamość za pomocą dwóch lub więcej metod, takich jak hasło, odcisk palca lub jednorazowy kod wysłany na urządzenie mobilne. Redukuje to ryzyko nieautoryzowanego dostępu, nawet jeśli hasło zostanie skompromitowane.

Dla starszych systemów MFA często oznacza konieczność wprowadzenia kodu PIN i użycia karty dostępu. W przypadku nowoczesnych systemów obsługujących poświadczenia mobilne użytkownicy muszą odblokować swoje urządzenie mobilne przed przyłożeniem go do czytnika.

Komponenty Systemu

Czytniki i kontrolery

Czytniki powinny być wybierane w oparciu o poziom bezpieczeństwa, kompatybilność z systemem, obsługiwane typy kart oraz odporność na warunki środowiskowe. Dla instalacji zewnętrznych wymagane są czytniki odporne na warunki atmosferyczne z odpowiednim stopniem ochrony IP.

Kontrolery działają jako centralna jednostka odpowiedzialna za weryfikację poświadczeń dostępu i zarządzanie punktami dostępu poprzez przyznawanie lub odmawianie wejścia. Kontroler stanowi mózg systemu kontroli dostępu, podejmując decyzje w czasie rzeczywistym na podstawie otrzymanych danych.

Serwer kontroli dostępu

Serwer przechowuje dzienniki wejść, poświadczenia i dane użytkowników. Może być zlokalizowany lokalnie lub w chmurze, w zależności od potrzeb organizacji. Scentralizowane przechowywanie i zarządzanie danymi zapewnia spójne egzekwowanie uprawnień we wszystkich punktach dostępu.

Zamki elektroniczne

System musi być połączony z drzwiami wyposażonymi w zamki elektroniczne, które można zaprogramować do automatycznego otwierania po przedstawieniu ważnych poświadczeń. Można wybrać zamki fail-safe lub fail-secure, chociaż w przypadku ochrony określonych części budynku protokoły bezpieczeństwa mogą dyktować, który typ zamka zastosować. W przypadku braku poświadczeń dostęp powinien odbywać się wyłącznie w asyście osoby uprawnionej z wyraźnym uzasadnieniem, np. przeprowadzenie prac serwisowych.

Fail-safe vs Fail-secure

Zamki Fail-Safe: Odblokowują się podczas awarii zasilania, zapewniając bezpieczne wyjście w sytuacjach awaryjnych. Wymagają zasilania, aby pozostać zamkniętymi. Idealne dla obszarów o dużym natężeniu ruchu, takich jak biura i hale, gdzie szybka ewakuacja jest kluczowa.

Zamki Fail-Secure: Pozostają zamknięte podczas awarii zasilania, zachowując bezpieczeństwo dla wrażliwych obszarów. Można je ręcznie odblokować od wewnątrz, zapewniając, że mieszkańcy nadal mogą wyjść w razie potrzeby. Zalecane dla pomieszczeń serwerowych, magazynów IT i innych stref wysokiego bezpieczeństwa.

Ważne jest, aby zauważyć, że oba typy zamków pozwalają ludziom bezpiecznie opuścić pomieszczenie w przypadku awarii – terminologia fail-safe i fail-secure dotyczy tylko wejścia. W przypadku ewakuacji awaryjnej płyty zamków fail-secure nadal umożliwiają ręczną obsługę od wewnątrz, nadrzędną funkcję zamka.

Umiejscowienie Czytników

Punkty wejścia

Czytniki powinny być umieszczone we wszystkich punktach wejścia, w tym głównych wejściach, drzwiach bocznych, bramach i wejściach do parkingów. W przypadku budynków z obszarami recepcji czytniki powinny być umieszczone zarówno na drzwiach prowadzących do holu, jak i na drzwiach wychodzących z holu dalej do budynku. Pozwala to na pozostawienie zewnętrznych

drzwi otwartych, gdy recepcjonista jest na stanowisku, zapewniając jednocześnie członkom dostęp po godzinach pracy.

Interfejsy publiczne/prywatne

Jeśli obiekt ma obszary publiczne i prywatne, czytniki powinny być umieszczone na granicy między strefami. Można to również wykorzystać w przypadku wielopoziomowego członkostwa, aby zapewnić określonym użytkownikom dostęp do różnych obszarów obiektu.

Wysokość montażu

Czytniki kart powinny być montowane na wysokości około 1,2–1,5 metra nad poziomem podłogi dla łatwego użytkowania. Kontrolery powinny być instalowane po bezpiecznej stronie drzwi (najlepiej w miejscach trudnodostępnych (np. nad podwieszanym sufitem), aby zapobiec manipulacjom.

Scentralizowane Zarządzanie

System zarządzania dostępem

Dla większych organizacji zarządzanie uprawnieniami dostępu w wielu lokalizacjach lub działach może być wyzwaniem. Scentralizowany system zarządzania dostępem upraszcza ten proces, zapewniając jeden interfejs dla administratorów do monitorowania i kontrolowania praw dostępu. Takie podejście zwiększa widoczność, zapewnia spójność i ułatwia audyt dzienników dostępu.

Scentralizowane systemy mogą również generować alerty w czasie rzeczywistym dotyczące podejrzanych działań, umożliwiając zespołom bezpieczeństwa szybką reakcję na potencjalne naruszenia.

Automatyzacja harmonogramów dostępu

Automatyzacja dostępu zapewnia precyzyjną kontrolę nad dostępem do określonych obszarów obiektu w wyznaczonych godzinach, takich jak święta, zmniejszając ryzyko nieautoryzowanego wejścia. Ustawianie automatycznych harmonogramów dostępu nie tylko zwiększa bezpieczeństwo, ale także usprawnia operacje, umożliwiając szybkie dostosowania uprawnień dostępu.

Nowoczesne systemy mogą całkowicie odmówić dostępu w wybranych okresach, takich jak noc, nawet jeśli osoba z autoryzowanym dostępem próbuje wejść.

Integracje Systemowe

Integracja z systemami alarmowymi pożarowymi

Integracja systemów kontroli dostępu z systemami alarmowymi pożarowymi jest kluczowa dla bezpieczeństwa życia. W przypadku pożaru wszystkie drzwi powinny automatycznie się odblokowywać, aby ułatwić bezpieczną ewakuację. System kontroli dostępu powinien być podłączony do panelu alarmowego pożarowego za pomocą rezerwowego kontrolera zasilania.

Gdy alarm pożarowy jest aktywowany, komunikuje się on z rezerwowym kontrolerem, który z kolei wyzwala kontroler systemu kontroli dostępu do odblokowania wszystkich drzwi. W scenariuszach awaryjnych rzeczywista ochrona jest drugorzędna wobec ratowania życia.

System może również uszczelnić obszar, w którym występuje zdarzenie pożarowe, aby zatrzymać jego rozprzestrzenianie się, jednocześnie zachowując dostęp do obszarów ograniczonych.

Integracja z CCTV

Integracja kontroli dostępu z systemami CCTV tworzy inteligentniejsze i bardziej proaktywne bezpieczeństwo. Kluczowe funkcje obejmują:

- Mapowanie drzwi łączące kamery bezpieczeństwa ze zdarzeniami dostępu;
- Strumienie wideo w czasie rzeczywistym uruchamiane podczas incydentów;
- Rozpoznawanie twarzy do monitorowania aktywności gości;
- Odtwarzanie przy odmowie dostępu, tailgatingu lub wymuszonych drzwiach;
- Centralne monitorowanie przez zunifikowany interfejs.

Tworzy to niezbędne połączenie między danymi dostępu a wizualnym potwierdzeniem, umożliwiając szybsze dochodzenia i świadomość w czasie rzeczywistym.

Integracja z zarządzaniem gośćmi

Nowoczesne systemy kontroli dostępu powinny integrować się z platformami zarządzania gośćmi, umożliwiając przedzarejestrowanie, samodzielne zameldowanie i automatyczne powiadomienia gospodarzy. Administratorzy mogą wysyłać linki dostępu kilkoma kliknięciami, które są zgodne z zasadą najmniejszych uprawnień. Goście otrzymują te linki na e-mail, platformę czatu lub SMS-em i mogą odblokować drzwi, których potrzebują, dotykając swoich telefonów.

System powinien umożliwiać ustawienie zasad dostępu określających konkretne drzwi, piętra i godziny dla gości. W sytuacjach awaryjnych system zarządzania gośćmi może natychmiast generować kompletną, aktualną listę ewakuacyjną.

Integracja z oprogramowaniem HR

Integracja z systemami HR umożliwia automatyczne przyznawanie lub odbieranie dostępu na podstawie statusu zatrudnienia, zmniejszając obciążenie administracyjne i poprawiając

bezpieczeństwo. Gdy nowy pracownik jest zatrudniony, system automatycznie tworzy odpowiednie uprawnienia dostępu na podstawie roli. Gdy pracownik opuszcza organizację, dostęp jest natychmiast cofany.

Bezpieczeństwo Cybernetyczne

Segmentacja sieci

Ruch systemu kontroli dostępu powinien być oddzielony od innych sieci przy użyciu sieci VLAN (Virtual Local Area Networks), implementacji QoS (Quality of Service) oraz konfiguracji zapory sieciowej. Segmentacja sieci ogranicza potencjalny ruch boczny atakujących w ramach sieci, ograniczając ich do mniejszego segmentu.

Szyfrowanie

Wszystkie dane przesyłane między komponentami systemu powinny być szyfrowane zarówno w spoczynku, jak i w transzycie, aby zapobiec nieautoryzowanemu dostępowi. Należy wykorzystywać silne algorytmy szyfrowania i bezpiecznie zarządzać kluczami szyfrowania.

Listy kontroli dostępu (ACL)

Listy kontroli dostępu to mechanizm bezpieczeństwa określający, którzy użytkownicy lub systemy mają przyznany lub odmówiony dostęp do określonych zasobów sieciowych. ACL są zazwyczaj konfigurowane na poziomie punktu końcowego, takim jak routery, serwery lub laptopy, dzięki czemu tylko autoryzowane podmioty mogą uzyskać dostęp do określonych urządzeń lub danych.

ACL można podzielić na listy "dozwolone" i "zakazane". Lista dozwolonych przyznaje dostęp wyraźnie wymienionym podmiotom, zapewniając, że tylko te wymienione mogą uzyskać dostęp do zasobów. W przeciwieństwie do tego, lista zakazanych zezwala na dostęp wszystkim z wyjątkiem tych wyraźnie wykluczonych.

Wsparcie offline

Chociaż systemy kontroli dostępu oparte na chmurze są najlepsze pod każdym względem, niektóre obiekty trzymają się starszych systemów, ponieważ mogą oferować podstawową funkcjonalność bez stałego połączenia internetowego. Niektóre systemy kontroli dostępu oparte na chmurze, takie jak Kisi, oferują wsparcie offline, zapewniając funkcjonalność nawet w przypadku problemów z łącznością internetową.

Dzienniki Audytu i Zgodność

Wymagania GDPR dotyczące dzienników

Wszystkie systemy kontroli dostępu muszą być zaprojektowane z uwzględnieniem ochrony danych osobowych zgodnie z RODO (GDPR). Śledzenie dostępu do danych jest podstawowym wymogiem RODO w celu zapewnienia przejrzystości i odpowiedzialności.

Należy wdrożyć szczegółowe mechanizmy rejestrowania, aby rejestrować każdy przypadek dostępu do danych, w tym kto uzyskał dostęp do danych, kiedy uzyskano dostęp i cel dostępu. Dzienniki te powinny być bezpiecznie przechowywane i chronione przed manipulacją. Regularne przeglądy dzienników dostępu są kluczowe dla identyfikacji i rozwiązywania wszelkich prób nieautoryzowanego dostępu.

Rejestrowanie modyfikacji danych

Śledzenie modyfikacji danych jest niezbędne do utrzymania integralności i dokładności danych osobowych zgodnie z wymogami RODO. Organizacje powinny rejestrować wszystkie zmiany wprowadzone do danych osobowych, w tym jakie zmiany zostały dokonane, kto je wprowadził i kiedy zostały dokonane.

Szyfrowanie i przechowywanie dzienników

Dzienniki zawierające dane osobowe muszą być szyfrowane zarówno w spoczynku, jak i w transzycie, aby zapobiec nieautoryzowanemu dostępowi. Wdrożenie silnych protokołów szyfrowania zapewnia, że nawet jeśli dane zostaną przechwycone lub uzyskane bez autoryzacji, pozostają nieczytelne i bezpieczne.

Okres przechowywania

Organizacje powinny ustanowić politykę przechowywania danych określającą, jak długo dzienniki są przechowywane w oparciu o wymogi prawne i operacyjne. Zapewnia to, że dane osobowe nie są przechowywane dłużej niż to konieczne, przestrzegając zasady minimalizacji danych RODO.

Kontrola dostępu do dzienników

Dostęp do dzienników zawierających dane osobowe powinien być ograniczony tylko do autoryzowanego personelu z uzasadnionym zapotrzebowaniem. Wdrożenie ścisłych kontroli dostępu, takich jak uprawnienia dostępu oparte na rolach, pomaga to osiągnąć poprzez ograniczenie dostępu do dzienników w oparciu o rolę użytkownika w organizacji.

Meta-dzienniki

Należy zapewnić, że dostęp do dzienników i działania podjęte na zarejestrowanych danych są same rejestrowane i podlegają audytowi. Praktyka ta obejmuje tworzenie meta-dzienników, które rejestrują, kto uzyskał dostęp do głównych dzienników, kiedy to zrobił i wszelkie operacje wykonane na zarejestrowanych danych.

Testowanie i Uruchomienie

Proces uruchomienia

Uruchomienie odnosi się do ustrukturyzowanego procesu testowania, weryfikacji i walidacji, że zainstalowany system działa zgodnie z projektem i spełnia wymagania dotyczące wydajności, funkcjonalności i bezpieczeństwa klienta. Uruchomienie systemu bezpieczeństwa obejmuje szczegółową inspekcję, programowanie, testowanie funkcjonalne i dokumentację, aby zapewnić, że wszystkie komponenty i oprogramowanie działają prawidłowo, bezpiecznie i zgodnie z zamierzonym projektem.

Kluczowe etapy uruchomienia

Weryfikacja systemu: Upewnienie się, że wszystkie urządzenia są zainstalowane zgodnie z planami i specyfikacjami. Potwierdzenie umieszczenia urządzeń, zakończeń kabli i etykietowania.

Konfiguracja i programowanie: Programowanie poziomów dostępu, harmonogramów, grup drzwi i reguł alarmowych. Konfiguracja czytników, kontrolerów i systemu zarządzania.

Testowanie funkcjonalne: Testowanie sprzętu drzwiowego (zamki, REX, kontakty) dla kontroli dostępu. Potwierdzenie integracji (np. kontrola windy, alarmy włamaniowe).

Kontrola sieci i bezpieczeństwa cybernetycznego: Testowanie wydajności sieci, przepustowości i bezpiecznych protokołów komunikacyjnych. Stosowanie aktualizacji firmware i ochrony hasłem.

Testowanie akceptacji użytkownika (UAT): Przejście systemu z klientem w celu zademonstrowania kluczowych funkcji. Walidacja, że system spełnia cele i oczekiwania operacyjne.

Szkolenie i przekazanie: Zapewnienie szkoleń dla użytkowników końcowych i administratorów. **Dostarczenie dokumentacji:** rysunki as-built, listy urządzeń, eksporty programowania i instrukcje użytkownika.

Dokumentacja końcowa: Arkusze odbioru, listy kontrolne i aktywacja gwarancji. Rejestr testów uruchomieniowych i rozwiązywania problemów.

Skalowalność i Przyszłościowość

Architektura modułarna

System powinien być zaprojektowany z modułową architekturą umożliwiającą rozbudowę, aktualizację lub wymianę poszczególnych komponentów bez wpływu na cały system. Ta elastyczność jest niezbędna do skalowania systemu w miarę potrzeb i adaptacji do nowych technologii.

Otwarte standardy i interoperacyjność

Wybierając system kontroli dostępu, należy upewnić się, że oferuje on elastyczność i pozwala uniknąć uzależnienia od dostawcy. System powinien mieć:

- Otwarte API do dostosowywania;
- Kompatybilność ze sprzętem i oprogramowaniem stron trzecich;
- Możliwość eksportu danych, aby uniknąć komplikacji podczas przejścia na inną platformę;

Te funkcje nie tylko zabezpieczają inwestycję na przyszłość, ale także umożliwiają organizacjom zachowanie zwinności w ciągle zmieniającym się krajobrazie technologicznym.

Rozwiązania chmurowe

Systemy kontroli dostępu oparte na chmurze stanowią przyszłość branży, oferując elastyczność, skalowalność i zdalne zarządzanie. Platforma SaaS eliminuje potrzebę częstych aktualizacji i konserwacji na miejscu, umożliwiając firmom skupienie się na podstawowych działaniach przy jednoczesnym cieszeniu się zwiększonym bezpieczeństwem i niezawodnością.

Podejście hybrydowe zapewnia, że nawet w trudnych sytuacjach, takich jak przerwy w sieci, podstawowa funkcjonalność kontroli dostępu pozostaje nienaruszona. Chmura ułatwia bezproblemowe aktualizacje, intuicyjne zarządzanie i niezrównane doświadczenie użytkownika.

Model ACaaS

Access Control as a Service (ACaaS) rośnie ponad dwukrotnie szybciej niż tradycyjne systemy kontroli dostępu. Firmy mogą przejść z wydatków kapitałowych na wydatki operacyjne, dostosowując wydatki do wykorzystania. Model ten upraszcza budżetowanie i zmniejsza obciążenie finansowe dużych inwestycji początkowych.

Łatwość Użytkowania

System, który jest zbyt skomplikowany, raczej nie będzie efektywnie wykorzystywany. Rozwiązania powinny oferować prosty interfejs użytkownika i wymagać minimalnego szkolenia, aby zmaksymalizować ich efektywność. System bezpieczeństwa, który jest trudny w nawigacji, nigdy nie będzie w pełni wykorzystany, zmniejszając jego wartość.

Konserwacja i Wsparcie

Regularna konserwacja

System powinien być regularnie testowany i konserwowany, aby zapewnić ciągłą niezawodność. Wszystkie komponenty, w tym czytniki, kontrolery, zamki i połączenia sieciowe, powinny być okresowo sprawdzane.

Aktualizacje oprogramowania

Firmware i oprogramowanie systemu powinny być regularnie aktualizowane, aby załatać luki w zabezpieczeniach i dodać nowe funkcje. Systemy chmurowe oferują automatyczne aktualizacje Over-The-Air (OTA), eliminując potrzebę ręcznej interwencji.

Skuteczne projektowanie systemu kontroli dostępu wymaga zintegrowanego podejścia łączącego planowanie strategiczne, wybór odpowiednich technologii, architekturę wielowarstwową, integrację z innymi systemami bezpieczeństwa oraz zgodność z przepisami o ochronie danych. Systematyczne podejście do tych elementów zapewnia bezpieczny, niezawodny i skalowalny system kontroli dostępu, który chroni ludzi, mienie i zasoby organizacji przy jednoczesnym zapewnieniu wygody użytkowania i efektywności operacyjnej.