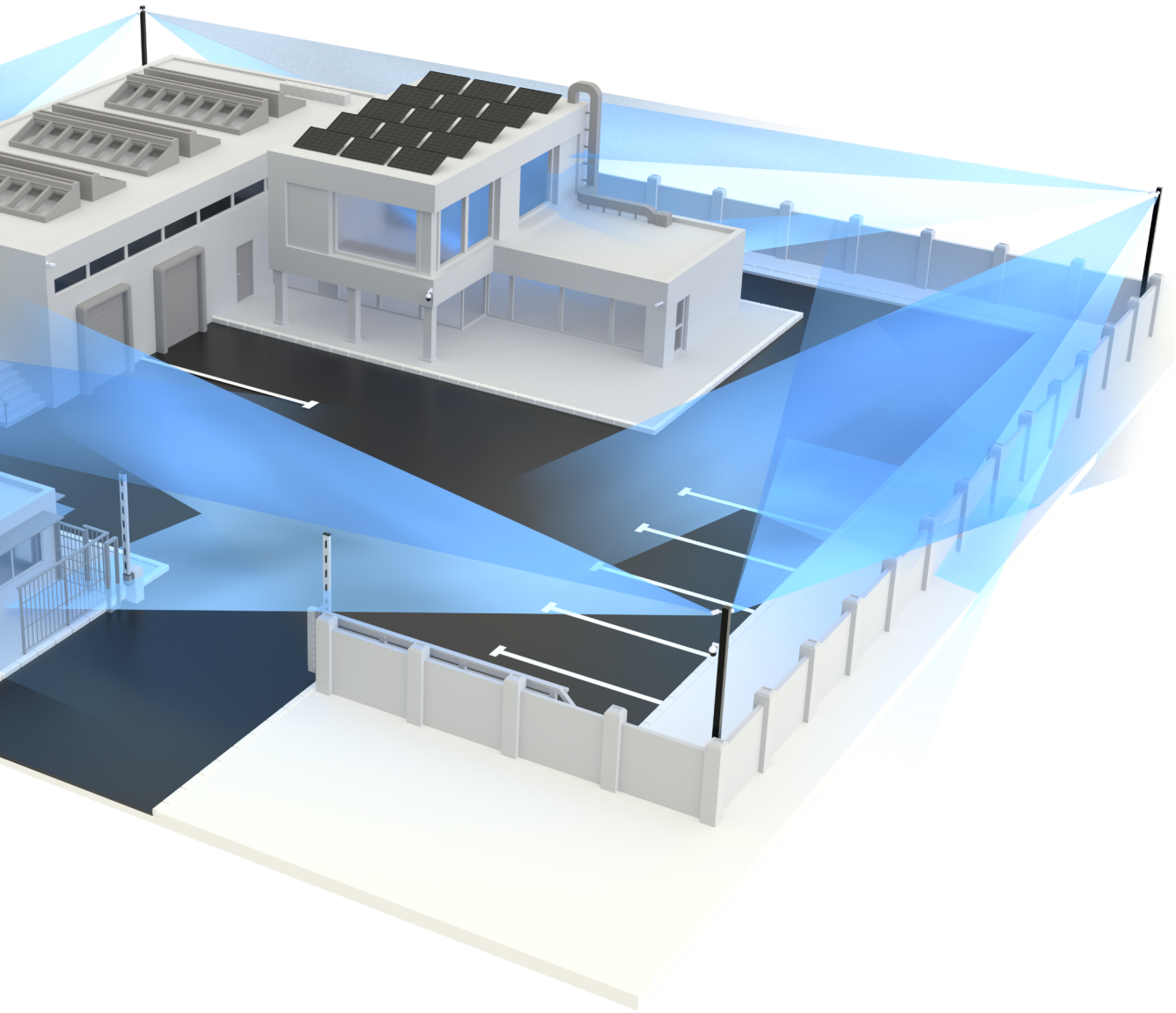


DELTAPRIME

Zmiana ochrony fizycznej na elektroniczną

Praktyczny poradnik Inwestora

Pora na zmianę

Zatwierdzasz płatności faktur za ochronę i masz poczucie, że wykazana kwota nie jest adekwatna do poziomu świadczonej usługi?

A może właśnie dostałeś aneks do umowy na ochronę fizyczną, który niesie za sobą jedynie wyższą stawkę za usługę, nie dając żadnej wartości w zamian?

Jeżeli rozważasz zmianę ochrony z fizycznej na elektroniczną to jesteś na dobrej drodze, aby w końcu przestać tracić setki tysięcy złotych rocznie w sferze, w której inni oszczędzają. Przed Tobą jednak ważne zadanie wyboru odpowiedniej technologii oraz partnera, który skutecznie przeprowadzi proces wdrożenia systemu monitoringu w Twojej organizacji.

Aby pomóc Ci w podjęciu tych kluczowych decyzji, przygotowaliśmy dla Ciebie krótkie opracowanie, z którego dowiesz się jak zakończyć proces inwestycji sukcesem już przy pierwszym podejściu.

1. Przygotuj procesy ochrony w Twojej organizacji

System ochrony elektronicznej to nie tylko dozór mienia. Jest to jego główna funkcja, ale nie jedyna. Prawdziwym zadaniem funkcjonalnego systemu jest realne zastąpienie agenta ochrony i wykonanie jego zadań w sposób nie tylko bardziej efektywny, ale też nie pozostawiający miejsca na błędy.

Jako przykład celu, który staramy się osiągnąć można wskazać gospodarkę kluczami. W tradycyjnym modelu to agent ochrony wydaje je pracownikom. Czasem weryfikuje ich uprawnienia do pobrania danego klucza, a czasem nie. Niekiedy zapisze ten fakt w ewidencji kluczy, a niekiedy nie. Raz upomni się, aby klucz wrócił na koniec dnia, a innym razem o tym zapomni. Dopiero w momencie, w którym ktoś inny będzie go potrzebował, rozpoczną się jego poszukiwania, a to przecież strata cennego czasu i pieniędzy.

O ile zawsze podpowiadamy naszym klientom, że najbezpieczniejszą metodą pełnienia nadzoru nad dostępem do danych stref/pomieszczeń obiektu jest kontrola dostępu i prawidłowa konfiguracja uprawnień, o tyle w przypadku, np. starszych i wielkopowierzchniowych obiektów nie zawsze jest to kosztowo efektywne. Z pomocą przychodzi depozytor kluczy. Programujemy w nim uprawnienia dla każdego klucza, maksymalny czas na jego oddanie, jak i miejsce odłożenia.

Dbamy też o to, by po przekroczeniu czasu zwrotu w systemie pojawiła się odpowiednia adnotacja, która pozwoli wyeliminować takie incydenty w przyszłości. Depozytor nigdy nie wyda klucza osobie, która nie ma do niego uprawnień. Ponadto zawsze odnotowuje każde zdarzenie w historii klucza, jak i samego użytkownika, który go pobrał. To właśnie przykład czynności, która została wykonana w sposób pożądany, czyli bardziej efektywny, tańszy i skuteczniejszy w kategoriach bezpieczeństwa obiektu.

Aby móc opracować koncepcję systemu zabezpieczeń, jako wykonawca musimy wiedzieć o wszystkich czynnościach i zadaniach jakie wykonują agenci ochrony. Nie dysponując odpowiednią wiedzą, pewna funkcjonalność najzwyczajniej może zostać pominięta.

Sposób działania każdego systemu można konfigurować, co w wielu przypadkach oznacza jedynie zmianę w warstwie oprogramowania, dzięki czemu odbywa się to bezkosztowo. Większym problemem staje się zmiana wymagająca fizycznej rozbudowy lub zmiany komponentów na takie, które będą wyposażone w określoną funkcjonalność. Z tego powodu warto przygotować koncepcję w sposób kompletny i przemyślany. W oparciu o nasze doświadczenie, sugerujemy klientom, aby na spotkanie dotyczące zakresu ochrony zaprosili również dodatkowe osoby, np. kierowników poszczególnych działów, którzy wchodzą w interakcje z ochroną. Pozwoli to uniknąć dodatkowych kosztów, uczyni system bardziej funkcjonalnym oraz przyspieszy proces jego projektowania i wdrożenia.

2. Dobierz odpowiedniego partnera do wdrożenia

Jak przy każdej inwestycji, nawiązanie współpracy z właściwym wykonawcą jest kluczowym czynnikiem powodzenia projektu. W kategoriach firm świadczących swoje usługi w zakresie ochrony mienia wybór wydaje się być olbrzymi. Niestety rzeczywistość jest zupełnie inna.

Nowoczesne systemy zabezpieczeń już na wstępie wymagają ogromu wiedzy z zakresu automatyki, programowania, uczenia maszynowego, czy sieci neuronowych. Te pojęcia częstokroć bywają całkowicie obce instalatorom, którzy od 20 lat montują proste systemy alarmowe i kamery - niejednokrotnie w dalszym ciągu analogowe. W praktyce oznacza to, że taka firma, nawet jeśli działa na rynku przez dwie dekady, stosuje rozwiązania technologicznie w sposób nieefektywny i bez wykorzystania pełni funkcjonalności sprzętowych, co może zgotować nie lada kłopoty.

Na co więc powinieneś zwrócić uwagę przy wyborze wykonawcy, któremu będziesz gotów powierzyć opracowanie oraz realizację systemu ochrony elektronicznej?

Odpowiedź na to pytanie przygotowaliśmy w formie kilku kluczowych punktów. Na etapie każdego z nich możesz odrzucać tych wykonawców, których propozycja nie spełnia Twoich oczekiwań lub znacząco odstaje od pozostałych. Punkty zostały przedstawione w takiej kolejności, aby móc w jak najkrótszym czasie odrzucić najsłabsze propozycje i tym samym wykorzystać pozostały czas na rozpatrzenie tych najwyższej wartości.

Zapytaj o czas gwarancji udzielanej na system

Wszyscy liczący się producenci systemów wizyjnych udzielają 36-miesięcznej gwarancji na swoje urządzenia. Mechanizm ochrony elektronicznej składa się z wielu różnych komponentów, jednak to kamery zarówno reprezentują najliczniejszą grupę w specyfikacji systemu, jak i największą składową budżetu. Pozostałe komponenty częstokroć są objęte krótszym, 24-miesięcznym okresem gwarancji. Jak jednak pokazuje praktyka, wybierając sprawdzone urządzenia renomowanych producentów możemy liczyć na to, że żywotność sprzętu zdecydowanie przekroczy okres 3 lat. Z naszego doświadczenia wynika, że jeżeli urządzenie nie ulegnie awarii w ciągu paru dni od momentu instalacji, to najpewniej nie dojdzie do niej też przez kilka kolejnych lat. Jeżeli coś ma się zepsuć, to zepsuje się od razu - jeszcze przed końcem montażu, a tym samym odbiorem systemu.

Sprawdź, czy rękojmia nie została w żaden sposób ograniczona

Ograniczenie rękojmi lub jej całkowite wyłączenie w przypadku umów B2B to częsta praktyka. Rękojmia jest jednak jedynym ratunkiem dla inwestora, który zakupił system niedziałający w oczekiwany sposób, czyli według ustalonej wcześniej koncepcji. Rynek jest pełen firm, które wręcz eksperymentują na klientach. Wykonują one systemy o zadanej funkcjonalności po raz pierwszy, bez wstępnego i wnikliwego przetestowania rozwiązania w ramach własnych struktur. Przypadki trafiających do nas Klientów na poprawę niedziałającego zgodnie z obietnicami systemu, moglibyśmy mnożyć bez końca. Podchodź zatem z dużą rezerwą do jakiejkolwiek próby ograniczenia rękojmi.

Poproś o zapisy umowy w zakresie serwisu, wsparcia, konserwacji oraz gwarancji ciągłości działania systemu

Systemy zabezpieczeń elektronicznych zwykle są niezawodne i odporne na awarie. Nie można jednak całkowicie wykluczyć takiego zdarzenia. Wówczas o sukcesie stanowią procedury postępowania. Zdecydowanie warto wiedzieć do czego jesteś zobowiązany Ty, a co leży po stronie wykonawcy zanim dojdzie do jakiejkolwiek awarii, np. w sobotę o 2:30 w nocy.

Za wszelką cenę staraj się unikać zapisów w umowie, które mówią o „podjęciu działań". Takie sformułowanie nie precyzuje, jak długo system będzie wyłączony z użycia oraz czy w ogóle zostanie przywrócona jego sprawność. Zapis pomija również najistotniejszy element - ile za taką usługę będziesz musiał dodatkowo zapłacić.

Najbardziej pożądanym rozwiązaniem w tym zakresie jest natychmiastowa reakcja serwisowa z określeniem maksymalnego czasu, przez jaki system może nie działać w ciągu całego roku w przypadku wystąpienia usterki. W naszej firmie jest to 10 godzin. Powyżej tego czasu zobowiązujemy się do zapewnienia ochrony zastępczej oraz pokrycia jej kosztów. Oczywiście warto mieć z góry ustaloną kwestię finansową dotyczącą ewentualnego serwisu. W Deltaprime opieka serwisowa jest zawarta w kwocie abonamentu, dzięki czemu nie narażamy naszych klientów na dodatkowe wydatki.

Dowiedz się, czy system będzie otwarty czy zamknięty

System zabezpieczeń elektronicznych i usługa ochrony elektronicznej (zwana często „monitoringiem wizyjnym") to dwie różne kwestie i często przedmiot dwóch, całkowicie odrębnych umów. Niejednokrotnie zdarza się, że inwestor ma już system lub jakąś jego cząstkę, np. w postaci alarmu, kontroli dostępu, czy kamer. Często zostają one zaadaptowane na potrzeby usługi ochrony elektronicznej. Na ogół to dobra informacja, gdyż znacząco obniża to koszt inwestycji. Gorzej jednak, gdy system będący w posiadaniu inwestora jest tak egzotyczny, że istnieje tylko jedna firma w kraju, która potrafi go obsługiwać lub ma wyłączność na jego serwisowanie. W takim przypadku mówimy o systemie zamkniętym.

Musisz się liczyć z tym, że potencjalnie firma obecnie świadcząca usługę ochrony może nie spełnić Twoich oczekiwań i może zajść konieczność jej zmiany. Upewnij się zatem, że platforma, w którą zamierzasz zainwestować spełnia kryterium systemu otwartego i w razie potrzeby z powodzeniem zostanie obsłużona przez inną firmę ochroniarską. Przestrzegając tej zasady, zyskujesz pewność, że nie będziesz musiał za system płacić dwa lub nawet więcej razy.

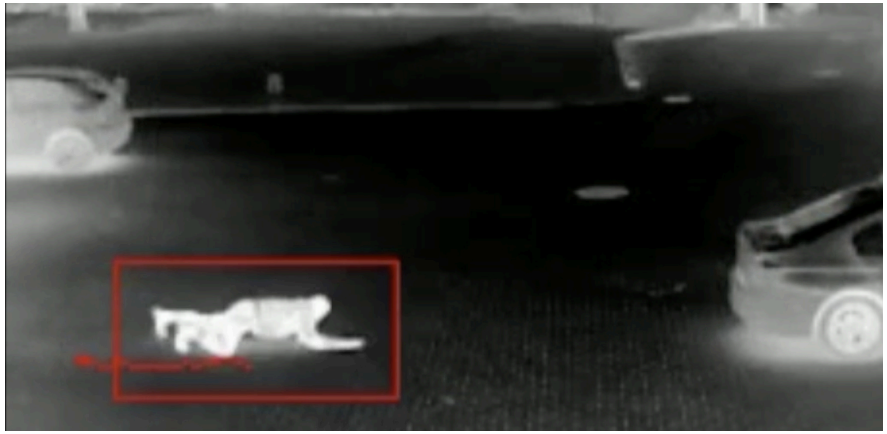
Poproś o instalację testową systemu oraz porównaj działanie

Otrzymane sygnały alarmowe z obiektu w postaci klatek referencyjnych i prealarmów (krótkich nagrań o długości zbliżonej do czterech sekund przed wystąpieniem zdarzenia i dwóch sekund po zdarzeniu) trafiają bezpośrednio do centrum monitorowania. Inwestor de facto nigdy ich nie widzi i tak naprawdę nie wie czy system wychwycił wszystkie zdarzenia, czy może tylko ich część.

Spory odsetek to fałszywe alarmy wywołane przez czynniki zewnętrzne, takie jak opady, poruszająca się na wietrze roślinność, cienie, światła czy zwierzęta, które nie stanowią potencjalnego zagrożenia. Jeżeli chcesz dokonać świadomego wyboru i zobaczyć, jak naprawdę działa system analityki obrazu, to już na wczesnym etapie weryfikacji ofert koniecznie poproś firmę o wykonanie instalacji testowej.

Instalacja testowa najczęściej jest oparta na dwóch-czterech kamerach w różnych technologiach, a jej przygotowanie zajmuje maksymalnie dwie godziny. Pozostawiona do testów na trzy-pięć dni, daje możliwość sprawdzenia skuteczności w typowych warunkach oświetleniowych oraz sytuacjach jakie zdarzają się na terenie Twojego obiektu.

W Deltaprime zawsze rekomendujemy naszym klientom przeprowadzenie takich testów, które najlepiej obrazują wszystkie istotne dla bezpieczeństwa obiektu kwestie oraz



uwypuklają zalety dobranych przez nas rozwiązań. W rzeczywistości jednak możesz spotkać się z różnym podejściem wykonawców do takiej propozycji. Nie brakuje firm, które odmawiają wykonania wspomnianej instalacji, a nawet rezygnują ze zlecenia!

Kiedy jednak już dojdzie do montażu instalacji testowej, powinieneś bacznie przyjrzeć się otrzymanym wynikom. Najgroźniejszym zjawiskiem, z jakim można się zetknąć jest niewykrycie rzeczywistego alarmu.

Dobrze sparametryzowany system da Ci nie więcej jak 10% fałszywych alarmów i nie pominie przy tym ani jednego prawdziwego. Jest to pożądana wartość. Oczywiście w wybranych warunkach (najczęściej industrialnych) ten współczynnik będzie o wiele niższy. Jeśli zweryfikujesz skuteczność działania systemu na tym etapie, w przyszłości nie będziesz musiał się martwić, czy w sytuacji zagrożenia wykryje on intruza.

Zobacz inne instalacje wykonawcy

Jeżeli ważna jest dla Ciebie estetyka wykonania instalacji, koniecznie poproś o wizytę referencyjną na dwóch lub trzech obiektach, których charakterystyka systemu jest zbliżona do Twojego. Zwróć uwagę, m.in. na wykorzystanie oryginalnych akcesoriów, takich jak puszki kamer, uchwyty lub sposób ułożenia kabli. Szybko dostrzeżesz też, czy instalacja została wykonana zarówno bezpiecznie, jak i estetycznie.

Wizyty referencyjne dadzą Ci również możliwość bezpośredniej rozmowy z klientem wykonawcy na temat świadczonej przez niego usługi. Koniecznie skorzystaj z tej okazji i zapytaj o tak ważne elementy, jak niezawodność systemu, reakcje firmy na alarmy, zachowanie w przypadku awarii systemu i opłaty pozaabonamentowe.

3. Poznaj sposób działania systemu

W 2020 r. otrzymaliśmy zaproszenie do rozmów w zakresie przejęcia i modernizacji świeżo zainstalowanego systemu ochrony elektronicznej, który - jak usłyszeliśmy - nie działa. Obiekt niesamowicie rozległy, o powierzchni 30 ha, zabezpieczony głównie po obwodzie. System został oparty na sieci kilkudziesięciu kamer termowizyjnych. W czym więc tkwił problem?

Wszystko stało się jasne, gdy tylko podjechaliśmy pod bramę obiektu. Na słupach spostrzegliśmy znane już nam kamery od popularnego w kraju dystrybutora, który przedstawiał nie do końca rzetelne informacje w kartach katalogowych sprzedawanych produktów. Nie tylko prezentował kamery jako własny produkt, mimo że w rzeczywistości był to jedynie rebranding, ale co najbardziej istotne - w karcie produktowej przedstawiał nieprawdziwe informacje dotyczące zasięgu - 100 m przy obiektywie o rozmiarze 6.8 mm. Od razu było dla nas jasne, że tak zbudowany system nie ma prawa zadziałać. Licząc samodzielnie efektywny zasięg takiej kamery, otrzymywaliśmy niespełna 34 m. Wyliczenia te znalazły również potwierdzenie w oficjalnej dokumentacji azjatyckiego producenta tych kamer, do której udało nam się dotrzeć. Podawał on zasięg 40 m, jednak zawsze należy pamiętać o tym, że dane z kart katalogowych pochodzą z dość „sterylnych" scen i bezpiecznie jest od nich odjąć 20-30% zasięgu.

Zatem na terenie obiektu zastaliśmy parędziesiąt słupów z kamerami rozstawionymi co 100 m, gdzie tylko ⅓ dystansu była zabezpieczona, a pozostałe ⅔ – całkowicie niechronione. W tym miejscu należy nadmienić, że cena jednej kamery wynosiła ok. 9000 zł netto. Nad reakcją klienta, który poznał prawdę nie trzeba się rozwodzić. Należy sobie jednak zadać pytanie: jak uniknąć takiej sytuacji?

Odpowiedź jest prosta: weryfikując wykonawcę zgodnie ze wskazanym przez nas poprzednim krokiem. Wówczas błędy w systemie zostałyby zauważone zarówno przy instalacji testowej, jak i podczas wizyt referencyjnych. To zaś mogłoby uchronić firmę przed wydaniem wielu pieniędzy na rozwiązanie, które - jak się okazało - nie miało prawa działać.

Zobacz, co jeszcze możesz sprawdzić, aby upewnić się, że nie tylko podobna sytuacja nie spotka i Ciebie, ale też sposób działania systemu będzie w 100% zgodny z Twoimi oczekiwaniami:

Sprawdź, czy technologia kamer została dobrana odpowiednio do obszaru

Każda technologia kamer ma swoje zastosowanie. W naszej działalności ich głównym zadaniem jest dostarczenie obrazu do systemu analityki obrazu. To bardzo mocno

zawęża ich wybór. Dla przykładu - producent kamer, z którym współpracujemy jest największym producentem tego typu urządzeń na świecie. W swojej ofercie ma co najmniej 200 różnych serii kamer. Ważne, aby wybrać z nich te, które mają największy potencjał technologiczny i dostarczają najbardziej wartościowy obraz do dalszej analizy.

Poniżej przedstawiamy najpopularniejsze technologie kamer i ich zastosowanie w usłudze ochrony elektronicznej:

- **kamery dzień/noc** - mają szersze zastosowanie w strefach zewnętrznych o nierównym kształcie, wymagających sporej liczby kamer oraz wszędzie tam, gdzie obszar jest słabo oświetlony. Zalecane są również do ochrony stref wewnętrznych. Koniecznie zwróć uwagę na odpowiedni dobór promienników podczerwieni, które powinny mieć wystarczająco daleki zasięg i odpowiednią moc, ale też nie powinny oślepiać innych kamer. Pożądane jest również, aby promienniki zewnętrzne były zamontowane pod kamerami. W ten sposób znacznie zmniejszamy szansę na to, że w oku kamery pojawią się, np. owady, czy pająki.

- **kamery full color** - świetnie współpracują z systemami analityki obrazu, jednakże wymagają dobrego oświetlenia terenu w nocy. Uwaga! Nie nadają się do ochrony nieoświetlonych stref wewnętrznych.

- **kamery termowizyjne** - bezkonkurencyjne w kategoriach skuteczności wykrycia, odporności na warunki atmosferyczne, a przede wszystkim zasięgu, w jakim można uchwycić wtargnięcie intruza. Pomimo, że ich cena jest wielokrotnie wyższa od kamer światła widzialnego, są one ekonomicznie uzasadnionym wyborem wszędzie tam, gdzie mamy do czynienia z dłuższymi dystansami, gdzie jedna kamera termowizyjna jest w stanie zastąpić nam parę innych.

Sprawdź, czy rozkład kamer został prawidłowo wykonany

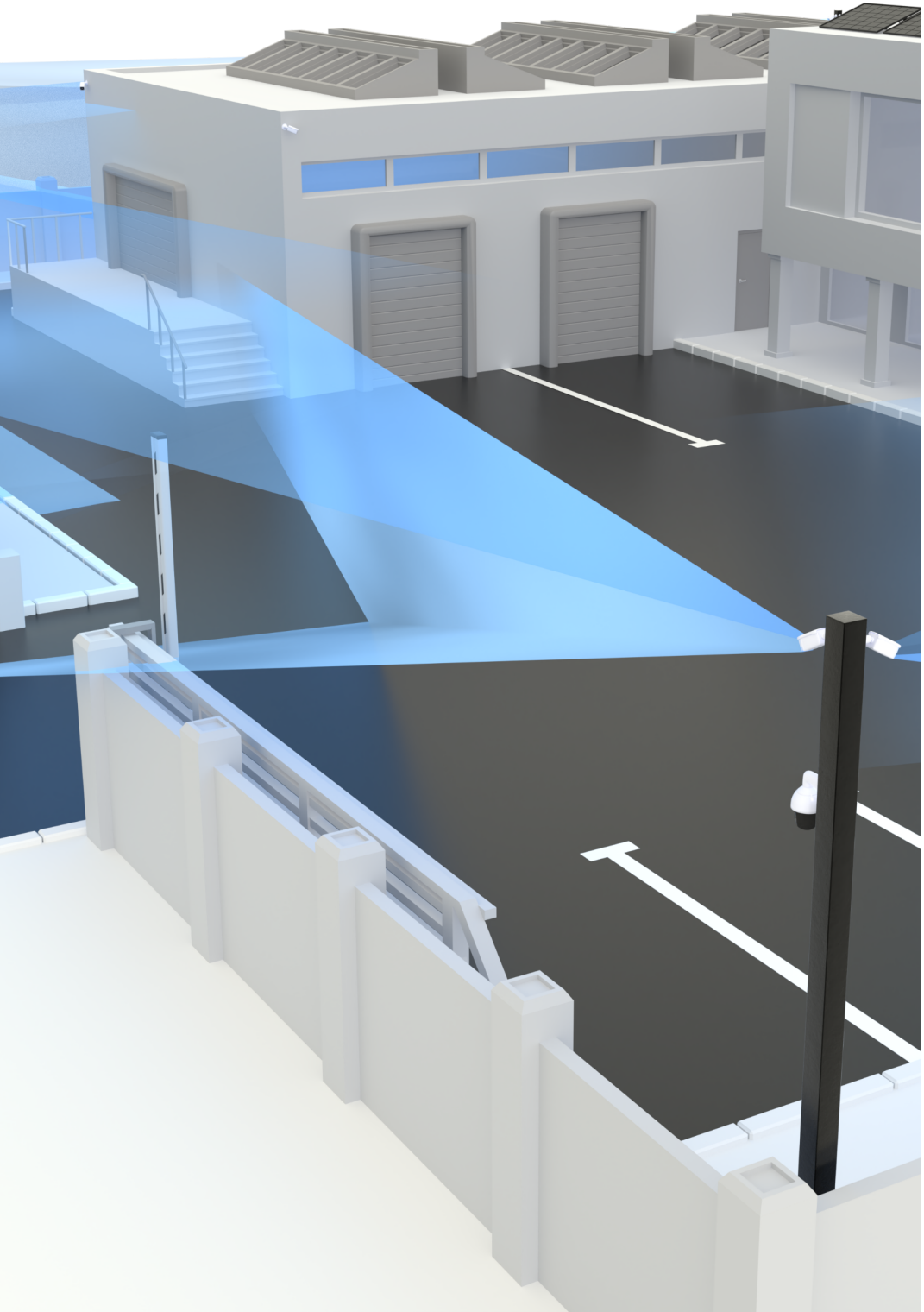
Jednym z najważniejszych zadań przy opracowywaniu koncepcji systemu jest odpowiednie rozmieszczenie jego elementów - w tym kamer. Znaczenie ma nie tylko ich ilość, ale również ich miejsce montażu. Zwróć uwagę na parę poniższych aspektów tak, aby system działał maksymalnie skutecznie i nie generował fałszywych alarmów:

Analityka w poprzek, a nie wzdłuż

Skuteczność wykrycia algorytmów analityki obrazu jest najwyższa, gdy intruz porusza się w poprzek sceny. Najlepszym przykładem jest widok z kamery zamontowanej wzdłuż ogrodzenia, która z jednej strony obejmuje teren zewnętrzny, a z drugiej już teren chronionego obiektu. Wysoka skuteczność takiego ustawienia wynika z paru czynników.

Przede wszystkim możemy liczyć na wczesne wykrycie i rozpoznanie intruza jeszcze po stronie zewnętrznej. Następnie jest on śledzony, a gdy tylko naruszy wyznaczoną granicę natychmiast otrzymujemy alarm. Dzięki takiej konfiguracji analityka nie traci czasu na wykrycie i klasyfikację obiektu (intruza), kiedy ten już przedostał się na chroniony teren.

Następnym czynnikiem przemawiającym za tym rozwiązaniem jest kwestia postrzegania przestrzennego sceny. Oprogramowanie analityki obrazu pilnuje tylko tego, aby obiekt nie przedostał się z jednej strony na drugą i nie musi zgłębiać kwestii odległości intruza od obiektu; czy znajduje się przy gruncie, czy też leci w powietrzu. Gdyby przyjąć, że dla każdego obiektu punktem styku jest jego podstawa to podskakujący człowiek w obrazie kamery termowizyjnej patrzącej na 300 metrów - a więc z bardzo niewielkim kątem pochylenia - mógłby łatwo zostać sklasyfikowany jako oddalony o 100 metrów od miejsca, w którym faktycznie się znajduje. Ułożenie scen kamer z uwzględnieniem potrzeb analityki obrazu daje wielokrotnie wyższą skuteczność działania całego systemu ochrony.



Perymetrycznie lub ze strefy podejścia

Opisane w powyższym punkcie kryterium jest szczególnie istotne w przypadku kamer o dalekim zasięgu, głównie termowizyjnych, montowanych z bardzo niewielkim kątem pochylenia. Obwodowe zabezpieczenie chronionego obiektu zawsze będzie uznawane za najlepsze. Zapewnia najwyższą skuteczność analityki, a co za tym idzie - bezpieczeństwa. Dodatkowo umożliwia pełną swobodę organizacji pracy firmy, np. na nocnej zmianie, podczas gdy cały teren jest chroniony, ale na terenie zakładu wciąż przebywają pracownicy. Kiedy zatem powinieneś zdecydować się na montaż kamer ze strefy podejścia, czyli, np. z elewacji budynku w stronę ogrodzenia?

Przede wszystkim dla podwójnego zabezpieczenia strefy obwodowej. Jest to sytuacja idealna dająca najwyższą skuteczność, zalecana szczególnie dla obiektów o średnim i wyższym stopniu ryzyka. Możesz również zdecydować się na takie rozmieszczenie kamer, jeżeli na terenie zewnętrznym Twojego obiektu nie jest przechowywane nic wartościowego lub teren ten nie wymaga ochrony w trakcie pracy zakładu (np. podczas dodatkowych zmian). Należy jednak mieć na uwadze fakt, że przy takim ułożeniu sceny, intruz może znajdować się już jakąś chwilę na strzeżonym terenie, zanim zostanie wykryty oraz poprawnie sklasyfikowany i oznaczony jako zagrożenie przez system analityki.

Sprawdź, czy zasięgi kamer zostały prawidłowo policzone

Wykrycie obiektu (osoba/pojazd - potencjalny intruz) przez system analityki obrazu wymaga spełnienia szeregu czynników. Takimi parametrami są: kształt, rozmiar i prędkość. Rozmiar ma szczególne znaczenie, gdyż obiekty znajdujące się zbyt daleko od kamery nie zostaną wykryte, a mocne podciągnięcie czułości algorytmów negatywnie wpłynie na liczbę generowanych fałszywych alarmów.

Dla każdej kamery oraz każdego systemu analityki obrazu, parametr zasięgu powinien zostać przeliczony indywidualnie. Uwzględnione powinny być takie parametry jak: miejsce montażu, sterylność sceny oraz jej oświetlenie.

Można jednak uśrednić otrzymane wyniki, które prezentujemy w tabeli poniżej. W tym miejscu warto zaznaczyć, że zdecydowanie odradzamy wykorzystanie w ochronie elektronicznej kamer światła widzialnego z obiektywem większym niż 6 mm.

W ich przypadku, już przy delikatnym zamgleniu lub niewielkich opadach atmosferycznych, pole widzenia ulega zbyt drastycznemu obniżeniu. Nawet jeżeli z pewnych przyczyn wykorzystywana jest kamera zmiennoogniskowa z nastawą maksymalną do 12 mm, powinno się skorzystać tylko i wyłącznie z pierwszej połowy zakresu regulacji. Jeżeli na projekcie, który otrzymałeś, kamera z obiektywem 2.8 mm odpowiada za obszar 50 - 100 metrów (z czym często się spotykamy), zdecydowanie powinieneś poprosić o przedstawienie obliczeń w zakresie zasięgów, a najlepiej o wykonanie instalacji testowej.

Kamery światła widzialnego (rozdzielczość minimalna Full HD)		**Kamery termowizyjne** (rozdzielczość 384 × 288 px)	
Rozmiar obiektywu (mm)	Zasięg (m)	Rozmiar obiektywu (mm)	Zasięg (m)
2.8	30	7	45
4	38	15	115
6	52	35	235

Zweryfikuj funkcjonalność oraz sposób realizacji poszczególnych zadań

Każdy system sterowany jest przez mniej lub bardziej zaawansowane funkcje logiczne. Programowanie może przebiegać na wiele sposobów, jednak pewne specyficzne funkcjonalności mogą wynikać z odpowiedniego doboru komponentów na etapie opracowywania koncepcji. Zadbaj o dobre zrozumienie zasad funkcjonowania całego systemu.

Lepiej zadać dwa - trzy pytania więcej lub poprosić o szczegółowe wyjaśnienia niż zdziwić się podczas odbioru, że sposób działania całkowicie nie wpisuje się w potrzeby Twojej firmy. W Deltaprime zawsze przygotowujemy opracowanie, które w jasny i czytelny sposób, godzina po godzinie oraz przypadek za przypadkiem, przedstawia jak system się zachowa, jak zareaguje i co się wydarzy, gdy zaistnieją dane przesłanki.

Sprawdź, do jakich elementów systemu otrzymasz dostęp oraz kto będzie administratorem systemu

Na etapie zatwierdzania koncepcji upewnij się do jakich elementów systemu otrzymasz dostęp oraz w przypadku, których będziesz odpowiedzialny za administrację, zarządzanie poświadczeniami, użytkownikami, itd. W Deltaprime dział supportu stanowi pełne wsparcie dla klientów. Kwestia ustawień i administracji systemów może pozostać po naszej stronie podczas całego okresu współpracy.

Dowiedz się, w jaki sposób będziesz włączał i wyłączał czuwanie

Sterowanie stanem uzbrojenia to niezwykle istotne zagadnienie. Odpowiednio dobrane rozwiązanie daje olbrzymie możliwości tworzenia ciągów logicznych wymaganych przy skomplikowanych strukturach i obiektach. Ponadto tworzy hierarchię uprawnień, loguje zdarzenia, ułatwia zarządzanie i daje możliwość obsługi całości, np. z aplikacji (dla wybranych użytkowników w Twojej firmie).

Często można się spotkać z takimi rozwiązaniami jak telefon do centrum monitorowania, czy stały, ustalony na sztywno harmonogram. Metody te drastycznie obniżają poziom bezpieczeństwa całego systemu, nie dają kontroli ani wiedzy w zakresie zdarzeń historycznych, a ostatecznie nie są elastyczne względem potrzeb użytkowników. Przykłady?

Trzeba pamiętać o zgłoszeniu zmian za każdym razem, kiedy trafia się święto w dzień pracujący lub praca w dzień wolny; jeżeli firma kończy zmianę wcześniej to zawsze ktoś musi pamiętać o przesterowaniu harmonogramu. Ponadto intruz może łatwo podszyć się pod użytkownika i nakazać wyłączenie czuwania na obiekcie. Odpowiedni wybór sterowania stanem uzbrojenia to ułamek inwestycji w cały system - warto postawić na sprawdzone rozwiązanie, które dopasuje się do Twoich potrzeb, a nie na odwrót.

4. Postaw na sprawdzone technologie i rozwiązania

Technologia technologii nierówna. Jednak, gdy w grę wchodzi bezpieczeństwo i majątek Twojej firmy, zdecydowanie warto szerzej rozeznać temat. Dzięki paru poniższym punktom dowiesz się, na co zwrócić uwagę, aby system, w który zamierzasz zainwestować wykonał swoje zadanie i spełnił Twoje oczekiwania.

Sprawdź system analityki obrazu

Największą część pracy w zakresie bezpieczeństwa Twojej firmy bierze na siebie system analityki obrazu. Jeżeli system nie zadziała, czyli nie wykryje, nie podniesie alarmu, nie prześle go w sposób skuteczny - to w przypadku zdecydowanej większości agencji ochrony, które odpowiadają jedynie za prawidłową reakcję na otrzymane sygnały, pozostaniesz z nie lada problemem. Właśnie z tego powodu jednym z najważniejszych elementów, jakie musisz sprawdzić jest system analityki obrazu. Oto parę sprawdzonych sposobów na to, jak łatwo to zrobić:

Sprawdź certyfikaty

Najbardziej renomowaną instytucją na świecie do certyfikowania systemów zabezpieczeń jest brytyjskie CPNI (Centre for the Protection of National Infrastructure - The UK Government's National Technical Authority for Physical and Personnel Protective Security). Pod poniższym linkiem znajdziesz zbiór wszystkich certyfikowanych rozwiązań. Jako podkategorię wybierz „Video Analytics".

https://www.cpni.gov.uk/cse-categories/detection-systems

Poproś o instalację testową systemu oraz porównaj działanie

Krok ten dokładnie opisaliśmy przy punkcie drugim. W celu podniesienia poprzeczki, warto poprosić wykonawców o podłączenie dokładnie tych samych kamer do swoich systemów analityki. Wówczas test będzie jeden do jednego. Zobaczysz, który z systemów działa stabilniej, pewniej i generuje mniej fałszywych alarmów.

Nie daj się zwieść - jeśli system zbyt często podnosi fałszywy alarm (wartość maksymalna to 10% wszystkich zdarzeń) oznacza to, że wykonawca zwiększył czułość systemu na potrzeby testu, a po instalacji ją obniży, aby nie narażać nikogo na dodatkowe koszty. Utrzymanie liczby fałszywych alarmów na akceptowalnym poziomie jest kluczowe.

Zweryfikuj czas przesyłu zdarzenia oraz jego wideoweryfikację

Czas jest kluczowym czynnikiem. Zarówno wykrycie, jak i reakcja muszą nastąpić natychmiastowo, aby interwencja miała realną szansę się powieść. Intruz nie będzie przecież czekał pod kamerą parunastu minut, aż operator wezwie go do opuszczenia obiektu. Nie będzie czekał ani sekundy!

Jeżeli reakcja operatora nie nastąpi w przeciągu chwili to cały system, włączając w to nagłośnienie, traci sens. Aby sprawdzić czynnik czasu, poproś o próbne włączenie instalacji testowej do sieci monitoringu i wywołaj kontrolne alarmy o wybranej przez siebie porze. Warto również zapytać o ten element usługi obecnych kontrahentów wykonawcy podczas wizyt referencyjnych.

Zwróć uwagę na podtrzymanie zasilania

Jednym z dwóch elementów świadczących o odporności systemu na sabotaże jest podtrzymanie zasilania całości instalacji na wypadek odłączenia napięcia sieciowego. Istotne jest, aby podtrzymanie systemu dotyczyło każdego jego elementu, włączając w to również punkty bezprzewodowe.

Podczas weryfikacji tego zagadnienia zwróć szczególną uwagę na sposób monitorowania samej informacji o zaniku. Agencja ochrony, którą wybierzesz musi wiedzieć o każdym zaniku napięcia, w każdym punkcie zasilania i dla każdego elementu systemu. Brak tej wiedzy nie da możliwości jakiejkolwiek reakcji, a to z kolei może doprowadzić do powstania wielogodzinnej wyrwy w systemie ochrony. W scenariuszu praktykowanym w Deltaprime, bezprzewodowy punkt kamerowy przechodzi na wielogodzinne zasilanie bateryjne, a operator centrum monitorowania natychmiast otrzymuje informację o szczegółach zdarzenia wraz z precyzyjną lokalizacją zaniku. Taka praktyka w połączeniu z odpowiednią informacją pozwala na bezzwłoczne podjęcie skutecznych działań i uniknięcie jakichkolwiek przerw w ochronie.

Zwróć uwagę na liczbę torów transmisji

Drugim elementem świadczącym o odporności systemu na sabotaże jest wielotorowość transmisji danych. Jest ona niezbędna do nieprzerwanej pracy systemu. Ochrona obiektu wymaga, aby użyte zostały co najmniej dwa niezależne łącza internetowe oraz technologia, która pozwoli na ich sprawne i automatyczne przełączanie względem zmieniającej się sytuacji. W Deltaprime zawsze zapewniamy co najmniej dwa tory transmisji, dodatkowo wzbogacone o telemetrię. Takie podejście sprawia, że prawdopodobieństwo całkowitej utraty łączności spada niemalże do zera.

Zwróć uwagę na informacje o sabotażach systemu (kamer)

Nowoczesne systemy analityki obrazu, oprócz najważniejszej funkcjonalności w postaci wykrycia wtargnięcia, oferują szereg dodatkowych algorytmów. W kategoriach bezpieczeństwa Twojego obiektu jednym z istotniejszych jest wykrycie zmiany sceny. Dochodzi do niej za każdym razem, kiedy kamera zostaje przysłonięta, oślepiona lub zmianie ulegnie jej ułożenie. Mówimy wówczas o sabotażu kamery.

Czasem wystarczy drobny obrót kamery lub pochylenie jej o 1-2 stopnie, aby otworzyć sobie możliwość do przedostania się na teren niezauważonym lub dokonania innego czynu (np. kradzieży) wewnątrz przedsiębiorstwa przez osoby w nim zatrudnione. Częstym procederem, którego dopuszczają się pracownicy jest zasłonięcie kamery paletą lub wózkiem widłowym. Bez względu na przyczynę, istotne jest by system zidentyfikował sabotaż kamery, natychmiast podniósł alarm oraz przesłał go do wideoweryfikacji przez operatora centrum monitorowania, który podejmie działania stosowne do zaistniałej sytuacji.

Zwróć uwagę na okres archiwizacji oraz jakość nagrań z monitoringu

Nie jest dobrą praktyką przechowywanie nagrań w słabej jakości, tj. w niższej rozdzielczości, z obniżonym bitrate'em oraz niewielką liczbą klatek na sekundę. Wartość kryminalistyczna takiego materiału dowodowego w procesach sądowych oraz odszkodowawczych zwykle okazuje się znikoma lub wręcz zerowa. Polecamy Ci określenie minimalnej liczby dni archiwizacji materiału wideo i zastrzeżenie, że jego jakość powinna być niemal bezstratna. Naszym standardowym ustawieniem dla rejestrowanego strumienia to bitrate 4Mbps, 25 fps oraz kodowanie H.265. Śmiało możesz podać te wartości jako wytyczne.

Dowiedz się, w jaki sposób zabezpieczane będą dane i obrazy przesyłane z Twojego systemu

W erze szerzącej się cyberprzestępczości skończyło się miejsce na lekkomyślne i bezkarne podejście do ochrony informacji. Inwestorzy częstokroć przykładają niezwykłą uwagę do prawidłowego zabezpieczenia własnej infrastruktury, a następnie pozwalają firmom ochroniarskim na otwarcie w niej szeregu luk. Na dodatek ma to związek z produktem, który powinien owo bezpieczeństwo zapewniać. Do analizy rozwiązań poszczególnych wykonawców zaangażuj na tym etapie swojego opiekuna IT.

Jako zaufana osoba z pewnością obiektywnie spojrzy na rozwiązania proponowane przez poszczególnych wykonawców. Zdecydowanie nie pozwoli na otwieranie żadnych publicznych portów w obszarze Twojej infrastruktury i przepuszczanie przez nie całego ruchu. W Deltaprime, chcąc sprostać współczesnym wyzwaniom cyberbezpieczeństwa, opracowaliśmy metodę bezpiecznego połączenia pomiędzy naszymi serwerami a obiektami klientów. Stworzyliśmy prywatną sieć, niewidoczną z poziomu internetu, wewnątrz której komunikacja pomiędzy punktami końcowymi jest całkowicie zaszyfrowana. Nasz algorytm o długości klucza 256 bitów, zdecydowanie wpisuje się we współczesne dobre praktyki cyberbezpieczeństwa.

5. Nie zawieraj umowy na fikcyjną ochronę

Wiesz już doskonale jak ma wyglądać ochrona elektroniczna w Twojej organizacji. Wybrałeś wykonawcę, który wie co robi. Zweryfikowałeś koncepcję i sprawdziłeś zaplecze technologiczne. Świetna robota! Na tym etapie możesz być pewien, że system na pewno sprawdzi się w Twojej firmie, a do tego będzie bardzo dobrze działał! Został Ci jeszcze jeden, ostatni punkt, który pominięty może z łatwością zniweczyć wszystkie wcześniejsze ustalenia.

Odpowiedzialność za działanie systemu, czy tylko za reakcję na otrzymane sygnały?

Nie ulega wątpliwości, że aspekty prawne to bardzo ważne zagadnienie. W umowach na ochronę elektroniczną w Polsce przyjęły się dwa podejścia. Zdecydowana większość agencji ochrony zastrzega sobie odpowiedzialność jedynie za prawidłową reakcję na otrzymane sygnały alarmowe z monitorowanego obiektu. Jeżeli system nie zadziała - nie ma odpowiedzialności. Jeżeli alarm nie zostanie wygenerowany i przesłany - nie ma odpowiedzialności. Jeżeli cokolwiek się stanie na miejscu - system jest Twój - agencja sygnału nie otrzymała - a zatem nie ponosi za to odpowiedzialności. Pozostałe, nieliczne firmy ochroniarskie faktycznie biorą odpowiedzialność zarówno za reakcję, jak i za prawidłowe działanie systemu. To tylko jeden krótki, jednozdaniowy zapis w umowie, lecz w rzeczywisty sposób definiuje on, czy usługa, którą zamierzasz zakupić będzie faktyczną ochroną Twojego biznesu, czy zwykłą fikcją.

Opłaty dodatkowe

Jeżeli rozważasz zmianę ochrony fizycznej na elektroniczną oznacza to, że potrafisz dobrze liczyć i już wiesz, że ta inwestycja zwróci Ci się w mgnieniu oka. O ile w tej chwili, najpewniej wydatki na ochronę fizyczną przyprawiają Cię o ból głowy, to - uwaga! - ochrona elektroniczna również może być obarczona wysokimi kosztami.

Zweryfikuj szczegóły oferty potencjalnego wykonawcy i sprawdź, jakie inne opłaty występują w umowie poza kwotą główną abonamentu. Z naszej analizy rynku wynika, że im niższa kwota proponowanego abonamentu, tym więcej opłat dodatkowych.

Jako przykłady można podać:

- wideoweryfikacje alarmów ponad ustalony limit,
- nieuzasadnione interwencje,
- podjazdy patroli,
- czynności serwisowe z zakresu standardowej obsługi,
- konserwacje i przeglądy systemu,
- wydawanie raportów.

W Deltaprime reprezentujemy tę drugą grupę. Nasi klienci otrzymują abonament w stałej wysokości. Nie musisz martwić się o naliczanie dodatkowych opłat za fałszywe alarmy, nieuzasadnione interwencje, czy przyjazd serwisantów w niedzielę, jeśli okaże się to konieczne. Tym samym zyskasz spokój i przewidywalnego partnera w biznesie, dzięki czemu będziesz mógł precyzyjniej zarządzać budżetem Twojej firmy.

Awarie systemu

Po odpowiedzialności i kosztach pozostaje omówienie ostatniego z trzech najważniejszych elementów umowy na usługi ochrony elektronicznej. Będziesz spał zdecydowanie spokojniej jeżeli z góry będziesz wiedział, jakie procedury obowiązują w firmie, której zamierzasz powierzyć bezpieczeństwo swojego przedsiębiorstwa. O sytuacjach i zapisach kontraktowych, z jakimi można się spotkać dałoby się napisać oddzielne opracowanie.

Wspomnimy więc o najkorzystniejszym dla klienta sposobie rozwiązania tej kwestii, który wypracowaliśmy na przestrzeni lat w Deltaprime. Zapewnia on brak jakichkolwiek zmartwień związanych z awariami i serwisem, gdyż poza cyklicznymi przeglądami całości systemu, zdecydowaliśmy się również zagwarantować usunięcie każdej usterki sprzętowej w ramach comiesięcznego abonamentu, bez dodatkowych kosztów oraz w czasie przewidzianym w SLA.

Jak widzisz, decyzja o zmianie systemu ochrony potrafi być bardzo złożonym zagadnieniem. Wierzymy, że po lekturze niniejszego opracowania unikniesz wielu błędów, które popełnili inni. Przejście z ochrony fizycznej na elektroniczną, czyli wdrożenie przemyślanego systemu jest zdecydowanie słusznym krokiem dla Twojego przedsiębiorstwa. Zmiana ta nie tylko pozytywnie wpłynie na finanse firmy, ale również realnie poprawi jej bezpieczeństwo.

Czy w trakcie czytania niniejszego opracowania zrodziły się jakieś pytania, na które chciałbyś poznać odpowiedź?

A może chciałbyś omówić z nami swoją koncepcję dotyczącą systemu ochrony elektronicznej?

Zespół Deltaprime pozostaje do Twojej dyspozycji!

www.deltaprime.pl