Rechenzentren

Axis Magazin, Ausgabe 1

Mehr Sicherheit und optimierte Betriebsabläufe mit Axis Sicherheitslösungen

Mehr Sicherheit in Rechenzentren durch einen fünfstufigen Ansatz

Sicherheit in 3D: Zunehmender Einsatz von Drohnen schafft neue Bedrohungslage

Umweltbilanz von Rechenzentren optimieren

Und mehr!

AXIS COMMUNICATIONS

Inhaltsverzeichnis

Heute sind mehr Menschen als je zuvor auf Rechenzentren angewiesen, da moderne Verhaltensmuster eine immer größere Datenflut erzeugen und diese Daten auch sicher verwahrt werden müssen.Fortschritte bei der künstlichen Intelligenz (KI), das Aufkommen von 5G, Video-on-Demand und eine ständig wachsende Anzahl von IoT-Geräten machen die Herausforderung nur noch größer.

Da die Rechenzentren jedoch immer größer werden und immer stärker geografisch verstreut sind, wird es immer schwieriger, ihren Betrieb zu überwachen und ihre Sicherheit zu gewährleisten. Axis nutzt sein Know-how und seine Erfahrung, um mit führenden Rechenzentren in ganz Europa zusammenzuarbeiten und diese auf vielfältige Weise zu unterstützen. In diesem Magazin erläutern wir einige damit verbundene Fragen und die Rolle, die die Technologie beim Unterstützen von Rechenzentren spielen kann.

Verbesserung der Standortsicherheit mit dem fünfstufigen Ansatz von Axis
Der fünfstufige Sicherheitsansatz von Axis deckt die Bereiche Eingrenzung, Gelände, Gebäude, Serverräume und Server-Racks ab. Durch den Einsatz von netzwerkfähiger Videosicherheit mit Analysefunktionen direkt im digitalen Endgerät ist Axis in der Lage, eine intelligente physische Sicherheitslösung zu implementieren. Das erhöht die Sicherheit, verbessert Betriebsabläufe und ermöglicht so eine größere Widerstandsfähigkeit und mehr Effizienz.

Erkennen von Drohnenaktivitäten zur Risikominderung
Die Anwesenheit von Drohnen im Umkreis des Rechenzentrums stellt ein wachsendes Risiko dar, das die Leiter von Rechenzentren dazu veranlassen sollte, die Sicherheit nicht mehr nur zweidimensional zu betrachten, sondern auch den Luftraum besser zu schützen. Der Einsatz spezieller Software zur Drohnenerkennung auf der Grundlage der von ihnen ausgesendeten RF-Hochfrequenzsignale wird durch die Netzwerk-Kameratechnologie von Axis ergänzt. Dadurch wird der Betreiber frühzeitig vor einer sich nähernden Drohne gewarnt und erhält Hinweise auf deren Absichten.

Verbessern der CO2-Bilanz und Erreichen von Nachhaltigkeitszielen
Die Leiter von Rechenzentren müssen die verwendeten Systeme, Produkte und Materialien genau unter die Lupe nehmen, um Fortschritte beim Reduzieren der CO2-Emissionen und Erreichen von Nachhaltigkeitszielen zu erzielen. Vertrauensvolle Partnerschaften, der Einsatz wiederverwendbarer Materialien und die richtige Technologie können zu einem umweltfreundlicheren und nachhaltigeren Betrieb von Rechenzentren führen. Axis kann Sie dabei gut unterstützen.

Die Rolle von Netzwerk-Kameras bei der digitalen Transformation
Rechenzentren können vorhandene Sensortechnologie kombinieren, um ihre Betriebsabläufe mittels moderner Business Intelligence zu verbessern. Die von Axis Kameras generierten Daten, die sich als intelligente Sensoren einsetzen lassen, können in moderne Data-Center-Infrastructure-Management-(DCIM)-Systeme integriert werden. Dies führt z. B. durch verbesserte Kühllösungen zu Effizienzsteigerungen. Gut informierte Ingenieure sind in der Lage, sofort zu handeln und alle Probleme zu beheben, wenn ihnen genaue Informationen vorliegen.

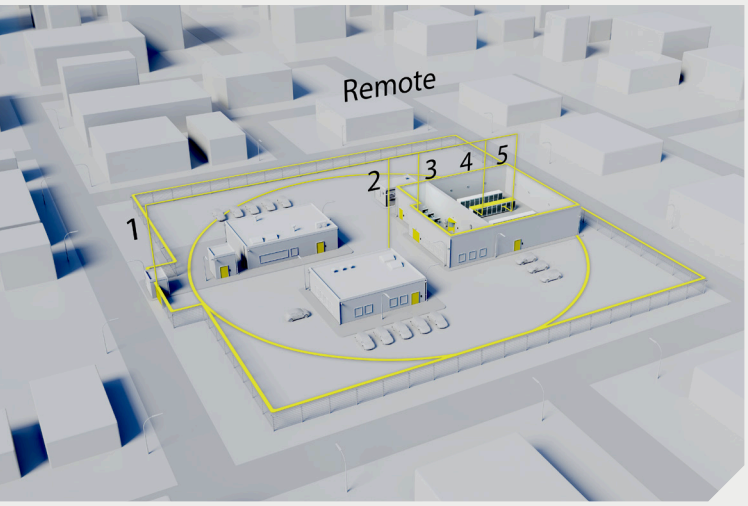
Verbessern der physischen Sicherheit durch Interoperabilität der Geräte
Die zunehmenden physischen Bedrohungen erfordern den Einsatz innovativer und vernetzter Technologien für einen intelligenteren Ansatz bei der Sicherheit von Rechenzentren. Da sie effektiv miteinander kommunizieren können die physischen Sicherheitslösungen von Axis eine wichtige Rolle beim Schutz des Rechenzentrums spielen. Dies führt zu einem wahrhaft intelligenten, weitgehend autonomen Abwehrsystem mit maximaler Schutzwirkung.

Wir hoffen, dass der Inhalt unseres Magazins für Sie nützlich ist und zum Nachdenken anregt. Ganz gleich, um welche Herausforderung es sich handelt: Axis arbeitet eng mit seinen Partnern und Kunden zusammen, um innovative Lösungen zur Schaffung einer intelligenteren und sichereren Welt zu entwickeln.

Ich wünsche Ihnen ein erfolgreiches Jahr.
Peter Dempsey, Key Account Manager, End Customers – EMEA

Mehr Sicherheit in Rechenzentren durch fünfstufigen Ansatz

Das Wachstum von Cloud-Services und Hyperscale Computing bedeutet, dass mehr Menschen als je zuvor auf die schiere Leistung und Kapazität von Rechenzentren angewiesen sind. Zudem steigt der Datenverbrauch aufgrund moderner Verhaltensmuster rapide an.



Rechenzentren werden immer größer und liegen oft abseits der Städte. Die Überwachung ihres Betriebs und die Gewährleistung eines hohen Sicherheitsniveaus ist eine Herausforderung und die Betreiber geraten zunehmend unter Druck, den Schutz vor physischen und Cyberbedrohungen zu gewährleisten. Jede Betriebsunterbrechung könnte sich als katastrophal erweisen, da Ausfallzeiten erhebliche Kosten verursachen und den Alltag der Menschen und Unternehmen, die sich auf die nahtlose Datenübertragung verlassen, massiv beeinträchtigen. Deshalb müssen geeignete Tools und Technologien für einen umfassenden und übergreifenden Schutz eingesetzt und gleichzeitig muss sichergestellt werden, dass diese Lösungen vollständig skalierbar sind, um so mit der stetigen Expansion der Rechenzentren Schritt zu halten.

Umfassende Standortsicherheit – innen und außen

Integrierte Video- und Audiolösungen von Axis können eingesetzt werden, um Rechenzentren zu schützen und einen reibungsloseren Betrieb zu gewährleisten. Unser fünfstufiger Ansatz deckt Umgrenzung, Gelände, Gebäude, Serverräume und Server-Racks ab und verwendet netzwerkfähige Sicherheitsprodukte mit integrierten Analysefunktionen. Das Erkennen und die Lösung von Vorfällen wird zum Kinderspiel.

Axis Netzwerk-Video und -Audio hilft beim Schutz der Umgebung des Rechenzentrums, indem Videosicherheitskameras, Wärmebildkameras und Radar eingesetzt werden, um Bewegungsabläufe am oder in der Nähe des Standorts zu erkennen und Eindringlinge zu verfolgen, die sich zu Fuß oder in einem Fahrzeug nähern. Über die Netzwerk-Lautsprecher können automatische Warnungen und Alarme ausgelöst werden, um potenzielle Kriminelle abzuschrecken. Diese können auch vom Personal genutzt werden, um Eindringlinge direkt in Echtzeit anzusprechen. Da eine solche Technologie, die auf leistungsstarken Analysefunktionen beruht, sehr genau ist, führt sie zu weniger Fehlalarmen und dadurch zu Kosteneinsparungen.

Auf dem Gelände werden an allen Zugangspunkten Zutrittskontrollsysteme eingesetzt, die die Videosicherheit als zweiten Authentifizierungsfaktor nutzen, um den Zutritt zu identifizieren, zu authentifizieren und zu autorisieren. Dabei werden auch Analysefunktionen zur Gesichtserkennung eingesetzt, um den Zutritt zu Gebäuden, Räumen und sogar einzelnen Server-Racks zu verwalten. Netzwerk-Audio kann auch eine Rolle beim Schutz vor Kriminalität aus internen Quellen spielen, indem Alarme und Warnungen durch Netzwerk-Kameras ausgelöst werden, die die zahlreichen Gebäude des Rechenzentrums auf ungewöhnliche Aktivitäten überwachen. Zu solchen Aktivitäten gehören beispielsweise der unbefugte Zugriff auf ein Server-Rack oder Versuche, sich zu unerwarteten Zeiten Zutritt zu kontrollierten Bereichen zu verschaffen.

Ein hochsicheres, aber auch vollständig skalierbares System, das mit dem Wachstum des Rechenzentrums Schritt halten kann, ist angesichts der großen Datenmengen unerlässlich. Jedes Gerät, das nicht ausreichend geschützt ist, kann von internen Bedrohungsakteuren oder von Personen, die versuchen, von außen auf das Gerät zuzugreifen, kompromittiert werden. Axis geht diese Probleme an, indem die Cybersicherheit der Geräte durch Firmware-Upgrades, Updates und Wartungstests kontinuierlich verbessert wird.

Axis bietet eine breite Palette an Netzwerklösungen für moderne Rechenzentren an, die verschlüsselte Kommunikation, IP-Adressfilterung, Secure Boot und signierte Firmware ermöglichen, um die Sicherheit von Anlagen und Einrichtungen zu gewährleisten. Der Ansatz von Axis stellt sicher, dass Cybersicherheit nicht nachträglich, sondern von Anfang an mit bedacht wird.

5 Schutzebenen

- Umgrenzung
- Gelände
- Gebäude
- Serverräume
- Server-Racks

Unterstützung von Rechenzentren bei der Umstellung auf digitale Netzwerk-Kameras

Daten sind wahrscheinlich unsere wertvollste strategische Ressource. Das gilt aber nur, wenn wir sie effizient nutzen. Datensilos helfen, den Zugriff auf einzelne Systeme zu sichern. Sie stellen aber auch eine verpasste Chance dar, denn Daten zu vereinheitlichen ist der Schlüssel zu einer wirklich leistungsfähigen Business Intelligence.

Die Integration von Daten und die Verknüpfung von Sensoren und Aktoren mit künstlicher Intelligenz führt zu verwertbaren Erkenntnissen, die in vielen Branchen und Sektoren zu erheblichen Effizienzsteigerungen führen können.

Richtig analysierte Daten verbinden Dienstleistungen mit den Menschen, die sie in Anspruch nehmen, und integrieren ein umfassendes System zu einem effizienten Ganzen. Aber warum ist das im Rechenzentrum nicht immer der Fall? Energieeffizienz, Anlagensicherheit und Servicequalität rücken heute immer mehr in den Vordergrund. Darüber hinaus müssen sich Rechenzentren mit gestiegenen Anforderungen an Rechenleistung und Wärmebedarf auseinandersetzen, da die Kunden immer komplexere Datenanalysen verlangen. Obwohl die Gebäudesicherheit und Hardware und Hardware-Management oft in getrennten Silos implementiert sind, müssen die Rechenzentren alle verfügbaren Ressourcen nutzen, um diesen Anforderungen gerecht werden..

Das neue Paradigma der intelligenten Netzwerktechnologie

Glücklicherweise erwächst die Notwendigkeit für eine entsprechende Anpassung zu einer Zeit, in der die dafür erforderlichen Instrumente leichter verfügbar sind als je zuvor. IoT-Geräte verfügen jetzt über mehr Möglichkeiten, um Daten zu sammeln, zu verarbeiten und intern zu analysieren. Da sie direkt im Endgerät implementiert sind, reduzieren sie die Bandbreitenanforderungen erheblich, senken die externen Verarbeitungsanforderungen und verringern die End-to-End-Latenz von 100–250 ms auf 10–20 ms*, da die Notwendigkeit entfällt, ständig große Datenmengen zwischen den Cloud-Servern hin und her zu senden.

Endlich sprechen IoT-Geräte dieselbe Sprache wie alle anderen Geräte. Die wachsende Beliebtheit des Message Queue-Telemetry-Transport-(MQTT)-Protokolls, das auf der branchentypischen TCP/IP-Netzwerktechnologie aufsetzt, bedeutet, dass sich die Daten aus diesen Geräten einfacher in server- oder cloudbasierte Anwendungen integrieren lassen als je zuvor. Zudem ist MQTT quelloffen und basiert auf offenen Standards. Dadurch lassen sich neue Endpunkt-Integrationen oder -Automatisierungen, die auf seinen Daten basieren, sehr einfach entwickeln. Es gibt also keinen Grund mehr, warum die Sicherheitssysteme eines Rechenzentrums in einem von den Data-Center-Infrastructure-Management-(DCIM)-Sensoren getrennten Netzwerk betrieben werden müssen.

Die immer wichtigere Rolle von Netzwerk-Kameras

Durch seine offene Beschaffenheit bietet das MQTT-Protokoll die Möglichkeit, Daten zu integrieren, die den Anforderungen moderner DCIM-Systeme gerecht werden, indem Netzwerk-Kameras als intelligente Sensoren eingesetzt werden. Nehmen wir beispielsweise die Wärmeüberwachung. Ein interner Wärmesensor könnte einen Hotspot an einem Server-Rack erkennen und seine Daten an eine Wärmebildkamera weiterleiten. Diese Kamera könnte dann ein Bild mit allen relevanten Daten an ein Video Management System weiterleiten, sodass ein Techniker einen echten visuellen Hinweis darauf erhält, wo das Problem liegt. Eine Kombination von Daten aus einer Vielzahl von Sensoren kann wiederum zu einer höheren Effizienz führen, z. B. zur Feinabstimmung von Kühllösungen für eine optimale Energienutzung.

Die Suche nach neuen Wegen zur Nutzung der von Netzwerk-Kameras erfassten Daten ist eine weitere Möglichkeit, um die Kosten und Komplexität von DCIM-Lösungen erheblich zu reduzieren. Rechenzentren bemühen sich um Effizienzsteigerungen, wo immer es ihnen möglich ist. Daher könnte sich der Einsatz von Netzwerk-Kameras bei einer Vielzahl von Anwendungen als kluger Schachzug erweisen. Darüber hinaus können diejenigen, die bereits Kameras für Sicherheitszwecke einsetzen, das volle Potenzial dieser Geräte auch zum Erzielen operativer Vorteile nutzen.

Es ist an der Zeit, dass das wahrhaft intelligente Rechenzentrum zur neuen Norm wird. Das bedeutet nicht, dass bestehende DCIM-Lösungen über Bord geworfen oder kritische Sensoren ausgetauscht werden müssen – es bedeutet lediglich, dass alle vorhandenen Daten restlos genutzt werden müssen, um neue Möglichkeiten zu schaffen und das Potenzial moderner vernetzter Geräte und Lösungen maximal auszuschöpfen.

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

Sicherheit in 3D

Zunehmender Einsatz von Drohnen schafft neue Bedrohungslage

Drohnen entwickeln sich zusehends zu einem Verkaufsschlager, da ihre legitime Funktion in Unternehmensumgebungen erhebliche operative Vorteile mit sich bringt. Ihr erwarteter Beliebtheitszuwachs[1] wird jedoch nicht ohne Folgen für die Sicherheit bleiben. Im Jahr 2018 musste der britische Flughafen Gatwick ausgerechnet zu Weihnachten für 33 Stunden geschlossen werden, wovon über 140.000 Passagiere betroffen waren. Trotz mehrerer Augenzeugenberichte konnte die Anwesenheit einer Drohne letztlich nicht bestätigt werden[2].

Damit wurde ein großes Problem offensichtlich. Die Methoden des Perimeterschutzes wurden durch eine Drohne, die es schon für ein paar Hundert Euro zu kaufen gibt, aber der Luftfahrtindustrie Schäden in Millionenhöhe verursachte, effektiv ausgehebelt. Und wenn man an die möglichen Nutzlasten denkt, die Drohnen transportieren können, die von einer Kamera zur feindlichen Aufklärung bis zu Geräten, die ein WLAN-Signal kapern können, um Softwarelösungen und Systeme zu stören, oder im schlimmsten Fall sogar eine biologische Waffe, dann wird das Problem in seinem vollen Ausmaß deutlich.

Erkennen, identifizieren und lokalisieren

Innerhalb der Rechenzentren ist die Gewährleistung eines hohen Sicherheitsniveaus durch den Schutz vor physischen und Cyberbedrohungen eine entscheidende Fähigkeit. Jede Ausfallzeit hätte erhebliche Kosten zur Folge und würde die Menschen und Unternehmen, die dermaßen stark auf eine reibungslose Datenübertragung angewiesen sind, massiv beeinträchtigen.

Moderne netzwerkfähige Systeme bringen erhebliche Fortschritte bei den Möglichkeiten des Perimeterschutzes mit sich, indem sie Videosicherheitskameras, Wärmebildkameras und Radar zum Verfolgen der Bewegungsabläufe von Eindringlingen miteinander vereinen. Und obwohl sich die Sicherheit in den Rechenzentren in den letzten Jahren ungemein erhöht hat, muss man dennoch stets mit neuen Bedrohungen rechnen, um diesen einen Schritt voraus zu sein. Und diese neue Bedrohung kann jetzt buchstäblich aus heiterem Himmel kommen.

Durch den Einsatz spezieller Software zur Ergänzung netzwerkfähiger physischer Sicherheitslösungen können Drohnen nun anhand der von ihnen ausgesendeten RF-Hochfrequenzsignale erkannt werden. Damit lassen sich Marke und Modell von mehr als 200 Drohnen identifizieren, darunter kommerzielle, Hobby- und Eigenbau-Drohnen. Selbst der Standort des Drohnenpiloten lässt sich ermitteln. Diese Technologie ist weitaus leistungsfähiger, als sich allein auf die Augen und Ohren des Sicherheitspersonals zu verlassen, da sie eine Vorwarnung vor einer sich nähernden Drohne und frühe Hinweise auf deren Absichten liefern kann.

Obwohl der Einsatz von Drohnen vielversprechend ist, wenn er einem legitimen Zweck dient und vorschriftsgemäß erfolgt, müssen wir uns wie bei vielen anderen Dingen auch über ihre möglichen Tücken im Klaren sein.

Drohnenanalyse und Bedrohungsabwehr

Sobald eine Drohne entdeckt wurde, ist es wichtig, den Grund für ihre Anwesenheit zu ermitteln. Da sich Rechenzentren in der Regel in einer für sie eingerichteten Flugverbotszone befinden, müssen Sicherheitskräfte oder die Polizei schnell zwischen einem unvorsichtigen Drohnenpiloten und einem Bedrohungsakteur mit böswilligen Absichten unterscheiden können. Durch die Ortung einer Drohne und die Erkennung der Signale, die von der Fernsteuerung des Piloten ausgesendet werden, kann Sicherheitspersonal entsandt werden, um mit dem Piloten zu sprechen.

Bei der Überprüfung eines Vorfalls ist eine schnelle Identifizierung unerlässlich, um zeitnah Entscheidungen treffen zu können. Eine spezielle Erkennungssoftware, die ein Signal an eine PTZ-Kamera (Pan/Tilt/Zoom) senden kann, hilft, die Bewegungen einer Drohne zu erfassen und zu verfolgen. Die gestochen scharfen Bilder können dazu verwendet werden, den Inhalt der Nutzlast bis ins kleinste Detail zu bestimmen und Freund von Feind zu unterscheiden.

Eine Drohnenerkennungslösung, die im Rahmen einer Partnerschaft entwickelt wird

Angesichts der zunehmenden Bedrohung durch Drohnenaktivitäten hat Axis mit seinem Partner Dedrone zusammengearbeitet, um eine einzigartige Branchenlösung für eine intelligentere Luftraumsicherheit zu entwickeln. Dabei ist die Datenerfassung der Schlüssel zum Erfolg der Lösung. Bisher wurden über 17 Millionen Drohnenbilder verwendet, um eine kamerabasierte KI/ML-Software zu trainieren, damit diese selbst stark getarnte Drohnen zuverlässig identifizieren kann. Darüber hinaus liefern als RemoteID bekannte Fernidentifizierungsprotokolle Informationen zur Überprüfung der Legitimität einer Drohne. Damit werden auch die Bedrohungserkennungsfähigkeiten der Software verbessert.

Obwohl der Einsatz von Drohnen vielversprechend ist, wenn er einem legitimen Zweck dient und vorschriftsgemäß erfolgt, müssen wir uns wie bei vielen anderen Dingen auch über ihre möglichen Tücken im Klaren sein.

Mit einer solchen Lösung lässt sich der Himmel im Umkreis des Rechenzentrums genauso zuverlässig überwachen wie der Boden. Die Integration in bestehende Videoverwaltungssysteme bedeutet auch, dass eine Drohnenerkennungslösung Teil eines übergreifenden und integrierten Systems sein kann, um die gesamte Sicherheitslage zu verbessern.

[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

Unterstützung von Rechenzentren bei der **Optimierung ihrer physischen Sicherheit** durch Interoperabilität von Geräten

Obwohl bereits viel über das hohe Cybersicherheitsniveau geschrieben wurde, das zum Schutz von Rechenzentren erforderlich ist, bleibt die physische Sicherheit ein Problem. Eine Geschichte, die es in den USA in die Mainstream-Medien schaffte, betraf die Verhaftung eines Mannes, der angeblich ein Komplott zur Sprengung eines großen Rechenzentrums im US-Bundesstaat Virginia* geschmiedet hatte. Wenn man bedenkt, welche Maßnahmen ergriffen werden sollten, um eine solche Bedrohung abzuwehren, liegt die Einführung von fortschrittlichen physischen Sicherheitslösungen auf der Hand. Was jedoch nicht immer offensichtlich ist, ist die Fähigkeit solcher Lösungen, Sicherheit und Schutz zu gewährleisten, wenn sie zur Abwehrmaximierung miteinander vernetzt werden.

Innovationen bei Radar und Netzwerk-Video

Netzwerk-Kameras haben sich bereits so weit entwickelt, dass man ihre integrierten Analysefunktionen nutzen kann, um Bewegungen zu kategorisieren (d. h. Eindringen im Gegensatz zu Herumlungern) und Personen an der Eingrenzung eines Standorts von Fahrzeugen und Objekten zu unterscheiden. Die Genauigkeit moderner Kameras ist so hoch, dass sich die Zahl von Fehlalarmen stark reduziert. Darüber hinaus stellt die Verarbeitung direkt im Endgerät sicher, dass nur die notwendigsten Daten zur Analyse über das Netzwerk zurückgesendet werden. Dies ermöglicht eine schnellere Entscheidungsfindung und spart Zeit und Geld.

Obwohl physische Sicherheitslösungen eine wichtige Rolle beim Schutz von Rechenzentren spielen können, führt jedoch erst ihre Fähigkeit, effektiv miteinander zu kommunizieren, zu einem wahrhaft intelligenten, weitgehend autonomen System. So kann beispielsweise eine kombinierte Radar- und Kameralösung Bewegungsabläufe am Rand der Umgrenzung erkennen und klassifizieren und dadurch wiederum eine Wärmebildkamera aktivieren, die eine Wärmesignatur sowie weitere Beweise für die Anwesenheit unbefugter Personen erkennt. Anschließend wird eine PTZ-Kamera (Schwenken/Neigen/Zoomen) zur Bewegungsverfolgung eingesetzt, während ein IP-Audio-Lautsprecher eine zuvor aufgezeichnete Ansage zur Abschreckung abspielt. Eine IP-Stroboskopsirene wird aktiviert, wenn sich der Eindringling weiter nähert, und gibt als letzte Warnung gleichzeitig einen Licht- und Tonimpuls ab.

Natürlich kann eine Bedrohung auch von anderen Faktoren ausgehen. Innerhalb der Einrichtung können Netzwerk-Kameras mit integrierten Analysefunktionen als erste Anlaufstelle genutzt werden, um Gaslecks oder Rauch zu erkennen, während vernetzte Kameras und Sensoren Wasserlecks erkennen können.

Wärmebildkameras mit Messfunktion können eine entscheidende Rolle beim Erkennen eines Anstiegs der Umgebungstemperatur spielen, der auf ein größeres Problem hindeuten könnte. Bei der Überwachung von Stromgeneratoren wird beispielsweise schon bei der geringsten Temperaturschwankung ein Alarm ausgelöst, sobald ein zuvor festgelegter Temperaturgrenzwert erreicht wird.

Partnerschaften für einen umfassenden Schutz

Das Zentrum für den Schutz nationaler Infrastrukturen (Centre for the Protection of National Infrastructure, CPNI) hat Leitlinien und Standards für alle kritischen nationalen Infrastrukturen entwickelt. Dazu zählen auch Rechenzentren, da diese wichtige Dienstleistungen erbringen. Die Zusammenarbeit mit einem vertrauenswürdigen Anbieter von physischen Sicherheitslösungen, die vom CPNI zugelassen wurden, gibt den Leitern von Rechenzentren die Gewissheit, dass die von ihnen gewählten Produkte von bester Qualität sind und hohe Standards erfüllen.

Durch die Auswahl von Tools, die auch im Bereich Innovation führend sind, profitieren Rechenzentren von vernetzten und autonomen physischen Sicherheitslösungen, die ihnen Schutz auf höchstem Niveau bieten.

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

Unterstützung von Rechenzentren in Hinblick auf eine bessere Umweltbilanz und mehr Nachhaltigkeit

Es wird erwartet, dass der globale Markt für umweltfreundliche Rechenzentren bis zum Jahr 2026 ein Volumen von 142,8 Milliarden US-Dollar bei einer jährlichen Wachstumsrate (CAGR) von fast 20 % erreichen wird[1]. Für Betreiber solcher Rechenzentren bedeutet das, dass sie nicht nur einen robusten und hochsicheren Datenspeicher bieten, sondern auch ihre Energieeffizienz optimieren müssen, um die Umweltbelastung zu verringern. Dies ist vor allem im Hinblick auf die Verpflichtung des Pakts für klimaneutrale Rechenzentren (Climate Neutral Data Center Pact) wichtig, der die Klimaneutralität von Rechenzentren bis zum Jahr 2030 vorsieht[2].

Um diese und andere Nachhaltigkeitsziele zu erreichen, ist in vielen Rechenzentren jedoch ein erhebliches Umdenken erforderlich. Dabei geht es nicht nur um den enormen Energie- und Wärmeverbrauch, sondern auch um die Frage, wie die Auswirkungen auf die Umwelt reduziert werden können. Verständlicherweise wächst der Druck auf Rechenzentren, die noch nicht im Einklang mit Nachhaltigkeitsinitiativen arbeiten, sich stärker auf die Erreichung von Nachhaltigkeitszielen zu konzentrieren. Die Herausforderung für die Betreiber von Rechenzentren besteht darin, die Nachhaltigkeit zu verbessern und gleichzeitig ihren Kunden weiterhin den bestmöglichen Service zu bieten.

Nachhaltige Rahmenbedingungen und vertrauenswürdige Lieferketten

Ein stärkeres Bewusstsein dafür, wie positive Maßnahmen sich auf die Umwelt auswirken können, zieht Unternehmen an, die sich in ähnlicher Weise für Nachhaltigkeit engagieren[3]. Die Einhaltung internationaler Rahmenwerke und Standards, wie z. B. des Global Compact der Vereinten Nationen, den Axis unterzeichnet hat[4], kann Unternehmen dabei helfen, die Nachhaltigkeitsziele der Vereinten Nationen (Sustainable Development Goals, SDGs)5 zu erreichen und zu zeigen, dass sie sich nicht nur mit Worten, sondern auch mit Taten engagieren.

In der Tat spricht die Einhaltung international anerkannter Rahmenwerke auch für gemeinsame Werte. Da der Schwerpunkt mehr denn je auf einer höheren Kosteneffizienz, dem Zugang zu Hightech-Fähigkeiten, einer besseren Servicebereitstellung und der Innovationsförderung liegt, spielen Partnerschaften eine entscheidende Rolle. Da Unternehmen engere Allianzen anstreben, sollten sich alle Beteiligten in der Lieferkette an Grundwerten orientieren, um Vertrauen aufzubauen.

Verbessern der CO2-Bilanz und Erreichen von Nachhaltigkeitszielen

Die Tatsache, dass Rechenzentren große Mengen an Strom verbrauchen und viel Wärme erzeugen, gibt umweltbewussten Managern zu denken. Obwohl es keine einfache und schnelle Lösung gibt, müssen die Leiter von Rechenzentren die verwendeten Systeme, Produkte und Materialien genau unter die Lupe nehmen, um Fortschritte beim Reduzieren der CO2-Emissionen und Erreichen von Nachhaltigkeitszielen zu erzielen. Dies schließt auch die Beschaffung von Produkten bei Lieferanten ein, bei denen ein niedriger Stromverbrauch eine hohe Priorität hat.

Durch den Einsatz von Analytik direkt in den Axis Netzwerk-Kameras selbst können Bandbreite und Stromverbrauch reduziert werden. Die Zipstream-Technologie von Axis reduziert den Bandbreiten- und Speicherbedarf um durchschnittlich 50 % und trägt so zu einer umweltfreundlicheren Geschäftsstrategie bei.

Axis unterstützt Rechenzentren dabei, ihre Nachhaltigkeit zu verbessern, indem wir innovative Lösungen für höchste Sicherheit bei geringstmöglicher Umweltbelastung bieten. Durch die sorgfältige Auswahl von Materialien und die Verpflichtung zur Abfallvermeidung in unseren Prozessen zeigen wir, dass wir unsere Verantwortung über die gesamte Produktionskette hinweg ernst nehmen. Damit verpflichten wir uns, Rechenzentren beim Erfüllen ihrer Umweltschutzziele zu unterstützen und gleichzeitig Innovationen für eine intelligentere, sicherere und nachhaltigere Welt hervorzubringen.

Empfohlene Lösungen für Rechenzentren

Axis
Radar-Fusions-kameras

Video und Radar in einem Gerät: Schützen Sie große Bereiche mit zwei leistungsstarken Technologien und 24/7-Erkennung zuverlässig vor Eindringlingen. Diese Kamera überzeugt mit modernster Objektklassifizierung auf Basis von Deep Learning und setzt damit neue Maßstäbe für Erkennung und Visualisierung.

Axis
PTZ-Kameras

Die PTZ-Kameras überwachen dank der Schwenk, Neige und Zoom-Funktionalität große Bereiche in Echtzeit. Die AXIS Q61-Serie sorgt oberhalb und unterhalb des Horizonts in jeder Richtung für absolute Szenentreue und perfekte Bildqualität. Die Modelle der Serie sind somit besonders beim Überwachen von leicht unebenem Gelände unschlagbar. Die AXIS Q62-Serie umfasst besonders robuste Kameras, die allen Wetterbedingungen standhalten. Die AXIS Q63-Serie überzeugt mit schnellem Zoom und Laserfokus selbst bei Dämmerung bis nahezu Dunkelheit. Dank der Speed-Dry-Funktionalität sind die Bilder, selbst wenn es regnet, gestochen scharf.

AXIS Q1961-TE
Thermal Camera

Mit dieser halogenfreien thermografischen Kamera können Sie Temperaturen aus der Ferne überwachen und temperaturbasierte Ereignisse auslösen. Sie eignet sich ideal zum Verbessern der betrieblichen Effizienz. Sie ist robust und schlagfest, verfügt über Analysefunktionen zur Brandfrüherkennung sowie integrierte Cybersicherheitsfunktionen.

Axis
Zutrittskontrolle

Axis bietet die Hardware und Analysefunktionen zur Identifizierung, Authentifizierung und Autorisierung des Zutritts zu Gebäuden und Räumen. Unsere Technologie zur Zutrittskontrolle schützt kritische oder sensible Bereiche durch automatische (Schlüsselkarten, PIN-Codes, QR-Codes) oder manuelle Authentifizierung (2-Wege-Netzwerk-Video und -Audio).

Axis
Netzwerk-Lautsprecher

Mit den Axis Netzwerk-Lautsprechern können Sie unerwünschte Aktivitäten unterbinden und die von den Kameras erkannten Täter abschrecken. Beispielsweise lassen sich die Lautsprecher dafür nutzen, um unerwünschte Anwesenheit/Aktivitäten an der Eingrenzung des Standorts zu verhindern. Die Lautsprecher können auch verwendet werden, um in Notfällen Sprachanweisungen zu geben oder auf Falschparken hinzuweisen.

Warum Axis?

Cybersicherheit fördern

Cyberattacken auf die Infrastruktur oder Datendiebstahl können katastrophale Folgen für eine Stadt haben. Wir wären äußerst angreifbar, wenn beispielsweise Kameras in Ampelanlagen gehackt würden. Die Abwehr solcher Bedrohungen steht daher ganz oben auf der Agenda der Behörden. In Sachen Schutz, Sicherheit und Rechtskonformität von Daten einer Smart City liefert Axis als führender Anbieter sicherer Lösungen stets Bestnoten ab. Wir sind Experten darin, in jedem Baustein unserer Lösungen Risiken einzuschätzen und Datenschutzprozesse zu implementieren, die alle aktuellen und künftigen Gesetze, Vorschriften und Richtlinien erfüllen.

Unsere Arbeit zeichnet sich durch Qualität aus

Wir bei Axis handeln und arbeiten immer qualitätsorientiert. Alle unsere Produkte sind so gebaut, dass sie auch schwierigen Bedingungen standhalten und widerstandsfähig gegen Vandalismus und Wettereinflüsse sind. Die Produkte wurden ausgiebig getestet, um sicherzustellen, dass sie langlebig sind und unter allen Bedingungen gestochen scharfe Bilder liefern. Unser Qualitätsbewusstsein spiegelt sich in den hervorragenden HDTV-Bildern unserer Kameras wider. Die Qualität ist so hoch, dass sie als Beweismittel vor Gericht Bestand haben.

Die Stärke von Partnerschaften

Da die offene Plattform von Axis flexibel, skalierbar und leicht zu integrieren ist, lässt sie sich mit der Hard- und Software zahlreicher anderer Anbieter kombinieren.

Innovative Technologie

Wir streben ständig danach, das Beste aus Technologie und menschlichem Einfallsreichtum zu kombinieren, um unsere Produkte noch leistungsstärker zu machen. Die Analyse und Nutzung von Daten von Daten direkt im Endgerät setzt sich immer stärker durch und kann Ihnen entscheidungsrelevante Erkenntnisse liefern.

Erfahren Sie mehr über Axis-Lösungen für Rechenzentren:
www.axis.com/de-de/solutions/data-centers

Über Axis Communications

Axis ermöglicht eine smartere und sichere Welt durch die Entwicklung von Lösungen zur Verbesserung von Sicherheit und Geschäftsperformance. Als Technologieführer im Bereich Netzwerk-Video bietet Axis Produkte für die Videosicherheit und Zutrittskontrolle sowie Intercoms, Audiosysteme und intelligente Analyseanwendungen. Die branchenweit anerkannten Schulungen der Axis Communications Academy vermitteln fundiertes Expertenwissen zu den neuesten Technologien.

Das 1984 gegründete schwedische Unternehmen beschäftigt etwa 4.000 engagierte MitarbeiterInnen in über 50 Ländern und bietet mit Technologie- und Systemintegrationspartnern auf der ganzen Welt kundenspezifische Lösungen an. Der Hauptsitz ist in Lund, Schweden.

Weitere Informationen über Axis finden Sie unter www.axis.com/de-de