Jak podnieść poziom bezpieczeństwa fizycznego?

Bezpieczeństwo fizyczne jest bardzo ważnym ogniwem w całym łańcuchu zabezpieczeń zapewniających trwałość aktywów i informacji w firmie. Zintegrowany system bezpieczeństwa fizycznego powinien być kompleksowym uzupełnieniem istniejących systemów bezpieczeństwa informatycznego, prawnego i środowiskowego. W taki sposób w organizacjach zapewniane jest całościowe i kompletne bezpieczeństwo. Zaniedbania w tym obszarze mogą stanowić poważny problem na drodze do spełnienia wymagań jakie stawiane są zarówno przez przepisy prawne, jak i normy bezpieczeństwa oraz wymagania na rynku.

Planując podnieść poziom bezpieczeństwa fizycznego organizacji dobrze jest rozważyć wdrożenie kompleksowego systemu ochrony fizycznej, który zintegrowałby wszystkie funkcjonujące w firmie systemy bezpieczeństwa, takie jak: System Kontroli Dostępu (SKD), System Sygnalizacji Włamania i Napadu (SSWiN),Elektroniczny Systemu Wydawania Kluczy (ESWK).

SYSTEMY OCHRONY FIZYCZNEJ

Nowoczesne kompleksowe systemy ochrony fizycznej zapewniają integrację z systemami kontroli dostępu i rejestracją czasu pracy. Obejmują swym zakresem zarówno konfigurację, wizualizację ze sterowaniem, jak i obsługę rejestracji czasu pracy. Integracja z Systemem Sygnalizacji Włamania i Napadu pozwala na zarządzanie uzbrajaniem/rozbrajaniem grup alarmowych i sterowaniem wyjściami, oraz pełną wizualizację na planach obiektu. Integracja Elektronicznym Systemem Wydawania Kluczy pozwala na pełne zarządzanie użytkownikami i ich uprawnieniami do poszczególnych kluczy, oraz mechanizmem kontroli zdania klucza. Takie rozwiązanie pozwala na pełny monitoring zarzadzania bezpieczeństwem fizycznym w obiektach firmy.

WIZUALIZACJA I INTEGRACJA

Wizualizacja jest aktywną prezentacją aktualnych stanów urządzeń (grup alarmowych, czujek, depozytora kluczy, przejść itp.) naniesioną na plany architektoniczne poszczególnych pomieszczeń. Dzięki temu rozwiązaniu operator w sposób prosty, szybki i skuteczny jest w stanie zarządzać bardzo skomplikowanym systemem bezpieczeństwa zainstalowanym w obiekcie. Wizualizacja nie tylko zapewnia aktualny podgląd stanu elementów systemu bezpieczeństwa, ale również umożliwia zdalne nimi sterowanie (np. otwarcie drzwi poprzez kliknięcie ich ikony widocznej na wizualizacji). Integracja umożliwia połączenie wszystkich systemów bezpieczeństwa oraz monitorowanie parametrów środowiskowych (np. temperatury i wilgotności w serwerowni), czy też zużycia mediów (np. kontrola zużycia energii, wody, ciepła itp.).

Dzięki integracji np. kontroli dostępu z depozytorem kluczy ostatnia osoba wychodząca z obiektu nie może go opuścić gdy nie zda pobranych kluczy. Prezentacja alarmów realizowana jest, oprócz wskazania lokalizacji na grafice (miejsce na obiekcie oraz dokładnie czujkę, lub drzwi), również w postaci tekstowej. Alarmy są prezentowane w pierwszej kolejności względem priorytetu (alarmy o większej wadze prezentowane są zawsze na samym początku), a w drugiej względem czasu. Alarm posiada pełen opis rodzaju zdarzenia oraz z jakiego urządzenia przyszedł.

SYSTEMU KONTROLI DOSTĘPU (SKD)

Systemy Kontroli Dostępu umożliwiają identyfikację osób oraz przydzielanie dostępów użytkownikom do wyznaczonych obszarów (stref) w firmie.

Nowoczesne Systemy Kontroli Dostępu posiadają cechy, które definiują ich przydatność oraz skuteczność takich rozwiązań. Przykładowe cechy SKD:

- Stopień bezpieczeństwa w czterostopniowej skali klasyfikacji urządzeń
- Pełne szyfrowanie (na każdym etapie transmisji danych wykorzystywane są algorytmy szyfrujące AES128, CTR, CMAC zapewniając tym samym maksymalny poziom bezpieczeństwa),
- Zgodność z Normami Obronnymi, np. NO-04-A004 i innymi normami związanymi z bezpieczeństwem
- Struktura kontrolerów oparta na sieci Ethernet, ułatwiająca rozbudowę systemów w dowolnej lokalizacji sieci
- Możliwość zarządzania gośćmi, pracownikami, samochodami pracowników, gości i służbowymi,
- Wbudowane oprogramowanie do rejestracji czasu pracy.

Rafał Król – Pełnomocnik Zarządu ds. bezpieczeństwa w jednej ze spółek z sektora obronnego. Doświadczenie zawodowe zdobywał m.in. w spółkach zbrojeniowych i z sektora lotniczego, gdzie zarządzał szeroko pojętym bezpieczeństwem. Kwalifikowany pracownik ochrony fizycznej i zabezpieczenia technicznego, pełnomocnik ds. ochrony informacji niejawnych, administrator i inspektor niejawnych systemów teleinformatycznych. Ukończył studia podyplomowe z zakresu bezpieczeństwa systemów informacyjnych i bezpieczeństwa sieci komunikacji mobilnej. Z bezpieczeństwem związany od 2008 roku.

SYSTEM SYGNALIZACJI WŁAMANIA I NAPADU (SSWIN)

Systemy Sygnalizacji Włamania i Napadu mają za zadanie jak najszybsze i skuteczne wykrycie osób niepożądanych i właściwe przekazanie tej informacji celem reakcji na incydent i podjęcia koniecznych działań. W skład takiego sytemu wchodzą różnego rodzaju detektory ruchu (czujki podczerwieni, ultradźwiękowe i mikrofalowe, detektory stłuczeniowe szyby czy czujki drgań i wibracji. Głównym komponentem systemu jest centrala alarmowa, której zadaniem jest zarządzanie całym systemem.

ELEKTRONICZNY SYSTEMU WYDAWANIA KLUCZY (ESWK)

Elektroniczny System Wydawani Kluczy w kompleksowy sposób zarządza polityką kluczy w firmie. ESKW oparty jest na depozytorze kluczy. Wdrażając go do użytku firma uzyska:

- bezpieczną gospodarkę kluczami i ich obiegiem,
- sprawny, zautomatyzowany i łatwy sposób przechowywania i wydawania wszelkiego rodzaju kluczy,
- możliwość nadawania uprawnień, raportowania kto, kiedy pobrał i zwrócił klucz (to wszystko w jednym w pełni zautomatyzowanym procesie),

ponadto:

- całkowicie wyeliminowane zostaną błędy spowodowane tzw. czynnikiem ludzkim,
- skrócony zostanie czas potrzeby na pobranie i zdanie klucza,
- wyeliminowane zostaną przypadki dostępu do kluczy przez osoby nieuprawnione.

AUTOMATYCZNY SYSTEM IDENTYFIKACJI TABLIC REJESTRACYJNYCH (ASITR)

Zarządzanie ruchem pojazdów, kontrolowanie, kto wjechał na teren obiektu, a kto z niego wyjechał to kluczowe elementy bezpieczeństwa każdego obiektu. Wdrażając Automatyczny System Identyfikacji Tablic Rejestracyjnych firma uzyskuje:

- automatyczne rozpoznanie i identyfikację samochodu bez potrzeby używania kart dostępu czy pilota,
- bezpieczne, automatyczne zarządzanie i monitorowanie obiegu pojazdów na terenie spółki,
- automatyczne prowadzenie bazy danych zawierającej m.in. dane na temat czasu i ilości wjazdów, wyjazdów, ilości pojazdów, ich pochodzenia,
- możliwość tworzenia dowolnych raportów i analiz.

Wdrażając systemy bezpieczeństwa informacyjnego w firmach warto zwrócić uwagę na bezpieczeństwo fizyczne. Kompleksowe podejście do zarządzania bezpieczeństwem informacji wymaga, aby poziom bezpieczeństwa fizycznego był adekwatny do ewentualnych zagrożeń i stanowił mocny element budowanego bezpieczeństwa informacyjnego w firmach.