White Paper

5 Technologien für mehr Sicherheit von Rechenzentren

März 2019

AXIS COMMUNICATIONS

Inhalt

1. Einführung

Von Online-Handel über mobiles Banking bis zu Cloud-Anwendungen für Unternehmensproduktivität und digitalem Infrastrukturmanagement gibt es mittlerweile eine Fülle von Daten, die in Rechenzentren ausgelagert und dort verwaltet werden. Die hinterlegten Datensätze haben einen enormen Wert für die Unternehmen und sind damit in den Fokus von Kriminellen gerückt. Ihr Ziel: durch den illegalen Zugriff und dem Verkauf der Informationen den eigenen Profit steigern oder gezielt, im Auftrag Dritter, die Geschäftsprozesse von Unternehmen stören. Darum ist es für die Betreiber von Rechenzentren extrem wichtig, dafür zu sorgen, dass ihre Infrastruktur auf einem hohen Niveau geschützt wird.

Zum Schutz solch einer kritischen Infrastruktur ist die Implementierung eines hocheffizienten Überwachungssystems unabdingbar - ein Bereich, in dem Axis weltweit führend ist.

Die stete Weiterentwicklung der Technik hilft hier. Auf Basis der IP-Infrastruktur lässt sich die Videoüberwachung, die Zutrittskontrolle, Audio-Systeme und die Videoanalytik effizient zu einem System bündeln, um so den Schutz eines Rechenzentrums zu erweitern und erhöhen.

Dieses Whitepaper stellt die wichtigsten Herausforderungen dar, mit denen Rechenzentren konfrontiert sind und zeigt effiziente Lösungen zur Erweiterung bestehender oder zum Aufbau neuer Schutzmaßnahmen.

2. Perimeter- und interner Schutz

Der Standort eines Rechenzentrums wird sorgfältig ausgewählt, um Risiken - die von klimatischen Widrigkeiten wie Tsunamis und Erdbeben bis zu Überfällen reichen - zu reduzieren. Einige der Zentren befinden sich an isolierten, schwer erreichbaren Orten, so dass schon die Annäherung eines Fremden auf ein potenzielles Risiko hindeuten kann.

Heutzutage ist es möglich, sich an abgelegenen Standorten ohne Wachpatrouillen per Smartphone vor Eindringlingen warnen zu lassen, wenn sich jemand den Außengrenzen eines Rechenzentrums nähert. Der Mitarbeiter in der Kontrollstelle wird automatisch informiert und kann Tag und Nacht direkt auf eine Aufzeichnung der verdächtigen Vorgänge zugreifen. Sobald eine Bedrohung (bspw. wenn jemand versucht, die Mauern zu überwinden) erkannt wird, kann moderne Technologie dank leistungsfähiger Alarmierungssysteme mit einer akustische Warnung über IP-Hornlautsprecher reagieren.

Potenzielle Angreifer lassen sich immer neue Strategien einfallen, und so kann eine Perimeterverletzung auch oberhalb des Zauns stattfinden, nämlich mit Drohnen. Genau wie das Internet Hackern neue Möglichkeiten eröffnet hat, einer Organisation zu schaden, sind nun mit Hilfe von Drohnen Aktivitäten wie Wirtschaftsspionage, Terrorismus und unbefugtes Eindringen möglich. Drohnen stellen somit inzwischen eine schwerwiegende Sicherheitsbedrohung für Rechenzentren dar. Diese Anlagen sind nun dem Risiko ausgesetzt, dass ihr Betrieb unterbrochen wird oder physischen Schaden nimmt. Einen Schutz vor solchen Angriffen auf Rechenzentren bietet der Einsatz von Luftabwehr-Technologie: die Einrichtung eines Frühwarnsystems durch die Kombination von Kameras mit spezieller Software zur Drohnenerfassung. Die kombinierte Lösung kann Drohnen erfassen und den gefährdeten Luftraum vor Bedrohungen schützen, selbst wenn das Fluggerät autark über GPS-Koordinaten geführt wird.

Zusätzlich wird empfohlen, den physischen Zutritt zum Rechenzentrum dahingehend zu überwachen, dass genau festgehalten wird, welche Personen die Räume betreten, wobei auch die Zeiten dafür aufzuzeichnen sind. Des Weiteren ist es nützlich, zu verfolgen, wie viel Zeit dort verbracht wird und welche Bereiche betreten werden. Viele Technologien sind auf diese Art von Kontrolle ausgerichtet. Einige Rechenzentren setzen nicht nur passwort- oder kartenbasierte Systeme ein, die immer mit dem Risiko verbunden sind, kopiert zu werden, sondern auch eine Art physischer Überprüfung wie beispielsweise Gesichtserkennung. Dies lässt sich beispielsweise beim Einsatz von Videosprechanlagen (für Außenbereiche vorzugsweise in vandalismusgeschützter Ausführung) mit einer Gesichtserkennungssoftware kombinieren. Wenn das Gesicht den aufgezeichneten Erkennungsdaten entspricht und der Zeitpunkt im autorisierten Zeitrahmen liegt, erfolgt die Türöffnung über Netzwerk-Zutrittscontroller.

Zusätzlich lässt sich das Zutrittskontrollsystem über die Hauptbereiche hinaus erweitern. Es kann auch kleinere Räume und sogar Rack-Türen miteinbeziehen. Bestimmte intelligente Module können E/A-Geräte verbinden, um Warnungen zu generieren, beispielsweise wenn die Rack-Tür offen gelassen wurde. Gleichzeitig können unauffällige Kameras helfen, unbefugtes Betreten oder Öffnen von Türen zu unüblichen Zeiten zu erkennen.

3. Prozessanalyse und Einhaltung der Protokolle.

Der Zutritt zum Rechenzentrum stellt weitere Herausforderungen dar. Schließlich haben wir es mit einer physikalischen Umgebung zu tun, die die Einhaltung von Sicherheitsabläufen voraussetzt. Nur so lässt sich ein effektiver Schutz gewährleisten. In solchen Umgebungen ist z. B. die Nutzung von Smartphones mit Kameras generell untersagt. Auch beschränken viele Rechenzentren die Anzahl der Personen, die gleichzeitig Zutritt haben dürfen.

Ein intelligentes Videoüberwachungssystem kann die genaue Anzahl der Personen erfassen, die sich gegenwärtig im überwachten Bereich aufhalten, und sofort eine Warnung ausgeben, wenn der zulässige Wert überschritten wird.

Über die Anzahl der Personen hinaus meldet diese Analysefunktion, die in die Kamera eingebettet ist, auch die durchschnittliche Aufenthaltsdauer. Wenn ein externer Spezialist beispielsweise in der Regel 30 Minuten zur Wahrnehmung einer bestimmten Aufgabe benötigt, kann das System so programmiert werden, dass es eine Benachrichtigung schickt, wenn jemand diese Zeitspanne überschreitet.
Diese Funktion kann in Rechenzentren nützlich sein, denn dort gibt es typischerweise Zeiträume, in denen sich niemand in den Räumlichkeiten aufhalten darf.

Diese und andere Ereignisse, beispielsweise ein am Boden zurückgelassenes Objekt, können Warntöne über IP-Lautsprecher auslösen. Diese Meldungen sind nützlich, um mutwillige Personen von ihrer Absicht abzuhalten und die Mitarbeiter vor Achtlosigkeit zu warnen. Eine Studie der CompTIA[1] (Computation Technology Industry Association) hat gezeigt, dass 42% der überprüften Sicherheitsvorfälle entweder auf mangelnde Aufmerksamkeit des Endbenutzers oder auf das Nichteinhalten von Sicherheitsabläufen zurückzuführen sind.

[1] Studie "Trends In Information Security":
www.comptia.org/resources/trends-in-information-security-study

Es können sogar wiederkehrende Warnungen programmiert werden, die den Zuständigen als Erinnerung an die Wahrnehmung einer Aufgabe dienen. All das sind effektive Sicherheitsmaßnahmen zur zuverlässigen Einhaltung von Sicherheitsabläufen und zur Reduzierung von Risiken in einer kritischen Umgebung.

4. Effizientes Datenmanagement vom Videoüberwachungssystem

In den letzten Jahren haben Rechenzentren (insbesondere die Großen) in die Optimierung des Energieverbrauchs investiert. Dies ließ sich dadurch erreichen, dass intelligente Strategien zur Kühlung zusammen mit effizienter Software zum Energiemanagement eingesetzt wurden. Auch konnte die Anzahl der Server zur Verarbeitung der entsprechenden Datenmengen reduziert werden. Dieselbe Logik lässt sich auch auf Videoüberwachungsgeräte übertragen.

Alle mit einem Netzwerk verbundenen Geräte erzeugen Informationen, die verarbeitet werden müssen. Dazu muss ein effizientes Rechenzentrum zwei Faktoren berücksichtigen: die Informationsmenge, die es von den Kameras bis zu den Servern bewältigt, und den erforderlichen Speicher für Ihre Aufbewahrung über einen bestimmten Zeitraum.

Ein effizientes Datenmanagement ist daher von entscheidender Bedeutung. Der Standard H.264 (das am häufigsten verwendete Format zur Aufzeichnung, Komprimierung und Verteilung von Videoinhalten) bietet eine starke Bildkomprimierung, die durch Technologien wie Axis Zipstream noch gesteigert werden kann. Damit stehen verschiedene Methoden zur Reduzierung der Video-Bitrate ohne erkennbare Qualitätseinbußen zur Verfügung. Durch sinnvollen Einsatz ist bis zur Hälfte weniger Bandbreite erforderlich - eine deutliche Reduzierung gegenüber Systemen, die auf H.264 beschränkt sind.

Infolgedessen wird auch die gespeicherte Informationsmenge halbiert. Mit dem Standard H.264 reicht eine Speicherkapazität von 2 TB für Videoaufzeichnungen mit 20 Bildern pro Sekunde in hoher Auflösung (1280 x 1024) gerade mal 28 Tage[2]. Durch den Zusatz von Zipstream kann diese Speicherung ohne Verluste auf 56 Tage verlängert werden - oder man kann den Investitionsaufwand durch den Einsatz eines preisgünstigeren 1 TB-Speichers verkleinern, um auf dieselben 28 Tage zu kommen.

Über diese Komprimierung hinaus gibt es weitere Möglichkeiten, den Datenstrom von Videoüberwachungssystemen zu reduzieren. Eine besteht darin, das Bildformat so anzupassen, dass es dem beobachteten Bereich entspricht. Bei der Betrachtung eines Korridors wäre es beispielsweise sinnvoller, eine vertikale Kameraausrichtung zu wählen, statt ein Bild im Querformat zu generieren. Die einfache und einzigartige Lösung für dieses Problem ist das Corridor Format von Axis.

Eine vertikale Aufnahme bietet mehr Detailschärfe am Ende des Korridors. So kann eine einzige Kamera 50 Meter abdecken. Durch eine reduzierte Anzahl von Kameras kann das Rechenzentrum auch die Menge gespeicherten Videomaterials auf die Hälfte reduzieren. In Kombination mit Komprimierungstechnologie lässt sich die Datenmenge um durchschnittlich 75% reduzieren.

[2] Videoüberwachungsspeicher: wie viel ist genug?
www.seagate.com/files/staticfiles/docs/pdf/whitepaper/video-surv-storage-tp571-3-1202-us.pdf

Ein weiteres bekanntes Konzept ist Edge Storage. Die an der Tür eines Racks oder in der Decke des Rechenzentrums installierte Kamera kann eine für die Videoüberwachung optimierte Speicherkarte (z. B. 128 GB) enthalten. Mit Bewegungserkennung als Auslöser können ohne Weiteres 51 Tage im Rechenzentrum verstreichen, bevor Informationen auf der Speicherkarte überschrieben werden. Der Videostrom wird nicht über das Netzwerk übertragen. Bei Rechenzentren mit höheren Sicherheitsanforderungen lässt sich dasselbe Konzept auch zu Redundanzzwecken verwenden, was bedeutet, dass das Videomaterial zweifach gespeichert wird: in der Kamera und zusätzlich im Zentralspeicher.

5. Gesundheitsüberwachung und Cybersicherheit

Wenn die Grenzen und der Luftraum von Rechenzentren geschützt sind, die Zutrittskontrolle intelligent funktioniert und Informationsmenge und -speicher minimal sind, müsste alles unter Kontrolle sein, richtig? Keinesfalls.

2015 verwies CompTIA in einem Bericht mit dem Titel "Trends in Information Security" darauf, dass 85% aller geglückten Dateneinbrüche die zehn bekanntesten Schwachstellen ausnutzten. Obwohl die erforderliche Software zur Verfügung stand, sind diese Schwachstellen nie behoben worden.

Und noch schlimmer: 83% der Ziele von Datenschutzverletzungen brauchten über eine Woche, um den Zugriff überhaupt erst festzustellen. Die Folgen lassen sich in Dollar berechnen. Man geht davon aus, dass der in den Jahren 2013 bis 2014 unternommene Angriff auf fast 3 Milliarden Yahoo-Benutzerkonten den Verkaufswert des Unternehmens um 350 Millionen Dollar verringerte.

Deshalb ist es von grundsätzlicher Bedeutung, die Systemgesundheit in einem Rechenzentrum zu überwachen. Unternehmen und Regierungsorganisationen, die ihre eigenen Rechenzentren verwalten, können ihre Installationen besser kontrollieren, wenn sie Gerätemanagementsoftware einsetzen, die den Zustand aller mit dem Netzwerk verbundenen Geräte fortlaufend analysiert: Kameras, Zutrittskontrolle, Audioausstattung usw.. Firmware-Updates erfolgen automatisch.

Unternehmen mit einem hohen Sicherheitsstandard setzen beispielsweise voraus, dass die mit dem Hausnetzwerk verbundenen Geräte mit kundenspezifischen Sicherheitszertifikaten ausgestattet werden. Um einem solchen Bedarfsniveau gerecht zu werden, kann bedarfsgerechte Firmware für ein bestimmtes Projekt angefordert werden.

6. Einheitliche Verwaltung

Es ist unverkennbar, dass diese Technologien in die gleiche Richtung weisen. Die modernsten Rechenzentren weltweit profitieren bereits von den neuen Integrationsmöglichkeiten verschiedener Geräte, die mit einem Netzwerk verbunden sind. Es wird zunehmend deutlich, dass ein zentralisiertes Systemmanagement extrem effizient ist.

Nehmen wir beispielsweise die Einfahrt von Fahrzeugen zu einem Rechenzentrum: ein Fahrzeug nähert sich dem Erfassungsbereich der Kamera, die in der Einfahrt platziert ist. Dann erfasst die eingebettete Software das Kennzeichen. Die Kamera schickt dieses an einen Access Controller, der überprüft, ob das Fahrzeug einfahren darf. Für ein höheres Maß an Sicherheit kann eine Videosprechanlage, die in Fahrerhöhe installiert ist, einen QR-Code anfordern, der vorher per Smartphone empfangen wurde. Zum Abschluss des Vorgangs öffnet sich das Tor oder die Schranke. Die gesamte Ereignisabfolge wird aufgezeichnet und gespeichert. Auch hier wirken Sicherheit und Zutrittskontrolle zusammen.

In einer reinen IP-Umgebung, in der sogar Audiogeräte das SIP-Protokoll anwenden, um mit IP-Telefonen zu kommunizieren, kann ein Rechenzentrum schnell Informationen teilen und effizient vorgehen.

Diese Vorteile sind in der Regel größer für diejenigen, die in offene Hard- und Softwaretechnologien investieren, denn diese lassen sich problemlos mit anderen Technologien kombinieren. Deshalb befürworten Organisationen wie ONVIF, die sich für Interoperabilität einsetzen, weiterhin innovative Lösungen. Sie werden insbesondere benötigt, um verschiedene Herausforderungen in Rechenzentren zu bewältigen, in denen physischer und virtueller Schutz und Zutrittskontrollsicherheit naturgemäß zusammenhängen.

73006/DE/R1/1903

Über Axis Communications

Axis ermöglicht eine smarte und sichere Welt durch die Entwicklung von Netzwerklösungen. Diese bieten Erkenntnisse, um die Sicherheit und Geschäftsmethoden zu verbessern. Als Marktführer im Bereich Netzwerk-Video bietet Axis Produkte und Dienstleistungen für Videoüberwachung und -analyse sowie Zutrittskontrolle und Audiosysteme. Axis beschäftigt mehr als 3.000 engagierte Mitarbeiter in über 50 Ländern. Gemeinsam mit seinen Partnern auf der ganzen Welt bietet das Unternehmen kundenspezifische Lösungen an. Axis wurde 1984 gegründet, die Unternehmenszentrale befindet sich in Lund, Schweden.

Weitere Informationen über Axis finden Sie unter www.axis.com

AXIS COMMUNICATIONS