

BHE-Hinweise zu PC-basierten Videoaufzeichnungskarten

Inhalt:

1. Einleitung
2. Technologie
3. Der PC als Sicherheitssystem
4. Herstellerrisiken
5. BGV-Kassen zertifizierte Videoaufzeichnungskarten
6. Fazit

1. Einleitung

Bei der Vielzahl verfügbarer digitaler Aufzeichnungssysteme für Sicherheitsanwendungen lassen sich im Wesentlichen drei Systembauarten unterscheiden:

- a) Komplette Videoaufzeichnungsgeräte (auch Digitalrekorder genannt), die aus einer abgestimmten Konfiguration von Hardware und Software bestehen und von Herstellern für Sicherheitstechnik in verschiedenen Varianten als Gesamtlösung geliefert werden. Hierbei handelt es sich um bestimmte Systeme, die speziell für die Anwendung von Bildaufzeichnungen von Sicherheitskameras entwickelt wurden und i.d.R. ein hohes Maß an Systemsicherheit und Zuverlässigkeit bieten. Am Markt gibt es sowohl Windows-basierte Komplettsysteme wie auch Systeme, die z.B. auf Linux basieren oder herstellerspezifische Betriebssysteme nutzen.
- b) Netzwerkbasierte Videolösungen, bei denen IP Video Ströme auf Standard Server-Hardware-Plattformen mittels IP Video Software aufgezeichnet werden.
- c) Weiterhin existiert eine große Anzahl von PC-Videoaufzeichnungskarten am Markt. Diese Karten lassen sich meist sehr einfach in einen Standard-PC (meist Windows-basiert) einbauen, wodurch der PC in die Lage versetzt wird, mehrere Videokanäle aufzuzeichnen.

In den folgenden Abschnitten werden speziell Windows-basierte Systeme betrachtet:

Die Unterschiede zwischen einem Windows-basierten Komplettsystem und einem PC, der mittels einer Videoaufzeichnungskarte zu einem digitalen Videorekorder aufgerüstet wird, liegen dabei auf verschiedenen Ebenen. Betrachtet man die Hardware, so sind auf den ersten Blick auch PC-basierte Komplettsysteme nichts anderes als Windows-PCs mit eingebauten Videoaufzeichnungskarten und einer dazugehörigen Software. Die Softwarefunktionen sind ebenfalls in vielen Punkten sehr vergleichbar. Gute, hochwertige Videoaufzeichnungskarten verfügen heute ebenfalls über vielfältige Funktionen, hohe Auflösung und schnelle Aufzeichnungsraten. Daher kommt sehr schnell die Frage auf, warum sich der Nutzer seinen Rekorder nicht selbst zusammenbauen sollte. Vor allem, da PCs auch für andere Zwecke häufig vom Benutzer selber individuell aufgerüstet werden.

2. Technologie

Ein digitales Aufzeichnungssystem ist in der Regel ein Sicherheitssystem, welches vom Endkunden zur Aufzeichnung und Auswertung von sicherheitsrelevanten Bilddaten eingesetzt wird. Wie bei allen Sicherheitssystemen steht die Zuverlässigkeit und Verfügbarkeit des Systems an erster Stelle. Ein Sicherheitssystem darf vieles, nur eines nicht: ausfallen oder fehlerhaft arbeiten.

Betrachtet man Windows-PCs im Allgemeinen, so sind diese nicht unbedingt für ihre Zuverlässigkeit bekannt - Systemabstürze und "eingefrorene" Bildschirme sind unter Windows keine Seltenheit. Ein Windows-basierter PC kann also nur dann als Sicherheitssystem eingesetzt werden, wenn sichergestellt ist, dass dieser ohne Probleme 365 Tage im Jahr im 24 Stunden Betrieb läuft und nicht selbst ein Sicher-

heitsrisiko darstellt. Die Hersteller von kompletten digitalen Videorekordern betreiben daher in der Regel einen sehr hohen Aufwand, um dieses zu gewährleisten.

Zum einen muss die Hardware den hohen Anforderungen eines Dauerbetriebes genügen. Ein handelsüblicher Standard-PC ist für den normalen Büroeinsatz konzipiert worden. Dies bedeutet, dass besonders kritische Bauteile, wie z.B. das Netzteil, die Festplatte oder das Mainboard, darauf ausgelegt sind, im Durchschnitt 8 Stunden am Tag in Betrieb zu sein. Die Komponenten in einem digitalen Videorekorder, der 24 Stunden am Tag aufzeichnet, müssen also für eine mindestens dreimal so lange Lebensdauer ausgelegt sein. Dies schlägt sich in der Auswahl und dem Test der Bauteile und nicht zuletzt auch im Preis nieder.

Die Software für die Videoaufzeichnung selbst kann, wie bereits erwähnt, durchaus vergleichbar sein. Kritisch ist hier jedoch meistens die Windows-Software. Die heutigen Windows-Versionen, wie z.B. Windows 7, verfügen über eine Vielzahl von einzelnen Funktionen. Diese Vielzahl ist einerseits der Erfolgsfaktor von Windows, weil ein PC dadurch sehr flexibel wird und sich für sehr viele verschiedene Anwendungen nutzen lässt. Diese Flexibilität ist ein Grund, weshalb sich viele Hersteller von digitalen Videoaufzeichnungssystemen für Windows entschieden haben. Gleichzeitig führt aber genau dieselbe Flexibilität dazu, dass Windows unter bestimmten Umständen Instabilitäten aufzeigt und es tatsächlich zu Fehlern oder Abstürzen kommen kann.

Daher schränken viele Hersteller von digitalen Aufzeichnungssystemen die Funktionalität von Windows auf das für ein digitales Sicherheitssystem notwendige Mindestmaß ein, um gleichzeitig ein Höchstmaß an Sicherheit und Zuverlässigkeit zu gewährleisten.

3. Der PC als Sicherheitssystem

Nutzer einer PC-basierten Videoaufzeichnungskarte sollten prinzipiell dieselben Überlegungen wie die Hersteller von Videoaufzeichnungsgeräten anstellen. So lassen sich die PC-Karten grundsätzlich in fast jeden PC einbauen. Um jedoch aus einem PC ein Sicherheitssystem zu machen, bedarf es weiterer Schritte.

Zunächst muss gewährleistet sein, dass die Hardware den hohen Anforderungen für den Einsatz in der Sicherheitstechnik genügt. Bei vielen Videoaufzeichnungskarten fehlen z.B. die für die Sicherheitsanwendungen wichtigen Alarm- bzw. Steuereingänge, so dass eine ereignisgesteuerte Aufzeichnung oder eine intelligente Verknüpfung mit der Einbruchmeldetechnik (z.B. Scharfschaltung) überhaupt nicht möglich ist. Darüber hinaus kann man davon ausgehen, dass ein günstiger PC aus dem Supermarkt im Zweifelsfall nicht für den Dauerbetrieb geeignet ist. Weiter sollte gewährleistet sein, dass auf dem PC ausschließlich die Software für die Videoaufzeichnung läuft und der PC nicht nebenbei noch als Büroarbeitsplatz oder für andere Anwendungen genutzt wird. So eine Mehrfachnutzung des Systems ist eventuell kostengünstig, wird aber dann teuer, wenn die Aufzeichnung durch Konflikte mit anderer Software gestört wird und im Bedarfsfall die entscheidenden Bilder nicht zu sehen sind.

Daher ist der Einbau von PC-Videoaufzeichnungskarten in bereits bestehende oder allgemein genutzte PCs ausschließlich für den privaten Bereich oder für absolut nicht sicherheitsrelevante Zwecke zu tolerieren. Ein digitales Videosystem, welches für professionelle Zwecke eingesetzt wird, sollte daher wie andere Sicherheitssysteme möglichst unabhängig von anderen Systemen arbeiten und auf absolute Zuverlässigkeit hin gefertigt sein.

4. Herstellerrisiken

Ein weiterer Aspekt, der hier nicht unerwähnt bleiben soll, ist die Haftung für Mängel. Wenn ein Wiederverkäufer oder Errichter ein digitales Videoaufzeichnungssystem mittels einer PC-Aufzeichnungskarte selbst zusammenbaut, so wird dieser zum Hersteller dieses digitalen Videoaufzeichnungssystems. Dies bedeutet, dass er gegenüber seinen Kunden die alleinige Haftung für das System zu tragen hat. Ein Risiko, welches auf jeden Fall mit berücksichtigt werden sollte.

Auch sollte der Aufwand, ein System zu bauen, in die Kalkulation mit einfließen. Wenn ein Fachhändler oder Errichter durch den Einbau von PC-Karten in einen PC quasi zum "Hersteller" wird, muss der „Inverkehrbringer“ eine Konformitätserklärung über die Elektromagnetische Verträglichkeit (EMV -> CE) ausstellen. Dabei ist zu bedenken, dass durch den Zusammenbau von 2 CE-konformen Bausteinen das Endprodukt nicht automatisch auch CE-konform ist. Darüber hinaus verpflichtet sich der "Hersteller" zur zusätzlichen Lieferung von deutschsprachigen Benutzerunterlagen.

5. BGV-Kassen-zertifizierte Videoaufzeichnungskarten

Seit einiger Zeit sind BGV-zertifizierte Videoaufzeichnungskarten am Markt erhältlich. Diese Karten werden häufig mit dem Hinweis beworben, dass auf diese Weise aus jedem PC ein digitales Überwachungssystem nach BGV-Kassen-Standard zusammengebaut werden kann. Diese Aussage trifft jedoch nur bedingt zu.

Die BGV-Kassen-Zertifizierungsstelle zertifiziert im Wesentlichen die Software, die zu der Karte gehört - nicht jedoch das Gesamtsystem und auch nicht die Karte, also die Hardware selber. Die BGV-Kassen-Prüfstelle macht daher lediglich eine Aussage darüber, ob das System den Anforderungen bezüglich Bildqualität und Aufzeichnungsrate dem BGV-Kassen-Standard entspricht. Eine Prüfung der Zuverlässigkeit der Hardware, also der Karte (und des PCs!) selbst erfolgt nicht.

Die Videoaufzeichnungskarte stellt somit nur einen Teil eines BGV-Kassen-fähigen Gesamtsystems dar. BGV-fähig im Sinne einer qualitativ hochwertigen Überwachung nach BGV-Standard wird das System erst, wenn zusätzlich die ebenfalls zertifizierte Alarmkarte mit den Alarmeingängen in den PC eingebaut wird und der PC selbst den im Handbuch der Videoaufzeichnungskarten genannten Mindestanforderungen entspricht. Es gilt also auch hier, dass der Kunde selbst darüber entscheidet, ob das Gesamtsystem am Ende ein zuverlässiges Sicherheitssystem darstellt.

Die Aussage „BGV-Kassen zertifiziert“ alleine garantiert dieses noch nicht, sondern gibt lediglich einen Hinweis darauf, dass sich mit dieser Karte eine Aufzeichnung im Sinne der Anforderungen der BGV-Kassen realisieren lässt.

6. Fazit

Der Nutzer einer Videoaufzeichnungskarte sollte sich sehr genau über den Einsatzzweck im Klaren sein. Sobald das Videosystem im professionellen Umfeld eingesetzt wird und als Sicherheitssystem arbeiten soll, ist zu prüfen, ob die Hard- und Software des PC selbst diesen Anforderungen entspricht. Ein selbst zusammengebautes Videoaufzeichnungssystem kann dies in aller Regel in Bezug auf Zuverlässigkeit und Qualität nicht leisten.

Ist man als Käufer einer Videoaufzeichnungskarte nicht sicher, ob man selbst ein System erstellen kann, welches in allen Punkten einem Sicherheitssystem gerecht wird, so sollte besser auf ein Komplettsystem eines professionellen Herstellers von Videoaufzeichnungssystemen zurück gegriffen werden.

Die Vorteile wie Erfahrung, Garantie- und Supportleistungen der Hersteller und die Sicherheit, ein getestetes System zu erwerben, welches bereits in dieser Konstellation zigfach im Einsatz ist, sollten für eine Sicherheitsanwendung ausschlaggebend sein.