WHITEPAPER

Perimeterschutz mit intelligenter Überwachung

Eine Studie der Sensoroptionen, Anwendungen und Schlüsselaspekte für eine zukunftsfähige Sicherheitslösung in einer Reihe von Branchen

Juli 2021

AXIS COMMUNICATIONS

Inhalt

1 Zusammenfassung

Ein Zaun ist oft eine fundamentale Komponente der ‚äußeren Schutzebene' eines Standorts, und er kann als Barriere, als Bildschirm oder als Abschreckungsinstrument sowohl für Personen als auch Tiere fungieren. Weitere Merkmale lassen sich integrieren, um die Wirksamkeit des Zauns zu erhöhen, denn jede physische Barriere kann ein Eindringen nur hinauszögern oder behindern.

Verschiedene Typen von Meldern kommen an Zäunen entlang zum Einsatz. Kabelbasierte Melder können dem Weg des Zauns folgen, und Radarsensoren (Mikrowellen), Infrarotbarrieren oder Laser können an strategischen Punkten positioniert werden.

Alle Typen von Meldern können Fehlalarme hervorrufen, die beispielsweise von Tieren, Pflanzen und Bäumen in Bewegung und schlechtem Wetter verursacht werden. Es kann auch noch weitere hemmende Faktoren geben, etwa Frequenzüberschneidungen beim Einsatz von Mikrowellensensoren oder physischen Installationen in der Installationsumgebung.

Kameras bieten einen offensichtlichen Vorteil für diejenigen, die große Bereiche oder mehrere Standorte überwachen wollen. Moderne vernetzte Videolösungen kombinieren die elektronische Verarbeitung in der Kamera mit künstlicher Intelligenz. Die inhärente Flexibilität, Effektivität und Abschreckungswirkung der Technologie bedeutet, dass Videokameras potentiell eine äußerst kosteneffiziente Ergänzung eines Sicherheitssystem darstellen.

Auch wenn Kameras und Bewegungserkennungssoftware die Reichweite und Fähigkeiten des Perimeterschutzes vergrößert haben, können solche Lösungen dadurch eingeschränkt sein, dass sie bei widrigen Witterungsbedingungen nicht erfassen können. Wenn Wärmebildkameras einwandfrei kalibriert und mit Videoanalyse gekoppelt sind, leisten sie effektive Überwachung, die von den Lichtverhältnissen unbeeinflusst und von Wetterextremen buchstäblich unbehindert bleibt.

Videoanalysefunktionen wurden im Laufe der Zeit erheblich weiterentwickelt und sind nun selbst in Kameras üblich, die für den Markt der Heimanwendungen bestimmt sind. Analysefunktionen können den Speicherbedarf reduzieren, indem sie nur Video aufzeichnen, das Aktivität von Interesse enthält. Indem das aufgezeichnete Video soweit wie möglich innerhalb der Kamera selbst verarbeitet wird, nimmt die Auslastung des Netzwerks deutlich ab, da von den Kameras nur relevantes Video gestreamt wird. Dadurch ergeben sich für ein Leitstellenszenario offensichtliche Vorteile.

Wie bei jeder Sicherheitsmaßnahme sollte die Bewertung einer Lösung zum Perimeterschutz sowohl angemessen als auch verhältnismäßig sein. Wie immer muss die Bedrohung höchste Priorität haben.

Ein abgestimmtes Sicherheitskonzept, das Input und Überlegungen aus anderen Abteilungen wie beispielsweise IT und Operations einschließt, wird rasch Best Practice. Dazu gehört die Notwendigkeit, möglichst früh die Personen einzubinden, die für die Technik verantwortlich sind.

Es ist bekanntermaßen schwierig, die Kapitalrendite einer Sicherheitslösung aufzuzeigen, mit der ein Ereignis verhindert werden soll. Das liegt vor allem daran, dass es keine potenziellen Einnahmen gibt, die den Kosten gegenübergestellt werden könnten. Eine besser konkretisierbare Kapitalrendite kann aufgezeigt werden; zu den Beispielen gehören Lösungen, die nicht nur Mitarbeiter bei verdächtigem Verhalten oder Eindringvorgängen warnen, sondern auch automatisierte Reaktionen produzieren.

2 Einführung

Elektronische Lösungen zum Perimeterschutz bestehen traditionell in der Aufrechterhaltung hoher Sicherheit an behördlichen und kommerziellen Standorten oder den Anwesen wohlhabender Bürger. Mit den technologischen Fortschritten, einem konkurrenzfähigeren Markt und der resultierenden Kostensenkung sind jetzt relativ hochtechnologische Lösungen für viel größere Interessentengruppen erhältlich.

Woraus besteht also eine moderne Perimeterschutzlösung? Welche Technologie kommt zum Einsatz, und wie kann sie sowohl beruhigen als auch echten Schutz bieten?

In diesem Whitepaper werden einige der üblichen sensorbasierten Optionen zum Schutz einer Umgrenzung untersucht und Einblicke in die Technologie hinter den Lösungen vermittelt.

3 Lösungen zum Perimeterschutz

3.1 Physische Lösungen

Physische Lösungen sind oft eine grundlegende Komponente der ‚äußeren Schicht' eines detaillierten Ansatzes zur Sicherung eines Standorts. In der Regel umfassen sie einen Zaun an der Umgrenzung, der oft aus Draht oder geschweißten Gittern in verschweißten Platten oder Betonplatten besteht. Ein Umgrenzungszaun dient vielen Zwecken. Einer davon ist der Aufbau einer physischen Barriere, die ein Eindringen verzögert oder verhindert. Ein Zaun kann außerdem Überwachung durch Screening eines Vermögenswerts verhindern; und er dient der Abschreckung und hindert Tiere am Eindringen. Merkmale wie beispielsweise Kletterschutz, ausgewiesene Fahrzeugzufahrten, Passierschutz und Zaunbildschirme lassen sich ebenfalls integrieren, um die Effektivität eines Umgrenzungszauns zu erhöhen.

Allerdings wird jede physische Barriere ein Eindringen nur verzögern. Deshalb sollte die Umgrenzung außerdem mit automatischer Eindringerfassungstechnologie ausgestattet sein, die verifizierbare Echtzeitalarme und Standortdaten ausgibt, Zielverfolgung leistet und den Nachweis und die Daten für die Untersuchung nach dem Ereignis packen kann.

3.2 Eindringerfassung an der physischen Umgrenzung

Oft werden zur Sicherung ausgedehnter Umgrenzungen verschiedene Arten von ‚Kabelmeldern' eingesetzt. Diese kabelbasierten Melder werden in der Regel in die Erde eingegraben oder am Zaun montiert; sie folgen dem Zaunverlauf und müssen nicht geradlinig verlegt werden. Sie bieten außerdem Abdeckung in Ecken und **erdfreien Bereichen**. Einige Lieferanten bieten Zäune, die mit automatischen Erfassungslösungen ausgestattet sind.

Wie jede Erfassungslösung können kabelbasierte Melder Fehlalarme produzieren, die als ‚Falschmeldungen' bezeichnet werden. Zu üblichen Ursachen von Falschmeldungen gehören Tiere, Pflanzen und Bäume in Bewegung sowie Unwetter. Kabelbasierte Lösungen funktionieren am besten, wenn sie durch Videoüberwachung ergänzt werden. Video kann nicht nur zur Verifizierung eines Eindringvorgangs, sondern auch zur Feststellung der Ursache eines Alarms genutzt werden. Eine kabelbasierte Lösung kann nur aufgrund des Eindringens selbst eine Warnung liefern; sie kann keine Informationen zur Anzahl der Eindringlinge oder irgendwelche sonstigen Details zur Verfügung stellen, die zur Vorbereitung einer Reaktion benötigt werden.

3.3 Andere Sensoren zur Eindringerfassung

Andere Eindringmelder wie beispielsweise Radar (Mikrowellensensoren), Infrarotbarrieren oder Laser können an strategischen Punkten rund um die Flughafenumgrenzung platziert werden. Auch diese Technologien können durch Probleme wie beispielsweise Falschmeldungen und im Hinblick auf Abstand und Höhe begrenzte Erfassungsfähigkeiten beeinträchtigt sein, wenn Installationsregeln nicht richtig eingehalten werden.

Die Nutzung von Radar an der Umgrenzung kann in einer Umgebung, in der andere elektronische Geräte im Einsatz sind, besonders problematisch sein. Diese können auf derselben Frequenz und im selben Spektrum arbeiten, und auch wenn die sorgfältige Frequenzwahl oder eine Leistungsreduzierung die Störung verringern kann, wird damit auch die effektive Reichweite des Geräts beeinträchtigt.

4 Videobasierte Lösungen

4.1 Die Anwendung von Videokameras

Die veralteten Videoüberwachungstechnologien mit Einzelgeräten haben mit den heute erhältlichen Hightech-Netzwerk-Kameralösungen kaum noch etwas gemeinsam. Moderne Netzwerklösungen können elektronische Verarbeitung in der Kamera mit künstlicher Intelligenz kombinieren. Dieses Technologieniveau steht allerdings erst seit kurzem zur Verfügung und steckt noch in den Kinderschuhen.

Kameras bieten einen offensichtlichen Vorteil für diejenigen, die große Bereiche oder mehrere Standorte überwachen wollen. Die inhärente Flexibilität, Effektivität und Abschreckungswirkung der Technologie bedeutet, dass Videokameras potentiell eine äußerst kosteneffiziente Ergänzung eines Sicherheitssystem darstellen.

Je nach der lokalen Gesetzgebung kann Kameratechnologie zur Überwachung über die physische Eingrenzung hinaus eingesetzt werden, um einen zusätzlichen Überwachungspuffer zu haben und dem Anwender potenziell mehr Reaktionszeit zu lassen. Lösungen, die Videoanalysefunktionen nutzen, lassen eine Alarmauslösung gemäß festgesetzten Regeln zu. Beispielsweise ertönt ein Alarm, wenn sich eine Person innerhalb von 50 Metern einem Zaun nähert; eine höhere Alarmstufe könnte ausgelöst werden, wenn dieselbe Person längere Zeit herumlungert oder in den Bereich von 10 Metern Abstand vordringt.

4.2 Thermographische Videoüberwachungslösungen

Die Kombination aus Videoüberwachungskameras und Bewegungserkennungssoftware hat die Reichweite und Leistungsfähigkeit von Perimeterschutzlösungen von einfacher Erfassung auf komplexe Eindringanalysen ausgeweitet. Allerdings kann die Wirksamkeit von Video dadurch stark eingeschränkt werden, dass bei widrigen Witterungsbedingungen keine Erfassung möglich ist.

Die höhere Verfügbarkeit der Wärmebildkameratechnologie hat dazu geführt, dass ihr Einsatz an der Umgrenzung dominiert. Wenn Wärmebildkameras einwandfrei kalibriert und mit Videoanalyse gekoppelt sind, können sie effektive Überwachung leisten, die von den Lichtverhältnissen unbeeinflusst und von extremen Witterungsbedingungen buchstäblich unbehindert bleibt. Sensoren, die mit Thermotechnik arbeiten, liefern einen höheren Kontrast im Vergleich zu einer typischen Kamera für sichtbares Licht und sind infolgedessen aufgrund deutlich verbesserter Eindringerfassungsfähigkeiten für den Perimeterschutz von Vorteil.

Thermosensoren erstellen anhand der von Objekten wie beispielsweise Fahrzeugen oder Personen abgegebenen Infrarotstrahlung ein Bild. In Kombination mit Videoanalyse können moderne Wärmebildkameras mit ausreichender Verarbeitungsleistung zwischen verschiedenen Typen von Eindringzielen unterscheiden und den Sicherheitsmitarbeiter ausgehend von einer vordefinierten Liste von Bedingungen warnen. Dazu könnte die Richtung und Geschwindigkeit einer Person oder eines Fahrzeugs gehören. Traditionelle Kameras können das auch, aber sie benötigen dazu sichtbares Licht. Diese Kameras werden im folgenden Abschnitt untersucht.

4.3 Kameras für sichtbares Licht

Alle Standard-Überwachungskameras für sichtbares Licht brauchen entweder natürliche oder verstärkte Beleuchtung, um Bilder zu liefern. Beleuchtung zur Unterstützung von Videoüberwachung ist aus gutem Grund ein eigenes Fachgebiet, und zu diesem wichtigen Thema wurden verschiedene Abhandlungen verfasst. Allerdings müssen wir den offensichtlich recht kritischen Punkt erneut ansprechen, dass Standardkameras sichtbares Licht benötigen. Licht kann aufgrund der offensichtlichen Wirkung jeder Änderung der Lichtqualität in jeder Umgebung eine Herausforderung darstellen. Nicht immer berücksichtigt oder verstanden, insbesondere von denen, die die Lösungen vorgeben, sind Witterungseinflüsse.

Wärmebildkameras haben ihre Vorteile, aber damit soll nicht gesagt sein, dass Wärmebildkameras ein direkter Ersatz für Kameras für sichtbares Licht sein sollten oder können - sie sind alles andere als das. Diese beiden Technologien funktionieren am besten, wenn sie in dieselbe Lösung integriert sind. Traditionelle Kameras können Objekte nicht mit der Reichweite von Wärmebildkameras erfassen; aber Wärmebildkameras können nicht die forensisch relevanten Details liefern, die Kameras für sichtbares Licht zur Verfügung stellen können. Die beiden Technologien werden oft kombiniert, wobei die Wärmebildkamera den Erfassungsalarm ausgibt und der forensische Vorteil der Kamera für sichtbares Licht sowohl im Nachweis als auch in der Zielverfolgung besteht.

4.4 Videoinhaltsanalyse

Die Netzwerk-basierte Videoüberwachung hat zu Sicherheitsmaßnahmen nie dagewesenen Umfangs geführt. Eine effektive Genehmigungshierarchie lässt kontrollierten Videozugriff, Verteilung und Speicherung für eine theoretisch unbegrenzte Anzahl von Stakeholdern zu. Insbesondere ein technologischer Fortschritt bringt sogar noch höhere Skalierbarkeit - Videoanalysefunktionen.

Die Videoanalyse hat sich im Laufe der Zeit erheblich weiterentwickelt, nicht zuletzt aufgrund der Entwicklung von IP-Kameratechnologie. Das lässt sich an Kameras aufzeigen, die für den Markt der Heimanwendungen bestimmt sind und von denen viele inzwischen gewisse Analysefunktionen umfassen, um beispielsweise Bewegung in der Szene erfassen zu können. Zusätzliche Funktionen können ‚gebündelt' mit einer Kamera erworben werden, einschließlich virtuellen Stolperdrahts, bewegter Objekte oder sogar Personenzählung.

Mit Videoanalysefunktionen kann sich Speicherbedarf erübrigen, indem nur Video aufgezeichnet wird, das Aktivität enthält. Außerdem wird durch die sogenannte „Intelligenz vor Ort" das aufgezeichnete Video soweit wie möglich innerhalb der Kamera selbst verarbeitet. Dies senkt die Auslastung des Netzwerks deutlich, da von den Kameras nur relevantes Video gestreamt wird. Das hat offensichtliche Vorteile im Szenario einer Leitstelle, in der ein Sicherheitsmitarbeiter Videomaterial nur untersuchen muss, wenn ein Alarm eingeht. Dies bedeutet eine wichtige Verbesserung sowohl für den Sicherheitsmitarbeiter als auch die Betriebseffizienz der Organisation.

Es gibt zwei Hauptkategorien für die Systemarchitektur zur Implementierung von Videoanalysefunktionen: zentralisiert und verteilt. Bei zentralen Netzwerkarchitekturen werden Videodaten und andere Informationen von Kameras und Sensoren erfasst und zur Analyse zu einem zentralen Server übertragen. In verteilten Netzwerkarchitekturen können die peripheren Geräte (Netzwerkkameras und Video-Encoder) selbst Videomaterial verarbeiten und relevante Informationen herausfiltern. Mit dezentralen Analysefunktionen entfällt der Bedarf an dedizierten Analyseservern, und da Komprimierung nur angewandt wird, wenn Videodaten zu einem zentralen Server übertragen werden, lassen sich Analysen jetzt am unkomprimierten Videomaterial durchführen. Daraus resultiert eine sehr viel günstigere und flexiblere Architektur. Heute können die gleichen Server, die typischerweise aufgrund der erforderlichen Verarbeitungsleistung nur wenige Videostreams verarbeiten konnten, mit Hunderten Videostreams umgehen, wenn ein großer Teil der Verarbeitung in den Kameras erfolgt.

4.4.1 Verarbeitungsgeschwindigkeiten und Grafikkarten

Auch wenn einige führende Tech-Firmen bezogen auf die genaue Vorhersage von Gordon E Moore (alias Mooresches Gesetz) zum exponentiellen Wachstum von Verarbeitungsgeschwindigkeiten und Kapazität in naher Zukunft eine Verlangsamung prognostiziert haben, bedeutet die derzeitige Leistungssteigerung in Kombination mit der Verkleinerung, dass Kamerahersteller und Entwickler die Art und Weise der Nutzung von Verarbeitungsleistung ändern können.

Bis vor kurzem wurde jede zusätzliche Verarbeitungsleistung zur Verbesserung der Bildqualität genutzt, indem die Auflösung erhöht und effizientere Videokomprimierung herbeigeführt wurde. Derzeit scheint der Markt allerdings im Hinblick auf die Nachfrage nach höherer Bildauflösung an seine Grenzen zu stoßen. Infolgedessen nutzen die Hersteller jetzt die Verarbeitungsleistung, um ein nie dagewesenes Maß an Intelligenz in der Edge bereitzustellen. In vielen Fällen bedeutet das, dass leistungsstarke, serverbasierte Videoanalysefunktionen jetzt von der Verarbeitung in der Kamera profitieren können.

Dank der modernen, kleineren und schnelleren Prozessoren können Kameras Grafikprozessoren (GPUs) aufnehmen, die parallele Verarbeitungsmöglichkeiten erschließen und neue Chancen und Analysemöglichkeiten eröffnen. Diese neue Fähigkeit hat dazu geführt, dass sich Softwareentwickler darauf konzentrieren, neuere Versionen vorhandener und bewährter serverbasierter Analysefunktionen in Edge-basierten Varianten anzubieten, was zu wachsender Nachfrage nach intelligenteren Kameras beiträgt, die weit über bloße Sicherheit und Videoüberwachung hinaus Wert beitragen können.

4.4.2 Deep Learning und Künstliche Intelligenz (KI)

Grafikprozessoren haben einen enormen Sprung in der Analyseleistung am Rand des Systems ermöglicht, aber die Nachfrage nach der Anwendung anderer Technologietypen wächst, die Merkmale wie Personenzählung und Auslastungsmanagement bieten. Weiterentwicklungen von KI und Maschinellem Lernen haben dazu geführt, dass Deep Learning Processing Units (DLPU) in Kameras integriert werden, was sich als bahnbrechend erweist.

Eine DLPU ist speziell auf die breitere Anwendung von Deep-Learning-Analysen ausgelegt. Analysefunktionen, die auf Deep Learning basieren, können größere Genauigkeit zur Erfassung und Klassifizierung bieten, denn der Algorithmus ist effektiv darauf trainiert, wie ein Satz vorgeschriebener Objekte aussieht. Das bedeutet, dass eine Lösung zur Eindringerfassung an einer Umgrenzung so eingerichtet werden kann, dass nur bei ganz speziellen Objekten und Szenarien Alarm ausgegeben wird; eine fortgeschrittene Version von If This Then That (IFTTT).

In einigen Fällen ist ein Objekt möglicherweise nur teilweise zu sehen, etwa der hintere Stoßfänger eines Fahrzeugs, aber die Systemanalytik erkennt und identifiziert es trotzdem. Zum Zeitpunkt der Abfassung und trotz einiger anderslautender Ansprüche sind die meisten bewährten Lösungen auf dem Markt darauf beschränkt, zwischen Personen und Fahrzeugtypen zu unterscheiden und sie zu identifizieren. Allerdings befinden sich Beispiele für kamerabasierte Analysemodelle, die detailliertere Unterscheidungen treffen können, beispielsweise die Farbe der Kleidung, die eine Person trägt, in einem fortgeschrittenen Teststadium.

Diese technologischen Fortschritte könnten potenziell zu äußerst gezielten Erfassungssystemen führen, die zwischen Mitarbeitern, Kunden, Mitgliedern der Öffentlichkeit oder potenziellen Bedrohungen unterscheiden und sie identifizieren können. Aus einer Sicherheitsperspektive können erweiterte Analysefunktionen in einem Umfeld mit gut umgesetzter physischer Sicherheit nur zu einem noch effizienteren und präziseren System zur Erfassung und Verhütung von Verbrechen führen. Die Weiterentwicklung zur nächsten Fähigkeitsstufe ist möglicherweise nicht allzu weit entfernt.

5 Kosten

5.1 Bewertung und Messung einer Kapitalrendite

Wie bei jeder Sicherheitsmaßnahme, sei es im Hinblick auf eine Schwachstelle oder auf Widerstandsfähigkeit, sollte die Bewertung einer Perimeterschutzlösung sowohl angemessen als auch verhältnismäßig sein. Wie immer muss die Bedrohung höchste Priorität haben. Sie kann sich heutzutage an fast jedem größeren Firmen- oder Behördenstandort als versehentlicher Übertritt darstellen, jedoch auch von Demonstranten bis hin zu Terroristen ausgehen.

Ein abgestimmtes Sicherheitskonzept, das Input und Überlegungen aus anderen Abteilungen wie beispielsweise IT und Operations einschließt, wird rasch Best Practice. Das schließt die Notwendigkeit ein, Personen einzubinden, die Erfahrung mit technischen Anforderungen haben, und sie sollten so früh wie möglich herangezogen werden. Bei den Überlegungen dazu, welche Maßnahmen ergriffen werden sollten, stellten in der Vergangenheit die eher traditionellen Maßnahmen, mit denen typischer Weise ein potenzieller Eindringlich abgeschreckt und aufgehalten wird, immer einen guten Ausgangspunkt für die Umgrenzung dar. Erst dann ging der Sicherheitsplaner zu ‚strategischen' technischen Erfassungssystemen über. Aber bei den vielen Maßnahmen und Systemen, die sich inzwischen integrieren lassen, ist ein durchdachteres und ganzheitliches Konzept erforderlich.

Es ist bekanntermaßen schwierig, die Kapitalrendite einer Sicherheitslösung aufzuzeigen, mit der ein Ereignis verhindert werden soll. Das liegt vor allem daran, dass es keine potenziellen Einnahmen gibt, die den Kosten gegenübergestellt werden könnten. In der Regel arbeitet das Sicherheitspersonal mit einen Kollegen in der Finanzabteilung zusammen, um die verschiedenen Kostenarten von Sicherheitsereignissen zu verdeutlichen. Dabei handelt es sich um direkte Kosten aufgrund des Verlusts oder der Vernichtung von Vermögen oder - weniger unmittelbare, aber ebenso schädliche - Kosten im Zusammenhang mit Reputationsverlust.

Allerdings ist es möglich, eine besser konkretisierbare Kapitalrendite aufzuzeigen, insbesondere bei bestimmten Technologien, die spezifische manuelle Tätigkeiten reduzieren oder zulassen können, dass Sicherheitsmitarbeiter für andere Aufgaben eingeteilt werden. Beispiele lassen sich in Lösungen finden, die nicht nur das Personal bei verdächtigem Verhalten oder Eindringversuchen warnen, sondern auch eine automatisierte ‚weiche' Reaktion produzieren können. Dazu könnten IP-Audiosysteme gehören, die vorher aufgezeichnete Durchsagen wiedergeben, oder Leuchthinweise, die potenzielle Eindringlinge darüber informieren, dass sie erfasst wurden, und sie anweisen, den Bereich zu verlassen.

Wenn die Lösung Überwachungskameras umfasst, lässt sich höhere Wirksamkeit erzielen, indem dem Eindringling ein Nachweis seiner Identifizierung wie beispielsweise ein Bildschirm gezeigt wird, auf dem zu sehen ist, dass sein Fahrzeugkennzeichen erfasst wurde, oder sogar ein Bild des Eindringlings. Nur wenn dies nicht zum erwünschten Ergebnis führt, muss das Sicherheitsteam für direktere Maßnahmen eingesetzt werden. Dieses abgestufte Konzept für die Reaktion auf Warnungen ist möglicherweise besser geeignet für die Anwendung außerhalb der Umgrenzung, aber trägt dazu bei, die Notwendigkeit der frühzeitigen Einbeziehung von Sicherheitspersonal zu minimieren und so Arbeitsstunden anderweitig nutzen zu können, was einem klaren Effizienzgewinn entspricht.

5.2 Kostenberechnung

Die Kostenschätzung sollte auf einer TCO-Berechnung (Gesamtinvestitionskosten) basieren. Die TCO-Berechnung umfasst alle Kosten in Verbindung mit einer Lösung über ihren gesamten Lebenszyklus: Material- und Arbeitskosten, Studienkosten, Systeminstallationskosten, Betriebskosten, Wartungskosten, Außerbetriebnahme- und Recyclingkosten. Dazu könnte ein anderes Konzept in den Finanz- und

Beschaffungsabteilungen erforderlich sein, denn unter Umständen muss Kapital zwischen den Betriebs- und Investitionskostenbudgets umgeschichtet werden.

Wie bei allen Sachanlagen muss die Organisation die Nutzungsdauer der Perimeterschutzlösung kennen. Sicherheits- und IT Manager können ihren Kollegen im Finanzwesen helfen, indem sie erklären und demonstrieren, wie die Beschaffung der richtigen Technologie als Plattform für künftige Lösungen zur Einsparungen führt. Eine Charakteristik ausgereifter, intelligenter Überwachungsgeräte ist die, dass sie in gewissem Umfang inhärent zukunftsfähig sind. Das heißt, Geräte mit geeigneter Verarbeitungsleistung können im Laufe der Zeit wiederholt technologische Fortschritte nutzen, insbesondere durch Verarbeitungsanalysen basierend auf KI und Maschinellem Lernen.

6 Angebot von Axis Communications

Der offene Ansatz von Axis bei der Integration in Partnerlösungen bedeutet, dass die vernetzten Sensoren in Kombination mit bewährter Videoanalyse und der Nutzung von KI es den Kunden ermöglichen, leistungsstarke, integrierte Perimeterschutzlösungen zu implementieren, die im gesamten Unternehmen und über die gesamte Lebensdauer des Systems hinweg cybersicher und kostengünstig sind.

Wo thermische Sensoren unter Umständen nicht geeignet sind, stellt Mikrowellentechnologie (Radar) eine großartige Alternative dar, denn sie kann viele der gleichen Vorteile bieten wie die Wärmebildtechnik, mit potenziell weniger Falschmeldungen. Auch die Radartechnologie von Axis profitiert von Maschinellem Lernen und Deep Learning wie moderne Überwachungskameras. Radargeräte von Axis können Personen und Fahrzeuge präzise und fast ohne Fehlalarme erfassen, klassifizieren und verfolgen.

Radartechnologie funktioniert rund um die Uhr und bleibt von üblichen Auslösern wie beispielsweise sich bewegenden Schatten oder Lichtstrahlen, kleinen Tieren oder Insekten sowie widrigen Wetterbedingungen buchstäblich unbeeinflusst. Das führt zu einem äußerst kosteneffizienten Betrieb und sorgt dafür, dass sich das Sicherheitspersonal auf echte, bestätigte Bedrohungen fokussieren kann. Radar kann darüber hinaus die Geschwindigkeit eines Objekts liefern, so dass eine genaue Berechnung entweder des Kontaktpunkts oder auch zur Durchsetzung von Geschwindigkeitsbegrenzungen erfolgen kann.

Die Performance einer Lösung ist oft der erste Teil einer Informationsanfrage (RFI) oder Fragebogens zur Marktanalyse. Axis Kameras verfügen über eigene Axis ARTPEC-Prozessoren mit der branchenweit besten Kapazität. Damit können einige der komplexesten Lösungen zur Videoanalyse für den Perimeterschutz in der Kamera (dezentral) eingebettet werden. Entscheidend ist, dass damit auch gewährleistet wird, dass die Lösung die Leistungsfähigkeit der internen Technologie und nicht die von Fremdkomponenten nutzt.

Diese ‚On the Edge'-Intelligenz bedeutet, dass mehrere Kameras mehrere Ereignisse verfolgen können, die gleichzeitig an verschiedenen Standorten eintreten. Dank dieser so genannten verteilten technischen Architektur kann die Lösung auf so viele Kameras wie erforderlich ausgeweitet werden, während Investitionen in zentralisierte Servertechnologie überflüssig werden.

Mit dem von der britischen Regierung zugelassenen AXIS Perimeter Defender (APD) werden vier verschiedene Ereignistypen für eine oder mehrere Personen oder Fahrzeuge erfasst:

- Eindringen in einen vordefinierten Bereich
- Überqueren von Zonen in einer vordefinierten Reihenfolge und Richtung
- Bedingtes Überqueren von Zonen
- Die Präsenz von Herumtreibern

APD kann mehr als nur einen Eindringalarm und das entsprechende Video liefern. Er liefert außerdem Metadaten, die zum Anzeigen eines Overlays im Video genutzt werden können, um die Grenzen und Bewegungsbahnen von Personen und Fahrzeugen in Bewegung zu zeigen. Für ein stärker integriertes Konzept können Axis Kameras (für sichtbares Licht oder Wärmebilder) auch mit IP-Lautsprechern arbeiten, um bei der Erfassung automatische Meldungen zu senden, potenziell als eigenständige Lösung. Dieser Typ automatisierter Warnung lässt eine ‚Eskalation' von Maßnahmen und Gegenmaßnahmen zu, was zur Bestimmung der Absicht eines Eindringlings und jeder anschließenden erforderlichen Reaktion wichtig ist.

APD lässt sich direkt in die üblicherweise auf Enterprise-Plattformen genutzte Software (z. B. Genetec, Milestone, Seetec, Prysm, Quognify und andere) integrieren.

Axis bietet ergänzende Design Tools zur Unterstützung bei der Planung nach der Bestandsaufnahme sowie Support in jeder Phase eines Projekts, von der Suche nach den richtigen Produkten auf der Grundlage spezifischer Kriterien bis hin zur Berechnung des Speicherbedarfs, der Installation der Technologie und der Verwaltung der Systeme. Der Einsatz von Axis Tools hilft Consultants bei der Planung und Kostenschätzung und einem Integrator beim reibungsloseren und effizienteren Projektmanagement. Diese Tools gewährleisten auch leichter die Sicherheit des installierten Systems, denn mit der zugehörigen Software lassen sich Upgrades und Sicherheits-Patches ohne Weiteres installieren.

Mit der Weiterentwicklung von Bedrohungen und Gegenmaßnahmen bleibt ein kritischer Punkt konstant: die Integrität und Sicherheit der Umgrenzung. Die Umgrenzung ist ein grundlegender Aspekt für diejenigen, die die Verpflichtung einer Organisation wahrnehmen, Mitarbeitern, Besuchern und Öffentlichkeit eine sichere und geschützte Umgebung zu bieten. Dieses Papier soll bei Organisationen für die Vorteile eines integrierten Technologiekonzepts zur Planung der Perimetersicherheit werben. Außerdem wird hervorgehoben, dass Investition in Sicherheitstechnologie auf einer nachweisbaren Kapitalrendite beruhen sollte. In jedem Fall stellt das Verständnis derzeit relevanter technologischer Fähigkeiten in Verbindung mit einem Gespür für künftige Trends ein solides Betriebssicherungs- und Beschaffungskonzept für jeden Sicherheitspraktiker unabhängig von Abteilung, Titel oder Branche dar.

Produktreferenzen

IP-Wärmebildkameras:

AXIS Q19 und mehr www.axis.com/en-gb/products/thermal-cameras

Analysesoftware:

AXIS Perimeter Defender

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

Externe IP-Lautsprecher:

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

IP-Sicherheitsradar:

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

T10169467/DE/M1.3/2107

Über Axis Communications

Axis ermöglicht eine smarte und sichere Welt durch die Entwicklung von Netzwerk-Lösungen. Diese bieten Erkenntnisse, um die Sicherheit und Geschäftsmethoden zu verbessern. Als Technologieführer im Bereich Netzwerk-Video bietet Axis Produkte und Dienstleistungen für die Videoüberwachung/-analyse und Zutrittskontrolle sowie Sprechanlagen und Audiosysteme. Das 1984 gegründete schwedische Unternehmen beschäftigt mehr als 3.800 engagierte Mitarbeiter in über 50 Ländern. Gemeinsam mit seinen Partnern auf der ganzen Welt bietet das Unternehmen kundenspezifische Lösungen an.

Weitere Informationen zu Axis bietet Ihnen unsere Webseite *axis.com*.