WHITE PAPER

Erhöhung der physischen Sicherheit durch Systemvereinheitlichung

Genetec™

genetec.de

Zusammenfassung

Während Unternehmen nach Videoüberwachungs- und Zutrittskontrollsystemen suchen, die im Rahmen ihrer Sicherheitsstrategie größere Interoperabilität bieten, stellt die Mehrheit der Hersteller im Sicherheitsbereich weiterhin unterschiedliche Systeme mit begrenzter Kommunikation zwischen den Systemen zur Verfügung.

Mit den jüngsten Fortschritten bei Softwaretechnologien und den laufenden Partnerschaften zwischen Sicherheitsherstellern ist die Integration zu einem beliebten Ersatz für traditionelle Schnittstellen geworden. Aber auch Integration hat ihre Grenzen. Die Antwort darauf liegt in einzigen Softwareplattform, die Zutrittskontrolle, Gegensprechanlage, Einbruchs und Videogeräte verwaltet und gleichzeitig eine einheitliche Schnittstelle zur Überwachung des gesamten Systems bietet. Ein solches System geht weit über die grundlegenden Funktionalitäten der Vernetzung und Integration hinaus und bietet Endnutzern eine effiziente, flexible und kostengünstige Option zur Systemvereinheitlichung, die bei maßgeschneiderten und teuren Lösungen wie PSIMs nicht erhältlich ist.

Entwicklung von Sicherheitslösungen nach den Bedürfnissen der Endnutzer

Trotz aller heute verfügbaren Technologien, hat die Branche Schwierigkeiten, Sicherheitslösungen zu entwickeln, die die wahren Bedürfnisse der Nutzer erfüllen: ein kohärentes, effizientes, nicht proprietäres und kostengünstiges Video- und Zutrittskontrollsystem. Es ist wichtig zu erkennen, dass ein vereinheitlichtes Video- und Zutrittskontrollsystem ohne diese grundlegenden Kriterien für Kunden nicht zweckmäßig erscheint und daher nicht genügend Nachfrage für Hersteller generiert, um die Entwicklung eines solchen Produkts zu rechtfertigen.

Effizienz gewinnt an Bedeutung

Die Priorität der Sicherheitskräfte besteht darin, ihre Kernaufgaben wie Überwachung, Ermittlung und Reaktion auf Vorfälle zu erfüllen, um die Sicherheit des Unternehmens zu gewährleisten. Sie sollten nicht durch die Verwaltung der Technologie an der Erfüllung dieser wichtigen Aufgaben gehindert werden. Mit anderen Worten, die verwendeten Sicherheitstechnologien sollten ihnen helfen, effizienter und effektiver zu sein, ohne sie zu verlangsamen.

Rich Anderson, CTO von Razberi Technologies, zuvor VP of Marketing für GE Security und VP of Engineering für CASI-RUSCO, illustriert in einem seiner Artikel das Problem der heutigen disparaten Systeme folgendermaßen: „Zutrittskontrollsysteme schlagen vor allem wegen ungültiger Ausweise, erzwungenen Zutritts und offener Türen Alarm. Diese Vorfälle müssen untersucht werden. Mit einem isolierten Überwachungssystem ist das jedoch mühsam. Der Alarm wird auf einem System empfangen und Ihr Sicherheitsteam muss den Vorfall auf einem völlig anderen System untersuchen. Da das Überwachungssystem eine andere Benutzerschnittstelle hat, muss er „umschalten". Welche Kamera soll er aufrufen, um den Vorfall zu sehen? Ein erfahrener Bediener weiß es, aber diese „Erfahrung" ist eine teure Schulung." [1]

Kombination von erstklassigen Technologien

Der PC-Industrie ist es gelungen, interoperable Produkte herzustellen. Jeder kann heute einen PC kaufen und neue Hardware wie Drucker, Webcam, Gaming-Gerät hinzufügen oder sogar eine neue Festplatte installieren, die Informationen doppelt so schnell verarbeitet wie die vorherige. Das funktioniert fast alles, ohne den gesamten PC oder das Betriebssystem auszutauschen.

In der Sicherheitsbranche ist dies jedoch nicht der Fall. Ein Anwender kann nicht einfach den neuesten drahtlosen High-Tech-Türcontroller kaufen und ihn zu einem bestehenden Zutrittskontrollsystem hinzufügen. Oder die neuesten und besten IP-Kameras kaufen und mit einem Video-Management-System (VMS) verbinden, ohne zuvor zu überprüfen, ob dieses Modell unterstützt wird. Aus diesen und vielen anderen Gründen hinkt die Sicherheitsbranche der PC-Industrie hinterher.

[1] Video and Access Control Integration, SecurityInfoWatch.com, Rich Anderson, 25.03.2009

In Wirklichkeit wird sie das, was die PC-Industrie in Bezug auf Interoperabilität kann, vielleicht nie erreichen. Auf eine proprietäre Technologie zu setzen, kann kostspielig sein. Beim Erscheinen einer neuen Technologie wirft die Option der Integration die Frage auf, ob man bestehende Investitionen aufgeben und mit einer neuen Investition von vorne anfangen soll oder nicht.

Auf der andern Seite bietet die Möglichkeit, erstklassige Produkte verschiedener Hersteller miteinander zu kombinieren und die neuesten technologischen Fortschritte in ein Sicherheitssystem zu integrieren, letztendlich mehr Flexibilität sowie die Gewissheit, dass Ihre Investition zukunftssicher ist.

Verwaltung von Investitionen

Eine Lösung, die perfekt an alle bestehenden Systeme und die Infrastruktur eines Unternehmens angepasst ist, kann effizient und attraktiv sein, ist aber wahrscheinlich wie jeder maßgeschneiderter Ansatz auch teuer. So etwa die ERP-Systeme (Enterprise Resource Planning), die von vielen Unternehmen genutzt werden. Ein ERP-System kann durch spezialisierte ERP-Systemintegratoren an nahezu jedes Geschäftsmodell und seine Umgebung angepasst werden. Obwohl die Kosten für die Anpassung eines solchen Systems sehr hoch sind, rechtfertigt normalerweise ein signifikanter Produktivitätsgewinn nach der Installation die Investition.

Investitionen in Sicherheitsabteilungen und Ausrüstung werden immer als Kosten betrachtet und es ist unwahrscheinlich, dass Sicherheitssysteme an jeden internen Prozess angepasst werden können. Da diese Systeme selten Einnahmen generieren, werden die Budgets üblicherweise streng kontrolliert. Die vollständige Überholung eines Systems, unabhängig von der eingesetzten Technologie, hängt ganz vom verfügbaren Budget und dem Buy-in der Geschäftsleitung ab. Oft finden Diskussionen über eine Modernisierung oder den Ersatz eines Systems erst aus der Not heraus statt (z. B. Alterung des Systems oder Sicherheitsmängel) und der Prozess der Beschaffung und Implementierung eines Systems dauert Monate, wenn nicht Jahre.

Daher ist es äußerst wichtig, die Gesamtbetriebskosten eines kohärenten Video- und Zutrittskontrollsystems zu rechtfertigen.

Integrierte Systeme

Mit den jüngsten technologischen Fortschritten und der verstärkten Zusammenarbeit zwischen Herstellern ist die Integration zu einem beliebten Ersatz für traditionelle Schnittstellen geworden.

„Systemintegration ist im Bereich der Informationstechnologie die physische oder funktionelle Verknüpfung verschiedener Computersysteme und Softwareanwendungen.“ [2]

Die beliebtesten Integrationsmethoden beinhalten, speziell in der Sicherheitsbranche, Netzwerkprotokolle und Software Development Kits (SDK).

Netzwerkprotokolle sind sehr leistungsfähig, da sie verschiedene Betriebssysteme unterstützen und Ihnen ermöglichen, Ihre Anwendungen in Echtzeit zu verwalten. Die Integration zweier Systeme über ein Netzwerkprotokoll ist zeitaufwändiger als mit einem SDK. Sie kann aber auch eine gemeinsame Datenbank für zwei Systeme erfordern. Netzwerkprotokolle sind bei Edge-Device-Integrationen wie IP-Kameras oder Türsteuerungen beliebt, werden aber noch häufiger zwischen zwei Softwareanwendungen verwendet. Netzwerkprotokolle gelten einfach als effektiver.

Ein SDK, auch Application Programming Interface (API) genannt, besteht aus einem DLL-Paket, das von Softwareherstellern erstellt und vertrieben wird, damit andere Softwareentwickler sich in ihr System integrieren können.

SDKs vereinfachen die Integration, indem sie komplexe Mechanismen wie Authentifizierung, Dekodierung von Videos, komplexe Netzwerkprotokolle usw. vor Entwicklern verbergen. Da sie die Aufgabe eines Software-Integrators vereinfachen, bieten die meisten Hersteller von DVR, NVR und Zutrittskontrollsystemen anstelle eines Netzwerkprotokolls ein SDK oder API an.

Die meisten Videoüberwachungshersteller bieten ein SDK an, mit dem Live- und Abspielvideos in jede Anwendung integriert werden können. Einige Hersteller von Zutrittskontrollsystemen verwenden beispielsweise das SDK von DVR-Anbietern, um einen Zutrittskontrollalarm für eine schnelle Wiedergabe mit dem zugehörigen Video zu verknüpfen. Die Mehrheit der Hersteller von Zutrittskontrollsoftware bietet auch ein SDK an, damit VMS-Systeme Zutrittskontrollereignisse von ihrem System empfangen können. Einige Anbieter von Zutrittskontrollsystemen erlauben Videoherstellern sogar, einen Teil ihrer Funktionen in die Benutzeroberfläche des Zutrittskontrollsystems zu integrieren.

[2] System Integration Course Syllabus, Georgia State University, Webseite, abgerufen 27. Juni 2007

Unabhängig von der gewählten Integrationsmethode beginnen integrierte Systeme auf jeden Fall, Benutzern für größere Effizienz Hilfsmittel an die Hand zu geben. Es ist üblich, dass eine integrierte Zutrittskontroll- und Videolösung Live- oder Wiedergabedateien anzeigt, die mit einem Zutrittskontrollereignis von der Zutrittskontrollschnittstelle verbunden sind.

Darüber hinaus bieten integrierte Lösungen einen weiteren wichtigen Vorteil: Die Anwender sind nicht für das gesamte Sicherheitssystem auf einen einzigen Hersteller angewiesen. In einigen Fällen kann es von Vorteil sein, mit zwei unabhängigen Anbietern zu arbeiten, die jeweils mehrere eigene Technologiepartner haben. In diesem Fall können Nutzer, die ihre aktuelle Videoüberwachungslösung nicht mögen, zu einem anderen Hersteller wechseln, solange diese mit dem Zutrittskontrollsystem kompatibel ist.

Obwohl die Senkung der Umstellungskosten für Endbenutzer und die Verwendung eines SDK oder einer API zur Erreichung eines tieferen Integrationsgrades zwischen den Produkten Vorteile hat, kann die Integration auch einige Risiken mit sich bringen.

Bei den meisten dieser Integrationen müssen die Bediener zwei Systeme parallel nutzen, da weder das Video noch das Zutrittskontrollsystem alle erforderlichen Funktionen in einer Benutzeroberfläche bietet.

Mögliche Einschränkungen:

- Das Zutrittskontrollsystem unterstützt keine Kamerasequenzen
- Es ist nicht einfach, alle aufgezeichneten Videoaufnahmen mit Zutrittskontrolle zu durchsuchen
- Das Zutrittskontrollsystem enthält keine Bewegungssuchfunktionen
- Schwenk- und Zoom-Funktionen (PTZ) sind im Vergleich zum Videosystem in der Zutrittskontrolle eingeschränkt

Ein weiterer Nachteil, der bei einem integrierten System häufig zu berücksichtigen ist, liegt in der zukünftigen Wartung und Konfiguration dieses Systems. Der Administrator muss zwei oder drei unabhängige Systeme

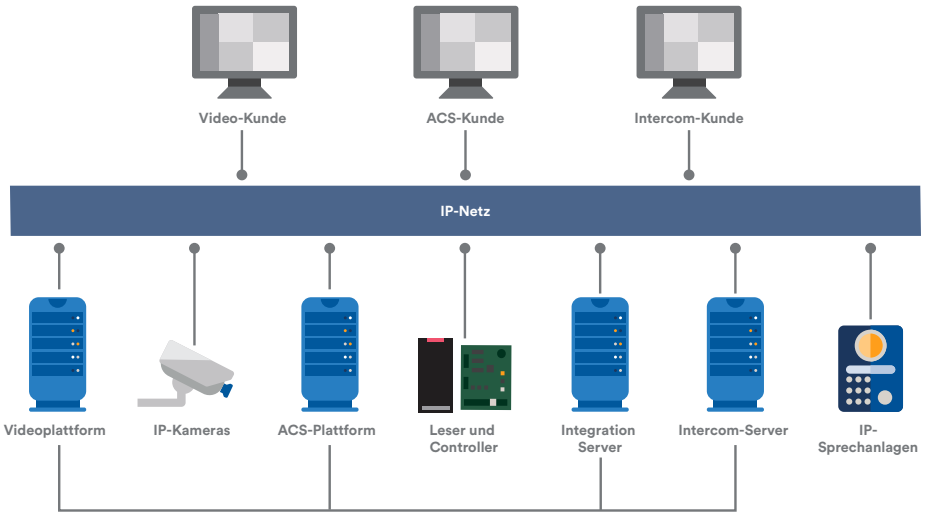

Abbildung 1 – Integrierte Lösungen

konfigurieren und synchronisieren und benötigt daher für die Wartung der Systeme mehr Zeit.

Außerdem sind viele der erforderlichen Konfigurationen redundant und zwingen den Administrator, dieselbe Arbeit auf allen Systemen zu wiederholen.

Einige Beispiele:

- Unabhängige Alarmmanagement-Konfigurationen
- Benutzerverwaltung: Für jeden Bediener muss der Sicherheitsmanager zwei Konten erstellen und in jedem System Berechtigungen angeben
- Jede neue Kamera erfordert eine Konfiguration in zwei unabhängigen Systemen

Schließlich kann es schwierig sein, für ein integriertes System Upgrades durchzuführen und Unterstützung zu erhalten. Bei neueren Versionen einer Anwendung können Änderungen an der Software die Kompatibilität einer Integration zwischen zwei Systemen zerstören, was in einem Unternehmen zu Verzögerungen bei der Systemaktualisierung führt oder die Investition in Maßarbeit erforderlich macht, um die Systeme wieder zu integrieren.

Hersteller ändern ständig ihre Software, um neue Funktionalitäten zu unterstützen, und können damit auch die Funktionsweise bestehender Integrationen beeinflussen, insbesondere wenn sie ihr SDK oder API ändern.

Dadurch, dass sich die neueste Softwareversion eines Systems, das Teil einer integrierten Lösung ist, Auswirkungen auf die Integration haben kann, ist der Installierer dafür verantwortlich, dass die neueste VMS-Software weiterhin vollständig mit der Zutrittskontrollsoftware kompatibel ist. Anstatt das System eines Endbenutzers herunterzufahren und zu aktualisieren, bevorzugen viele Integratoren den Aufbau eines Testsystems in ihrem Labor, um die Integration zu validieren.

Die Suche nach Unterstützung für eine integrierte Lösung kann zu einer komplizierten Angelegenheit werden. Da zwei unterschiedliche Systeme beteiligt sind, die wahrscheinlich von zwei verschiedenen Anbietern stammen, dauert es bei Auftreten eines Problems länger, bis dieses gelöst wird. Beide Hersteller und oft auch der Integrator müssen herausfinden, welches System sich nicht richtig verhält. Die Zeit, die zur Lösung des Problems benötigt wird, hängt auch vom Verhältnis der beiden Softwarehersteller zueinander ab.

Obwohl ein integriertes System im Vergleich zu herkömmlichen Schnittstellen viele Vorteile mit sich bringt, ergeben sich bei diesem Integrationsgrad immer noch viele Probleme.

Open-Platform Systeme

Open-Platform-Produkte, wie sie in der Sicherheitsbranche genannt werden, lassen sich mit verschiedenen Hardwareherstellern integrieren, ohne unbedingt Industriestandards wie Open-Architecture-Systeme zu verwenden.

Hersteller von offenen Plattformen entwickeln, testen und pflegen die Integration mit jedem einzelnen Gerät, das vom Produkt unterstützt wird. Open-Platform-Produkte unterstützen tendenziell ein breites Spektrum von Herstellern, die ähnliche standardisierte Funktionalitäten und Produkte anbieten. Dazu bauen Hersteller solcher Systeme eine allgemeine Integrationsschicht mit den häufigsten Funktionalitäten auf und entwickeln dann für jedes einzelne Produkt, mit dem das System integriert ist, einen Treiber. Diese Strategie funktioniert für spezialisierte Geräte gut, weil sie feste und gut definierte Funktionalitäten haben.

Beispielsweise hat sich das Konzept der offenen Plattform VMS gut am Markt etabliert, da alle IP-Kameras oder IP-Encoder gemeinsame Funktionen bieten.

Solche Systeme bieten Endanwendern enorme Vorteile, da diese nun die Freiheit haben, Software- oder Hardwarehersteller zu wechseln, ohne alle Geräte entsorgen zu müssen.

Die Zutrittskontrollbranche, darunter einzelne Hersteller für Türsteuerungen und Verwaltungssoftware, basiert jedoch traditionell auf proprietären Lösungen. Heute ist es für Anbieter einfacher, geschlossene Zutrittskontrollsysteme aufzubauen. Denn ein geschlossenes System reduziert die Komplexität, vereinfacht den Testaufwand und erhöht den Umsatz pro Kunde durch den Verkauf von Hardware und Software. Jedoch verliert der Endverbraucher durch diese geschlossene Architektur viel Flexibilität.

Aufgrund des Erfolgs in der Videoüberwachung und weil Endnutzer mehr Freiheit fordern, entstehen inzwischen in der Zutrittskontrollbranche ähnliche Open-Platform-Produkte. Heute werden IP-basierte Türcontroller von Herstellern verkauft, die nicht einmal Zutrittskontrollsoftware anbieten. Diese Hardwarehersteller veröffentlichen ihr kabelgebundenes Protokoll oder stellen für die Kommunikation mit ihren Controllern ein SDK zur Verfügung. Andere Hardware-Unternehmen bieten zunehmend auch drahtlose IP-Schlösser, die zur Reduzierung der Installationskosten mit Lesegeräten gebündelt sind.

Absolut führend: Die offene, vereinheitlichte Plattform

Mit dem Open-Platform-Konzept, das in der Videoüberwachungsbranche bereits etabliert ist, dem neuen Trend zu nicht proprietären Türsteuerungen in der Zutrittskontrollbranche und neuen Sicherheitsstandards ist nun eine einheitliche Sicherheitsplattform erzielbar.

Eine vereinheitlichte Plattform ist eine umfassende Softwarelösung, die Zutrittskontrolle, Gegensprechanlage, Einbruch und Videofunktionen über nicht-proprietäre Sicherheitsgeräte verwaltet.

Eine einheitliche Plattform geht über das Tagging oder Bookmarking von Videos hinaus, wenn ein Zutrittskontrollereignis auftritt oder eine zutrittsgesteuerte Tür über die Benutzeroberfläche der Videoüberwachung entriegelt wird. Es ist eine einheitliche Benutzeroberfläche, die eine nahtlose Integration zwischen Video-, Sprechanlagen-, Zutritts- und Einbruchsystemen mit eingebauten Reporting- und Alarmmanagementfunktionen bietet.

Mit dieser Lösung ist es möglich, Videokameras zu konfigurieren und zu verwalten, auf kontrollierte Türen zuzugreifen, Ausweise auszudrucken, Einbruchmeldeanlagen zu überwachen und innerhalb einer einheitlichen Software-Suite dem Sicherheitspersonal alles Nötige zur Verfügung zu stellen, um das Sicherheitsniveau einer Einrichtung zu gewährleisten.

Eine offene, vereinheitlichte Lösung schützt die Investition des Endbenutzers durch Interoperabilität, erfüllt seine Sicherheitsanforderungen und ist kostengünstig in Anschaffung und Wartung.

Eine offene, einheitliche Plattform ist ein Produkt für das Massengeschäft, da es integrierte Unterstützung für standardisierte Sicherheitsprodukte wie IP-Kameras, DVRs, Türcontroller, Alarmzentralen, Sprechanlagen, Ausweisdrucker, Active Directory zur Authentifizierung und Kartenverwaltung bietet, ohne dass für jede Installation eine Anpassung erforderlich ist.

Diese Art von Lösung zielt auf das Massengeschäft, bietet eine gebrauchsfertige Interoperabilität und ist tendenziell günstiger als eine kundenspezifische integrierte Lösung.

Da eine einheitliche Plattform Standardprodukte unterstützt, sind auch Hardware-Investitionen geschützt. Daher kann ein Endbenutzer, der mit der einheitlichen Softwarelösung nicht zufrieden ist, Softwarekomponenten ändern, ohne in spezielle Geräte reinvestieren zu müssen.

Jedoch ist zu bedenken, dass, auch wenn eine Anpassung nicht obligatorisch ist, um eine einheitliche Plattform bereitzustellen, diese dennoch die Integration und Anpassung von Drittanbietern über ein SDK oder API ermöglichen muss. Endbenutzer benötigen solche Tools, um die benutzerdefinierten Integrationen über ihre Video- und Zutrittskontrollanwendungen hinaus entwickeln und pflegen zu können und für solche Maßnahmen nicht nur auf den Hersteller der einheitlichen Plattform angewiesen zu sein.

Die Infrastruktur des einheitlichen Servers

Eine wirklich vereinheitlichte Plattform optimiert durch die gemeinsame Nutzung von Server und Datenbanken Ressourcen für:

- Authentifizierung und Berechtigungen
- Lizenzierungen
- Konfigurationseinstellungen
- Alarme und Ereignisse
- Audit- und Aktivitätsprotokolle
- Videoaufzeichnungen
- Zutrittsprotokolle

Diese Architektur ist einfacher zu installieren und zu verwalten, da sie aus einer einzigen Software-Suite besteht, die gelernt, konfiguriert, aktualisiert und gesichert werden muss, im Gegensatz zum integrierten System, wo diese Aufgaben für alle beteiligten Systeme durchgeführt werden müssen.

Eine zentrale Server-Infrastruktur vereinfacht auch die Arbeit der Endbenutzer, da sie sich nur durch einen einzigen Login mit einem einzigen Server verbinden müssen. Von diesem Server aus haben sie Zugriff auf alle von der vereinheitlichten Plattform angebotenen Dienste. Sie müssen sich nicht mehr mit verschiedenen Servern verbinden, um sowohl Video- als auch Zutrittskontrollermittlungen durchzuführen.

Die Vereinheitlichung vom Server bis zur Schnittstelle bietet Vorteile, die über die ursprünglichen Bedürfnisse des Endbenutzers hinausgehen:

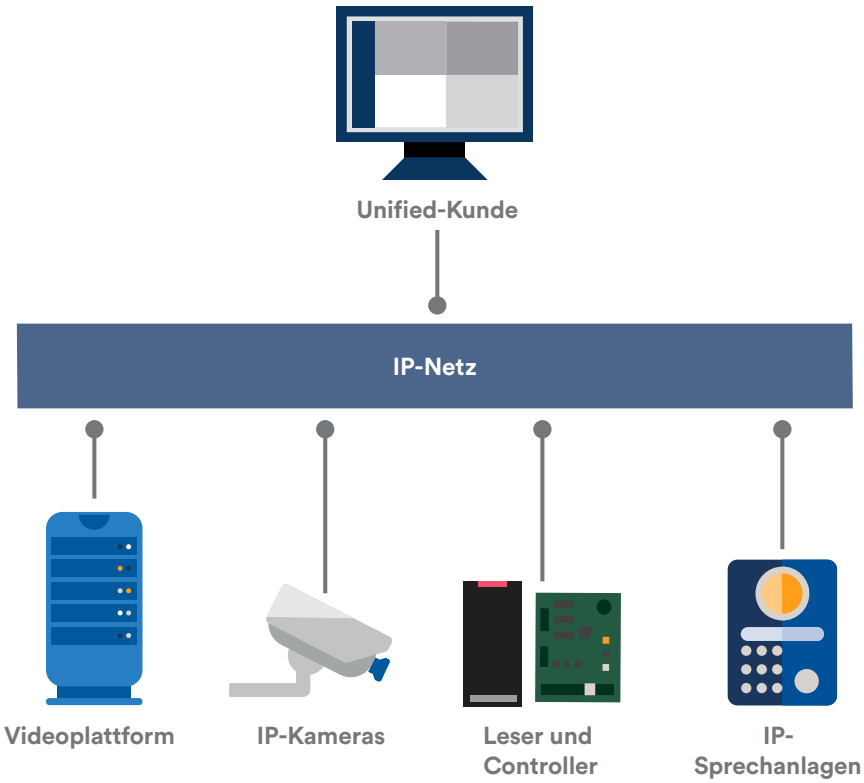

Abbildung 2 – Architektur einer vereinheitlichten Plattform

- Mehr Effizienz durch den Einsatz einer einzigen Schnittstelle
- Systemübergreifende automatisierte Ereigniskorrelation
- Kosteneffizienz durch gemeinsame Konfiguration und Wartung

Die Benutzererfahrung

Eine einzige Benutzeroberfläche für mehrere Sicherheitsanwendungen ermöglicht es dem Bediener, innerhalb derselben Schnittstelle einfach und effizient von einer Sicherheitsaufgabe zur nächsten zu wechseln, wodurch komplizierte Arbeitsabläufe und Schnittstellenmanipulationen auf dem Weg zum gewünschten Fenster vermieden werden.

Die Arbeitsabläufe des Benutzers zwischen den Video- und Zutrittskontroll-aufgaben sind konsistent, so dass der Benutzer mit dem System vertraut wird, eigenständiges Lernen erlebt und mehr Vertrauen in seine Fähigkeit gewinnt, das System zu nutzen.

Darüber hinaus wird die Gesamtzahl der zu verstehenden Workflows durch gemeinsame Kernfunktionen reduziert. Beispielsweise sind die Arbeitsabläufe für Alarmmanagement, Ereignisbewältigung, Berichterstattung, Untersuchung und Reaktionen auf Vorfälle alle gleich, unabhängig davon, ob sie Video, Zutrittskontrolle oder Sprachkommunikation betreffen.

Da vereinheitlichte Systeme eine gemeinsame Benutzeroberfläche haben, erfolgt der Wechsel von einer Anwendung zur anderen nahtlos und es ist weniger Zeit erforderlich, um neue Bediener auf einzelne Systeme zu schulen.

Ereigniskorrelation

Ein einheitliches System bietet Ereigniskorrelation, da Ereignisse und Alarme von einer einzigen Server-Infrastruktur verwaltet werden. Zutritt und Videoereignisse sind korreliert, damit die Bediener Alarme schnell im System überprüfen können. Beispielsweise kann ein Bediener bei einem Zutrittsereignis die Identität eines Karteninhabers schnell verifizieren, um die Authentizität eines Ausweises sicherzustellen.

Eine vereinheitlichte Plattform mit guter Ereigniskorrelation kann die Ermittlungszeit durch das Ausfiltern von Fehlalarmen erheblich reduzieren.

Einfache Wartung und Support

Bei einem einheitlichen System muss nur eine einzige Softwareplattform aktualisiert und gewartet werden, im Gegensatz zu einer integrierten Lösung, bei der mehrere einzelne Systeme bearbeitet werden müssen. Dieser größere Komfort ermöglicht es Integratoren, beim Upgrade des Sicherheitssystems Zeit zu sparen sowie, mit einem einzigen Hersteller zu zusammenzuarbeiten, sollte Unterstützung erforderlich sein. Dies ermöglicht Endbenutzern auch, Systemausfallzeiten während Upgrades zu minimieren und sorgt für eine schnellere Reaktionszeit, um die Anforderungen ihres Systems zu erfüllen.

Was ist PSIM?

Physical Security Information Management (PSIM) ist ein Softwareprodukt zur Überwachung verschiedener Systeme. Die primäre Funktion eines PSIM besteht in der Verwaltung von Informationen aus verschiedenen Systemen und ihrer Darstellung in einer einzigen Benutzeroberfläche.

Im Gegensatz zu einer vereinheitlichten Plattform verfügt ein PSIM in der Regel nicht über eine integrierte Zutrittskontroll-, Einbruchs- oder Videoüberwachungslösung. Stattdessen integriert es verschiedene Systeme über proprietäre SDKs und APIs. Kompatibilitätsprobleme können auch auftreten, wenn eines der Subsysteme ein Upgrade oder eine Wartung erfordert. Zusätzlich muss jedes System, das in eine PSIM integriert ist, separat konfiguriert werden und es gibt einen hohen Grad an Redundanz und doppelten Aufwand (z. B. Konfiguration der Benutzer innerhalb einer PSIM und der zugrundeliegenden Zutrittskontroll-, Video-, Sprachkommunikations- und Einruchssysteme).

Andererseits integriert sich eine PSIM in eine breitere Produktpalette, weil sie das System auf mehrere Sicherheitssysteme innerhalb eines Unternehmens aufbaut. Dennoch kann die Entscheidung für eine PSIM schwierig und teuer sein.

Die Nachteile von kundenspezifischen Integrationen innerhalb einer PSIM und die damit verbundenen langfristigen Kosten für die Aufrechterhaltung der Unterstützung einer Reihe von hochgradig kundenspezifischen Produkten müssen bei der Auswahl der besten Sicherheitstechnologie für die Bedürfnisse eines Unternehmens objektiv betrachtet werden.

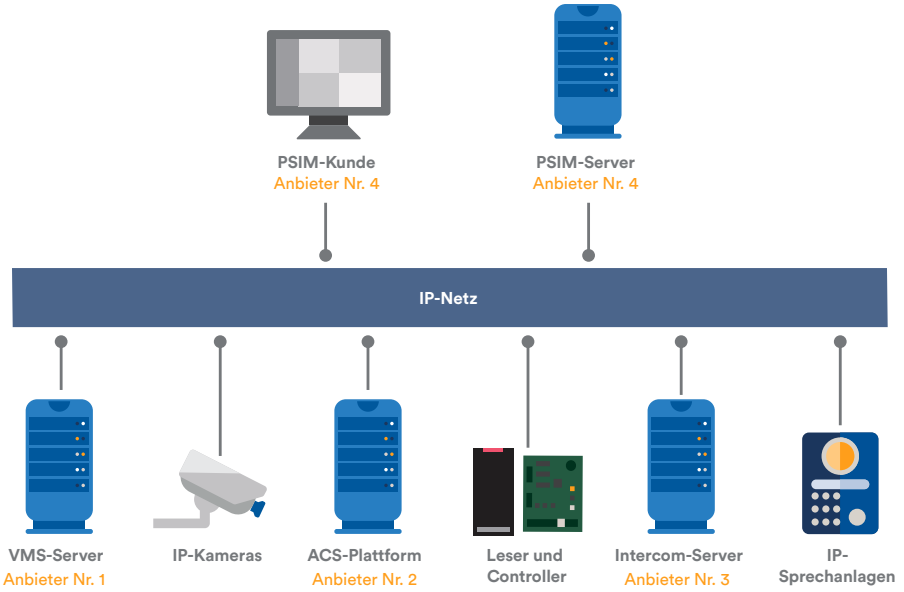

Abbildung 3 – Nachteil einer PSIM-Architektur gegenüber der Architektur einer vereinheitlichten Plattform

Die Wahl einer Lösung

Gehen Sie auf effiziente, flexible und kostengünstige Weise an die Integration von Video- und Zutrittskontrolle heran?

Wie Sie auf den vorherigen Seiten gelesen haben, gibt es viele Möglichkeiten, ein physisches Sicherheitssystem einzusetzen, das sowohl Videoüberwachung als auch Zutrittsskontrolle umfasst. Obwohl Schnittstellen und Integration, die am häufigsten eingesetzten Methoden sind, bietet die vereinheitlichte offene Plattform die effizientesten, flexibelsten und kostengünstigsten Video- und Zutrittskontrollanwendungen.

Deshalb ist es wichtig, sich einen Moment Zeit zu nehmen, um zu prüfen, ob Sie die optimale Methode zur Vereinheitlichung Ihrer Video- und Zutrittskontrollsysteme anwenden. Die Antwort könnte Ihnen helfen, Zeit zu sparen und Kosten zu senken.

Über Genetec

Genetec™ entwickelt eine Open-Platform-Software, Hardware und Cloud-basierte Services für die physische und öffentliche Sicherheit. Das Hauptprodukt, Security Center, vereint IP-basierte Videoüberwachung, Zutrittskontrolle und automatische Kennzeichenerkennung (ALPR) auf einer Plattform. Genetec™, seit 1997 globaler Pionier, hat seinen Hauptsitz in Montreal, Kanada, und beliefert Unternehmen und Regierungsorganisationen über ein Verbundnetz von Vertriebspartnern, Integratoren und Beratern in über 80 Ländern. Genetec™ gründet auf dem Prinzip der Innovation und steht an der Spitze neuer Technologien, die physische Sicherheitssysteme vereinheitlichen. Weitere Informationen über Genetec™ finden Sie unter genetec.de

Lernen Sie Genetec kennen.

genetec.de