



IT-Überlegungen zur Gestaltung eines IP-Videosystems

Neun wichtige IT-Überlegungen zur Gestaltung eines IP-Videosystems

Inhaltsverzeichnis

Einführung.....	3
1. Die Bedeutung von IT-Fachwissen bei Videosystemen	4
2. Die richtige Ausrüstung für die jeweiligen Anforderungen an die Videoüberwachung.....	5
3. Die entscheidende Rolle des Netzwerks	6
4. Der Wert ist wichtiger als der Preis	7
5. Cyberbedrohungen und Abhilfemaßnahmen	7
6. Grenzen eines Air-Gap-Ansatzes	8
7. Keine Videodaten mehr verlieren	9
8. Verwaltung von Lebenszyklen in IP-Überwachungssystemen	10
9. Das IT-Ökosystem in Videosystemen	10

Dieses Dokument wurde von SourceSecurity.com im Auftrag von Alcatel-Lucent Enterprise erstellt.



Einführung

Ein Videoüberwachungssystem stellt besondere Anforderungen an die Informationstechnologie (IT). Ein digitales Videosystem nutzt zwar die gleichen Technologien wie andere IT-Systeme, ist aber anders aufgebaut und auf die speziellen Anforderungen der Videoüberwachung ausgerichtet.

Videosysteme sind eine anspruchsvollere Umgebung und belasten alle Bereiche eines IT-Systems stärker. Bei Belastung und insbesondere bei größeren Unternehmenssystemen kann es zu Problemen kommen. Die Wahl der richtigen Ausrüstung für die jeweilige Aufgabe gewährleistet auf lange Sicht eine höhere Zuverlässigkeit.

Alcatel-Lucent Enterprise hat – in Zusammenarbeit mit den Branchenexperten SourceSecurity.com und Stone Security – neun IT-Überlegungen ermittelt, die bei der Gestaltung eines IP-Videosystems eine zentrale Rolle spielen. In diesem White Paper untersuchen wir, wie sich die speziellen Anforderungen eines Videoüberwachungssystems darauf auswirken, welche IT-Technologien eingesetzt werden und wie sie genutzt werden.



1. Die Bedeutung von IT-Fachwissen bei Videosystemen

Die Entwicklung und Einrichtung eines Videoüberwachungssystems auf der Grundlage des Internetprotokolls (IP) erfordert ein hohes Maß an IT-Fachwissen in der Integratorgemeinschaft.

Einige Integratoren verfügen über die nötigen Fähigkeiten, um ein IP-Videosystem fachgerecht einzuführen, während andere damit Schwierigkeiten haben.

Die zusätzlichen Schulungen und Zertifizierungen, die den meisten in der IT-Welt vertraut sind, können Integratoren in die Lage versetzen, das erforderliche hohe Serviceniveau zu bieten. Zunächst einmal müssen die Installateure über die richtige Eignung und ein grundlegendes Verständnis von Netzwerken sowie die Fähigkeiten zur Fehlersuche verfügen.

Integratoren brauchen zunächst eine sachkundige Belegschaft. Dazu sollten sie die Auswahl an Technologien begrenzen und sicherstellen, dass jeder Mitarbeiter in der geringeren Anzahl von Technologien gut ausgebildet ist. Durch die Auswahl der besten Lösungen und die Gewährleistung, dass die Mitarbeiter mit diesen Produkten vertraut sind, kann ein Integrator seinen Kunden eine hochwertige Gesamtlösung anbieten.

Die Begrenzung des Produktmixes ermöglicht es einem Integrator auch, die Bandbreite der von einem bestimmten Produkt gebotenen Funktionen besser zu verstehen. Allzu oft kauft ein Kunde ein System, das eine Vielzahl von Funktionen bietet, und nutzt dann nur eine begrenzte Anzahl dieser Funktionen im täglichen Betrieb, wodurch der Wert des Systems, für das er bezahlt hat, untergraben wird.

Integratoren können ihren Kunden helfen, indem sie sie so schulen, dass sie den vollen Nutzen aus jedem System, das sie kaufen, ziehen können.

Integratoren können sich auch auf die Vorab-Beratungsdienste von Geräteherstellern verlassen, um sich informieren zu informieren. In einigen Fällen verfügen die Hersteller von Ausrüstungen über spezifische Kenntnisse über verschiedene vertikale Märkte, die sie im Laufe ihrer Tätigkeit auf diesen Märkten erworben haben.

Hersteller, die es mit einem bestimmten vertikalen Markt ernst meinen, beschäftigen Branchenexperten, um eine auf die Bedürfnisse des jeweiligen Kunden zugeschnittene Unterstützung zu gewährleisten. Ihre Beratung kann Integratoren dabei helfen, auf neuen Märkten erfolgreich zu sein und/oder bewährte Verfahren für die Märkte, auf denen sie tätig sind, zu optimieren.

Die Hersteller bieten auch Schulungen und Zertifizierungen an, um sicherzustellen, dass die Integratoren für die Installation ihrer Systeme gut gerüstet sind. Eine effiziente und inhaltliche Ausbildung sollte in kürzeren Sitzungen erfolgen, die den Wert der Zeit jedes Teilnehmers respektieren.

2. Die richtige Ausrüstung für die jeweiligen Anforderungen an die Videoüberwachung

Fragen wie die Bandbreite und die Anforderungen an Power over Ethernet (PoE) sind wichtige Variablen in einem Videosystem. Und der Videosever ist stärker belastet, vor allem wenn es sich um Videos von einer Live-Übertragung handelt. Alle Daten landen auf dem Server, auch Daten, die nicht aufgezeichnet werden.

Die Videoaufzeichnung wird gestoppt, so dass zumindest einige Sekunden der Videoaufzeichnung vor der eigentlichen Alarmauslösung gespeichert werden können. Längere Pufferphasen können erforderlich sein, um ein Bild zu erkennen, das sich aus größerer Entfernung nähert. Alle Ein- und Ausgaben laufen über den Server, auch wenn nur eine begrenzte Menge an Daten in den Langzeitspeicher geschrieben wird.

Es besteht ein grundlegender Unterschied zwischen der Sichtweise von Sicherheitssystemintegratoren und der von IT-Fachleuten auf die Systemgröße. Systemintegratoren sprechen eher von der Anzahl der Kameras, während IT-Fachleute eher von der Verwaltung der Daten des Systems sprechen. Die beiden sind natürlich untrennbar miteinander verbunden, aber die Beziehung ist nicht linear. Im Allgemeinen bedeutet eine höhere Anzahl von Kameras, dass mehr Daten von der IT-Abteilung verwaltet werden müssen. Es gibt jedoch noch weitere Faktoren, die sich auf den Datenbedarf auswirken, z. B. die Anzahl der Bilder, die Anforderungen an die Bildqualität, der Speicherbedarf, Tag-/Nachtanwendungen und die Verwendung von Videoanalysen.

Eine wichtige Fähigkeit bei der Spezifikation eines IP-Sicherheitssystems besteht darin, die Anforderungen an die Ausrüstung und die Funktionalität des Systems in die Daten zu übersetzen, die zur Erfüllung dieser Anforderungen erforderlich sind. Für ein Vor-Ort-System bedeutet dies, dass ein Computerserver spezifiziert werden muss, der die Systemleistung maximiert und gleichzeitig die Kosten senkt. Themen wie Virtualisierung und Cloud-Systeme können die Gleichung komplizierter machen und gleichzeitig neue Flexibilität bieten.

Eine weitere Variable im Zusammenhang mit dem Systemdesign ist die Verwendung von Edge-Kameras zur Aufzeichnung von Videos mit SD-Karten. Es gibt heute sogar Systeme, die "serverlos" sind. Dort findet zum Beispiel die gesamte Aufzeichnung am Netzzugang statt. Ein solcher Ansatz verlagert die Rechenlast vom Server auf den Serrerrand, wodurch der Bedarf an Serverkapazität sinkt. Heutige Kameras liefern Daten, die über den Videostrom hinausgehen, z. B. Metadaten und Audio, was sich ebenfalls auf das Systemdesign auswirkt.

IT-Fachleute sollten sich einen genauen Überblick über das Gesamtsystem verschaffen, z. B. über die angeschlossenen Geräte, die Bildfrequenz, die Auflösung und die Videocodecs der Kameras. Anhand dieser Informationen können sie die Anforderungen in Bezug auf Netzwerk, Strom, Server, Festplattenkapazität, Arbeitsspeicher und Speicherplatz berechnen und entscheiden, ob Cloud- oder On-Premises-Systeme verwendet werden sollen. Dies gewährleistet einen gründlichen und durchdachten Ansatz bei Entwurf und Einführung.

Die Hersteller bieten Software-"Rechner" an, die den Integratoren bei der Entwicklung von Systemen helfen, indem sie die Systemanforderungen in spezifische Ausrüstungsspezifikationen umsetzen. Denken Sie daran, dass die Berechnungen die Erwartungen erfüllen oder übertreffen und ein künftiges Wachstum ermöglichen sollten.

Die Implementierung von Cloud-Systemen ist eine weitere Variable, wenn es um die Gestaltung von Videoüberwachungssystemen geht. Der Trend geht eindeutig zum Einsatz von mehr Cloud-Systemen für die Videoüberwachung. Die Entscheidung zwischen Cloud- und On-Premises-Lösungen sollte jedoch von Fall zu Fall getroffen werden. Systementwickler und Endnutzer sollten sich gegen die scheinbare Unvermeidbarkeit der Cloud wehren und ihre Entscheidungen lieber auf der Grundlage der Bedürfnisse des Kunden treffen.

Viele Hersteller stehen unter dem Druck, ihre Systeme in die Cloud zu verlagern, sollten ihren Kunden aber idealerweise eine Auswahl an Systemen und keine Einheitslösung anbieten.

Die Hersteller sind in einer guten Position, um ihre Kunden zu beraten, ob eine Cloud-Konfiguration oder ein On-Premises-Design wünschenswert ist. Die Integratoren sollten auch die Vorteile beider Ansätze kennen und Kunden die Entscheidung für einen der beiden Ansätze erleichtern. Der Markt sollte Anwendungen nicht in die Cloud verlagern, wenn dies nicht für den jeweiligen Kunden optimal ist.

3. Die entscheidende Rolle des Netzwerks

Ein Videosystem ist nur so stark wie sein schwächstes Glied. Die Netzwerkswitches sind vielleicht nicht so sichtbar wie die Kameras und VMS, aber sie sind nicht weniger wichtig.

Es kommt jedoch häufig vor, dass die Kunden den Betrieb eines Netzes als selbstverständlich ansehen und wenig darauf achten, wie es funktioniert oder wie man seinen Nutzen maximieren kann. Manche Kunden möchten sogar ein Videosystem installieren, das eine bestehende Netzwerkinfrastruktur nutzt. Dies ist möglich, aber die Möglichkeiten zur Optimierung der Netzwerkkomponente eines Videosystems können begrenzt sein.

Im Idealfall entscheidet sich der Kunde für die besten Switches für die Videoüberwachung, die einen zuverlässigen und effektiven Betrieb des Systems gewährleisten.

Da jedes Videosystem anders ist, wird seinen individuellen Anforderungen besondere Aufmerksamkeit gewidmet, damit es seine einzigartige Aufgabe erfüllen kann. Bei der Inbetriebnahme eines Systems sollte das Netzwerk nicht als nachgelagert betrachtet werden. Vielmehr sollte es sorgfältig aus den besten Komponenten zusammengestellt werden, um den Betrieb systemweit zu ermöglichen und zu verbessern.

Switches, die mit Wire Speed arbeiten, d. h. über genügend Rechenleistung verfügen, um die volle Ethernet-Geschwindigkeit bei minimalen Paketgrößen zu bewältigen, sind heute Standard in der Branche. Ein neues Unterscheidungsmerkmal zwischen Switches ist die Fähigkeit, den Verkehr zu verstehen und zu verwalten.

Unmanaged Switches sind zwar auf dem Markt erhältlich, werden aber in der Regel nicht für kommerzielle und/oder Unternehmensanwendungen verwendet. Sie sind für den Einsatz in kleinen Netzen mit grundlegenden Anforderungen konzipiert. Es sind keine Einstellungen zu konfigurieren.

Umgekehrt ermöglichen Managed Switches die Erkennung und Diagnose von Leistungsproblemen und gewährleisten eine zuverlässige Leistung von Videoüberwachungssystemen. Sie ermöglichen es den Nutzern, detailliert zu sehen, was im System Probleme verursachen könnte, und vermitteln ein Verständnis dafür, wie diese Informationen aussehen.

Der Wert von Managed Switches, die vollständig konfigurierbar und anpassbar sind und eine Reihe von Leistungsdaten liefern, wird im Laufe der Lebensdauer des Systems deutlich, da sie wichtige Einblicke in den Systembetrieb liefern und eine einfachere Fehlerbehebung zur Identifizierung von Problemen ermöglichen.

Die Switches sollten so konzipiert sein, dass sie den Anforderungen von IP-Videosystemen gerecht werden. Ein Beispiel: Für einen Switch mit 16 Ports ist ein ausreichendes Energiebudget für den Betrieb aller an den Switch angeschlossenen Videokameras nötig. Die heutigen PoE-Kameras verbrauchen mehr Strom als frühere Generationen. Integratoren müssen wissen, dass ein Switch ausreichend Leistung für die Anzahl der Kameras und künftiges Wachstum bietet.

„Bei der Auswahl unserer Hardware wollen wir, dass jeder Switch über die nötige Bandbreite und das nötige Energiebudget verfügt und ein Managed Switch ist, der uns bei der Fehlersuche viel Zeit spart. Das spart uns und unseren Kunden Geld. Es ist eine höhere Anfangsinvestition, die sich aber auf lange Sicht durch die Schaffung eines besser funktionierenden Systems auszahlt.“

Aaron H. Simpson, President und CTO, Stone Security

4. Der Wert ist wichtiger als der Preis

Zuverlässigkeit ist bei der Videoüberwachung von entscheidender Bedeutung und beginnt bereits bei der Auswahl der Geräte.

Die Verwendung von Komponenten minderer Qualität mag zu diesem Zeitpunkt wie eine wirtschaftliche Notwendigkeit erscheinen. Langfristig wird darunter allerdings der Betrieb des Systems leiden. Die Kosten, die durch die Wahl eines nicht optimalen Betriebs entstehen, sind bei der Entwicklung eines Systems vielleicht noch nicht offensichtlich, werden aber im Laufe der Zeit deutlich.

Die Wahl besserer Geräte zahlt sich aus – auch wenn sie teurer sind.

Es ist von entscheidender Bedeutung, die Kosten (z. B. den Preis einer besseren Ausrüstung) gegen die Risiken eines unzureichenden Systems oder eines Ausfalls abzuwägen. Die beste Strategie für die Bewertung von Kosten und Risiken ist die Betrachtung der Gesamtbetriebskosten (TCO). Ein weiteres langfristiges Kostenelement, das es zu berücksichtigen gilt, ist der Wert offener Systeme, die Flexibilität bei der Erweiterung oder Änderung eines Systems in der Zukunft gewährleisten können.

Es ist immer am besten, mit einem Lieferanten zusammenzuarbeiten, der ein Produkt anbietet, dem er vertraut und das er über einen langen Zeitraum hinweg unterstützen kann.

5. Cyberbedrohungen und Abhilfemaßnahmen

Eine Ironie der bisherigen Historie in der physischen Sicherheitsbranche war die mangelnde Aufmerksamkeit für die Cybersicherheit von IP-Systeme.

Glücklicherweise schenken die Akteure inzwischen nicht nur der physischen Sicherheit, sondern auch der Cybersicherheit auf allen Ebenen und in der gesamten Lieferkette der physischen Sicherheit mehr Aufmerksamkeit. In der Tat ist die Cybersicherheit zu einer der wichtigsten Säulen im Entscheidungsprozess für größere Videosicherheitssysteme geworden.

Ein Mindestschritt zum Schutz vor Cyberbedrohungen und zur Einschränkung des Zugangs zu einem System ist die Vermeidung der Verwendung von Standardpasswörtern. Diese sind weniger sicher und können von einem Hacker oder Bot leichter erraten werden. In Kalifornien sind Standard-Passwörter sogar verboten worden.

Cybersicherheitsrisiken beginnen in der Lieferkette, wo Angriffe ein Produkt gefährden können, bevor es überhaupt ausgeliefert wird. Die Analyse eines Produkts auf mögliche "Backdoor"- oder "Buffer overflow"-Angriffe vor der Auslieferung kann die Bedrohung entschärfen. Die Kunden können sich auch dafür entscheiden, nach der Auslieferung von Hardware-Produkten virtuell „guten Code“ zu installieren, um so die Cybersicherheit zu gewährleisten und jeglichen böartigen Code zu überschreiben, der während des Versands installiert worden sein könnte.

Es gibt auch eine Reihe von Maßnahmen zur Cybersicherheit, die während der Installation und in den verschiedenen Phasen der Systemimplementierung getroffen werden müssen. So sorgt beispielsweise die „gelernte Portsicherheit“ dafür, dass nur ein autorisiertes Gerät auf einen Port zugreifen kann. Wenn ein nicht autorisiertes Gerät versucht, sich mit dem System zu verbinden – z. B. um eine neue Kamera anzuschließen – wird ein Alarm ausgelöst, und der Zugriff auf den Anschluss wird verweigert, bis er von einem Menschen autorisiert wird.

Die Shortest Path Bridging (SPB)-Technologie kann verhindern, dass böartige Aktivitäten von einem System auf ein anderes übergreifen. Es werden Regeln aufgestellt, damit eine Kamera nur an den Rekorder streamen kann, und andere leistungsstarke Segmentierungstechnologien werden in Multi-IoT-Netzwerken eingesetzt.

Systeme sollten unsichere Protokolle wie FTP und Telnet deaktivieren, die die Kommunikation über ein Netzwerk erleichtern, aber zusätzliche Möglichkeiten für Hacker bieten können. Diese Funktionen sollten „standardmäßig sicher“ sein, um eine Verbindung zum Netz nur dann zuzulassen, wenn sie beabsichtigt ist.

Effektive Cybersicherheit erfordert auch eine Beschränkung des physischen Zugangs zu einem System. Wenn ein Switch in einem Hausmeisterraum aufgestellt wird, zu dem jeder Zugang hat, ist er nicht gut geschützt.

Wenn man den physischen Zugang zu einem System erlaubt, kann jeder – auch ein Mitarbeiter, der eine Insider-Bedrohung darstellt – leicht einen Laptop anschließen und auf das gesamte System zugreifen.

Kameras sollten den Zugang zu den Netzwerkgeräten aufzeichnen, um umfassenden Schutz zu gewährleisten.



6. Grenzen eines Air-Gap-Ansatzes

Wenn es darum geht, Videosysteme vor Cybersecurity-Angriffen über das Internet zu schützen, war es in der Vergangenheit üblich, Systeme mit Air Gaps einzurichten.

Bei einem Air-Gap-System wird ein Computer oder ein Netzwerk isoliert und daran gehindert, eine externe Verbindung herzustellen. Da ein Air-Gap-Computer physisch abgetrennt und nicht in der Lage ist, sich drahtlos oder physisch mit anderen Computern oder Netzwerkgeräten zu verbinden, wird dieser Ansatz als Allheilmittel zur Gewährleistung der Cybersicherheit von Videosystemen angesehen.

Es ist jedoch ein riskantes Unterfangen, sich auf Air Gaps als einzigen Cybersicherheitsschutz zu verlassen. Es gibt eine Vielzahl von Situationen, in denen ein Air-Gap-System mit dem Internet verbunden werden kann, auch wenn es nur kurzzeitig ist. In diesem Fall ist das System zum Schutz vor Katastrophen auf andere Cybersicherheitsmaßnahmen angewiesen, sofern es diese gibt.

Die Annahme, dass ein System für immer ein Air-Gap-System sein wird, ist keine Lösung für die Cybersicherheit. Stattdessen ist es eine Katastrophe, die nur darauf wartet, zu passieren.

Air-Gap-Systeme können auch nicht die Vorteile der künstlichen Intelligenz (KI) und anderer Funktionen nutzen, die auf dem Zugang vieler Nutzer und der Analyse gemeinsamer Erfahrungen beruhen. Die Daten eines einzelnen Kunden sind nicht so nützlich wie die Daten von Hunderten von Kunden, die in der Cloud verfügbar sind. Air-Gap-Systeme ermöglichen es den Kunden nicht, den zusätzlichen Wert intelligenter Analysen zu nutzen. Der Verzicht auf einige Daten (der mit Überlegungen zum Datenschutz einhergeht) ist ein Preis, den die Kunden zahlen, um einen größeren Nutzen zu erzielen.

Angesichts der heutigen Anforderungen der Kunden an die Verbindung und den ständigen Zugang zu ihren Systemen wird der Anwendungsfall für Air-Gap-Systeme immer begrenzter.

Unternehmen neigen auch dazu, sich dagegen zu wehren, eine völlig separate Netzwerkinfrastruktur für die Videoüberwachung zu schaffen. So etwas wie ein „separates, sicheres“ Netz gibt es nicht.

7. Keine Videodaten mehr verlieren

Datenverlust ist ein Problem für jedes IT-System, aber noch viel mehr für IT-Systeme, die Videoüberwachung bieten. Ein Videoüberwachungssystem ist unternehmenskritisch und muss rund um die Uhr funktionieren. Es gibt keine Ausfallzeiten, die es den Administratoren ermöglichen würden, Probleme mit Datenverlusten zu diagnostizieren und zu lösen. Vielmehr müssen die Probleme ständig und in Echtzeit angegangen werden.

Hier können Managed Switches helfen. Managed Switches ermöglichen es Systemadministratoren, Probleme mit Datenverlusten schnell zu diagnostizieren und zu beheben. Sie können auch die Quelle(n) des Datenverlusts leicht identifizieren. Es gibt keinen „Fingerzeig“ darauf, welche Systemkomponente fehlerhaft ist.

Pakete können verloren gehen, weil die Daten von der Glasfaserübertragung auf Kupfer und Ethernet umgestellt werden. Elektrische Sende- und Empfangsgeräte werden verwendet, um Daten von der Funkübertragung in die elektrische Übertragung umzuwandeln, und diese Geräte können eine Quelle für verlorene Datenpakete sein.

Bei der Videoüberwachung ist ein verlorenes Datenpaket gleichbedeutend mit einer Beeinträchtigung des Videobildes – es ist sozusagen für immer verloren. Es gibt keine Möglichkeit, Videobilder wiederherzustellen, die während eines Ausfalls verloren gegangen sind. Denken Sie zum Beispiel an eine Anwendung in einem Kasino, bei der die Folge eines ausgefallenen Videosystems der Verlust eines Spieltisches ist, was wiederum zu Umsatzeinbußen führen kann.

Bei der Vielzahl von Videoüberwachungsanwendungen ist Redundanz erforderlich, um einen kontinuierlichen Betrieb rund um die Uhr zu gewährleisten.

Das Bedürfnis nach Zuverlässigkeit muss im Kontext von Risiko und Nutzen abgewogen werden. Ein System kann weniger teuer, weniger komplex und/oder weniger fehlertolerant sein, aber es kann auch sein, dass ein solches System nicht wie vorgesehen funktioniert – was wiederum Kosten verursacht.

Eine weitere Variable, die zu Leistungsproblemen in Videosystemen führen kann, ist die Unterscheidung zwischen Unicast und Multicast, zwei Methoden zum Senden von Daten über ein Netzwerk. Unicast ist ein Eins-zu-Eins-Kommunikationsmodell, bei dem ein einzelner Sender Daten an einen einzelnen Empfänger übermittelt. Im Gegensatz dazu handelt es sich bei Multicast um ein One-to-many-Modell, bei dem ein einzelner Sender Daten an mehrere Empfänger übermittelt.

Viele Videoüberwachungsanwendungen arbeiten im Unicast-Modus. Das bedeutet, dass eine Kamera in Echtzeit von einer Person überwacht wird – es handelt sich um einen einzigen Videostream.

Manche Anwendungen erfordern jedoch Multicast, bei dem ein einzelner Videostream von mehreren Benutzern angesehen wird. Probleme entstehen, wenn ein System von Unicast auf Multicast umstellt. Bei der Umstellung geht es um mehr als nur das Umlegen eines Schalters, und Nuancen und Details der Umstellung können Probleme bei der Systemleistung verursachen. Probleme entstehen, wenn Teile eines Systems auf Unicast eingestellt sind, obwohl sie auf Multicast eingestellt sein sollten, oder umgekehrt. Eine ordnungsgemäße Konfiguration dieses Punktes im gesamten System ist entscheidend.

Intelligente Netzberatungsfunktionen ermöglichen es dem Endnutzer zu verstehen, was in Bezug auf die Netzleistung normal ist, um dann zu erkennen, wenn etwas abnormal ist oder außerhalb der üblichen Erwartungen liegt. Alle Abweichungen werden automatisch gemeldet, und Menschen können bei Bedarf eingreifen, um die Probleme zu lösen.



8. Verwaltung von Lebenszyklen in IP-Überwachungssystemen

In der Welt der IT können die Produktlebenszyklen je nach Branche und Produkt drei bis 10 Jahre betragen. Es gibt bereits Protokolle, die sich mit Fragen wie der Zeit zwischen zwei Ausfällen (MTBF), Firmware und Sicherheits-Patches befassen.

Im Bereich der Videoüberwachung sind die Produktlebenszyklen traditionell länger – es gibt jahrzehntealte Videokameras, die immer noch im Einsatz sind. Bei der Anpassung von IT-Verwaltungsstrategien an IP-Videosysteme kann es somit zu Unstimmigkeiten kommen.

Die IT-Unterstützung durch einen Hersteller ist für den Integrator und den Endnutzer von großem Wert. In der Vergangenheit haben längere Lebenszyklen im Bereich der physischen Sicherheit zu Systemen geführt, die über den erwarteten Zeitraum hinaus und in einer nicht unterstützten Umgebung betrieben werden.

Die weitere Verwendung von Geräten, die nicht vom Hersteller unterstützt werden, ist mit Risiken verbunden. Wenn beispielsweise die Software nicht aktualisiert wird, kann dies die Tür für Cyberbedrohungen öffnen.

Die meisten Geräte haben heute eine fünfjährige Garantie und könnten realistischere noch weitere fünf Jahre in Betrieb sein. Angesichts der sich schnell verändernden Technologielandschaft wollen die meisten Kunden jedoch die aktuellsten Funktionen nutzen. Die Beschleunigung der Technologie sorgt für kürzere Lebenszyklen in der Sicherheit, genau wie in der allgemeinen IT- und Netzwerkumgebung.

9. Das IT-Ökosystem in Videosystemen

Ein einheitliches IT-Ökosystem ist der beste Ansatz, um ein erfolgreiches IP-Videosystem zu gewährleisten. Der Erfolg jeder neuen Technologie hängt von einem IT-Ökosystem ab, das sie unterstützt. Themen wie die Interoperabilität von Hardware und Software sorgen für einen reibungslosen Systembetrieb.

Offene Standards gewährleisten maximale Flexibilität für die Kunden in der Gegenwart und in der Zukunft. Vereinfachte Abläufe sind ebenfalls nützlich. So verfügt beispielsweise [Alcatel-Lucent Enterprise](#) über ein einheitliches Betriebssystem, das mit jedem von dem Unternehmen verkauften Ethernet-Switch funktioniert.

Behalten Sie die Strategie bei, Produkte zu übernehmen, die in ihrer Umgebung und mit anderen Produkten im Ökosystem gut funktionieren, um den Erfolg zu gewährleisten.

Ein erfolgreiches IT-Ökosystem entsteht nicht von selbst. Vielmehr wird es von Partnern aus der Industrie gefördert, die zusammenarbeiten, um den Erfolg sicherzustellen. Grundsätze wie Offenheit und Interoperabilität tragen zum IT-Ökosystem bei. Erfolg steigert die Leistung aller Komponenten eines Systems und des Systems als Ganzes.

Erfahren Sie mehr über die [Videoüberwachungslösungen von Alcatel-Lucent Enterprise](#).