ZVEI
Die Elektroindustrie

ZVEI | MERKBLATT

33011:2016-02

Sicherer Aufbau und Nutzung von IP-fähigen Videosystemen

Fachverband Sicherheit

Autoren

Manfred Bulle	Honeywell Security Deutschland
René Kiefer	Siemens
Uwe Kühlewind	Bosch Sicherheitssysteme
Lukas Linke	ZVEI
Marco Pompili	AXIS Communications
Jochen Sauer	AXIS Communications
Artur Schmidt	Securiton
Jochen Winter	Geutebrück
Stefan Wallner	Bosch Sicherheitssysteme

ZVEI:
Die Elektroindustrie

Impressum

Merkblatt
Sicherer Aufbau und Nutzung von IP-fähigen Videosystemen

Herausgeber:
ZVEI - Zentralverband Elektrotechnik- und Elektronikindustrie e. V.
Fachverband Sicherheit
Lyoner Straße 9
60528 Frankfurt am Main

Telefon: 069 6302-272
Fax: 069 6302-322
E-Mail: krapp@zvei.org
www.sicherheit.org

Verantwortlich:
Peter Krapp

Februar 2016

Bildnachweis Grafiken:

ZVEI	5
ZVEI, Einige Elemente: freepik+fotolia	8
ZVEI, Einige Elemente: freepik+fotolia	9
ZVEI	10
ZVEI, Einige Elemente: freepik+fotolia	12

Inhalt

1. Einleitung

Dieses Merkblatt soll helfen, den Aufbau eines Videosystems zu veranschaulichen, die darin befindlichen Schwachstellen und Angriffspunkte darzulegen und Anhaltspunkte für geeignete Maßnahmen anzuzeigen.

Der anhaltend dynamische technische Fortschritt treibt die globale Vernetzung und die daraus resultierenden verbesserten Prozesse, die Verfügbarkeit von Ressourcen und Know-how voran. Aber auf Optimierung ausgelegte Wirtschaftsprozesse sind vernetzt und daher anfällig für Störungen, gezielte Angriffe, technisches oder menschliches Versagen.

Eine moderne Videosystemlösung ist heute im Aufbau und in den Einzelkomponenten mit einer IT-Systemlösung vergleichbar. Sie besteht aus Hardware, Software, PCs und Betriebssystem, Servern und Datenbanken, Infrastruktur und Netzwerk. Datenschutz und Datensicherheit sind von zunehmender und großer Bedeutung, sowohl für die IT-Landschaft als auch für die Videosystemlandschaft.

Videotechnik ist heute aus unserem Alltag nicht mehr wegzudenken und kommt in immer mehr Anwendungsfällen zum Einsatz. Videobilder liefern eine Vielzahl konkreter Informationen und versetzen den Anwender in die Lage, bei Bedarf ziel- und aufwandsgerecht zu reagieren. Selbst präventive, vorausschauende und vermeidende Handlungen sind dank Videotechnik heute möglich.

Durch die IP-Vernetzung entstehen aber nicht nur zusätzliche Funktionalitäten und Vorteile, sondern auch Risiken. Da auch in IP-vernetzten Videosystemen alle Daten wie Videobilder, Audiodaten und Steuerbefehle über überwiegend standardisierte Datenpakete übertragen werden, nimmt bei Sicherheitsbetrachtungen die Datensicherheit eine zentrale Stellung ein.

Der Begriff „Datensicherheit“ beschreibt die Eigenschaften von informationsverarbeitenden Systemen, die die Vertraulichkeit, Verfügbarkeit und Integrität der Daten sicherstellen.

Nur wenn die Vertraulichkeit, Verfügbarkeit und Authentizität der Daten zu jedem Zeitpunkt gewährleistet ist, bleiben die Funktionalität des Videosystems und der Schutz vor böswilligen Angriffen erhalten. Schäden und Risiken werden dadurch vermieden oder minimiert.

Der Begriff „Datenschutz“ beschreibt den Schutz des Einzelnen vor Beeinträchtigungen seines Rechtes auf informationelle Selbstbestimmung, kraft dessen jeder Bürger grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten bestimmen darf (aus BVerfGE 65, 1).

Nicht zu verwechseln mit der Datensicherheit ist der Begriff „Datenschutz“. Bilddaten enthalten in der Regel Informationen, die einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. Sie können damit datenschutzrechtlichen Bestimmungen unterliegen, deren Grundlagen unter anderem im Grundgesetz, dem Bundesdatenschutzgesetz (BDSG) und in den Datenschutzgesetzen der Länder niedergelegt sind.

Die Frage, ob und welche Datenschutzbestimmungen beim Betrieb von Videosystemen zu beachten sind, ist stark von den unternehmensinternen Rahmenbedingungen vor Ort abhängig und kann deshalb nur vom Betreiber selbst beantwortet werden. Darüber hinaus sind konkrete Rechtsberatungen nach dem Rechtsdienstleistungsgesetz (RDG) nur einem kleinen Personenkreis – beispielsweise Rechtsanwälten vorbehalten. Sie dürfen beispielsweise nicht von Herstellern, Planern oder Errichtern von Videosystemen wahrgenommen werden. Grundsätzlich ist die Einbindung eines Datenschutzbeauftragten zu empfehlen.

Im vorliegenden Merkblatt wird deshalb auf datenschutzrechtliche Aspekte nicht weiter eingegangen.

Relevanz und Auswirkungen

Videosysteme haben sich durch den Fortschritt der Digitalisierung und der Vernetzung grundlegend gewandelt: von

- in sich geschlossenen Systemen mit Zugängen vor Ort über
- vernetzten, aber immer noch geschlossenen Systemen hin zu
- Videosystemen mit externen Zugängen über das Internet

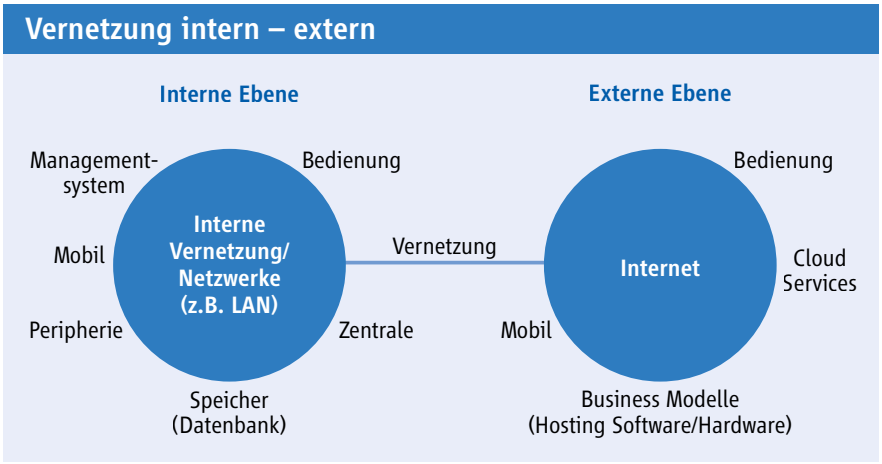

Abbildung 1

Zielsetzung und Aufgabenstellung

Künftig wird im Rahmen des Internet der Dinge die ständige und weltweite Verfügbarkeit von Videodaten möglich sein, was eine regelmäßige Sicherheitsüberprüfung erforderlich macht. Die zunehmende Vernetzung bedeutet auch, dass Systeme durch Angriffe und Manipulationen von innen und nun auch durch Externe gefährdet sein können. Folgerichtig wird auch in Normen und Richtlinien nicht mehr wie früher von „CCTV" (Closed Circuit Television), sondern allgemein von „VSS" (Video Surveillance Systems) gesprochen.

Zusätzlich haben sich die technischen Risiken verändert. Die zunehmende Intelligenz einzelner Komponenten (z. B. Speicher- und Analysefunktionen in Videokameras) kann durch die Vernetzung einen stärkeren Einfluss auf die Gesamtfunktionalität des Systems haben. Durch die schnellen Innovationszyklen der digitalen Welt kommt zunehmend auch eine dynamische Komponente ins Spiel. Was heute noch ein hohes Sicherheitsniveau darstellt, ist morgen bereits überwunden. Die Teilhabe am technischen Fortschritt steht dabei in einem ständigen Spannungsverhältnis zur Sicherstellung der technischen Funktionalität und Kompatibilität.

Durch die Vernetzung steigt auch die Anzahl der an Beschaffung und Betrieb beteiligten Vertragspartner und damit das juristische Risiko aus Verträgen und sich wandelnden gesetzlichen Rahmenbedingungen. Zu den beiden Vertragspartnern, die das System installieren und einsetzen, kommen in der vernetzten digitalen Welt Dienstleister, die Netzwerke, Internetfunktionalitäten, Rechenzentren oder Cloud-Dienste bereitstellen. Durch die zunehmende globale Bereitstellung dieser Dienstleistungen können die gesetzlichen Rahmenbedingungen und das Sicherheitsniveau in den entsprechenden Ländern zusätzliche Risiken bedeuten.

Bei allem technischen Fortschritt sind auch bei der Beschaffung und beim Betrieb von Videosystemen Menschen beteiligt, die Fehler begehen können – sei es aus Überlastung, Nachlässigkeit oder Absicht. Es liegt in der Verantwortung des Betreibers, derartige Risiken abzuschätzen und entsprechende Vorsorge zu treffen.

2. Mehrwert durch IP-Vernetzung in der Videotechnik

Die IP-Vernetzung ermöglicht einen globalen Zugriff auf das Videosystem. Dadurch werden u. a. Fernzugriffe einfacher, was einen wirtschaftlichen Betrieb und eine höhere Verfügbarkeit ermöglicht.

Grundsätzliche Vorteile der IP-Vernetzung sind:

- Globale Verfügbarkeit von Technik und Know How
- Globale Nutzung und Verfügbarkeit 24/7 – standortunabhängig
- Investitionssicherheit durch standardisierte Technik, Komponenten, Protokolle und Prozesse
- Durch IT-Standards und Normung kann die Integration mit anderen (Sicherheits-) Gewerken vereinfacht werden.

Neue Geschäfts- und Servicemodelle (z. B. Hosting-Modelle) sind durch IP-Vernetzung ebenso möglich wie eine Verbesserung der Qualität durch automatisierte Prozesse.

Die Normung als Grundlage für sichere und effiziente IP-vernetzte Systeme ist bei den Videosystemen weit fortgeschritten. Die Normenreihe DIN EN 62676 beschreibt ausführlich Anforderungen an die Systeme und die Datenübertragung in IP-vernetzten Videoüberwachungsanlagen in Sicherheitsanwendungen. Daraus resultierend lassen sich IP-basierte Videosysteme und Zutrittskontrollanlagen zum Beispiel mit Hilfe der Normenreihen DIN EN 50132, DIN EN 62676 und DIN EN 60839 herstellerunabhängig vernetzen. Die Industrieinitiative ONVIF fördert die sichere und einfache Vernetzung der Gewerke Video und Zutrittskontrolle. Weiterhin sind die Grundsätze der IT-Sicherheit zu beachten.

3. Systemdarstellung

Ein IP-vernetztes Videosystem besteht grundsätzlich aus Kameras, der Netzwerk-Infrastruktur, der Managementebene mit Controllern bzw. Computern und Systemen zur Datenspeicherung sowie mobilen und stationären Anzeigegeräten wie Computer- oder Videomonitoren, Tablets oder Smartphones. Jede Komponente besitzt unterschiedliche Eigenschaften, die unter Sicherheitsaspekten zu bewerten sind. (vgl. Abb. 2)

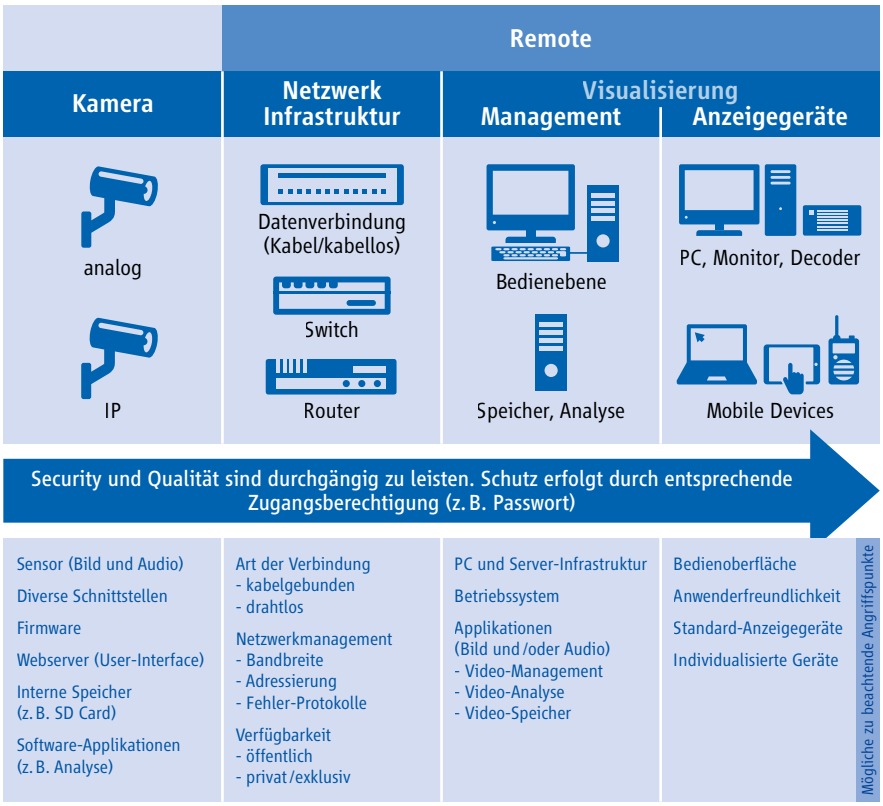

Abbildung 2:
Die Datensicherheit in IP-vernetzten Videosystemen ist durchgängig für jede Komponente zu gewährleisten

Mit wachsender Größe des Videosystems nehmen durch die steigende Anzahl an Komponenten zwangsläufig auch die Risiken insgesamt zu. Speziell die Datensicherheit ist jedoch unabhängig von der Systemgröße, denn ein einzelnes schwaches Element macht das ganze System angreifbar. Daher ist es unbedeutend, ob ein großes komplexes System oder nur ein Kleinstsystem betrachtet werden: Ist eine einzelne Komponente, beispielsweise eine Kamera, unzureichend geschützt, kann ein Angreifer eindringen, manipulieren, verfälschen, stehlen, stören oder spionieren. Er wird immer dort eindringen, wo es am einfachsten ist und am unwahrscheinlichsten, entdeckt zu werden (vgl. Abb. 2).

Durch die zunehmende Digitalisierung steigt dabei auch das Risiko von Angriffen durch sogenanntes „Social Engineering“. Damit werden sensible Daten wie Passwörter oder andere Zugangsdaten ausgespäht, beispielsweise durch Telefonanrufe oder fingierte E-Mails an Mitarbeiter. Insgesamt nimmt die Bedeutung einer ausreichenden Aufmerksamkeit der Mitarbeiter und des Betreibers zu, geeignete Regularien zu definieren, sei es beim Erkennen externer Angriffsversuche oder beim Verwenden sicherer Passwörter.

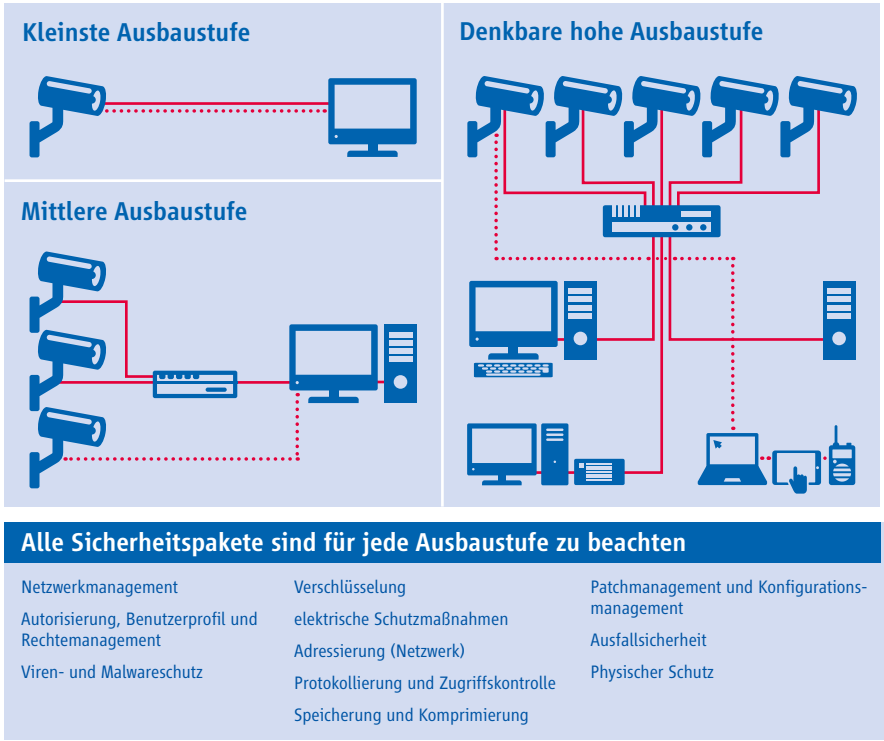

Abbildung 3:
Die Datensicherheit ist unabhängig von der Systemgröße. Bereits ein unzureichend geschütztes Element reicht aus, um die gesamte Anlage zu kompromittieren. Deshalb sind in jeder Ausbaustufe sämtliche Sicherheitsaspekte zu prüfen.

Videosysteme sind individuell auf die jeweilige Anwendung und die zu schützenden Objekte zugeschnitten und eng in die Organisationsabläufe des Betreibers eingebunden. Gerade IP-vernetzte Videosysteme bieten eine hohe Flexibilität, die Anlage passgenau und wirtschaftlich abzustimmen (vgl. Kap. 2). Genauso individuell wie die Anforderungen und Funktionalitäten sind jedoch auch die sich daraus ergebenden Risiken. Deshalb ist auch bei der Planung eines IP-basierten Videosystems möglichst frühzeitig eine Analyse der Anforderungen, Risiken und kritischen Unternehmensprozesse durchzuführen, um Schutzbedarf und Sicherheitsmaßnahmen bestimmen zu können. Nur so können die bei einer IP-Vernetzung notwendigen Schutzziele der Datensicherheit, Vertrauenswürdigkeit, Integrität und Verfügbarkeit erreicht werden. Dabei ist die Organisation ebenso wie die Technik zu bewerten, und auch der „Faktor Mensch“ muss mit berücksichtigt werden. Damit wird auch eine wirtschaftliche Umsetzung der Sicherheitsanforderungen erreicht. Anstatt alles auf maximaler Stufe abzusichern, werden nur die für die jeweilige Anwendung relevanten Risiken berücksichtigt (vgl. Abb. 4).

Sukzessiver Ablauf:

1. **Firewall für Netzwerk**
   Unterscheidung legitimierter und nicht legitimierter Zugriffsversuche
2. **Eindringversuche**
   Identifikation unauthorisierter Zugriffsversuche
3. **Firewall auf den vernetzten Geräten**
4. **„Secure Boot"**
   „White List" (Benutzer, Dienste, Programme)
5. **Software-Verschlüsselung**
   Verschlüsselung macht Daten-Diebstahl unattraktiv

Passwortmanagement

Gefährdung durch ...	Störung/Ausfall der technischen Funktionalität	Interne Risiken (z. B. Innentäter)	Externe Risiken (z. B. Hacker)
Maßnahmen	Netzwerkmnagement elektrische Schutzmaßnahmen Adressierung (Netzwerk) Speicherung und Komprimierung Physischer Schutz Ausfallsicherheit Patch- und Konfigurationsmanagement Hinweis: Patches können Verfügbarkeit beeinflußen Hinweis: Diagnosefähigkeiten wichtiger mit steigender Größe	Netzwerkmnagement Autorisierung, Benutzer-, Profil- und Rechtemanagement Viren- und Malwareschutz Verschlüsserung Protokollierung und Zugriffskontrolle Speicherung und Komprimierung Physischer Schutz Ausfallsicherheit	Netzwerkmnagement Autorisierung, Benutzer-, Profil- und Rechtemanagement Viren- und Malwareschutz Verschlüsserung Protokollierung und Zugriffskontrolle Speicherung und Komprimierung Ausfallsicherheit Übertragungsweg

Abbildung 4:
Die Sicherheit in IP-vernetzten Videosystemen lässt sich individuell und damit wirtschaftlich realisieren

Sicherheit im Allgemeinen und Datensicherheit im Besonderen sind dabei nicht nur einmalig bei Planung und Errichtung eines Videosystems zu berücksichtigen, sondern sind als Sicherheitskette im Lebenszyklus zu verstehen. Entsprechend fließen Sicherheitsbetrachtungen auch bei Erweiterungen oder Nutzungsänderungen in die Planung ein. Jede Änderung kann neue Risiken, in vernetzten Systemen unter Umständen mit Rückwirkungen auf bestehende Komponenten bedeuten. Die Qualität der Sicherheitskette wird durch die Auswahl der Geräte bestimmt. Diese müssen den natürlichen, rauen Witterungsbedingungen standhalten, energieeffizient sowie verlässlich arbeiten und wartungsfreundlich installiert sein. Die Geräte müssen wiederum von fachkundigen Errichtern und Integratoren installiert und anwendungsgerecht durch die Betreiber bedient werden, damit sie ihr Leistungsprofil erbringen können. Die Qualität und die Betriebsbereitschaft des Videosystems kann dabei nur durch regelmäßige, fachgerechte Wartung gemäß des vereinbarten Wartungsvertrages auf dem ursprünglichen Niveau gehalten werden.

Bei IP-vernetzten Videosystemen nimmt die Bedeutung der von den Herstellern angebotenen „Services“ deutlich zu. Im Unterschied und in Ergänzung zur Wartung optimieren die Services Videosysteme bedarfsgerecht und proaktiv. Die Optimierungen umfassen beispielsweise Aktualisierungen (Updates) sowie Erweiterungen (Upgrades) des technischen Leistungsprofils und passen das System so dem aktuellen technischen Stand an. Das ist bei IP-vernetzten Systemen besonders wichtig, da sich durch die kurzen Innovationszyklen der IT-Welt als sicher geltende Konzepte bereits nach kurzer Zeit als angreifbar erweisen und zusätzliche Maßnahmen erfordern können.

Ohne regelmäßige Services kann ein fachgerecht geplantes und betriebenes IP-vernetztes Videosystem bereits nach kurzer Zeit vollständig kompromittiert und damit unbrauchbar werden. Betreiber von Videosystemen stehen deshalb besonders in der Verantwortung, ihre Anlage stets auf dem aktuellen Stand zu halten. Dabei ist auch die Entscheidung zu treffen, ob die dazu notwendige (IT-) Kompetenz im eigenen Hause vorgehalten wird oder an externe Dienstleister vergeben wird.

4. Zu beachtende Sicherheitsaspekte der Vernetzung

Der zunehmende Grad der Vernetzung erhöht prinzipiell die Risiken, so dass zusätzliche Maßnahmen zur Absicherung getroffen werden müssen. Diese Herausforderung kommt sowohl auf Hersteller, Planer und Errichter als auch Betreiber und Nutzer zu. Die Sicherheit hängt dabei nicht zwingend von der Systemgröße ab (vgl. Kap. 3). So führt eine hohe Anzahl von Kameras nicht unbedingt zu einer erhöhten Angreifbarkeit. Eine weiträumige Vernetzung über eine physisch geschützte Liegenschaft hinaus bietet dagegen zusätzliche Angriffspunkte. Ist die Übertragungsstrecke privat und wird exklusiv für die Videoübertragung genutzt, erfordert sie die geringsten zusätzlichen Maßnahmen. Wird aber öffentlich z. B. über das Internet übertragen, sind zusätzliche Sicherheitsmaßnahmen notwendig. Das Management des Netzwerkes ist deshalb essentieller Bestandteil der Sicherungsstrategie.

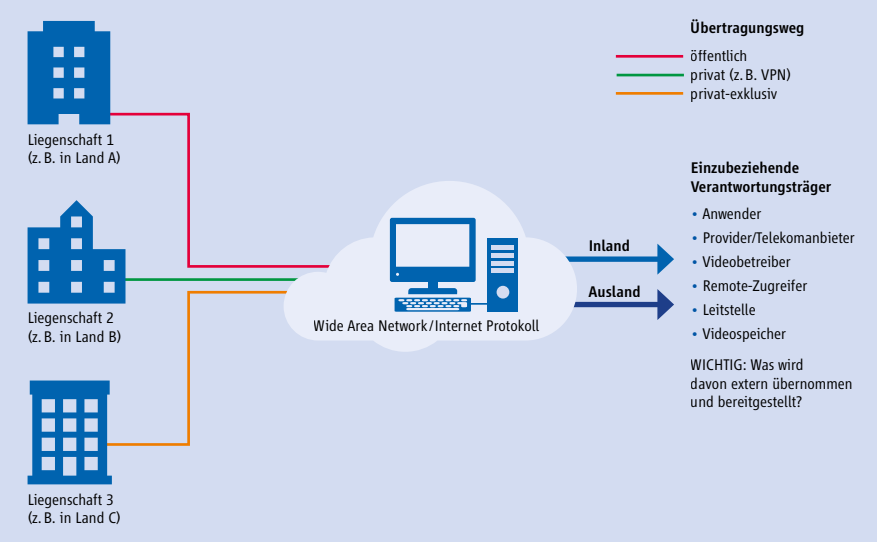

Abbildung 5:
Die Übertragung, Verarbeitung und Speicherung von Videodaten außerhalb der Server der Betreiber erfordert besondere Sicherheitsmaßnahmen.

Zu beachten ist, dass bei zunehmender weiträumiger Vernetzung – auch innerhalb Deutschlands – in der Regel mehrere Anbieter (Provider) die nötigen Kommunikationsinfrastrukturen wie beispielsweise Internetzugänge bereitstellen. Das kann zu erhöhten technischen Risiken führen, da der Betreiber keine Kontrolle mehr über die Infrastrukturen besitzt und ein erhöhtes Ausfallrisiko die Folge sein kann. Ebenso wenig hat der Betreiber die Datensicherheit in den externen Kommunikationsstrukturen unter Kontrolle und muss sich auf die zugesicherten Eigenschaften des Dienstleisters verlassen. Daher sollte eine Qualitätsvereinbarung mit dem Provider geschlossen werden.

Insbesondere bei einer Vernetzung über Landesgrenzen und/oder eine zentralen Datenverarbeitung/-speicherung außer Landes sind besondere Überlegungen und Maßnahmen erforderlich. Bei Nutzung von Dienstleistungen über Landesgrenzen hinweg müssen entstehende technische und juristische Anforderungen als auch zusätzliche Angriffsvektoren berücksichtigt werden, denn Übertragung, Verarbeitung bzw. Speicherung der Daten unterliegen zuerst einmal den Rechtsvorschriften des Landes, in dem sie stattfinden. Die Anforderungen an Datensicherheit und Datenschutz unterscheiden sich in den einzelnen Ländern zum Teil erheblich. Das IT-Sicherheitsgesetz unterscheidet je nach Anwendung zwischen einer Speicherung der Daten in Deutschland, im Schengen-Raum und im übrigen Ausland.

Der sorgfältigen Auswahl vertrauenswürdiger Dienstleister und der detaillierten Prüfung ihrer Sicherheits- und Datenschutzkonzepte sowie dem Einsatz geeigneter Sicherungsmaßnahmen (zum Beispiel Verschlüsselung der Daten) durch den Betreiber kommt deshalb bei IP-vernetzten Videosystemen eine besondere Bedeutung zu.

5. Zusammenfassung und Ausblick

Die IP-Vernetzung von Videosystemen bietet Betreibern und Anwendern eine höhere Flexibilität, zusätzliche Funktionalitäten und erweiterte Anwendungsmöglichkeiten sowie eine verbesserte Wirtschaftlichkeit.

Gleichzeitig steigen die Anforderungen an die Systemsicherheit. Deshalb ist die Auswahl kompetenter Partner im gesamten Prozessverlauf von der Planung über die Errichtung bis zum Betrieb und den Service sowie die Prüfung der Sicherheitskonzepte durch den Betreiber der Videosysteme dringend zu empfehlen.

Der ZVEI-Fachkreis Videosysteme unterstützt diese Entwicklung. Denn die IP-Vernetzung von Videosystemen mit anderen Gewerken der Sicherheits- und Gebäudetechnik (und darüber hinaus z. B. Social Media, Assistenzsysteme in der Automobiltechnologie, etc.) schafft einen erheblichen zusätzlichen Mehrwert. Naheliegend ist daher die Erstellung praktisch anwendbarer Normen und Richtlinien zur Vernetzung, um Herstellern und Betreibern, Planern und Errichtern eine zuverlässige Arbeitsgrundlage an die Hand zu geben.

Über den ZVEI

Der ZVEI - Zentralverband Elektrotechnik- und Elektronikindustrie e. V. vertritt die gemeinsamen Interessen der Elektroindustrie und der zugehörigen Dienstleistungsunternehmen in Deutschland. Rund 1.600 Unternehmen haben sich für die Mitgliedschaft im ZVEI entschieden. Die Branche beschäftigt in Deutschland über 849.000 Arbeitnehmer und weitere 690.000 weltweit. Der ZVEI repräsentiert eine Branche mit 172 Milliarden Euro Umsatz im Jahr 2014. Etwa 40 Prozent davon entfallen auf neuartige Produkte und Systeme. Jede dritte Neuerung im Verarbeitenden Gewerbe insgesamt erfährt ihren originären Anstoß aus der Elektroindustrie.

ZVEI - Zentralverband Elektrotechnik-
und Elektronikindustrie e. V.
Lyoner Straße 9
60528 Frankfurt am Main

Telefon: 069 6302-0
Fax: 069 6302-317
E-Mail: zvei@zvei.org
www.zvei.org