Checkliste zum Datenschutz in der Videoüberwachungstechnik

Videoüberwachungssysteme müssen aufgrund ihres Einsatzzweckes vielfältige allgemeine und spezifische Anforderungen erfüllen. Dies gilt insbesondere im Hinblick auf die Verarbeitung und Speicherung sensibler, personenbezogener Daten.

Zur Wahrung des Datenschutzes sollten verschiedene technische Möglichkeiten und Aspekte der Videoüberwachung beachtet und geklärt werden. Die nachfolgende Übersicht wurde von den Experten des BHE-Fachausschusses für Videoüberwachungstechnik (FA-VÜT) erstellt und dient Betreibern, Planern und Errichtern von Videoüberwachungssystemen als Leitfaden.
Ergänzend bietet das BHE-Papier „Rechtsfragen in Unternehmen“ allgemeine rechtliche Hinweise in Sachen Datenschutz beim Einsatz von Videoüberwachungssystemen.

Die Checkliste erhebt nicht den Anspruch auf Vollständigkeit, sondern soll als dynamische Hilfestellung bei der Planung und Errichtung von Videoüberwachungssystemen verstanden werden. Um die Auflistung aktuell halten zu können, sind Hinweise auf evtl. fehlende oder zu korrigierende Aspekte willkommen.

In Gesprächen mit Datenschutzbeauftragten haben sich folgende technische Aspekte ergeben:

System-Zugangssicherung

- Zugang erhalten nur registrierte Benutzer (für alle Funktionen).
- Ein Systemzugang ohne individuelle Identifizierung und Authentifizierung darf generell nicht möglich sein.
- Jeder Nutzer benötigt neben einem eigenen Passwort auch einen eigenen Benutzernamen (unter anderem wichtig für die Protokollierung).
- Der Benutzer muss sein Passwort selbst festlegen können.
- Ohne Anmeldung und Authentifizierung darf keine Systemfunktion genutzt werden können.
- Auch Systemadministratoren dürfen nur mittels Identifizierung und Authentifizierung auf das System zugreifen können.
- Für Fernwartung gelten die gleichen Anforderungen (Identifizierung und Authentifizierung), darüber hinaus muss der Betreiber die Möglichkeit haben, Fernwartungszugänge im Einzelfall freizuschalten.
- Passwörter sollten nach BSI-Vorgaben erstellt und erneuert werden.
- Die Herausgabe von Videodaten erfolgt nur auf richterliche Anordnung.

Benutzerkonten

- Ohne Verwendung eines Benutzerkontos (Identifizierung und Authentifizierung) dürfen keine (Fernwartungs-) Zugänge auf das System möglich sein.
- Können Benutzerkonten auch gesperrt statt gelöscht werden, so dass bei Bedarf das Konto nur aktiviert werden muss, ohne mühsam Berechtigungen zusammenzustellen?
- Kann die Fernzugriffsmöglichkeit generell blockiert bzw. aktiviert werden, auch ohne Veränderungen an den Benutzerkonten? (Herstellerpasswort, Hintertür)

- Der Zugang über bestimmte Benutzerkonten kann durch die Eingabe zweier Teilpasswörter abgesichert werden; dabei sollte gewährleistet werden, dass trotz zweier Teilpasswörter die Identifikation des „Paares“ möglich sein muss. Jedes Teilpasswort kann eine Länge von mindestens 8 alphanumerischen Zeichen haben. Eine Mindestpasswortlänge ist erzwingbar.
- Kann nur der Zugang zu den Videoarchiven nach dem 4-Augen-Prinzip gesichert werden? Oder ist das bei jedem Benutzerkonto möglich, so dass z.B. der Zugriff auf die Grundeinstellungen des Systems nur nach Eingabe zweier Passwörter geändert werden kann?
- Passwörter können aus dem System nicht ausgelesen werden. Im System werden ausschließlich Hash-Werte der Passwörter abgelegt, oder die Passwörter werden sicher verschlüsselt gespeichert.
- Es gibt kein Universal-Benutzerkonto und/oder Universalpasswort, das unabhängig von den durch den Betreiber eingerichteten Benutzerkonten stets den Zugriff auf das System freischaltet.
- Jede einzelne Systemfunktion kann für jeden einzelnen Benutzer individuell freigegeben oder gesperrt werden. Für jeden Benutzer muss der Betreiber festlegen können, welche Funktionen er auf welche Datenobjekte (insbesondere auf Videoaufzeichnungen und Systemeinstellungen) anwenden darf. Unerlaubte Zugriffe muss das System automatisch sperren.
- Ist es möglich, dass z.B. die Zuweisung von Berechtigungen zu Benutzern oder das Löschen von Systemprotokollen als Funktionen explizit freigegeben oder gesperrt werden kann?

Systemadministratoren

- Auch Funktionen der Systemadministration unterliegen der Kontrolle des automatischen Berechtigungssystems, insbesondere gilt dies für die Funktionen:
  - ❑ zur Einrichtung, Sperrung, Entsperrung oder Löschung von Benutzerkonten.
  - ❑ zur Zuweisung von Berechtigungen zu Benutzern.
  - ❑ zum Zurücksetzen von Passwörtern.
  - ❑ zur Herstellung und/oder zum Herunterladen von (Sicherungs-) Kopien der Videoaufzeichnung.
  - ❑ zur Parametrierung automatischer Protokollierungsfunktionen.
  - ❑ zum Löschen von Systemprotokollen.
- Es ist möglich, nicht gewünschte Systemfunktionen (z.B. Alarme aufgrund von Bewegungsanalysen, eine automatische Gesichtserkennung, die Freigabe von Netzwerkschnittstellen oder das Herunterladen von Video-Daten auf mobile Datenträger) gänzlich zu sperren.
- Für einen effizienten Systembetrieb ist es nicht erforderlich, einem Benutzer (Administrator) allumfassende Systemberechtigungen einzuräumen.

Systemebene

- Das System ist so konfigurierbar, dass die auf der Applikationsebene festgelegten Zugriffsbeschränkungen nicht auf der Datenbank- oder Betriebssystemebene unterlaufen werden können.
- Das System ermöglicht, dass z.B. Revisionsinstanzen nur zum Lesen von Systemeinstellungen und Protokollen berechtigt sind, ohne irgendwelche Änderungen daran vornehmen zu können.
- Für bestimmte Benutzer kann man die Berechtigung zum Ansehen von Video-Aufzeichnungen auf die Aufzeichnungen der jeweils letzten x Stunden begrenzen.
- Über sicherheitsrelevante Ereignisse werden automatisch Vermerke in einer Protokolldatei abgelegt. Jeder Protokolleintrag enthält den Namen des Ereignisses, den Zeitpunkt seines Eintretens sowie die Kennung des veranlassenden Benutzers.
- Die maximale Größe des Protokolls ist durch das System möglichst nicht begrenzt. Die Protokolldatei kann jedenfalls die protokollierungsbedürftigen Ereignisse mindestens eines halben Jahres aufnehmen.

- Wie lange reicht das Log zurück, wenn - wie oben erwähnt - „sämtliche Aktivitäten, Störungen, Alarme, Zugriffe auf das System“ usw. einen Protokolleintrag auslösen?
- Das System verfügt über Funktionen zur gezielten Löschung ausgewählter Protokolleintragungen (Archive und Logdateien), die eine gewisse Speicherdauer überschritten haben. *Löschen bedeutet die endgültige Vernichtung der Daten.*
- Eine vollständige Dokumentation sämtlicher Systemfunktionen gehört zum Lieferumfang. Auch und gerade die Administrationsfunktionen (Parametrisierung des Systems/Customizing, Benutzer- und Berechtigungsverwaltung usw.) sind genau beschrieben, ebenso die Protokollierung und die Bedeutung der Protokolleintragungen.
- Für die Analyse der Protokolle stehen automatische Hilfsmittel bereit, wenigstens Such- und Sortierfunktionen. Alternativ können die Protokolle in einem für Bürosoftware lesbaren Format heruntergeladen werden.

Löschen von Videoaufzeichnungen

- Sämtliche Video-Aufzeichnungen können gelöscht werden.
- Auch eine gezielte Löschung beliebig abgegrenzter Ausschnitte aus einer Aufnahme ist möglich.
- Kann man auch einen zeitlich abgegrenzten Ausschnitt einer Aufzeichnung löschen - z.B. die Aufnahmen der Kamera 3 aus der Zeit vom 3.4.2015 8:00 Uhr bis zum 4.4.2015 18:00 Uhr?
- Automatische Löschung aller Aufzeichnungen, die ein gewisses Alter überschritten haben: die Aufbewahrungsdauer kann vom Betreiber mindestens tagesgenau frei gewählt werden, so dass z.B. täglich um 0:00 Uhr alle Aufzeichnungen gelöscht werden, die älter als 72 Stunden sind.
- Vorteilhaft wäre ebenfalls eine Funktion, mit Hilfe derer für die Aufzeichnungen an Wochenenden eine abweichende Löschfrist eingestellt werden könnte.
- Löschen bedeutet die endgültige Vernichtung der Daten, so dass die gelöschten Aufzeichnungen nicht mit System-Bordmitteln rekonstruiert werden können.
- Der Betreiber kann in Sonderfällen (z.B. zur Beweissicherung) Ausschnitte aus Videoaufzeichnungen vor der automatischen Löschung schützen, etwa durch Übertragen auf einen besonderen Datenträger. Die zu schützenden Ausschnitte können beliebig gewählt werden, so dass wirklich nur die jeweils relevanten Aufnahmen aufbewahrt werden.
- Bei manuellem Löschen sollte protokolliert werden, wer die Daten gelöscht hat. Die Angabe eines Grundes ist empfehlenswert.

Technische Maßnahmen

- Mehrstufiger Passwortschutz
- Individuell konfigurierbar für Live-Bilder und/oder Archivauswertung
- Frei konfigurierbare Benutzer- und Zugriffsrechte
- Frei konfigurierbares Spurmanagement zum Löschen und Aufzeichnen von Videobildern
- Frei konfigurierbare Privacy Zones für Live- und Archivbilder
- Manipulationsschutz der Bilder durch z.B. Prüfsummen, Wasserzeichen oder digitale Signatur
- Mindestens Vier-Augen-Prinzip
- Systemprotokollierung nicht löschbar bei Netzverlust oder Updates im System
- Gesamtsystem muss verbindliche Zeitangabe enthalten (z.B. über NTP)

BHE Bundesverband Sicherheitstechnik e.V., Feldstraße 28, 66904 Brücken, Tel.: 06386 9214-0, Fax: 06386 9214-99, info@bhe.de, www.bhe.de