

Video-Überwachung und Zutrittskontrolle sind meistens zwei völlig getrennte Welten. Das Thema Video-Überwachung wird in vielen Firmen vom Facility-Management oder vom Sicherheitsdienst betreut. Im Gegensatz dazu liegt die Verantwortung für ein Zutrittssystem in den Händen der IT-Abteilung, die sich mit der Personal-Abteilung abstimmen muss. Der Grund für diese Aufteilung ist einfach: Zutrittssysteme sind bei großen Unternehmen mit dem hausinternen ERP-System gekoppelt, um so die Stammdaten der Mitarbeiter und deren Zutrittsrechten in das Zutrittssystem laden zu können. Dagegen ist die klassische Video-Überwachung mit analogen Kameras ein unabhängiges System, eine Insel-Lösung, die keiner Anbindung in die IT-Infrastruktur bedarf. Etwas vereinfacht gesagt: Die vielen analogen Kameras werden über Koax-Kabel mit den Aufzeichnungsgeräten und den Monitoren verbunden – und schon steht die Überwachungslösung. Firewalls, Router oder IP-Adressen spielen dabei keine Rolle. Entsprechend der Komplexität der beiden Systeme können Video-Überwachungslösungen problemlos von Errichtern installiert werden. Bei Zutrittslösungen ist die Lage nicht so eindeutig. Kleinere Zutrittslösungen ohne Anbindung an ein internes ERP-System sind für kleinere Errichter-Betriebe kein Problem. Sobald jedoch eine

## Video meets Access

ERP-Anbindung erforderlich ist, muss ein Errichter dieses Know-how aufbauen. In den meisten Fällen liegt daher die Projektverantwortung bei Systemhäusern, die sich besser mit komplexen Systemen auskennen.

### Analoge Video-Lösungen versus Netzwerk-Kameras

Seit einiger Zeit drängen immer mehr Netzwerk-Kameras in den Markt der Video-Überwachung. Bei diesen IP-basierenden Überwachungskameras wird das Bild nicht mehr als analoges Signal über Koaxkabel weitergeleitet, sondern als Datenstrom über LAN-Kabel. Damit ändert sich die Situation für alle Beteiligten vollkommen. Video-Überwachungssysteme werden flexibler, um einiges leistungsfähiger, allerdings wird die Installation auch wesentlich komplexer und aufwendiger. Die Einbindung von Netzwerk-Kameras in ein Firmen-LAN – oder besser noch: in ein Überwachungs-Netzwerk – erfordert auf alle Fälle zumindest eine enge Abstimmung mit der IT-Abteilung. Wenn somit beide Systeme bei der IT-Abteilung zusammenlaufen, liegt es sehr nahe, das Video-Überwachungssystem in ein Zutrittssystem einzubinden.

Vor der Komplexität IP-basierender Video-Lösungen schrecken viele kleinere Errichter-Betriebe konsequenterweise zurück. Ohne entsprechendes Netzwerk-Know-how kann ein Kunde nicht kompetent beraten werden und entsprechend risikoreich wäre die Installation für alle Beteiligten. Das mag einer der Gründe dafür sein, dass auch in den nächsten Jahren viele kleinere Errichter-Betriebe ihren Interessenten und Kunden eine analoge Videolösung empfehlen werden. Hinzu kommt, dass sich auch analoge Überwachungskameras problemlos in ein LAN einbinden lassen. Der Anschluss von analogen Kameras an einen IP-Video-Server kombiniert die Vorteile der analogen Welt – wie die riesige Auswahl an Spezial-Kameras und die 100-prozentige Kompatibilität aller Kameras untereinander – mit den Vorteilen der IP-basierten Video-Überwachung.



## Integrierte Lösungen für die Netzwerk-Optimierung

Auch wenn es nach Einschätzung von Experten noch eine geraume Zeit dauern wird, bis sich IP-basierende Video-Lösungen auf dem Markt flächendeckend durchgesetzt haben, ist der Trend zu solchen Lösungen unumkehrbar. Netzwerk-Kameras sind zwar immer noch relativ teuer und hinken bei manchen Lösungen noch hinter den analogen Kameras her (beispielsweise bei Bewegtbildern in der Dunkelheit). Die nächste Generation von Netzwerk-Kameras wird aber immer mehr die Bereiche abdecken, in denen heute sinnvollerweise noch analoge Kameras eingesetzt werden. Neben den Megapixel-Kameras, die sich meistens mit einer hohen Auflösung beim Aufnahme-Chip begnügen, gibt es Netzwerk-Kameras, die mit einem optischen Zoom ausgestattet sind. Und der unausweichliche Preisdruck tut ein Übriges. Der einzige wirklich gravierende Nachteil ist die Inkompatibilität der Netzwerk-Kameras untereinander. Inkompatibilitäten und proprietäre Schnittstellen sind immer ein K.-o.-Kriterium für eine breite Marktdurchdringung. Man kann nur hoffen, dass sich die Hersteller bald auf entsprechende Standards einigen.

Der große Vorteil der IP-basierenden Video-Überwachung ist, dass sie sich in andere Lösungen, wie die Zutrittskontrolle, integrieren lässt. In einem Zutrittssystem ist im Detail hinterlegt, welcher Mitarbeiter oder externe Dienstleister zu welchem Zeitpunkt an welcher Tür eine Zutrittsberechtigung besitzt. Diese Information kann das Zutrittssystem dem Video-System mitteilen. Natürlich sind solche Daten nicht statisch, sondern können sich für bestimmte Mitarbeiter täglich ändern. Das Video-Überwachungssystem kann mit dieser Information die Anzahl der aufgezeichneten und weitergeleiteten Videobilder drastisch reduzieren. Das ist gerade bei großen Installationen notwendig, wenn Hunderte von Kameras an ein lokales Netzwerk angeschlossen sind und die Gefahr besteht, dass das Netzwerk durch die große Anzahl der Kameras überlastet wird. Zwar gibt es auch bei Netzwerk-Kameras Ansätze, den Datenstrom zu optimieren.

So lässt sich bei den meisten Systemen einstellen, dass die Video-Aufzeichnung ereignisgesteuert erfolgt. Durch das Abfragen von Türkontakten startet beispielsweise eine Kamera erst dann die Aufzeichnung oder Bildübertragung, wenn eine bestimmte Tür geöffnet wird. In der Mehrzahl der Fälle ist aber auch das Öffnen der Tür völlig harmlos. Mit der Integration der Video-Überwachung in ein Zutrittskontroll-System kann dieses Prinzip wesentlich effizienter gestaltet werden. Erst beim Versuch eines unberechtigten Zutritts zeichnet das System automatisch Bilder vor und nach dem Zutrittsversuch auf und leitet diese an eine zentrale Stelle weiter. Alle berechtigten Zutritte ignoriert das Video-Überwachungssystem.

Auch komplexere Lösungen lassen sich problemlos realisieren. Beispielsweise können alle Zutrittsversuche von fremden Mitarbeitern in einem bestimmten kritischen Bereich aufgezeichnet wer-



den, während die Zutritte der gleichen Mitarbeiter in unkritischen Zonen wie der Kantine oder dem Raucherzimmer unberücksichtigt bleiben. Fehlalarme und falsch interpretierte Meldungen am Bildschirm des Zutrittssystems lassen sich zuverlässig vermeiden. Für spätere Analysen sind beweiskräftige Bilder archiviert. Mit der Kombination von Zutritt und Video lassen sich differenzierte Lösungen aufbauen. So werden aus anonymen Alarmmeldungen im Zutrittskontroll-System anschauliche und dokumentierte Vorgänge. Und die Netzwerk-Belastung durch das Übertragen von Bildern reduziert sich auf das notwendige Minimum.