

# **IP Video Surveillance - Videoüberwachung in Geldinstituten**

## INHALT

<b>1</b>	<b>VIDEOÜBERWACHUNG IN GELDINSTITUTEN</b>	<b>3</b>
<b>2</b>	<b>RECHTLICHE BESTIMMUNGEN UND ANFORDERUNGEN</b>	<b>3</b>
<b>2.1</b>	<b>Vorschriften der Verwaltungs-Berufsgenossenschaft</b>	<b>3</b>
<b>2.2</b>	<b>Datenschutzbestimmungen</b>	<b>5</b>
<b>2.3</b>	<b>Mitbestimmungsrecht gemäß BetrVG</b>	<b>6</b>
<b>3</b>	<b>EINSATZBEREICHE DER VIDEOÜBERWACHUNG</b>	<b>6</b>
<b>3.1</b>	<b>Bestimmungszweck</b>	<b>6</b>
<b>3.2</b>	<b>Räumliche Abgrenzung</b>	<b>7</b>
<b>4</b>	<b>EVOLUTION DER RAUMÜBERWACHUNG IN GELDINSTITUTEN</b>	<b>8</b>
<b>4.1</b>	<b>Film-/ Einzelbildkameras</b>	<b>8</b>
<b>4.2</b>	<b>CCTV-Kameras</b>	<b>8</b>
<b>4.3</b>	<b>ORÜA mit Netzkameras</b>	<b>9</b>
<b>4.4</b>	<b>Videoüberwachung in Geldausgabeautomaten (GAA)</b>	<b>9</b>
<b>5</b>	<b>FAZIT</b>	<b>10</b>
<b>6</b>	<b>FIRMENPROFIL IP@VISION CONSULTING</b>	<b>10</b>
<b>7</b>	<b>IMPRESSUM</b>	<b>10</b>

## 1 Videoüberwachung in Geldinstituten

Banken und Sparkassen nutzen Videoüberwachung als multifunktionales Instrument für diverse Formen des Risikomanagements zum Schutz von Kunden, Mitarbeitern und Sachwerten. Präventiver Schutz durch Abschreckung, schnelle Abhilfemaßnahmen durch zeitnahe Intervention und die Dokumentation von Vorgängen und Unregelmäßigkeiten stehen im Vordergrund. Vor allem die Gefahr eines Raubüberfalls und eine damit verbundene Bedrohung von Leib und Leben sind jeder Zeit latent vorhanden, aber auch einem Missbrauch von personenbezogenen Daten muss effektiv vorgebeugt werden. Der Einsatz von Videoüberwachung in Geldinstituten unterliegt deshalb ganz bestimmten Vorschriften, z. B. VBG-Kassen „Optische Raumüberwachungsanlagen“ (ORÜA) und den Bestimmungen des Bundesdatenschutzgesetzes (BDSG).

Der technologische Fortschritt in der Videoüberwachung, der Einzug von Digitalisierung und IP-Technologie, die Loslösung von den Standards der Fernsehtechnologie (z.B. PAL) bei Netzwerkkameras, aber auch bereits die fast überall vorhandenen (Netzwerk-) Infrastrukturen zur Datenübertragung bieten ganz neue Lösungsansätze und Synergien. Doch diese einfache und praktisch weltweite Verfügbarkeit der Daten (Bilder) verunsichert viele Menschen und erfordert auf der anderen Seite aber auch eine konsequente Umsetzung der Bestimmungen des Bundesdatenschutzgesetzes. Werden technischer Fortschritt und Datenschutzbestimmungen in Einklang gebracht, so kann zwar nicht das komplette Potenzial ausgeschöpft werden, aber die Vorteile hinsichtlich Sicherheit, Effizienz und Wirtschaftlichkeit sind immer noch enorm.

## 2 Rechtliche Bestimmungen und Anforderungen

Videoüberwachungsanlagen in Banken und Sparkassen unterliegen rechtlichen Bestimmungen und Vorschriften. So schreibt einerseits die Verwaltungs-Berufgenossenschaft den Einsatz von Optischen Raumüberwachungsanlagen in Kredit- und Geldwechsellinstituten vor (diese Vorschriften haben Gesetzeskraft), andererseits gilt es, diese Vorschriften mit dem Bundesdatenschutzgesetz (BDSG) in Einklang zu bringen. Soll zusätzlich zu den vorgeschriebenen Überwachungsmaßnahmen auch nicht öffentlich zugängliche Bereiche in Videoüberwachung mit einbezogen werden, ist auch das Betriebsverfassungsrecht ggf. zu beachten.

### 2.1 Vorschriften der Verwaltungs-Berufgenossenschaft

Die Berufsgenossenschaftliche Vorschrift für Sicherheit und Gesundheit bei der Arbeit (BG-Vorschrift) „Kassen“ (BGV C9) vom 01.10.1988, Stand 01.01.97, fordert im § 6:

- (1) Öffentlich zugängliche Bereiche, in denen Banknoten von Versicherten ausgegeben oder angenommen werden, müssen mit einer optischen Raumüberwachungsanlage ausgerüstet sein.
- (2) Optische Raumüberwachungsanlagen müssen so installiert sein, dass wesentliche Phasen eines Überfalles optisch wiedergegeben werden können.

Des Weiteren heißt es: Diese Forderungen sind erfüllt, wenn optische Raumüberwachungsanlagen (ORÜA) der BG-Information „Kredit- und Geldwechsellinstitute; Installationshinweise für optische Raumüberwachungsanlagen (ORÜA)“ (BGI 819-5) entsprechen. Darüber hinausgehend kann zur Identifikation des Täters eine Kopplung der ORÜA mit der gegebenenfalls im SB-Foyer vorhandenen Videokamera sinnvoll sein.

§ 27 besagt: „Die Versicherten haben Überfallmeldeanlagen sowie optische Raumüberwachungsanlagen bei Überfällen unverzüglich auszulösen, sofern dadurch keine zusätzliche Gefährdung zu erwarten ist“.

**BG-Information: „Kredit- und Geldwechsellinstitute; Installationshinweise für Optische Raumüberwachungsanlagen“ – BGI 819-5, Fassung Januar 2002**

Die BGI 819-5 spezifiziert die technischen Anforderungen an die einzusetzende optische Raumüberwachungsanlage, gibt Aufstellungsorte und Überwachungsbereiche der Kameras vor, regelt Datensicherung und Schutz vor Missbrauch, schreibt eine Verknüpfung mit der vorgeschriebenen Überfallmeldeanlage vor und regelt die Übergabe an den Betreiber.

Ziel ist es, dass der Anreiz, ein Kredit- oder Geldwechsellinstitut zu überfallen, nachhaltig verringert wird. Dabei wird davon ausgegangen, dass der Anreiz reduziert wird, wenn die Täter schnell gefasst werden. Fahndungshilfe ist dabei die optische Raumüberwachungsanlage als wichtiges Hilfsmittel, da die Polizei aus qualitativ guten Bildern zahlreiche Hinweise auf die Täter erhält. Dabei kommt es darauf an, dass die Täter auf den Bildern erkannt und wesentliche Phasen eines Überfalls festgehalten werden können. Diese Bilder können dann auch vor Gericht als Beweismittel verwendet werden.

Als optische Überwachungssysteme sind sowohl Einzelbildkameras als auch Videosysteme zugelassen die die vorgeschriebenen Kriterien erfüllen. Die Kriterien sind für beide Technologien verschieden, da ihre technischen Voraussetzungen und damit ihre Stärken und Schwächen nicht gleich sind. Einzelbildkameras (Fotokameras) besitzen gegenüber CCTV-Kameras eine wesentlich höhere Bildauflösung (ca. 3-mal soviel), können jedoch durch die Verwendung von Negativfilmen nur eine sehr kurze Zeit dokumentieren (min. 3 Minuten) und sind in ihren Betriebskosten sehr hoch. Wird der Aufnahmeprozess nicht manuell durch Betätigung der Überfallmeldeanlage während des Tatvorgangs ausgelöst, so stehen zwangsläufig keine Fotos zur Verfügung.

Videosysteme mit CCTV-Kameras zeichnen permanent Bilder auf digitale Bildspeicher auf und können so die komplette Historie eines Tatvorgangs dokumentieren. Gegenüber niedrigeren Betriebskosten stehen aber wesentlich höhere Anschaffungskosten.

**Technische Anforderungen Videosysteme**

Um die Forderung nach auswertbaren Bildern zu erfüllen, sind zwei Erfassungsbereiche definiert. Beide Anforderungen müssen von dem Videosystem erfüllt werden. Die sind:

- a) Erkennung des Täters
- b) Erfassen der wesentlichen Phasen eines Überfalls

Um die definierten Anforderungen zu erfüllen, ist daher die Anzahl der erforderlichen Videokameras abhängig von der Größe und Beschaffenheit der zu überwachenden Bereiche des jeweiligen Kreditinstitutes.

Zusätzlich muss die Möglichkeit bestehen, dass Verdachtsaufzeichnungen separat abgespeichert werden können. Hierzu muss ausreichende Speicherkapazität zu Verfügung stehen.

Zusammen mit den Bildern müssen Datum und Uhrzeit abgespeichert werden können.

Die Videoanlage muss in der Lage sein, mind. 15 Minuten lang Videobilder mit 1 Bild/Sekunde und Kamera ohne Auslösung der Überfallmeldeanlage aufzuzeichnen.

Mit der Alarmauslösung muss für weitere 15 Minuten lang eine Aufzeichnung von mindestens 2 Bildern/Sekunde und Kamera erfolgen.

Das Kamerasystem ist grundsätzlich auf die Überfallmeldeanlage aufzuschalten.

Des Weiteren ist die **Datensicherung** in der BGI 819-5 geregelt. Um einen Missbrauch der gespeicherten Bilder zu verhindern, müssen Sicherungen gegen unberechtigtes Überspielen von Bildmaterial auf andere Datenträger sowie die Wiedergabe der gespeicherten Bilder auf einem Monitor vorhanden sein, außerdem gelten die Bestimmungen

des Bundesdatenschutzgesetzes. Nach einem Überfall müssen der Polizei unverzüglich Bildmaterial verlustfrei auf entsprechenden Datenträgern zur Verfügung gestellt werden. Auf die Gerichtsverwertbarkeit der gespeicherten Daten ist zu achten.

Die BG-Information „**Kredit- und Geldwechsellinstitute; Anforderungen an die Prüfung von Optischen Raumüberwachungsanlagen**“ – BGI 819-7, Fassung Januar 2002 – regelt die regelmäßig vorgeschriebenen Kontrollen (Funktionsprüfung) der optischen Raumüberwachungsanlage.

§ 37 Abs. 3 der BG-Vorschrift „Kassen“ (BGV C 9) schreibt eine monatliche Funktionsprüfung der optischen Raumüberwachungsanlage vor. Diese Prüfung kann durch unterwiesene Personen, z.B. Mitarbeiter des Geldinstitutes, durchgeführt werden. Die Betriebsbereitschaft der Anlage selbst ist arbeitstäglich zu überprüfen.

## 2.2 Datenschutzbestimmungen

Das Bundesdatenschutzgesetz (BDSG) regelt die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten. Es soll den einzelnen davor schützen dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird. Videoaufzeichnungen sind Dateien mit personenbezogenen Daten im Sinne von § 3 des Bundesdatenschutzgesetzes. Die Bestimmungen des BDSG sind daher auch auf Videoüberwachungsanlagen in Geldinstituten anzuwenden und haben so Auswirkungen auf deren Nutzung und erfordern sowohl technische als auch organisatorische Maßnahmen zu deren Einhaltung.

§ 28 des BDSG erlaubt die Speicherung und Nutzung von Videoaufzeichnungen, soweit es zur Wahrung berechtigter Interessen des Geldinstitutes erforderlich ist und kein Grund zur Annahme vorliegt, dass das schutzwürdige Interesse der Betroffenen an dem Anschluss der Verarbeitung oder Nutzung überwiegt. Der Erforderlichkeitsgrundsatz besagt also, dass die Videoaufzeichnungen nur im Bedarfsfall ausgewertet werden dürfen. Ein solcher begründeter Fall liegt vor, wenn es um Aufklärung von Straftaten geht. Der § 28 besagt des Weiteren, dass die Daten nach Treu und Glauben und auf rechtmäßige Weise erhoben werden müssen. Der Einsatz von Videoüberwachung in Geldinstituten muss daher durch Hinweisschilder deutlich sichtbar angezeigt werden.

So schreibt die Ergänzung des Bundesdatenschutzgesetzes vom Mai 2001 vor, dass in Deutschland die Überwachung öffentlich zugänglicher Räume mit Videokameras und die dafür jeweils verantwortliche Stelle durch geeignete Maßnahmen erkennbar zu machen sind. Die Norm DIN 33450 „Graphisches Symbol zum Hinweis auf Beobachtung mit optisch-elektronischen Einrichtungen (Video-Infozeichen)“ mit Fassung vom Dezember 2004, gibt die Ausführung der Kennzeichnung eindeutig vor.

Aufgrund der Datenschutzbestimmung lassen sich folgende technischen und Organisatorischen Maßnahmen ableiten:

- ❖ Der Einsatz von Videoüberwachung ist durch Hinweisschilder eindeutig anzuzeigen
- ❖ Die Zuständigkeit für die Auswertung, aber auch für die Bereuung und Wartung muss durch eine Dienst- bzw. Arbeitsanweisung geregelt sein.
- ❖ Die Aufzeichnungsgeräte dürfen nur autorisierten Personen zugänglich sein.
- ❖ Aufzeichnungen dürfen nur durch autorisierten Personen ausgewertet werden.
- ❖ Der autorisierte Zugriff am Gerät ist durch geeignete Maßnahmen (z.B. Schlüsselschalter, Passwortschutz, etc.) sicherzustellen.
- ❖ Alle Auswertungen müssen protokolliert werden.
- ❖ Nicht mehr benötigte Videoaufzeichnungen müssen spätestens nach 6 Monaten unwiderrufbar gelöscht werden.
- ❖ Alle Personen, die mit dem Videoüberwachungssystem arbeiten sind, soweit sie bei nicht-öffentlichen Stellen beschäftigt werden, bei der Aufnahme ihrer Tätigkeit

auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

## 2.3 Mitbestimmungsrecht gemäß BetrVG

Gemäß § 87 Abs. 1 Nr. 6 des Betriebsverfassungsgesetzes (BetrVG) sind technische Einrichtungen, die objektiv geeignet sind, das Verhalten oder die Leistungen der Arbeitnehmer zu überwachen, dem Mitbestimmungsrecht eines bestehenden Betriebsrats. Dieses bedeutet, dass sich der Arbeitgeber mit dem Betriebsrat über die Einführung und Anwendung einer Videoüberwachungsanlage einigen muss. Da die Videoüberwachung jedoch gemäß der Verwaltungs-Berufsgenossenschaft für die öffentlich zugänglichen Bereiche vorgeschrieben ist und ausschließlich aufgrund seiner Zweckbestimmung dazu eingesetzt wird, die Sicherheit in diesem Bereich zu gewährleisten, besteht hier kein Mitbestimmungsrecht von Seiten des Betriebsrats, so lange die Bestimmungen eingehalten werden.

Eine Verwendung der Videoüberwachungsanlage zur Überwachung von Mitarbeitern sollte bei Einhaltung der Bestimmungen des Bundesdatenschutzgesetzes ausgeschlossen sein, auch bei Einsatz von digitalen und netzwerkbasierenden Systemen. Der Betriebsrat sollte jedoch bei der Einführung, aber auch bei technischen Änderungen, von optischen Raumüberwachungsanlagen informiert und in die Planung mit einbezogen werden.

Aus Sicherheitsgründen kann auch der Einbezug von nicht öffentlich zugänglichen Bereichen in die Videoüberwachungsanlage sinnvoll sein, hier muss der Betriebsrat auf jeden Fall mit einbezogen werden, da je nach Zweck und Ausführung des Systems sein Mitbestimmungsrecht gemäß § 87 des Betriebsverfassungsgesetzes zu berücksichtigen ist. Ist dieses der Fall, so muss sich Arbeitgeber und Betriebsrat über die Einführung und Anwendung der Videoüberwachungsanlage einigen, diese Einigung wird in der Regel im Abschluss einer Betriebsvereinbarung bestehen. Die Mitbestimmung des Betriebsrates dient nicht der Verhinderung einer Einführung von Videoüberwachung, sondern dazu, dass die Interessen beider Seiten angemessen bei Ausführung und Anwendung berücksichtigt werden.

## 3 Einsatzbereiche der Videoüberwachung

Die Einsatzbereiche von Videoüberwachung in Geldinstituten lassen sich einmal über ihren Bestimmungszweck, zum anderen aber auch über ihren räumlichen Einsatz definieren.

### 3.1 Bestimmungszweck

#### **Schutz und Hilfe vor/ bei Raubüberfall**

Geldinstitute sind permanent der Gefahr von Raubüberfällen ausgesetzt, die Leib und Leben von Mitarbeitern und Kunden bedrohen. Aus diesem Grund schreibt die Verwaltungs-Berufsgenossenschaft den Einsatz von so genannten optischen Raumüberwachungsanlagen in Verbindung mit Überfallmeldeanlagen für Kredit- und Geldwechsellinstituten vor. Oberstes Ziel ist die Minimierung des Risikos durch Prävention und im Ernstfall eine zeitnahe Intervention durch hilfeleistende Stellen. Aussagekräftiges Bildmaterial soll im Nachhinein die Fandung nach den Tätern erleichtern und beschleunigen.

#### **Schutz vor Einbruch, Diebstahl und Vandalismus**

Die Prävention steht auch beim Schutz von Gebäuden und Einrichtungen gegen Diebstahl und Vandalismus im Vordergrund. Einbrüche erfolgen außerhalb der Öffnungszeiten, zumeist nachts oder am Wochenende, wenn sich keine Mitarbeiter Vorort befinden. Videoüberwachung schreckt potenzielle Täter ab und dokumentiert Ereignisse. In Verbindung mit vorhandener Einbruchmeldetechnik und Aufschaltung zu einem Wachdienst

ermöglicht sie aber auch die visuelle Vorprüfung von Alarmmeldungen, unterstützt so eine schnelle und effektive Intervention und hilft damit bei der Schadensbegrenzung.

### **Dokumentation von Transaktionen am Geldausgabeautomat (GAA)**

Geldausgabeautomaten (GAA) sind im Rahmen der Automatisierung von Banken und Sparkassen zu einem Hauptmedium des Bargeldauszahlungsverkehrs geworden und an ca. 50.000 Aufstellungsorten in Deutschland zu finden. Dank dieser Entwicklung können die Kunden von Geldinstituten mittels Kundenkarten und PIN-Code rund um die Uhr über ihre Girokonten verfügen. Der technische Fortschritt bringt aber auch neue Gefahren mit sich, so werden in Deutschland jedes Jahr über 35.000 Fälle mit EC-Kartenmissbrauch mit PIN-Code zur Anzeige gebracht. Aber auch die Geldautomaten selbst werden immer öfter Ziel von Angriffen und Sachbeschädigungen. Der Einsatz von Videotechnik in den Geldautomaten dokumentiert alle Transaktionen in dem sie Aufnahmen des Abhebenden und des Geldausgabeschachts macht und diese zusammen mit den Transaktionsdaten abspeichert. Videoüberwachung am Aufstellungsort des Geldausgabeautomaten, meist das Foyer des Geldinstituts, unterstützt diese Dokumentation wirkt aber auch präventiv gegen Vandalismus vor.

## **3.2 Räumliche Abgrenzung**

Bei der räumlichen Abgrenzung ist zwischen dem öffentlich zugänglichen und denen für Mitarbeitern des Geldinstituts vorbehaltenen Räumlichkeiten zu unterscheiden. Für die öffentlich zugänglichen Räumlichkeiten – Foyer, SB-Bereich, Service-Bereich und Kundentresor – müssen die Vorschriften des Bundesdatenschutzgesetzes (BDSG) bzgl. Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten berücksichtigt werden, auch gelten hierfür die Vorschriften für optische Raumüberwachungsanlagen der UVV-Kassen. Für die für Mitarbeiter vorbehaltenen Räumlichkeiten – Verwaltung, Pausenräume, etc. – unterliegen den Bestimmungen des Betriebsverfassungsgesetzes (BetrVG).

Der öffentlich zugängliche Bereich in Geldinstituten unterteilt sich in die Bereiche Foyer, Selbstbedienungszone (SB-Bereich), Servicezone und Tresor.

### **Foyer und SB-Bereich**

Foyer und SB-Bereich bilden meist eine Einheit, bzw. gehen in einander über. Erfahrungsgemäß ist das Foyer der Bereich in dem sich Bankräuber maskieren und vor verlassen der Bank wieder demaskieren, von daher sollte er in die vorgeschriebenen Überwachungsmaßnahmen nach VBG-Kassen mit einbezogen werden. Im Foyer stehen aber auch die Geldausgabeautomaten (GAA) die nach Geschäftsstellenschluss zugänglich sind. Neben der internen Videoüberwachung der Geldausgabeautomaten selbst (Porträt und Geldausgabeschacht) sollte auch der Zutritt zum Foyer außerhalb der Geschäftszeiten in die Dokumentation der Transaktionen einbezogen werden. Zur eindeutigen Identifizierung des Zutrittsberechtigten kann hier eine Verknüpfung mit dem Kundenkartenleser der Zutrittskontrolle erfolgen. Des Weiteren ist der Foyerbereich außerhalb der Geschäftszeiten vor unberechtigten Aufenthalt von Personen zu schützen.

### **Servicebereich**

Der Einsatz von Videotechnik im Servicebereich eines Geldinstituts ist durch die UVV-Kassen geregelt. Besonders der Kassenbereich gilt als neuralgischer Punkt, da er Anlaufstelle eines jeden Banküberfalls ist. Um die Forderung der UVV-Kassen nach auswertbaren Bildern zu erfüllen, wurden zwei Erfassungsbereiche für die optische Raumüberwachungsanlage definiert. So muss sie das Erkennen der Täter ermöglichen und gleichzeitig die wesentlichen Phasen eines Überfalls dokumentieren. Zur Einhaltung der Anforderungen, die auch die Detailerkennung anhand von Prüftafeln definieren, muss eine entsprechende Anzahl von Kameras so installiert werden, dass die Täter voraussichtlich mit dem Gesicht zu einer Kamera oder im Profil erfasst werden. Als Kamerastandorte eignen sich deshalb die Geldübergabebereiche oder auch Eingänge. Zur Er-

fassung der wesentlichen Phasen eines Überfalls sind die Standorte der Kameras so zu wählen, dass Bereiche in denen die Täter voraussichtlich Mitarbeiter oder Kunden bedrohen erfasst werden.

### **Tresorbereich**

Videoüberwachung im (Kunden-) Tresorbereich wirkt präventiv gegen Einbruch und Überfall, dokumentiert Unregelmäßigkeiten und vermittelt Kunden und Mitarbeitern Sicherheit.

Für alle Bereiche gilt, dass die Kameras möglichst sichtbar installiert werden, um den Anreiz zur Durchführung eines Überfalls zu reduzieren. Auch sollten sie gegen Wegnahme und Zerstörung geschützt installiert werden.

## **4 Evolution der Raumüberwachung in Geldinstituten**

Die Raumüberwachung in Kredit- und Geldwechsellinstituten kann auf eine über 30 jährige Geschichte zurückblicken. Waren in den ersten 25 Jahren analoge Fotokamerasysteme vorherrschend, so entwickeln sich die Technologien mit der Digitalisierung immer rasanter. So haben digitale Bildspeicherung und Analyse, aber auch die Übertragung über IP-basierte Netzwerke längst Einzug in die Videoüberwachungstechnologie gehalten.

### **4.1 Film-/ Einzelbildkameras**

Bereits in den siebziger Jahren kamen die ersten speziell für die Dokumentation von Banküberfallvorgängen entwickelten Fotokameras auf den Markt. Diese waren in der Lage, im Alarmfall Einzelbilder auf einen 35mm S/W-Film mit einer Frequenz von 12 Bildern pro Sekunde 3 Minuten lang aufzunehmen. Außerdem konnten sie auf Anforderung auch so genannte Verdachtsaufnahmen generieren. Viele dieser Kameras sind heute noch im Einsatz, denn ein wesentlicher Vorteil der Fototechnik ist ihre hohe Bildauflösung von mehr als 1.000.000 Bildpunkten und somit hohe Detailerkennbarkeit.

Die wesentlichen Nachteile sind jedoch das Fehlen von sog. Voralarmbildern (der Aufnahmevorgang fängt erst mit dem Überfallalarm an), relativ wenigen Alarmbildern zur Dokumentation des Tatvorgangs (nur 3 Minuten mit einer Bildfrequenz von einem Bild pro Sekunde) und ohne manuelle Alarmauslösung sind zwangsläufig keine Bilder vorhanden. Nach einem Überfall müssen die Fotofilme erst aus den Kameras entnommen und dann entwickelt werden, so dass Fahndungsfotos relativ spät zur Verfügung stehen. Da sich die Alarmaufnahmen in der Kamera befinden, ist auch die Gefahr der Zerstörung beim Überfallvorgang gegeben. Der Betrieb der Kameras ist außerdem mit hohen Kosten verbunden, da die durch die UVV-Kassen vorgeschriebene Funktionsprüfung auf jedes Mal 3 Probefotos pro Kamera erfordert.

### **4.2 CCTV-Kameras**

Aufgrund der zuvor genannten Nachteile der analogen Fototechnik und der Marktreife von digitalen Bildspeichergeräten wurde 1996 von dem Verband der Berufsgenossenschaften die Videotechnik als Alternative zugelassen. Die Bilder werden in diesem Fall von analogen Videoüberwachungskameras generiert, durch spezielle Industrie-PCs digitalisiert und z. B. als JPEG-Datei auf Festplatte gespeichert. Mit Zulassung dieser Technologie war es nun auch möglich, eine komplette Historie des Tatherganges zu dokumentieren (Vor- und Nachalarmbilder), ohne das sofort ein manueller Alarm ausgelöst werden musste (Permanentaufzeichnung in einen Ringspeicher). Durch räumliche Trennung von Bildaufnahme und Speicherung sind die Bilder besser geschützt und nach Überfall sofort verfügbar.

Ein weiterer Vorteil ist auch, dass die innerhalb der monatlichen Funktionsprüfung vorgeschriebene Kontrolle der Überwachungsbereiche und Kameraeinstellungen ohne Kos-

ten für Materialeinsatz schnell und unkompliziert durchgeführt werden können. Die Technologie hat aber auch Nachteile gegenüber der Fotokameratechnologie, so ist zusätzlich zur Verkabelung zwischen Alarmsensorik (Überfallmeldeanlage mit Überfalltaster oder Geldscheinkontakt) nun auch eine Verkabelung zwischen Kamera und Aufzeichnungsgerät erforderlich, da beides keine Einheit mehr bildet. Da analoge Signale auf Kupferleitung Verluste erleiden (Reduzierung der Bildqualität) ist die Distanz zwischen beiden stark eingeschränkt (bei RG-59 max. 115m).

Der größte Nachteil ist jedoch die deutlich geringere Bildqualität gegenüber der Fototechnologie. Sie beträgt, bedingt durch den PAL-Standard **414.720 Bildpunkte** (720 x 576 Pixel) und hat somit, deutlich weniger Detailerkennung zur Folge. Dieser Nachteil kann nur mit der Installation von wesentlich mehr Kameras ausgeglichen werden (ohne das die Fotobildqualität erreicht wird) welches wiederum die Erstinvestitionskosten erhöht.

### 4.3 ORÜA mit Netzwerkkameras

Eine relativ neue Entwicklung im Bereich der optischen Raumüberwachungsanlagen stellen Lösungen mit Netzwerkkameras dar, die alle Vorteile von analogen Filmkameras und Videosystemen mit digitaler Bildaufzeichnung in sich vereinigen. Direkt an das EDV-Netzwerk angeschlossen, mit Bildauflösungen über 1,2 Mio. Bildpunkten und Zertifizierung gemäß VBG 120 – UVV-Kassen – bieten sie die Bildqualität einer Fotokamera und wesentlich höhere Funktionalität als die eines digitalen Videoüberwachungssystems mit CCTV-Kameras. Dieses reduziert die Investitionskosten, da nur wenige Netzwerkkameras (im Vergleich zur Videoüberwachung mit CCTV-Kameras etwa ein Drittel!!!) benötigt werden, und die vorhandene Netzwerkinfrastruktur oftmals verwendet werden kann.

Integration in eine vorhandene Netzwerkinfrastruktur bedeutet auch weiteres Einsparpotenzial, da Dienste und Wartungsfunktionen geschäftsstellenübergreifend zentralisiert und automatisiert werden können. So lassen sich viele Netzwerkkameras mittels integrierten Simple Network Management Protocol (SNMP) in die Echtzeit-Netzwerküberwachungssysteme von Banken einbinden, die auch zur Überwachung der ordnungsgemäßen Funktion von GAAs, Servern, und anderen aktiven IT-Komponenten dienen. Die Geldinstitute können so ohne personellen Aufwand die von der „UVV-Kassen“ geforderte tägliche Überprüfung der Betriebsbereitschaft des „Optischen Raumüberwachungssystems“ gewährleisten. Bei einer Störung oder dem Ausfall des Systems werden die verantwortlichen Personen automatisch benachrichtigt.

Auch kann die geforderte monatliche Überprüfung von abgespeicherten Bildern des Überwachungssystems von zentraler Stelle aus online erfolgen. So bieten Netzwerkkamera basierte „Optische Raumüberwachungssysteme“ gegenüber herkömmlichen Lösungen eine wesentlich höhere Wirtschaftlichkeit, Skalierbarkeit, Funktionalität und Flexibilität.

### 4.4 Videoüberwachung in Geldausgabeautomaten (GAA)

Die Bilder und Informationen von Videoüberwachung in Geldautomaten zur Dokumentation von Transaktionen stehen bereits heute über das Netzwerk des Geldinstituts online zur Verfügung. So können autorisierte Mitarbeiter bei gemeldeten Unregelmäßigkeiten einfach die Transaktionsdaten mit den dazugehörigen Aufnahmen abrufen, bei Kartenmissbrauch weiterleiten und zur Klärung von Betrugsfällen wesentlich beitragen.

Aus technologischer Sicht werden die in den Geldausgabeautomaten integrierten Kameras vor großen Herausforderungen gestellt, so machen Gegenlicht und starke Kontraständerungen vielfach die Bilder der Portraitkamera nur bedingt als Beweismittel brauchbar. Der Einsatz von Kameras mit CMOS-Aufnahmetechnologie und frei definierbaren Zonen zur Belichtungsmessung und Steuerung bietet sich an und da sich in Geldauto-

mat sowieso ein PC befindet, werden Lösungen mit professionellen USB-Kameras nicht lange auf sich warten lassen.

## 5 Fazit

Netzwerkkameras der neuesten Generation mit Bildauflösungen im Megapixelbereich und UVV-Kassen Zulassung bieten erhebliche Potenziale zur Kostenreduzierung gegenüber traditionellen Videoüberwachungslösungen. Speziell im Bereich Bildauflösung und Detailerkennbarkeit sind sie Analogen CCTV-Kameras bei weiten überlegen und sollten deren Einsatz bei „optischen Raumüberwachungsanlagen“ eigentlich verbieten. Die Integration der Videoüberwachung in die vorhandene Netzwerkinfrastruktur des Geldinstituts kann nicht nur die Betriebskosten optimieren sondern erhöht auch die Sicherheit, da bereits während der Überfallphase Bilder außerhalb der Geschäftsstelle verfügbar sind und so die Intervention der Polizei effektiv unterstützt.

## 6 Firmenprofil ip@vision consulting

Die ip@vision consulting ist eine unabhängige Unternehmensberatung und ein Fachplaner im Bereich der professionellen Videoüberwachungstechnik mit besonderem Focus auf Systemintegration, intelligente Bildanalyse und netzwerkbasierte Videoüberwachungslösungen, auch "IP Video Surveillance" genannt. Darüber hinaus bietet das Unternehmen seinen Kunden Dienstleistungen in den Bereichen Projektentwicklung, Marketing, PR und Communication, Vertrieb und Weiterbildung zum Thema IP Video und Informationstechnologie an.

Dabei versteht sich die ip@vision consulting als Mittler zwischen der Security- und IT-Welt zum Nutzen von Anwendern, Händlern, Errichtern, Integratoren, Distributoren und Hersteller. Die ip@vision consulting will durch Leistungsfähigkeit, Flexibilität und einen offenen Dialog überzeugen. Qualität auf dem höchsten Niveau ist dabei für das Unternehmen selbstverständlich. Zur Erweiterung ihres Leistungsspektrums arbeitet die ip@vision consulting mit einem Netzwerk von Spezialisten, die diesem hohen Qualitätsanspruch genügen.

## 7 Impressum

Adresse: **ip@vision consulting**  
Gereon Schroeder  
Händelstrasse 44  
D-47506 Neukirchen-Vluyn

Telefon: +49 (0) 2845 377410  
Fax: +49 (0) 2845 377411  
E-Mail: info@ip-vision.de  
Internet: www.ip-video-surveillance.de

**ip@vision consulting**  
Ihr Ansprechpartner für IP Video Surveillance!

Weitere Informationen zu unseren Dienstleistungen finden Sie im Internet unter:  
[www.ip-video-surveillance.de](http://www.ip-video-surveillance.de)