

Doppelt sicher

Kombination von Zutrittskontrolle und Videoüberwachung

Zutrittskontrolle und Videoüberwachung sind wie Messer und Gabel: Jedes für sich genommen sinnvoll, zusammen aber erst wirklich effektiv. Die kombinierte Zutrittskontrolle mit Videodokumentation vermeidet Fehlentscheidungen und Fehlalarme, dokumentiert automatisch die Entscheidungsgrundlage und erhöht damit wesentlich die Effizienz des Wachpersonals.

Die betriebliche, elektronische Zutrittskontrolle als eine wirkungsvolle Komponente der Sicherheitstechnik hat die Bewährungsprobe längst hinter sich und ist in vielen Unternehmen nicht wegzudenken. Besonders hervorzuheben sind hierbei die sicherheitstechnischen als auch organisatorischen Vorteile gegenüber veralteter mechanischer Schließtechnik.

Zutrittskontrolle gewährt berechtigten Personen schnell und einfach den Zutritt, verwehrt diesen aber Unberechtigten. Zusätzlich managt Zutrittskontrolle zum Beispiel den Zutritt von Besuchern, die Kunden- und Mitarbeiter-Parkplätze, den Zutritt zur Werkkantine und in Serverräume. In vielen Betrieben ist die Zutrittskontrolle eine von vielen kartengesteuerten Anwendungen (Bild 1) und sehr oft in Kombination mit der Personalzeiterfassung anzutreffen. Mit Hilfe moderner Terminals und Identleser lassen sich flexible Lösungen konfigurieren, die hohen Ansprüchen an Sicherheit und Komfort im Sinne von Bedienungskomfort und Ergonomie genügen. Zutrittskontrolle schützt Personen und Sachwerte und eine Firma vor Diebstahl von geistigen und materiellen Gütern durch ungebetene Gäste.

Umfassend verknüpft

Mit einem einzigen Identifizierungs-Medium wird der räumlich-zeitliche Zutritt zu Gebäuden und Räumen sowie der Netz- und PC-Zugang organisiert. Die Biometrie, wie Fingerprint

und Iriserkennung, bietet zusätzlichen Bedienkomfort und noch höhere Sicherheit und wird oft mit der Videoüberwachung ergänzt beziehungsweise kombiniert.

Zutrittskontrolle dient aber auch der Abschreckung vor Übergriffen auf materielles und geistiges Eigentum. Anbieter von integrierten Lösungen haben umfassende Konzepte mit allen marktrelevanten Identverfahren, mit Biometrie, mit perfekter Vernetzung, mit Long-Range-Identifikation, mit Schnittstellen zu vielen Herstellern im Türen-Umfeld, zur Videoüberwachung der Zutrittspunkte und natürlich zur gesamten Zeitwirtschaft.

Da nicht immer sichergestellt werden kann, dass die Besitzer eines Ausweises auch die berechtigte Person ist, kann die Identifikation auch durch ein biometrisches Verfahren ersetzt oder ergänzt werden. Bei der Identifikation mit dem Fingerprint (Bild 2) kann zum Beispiel komplett auf den Einsatz eines Ausweismediums verzichtet werden. Bei der Handvenenmustererkennung kann gänzlich auf die Berührung eines Sensors verzichtet werden. Komfort aber auch hygienische Anforderungen finden hier ganz neue Anwendungen. Die Technologie bei dem Handvenenmustererkennungsverfahren basiert auf einem Sensor, der das Venenmuster der Handfläche

Bild 2: Biometrische Personenidentifikation mittels Fingerprint



per Nah-Infrarot-Beleuchtung erfasst, digitalisiert, verschlüsselt und abgespeichert.

Abhängig vom Einsatzgebiet

Bei der Videoüberwachung steht die Livebildübertragung für das Wachpersonal im Vordergrund. Es erfolgt oft eine komplette Aufzeichnung aller Bilder auf einer Festplatte nach einem





Bild 1: Kontaktlose Personenidentifikation mit kontaktloser Chipkarte an einem kombinierten Zutritts- und Zeiterfassungsterminal mit hinterlagter Videoüberwachung.

bestimmten Algorithmus. Ein Videoüberwachungssystem besteht aus Kameras, Videoservert und entsprechender Software. Die Videoservert dienen der Konvertierung analoger Signale von Videokameras in digitale Signale, die per TCP/IP über das Ethernet übertragen werden. Gleichzeitig werden die Videodaten dezentral in den Videosevertern für eine spätere Analyse aufgezeichnet. Hybridserver dienen dem Gemischtbetrieb von analogen Kameras und Netzwerk-Kameras.

Bei den analogen Kameras gibt es eine nahezu unüberschaubare Auswahl an Modellen: Innen- und Außenkameras mit und ohne IR-LEDs, Miniaturkameras oder vandalismusgeschützte Kameras. Durch das genormte FBAS-Signal (Farb-Bild-Austast-Synchron-Signal) sind analoge Kameras – im Gegenteil zu Netzwerk-Kameras – miteinander kompatibel. Netzwerk-Kameras sind dagegen proprietär bezüglich Konfiguration und erweiterten Funktionen.

Moderne IP-Videoserver verfügen über eine integrierte Bewegungserkennung (Motion Detection). Über diese werden ereignisgesteuert Aufnahmen gestartet – gegenüber Langzeitaufnahmen eine wesentlich effizientere Nutzung des Speicherplatzes. Sie arbeiten mit einem embedded Betriebssystem, das speziell für industrielle Anwendungen entwickelt ist. Nach einem Stromausfall ist der Server in weniger als 20 Sekunden wieder einsatzbereit.

Für eine größere Effizienz

Die klassische Zutrittskontrolle bietet wie oben gezeigt jeden Komfort bei der Überwachung von Gebäuden und Räumen. Bei einem Alarm jedoch reduziert sich die Information maximal auf einen animierten Lageplan. Die Videoüberwachung wiederum ist in vielen Fällen eine Insellösung innerhalb der Unternehmen. Oft sehr leistungsfähig, aber abgeschnitten vom Zutrittsystem und seinen vielfältigen Möglichkeiten. Videoüberwachung und Zutrittskontrolle sind also oft völlig getrennte Welten, die nicht miteinander kommunizieren können.

Mit der Integration von Zutrittskontrolle und Videoüberwachung werden aus anonymen Zutrittsmeldungen anschauliche Vorgänge. Bei der Auslösung des Alarms zeichnet die Video-Dokumentation Bilder vor und nach dem Alarm auf und gibt sie an die Zentrale weiter. Fehlalarme und falsch interpretierte Meldungen am Bildschirm lassen sich zuverlässig vermeiden. Für spätere Analysen sind beweiskräftige Bilder archiviert. Wenn das Zutrittsystem dem Videosystem mitteilen kann, welche Person zu welchem Zeitpunkt eine Zutrittsberechtigung besitzt, kann die Anzahl der aufgezeichneten und weitergeleiteten Bilder drastisch reduziert werden. Der Access Control Manager hat detaillierte Kenntnisse über den Türstatus (Türfallen- und Rahmenkontakt) und den Leserstatus, so dass der Videoserver nur eine Aufzeichnung wirklich relevanter Situationen vornimmt. Zugleich schaut er quasi in die Vergangenheit: aufgezeichnet werden mehrere Bilder vor dem Trigger-Ereignis und mehrere

Bilder danach (Bild 3). Diese jpg-Bilder können zur Archivierung gespeichert werden.

Sehr effizient ist der automatische Versand per E-Mail an eine berechtigte Person. Der Videoserver wird über Ethernet und mit dem Access Control Manager über Standard-Schnittstellen verbunden und entsprechend den Sicherheitsanforderungen parametrierbar.

Die Terminals und Zutrittsgeräte kommunizieren miteinander über Ethernet und basieren damit auf der IP-Technologie, die zunehmend auch im Videobereich an Bedeutung gewinnt. Bedingt durch die große installierte Basis an analoger Videotechnik setzen viele Firmen heute auf hybride Lö-



Bild 3: Per Videodokumentation werden mehrere Bilder vor und nach dem Ereignis aufgezeichnet.

sungen, bei denen sie die existierenden analogen Kameras mit IP-Kameras gemischt einsetzen können.

Für die traditionellen Anbieter von Videoüberwachungsanlagen – die Errichter – ist der Markt der analogen Systeme auf Grund der günstigen Preise zwar noch auf Jahre gesichert, mittelfristig müssen sich aber die Errichter mit dieser neuen Technologie intensiv auseinandersetzen. □

→ AUTOR

Werner Störmer ist Prokurist bei der PCS Systemtechnik GmbH, Essen.
Tel.: +49(0)201/8941630
E-Mail: wstoermer@pcs.com
www.pcs.com

