Centra danych

Magazyn firmy Axis, numer 1

Rozwiązania Axis w dziedzinie bezpieczeństwa i eksploatacji

Pięciowarstwowa strategia dla skuteczności i jakości ochrony centrum danych

Ochrona w 3D: przed dronami, które coraz częściej są nowym wektorem ataku

Większa wiarygodność centrów danych w obszarze zrównoważonego rozwoju

I nie tylko!

AXIS COMMUNICATIONS

Spis treści

Jesteśmy, jako społeczeństwo, coraz bardziej zależni od centrów danych, ponieważ współczesny styl życia nieodłącznie wiąże się z konsumpcją informacji. Tę tendencję pogłębiają tylko postępy w dziedzinie sztucznej inteligencji (AI), pojawienie się technologii 5G, wideo na żądanie i wciąż rosnąca liczba urządzeń IoT.

A w miarę jak centra danych stają się coraz większe i bardziej rozproszone, monitorowanie ich działania i zapewnienie ich bezpieczeństwa stanowi coraz większe wyzwanie. Firma Axis wykorzystuje swoją specjalistyczną wiedzę we współpracy z czołowymi europejskimi operatorami centrów danych, by na różne sposoby wspierać ich działalność. W tym numerze magazynu piszemy o kilku problemach, które wymagają rozwiązania, oraz roli, jaką może w tym odegrać technologia.

Skuteczniejsza ochrona obiektu według pięciowarstwowej strategii Axis
Proponowana przez firmę Axis pięciowarstwowa strategia ochrony obejmuje perymetr, teren, budynki, serwerownie i szafy serwerowe. Korzystając z sieciowego dozoru wizyjnego i analiz realizowanych w urządzeniach brzegowych, Axis jest w stanie zbudować prawdziwie inteligentne rozwiązanie do fizycznej ochrony obiektów — by prowadzona w nich działalność była bardziej odporna i efektywna.

Wykrywanie aktywności dronów w celu ograniczenia ryzyka
Obecność dronów w pobliżu centrum danych jest coraz poważniejszym ryzykiem, a menedżerowie centrów danych powinni porzucić myślenie o ochronie jedynie w dwóch wymiarach i wdrożyć środki obrony przed zagrożeniami z powietrza. Specjalne oprogramowanie, które wykrywa drony na podstawie emitowanych przez nie sygnałów radiowych, jest komplementarne wobec systemu kamer sieciowych Axis, zawczasu ostrzega operatorów o zbliżającym się dronie i wskazuje na jego możliwe zamiary.

Redukcja śladu węglowego i osiąganie „zielonych" celów
Operatorzy centrów danych powinni analitycznie przyglądać się swoim systemom oraz używanym produktom i materiałom, aby dokonywać niewielkich, przyrostowych zmian w kierunku celów zrównoważonego rozwoju, a w szczególności redukcji śladu węglowego. Wiarygodność partnerów, takich jak Axis, stosowanie materiałów ze źródeł odnawialnych oraz właściwych rozwiązań technicznych może przyczynić się do bardziej ekologicznej i zrównoważonej eksploatacji centrum danych.

Cyfrowa transformacja i rola kamery sieciowej
W centrach danych można zintegrować istniejące już czujniki, aby optymalizować eksploatację na podstawie inteligentnej analizy danych. Dane generowane przez kamery Axis, wykorzystywane jako inteligentne czujniki, można wykorzystać w nowoczesnych systemach zarządzania infrastrukturą centrum danych (DCIM, data center infrastructure management), aby osiągnąć poprawę efektywności, na przykład, chłodzenia. Inżynierowie, którzy dysponują użytecznymi i dokładnymi informacjami, mogą natychmiast reagować na ewentualne problemy.

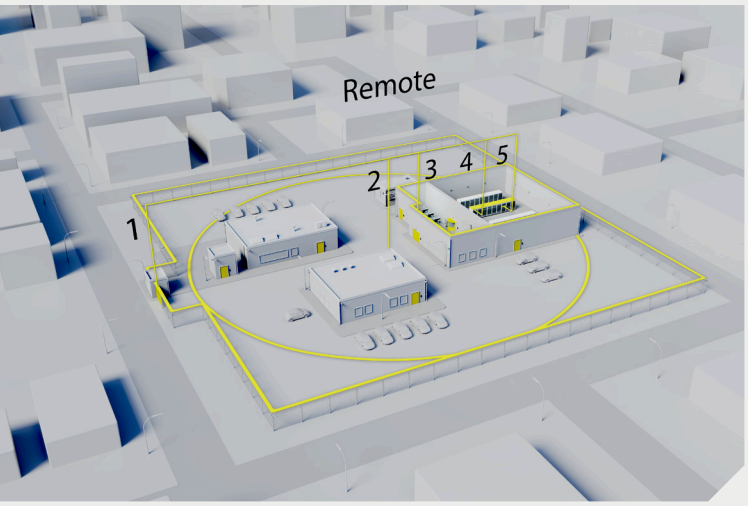
Jak wzmocnić ochronę fizyczną poprzez współdziałanie urządzeń
Wzrost zagrożenia fizycznego wymusza stosowanie innowacyjnych, sieciowych technologii do inteligentnej ochrony centrum danych. Rozwiązania Axis do ochrony fizycznej mogą odegrać istotną rolę w zabezpieczaniu centrum danych, ponieważ są w stanie komunikować się ze sobą, tworząc inteligentny, w dużym stopniu autonomiczny system obronny.

Mamy nadzieję, że treść naszego magazynu okaże się przydatna i będzie inspiracją do przemyśleń. Niezależnie od wyzwań, przed jakimi wspólnie stajemy, Axis z zaangażowaniem współpracuje z partnerami i klientami przy opracowywaniu nowoczesnych rozwiązań dla inteligentnego, bezpieczniejszego świata.

Z życzeniami udanego roku
Peter Dempsey, menedżer ds. kluczowych klientów końcowych — EMEA

Pięciowarstwowa strategia dla skuteczności i jakości ochrony centrum danych

Rozwój usług chmurowych i przetwarzania w hiperskali oznacza, że coraz więcej osób polega w swojej pracy i życiu na mocy obliczeniowej i pojemności centrów danych. Konsumpcja informacji szybko rośnie jako pochodna współczesnego stylu życia.



W miarę jak centra danych stają się coraz bardziej złożone i rozległe, monitorowanie ich eksploatacji i zapewnienie wysokiego poziomu bezpieczeństwa stanowi coraz większe wyzwanie, a personel znajduje się pod rosnącą presją zagrożeń fizycznych i cyberataków. Każde zakłócenie działania centrum danych może przynieść katastrofalne skutki, a przestoje generują znaczne koszty i wywołują poważne zakłócenia w życiu ludzi i działalności przedsiębiorstw — ponieważ bezproblemowy przepływ danych jest nam dziś niezbędny do codziennego funkcjonowania. Dlatego tak ważne jest wdrożenie odpowiednich narzędzi i technologii, które zapewnią kompleksową, wielowymiarową ochronę, a przy tym będą dawały się skalować w ślad za rozbudową i ewolucją centrów danych.

Kompleksowa ochrona obiektu — przed zagrożeniami wewnętrznymi i zewnętrznymi

Zintegrowane rozwiązania wideo i audio firmy Axis można z powodzeniem stosować do ochrony centrów danych i wspierania ich działalności. Nasza pięciowarstwowa strategia obejmuje perymetr, teren, budynki, serwerownie i szafy serwerowe, bazując na wykorzystaniu urządzeń sieciowych z wbudowanymi funkcjami analitycznymi. W efekcie powstaje prawdziwie inteligentne rozwiązanie, które zapewnia kompleksową ochronę. Wykrywanie i eliminowanie incydentów stanie się proste, a możliwość zastosowania szerokiej gamy kamer i czujników sprawi, że operatorzy będą mieli większe zaufanie do skuteczności systemu ochrony.

Sieciowe systemy wideo i audio firmy Axis pomagają chronić perymetr centrum danych za pomocą kamer do nadzoru wizyjnego, kamer termowizyjnych i radarów wykrywających ruch w obiekcie lub w jego pobliżu oraz umożliwiających śledzenie intruzów poruszających się pieszo lub w pojazdach. Możliwe jest zautomatyzowane generowanie alertów i alarmów przez głośniki sieciowe w celu odstraszenia potencjalnych przestępców. Przez te same głośniki operatorzy mogą w czasie rzeczywistym zwracać się bezpośrednio do intruzów. Takie rozwiązania techniczne, oparte na zaawansowanych analizach, cechują się wysoką dokładnością, co przekłada się na mniejszą liczbę fałszywych alarmów generujących zbędne koszty.

Wszystkie wejścia na teren obiektu są zaopatrzone w systemy kontroli dostępu, w których nadzór wideo jest drugim czynnikiem uwierzytelniania, stosowanym do identyfikacji i autoryzacji. Rozpoznawanie twarzy stosowane jest także jako mechanizm kontroli dostępu do budynków, pomieszczeń, a nawet poszczególnych szaf serwerowych. Sieciowe audio może też odegrać rolę w ochronie przed zagrożeniami wewnętrznymi, jeśli będzie generowało alarmy i alerty w reakcji na sygnały z kamer sieciowych wykrywających nietypową aktywność w budynkach centrum danych. Taka aktywność to, na przykład, dostęp do szafy serwerowej bez autoryzacji lub próba dostępu do kontrolowanych obszarów o nietypowych porach.

Gdy na szali jest bezpieczeństwo ogromnych zasobów danych, bezwzględnie konieczne jest wdrożenie systemu nie tylko bardzo bezpiecznego, lecz także skalowalnego. Każde urządzenie pozostawione bez należytych zabezpieczeń może zostać wykorzystane przez osoby z wewnątrz działające w złej wierze, jak i przez potencjalnych intruzów. Odpowiedzią firmy Axis jest ciągłe wzmacnianie cyberbezpieczeństwa urządzeń poprzez aktualizacje firmware i oprogramowania, a także regularne testy.

Axis ma wszystko, czego potrzeba do ochrony zasobów i terenu nowoczesnego centrum danych, w tym różne rozwiązania sieciowe, które oferują szyfrowanie komunikacji, filtrowanie adresów IP, bezpieczny start i podpisywanie firmware. Strategia Axis gwarantuje, że cyberbezpieczeństwo nie jest dodatkiem, lecz czynnikiem branym pod uwagę już na początku projektowania systemów.

5 warstw

- Perymetr
- Teren
- Budynki
- Serwerownie
- Szafy serwerowe

Kamery sieciowe wsparciem w cyfrowej transformacji centrów danych

Dane mogą być najcenniejszym zasobem strategicznym, jaki posiadamy, ale tylko wtedy, gdy potrafimy je efektywnie wykorzystać. Zamykanie danych w odrębnych systemach sprawia, że te systemy są prostsze, ale z drugiej strony — jest straconą szansą. Integracja danych to klucz do prawdziwie użytecznej inteligentnej analizy.

Uwspólnienie danych oraz sprzężenie czujników i elementów wykonawczych ze sztuczną inteligencją prowadzi do generowania praktycznych spostrzeżeń, które z kolei można wykorzystać do optymalizacji działalności w różnych branżach.

Odpowiednio analizowane dane łączą usługi z ludźmi, którzy z nich korzystają, zmieniając skomplikowany system w efektywny, zintegrowany mechanizm. Dlaczego w centrach danych nie zawsze się to udaje? We współczesnym otoczeniu biznesowym duży nacisk kładzie się na efektywność energetyczną, bezpieczeństwo aktywów i jakość usług. Z drugiej strony centra danych muszą radzić sobie z coraz większym obciążeniem przetwarzaniem, a co za tym idzie — obciążeniem termicznym. Systemy ochrony budynku i zarządzania sprzętem często funkcjonują zupełnie odrębnie, a przecież centra danych, by sprostać stawianym przed nimi oczekiwaniom, powinny korzystać ze wszystkich posiadanych zasobów.

Nowy paradygmat: inteligentna sieć

Na szczęście ta konieczność integracji pojawia się w czasie, gdy mamy już narzędzia potrzebne do jej realizacji. Urządzenia składające się na internet rzeczy (IoT, Internet of Things) mają dziś większe możliwości samodzielnego zbierania, przetwarzania i analizowania danych. Wykonywanie tych zadań bezpośrednio w urządzeniach brzegowych ogranicza zapotrzebowanie na przepustowość sieci i zewnętrzną moc obliczeniową, a do tego może zmniejszyć opóźnienie na całej trasie ze 100–250 ms do 10–20 ms* — po prostu dzięki wyeliminowaniu przesyłania dużych ilości danych do/z serwerów chmurowych.

Urządzenia IoT (nareszcie!) mówią do siebie tym samym językiem. Rosnąca popularność protokołu MQTT (Message Queue Telemetry Transport), który działa powyżej warstwy protokołu sieciowego TCP/IP, znacznie ułatwia integrację danych między urządzeniami IoT a serwerami lub aplikacjami chmurowymi. MQTT jest rozwiązaniem Open Source opartym na otwartych standardach, co upraszcza opracowywanie nowych mechanizmów integracji punktów końcowych i automatyzacji na podstawie danych. Nie ma już powodu, by systemy bezpieczeństwa centrum danych funkcjonowały w innej sieci niż ta, do której są podłączone czujniki systemu zarządzania infrastrukturą centrum danych (DCIM, data center infrastructure management).

Zmieniająca się rola kamery sieciowej

Otwarty charakter protokołu MQTT stwarza warunki do wykorzystania danych z kamer sieciowych, traktowanych jako inteligentne czujniki, w nowoczesnym systemie DCIM. Przyjrzyjmy się temu na przykładzie monitorowania temperatury. Wewnętrzny czujnik temperatury może wykryć gorący punkt na szafie serwerowej i przekazać informację o nim do kamery termowizyjnej; następnie kamera może przekazać obraz zawierający wszystkie istotne dane do systemu zarządzania materiałem wizyjnym. Na podstawie takiego obrazu inżynier ustali, gdzie występuje problem. Łączne wykorzystanie danych z różnych czujników może z kolei przynieść wzrost efektywności, np. w wyniku precyzyjnego wyregulowania systemów chłodzących, tak by zużywały jak najmniej energii.

Nowe zastosowania danych pozyskiwanych przez kamery sieciowe są także okazją do istotnej redukcji kosztu i złożoności systemu DCIM. Operatorzy centrów danych, gdzie tylko mogą, poszukują sposobów na poprawę efektywności, zatem nowatorskie zastosowanie kamer sieciowych może okazać się sprytnym posunięciem. Tam, gdzie kamery są już używane do monitoringu jako część systemu ochrony, można wykorzystać je również w sferze eksploatacji centrum danych.

Nadszedł czas, aby prawdziwie inteligentne centrum danych stało się normą. Nie oznacza to rezygnacji z obecnych systemów DCIM ani wymiany newralgicznych czujników, a jedynie wykorzystanie wszystkich już posiadanych informacji, nowoczesnych urządzeń i rozwiązań sieciowych do kreowania nowych szans na poprawę efektywności.

*www.ibm.com/blogs/internet-of-things/iot-5g-transforms/

Ochrona w 3D

Przed dronami, które coraz częściej są nowym wektorem ataku.

Sektor produkcji i zastosowań dronów rośnie w siłę, ponieważ bezzałogowe statki powietrzne realizują szereg pożytecznych zadań z korzyścią dla efektywności działania przedsiębiorstw. Jednak ich upowszechnienie[1] ma też negatywne konsekwencje dla bezpieczeństwa. W Boże Narodzenie 2018 roku brytyjski port lotniczy Gatwick został zamknięty na 33 godziny, co zakłóciło podróż ponad 140 000 pasażerów. Mimo relacji wielu naocznych świadków nie udało się z całą pewnością potwierdzić ani wykluczyć obecności drona[2].

Ten przykład ilustruje bardzo poważny problem. Do skutecznego obejścia ochrony obwodowej lotniska — i spowodowania milionowych strat — wystarczył jeden dron, którego każdy może sobie kupić za nieco ponad 1000 złotych. Skalę zagrożenia uświadomimy sobie z pełną ostrością, jeśli weźmiemy pod uwagę rodzaje środków, jakie drony mogą przenosić: kamery szpiegowskie, sprzęt do przechwytywania sygnału Wi-Fi i zakłócania pracy oprogramowania oraz systemów, a nawet broń biologiczną.

Wykrywanie, identyfikacja, lokalizacja

Ochrona przed zagrożeniami cybernetycznymi i fizycznymi jest jedną z newralgicznych funkcji w centrum danych. Każda przerwa w działaniu może wygenerować znaczne koszty i wywołać poważne zakłócenia w życiu ludzi i działalności przedsiębiorstw — ponieważ bezproblemowy przepływ danych jest nam dziś niezbędny do codziennego funkcjonowania.

Nowoczesne systemy sieciowe oferują zaawansowane funkcje ochrony obwodowej, pozwalając śledzić ruchy intruzów przy użyciu kamer do nadzoru wizyjnego, kamer termowizyjnych i radarów. I choć ostatnimi laty centra danych zyskały zabezpieczenia nieporównywalnie lepsze od tych, jakie stosowano dawniej, kluczem do powstrzymywania nowych zagrożeń jest ciągłe bycie o krok przed nimi. Takie nowe zagrożenie może teraz nadejść z powietrza.

Specjalistyczne oprogramowanie, komplementarne w stosunku do sieciowych systemów ochrony fizycznej, umożliwia teraz wykrywanie dronów na podstawie emitowanych przez nie sygnałów radiowych. Można za jego pomocą zidentyfikować ponad 200 modeli dronów różnych marek, w tym dronów komercyjnych i hobbystycznych, a nawet określić lokalizację operatora, który pilotuje drona. To rozwiązanie techniczne, znacznie bardziej efektywne niż oczy i uszy personelu ochrony, zawczasu ostrzega o zbliżającym się dronie i wskazuje na jego możliwe zamiary.

We właściwych rękach drony są niezwykle pożytecznymi maszynami, ale nie oznacza to, że wolno nam ignorować związane z nimi zagrożenia.

Analiza drona i minimalizacja zagrożenia

Ważne jest, aby po wykryciu drona ustalić przyczynę jego obecności. Centra danych zwykle otoczone są strefą zakazu lotów, dlatego pracownicy ochrony lub funkcjonariusze policji muszą mieć możliwość błyskawicznego odróżnienia pomyłki pilota od celowego działania osoby o złych zamiarach. Po zlokalizowaniu drona i wykryciu sygnałów emitowanych przez sterujące nim zdalnie urządzenie można skierować pracowników ochrony w teren, aby odszukali pilota i z nim porozmawiali.

Szybka identyfikacja jest niezbędna do podjęcia decyzji, które nie mogą czekać. Oprogramowanie wykrywające drony, zdolne do sterowania kamerą PTZ (obrót/pochylenie/zbliżenie), można wykorzystać do śledzenia ruchów statku powietrznego, a wyraźny obraz pozwala ocenić rodzaj ładunku i odróżnić niegroźny obiekt od takiego, za którym stoją nieprzyjazne intencje.

Rozwiązanie do wykrywania dronów opracowane we współpracy z partnerem

Wobec rosnącego zagrożenia, jakie wiąże się z aktywnością dronów, firmy Axis i Dedrone wspólnie opracowały unikalne rozwiązanie do inteligentnej ochrony przestrzeni powietrznej. Kluczem do skuteczności tego rozwiązania jest zasób danych. Do tej pory do trenowania oprogramowania AI/ML (wykorzystującego sztuczną inteligencję / samouczenie maszyn) działającego w kamerach wykorzystano już ponad 17 milionów zdjęć dronów. Wszystko po to, aby oprogramowanie potrafiło bezbłędnie identyfikować nawet zamaskowane maszyny. Ponadto protokoły do zdalnej identyfikacji (tzw. RemoteID) dostarczają informacji potrzebnych do sprawdzania, czy obecność drona jest dopuszczalna. Są kolejnym środkiem zwiększającym zdolność do detekcji zagrożeń.

We właściwych rękach drony są niezwykle pożytecznymi maszynami, ale nie oznacza to, że wolno nam ignorować związane z nimi zagrożenia.

Mając takie rozwiązanie, można monitorować przestrzeń powietrzną wokół centrum danych równie skutecznie, jak teren. Integracja z istniejącymi systemami zarządzania materiałem wizyjnym pozwala włączyć wykrywanie dronów do kompleksowego systemu ochrony.

[1] www.insiderintelligence.com/insights/drone-industry-analysis-market-trends-growth-forecasts/
[2] www.theguardian.com/uk-news/2020/dec/01/the-mystery-of-the-gatwick-drone

Wzmocnienie ochrony fizycznej centrów danych poprzez współdziałanie urządzeń

Wiele już napisano o niebezpieczeństwie w kontekście ochrony centrów danych. Jednak również zagrożenia fizyczne stanowią powód do zmartwień. W mainstreamowych mediach amerykańskich głośno było swego czasu o aresztowaniu mężczyzny, który rzekomo przygotowywał się do wysadzenia dużego centrum danych w stanie Wirginia*. Gdy rozważamy możliwe środki ochrony przed takim zagrożeniem, oczywista wydaje się potrzeba wdrożenia nowoczesnych rozwiązań do ochrony fizycznej. Jednak nie zawsze oczywisty jest potencjał połączenia takich rozwiązań w zintegrowany system.

Innowacje w dziedzinie radarów i sieciowych systemów wizyjnych

Kamery sieciowe osiągnęły już ten etap rozwoju, na którym są zdolne do samodzielnej kategoryzacji ruchu (np. odróżnienie wtargnięcia od podejrzanej obecności) oraz odróżniania ludzi od pojazdów i innych obiektów na perymetrze obiektu. Dokładność nowoczesnych kamer jest tak wysoka, że udaje się znacznie zmniejszyć liczbę fałszywych alarmów. Ponadto, ponieważ przetwarzanie odbywa się bezpośrednio w urządzeniach brzegowych, przez sieć przesyłane są tylko najbardziej niezbędne dane, co oznacza szybsze podejmowanie decyzji oraz oszczędność czasu i pieniędzy.

Choć rozwiązania do ochrony fizycznej mogą odegrać istotną rolę w zabezpieczaniu centrum danych, to dopiero wtedy, gdy potrafią się ze sobą komunikować, tworzą inteligentny, w dużym stopniu autonomiczny system obronny. Na przykład zintegrowane rozwiązanie złożone z radaru i kamery może wykrywać i klasyfikować ruch na perymetrze obiektu, a w uzasadnionych przypadkach nakazać kamerze termowizyjnej zarejestrowanie śladu termicznego i dodatkowe udokumentowanie obecności nieupoważnionej osoby. Inny przykład: kamera PTZ (obrót/pochylenie/zbliżenie) śledzi ruch, a głośnik podłączony do sieci IP odtwarza nagrany wcześniej komunikat odstraszający intruza. Jeśli ten nie zareaguje i nadal się zbliża, włączana jest syrena z pulsującym światłem ostrzegawczym.

Oczywiście źródłem zagrożenia mogą być także inne czynniki. Wewnątrz obiektu kamery sieciowe z wbudowaną funkcją analityczną mogą pełnić rolę pierwszej linii detekcji dymu i wycieków gazu, a kamery połączone z czujnikami mogą wykrywać wycieki wody.

Kamery z funkcją pomiaru temperatury mogą odgrywać newralgiczną rolę w wykrywaniu wzrostu temperatury powietrza w otoczeniu, potencjalnie wskazującego na problem o większej skali. Przykładowo, w systemie monitorowania generatorów energii elektrycznej najmniejsze wahanie temperatury poza ustalony próg może powodować sygnalizację alarmu.

Współpraca na rzecz kompleksowej ochrony

Brytyjska instytucja rządowa Centre for the Protection of National Infrastructure (CPNI) opracowała wytyczne i standardy obowiązujące we wszystkich obiektach krytycznych dla funkcjonowania państwa. Do obiektów tych zaliczono również centra danych, ponieważ świadczą one usługi o newralgicznym znaczeniu. Współpraca z wiarygodnym dostawcą rozwiązań do ochrony fizycznej, który uzyskał aprobatę CPNI, jest dla operatora centrum danych gwarancją jakości nabywanych produktów i zachowywania wysokich standardów.

Jeśli produkty te będą jednocześnie innowacyjne, centrum danych będzie czerpać korzyści ze zintegrowanego, wysoce autonomicznego systemu, zapewniającego najwyższy poziom ochrony.

*www.bbc.co.uk/news/technology-56719618

Większa wiarygodność i efektywność centrów danych w obszarze zrównoważonego rozwoju

Prognozy mówią, że światowy rynek „zielonych" centrów danych będzie w 2026 roku wart 142,8 miliarda USD, co oznacza skumulowany roczny wskaźnik wzrostu na poziomie prawie 20%[1]. Aby zasłużyć na miano „zielonego", centrum danych musi oferować niezawodne i bezpieczne przechowywanie danych, a jednocześnie optymalizować swoją efektywność energetyczną, by minimalizować wpływ swojej działalności na środowisko. Jest to szczególnie istotne w kontekście zobowiązania, jakie podjęli operatorzy zrzeszeni w Climate Neutral Data Center Pact: osiągnięcia do roku 2030 klimatycznej neutralności centrów danych[2].

W przypadku wielu centrów danych zrównoważony rozwój wymagał będzie poważnego przemyślenia dotychczasowego modelu eksploatacji. Główne problemy to ilość zużywanej energii, ilość wytwarzanego ciepła, a także minimalizacja i kompensacja wpływu na środowisko. Trudno się dziwić, że centra danych, które jeszcze nie podjęły inicjatyw na rzecz zrównoważonego rozwoju, znajdują się pod coraz większą presją. Dla menedżerów centrum danych poważnym wyzwaniem jest ograniczenie wpływu na środowisko przy utrzymaniu wysokiego poziomu usług.

Uporządkowane ramy zrównoważonego rozwoju i wiarygodne łańcuchy dostaw

Centrum danych, którego operator wykazuje się świadomością środowiskową, będzie przyciągać klientów podobnie zapatrujących się na kwestie zrównoważonego rozwoju[3]. Działanie zgodne ze standardami i w uporządkowanych ramach, takich jak inicjatywa UN Global Compact, której Axis jest sygnatariuszem[4], może pomagać przedsiębiorstwom w osiąganiu celów zrównoważonego rozwoju wyznaczonych przez ONZ[5], a także jest dowodem, że za deklaracjami firmy stoją konkretne czyny.

Udział w międzynarodowych inicjatywach świadczy o wspólnocie wartości. Gdy efektywność kosztowa, dostęp do wykwalifikowanych kadr technicznych, jakość usług i innowacyjność znajdują się w centrum zainteresowania przedsiębiorstw, partnerska współpraca jest koniecznością. Organizacje, które budują alianse i współdziałają w łańcuchu dostaw, powinny wyznawać te same fundamentalne wartości, które będą podstawą wzajemnego zaufania.

Redukcja śladu węglowego i osiąganie „zielonych" celów

Centra danych zużywają dużo energii i wytwarzają dużo ciepła, co spędza sen z powiek menedżerom odpowiedzialnym za „zielone" standardy. Choć nie ma prostego, szybkiego rozwiązania, operatorzy centrów danych powinni analitycznie przyglądać się swoim systemom oraz używanym produktom i materiałom, aby podejmować niewielkie, przyrostowe działania przybliżające do celów zrównoważonego rozwoju, a w szczególności redukcji śladu węglowego. Do takich działań należeć może, na przykład, wybór dostawców, którzy priorytetowo traktują energooszczędność swoich rozwiązań.

Na przykład fakt, że kamery sieciowe Axis wewnętrznie analizują dane wideo i realizują algorytmy decyzyjne, skutkuje ograniczeniem obciążenia sieci i zużycia energii związanej z przesyłaniem danych do przetwarzania zewnętrznego. Technologia Axis Zipstream[6] zmniejsza obciążenie sieci i objętość przechowywanych danych średnio o 50%, dodatkowo wspomagając realizację celów „zielonego" centrum danych.

Axis pomaga operatorom centrów danych na drodze do zrównoważonego rozwoju, oferując innowacyjne rozwiązania, które charakteryzują się najwyższym poziomem bezpieczeństwa i jak najmniejszym wpływem na środowisko. Staranny wybór materiałów i unikanie marnotrawstwa w procesach dowodzi naszego odpowiedzialnego podejścia do całego łańcucha produkcyjnego. W ten sposób wspieramy centra danych w realizacji celów zrównoważonego rozwoju, a jednocześnie kreujemy innowacje dla inteligentnego, bezpiecznego świata.

Rozwiązania polecane do centrów danych

Kamery **Axis** zintegrowane z radarami

Fuzja dwóch zaawansowanych technologii, wideo i radaru, umożliwia ochronę i niezawodną, nieprzerwaną (24/7) detekcję na dużym obszarze. To wyjątkowe urządzenie klasyfikuje obiekty przy użyciu najnowocześniejszych algorytmów uczenia głębokiego, przenosząc detekcję i wizualizację na nowy poziom.

Kamery PTZ **Axis**

Kamery PTZ umożliwiają dozór dużych obszarów w czasie rzeczywistym dzięki funkcjom obracania, pochylania i zbliżania. Kamera AXIS Q61 Series zapewnia pełną wierność sceny i doskonałą jakość obrazu we wszystkich kierunkach — poniżej i powyżej linii horyzontu. Dlatego kamery z tej rodziny nadają się idealnie do stosowania w terenie o niewielkich nierównościach. Do rodziny AXIS Q62 Series należą kamery przystosowane do eksploatacji w każdych warunkach pogodowych. AXIS Q63 Series oferują szybki zoom i laserowe ustawianie ostrości, również w ciemności. Dzięki funkcji Speed Dry generują ostry i wyraźny obraz nawet przy deszczowej pogodzie.

AXIS Q1961-TE Thermal Camera

Ta bezhalogenowa kamera termometryczna umożliwia zdalne monitorowanie temperatur i wyzwalanie zdarzeń w oparciu o temperaturę. Idealnie sprawdza się jako element systemu, który ma dbać o efektywność eksploatacji. Jest trwała i odporna na uderzenia, a także ma funkcje analizy do wczesnego wykrywania pożaru i wbudowane funkcje cyberbezpieczeństwa.

Rozwiązania **Axis** do kontroli dostępu

Axis zapewnia sprzęt i narzędzia analityczne do identyfikacji, uwierzytelniania i autoryzacji wstępu do budynków i pomieszczeń. Nasza technologia kontroli dostępu chroni krytyczne lub wrażliwe obszary za pomocą uwierzytelniania automatycznego (karty, kody PIN, kody QR) lub ręcznego (dwukierunkowa sieć audio i wideo).

Tubowe głośniki sieciowe **Axis**

Głośniki sieciowe Axis umożliwiają aktywne zniechęcanie do niepożądanych zachowań i ostrzeganie osób naruszających przepisy, wykrytych przez kamery. Głośniki można wykorzystać do emisji komunikatów, które odwiodą osoby od niepożądanych zachowań lub przebywania na granicy obiektu. Mogą służyć również do przekazywania instrukcji głosowych w sytuacji zagrożenia lub do informowania o naruszeniu zasad parkowania.

Dlaczego Axis?

Zwiększanie cyberbezpieczeństwa

Atak na infrastrukturę lub kradzież danych może mieć katastrofalne konsekwencje. Jakie zagrożenia wiązałyby się ze zhakowaniem kamer zamocowanych przy światłach drogowych? Ograniczenie takiego ryzyka to w najbliższym czasie priorytet dla władz. Axis jest liderem w obszarze rozwiązań zabezpieczających i może się pochwalić znakomitymi osiągnięciami w zakresie dbania o bezpieczeństwo danych oraz ich zgodność z przepisami w inteligentnych miastach. Staliśmy się ekspertami, jeśli chodzi o ocenę ryzyka i uwzględnianie procesów ochrony danych w każdym elemencie oferty. Dbamy o przestrzeganie obecnych i przyszłych zasad oraz przepisów ustawowych i wykonawczych.

Jakość we wszystkich aspektach

W swojej działalności Axis zawsze stawia na jakość. Wszystkie nasze produkty są tworzone tak, aby wytrzymywały ekstremalne warunki, były odporne na wandalizm i trudne warunki pogodowe. Poddajemy je szeroko zakrojonym testom, aby upewnić się, że są trwałe i zdolne do generowania wyraźnych obrazów w każdych warunkach. Nasze podejście do jakości dostrzegalne jest na obrazach HDTV generowanych przez nasze kamery — obrazach tak dobrych, że mogą służyć za dowody w sądzie.

Potęga partnerstwa

Otwarta platforma Axis jest elastyczna, skalowalna i łatwa w integracji. Współpracuje z produktami wielu partnerów oraz zewnętrznymi rozwiązaniami sprzętowymi i programowymi.

Innowacyjne technologie

Wciąż pragniemy łączyć najlepszą technologię z ludzką kreatywnością, aby nasze urządzenia działały jak najlepiej. Pojawia się coraz więcej argumentów przemawiających za analizą i wykorzystaniem danych bezpośrednio w urządzeniach brzegowych.

Dowiedz się więcej na temat rozwiązań Axis dla centrów danych:
www.axis.com/data-centers

O firmie Axis Communications

Axis wspiera rozwój inteligentnego oraz bezpiecznego świata przez tworzenie rozwiązań umożliwiających poprawę bezpieczeństwa i efektywności biznesowej. Jako firma zajmująca się technologiami sieciowymi oraz lider branży, Axis oferuje rozwiązania z zakresu dozoru wizyjnego, kontroli dostępu, systemów domofonowych i systemów audio. Ich rozszerzeniem i uzupełnieniem są inteligentne aplikacje analityczne oraz wysokiej jakości szkolenia.

Axis zatrudnia około 4 000 pracowników w ponad 50 krajach oraz współpracuje z partnerami z obszaru technologii i integracji systemów na całym świecie w celu dostarczania swoich rozwiązań klientom. Firma została założona w 1984 roku i ma swoją siedzibę w Lund w Szwecji.