BIAŁA KSIĘGA

Ochrona obwodowa za pomocą inteligentnego dozoru

Omówienie dostępnych czujników, możliwych zastosowań i najważniejszych czynników, które należy uwzględnić podczas projektowania przyszłościowego rozwiązania bezpieczeństwa dla różnych branż

Lipiec 2021

AXIS COMMUNICATIONS

Spis treści

1 Streszczenie

Ogrodzenie często stanowi zasadniczy element „zewnętrznej warstwy" zabezpieczeń obiektu, pełniący funkcję bariery, zasłony lub czynnika odstraszającego w stosunku do ludzi i zwierząt. Ponieważ każda bariera fizyczna może jedynie opóźnić lub utrudnić wtargnięcie na teren chronionego obiektu, często stosowane są inne elementy zwiększające skuteczność ogrodzenia.

Wzdłuż ogrodzeń stosowane są różnego rodzaju detektory. Detektory drutowe instaluje się zgodnie z przebiegiem ogrodzenia, a czujniki radarowe (mikrofalowe), bariery na podczerwień lub lasery rozmieszcza się w strategicznych miejscach.

Wszystkie rodzaje detektorów mogą wszczynać fałszywe alarmy, wywoływane na przykład przez zwierzęta, poruszające się drzewa i inne rośliny oraz złe warunki pogodowe. Mogą też występować inne czynniki ograniczające, takie jak konflikty częstotliwości w przypadku czujników mikrofalowych czy fizyczne ograniczenia w środowisku instalacji.

Kamery mają oczywiste zalety w sytuacjach, gdy chodzi o monitorowanie rozległego obszaru lub wielu lokalizacji. Nowoczesne sieciowe rozwiązania wizyjne łączą dostępną w kamerach moc obliczeniową i sztuczną inteligencję. Typowa dla kamer skalowalność, skuteczność i zdolność do odstraszania sprawia, że mogą one być bardzo ekonomicznym dodatkiem do systemu bezpieczeństwa.

Chociaż kamery i oprogramowanie do detekcji ruchu poszerzyły zakres i możliwości ochrony obwodowej, częstym ograniczeniem tych rozwiązań jest brak zdolności do detekcji w trudnych warunkach pogodowych. Kamery termowizyjne — odpowiednio skalibrowane i powiązane z narzędziami do analizy wideo — mogą zapewnić skuteczny dozór i monitoring w każdych warunkach oświetleniowych oraz niemal każdych (poza naprawdę ekstremalnymi) warunkach pogodowych.

Na przestrzeni lat funkcje analizy wideo przeszły znaczną ewolucję i obecnie są powszechnie dostępne, nawet w kamerach przeznaczonych do monitoringu domowego. Oprogramowanie analityczne może znacznie zmniejszyć zapotrzebowanie na pamięć masową, ponieważ rejestruje wyłącznie materiał wizyjny zawierający interesującą aktywność. W związku z tym, że zarejestrowany materiał wizyjny jest w maksymalnym stopniu przetwarzany w samej kamerze, obciążenie sieci jest znacznie mniejsze, ponieważ kamery przesyłają wyłącznie materiał interesujący odbiorcę. Ma to oczywiste zalety w scenariuszu z pomieszczeniem kontrolnym.

Tak jak w przypadku każdego środka bezpieczeństwa ocena rozwiązania ochrony obwodowej powinna być odpowiednia i proporcjonalna. Co oczywiste, przede wszystkim należy wziąć pod uwagę potencjalne zagrożenia.

Coraz częstszą praktyką jest zintegrowane podejście do bezpieczeństwa, które uwzględnia dane i opinie pochodzące z innych działów, na przykład IT i operacyjnego. Obejmuje ono konieczność jak najwcześniejszego zaangażowania osób odpowiedzialnych za kwestie inżynieryjne.

Zazwyczaj bardzo trudno jest wykazać zwrot z inwestycji w rozwiązanie bezpieczeństwa mające na celu zapobieganie incydentom. Wynika to głównie z braku potencjalnych przychodów, które można by porównać z kosztami. Istnieje jednak możliwość wykazania bardziej namacalnego zwrotu z inwestycji: dobrym przykładem są rozwiązania, które nie tylko alarmują personel o podejrzanym zachowaniu czy wtargnięciu, ale także automatycznie inicjują odpowiednią reakcję.

2 Wprowadzenie

Kiedyś elektroniczne rozwiązania ochrony obwodowej były stosowane wyłącznie w newralgicznych obiektach rządowych i komercyjnych lub posiadłościach najzamożniejszych ludzi. Postęp technologiczny,

rosnąca konkurencja rynkowa i związana z nią redukcja kosztów sprawiły, że obecnie stosunkowo nowoczesne rozwiązania są dostępne na znacznie większą skalę.

A zatem z czego składa się nowoczesne rozwiązanie ochrony obwodowej? Jakie technologie są w nim stosowane i jak mogą one dać zarówno pewność, jak i autentyczną ochronę?

W tym dokumencie omówiono wybrane metody ochrony obwodowej z wykorzystaniem czujników, a także technologie stosowane w dostępnych rozwiązaniach.

3 Rozwiązania ochrony obwodowej

3.1 Rozwiązania fizyczne

Rozwiązania fizyczne często stanowią zasadniczy element „zewnętrznej warstwy" wieloskładnikowego systemu zabezpieczeń obiektu. Zazwyczaj obejmują one ogrodzenie na obwodzie obiektu, często zbudowane z siatki drucianej lub zgrzewanej, w panelach zgrzewanych lub betonowych. Takie ogrodzenie pełni wiele funkcji, w tym przede wszystkim funkcję fizycznej bariery spowalniającej lub zniechęcającej intruzów. Ogrodzenie może także zapobiegać inwigilacji przez zasłanianie określonych zasobów, a ponadto odstrasza zwierzęta i zapobiega ich wchodzeniu na teren obiektu. Aby zwiększyć skuteczność ogrodzenia, można też zastosować takie elementy jak urządzenia zapobiegające wspinaniu się, wyznaczone drogi dojazdowe, urządzenia zapobiegające przekraczaniu i ekrany ogrodzeniowe.

Jednak bariery fizyczne mogą jedynie spowolnić intruza. Dlatego na obwodzie obiektu warto dodatkowo zastosować technologię automatycznej detekcji wtargnięć, która udostępnia weryfikowalne alarmy dostarczane w czasie rzeczywistym, dane lokalizacyjne, śledzenie celów oraz możliwość wyodrębniania materiału dowodowego i danych na potrzeby późniejszego wyjaśniania incydentów.

3.2 Detekcja wtargnięć na fizycznym obwodzie obiektu

Do zabezpieczenia długich obwodów często używa się różnego rodzaju „detektorów" drutowych. Zazwyczaj są one zakopane w ziemi lub zamontowane na ogrodzeniu, odwzorowują jego przebieg i nie muszą tworzyć linii prostych. Umożliwiają również zabezpieczanie narożników i **martwych pól**. Niektórzy dostawcy oferują ogrodzenia wyposażone w rozwiązania do automatycznej detekcji.

Jak każde rozwiązanie do detekcji, również detektory drutowe mogą wyzwalać fałszywe alarmy, czyli tzw. „fałszywe trafienia". Do częstych przyczyn fałszywych trafień należą zwierzęta, poruszające się drzewa i inne rośliny oraz złe warunki pogodowe. Rozwiązania drutowe sprawdzają się najlepiej w połączeniu z dozorem wizyjnym. Materiał wizyjny pozwala nie tylko zweryfikować wtargnięcie, ale też sprawdzić przyczynę alarmu. Detektor drutowy jedynie alarmuje o wtargnięciu — nie przekazuje informacji na temat liczby intruzów ani innych danych wymaganych do przygotowania reakcji.

3.3 Inne czujniki do detekcji wtargnięć

Inne detektory wtargnięć, takie jak czujniki radarowe (mikrofalowe), bariery na podczerwień lub lasery, mogą być rozmieszczone w strategicznych punktach wokół ogrodzenia lotniska. Również w ich przypadku brak prawidłowego przestrzegania zasad instalacji może doprowadzić do takich problemów jak fałszywe trafienia oraz ograniczona odległość i wysokość detekcji.

Szczególne problemy może rodzić zastosowanie radaru na obwodzie obiektu, jeśli na jego terenie używane są też inne urządzenia elektroniczne. Mogą one korzystać z tego samego spektrum częstotliwości i chociaż

staranny dobór częstotliwości lub obniżenie mocy często pozwala ograniczyć zakłócenia, konsekwencją może też być zmniejszenie skutecznego zasięgu urządzenia.

4 Rozwiązania oparte na technologii wizyjnej

4.1 Zastosowanie kamer wideo

Znane z przeszłości autonomiczne systemy CCTV w niewielkim stopniu przypominają dzisiejsze nowoczesne rozwiązania oparte na kamerach sieciowych. W nowoczesnych rozwiązaniach sieciowych można połączyć przetwarzanie materiału w kamerze i mechanizmy sztucznej inteligencji. Jednak ten poziom technologii jest dostępny od niedawna i wciąż znajduje się we wczesnej fazie rozwoju.

Kamery mają oczywiste zalety w sytuacjach, gdy chodzi o monitorowanie rozległego obszaru lub wielu lokalizacji. Typowa dla kamer skalowalność, skuteczność i zdolność do odstraszania sprawia, że mogą one być bardzo ekonomicznym dodatkiem do systemu bezpieczeństwa.

W zależności od lokalnych przepisów kamer można używać do monitoringu wykraczającego poza fizyczne ogrodzenie obiektu, zyskując dodatkowy bufor dozoru i dając operatorowi więcej czasu na reakcję. Rozwiązania obejmujące analizę wideo pozwalają wyzwolić alarm po spełnieniu określonych kryteriów. Na przykład gdy ktoś podejdzie do ogrodzenia na odległość mniejszą niż 50 metrów, rozlega się alarm dźwiękowy, natomiast gdy ta sama osoba przez dłuższy czas przebywa w danej strefie lub zbliży się na mniej niż 10 metrów, poziom alarmu rośnie.

4.2 Termograficzne rozwiązania dozoru wizyjnego

Połączenie kamer do dozoru wizyjnego oraz oprogramowania do detekcji ruchu poszerzyło zakres i możliwości rozwiązań ochrony obwodowej, umożliwiając przejście od prostej detekcji do złożonej analizy wtargnięć. Jednak skuteczność dozoru wizyjnego może znacznie spaść w niekorzystnych warunkach pogodowych, które ograniczają zdolności detekcyjne kamery.

Rosnąca dostępność technologii termowizyjnej upowszechniła jej stosowanie w obszarze ochrony obwodowej. Kamery termowizyjne (inaczej termograficzne) — odpowiednio skalibrowane i powiązane z narzędziami do analizy wideo — mogą zapewnić skuteczny dozór i monitoring w każdych warunkach oświetleniowych oraz niemal każdych (poza naprawdę ekstremalnymi) warunkach pogodowych. Czujniki oparte na technologii termowizyjnej cechują się znakomitym kontrastem w porównaniu z typową kamerą na światło widzialne i dlatego dobrze się sprawdzają w ochronie obwodowej, oferując znacznie lepsze możliwości detekcji wtargnięć.

Czujniki termowizyjne tworzą obraz na podstawie promieniowania podczerwonego emitowanego przez takie obiekty jak pojazdy i ludzie. W połączeniu z narzędziami do analizy wideo nowoczesne kamery termowizyjne dysponujące wystarczającą mocą obliczeniową potrafią rozróżniać różne rodzaje obiektów-intruzów i mogą powiadamiać operatora na podstawie określonego zbioru warunków, takich jak kierunek i prędkość przemieszczania się osoby lub pojazdu. Tradycyjne kamery również dają tę możliwość, ale potrzebują światła widzialnego. Ten rodzaj kamer omówiono w kolejnej sekcji.

4.3 Kamery na światło widzialne

Wszystkie zwykłe kamery dozorowe na światło widzialne potrzebują oświetlenia naturalnego lub wzmocnionego w celu tworzenia obrazów. Oświetlenie wspierające dozór wizyjny to odrębny, ważny obszar specjalizacji, na temat którego napisano wiele osobnych dokumentów. Mimo to warto podkreślić

ten oczywisty, lecz kluczowy fakt, że zwykłe kamery potrzebują światła widzialnego. Oświetlenie może być problemem w każdym środowisku, a zmiana charakteru światła rodzi oczywiste skutki. Aspektem nie zawsze uwzględnianym lub dobrze rozumianym, zwłaszcza przez osoby opracowujące specyfikację rozwiązania, są skutki czynników pogodowych.

Kamery termowizyjne mają oczywiste zalety, ale nie znaczy to, że stanowią bezpośredni zamiennik kamer na światło widzialne — tak na pewno nie jest. Obie technologie działają optymalnie, gdy zostaną zintegrowane w ramach jednego rozwiązania. Tradycyjne kamery nie są w stanie wykrywać obiektów z takiej odległości jak kamery termowizyjne, natomiast kamery termowizyjne nie dorównują kamerom na światło widzialne pod względem stopnia odwzorowania szczegółów na potrzeby prac wyjaśniających. Obie technologie często łączy się w taki sposób, że kamera termowizyjna odpowiada za detekcję i alarmy, a kamera na światło widzialne zapewnia szczegółowość niezbędną w materiale dowodowym i podczas śledzeniu celu.

4.4 Analiza materiału wizyjnego

Sieciowe systemy dozoru wizyjnego umożliwiły prowadzenie działań z zakresu bezpieczeństwa i ochrony na niespotykaną dotąd skalę. Dobrze zaprojektowana hierarchia uprawnień umożliwia kontrolowany dostęp do materiału wizyjnego oraz jego dystrybucję i przechowywanie w środowisku obejmującym teoretycznie nieograniczoną liczbę podmiotów. Na wzrost skalowalności szczególnie wpływa rozwój techniczny w jednym obszarze: analizy wideo.

Na przestrzeni lat narzędzia do analizy wideo znacznie się rozwinęły, w dużej mierze dzięki stale udoskonalanym kamerom IP. Dobrze to widać w kamerach przeznaczonych do monitoringu domowego, z których wiele oferuje takie czy inne funkcje analityczne, na przykład umożliwiające detekcję ruchu w obserwowanej scenie. Kamera może również zawierać funkcje dodatkowe, takie jak detekcja przekroczenia linii czy przemieszczenia obiektów, a nawet zliczanie osób.

Narzędzia do analizy wideo mogą zmniejszyć zapotrzebowanie na pamięć masową, rejestrując tylko materiał wizyjny zawierający aktywność. Ponadto w związku z tym, że zarejestrowany materiał wizyjny jest w maksymalnym stopniu przetwarzany w samej kamerze (zgodnie z koncepcją „inteligencji na brzegu sieci"), obciążenie sieci jest znacznie mniejsze, ponieważ kamery przesyłają wyłącznie materiał interesujący odbiorcę. Ma to oczywiste zalety w scenariuszu z pomieszczeniem kontrolnym, gdzie operator systemu bezpieczeństwa musi analizować materiał wizyjny tylko w przypadku otrzymania alertu. To ogromny atut zarówno dla operatora, jak i dla efektywności operacyjnej całej firmy lub instytucji.

Istnieją dwie szerokie kategorie architektur systemowych umożliwiających wdrażanie analizy wideo: scentralizowane i rozproszone. W architekturze scentralizowanej materiał wizyjny i inne informacje są gromadzone przez kamery i czujniki, a następnie wysyłane do centralnego serwera w celu analizy. W architekturze rozproszonej same urządzenia brzegowe (kamery i wideoenkodery sieciowe) potrafią przetwarzać materiał wizyjny i wydobywać z niego odpowiednie informacje. Analizy brzegowe eliminują potrzebę korzystania ze specjalnych serwerów analitycznych, a ponieważ kompresja jest stosowana tylko na etapie przesyłania danych wideo na centralny serwer, analizy mogą być wykonywane na nieskompresowanym materiale wizyjnym. Rezultatem jest znacznie bardziej ekonomiczna i elastyczna architektura. Ponieważ duża część przetwarzania odbywa się w kamerach, te same serwery, które normalnie mogłyby przetworzyć zaledwie kilka strumieni wideo ze względu na wymaganą moc obliczeniową, teraz mogą obsłużyć kilkaset strumieni.

4.4.1 Szybkość przetwarzania i procesory graficzne

Jeśli wierzyć prognozom czołowych firm technologicznych, dynamiczny wzrost szybkości i możliwości przetwarzania, precyzyjnie przewidziany przez Gordona E. Moore'a (twórcy tzw. prawa Moore'a), w niedalekiej przyszłości nieco wyhamuje. Jednak połączenie rosnącej mocy i coraz mniejszych rozmiarów i tak pozwoliło producentom kamer oraz programistom na zmianę wykorzystania możliwości obliczeniowych.

Jeszcze do niedawna każdy wzrost mocy obliczeniowej wykorzystywano do poprawy jakości obrazu, co oznaczało wyższą rozdzielczość i bardziej efektywną kompresję wideo. Jednak rynek doszedł do takiego poziomu, że w zasadzie nie widać zapotrzebowania na dalsze podnoszenie rozdzielczości obrazu. Dlatego obecnie producenci wykorzystują moc obliczeniową, aby zapewnić niespotykany dotąd poziom funkcji inteligentnych. W wielu przypadkach oznacza to, że zaawansowane analizy wideo, które dotychczas były wykonywane na serwerze, teraz można realizować w kamerach.

Ponieważ nowoczesne układy scalone są coraz mniejsze i działają coraz szybciej, kamery mogą zawierać procesory graficzne, które umożliwiają przetwarzanie równoległe oraz otwierają nowe możliwości w obszarze analiz i innych zastosowań. To nowe zjawisko sprawiło, że firmy programistyczne zaczęły opracowywać nowe, brzegowe wersje dotychczasowych sprawdzonych aplikacji analitycznych przeznaczonych dla serwerów. Przyczynia się to do wzrostu zapotrzebowania na bardziej inteligentne kamery, których zalety znacznie wykraczają poza dziedzinę bezpieczeństwa i dozoru wizyjnego.

4.4.2 Głębokie uczenie i sztuczna inteligencja

Procesory graficzne umożliwiły skokowy wzrost wydajności analiz brzegowych, ale w systemach dozoru rośnie zapotrzebowanie na inne technologie, udostępniające takie funkcje jak zliczanie osób i zarządzanie zajętością. Rozwój sztucznej inteligencji i uczenia maszynowego sprawił, że do kamer zaczęły trafiać jednostki przetwarzania głębokiego uczenia (Deep Learning Processing Unit — DLPU), które okazały się przełomem.

DLPU to układ zaprojektowany specjalnie z myślą o upowszechnieniu analiz wykorzystujących głębokie uczenie. Analizy oparte na głębokim uczeniu mogą znacznie zwiększyć dokładność detekcji i klasyfikacji, ponieważ algorytm jest szkolony z użyciem zbioru obrazów przedstawiających wygląd docelowych obiektów. Oznacza to, że rozwiązanie do detekcji wtargnięć wchodzące w skład ochrony obwodowej można skonfigurować tak, aby wszczynało alarm tylko w przypadku ściśle zdefiniowanych obiektów i scenariuszy. Przypomina to zaawansowaną wersję instrukcji warunkowej typu ITTT (If-this-then-this).

W niektórych przypadkach widoczna jest tylko część obiektu, na przykład tylny zderzak samochodu, ale system analityczny i tak go rozpozna i zidentyfikuje. W czasie tworzenia tego dokumentu (i wbrew niektórym twierdzeniom) większość sprawdzonych rozwiązań dostępnych na rynku ograniczała się do identyfikacji oraz rozróżniania typów osób i pojazdów. Trwały jednak zaawansowane testy opartych na kamerach modeli analitycznych mających umożliwić dokonywanie bardziej szczegółowych rozróżnień, na przykład dotyczących koloru odzieży obserwowanej osoby.

Ten rozwój technologiczny może doprowadzić do powstania mocno wyspecjalizowanych systemów detekcji, które umożliwią rozróżnianie między pracownikami, klientami, zwykłymi obywatelami i potencjalnymi zagrożeniami. Z perspektywy bezpieczeństwa wdrożenie zaawansowanych funkcji analiz w środowisku z prawidłowo zastosowanymi zabezpieczeniami fizycznymi może tylko zwiększyć efektywność oraz dokładność systemu detekcji i zapobiegania przestępstwom. Przejście na nowy poziom możliwości wydaje się tylko kwestią czasu.

5 Koszty

5.1 Ocena i pomiar zwrotu z inwestycji

Tak jak w przypadku każdego środka bezpieczeństwa — z perspektywy podatności na zagrożenia lub odporności na nie — ocena rozwiązania ochrony obwodowej powinna być odpowiednia i proporcjonalna. Co oczywiste, przede wszystkim należy wziąć pod uwagę potencjalne zagrożenia, które w dzisiejszych dużych

przedsiębiorstwach czy organach administracji publicznej mogą mieć różną postać — od przypadkowych intruzów po uczestników protestów, a nawet terrorystów.

Coraz częstszą praktyką jest zintegrowane podejście do bezpieczeństwa, które uwzględnia dane i opinie pochodzące z innych działów, na przykład IT i operacyjnego. Obejmuje ono konieczność jak najwcześniejszego zaangażowania osób, które odpowiadają za wymogi inżynieryjne. Jeśli chodzi o wybór środków ochrony obwodowej, kiedyś punktem wyjścia zawsze były bardziej tradycyjne metody, mające na celu głównie odstraszanie i spowalnianie potencjalnych intruzów. Dopiero po nich projektant stosował dodatkowe, techniczne systemy detekcji. Jednak obecnie, w dobie coraz ściślejszej integracji różnych metod i systemów, potrzebne jest bardziej przemyślane i całościowe podejście.

Zazwyczaj bardzo trudno jest wykazać zwrot z inwestycji w rozwiązanie bezpieczeństwa mające na celu zapobieganie incydentom. Wynika to głównie z braku potencjalnych przychodów, które można by porównać z kosztami. Zazwyczaj pracownicy działu ochrony muszą wyjaśnić kolegom z działu finansów koszty różnego rodzaju incydentów związanych z bezpieczeństwem: czy to koszty bezpośrednie związane z utratą lub zniszczeniem mienia czy mniej oczywiste, ale równie dotkliwe koszty w postaci szkód wizerunkowych.

Istnieje jednak możliwość wykazania bardziej namacalnego zwrotu z inwestycji, zwłaszcza w przypadku pewnych technologii, które ograniczają potrzebę określonych czynności ręcznych lub umożliwiają przekierowanie pracowników do wykonywania innych zadań. Dobrym przykładem są rozwiązania, które nie tylko alarmują personel o podejrzanym zachowaniu czy wtargnięciu, ale mogą także automatycznie zainicjować odpowiednią „miękką" reakcję. Obejmują one systemy audio IP mogące emitować gotowe komunikaty lub znaki świetlne informujące intruza, że został wykryty, i nakazujące mu opuszczenie terenu obiektu.

Jeśli rozwiązanie obejmuje kamery dozorowe, można zwiększyć jego efektywność przez pokazywanie intruzom dowodu ich identyfikacji. Przykładowo można na ekranie wyświetlić zarejestrowaną tablicę rejestracyjną pojazdu, a nawet zdjęcie samego intruza. Dopiero gdy te środki nie dadzą zamierzonego rezultatu, trzeba wysłać pracowników ochrony, by wyjaśnili sprawę bezpośrednio na miejscu. Niewykluczone, że taki etapowy sposób reagowania na alarmy lepiej się sprawdza na zewnątrz chronionego obwodu, ale i tak zmniejsza potrzebę wczesnego angażowania pracowników ochrony, co daje niewątpliwą korzyść w postaci zwolnienia zasobów osobowych.

5.2 Oszacowanie kosztów

Kosztorys powinien być oparty na całkowitym koszcie posiadania. Obejmuje on wszystkie koszty rozwiązania w całym cyklu jego istnienia, a więc: koszty materiałów i robocizny, koszty badań, koszty instalacji systemu, koszty operacyjne, koszty konserwacji oraz koszty wycofania z eksploatacji i recyklingu. Może to wymagać zmiany podejścia w działach finansów i zaopatrzenia, ponieważ może wystąpić potrzeba realokacji kapitału między kosztami operacyjnymi a nakładami inwestycyjnymi.

Podobnie jak w przypadku innych środków trwałych klient chce znać przewidywany okres eksploatacji rozwiązania ochrony obwodowej. Kierownicy działów ochrony i IT mogą pomóc kolegom z działu finansów, wyjaśniając i pokazując, że zakup właściwej technologii jako platformy przyszłych rozwiązań przełoży się na oszczędności. Cechą zaawansowanych inteligentnych urządzeń dozorowych jest to, że do pewnego stopnia są one przygotowane na przyszłe wyzwania. Oznacza to, że w urządzeniach z wystarczającą mocą obliczeniową można wdrażać kolejne osiągnięcia techniczne, przede wszystkim w postaci funkcji analiz opartych na sztucznej inteligencji i uczeniu maszynowym.

6 Oferta Axis Communications

Otwarte podejście firmy Axis do integracji z rozwiązaniami partnerów sprawia, że jej czujniki sieciowe w połączeniu ze sprawdzonymi narzędziami do analizy wideo i mechanizmami sztucznej inteligencji umożliwiają klientom wdrażanie wysokowydajnych, zintegrowanych rozwiązań ochrony obwodowej, które są zabezpieczone przed cyberatakami i opłacalne w całym okresie eksploatacji systemu.

Tam, gdzie czujniki termiczne mogą nie być odpowiednim rozwiązaniem, znakomitą alternatywą jest technologia mikrofalowa (radar), która oferuje wiele zalet technologii termowizyjnej, często w połączeniu z mniejszą liczbą fałszywych trafień. Technologię radarową Axis można połączyć z tymi samymi funkcjami uczenia maszynowego i głębokiego uczenia co bardziej zaawansowane kamery dozorowe. Urządzenia radarowe Axis umożliwiają dokładne wykrywanie, klasyfikowanie oraz śledzenie osób i pojazdów z niemal zerowym współczynnikiem fałszywych alarmów.

Radar działa w trybie 24/7 i jest praktycznie nieczuły na typowe czynniki wyzwalające, takie jak poruszające się cienie lub wiązki światła, małe zwierzęta i owady czy złe warunki pogodowe. Przekłada się to na bardzo duże walory ekonomiczne, ponieważ pracownicy ochrony mogą się skoncentrować na prawdziwych, potwierdzonych zagrożeniach. Radar może też przekazywać informacje o prędkości obiektu, umożliwiając dokładne obliczenie punktu kontaktu, a nawet egzekwowanie ograniczeń prędkości.

Pierwsza część dowolnego wniosku o udzielenie informacji lub kwestionariusza analizy rynku często dotyczy wydajności rozwiązania. Kamery Axis zawierają stworzony przez Axis procesor ARTPEC, który oferuje najlepsze możliwości obliczeniowe w branży i umożliwia osadzanie w kamerze (czyli na tzw. brzegu sieci) bardzo zaawansowanych rozwiązań do analizy wideo z zakresu ochrony obwodowej. Co ważne, daje to też pewność, że rozwiązanie wykorzystuje technologię opracowaną przez tego samego producenta, a nie komponenty innych firm.

Ta „inteligencja na brzegu sieci" sprawia, że kilka kamer może śledzić wiele zdarzeń, do których dochodzi jednocześnie w różnych miejscach. Ta rozproszona architektura techniczna pozwala objąć rozwiązaniem dowolną liczbę kamer, a jednocześnie eliminuje konieczność inwestowania w scentralizowaną technologię serwerową.

Zatwierdzona przez rząd Wielkiej Brytanii aplikacja AXIS Perimeter Defender (APD) wykrywa cztery rodzaje zdarzeń dotyczących jednej lub kilku osób albo pojazdów:

- nieupoważnione wejście lub wjazd (wtargnięcie) na zdefiniowany obszar
- przechodzenie lub przejeżdżanie przez strefy w zdefiniowanej kolejności i zdefiniowanym kierunku
- warunkowe przechodzenie lub przejeżdżanie przez strefy
- przedłużająca się obecność

Aplikacja APD przekazuje nie tylko alarm o wtargnięciu i odpowiadający mu materiał wizyjny. Udostępnia także metadane, dzięki którym na materiale wizyjnym można wyświetlić nakładkę przedstawiającą granice oraz trajektorie ruchu osób i pojazdów. Z perspektywy integracji dużą zaletą jest fakt, że zarówno tradycyjne, jak i termowizyjne kamery Axis współpracują z głośnikami IP, umożliwiając automatyczne emitowanie komunikatów z chwilą detekcji (również w ramach autonomicznego rozwiązania). Tego rodzaju automatyczne ostrzeżenia umożliwiają „eskalowanie" działań i przeciwdziałań, co jest ważne dla określenia zamiarów intruza i przygotowania ewentualnej reakcji.

Aplikację APD można bezpośrednio zintegrować z popularnym oprogramowaniem używanym w przedsiębiorstwach (Genetec, Milestone, Seetec, Prysm, Qognify itd.).

Axis udostępnia uzupełniające narzędzia projektowe, które ułatwiają planowanie rozwiązań i zapewniają wsparcie na każdym etapie inwestycji — od identyfikacji właściwych produktów na podstawie

szczegółowych kryteriów przez precyzyjne obliczanie zapotrzebowania na pamięć masową po instalowanie urządzeń i zarządzanie systemami. Narzędzia Axis pomagają konsultantom w tworzeniu planów i kosztorysów, a integratorom ułatwiają płynniejszą i efektywniejszą realizację projektów. Narzędzia te umożliwiają nawet dbanie o bezpieczeństwo zainstalowanego systemu, ponieważ dostarczone oprogramowanie ułatwia instalowanie uaktualnień i poprawek zabezpieczeń.

W warunkach stale ewoluujących zagrożeń i środków zaradczych niezmienny pozostaje jeden istotny aspekt: integralność i bezpieczeństwo obwodu obiektu. Ochrona obwodowa to jedno z kluczowych zadań osób, które w swojej firmie lub instytucji odpowiadają za kształtowanie bezpiecznego środowiska dla pracowników, gości i zwykłych obywateli. Celem tego dokumentu jest promowanie zintegrowanego podejścia technicznego do planowania zabezpieczeń obwodowych. W dokumencie podkreślono także, że przed zakupem technologii bezpieczeństwa należy oszacować zwrot z takiej inwestycji. Tak czy inaczej, każdy specjalista ds. bezpieczeństwa, niezależnie od działu, stanowiska i branży, powinien dobrze poznać możliwości dostępnych technologii i zarysować przyszłe trendy. Pomoże to w podjęciu optymalnych decyzji w sferach bezpieczeństwa operacyjnego i zaopatrzenia.

Odnośniki do produktów

Termowizyjne kamery IP:

AXIS Q19 i inne www.axis.com/en-gb/products/thermal-cameras

Oprogramowanie analityczne:

AXIS Perimeter Defender

www.axis.com/en-gb/products/axis-perimeter-defender

Zewnętrzne głośniki IP:

AXIS C1310-E www.axis.com/en-gb/products/axis-c1310-e

Radar IP:

D2110-VE www.axis.com/en-gb/products/axis-d2110-ve

T10169467/PL/M1.3/2107

O firmie Axis Communications

Firma Axis wspiera rozwój inteligentnego oraz bezpiecznego świata poprzez tworzenie rozwiązań sieciowych, które dostarczają wiedzę umożliwiającą poprawę bezpieczeństwa i wdrażanie nowych sposobów prowadzenia działalności. Jako lider rynku sieciowych systemów wizyjnych Axis oferuje produkty i usługi z zakresu dozoru wizyjnego i analiz wideo, kontroli dostępu, systemów domofonowych oraz systemów audio. Axis zatrudnia ponad 3800 wysoce zaangażowanych pracowników w ponad 50 krajach i współpracuje z partnerami na całym świecie w celu dostarczania swoich rozwiązań klientom. Firma Axis została założona w 1984 roku i ma siedzibę w Lundzie w Szwecji.

Więcej informacji o firmie Axis można znaleźć na stronie internetowej firmy pod adresem *axis.com*.